ABISHANKA SAHA

MIRROR THEORY AND ITS APPLICATIONS IN CRYPTOGRAPHY

MIRROR THEORY AND ITS APPLICATIONS IN CRYPTOGRAPHY

ABISHANKA SAHA

Dissertation written towards fulfillment of
Doctorate of Philosophy in Computer Science

Under the supervision of
PROF. DR. MRIDUL NANDI

Applied Statistics Unit
Indian Statistical Institute

To my wife and best friend, Boomlee.

ABSTRACT

The indistinguishability security of a cryptographic construction refers to the maximum advantage of an interactive adversary to distinguish between the real and ideal world, where in the real world it interacts with the construction, and in the ideal world it interacts with its idealized counterpart. In the field of information-theoretic provable security, we bound this indistinguishability advantage by the statistical distance between the random variables representing the transcript of interaction in the real and ideal worlds, respectively. One of the most popular techniques in bounding the statistical distance is the H-Coefficient Technique introduced by J. Patarin, for which a set of transcripts is identified as good, and the probability of realizing such a good transcript in the real world is lower-bounded. For numerous constructions in practice, lower-bounding this real-world interpolation probability reduces to lower-bounding the number of solutions to a system of equations and non-equations over a field. The theory of achieving optimum lower bounds to a system of equations and non-equations is termed Mirror Theory by J. Patarin. Although several Mirror Theory statements have been conjectured and profusely used in beyond-birthday bound analysis of a multitude of constructions, the proofs of such statements are either non-existent or at least have significant non-verifiable gaps.

In this thesis, we have presented the first simple verifiable proofs of several variants of Mirror Theory and applied them to security analyses of various cryptographic schemes.

As our first contribution, we proved that the number of pairwise disjoint solutions to a system of bivariate equations over n-bit variables, such that no two equations share any common variable, is at least the average number of such solutions. This translates via the H-coefficient technique to the n-bit security for the sum of permutations PRF constructions.

As our second contribution, we show that the number of pairwise disjoint solutions to a system of bivariate equations over n-bit variables, which even has quite a large block-maximality, is at least the average number of such solutions. Here block-maximality of a system of equations refers to the maximum number of variables that get determined when one variable is assigned a particular value. Note that, in our previous simpler result the block-maximality was just two. This translates via the H-coefficient technique to the n-bit security for several PRF constructions, like XORP[w], 2k-HtmB-p2, and the PRP construction, six-round Feistel network.

As our third contribution, we have used a Mirror Theory statement in the tweakable permutation setting, where the variables are partitioned into two sets and solutions need to be pairwise disjoint within the two sets only, to prove 3n/4-bit security of the tweakable blockcipher construction paradigm, LRW+, proposed by us, that includes as subcases the CLRW2 and 4LRW1 constructions proposed in the seminal paper of Liskov, Rivest, and Wagner. The LRW+ paradigm was proposed to achieve beyond-birthday-bound security, as we have given a birthday-bound attack on the TNT or 3LRW1 construction, disproving the long-held belief that the latter is beyond-birthday-bound tweakable blockcipher.

Finally, as our fourth contribution, we have given a lower bound to the number of solutions (which are pairwise disjoint within a partition of the variables) to a system of equations (need not be bivariate) where the solutions are not allowed to take values in certain forbidden sets. We have used this variant of Mirror Theory to prove optimal 3n/4-security of single key variants of double-block-hash-then-sum MAC constructions, like 1k-LightMAC+, 1k-PMAC+, and the PRF construction, sum of k Even-Mansour.

Several of the security proofs mentioned above are indeed tight.

PUBLICATIONS

[CDNPS23] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and **Abishanka Saha**. "Proof of Mirror Theory for a Wide Range of $\xi _{\max }$." In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 470–501. DOI: 10.1007/978-3-031-30634-1_16. URL: https://doi.org/10.1007/978-3-031-30634-1_16.

[CEJNS24] Benoît Cogliati, Jordan Ethan, Ashwin Jha, Mridul Nandi, and **Abishanka Saha**. *On the Number of Restricted Solutions to Constrained Systems and their Applications*. Cryptology ePrint Archive, Paper 2024/1163. https://eprint.iacr.org/2024/1163. 2024. URL: https://eprint.iacr.org/2024/1163.

[DNS22] Avijit Dutta, Mridul Nandi, and **Abishanka Saha**. "Proof of Mirror Theory for $\xi_{\max} = 2$." In: *IEEE Trans. Inf. Theory* 68.9 (2022), pp. 6218–6232. DOI: 10.1109/TIT.2022.3171178. URL: https://doi.org/10.1109/TIT.2022.3171178.

[JKNS24] Ashwin Jha, Mustafa Khairallah, Mridul Nandi, and **Abishanka Saha**. "Tight Security of TNT and Beyond - Attacks, Proofs and Possibilities for the Cascaded LRW Paradigm." In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I*. Ed. by Marc Joye and Gregor Leander. Vol. 14651. Lecture Notes in Computer Science. Springer, 2024, pp. 249–279. DOI: 10.1007/978-3-031-58716-0_9. URL: https://doi.org/10.1007/978-3-031-58716-0_9.

It is easy to acknowledge, but almost impossible to realize for long, that we are mirrors whose brightness, if we are bright, is wholly derived from the sun that shines upon us. — C. S. Lewis

ACKNOWLEDGMENTS

This dissertation is not the result of an individual endeavor but rather a cumulative effort of many people who have supported, guided, and inspired me throughout my journey. It reflects the collaborative spirit, encouragement, and invaluable contributions of mentors, colleagues, friends, and family, without whom this work would not have been possible.

I am profoundly grateful to my supervisor, Dr. Mridul Nandi, whose guidance and mentorship have been pivotal in shaping this thesis. His ability to come up with ingenious ideas and his mathematical brilliance have been nothing short of inspiring. Dr. Nandi is the living genius that I have had the privilege of knowing, and witnessing his dedication to research has left a lasting impression on me. His support and insights have been invaluable throughout my academic journey, and I am deeply thankful for his patience and encouragement.

I would also like to express my gratitude to Ashwin da for his immense support and for the long discussions that have greatly clarified my understanding of the provable security landscape. My heartfelt thanks go to my co-authors, especially Benoît Cogliati, Jacques Patarin, and Mustafa Khairallah. I am inspired by the work ethic of Benoît and Mustafa. I am grateful for having met such a mathematical heavyweight as Jacques. I also want to acknowledge Ritam da and Avijit da for their encouragement and collaboration.

I am very grateful to Dr. Gregor Leander for hosting me at Ruhr Universität Bochum for a two-month internship, having expository discussions on the crossroads between cryptanalysis and provable security.

My batchmates Santy da, Chandranan and Debasmita, and seniors such as Mama, Anik da, Suprita and Anondorup da, have made this journey memorable with their camaraderie and support. I am especially grateful to Soumit for standing by me through a remarkably challenging financial process, and to Chandranan for keeping me informed about the numerous bureaucratic aspects of research at ISI. Although it sounds dry, I cannot be thankful enough for such large favours.

I would like to thank my college friends Indranil, Mamba, Chowdhury, and Saagnik for growing up with me during the five years of our bachelor's and master's degrees. I would also like to mention my newer and even dearer friends Mou, Arundhati, Tuhin, Madhubanti, Smiha, Debarati, Sayan, Arijit, Sriya, Ala, who have been a boost of positive influence in my life. Your friendship and support have been invaluable and unforgettable.

I am deeply indebted to my family for their unwavering support. My mother, Prof. Babli Saha, instilled in me the love for mathematics and the enthusiasm to pursue it, which

might have led to this research career. My father, Nitai Chandra Saha, has always been the go-to guy for every little problem I had. Also, I am especially grateful to my little Bhai, who I forget is not so little anymore, for being the lovely brother that he is and for being my constant partner in crime. I am also grateful to my parents-in-law, Kaku and Kakima, and sister-in-law, Puchurani, for warmly welcoming me into their family, sharing with me their library of books, encouraging me with my work, and for being a constant source of appreciation and reassurance during times I needed them most.

And finally, my wife, Anasua, for whom nothing I say will be enough. Pursuing PhD is the getaway to research life, and the first steps are always a little shaky. The life of a scholar consists of long periods of draughts, when paper gets rejected time and again, when you don't find the proper motivation to work, when your supervisor is not at all happy with you, interspersed with the very occasional paper acceptance and appreciation. This might be mentally challenging for some people to handle, but it can never get to me, since I can always feel at peace knowing that I am the luckiest guy to have Anasua in my life, whom I can go to with my endless anxieties and she can just resolve them like Master Oogway.

CONTENTS

;

NOTATION : WHAT IT DENOTES

Sets, Tuples, & Multisets.	$\{\cdot\}$	:	A set is a collection of distinct objects. It is sometimes denoted as the enlisting of its elements enclosed by braces, $\{\cdot\}$.
	$(\cdot)$	:	A tuple is a sequence or ordered list of elements. It is denoted by the ordered enlisting of its elements enclosed by parentheses, $(\cdot)$.
	$\{\!\{\cdot\}\!\}$	:	A multiset is a modification of the concept of a set that, unlike a set, allows for multiple instances for each of its elements. It is denoted by an enlisting of its elements enclosed by double braces, $\{\!\{\cdot\}\!\}$.
	$[n]$	:	The set $\{1, 2, \ldots, n\}$, defined for any $n \in \mathbb{N}$.
	$[a, b]$	:	The set $\{a, a+1, \ldots, b\}$, defined for $a, b \in \mathbb{N}, a < b$. Thus $[1, n] = [n]$ are equivalent notations.
	$\lvert\mathscr{X}\rvert$	:	Number of elements in the set $\mathscr{X}$.
	x^q	:	The ordered q-tuple $(x_1, \ldots, x_q)$.
	$x^{[a,b]}$	:	The ordered $(b-a+1)$-tuple $(x_a, x_{a+1}, \ldots, x_b)$
	$x^{\sigma[q]}$	:	For any permutation $\sigma : [q] \to [q]$, $x^{\sigma[q]}$ denotes the reordered tuple $(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma q})$.
	$x^q \| x$	:	The ordered $(q+1)$-tuple $(x_1, \ldots, x_q, x)$.
	$\mathbb{1}_v(i, j)$	:	The binary $v \times 1$ vector whose i-th and j-th bits are 1, and the rest of the bits are 0.
	$x^{\{q\}}$	:	The set containing the distinct elements in the q-tuple $(x_1, \ldots, x_q)$.
	$x^{\{\!\{q\}\!\}}$	:	The multiset $\{\!\{x_1, \ldots, x_q\}\!\}$
	$\mathscr{X}^q$	:	The set of all ordered tuples $x^q = (x_1, \ldots, x_q) : x_i \in \mathscr{X}, i \in [q]$. We have $\lvert\mathscr{X}^q\rvert = \lvert\mathscr{X}\rvert^q$
	$\mathscr{X}^{q*}$	:	The set of all ordered tuples $x^q = (x_1, \ldots, x_q) : x_i \in \mathscr{X}, x_i \neq x_j$ for distinct $i, j \in [q]$.
	$\mathscr{X}^{\{q\}}$	:	The collection of all subsets of $\mathscr{X}$, of size q.

	$\mathscr{X}^{\{\!\{q\}\!\}}$	:	The collection of all multisets of q elements (counting duplicates) of $\mathscr{X}$.
Functions.	$\mathsf{Func}(\mathscr{X}, \mathscr{Y})$	:	The set of all functions $f : \mathscr{X} \to \mathscr{Y}$. A function can alternatively be thought of as a subset of $\mathscr{X} \times \mathscr{Y}$ such that for any pairs $(x, y), (x', y') \in f$, $x_1 = x_2 \implies y_1 = y_2$.
	$\mathsf{Perm}(\mathscr{X})$	:	The set of all permutations $p : \mathscr{X} \to \mathscr{X}$. $\mathsf{Perm}(\mathscr{X}) \subset \mathsf{Func}(\mathscr{X}, \mathscr{X})$. A permutation can alternatively be thought of as a subset of $\mathscr{X} \times \mathscr{Y}$ such that for any pairs $(x, y), (x', y') \in p$, $x_1 = x_2 \iff y_1 = y_2$.
	$\widetilde{\mathsf{Perm}}(\mathscr{T}, \mathscr{X})$	:	Alternatively, $\mathsf{Func}(\mathscr{T}, \mathsf{Perm}(\mathscr{X}))$ is the collection of all tweakble permutations with tweak space $\mathscr{T}$ and domain $\mathscr{X}$. For $\widetilde{p} \in \widetilde{\mathsf{Perm}}(\mathscr{T}, \mathscr{X})$ and any $t \in \mathscr{T}$, $\widetilde{p}(t) \in \mathsf{Perm}(\mathscr{X})$ is a permutation on $\mathscr{X}$.
Consistency of Tuples.	$x^q \mapsto y^q$	:	This denotes that the pair of tuples $(x^q, y^q) \in \mathscr{X}^q \times \mathscr{Y}^q$ is *function consistent*, i. e., there exists a function $f \in \mathsf{Func}(\mathscr{X}, \mathscr{Y})$ such that $f(x_i) = y_i \ \forall i \in [q]$. This can be equivalently stated as: for $i, j \in [q]$, $x_i = x_j \implies y_i = y_j$.
	$x^q \leftrightarrow y^q$	:	This denotes that the pair of tuples $(x^q, y^q) \in \mathscr{X}^q \times \mathscr{X}^q$ is *permutation consistent*, i. e., there exists a permutation $p \in \mathsf{Perm}(\mathscr{X})$ such that $p(x_i) = y_i \ \forall i \in [q]$. This can be equivalently stated as: for $i, j \in [q]$, $x_i = x_j \iff y_i = y_j$.
	$x^q \overset{t^q}{\leftrightarrow} y^q$	:	This denotes that the triplet of tuples $(t^q, x^q, y^q) \in \mathscr{T}^q \times \mathscr{X}^q \times \mathscr{Y}^q$ is *tweakable permutation compatible*, i. e., there exists a tweakable permutation $\widetilde{p} \in \widetilde{\mathsf{Perm}}(\mathscr{T}, \mathscr{X})$ such that $\widetilde{p}(t_i, x_i) = y_i \ \forall i \in [q]$. We can equivalently restate this condition as: $(t_i, x_i) = (t_j, x_j) \iff (t_i, y_i) = (t_j, y_j)$. Note that the tweakable permutation consistency of the tuples can be equivalently denoted as $(t^q, x^q) \leftrightarrow (t^q, y^q)$.
Labeled Graphs.	$\mathscr{G} = (V, E, L)$	:	The labeled undirected graph with vertex set $\mathscr{V}$, edge set $\mathscr{E} \subseteq \mathscr{V}^{\{2\}}$, and the edge labelling function $L : \mathscr{E} \to \mathscr{L}$, for some label set $\mathscr{L}$.
	$u \overset{\ell}{\text{——}} v$	:	The labeled edge between vertices u and v having label ℓ.

Fonts.	$\mathscr{A}, \mathscr{B}, \ldots$	:	We will use capital letters in script typeface font to label sets.
	$\Lambda, \Gamma, \cdots$	:	We will use capital greek letters λ and γ to denote multi-sets.
	$\boldsymbol{\lambda}, \boldsymbol{\gamma}, \cdots$	:	We will use bold greek letters $\boldsymbol{\lambda}$ and $\boldsymbol{\gamma}$ to denote a typical sent belonging to the multiset Λ or Γ, respectively.
	$\lambda, \gamma, \cdots$	:	We will use normal greek letters λ and γ to denote the elements of the set $\boldsymbol{\lambda}$ and $\boldsymbol{\gamma}$, respectively.

Part I

FOUNDATIONS

In the first two chapters we present the basic tenets of symmetric key cryptography and describe some useful cryptographic primitives.

1 INTRODUCTION

Solving systems of equations is a cornerstone of modern computational tasks, deeply embedded in numerous scientific, engineering, and technological applications. Its significance lies in the broad impact it has across various fields: nuclear simulations in physics, linear programming in operations research, backpropagation in neural networks, finding maximum flow in network theory, protein structure prediction in computational biology, econometric modeling and risk management in finance. A linear system of equations is typically solved using the polynomial-time Gaussian elimination algorithms or its more efficient versions. The situation does get much more complicated if we introduce non-linearity, for example, even with only degree two equations, the Multivariate Quadratic problem is NP-complete over any field!

In this dissertation we will deal only with linear systems of equations, however, with quite a non-traditional twist: we will consider systems of equations *and* non-equations. What we mean by a *non-equation* here is basically this: it specifies that a certain linear combination of variables is not equal to a particular constant, e. g., $a\mathsf{X} + b\mathsf{Y} \neq c$. There are no generic results till date, even about the *exact* number of solutions to a system of equations and non-equations. Jacques Patarin introduced the study of *lower bounds* to the number of solutions to a system of equations and non-equations, motivated by the *beyond birthday bound security proofs of cryptographic schemes*, more on this later. He coined the term *Mirror Theory* [Pat10a] for this class of combinatorial problems, which, according to him, is inspired by the visual similarity of the inductive properties of the number of solutions of such systems and the recursive pattern of mirror images.

The study of finding lower bounds to a system of equations and non-equations seems very general in scope and very open-ended about its end-results. Before delving into the intricate details of Mirror Theory, it is essential to elucidate why this problem merits our interest and how it relates to practical, real-world applications. To understand why the implications of this theoretical exploration goes far beyond the abstract, we look into the field of cryptography.

1.1 THE SAGA OF CRYPTOGRAPHY

Cryptography, the art and science of "writing (greek: *graphein*) securely (greek: *kryptòs*)", has a storied history that spans millennia. From its early uses in ancient civilizations to its

pivotal role in the digital age, cryptography has continually adapted to meet the demands of increasingly complex communication networks.

EARLY HISTORY OF CRYPTOGRAPHY. The earliest forms of cryptography date back to ancient Egypt, where hieroglyphs were used to obfuscate messages. The Greeks utilized the scytale, a tool that helped encode messages by transposing letters. Julius Caesar introduced the Caesar cipher, a substitution cipher that shifted letters by a fixed number of positions, enabling secure communication with his generals. The Vigenère cipher, invented in the 16th century, used a *keyword* to shift letters, significantly increasing the complexity of the cipher and making it more resistant to frequency analysis.

THE ADVENT OF MODERN CRYPTOGRAPHY. The field of cryptography underwent a profound transformation in the 20th century, particularly around World War II. The groundbreaking paper, "Communication Theory of Secrecy Systems", by Claude Shannon [Sha49], laid the foundation for modern cryptographic theory. In this seminal paper, Shannon introduced the concept of entropy as a measure of uncertainty or randomness in a system. Entropy, in the context of information theory, quantifies the unpredictability of a message or the information content. Shannon demonstrated that the security of an encryption system is intrinsically linked to the entropy of the key used for encryption. This gave cryptography the mathematical footing it needed. Shannon defined perfect secrecy as a situation where the ciphertext provides *no information* about the plaintext. For an encryption system to achieve perfect secrecy, the entropy of the key must be at least as large as the entropy of the message.

Until 1976, the field of cryptography is limited to *symmetric-key cryptography*, where both the encryption of messages and decryption of ciphertexts were done using the *same* key. Thus the prevalent cryptographic schemes necessitated that the parties exchanging messages should share a *common secret key*, and such a sharing requires a secure channel. Thus perfect secrecy, where you need larger keys than messages, turns out to be too impractical a goal to pursue. There were two apparent way-outs: remove the need of sharing the same secret key, or come up with a more practical notion of security.

A pivotal moment in cryptography came in 1976 with the publication of "New Directions in Cryptography" by Diffie and Hellman [DH76], which introduced the concept of public-key cryptography, by proposing a cryptographic system where each user has a pair of keys: a *public* key, which can be shared openly, and used by others to encrypt the messages they want to send to the user, and a *private* key, which is kept secret, used to decrypt the sent ciphertexts. Although this solved the key distribution problem, it turns out that public-key algorithms are computationally more intensive than symmetric-key algorithms, and hence is more expensive when applied to very large amounts of data. The hybrid workaround is to use public-key cryptography for the secret key exchange and then using symmetric cryptography with the shared key for communication.

On the other hand, the search for a more practical approach than perfect secrecy led to the concept of *computational* security, where the goal is to make it computationally infeasible for an adversary to break the cryptographic system. Thinking in the abstract, the ciphertext is a 'scrambled' version of the message, created by 'adding' to the message the randomness/entropy of the key. The idea is to assume certain bounds to the adversary's resources like time, memory, etc. (which is not that unreasonable), and the goal is to make the scrambling look as close to random as possible, in the adversary's constrained 'view'.

Goldwasser and Micali, in their seminal paper, "Probabilistic Encryption & how to play mental poker keeping secret all partial information" [GM82] (with a later improvisation [GM84]), introduced the notion of semantic security, where the underlying model is an interactive game between an adversary and a challenger. This formalized the above thought process in the following manner: the adversary has oracle access to the challenger, that is it can make queries and receive corresponding responses from the latter. The challenger has two systems, the cryptographic scheme and a randomized counterpart of the scheme, that has all the true randomness properties, the computational versions of which we want our scheme to have. The challenger secretly tosses a coin and chooses which of the two systems it is going to use for the interaction. The adversary sends several queries to the challenger and the challenger sends back the output of the system chosen by him, on input the received query. Based on the transcript of this interaction, which comprises of the query-response pairs thus collected, the adversary has to make a binary guess about which of the two systems the challenger has chosen secretly. The challenger is a stateful probabilistic algorithm, where the state in which the challenger chooses the cryptographic scheme is called the *real world*, and the state in which it chooses the idealized counterpart is called the *ideal world*. The advantage of the adversary in breaking the claimed security property of the scheme, is then any quantifier of how better the adversary is at guessing correctly than just guessing randomly. The conventional practice is to take as the quantifier the *statistical distance* between the probability distributions of the transcripts generated in the two worlds. This formalization is a slight modification of the one presented in [GM82], we have reshaped it for the purpose of this dissertation.

Note that the above definition of security is not specific to any particular cryptographic goal like encryption. Thus we have a paradigm shift where we can formulate any cryptographic randomness property, and check whether a scheme has said property, by finding the advantage of any adversary, having the assumed bound on its resources, in distinguishing between the real and ideal worlds. Thus the scope of cryptographic goals has expanded to address a wide range of security requirements like confidentiality, integrity, authenticity, unforgeability, etc. We give a probabilistic function model (borrowed from [JN22]) for the above interactive algorithms and give concrete definitions of security in Chapter 2.

WORKHORSES OF SYMMETRIC KEY-CRYPTOGRAPHY. Three very fundamental notions at the core of symmetric key cryptography are the notions of a pseudorandom function (PRF), a (strong) pseudorandom permutation ((S)PRP), a tweakable (strong) pseudorandom permutation (T(S)PRP), where the names suggest the idealized counterparts being random function, random permutation, and random tweakable permutation, respectively. Candidates of the above notions are actively used as building blocks for various cryptographic schemes: PRFs are used in designing message authentication codes (MAC), key derivation functions (KDF), authenticated encryption (AE), signatures, pseudorandom generators (PRG); PRPs in blockciphers, which is a very fundamental cryptographic primitive itself; TPRPs in authenticated encryption with associated data (AEAD) schemes, etc. Later in this dissertation, we will take certain candidates for PRF, PRP and TPRP, and 'prove' their respective security. Note that a function (which we assume is not bijective in general) can be only forward-queried, whereas a permutation or tweakable permutation can be reverse-queried too, since it has an inverse. When an adversary only makes forward queries, we call it a *chosen-plaintext-attack* (CPA), and the constructions secure from such attacks are called *CPA-secure*: for a function, we will call it a secure PRF, for a permutation we will call it a secure PRP, and for a tweakable permutation a secure TPRP. On the other hand, when the adversary can make both forward and backward queries, we call it a *chosen-ciphertext-attack* (CCA), and constructions secure from such attack *CCA-secure*: for a permutation, we call it a strongly secure PRP (in short SPRP), and for tweakable permutation, we call it strongly secure TPRP (in short TSPRP).

PROVABLE SECURITY. In general, a symmetric-key scheme consists of two main components:

- Underlying *primitives*, such as the pseudorandom permutation AES (Adavnced Encryption Standard) [Nat01], that works on short and fixed-length inputs.
- A suitable *mode of operation*, that produces a desired functionality from the underlying primitives, e.g. the XOR_2 PRF construction [BI99], that xors the two underlying independent PRPs.

The typical method for proving the computational security of a symmetric-key scheme involves two steps:

- Replacing the underlying primitives with suitable ideal counterparts. For example, two independent instances of AES is replaced with two independent uniform random permutations π_1 and π_2. This step relies on the computational indistinguishability of the underlying primitive with respect to the ideal object. This approach is generally heuristic and often depends on the confidence in a particular primitive. For example, AES is considered a good PRP, as it has been extensively analyzed over a long period.
- Proving the security of the mode of operation using this ideal primitive. For example, $\mathsf{XOR}_2^{\pi_1,\pi_2}$ (XOR instantiated with π_1 and π_2) is shown to be a secure pseudorandom

function. This second step often proves information-theoretic indistinguishability of the mode of operation, allowing the adversary unlimited computational time. In other cases, the original security game can be reduced to some variant of the indistinguishability game.

In this field of provable security, we primarily focus on the second step.

1.2 WHERE DOES MIRROR THEORY COME INTO THE PICTURE?

H-COEFFICIENT TECHNIQUE. Patarin formally introduced the Coefficient H technique tool at SAC 2008 [Pat09], though this technique had appeared in some of his earlier works [Pat91a; Pat91b; Pat98; Pat03]. Interestingly, it was Vaudenay who first exposed the H-technique in his decorrelation theory [Vau03] properly attributing the technique was initially described in Patarin's PhD thesis [Pat91a], which was written in French. Separately, Bernstein independently rediscovered a similar variant, known as the interpolation theorem [Ber99], which Nandi later strengthened as the strong interpolation theorem [Nan06]. Subsequently, Chen and Steinberger provided a renewed interpretation of the H-technique in their analysis of key alternating ciphers [CS14]. This modern interpretation indeed popularized the H-technique, and as far as we know, recent applications have extensively adopted this updated description. Finally in a survey paper on H-coefficient technique [JN22], Jha et al formulated the functional viewpoint of an interactive algorithm, and made a thorough exposure of the H-coefficient technique and its extended version, applying them to achieve simpler, unified and optimal security analyses of various cryptographic schemes. We adopt the methodology of [JN22] in this dissertation, and present it in Chapter 3.

In its simplest form, the H-technique asserts that the statistical distance between the probability distributions of the ideal and real-world transcripts (which upper bounds the distinguishing advantage of any adversary making q queries) is bounded by one minus a lower bound of the *ratio of the probability that an attainable transcript can be realized in the real world to the probability that it can be realized in the ideal world*. A transcript is deemed *attainable* if the probability of its realization in the ideal world is non-zero.

Example 1.1. Consider an adversary $\mathscr{A}$ trying to distinguish a uniform random function $\boldsymbol{\rho} : D \to D$ (the real world) from a uniform random permutation $\boldsymbol{\pi} : D \to D$ (the ideal world) by making q queries. A typical attainable transcript for this distinguishing game would be $\omega = ((x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q))$, where x_i and y_i denote the i-th query and response, respectively. For an attainable transcript for the uniform random permutation, we must have $x_i = x_j \Leftrightarrow y_i = y_j$ for all $i \neq j$, i. e., x^q and y^q should be permutation compatible, also denoted as $x^q \leftrightarrow y^q$. Without loss of generality, we may assume that

$x_i \neq x_j$, as $\mathscr{A}$ gains no advantage from duplicate queries. Let $\mathtt{\Theta}_0$ and $\mathtt{\Theta}_1$ be the transcript random variables generated by $\mathscr{A}$'s interaction with $\boldsymbol{\pi}$ and $\boldsymbol{\rho}$, respectively. It follows that

$$\Pr[\mathtt{\Theta}_0 = \omega] = \Pr_{\boldsymbol{\pi}}[\boldsymbol{\pi}(x_1) = y_1, \ldots, \boldsymbol{\pi}(x_q) = y_q] = \frac{1}{2^n(2^n-1)\cdots(2^n-q+1)},$$

and

$$\Pr[\mathtt{\Theta}_1 = \omega] = \Pr_{\boldsymbol{\rho}}[\boldsymbol{\rho}(x_1) = y_1, \ldots, \boldsymbol{\rho}(x_q) = y_q] = \frac{1}{2^{nq}}.$$

Thus, the ratio of these probabilities is lower bounded as

$$\frac{\Pr[\mathtt{\Theta}_0 = \omega]}{\Pr[\mathtt{\Theta}_1 = \omega]} = \frac{2^n(2^n-1)\cdots(2^n-q+1)}{2^{nq}} \geq 1 - \frac{q(q-1)}{2^{n+1}}.$$

Finally, the Coefficient H technique states that $\mathscr{A}$'s advantage in distinguishing $\boldsymbol{\rho}$ from $\boldsymbol{\pi}$ is upper bounded by $\frac{q^2}{2^{n+1}}$. This is commonly known as the *PRP-PRF switching lemma* [BR06].

The *expectation method* [HT16] is a generalization of the H-coefficient technique, where instead of bounding the ratio of ideal to real-world transcript probability by some constant for all attainable transcripts, the *expected value of the ratio* is taken as the upper bound on the statistical distance. This generally leads to a tighter bound, since the contribution of every transcript is taken into account, not only of the worst one as in the original H-technique.

ALGEBRAIC MANIFESTATION OF REAL WORLD-REALIZABILITY CONDITIONS. There are certain restrictions for an attainable transcript to be real-world realizable. If we denoted all the unknowns in the cryptographic design by variables, then the input-output variables of any of the underlying primitives should have the functionality constraint of the respective primitive, e. g., if the concerned primitive is a PRP, and $\{(\mathsf{W}_1, \mathsf{Z}_1), \ldots, (\mathsf{W}_q, \mathsf{Z}_q)\}$ denote its input-output variables for the q queries, then we have the constraint of permutation compatibility between the input and output tuples, $\mathsf{W}^q \leftrightarrow \mathsf{Z}^q$. This is where we get a system of non-equations, that the internal variables of an attainable transcript must satisfy for it to be real-world realizable. Moreover, the mode of operation combines the inputs and outputs across all primitives in a fixed way. The most common such combiner is linear, which gives the additional constraints on the variables, that some linear combination of variables corresponding to the i-th query is equal to the i-th response of the system recorded in the transcript. This is where we get a system of equations that the internal variables of an attainable transcript must satisfy for it to be real-world-realizable. Thus *the probability of obtaining a particular transcript in the real world is determined by the number of solutions to the system of equations and non-equations in the internal variables of the transcript. Thus to upper bound the real-to-ideal world probability ratio, we need a lower bound on the number of solutions*. Hence, Mirror Theory.

Example 1.2. Let us revisit the XOR_2 PRF construction: $\mathsf{XOR}_2^{\boldsymbol{\pi}_1,\boldsymbol{\pi}_2}(x) = \boldsymbol{\pi}_1(x) \oplus \boldsymbol{\pi}_2(x)$. This is the real world oracle. Since we will be interested in the PRF security of this construction, the ideal world oracle is a uniform random function $\boldsymbol{\rho}$. One can see that every transcript $\{(x_1, y_1), \ldots, (x_q, y_q)\}$, such that $x^q \mapsto y^q$, i. e., $x_i = x_j \implies y_i = y_j$, is attainable. However for an attainable transcript to be real world-realizable the internal variables $\mathsf{Z}_i := \boldsymbol{\pi}_1(x_i)$ and $\mathsf{W}_i := \boldsymbol{\pi}_2(x_i)$, for $i \in [q]$, have to satisfy the system of equations: $\mathsf{Z}_i \oplus \mathsf{W}_i = y_i$, $i \in [q]$; and the system of non-equations: $\mathsf{Z}_i \oplus \mathsf{Z}_j \neq 0^n, \mathsf{W}_i \oplus \mathsf{W}_j \neq 0^n$, $i \neq j \in [q]$.

THE BANE OF BIRTHDAY BOUND. Continuing the investigation of the PRF security of a PRP (see Example 1.1), consider the naive adversary that queries the oracle until it gets a *collision* in the responses. A collision is not possible in the real world where a PRP is used. However, in the ideal world, where the adversary makes q queries to a uniform random function, the probability of getting a collision is $1 - (2^n)_q / 2^{nq} \approx q^2/2^n$. Thus if the naive adversary can make about $2^{n/2}$ queries, it can distinguish between the real and ideal world with advantage ≈ 1. This is indeed a matching attack that proves the tightness of the security analysis in Example 1.1. This typical class of attacks, having $O(2^{n/2})$ query complexity, that exploits some kind of collision to distinguish between the two worlds, are termed *birthday attacks*. Modern adversaries have extensive computational resources (e. g., using distributed computation, etc.) in a world with increased attack area surface, since the volume of data processed and transmitted increases exponentially. This necessitates the need for cryptographic constructions having *beyond-birthday-bound* (BBB) security, constructions that remain indistinguishable from its idealized counterpart far beyond $2^{n/2}$ queries. Cryptographic constructions that are secure up to $O(2^{n/2})$ adversarial queries are said to have $n/2$*-bit security*. For a construction having beyond-birthday-bound security, we will say it is $rn/(r+1)$*-bit secure* if it is secure against all adversaries making at most $O(2^{rn/(r+1)})$ queries. Finally, a construction secure even against adversaries making $O(2^n)$ queries is called n*-bit secure*.

1.3 CRYPTOGRAPHIC MOTIVATIONS FOR THE DIFFERENT VARIANTS OF THE MIRROR THEORY PROBLEM

In this dissertation, we have included several cryptographic constructions, the security analyses of which inspired the study of lower bounds to the number of solutions to different classes of systems of equations and non-equations. We introduce the constructions here and the consequent classes of Mirror Theory problems.

1.3.1 *Constructing PRFs from PRPs.*

Despite the PRF being a very valuable building block in symmetric-key cryptography, practical candidates for PRF are very scarce. On the other hand, PRP or blockciphers are

available in plenty in practice. One can consider a blockcipher to be a pseudorandom function, but due to the PRP-PRF switching lemma, it comes at the cost of birthday-bound security. Such a bound is acceptable when n is moderately large, e.g., 128 bits. However, due to the ongoing trend of lightweight cryptography, several lightweight blockciphers have been designed with smaller block sizes e.g., 64 bits. In such a situation, a blockcipher is not considered to be a good PRF as birthday-bound security is not adequate with 64 bit block size. Therefore, the natural question arises: Can we design a pseudorandom function out of lightweight blockciphers that guarantees security beyond the birthday bound? It turns out that over the past several years researchers have invested a lot of effort in designing such pseudorandom functions [BKR98; HWKS98; IMV16; CS16; GSWG19; Yas10a; Yas11a; ZWSW12; Nai17a; DDNPZ17; DDNP18; IM16]. We pick certain constructions that stand out, in their near-optimal security properties and design efficiency.

THE XOR CONSTRUCTIONS. Out of several such designs, *xor of two pseudorandom permutations*, $\mathsf{XOR}_2(x) := \mathsf{E}_{k_1}(x) \oplus \mathsf{E}_{k_2}(x)$ [1] [BI99], and its single-keyed variant $\mathsf{XOR}_1(x) := \mathsf{E}_k(0\|x) \oplus \mathsf{E}_k(1\|x)$, are the most popular ones. In a series of papers [Pat08b; Pat10a; Pat13], Patarin claimed that XOR construction (i.e., both XOR_1 and XOR_2) is secure up to $O(2^n)$ queries, but the security analyses, done by H-technique, relied on conjectured lower bounds [Pat03] on the corresponding systems of equations, the available proofs of which [Pat05] were sometimes incomplete were containing unverifiable claims. However, there exists a proof of n-bit security of the XOR_1 construction using the χ^2-method [DHT17], which is another novel way of bounding the statistical distance between real and ideal world transcripts. Unfortunately, the χ^2-method, although being a very important tool, is out of scope of this dissertation.

Our Contributions. In [DNS22] we have given the first verifiable proofs to Patarin's conjectured lower bounds resulting from the security analyses of the XOR constructions, confirming their n-bit security. The security analyses are reproduced in Chapter 13.

THE XORP CONSTRUCTION. Now the XOR constructions, despite having the simplest design along with full security, is a fixed output length PRF, XOR_1 maps $(n-1)$-bit values to n-bit values and XOR_2 maps n-bit values to n-bit values. For Thus to obtain a kn-bit output, if we want to apply, say XOR_2 PRF, we will need k many PRF calls, each requiring 2 underlying blockcipher calls, i.e., a total of $2k$ blockciper calls.

However, PRFs with larger outputs are crucial for certain constructions to achieve BBB security. For example, consider the counter (CTR) mode of encryption, that xors an encryption of the incremental counter to the message blocks to get the ciphertexts in a stream, i.e., for a message $(M_1, \ldots, M_\ell)$, the CTR mode outputs $(C_1, \ldots, C_\ell)$, where $C_i = M_i \oplus E_k(\mathsf{ctr} \oplus i)$. This construction takes only k calls to the underlying blockcipher E_k for a kn-bit output. However, as proved in [BDJR97], this construction is secure only

1 Here, E_{k_1} and E_{k_2} denote two n-bit independent pseudorandom permutations

up to the birthday bound. It is known that the CTR mode would achieve BBB security if the underlying blockcipher E is replaced with a PRF. Many designs [BKR98; HWKS98; Luco0; BI99]tried to exploit this idea of first constructing PRFs from PRPs and then using the PRF in the CTR mode. But all of them had either efficiency problems like re-keying or using as many as $2k$ PRP calls as we discussed above. To remedy the situation Iwata [Iwa06] proposed the CENC mode of operation that uses as the underlying PRF, the XORP construction. To yield a kn-bit output, XORP function, takes a $(n - \log_2(k+1))$-bit input, concatenates $\langle i \rangle$, the $\log_2 k$-bit binary representation of $i \in [k+1]$, to the input to create k inputs for the underlying PRP, and then outputting the vector of k n-bit values, where the i-th component is the xor of the $(i+1)$-th PRP output and the first PRP output. This construction uses only k calls to the underlying PRP, avoids the re-keying problem, and the key-stream for the CTR mode can be pre-computed.

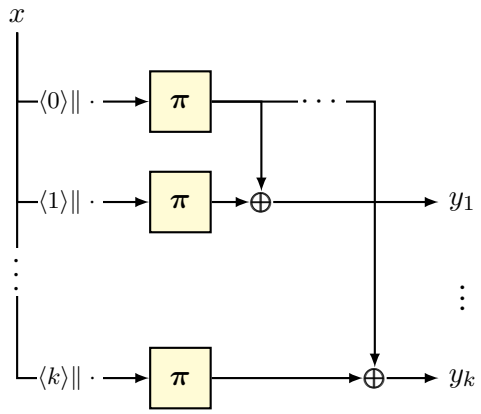


Figure 1.1: The XORP PRF construction

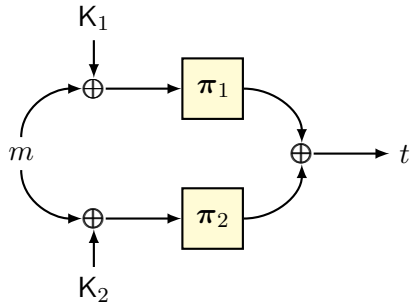
A n-bit security proof of the XORP construction is given by Iwata et al. in [IMV16], which vitally relies upon another Mirror theory conjecture by Patarin and needs to be revisited.

Our Contribution. In [CDNPS23], we prove the said Mirror Theory conjecture (for a range of parameters much higher than practical needs) and give an improved security bound following Iwata's analysis, presented in section 14.4.

SUM OF EVEN-MANSOUR. All the PRF designs discussed till now are blockcipher-based. Since we are designing functions, only the forward direction matters, and that is why using blockciphers for PRF constructions, seems superfluous to a degree, because blockciphers have the extraneous property of being efficient in the backward direction too. Instead, we could instantiate PRFs based on *public random permutations*, e. g., Keccac [BDPVA13], Gimli [BKLMM+17], SPONGENT [BKLTVV11], etc., which are designed to be very fast in the forward direction, but not necessarily in the backward direction. Public random permutation-based constructions like keyed sponge [ADMA15; MRV15], Farfalle [BDH-

PAK17], are variable length constructions. There is a scope of a more efficient/secure design for short fixed-length messages.

In [CLM19] Chen et al. proposed the public random permutation-based PRF construction, called the *sum of Even-Mansour* (SOEM^2), where the idea is to instantiate the blockciphers in the sum of permutations PRF construction, with the public-permutation based blockcipher $\mathsf{EM}^{\pi}(\mathsf{K}, m) = \pi(\mathsf{K} \oplus m) \oplus \mathsf{K}$. Chen et al. showed that the sum of two Even Mansour constructions, $\mathsf{SOEM}^2_{\pi_1,\pi_2}(\mathsf{K}_1, \mathsf{K}_2, m) = \mathsf{EM}^{\pi_1}(\mathsf{K}_1, m) \oplus \mathsf{EM}^{\pi_2}(\mathsf{K}_2, m)$ is a $2n/3$-bit secure PRF only if π_1 is independent of π_2 and K_1 is independent of K_2. Any weaker assumption would restrict the security to birthday-bound. In [ST23], Sibleyras et al. showed that post-adding the keys as in Even-Mansour is redundant, achieving the same security with a more efficient design, *keyed sum of permutations*, $\mathsf{KSoP}_{\pi_1,\pi_2}(\mathsf{K}_1, \mathsf{K}_2, m) = \pi_1(\mathsf{K}_1 \oplus m) \oplus \pi_2(\mathsf{K}_2 \oplus m)$. The authors point out that the independence requirements between π_1, π_2 and $\mathsf{K}_1, \mathsf{K}_2$, remain the same, in order to achieve said security.



Our Contributions. In this dissertation, we consider the sum of r Even-Mansour ciphers, which after removing the redundant post-addition of keys, is defined as $\mathsf{SOEM}^r_{\pi_1,\ldots,\pi_r}(\mathsf{K}_1, \ldots, \mathsf{K}_r, m) := \bigoplus_{i\in[r]} \pi_i(\mathsf{K}_i \oplus m)$. We show that this achieves $rn/(r+1)$-bit PRF security in the presence of (p, q)*-adversaries*, by which we mean that adversary can make total p queries to the public permutations in the offline phase, and can make q queries to the construction oracle in the online phase. The security analysis is done in Chapter 16 of this dissertation.

SINGLE-KEYED DBHTS MAC. A message authentication code (MAC) is a tag associated with a message that is used to check the authenticity and integrity of the message. The security requirement on MACs is that, any adversary querying the MAC oracle q messages, each message having at most ℓ blocks, such that total query size is σ, has negligible (in the parameters $\rho = (q, \ell, \sigma)$) probability to guess the MAC for a message not already present in the transcript of interaction. Such a MAC is called secure against *existential unforgeability under chosen message attacks*, in short EUF-CMA secure. Note that it is more than enough to investigate the PRF security of MAC constructions, as it is a stronger property than EUF-CMA.

Most common constructions of MAC are either based on blockciphers, e.g., CBC-MAC [BKR00], PMAC [BR02], OMAC [IK03], LightMAC [LPTY16], etc., or based on cryptographic hash functions, e.g., HMAC [BCK96]. At a high level, these constructions come under the umbrella of UHF-then-PRF designs, where first a message is compressed to a short string by a universal hash function (UHF) and then a PRF is applied on this string to generate the tag. However, due to the detectable collision property, that any collision among the outputs of the UHF results in a tag collision, this design paradigm cannot overcome the birthday bound. This becomes a problem when many MAC constructions have been proposed with lightweight blockciphers, e.g., PRESENT [BKLPPRSV07], LED [GPPR11], GIFT [BPPSST17].

To go beyond the birthday bound, one possible way to improve upon the UHF-then-PRF design is to replace the UHF by a hash function with double block output, such that each block behaves like the output of a UHF and then apply the sum-of-permutations PRF on the blocks, i. e., passing each block through a blockcipher, and the resulting pair of outputs being xored to get the tag. Such a design idea is bolstered by the fact that the XOR constructions are optimally secure. Dutta et al. [DDNP18] concretized this, naming the design *diblock hash-then-sum* (DBHtS). In this paper they proved that several constructions falling under the DBHtS design paradigm, e. g., PolyMAC [Boe93; BJKS93; Tay93], SUM-ECBC [Yas10b], PMAC+ [Yas11b], LightMAC+ [Nai17b] achieve $2n/3$-bit security. In [LNS18], Leurent et al. presented a $3n/4$-bit attack against DBHtS schemes. Finally, Kim et al. [KLL20] proved the $3n/4$-bit security of the above constructions, closing the gap.

Our Contributions. There remains one aspect where the DBHtS schemes can be made yet more efficient. Note that in the general implementations of DBHtS , three keys are used, one for all the blockcipher-calls corresponding to hash value evaluations, and one for each of the blockciphers constituting the sum-of-permutations PRF. Since rekeying is an expensive process, the obvious alternative is to use the same key for all the blockciphers, whether it be a part of the hash or the PRF, the design being called the 1k-DBHtS . In [CEJNS24] we give a $3n/4$ security bound for 1k-DBHtS , and showed that for its instantiations, 1k-PMAC+ and 1k-LightMAC+ , the corresponding hash functions PHash and LightHash are diblock hash functions having the desired properties. The security proofs are given in Chapter 17 of this dissertation.

THE 2K-HTMB-P2 CONSTRUCTION. Now we take a look at the opposite issue. We want to build variable input length (VIL) PRF constructions from PRPs. There are some candidates for BBB VIL PRFs, like SUM-ECBC [Yas10b], PMAC+ [Yas11b], LightMAC+ [Nai17b], all of which fall under the DBHtS design paradigm [DDNP18], as we discussed earlier. The other more traditional way is to adopt the Hash-then-PRF mode, the main components of which are: (a) a hash function with $2n$-bit output, (b) a $2n$-bit-to-n-bit PRF. The only candidates for the second component, for which the construction achieves n-bit security,

are: (1) the Benes and modified Benes (or mBenes) constructions [AV96] or (2) the Feistel networks of at least four rounds.

In [AV96], Aiello et al. proposed the Benes and mBenes constructions that uses, respectively, 6 and 4 independent n-bit PRFs. The conjectured n-bit security for both the constructions. In [Pato8a], Patarin proved that Benes is n-bit secure. Now if we intend to use PRPs as our basic building block, then the PRF primitives of the Benes constructions will have to be replaced by the XOR_2 construction, but as a consequence, we would need 12 and 8 PRP calls for Benes and mBenes constructions, respectively, which is no more efficient than the choice of Fiestel networks. In [CJN20], Cogliati et al. proposed the Hash-then-modified-Benes (HtmB in short) design where a sufficiently universal hash (in this case DbACU_q) is combined with the mBenes , yielding n-bit secure VIL PRFs. The types of HtmB constructions proposed by them are:

- HtmB-p1 - here among the 4 underlying PRF primitives of mBenes , two are replaced by PRPs and the other two are replaced by the XOR_2 construction.
- HtmB-p2 - mBenes where all the four underlying primitives are PRPs.

Their n-bit security proof of HtmB-p2, the more efficient of the two designs, relied on a Mirror Theory conjecture.

Our Contribution. In [CDNPS23] we proved a slightly better result than the conjecture, and in light of this improved bound we revisit the security proof of 2k-HtmB-p2 in [CJN20]. The security analysis is presented in section 14.3.

1.3.2 *Constructing PRP from PRF*

The Feistel scheme is one of the two most widely used domain-extending permutation schemes, the other one being substitution permutation networks (SPN). Feistel schemes have been classically used to design many blockciphers (like DES [Des], Lucifer [Sor84] etc.), which has the prime advantage over the alternative, substitution permutation networks, of being invertible even if the round functions are not. The Feistel scheme has also been used in format-preserving encryption, an important example being the Thorp shuffle [BM09], which is but an unbalanced Feistel cipher [SK96]. In [Pat10b], Patarin proved n-bit SPRP security of the six rounds of Feistel network, by using a Mirror Theory conjecture.

Our Contribution. In [CDNPS23], we revisit this security proof by Patarin. The security analysis is presented in section 14.4.

1.3.3 *Tweakable Blockciphers*

Tweakable blockcipher is another very important building block in symmetric-key cryptography. It has been used in constructing encryption schemes [BLN18], MAC [IMPS17], authenticated encryption [KR11; PS16], and leakage resilience [SPSCV22].

Liskov, Rivest and Wagner, in their seminal CRYPTO 2002 paper [LRW02] mathematically formulated the tweakbale blockciphers and presented two design paradigms, named after the authors as LRW1 and LRW2. Since then the design landscape of tweakable blockciphers has taken two paths. One of them is of ad-hoc designs, that gained popularity with the advent of TWEAKEY [JNP14] platform, e. g., the Deoxys-TBC [JNPS21], Skinny [BJKLMPSSS16], QARMA [Ava17], with their security bolstered by cryptanalysis. The other one is provably secure designs, e. g., the original constructions of [LRW02], LRW1 and LRW2, XEX [Rog04] and its extensions [CS08; Min06; GJMN16]. The security of provably secure designs depends on the security assumptions on the underlying primitives. However, the designs just mentioned have at most birthday-bound CCA security due to detectable internal collisions.

Landecker et al. [LST12] first noticed that cascading two independent instances of LRW2 achieves beyond birthday bound security. Their proof of $2n/3$-bit security of 2-LRW2 was later corrected by [Pro14]. [JN20] finally gave $3n/4$-bit security proof for 2-LRW2, improving upon the proof ideas of [Men18]. [Men18] also proposed a $3n/4$-bit attack against 2-LRW2, implying that the above security proof is tight. For the general $r \geq 2$-rounds of cascaded LRW2 the best known security bound is $rn/(r+2)$-bit security [LS13].

In [BGGS20], Bao et al. proposed cascading the LRW1 to achieve BBB security. They showed that three rounds of LRW1, in short 3-LRW1, has $2n/3$-bit security. Later it was shown that 3-LRW1 also has $3n/4$-bit CPA security. The 3-LRW1 is popularly known as TNT, greatly appreciated for its efficient design and highly believed to be capable of achieving even $3n/4$-bit CCA security. For the general $r \geq 3$ rounds of cascaded LRW1 the best known security bound is $(r-1)n/(r+1)$-bit security [ZQG23].

Our Contributions. In our paper [JKNS24], we have proposed a fully scalable birthday-bound CCA attack on TNT a.k.a. 3-LRW1. It is a matching attack since we also showed that TNT and even its single-keyed version (where the three blockciphers that constitute the underlying primitives of 3-LRW1 are not independent, but keyed by the same key) are birthday-bound secure. Our attack disproves the beyond-birthday-bound security claims by [BGGS20]. We identified the bug in the proof, where a random variable is erroneously assumed to have uniform distribution, leading to the overestimation of security. Our attack is explained in section 15.1 of this dissertation. We give the security analysis in section 15.2.

In [JKNS24] we also formulated the generalized view of the cascaded LRW paradigm: naming it the LRW+ design, which consists of two blockcipher calls sandwiched between a pair of tweakable universal hashes. We show that as long as the tweakable hashes are sufficiently universal, the LRW+ construction is CCA secure up to $2^{3n/4}$ queries. Note that LRW+ encompasses both 2-LRW2 and 4-LRW1. Thus, as a direct side-effect of our analysis, we have that 2-LRW2 and 4-LRW1 are CCA secure up to $2^{3n/4}$ queries. In case of 2-LRW2, our bound matches the tight analysis in [JN20].

1.3.4 *The consequent classes of Mirror Theory problem*

We will try to classify the systems of equations and non-equations obtained as the real-world realizability criteria of the transcript obtained in the security games of the above constructions. For the following discussion it is beneficial to understand the following points:

- The scope of this dissertation covers only *homogeneous systems of bivariate non-equations*, which contains non-equations of the form $\mathsf{X}_i \oplus \mathsf{X}_j \neq 0^n$, or in other words $\mathsf{X}_i \neq \mathsf{X}_j$. So whenever non-equations are mentioned, we might very well narrow down our gaze to these types of non-equations only.
- The *block-maximality* of a system is the maximum number of variables that gets determined if one variable is assigned a value. To aid visualization, one could think of a system of bivariate equations as a labeled undirected graph on the variables as vertices, having an edge between two vertices X_i and X_j labeled λ, if and only if there is an equation in the system $\mathsf{X}_i \oplus \mathsf{X}_j = \lambda$. Note that the block-maximality of a system of bivariate equations is simply the size of the maximum component of the corresponding graph. We often denote the block-maximality as $\xi_{\max}$.
- To prove beyond-birthday-bound security of a construction, we generally have to show that the lower bound on the number of solutions to the corresponding system of equations and non-equations is a very close approximation of the *expected number of solutions*. What we mean by the expected number of solutions to a system of equations and non-equations is the expected number of solutions to the system when the constants on the r.h.s. of the equation are chosen uniformly randomly.

COMPLETE MIRROR THEORY PROBLEM. Consider the transcript $\{(x_1, y_1), \ldots, (x_q, y_q)\}$ obtained in the security game of the XOR_1^{π} construction. If we denote $\mathsf{Y}_{2i-1} = \pi(0\|x_i)$ and $\mathsf{Y}_{2i} = \pi(1\|x_i)$, for $i \in [q]$, we get a bivariate system of equations $\mathsf{X}_{2i-1} \oplus \mathsf{X}_{2i} = y_i$ with $\xi_{\max} = 2$, and a system of non-equations $\mathsf{X}_i \oplus \mathsf{X}_j \neq 0^n$ for all $i \neq j \in [q]$. There is a non-equation between any two variables, hence *complete*. In our paper [DNS22] show that the number of solutions to the above system of equations and non-equations is at least as much as the expected number of solutions, which $(2^n)_{2q} / 2^{nql}$. The proof is presented in Chapter 6 of this dissertation. As an application of this result we show it implies that the XOR_1 is a n-bit secure PRF.

Now consider the transcript $\{(x_1, y_1^k), \ldots, (x_q, y_q^k)\}$, obtained in the security game of the $\mathsf{XORP}^{\pi}[k]$ construction. Here $y_i^k = (y_{i,1}, \ldots, y_{i,k})$ denotes the i-th response of the real/ideal oracle. Denoting the $k+1$ outputs of the underlying primitive as $\mathsf{Y}_{i,j} = \pi(\langle j \rangle \| x_i)$, $j \in [k+1]$, i is easy to check, that the corresponding systems of equations will be

$$\mathsf{Y}_{1,1} \oplus \mathsf{Y}_{1,2} = y_{1,1} \qquad\qquad \mathsf{Y}_{q,1} \oplus \mathsf{Y}_{q,2} = y_{q,1}$$

$$\begin{array}{ccc} \mathsf{Y}_{1,1} \oplus \mathsf{Y}_{1,3} = y_{1,2} & & \mathsf{Y}_{q,1} \oplus \mathsf{Y}_{q,3} = y_{q,2} \\ \vdots & \cdots & \vdots \\ \mathsf{Y}_{1,1} \oplus \mathsf{Y}_{1,k+1} = y_{1,k} & & \mathsf{Y}_{q,1} \oplus \mathsf{Y}_{q,k+1} = y_{1,k} \end{array}$$

and the system of non-equations will be complete. Note that, the above system of equations is bivariate but has block-maximality $k+1$. In our paper [CDNPS23], we showed the following:

Theorem 7.1 (informal): *For a wide range of $\xi_{\max}$ ($\xi_{\max} \approx O(2^{n/4})$) the number of solutions to a system of bivariate equations and a complete system of non-equations is at least the expected number of solutions, even if $q = O(2^n)$.*

We present this proof in Chapter 7 of this dissertation. As we will show later the PRF security game of 2k-HtmB-p2 and PRP security game of six-round Feistel construction both yield systems of bivariate equations with $\xi_{\max}$ in the order of $\log_2 n$. In Chapter 14, we revisit the n-bit PRF security proofs of the XORP and 2k-HtmB-p2 and the n-bit PRP security of six-round Feistel, using our revised bounds, as obtained in Chapter 7.

BIPARTITE MIRROR THEORY PROBLEM. As noted in Example 1.2, the security analysis of XOR_2 construction yields a system of bivariate equations, $\mathsf{X}_i \oplus \mathsf{Y}_i = \lambda_i$, and non-equations, where the non-equations are only between the X-variables or Y-variables, i. e., we can bipartition the variables into two sets, where all the variables in the same set have to be pairwise-distinct. There is no non-equation between two variables belonging to different sets. We name this class of Mirror Theory Problems, the *bipartite Mirror Theory problem*, BMTP. As for the system of equations obtained due to XOR_2 security analysis, the size of each component is 2. In [DNS22] we prove the following:

Theorem 8.1 (informal): *The number of solutions to a consistent* BMTP *problem with $\xi_{\max} = 2$ is at least $(1-\epsilon)$ times the expected number of solutions, where $\epsilon \approx O(q^2/2^{2n})$.*

The lower bound analysis is given in Chapter 8.

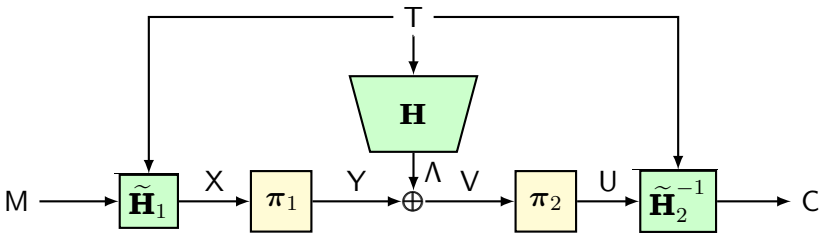


Figure 1.2: The LRW+ construction.

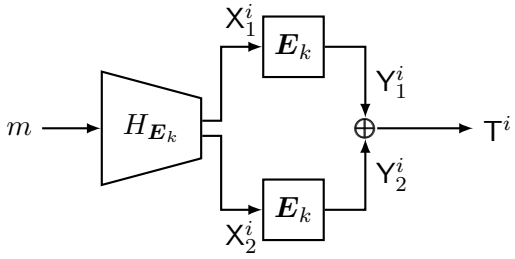
Now consider the LRW+ design, see Fig. 1.2. We can see that the security analysis of LRW+ will yield a system of bivariate equations $\mathsf{Y}_i \oplus \mathsf{V}_i = \Lambda_i$, $i \in [q]$. Now $\mathsf{X}^q \leftrightarrow \mathsf{Y}^q$ and $\mathsf{V}^q \leftrightarrow \mathsf{U}^q$. Thus we cannot assume that all Y-variables are pairwise distinct or all

V-variables are pairwise distinct because for that we need to guarantee that there is no collision in X or U-variables, leading to birthday bound. Now if we allow for collisions in the Y and V-variables, then we can basically club all the Y-variables colliding into one variable and we end up with components more complicated than isolated edges, i. e., a system of equations for which $\xi_{\max} \geq 2$. However, we can declare only those transcripts to be good for which the components are of manageable structure, like star graphs, and restrict our lower bound analysis to BMTP problems with this special graph structure only. In [JN20], Jha et al. have shown the following:

Theorem 9.1 (informal): *The number of solutions to a* BMTP *problem, with only star graphs as components, is at least* $(1-\epsilon) \times S$*, where is* $\epsilon \approx O(2^{3n/4})$ *and* $S \geq$ *the expected number of solutions.*

S is chosen in a convenient manner so as to simplify the real-to-ideal world probability ratio in the security proof of 2-LRW2. We present the lower bound analysis in Chapter 9.

RESTRICTED MIRROR THEORY PROBLEM. Let us consider the 1k-DBHtS construction.



Given a transcript of interaction and the hash evaluations corresponding to each query, one can lower bound the probability that the transcript is realizable, by lower bounding the number of pairwise-distinct solutions to the system of bivariate equations, $\mathsf{Y}_1^i \oplus \mathsf{Y}_2^i = \mathsf{T}^i$. The main point of departure of this problem from the previous variants of Mirror Theory is that none of the variables are allowed to take values in the forbidden set, consisting of all the blockcipher input-outputs generated during the given hash function evaluations, as $\boldsymbol{\pi}_0, \boldsymbol{\pi}_1$ and $\boldsymbol{\pi}_2$ are domain-separated versions of the same random permutation. Note that in this case, the system of non-equations is again complete. We call the Mirror Theory problem with a system of equations (may not be bivariate) and non-equations (among every two variables), such that none of the solutions can take values from a restricted set, the *complete restricted Mirror Theory problem*, in short, CRMTP.

On the other hand, the security analysis of the public permutation-based construction, the sum of r Even-Mansour, leads to q equations, each having r-variables, one corresponding to the output of each of the r underlying permutations, and non-equations between only the output variables of same permutation. Since the adversary can query the public permutations in the offline phase, the internal variables cannot be assigned any value from

the set of responses the adversary obtained in the offline phase. This class of Mirror Theory problems is called *regular partite restricted Mirror Theory problem*, or in short RPRMTP.

In [CEJNS24] we show the following:

Theorem 12.1 and 11.1 (informal): *Both the variants,* CRMTP *and* RPRMTP*, have number of solutions at least* $(1 - \epsilon)$ *times the expected number of solutions.*

We give the lower bound analysis of CRMTP in Chapter 12 and that of RPRMTP in Chapter 11.

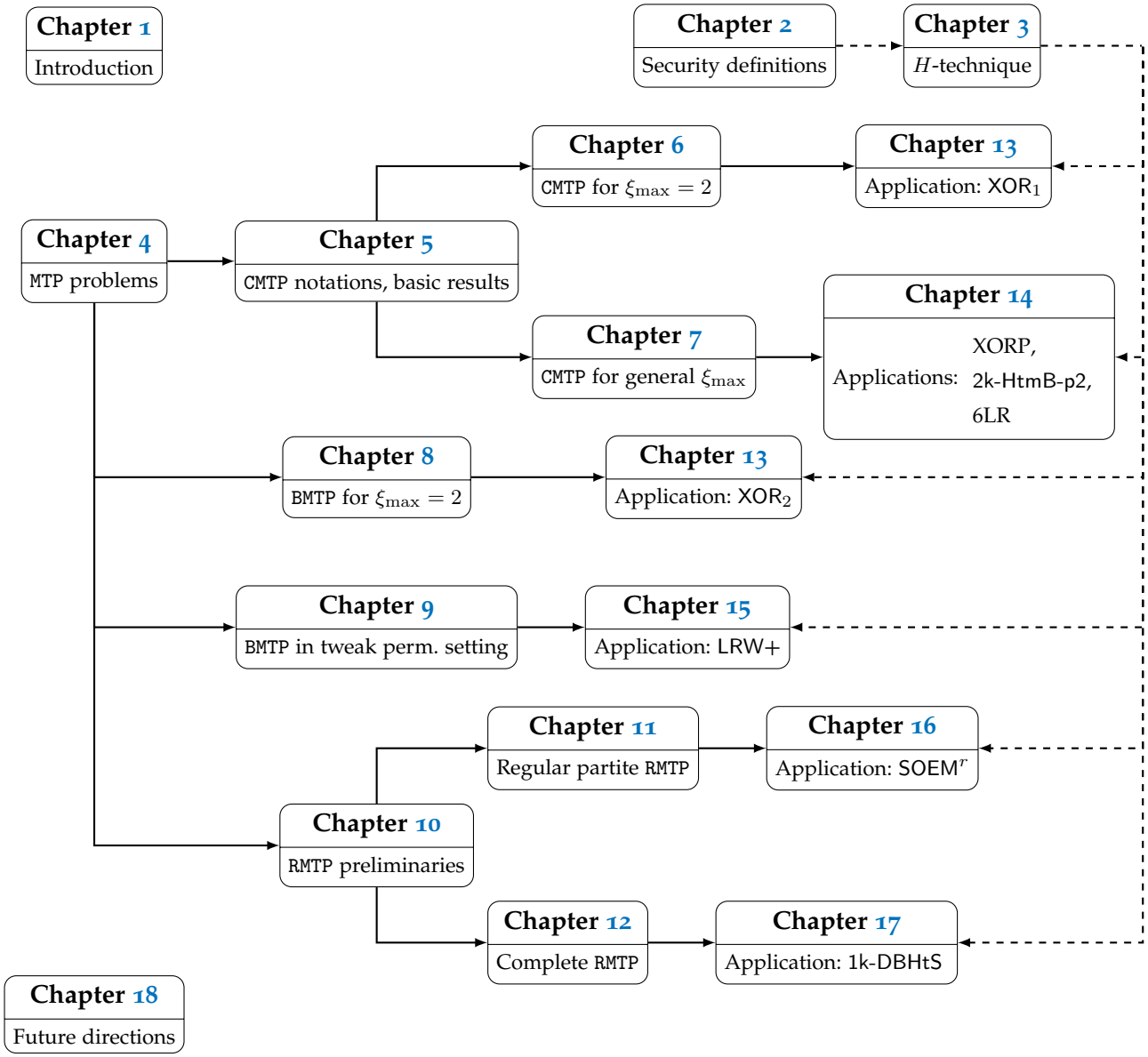


Figure 1.3: Directed tree indicating depndencies among chapters.

2

DEFINING SECURITY

In this chapter, we present a unified mathematical formulation of any interactive game between an adversary and a challenger in a typical security game considered in this dissertation. We call it the *probabilistic function model*. It was formulated in [JN22] and we adopt it here. We formally define all the assumptions about the adversaries considered in this dissertation. Finally, we define all the security notions that we will explore.

2.1 PROBABILISTIC FUNCTION MODEL FOR INTERACTIVE ALGORITHMS

Definition 2.1 (probabilistic function). *A* probabilistic function *from $\mathscr{X}$ to $\mathscr{Y}$ is a function $f : \Omega \times \mathscr{X} \to \mathscr{Y}$, for some sample space Ω. For the sake of brevity, we sometimes suppress the underlying sample space Ω and simply denote the above function as $f : \mathscr{X} \xrightarrow{*} \mathscr{Y}$.*

We can think of the probabilistic function $f : \Omega \times \mathscr{X} \to \mathscr{Y}$ as mapping $x \in \mathscr{X}$ to the random variable $f(\mathsf{W}, x)$, where $\mathsf{W} \xleftarrow{*} \Omega$ (popular choices are uniform or wor sampling). Thus a probabilistic function induces a family of probability measures on $\mathscr{Y}$, $\boldsymbol{\rho}_f = \{\boldsymbol{\rho}_{f,x} : x \in \mathscr{X}\}$, defined as $\boldsymbol{\rho}_{f,x}(y) := \Pr_{\mathsf{W} \xleftarrow{*} \Omega}(f(\mathsf{W}, x) = y)$ for $y \in \mathscr{Y}$. For a probabilistic function $f : \mathscr{X} \xrightarrow{*} \mathscr{Y}^q$, we can define its component probabilistic functions as $f_i : \mathscr{X}^q \xrightarrow{*} \mathscr{Y}$ such that $f(\mathsf{W}, x) = (f_1(\mathsf{W}, x), \ldots, f_q(\mathsf{W}, x))$ for $x \in \mathscr{X}$.

Definition 2.2 (computationally bounded challenge function). *A* q-bounded $(\mathscr{X}, \mathscr{Y})$ challenge function *is a probabilistic function $f : \mathscr{X}^q \xrightarrow{*} \mathscr{Y}^q$ such that f_i is functionally independent of $\mathscr{X}^{[i+1..q]}$.*

Definition 2.3 (computationally bounded adversarial function). *A* q-bounded $(\mathscr{X}, \mathscr{Y})$ adversarial function *is a probabilistic function $f : \mathscr{Y}^q \xrightarrow{*} \mathscr{X}^q$ such that f_i is functionally independent of $\mathscr{Y}^{[i..q]}$. Moreover, it is called* deterministic *if the underlying sample space Ω is a singleton, which can hence be ignored.*

An interactive (probabilistic) algorithm can be viewed as an adversarial function $\mathscr{A} : \mathscr{Y}^q \xrightarrow{*} \mathscr{X}^q$, where the underlying sample space is the space from which the algorithm draws its random coins, R, that interacts with its oracle, which in turn can be viewed as a challenge function, $\mathscr{O} : \mathscr{X}^q \xrightarrow{*} \mathscr{Y}^q$, whose random coins, R', are independent of R: the interactive algorithm starts the interaction by querying x_1, that depends only on the random coin of $\mathscr{A}$, and the oracle replies with y_1 that depends on x_1 and the random coins of $\mathscr{O}$. The adversary then queries x_2 as a function of y_1 and random coins of the adversary,

and the oracle replies with y_2, which depends on x_1, x_2 and the oracle's random coins, and so on. The interaction of any interactive algorithm with query complexity q, is thus modeled by q-bounded adversarial and challenge functions.

By definition of the adversarial and challenge function there exist functions $\mathscr{A}'_i : \mathscr{Y}^{i-1} \xrightarrow{*} \mathscr{X}$ and $\mathscr{O}'_i : \mathscr{X}^i \xrightarrow{*} \mathscr{Y}$, such that $\mathscr{A}_i(y^q) = \mathscr{A}'_i(y^{i-1})$ and $\mathscr{O}_i(x^q) = \mathscr{O}'_i(x^i)$.

Definition 2.4 (transcript of interaction). *Let $\mathscr{A}$ and $\mathscr{O}$ be q-bounded $(\mathscr{X}, \mathscr{Y})$ adversarial and challenge functions. Then the* transcript of interaction *between $\mathscr{A}$ and $\mathscr{O}$ is a random variable $\tau(\mathscr{A}^{\mathscr{O}}) := (\mathsf{X}^q, \mathsf{Y}^q)$, where the random variables X_i and Y_i are defined sequentially as:*

$$\mathsf{X}_i := \mathscr{A}'_i(\mathsf{R}, \mathsf{Y}^{i-1}), \qquad \mathsf{Y}_i = \mathscr{O}'_i(\mathsf{R}', \mathsf{X}^i),$$

where R and R' are the random coins of $\mathscr{A}$ and $\mathscr{O}$, respectively.

The randomness of the transcript is entirely derived from the random coins. Thus fixing $\mathsf{R} = r$ and $\mathsf{R}' = r'$ yields a unique value (x^q, y^q) for the transcript, where $x^q = \mathscr{A}(r, y^q)$ and $y^q = \mathscr{O}(r', x^q)$. Thus it follows from the independence of R and R' that

$$\Pr\left(\tau(\mathscr{A}^{\mathscr{O}}) = (x^q, y^q)\right) = \Pr\left(\mathscr{A}(\mathsf{R}, y^q) = x^q\right) \cdot \Pr\left(\mathscr{O}(\mathsf{R}', x^q) = y^q\right) = \boldsymbol{p}_{\mathscr{A}, y^q}(x^q) \cdot \boldsymbol{p}_{\mathscr{O}, x^q}(y^q)$$

Thus the distribution of $\tau(\mathscr{A}^{\mathscr{O}})$ is entirely determined by the family of distributions $\boldsymbol{p}_{\mathscr{A}}$ and $\boldsymbol{p}_{\mathscr{O}}$.

Definition 2.5 (extended transcript). *Given a challenge function $\mathscr{O}$, we define the $\mathscr{S}$-*extended challenge function *as a probabilistic function $\overline{\mathscr{O}} = (\mathscr{O}, \mathcal{S}) : \mathscr{X}^q \xrightarrow{*} \mathscr{Y}^q \times \mathscr{S}$. For any adversarial function $\mathscr{A} : \mathscr{Y}^q \xrightarrow{*} \mathscr{X}^q$, we define the extended transcript of interaction between $\mathscr{A}$ and $\mathscr{O}$, as*

$$\overline{\tau}(\mathscr{A}^{\mathscr{O}}) = \tau(\mathscr{A}^{\overline{\mathscr{O}}}) = (\tau(\mathscr{A}^{\mathscr{O}}) = (\mathsf{X}^q, \mathsf{Y}^q), \mathcal{S}(\mathsf{X}^q)) = (\tau(\mathscr{A}^{\mathscr{O}(\mathsf{R}, \cdot)}), \mathcal{S}(\mathsf{R}, \mathscr{X}^q))$$

where R is the random coins of $\overline{\mathscr{O}}$. The random variable $\mathcal{S}(\mathsf{W}^q)$ is called the supplement *to the challenge function $\mathscr{O}$.*

An $\mathscr{S}$-extended challenge function induces the family of distributions

$$\boldsymbol{p}_{\overline{\mathscr{O}}, x^q}(y^q, s) = \Pr\left(\mathscr{O}(x^q) = y^q, \mathscr{S}(x^q) = s\right)$$

Again by the independence of the random coins of $\mathscr{A}$ and $\overline{\mathscr{O}}$, we have that the distribution of the extended transcript is completely determined by the $\boldsymbol{p}_{\mathscr{A}}$ and $\boldsymbol{p}_{\overline{\mathscr{O}}}$,

$$\Pr\left(\overline{\tau}(\mathscr{A}^{\mathscr{O}}) = (x^q, y^q, s)\right) = \boldsymbol{p}_{\mathscr{A}, y^q}(x^q) \cdot \boldsymbol{p}_{\overline{\mathscr{O}}, x^q}(y^q, s)$$

The extended challenge function models those oracles that might release some extra information, depending on the queries of the interactive algorithm, after the interaction is over, implying that the queries are independent of this extra information.

2.1.1 *Some popular oracles*

In this dissertation we will quite frequently use the following oracles modeled as challenge functions.

KEYED FUNCTION. A family of functions from $\mathscr{X}$ to $\mathscr{Y}$, indexed by a key space $\mathscr{K}$, $F = \{F_k : k \in \mathscr{K}\}$, can be viewed as a function, $F : \mathscr{K} \times \mathscr{X} \to \mathscr{Y}$, defined as $F(k, x) := F_k(x)$. If we treat the key space as the sample space mentioned in the definition of a probabilistic function, we get a challenge function, which we call the *keyed function*,

$$\mathscr{F}(k, x^q) = (F(k, x_1), \ldots, F(k, x_q)),\ x^q \in \mathscr{X}^q.$$

KEYED STRONG PERMUTATION. If for every key $k \in \mathscr{K}$, $F(k, \cdot)$ is a permutation on $\mathscr{X}$, then one should make provision for an interactive algorithm to query this oracle both in the forward and backward direction. This motivates us to define the keyed function family, $F^{\pm} = \{F_k^{\pm} : k \in \mathscr{K}\}$, where

$$\begin{aligned} F_k^{\pm} :\ \{+1, -1\} \times \mathscr{X} &\to \mathscr{X} \\ (+1, x) &\mapsto F_k(x) \\ (-1, x) &\mapsto F_k^{-1}(x) \end{aligned}$$

The challenge function corresponding to the function $F^{\pm}$, denotes as $\mathscr{F}^{\pm}$, is called a *keyed strong permutation*.

It is easy to see that the family of distributions induced by $\mathscr{F}^{\pm}$ is completely determined by the family of distributions induced by $\mathscr{F}$, since for $(\delta^q, x^q, y^q) \in \{-1, +1\}^q \times \mathscr{X}^q \times \mathscr{X}^q$, we have

$$\Pr\left(\mathscr{F}^{\pm}(\delta^q, x^q) = y^q\right) = \Pr\left(\mathscr{F}(a^q) = b^q\right)$$

where (δ^q, a^q, b^q) is the *undirected representation* of (δ^q, x^q, y^q) defined as

$$(a_i, b_i) := \begin{cases} (x_i, y_i) & \text{if } \delta_i = 1 \\ (y_i, x_i) & \text{if } \delta_i = -1 \end{cases}$$

IDEAL ORACLES. We now define certain ideal challenge functions by specifying the family of distributions it must induce:

Definition 2.6 (random function). *A $(\mathscr{X}, \mathscr{Y})$ challenge function $\boldsymbol{\rho}$ is called a* random function *if for $(x^q, y^q) \in \mathscr{X}^q \times \mathscr{Y}^q$,*

$$\Pr\left(\boldsymbol{\rho}(x^q) = y^q\right) = \begin{cases} |\mathscr{Y}|^{-d} & \text{if } x^q \mapsto y^q \\ 0 & \text{otherwise} \end{cases}$$

where $d = |x^{\{q\}}|$.

A more direct way of describing a random function as a challenge function is to take $\mathsf{Func}(\mathscr{X}, \mathscr{Y})$ *as the sample space of the function,* $\boldsymbol{\rho} : \mathsf{Func}(\mathscr{X}, \mathscr{Y}) \times \mathscr{X} \to \mathscr{Y}$, *such that* $\boldsymbol{\rho}(f, x) = f(x)$.

Definition 2.7 (random permutation). *A* $(\mathscr{X}, \mathscr{X})$ *challenge function* $\boldsymbol{\pi}$ *is called a* random permutation *if for* $(x^q, y^q) \in \mathscr{X}^q \times \mathscr{X}^q$,

$$\Pr\left(\boldsymbol{\pi}(x^q) = y^q\right) = \begin{cases} 1/(|\mathscr{Y}|)_d & \text{if } x^q \leftrightarrow y^q \\ 0 & \text{otherwise} \end{cases}$$

where $d = |\{()x^q)|$.

A more direct way of describing a random permutation as a challenge function is to take $\mathsf{Perm}(\mathscr{X})$ *as the sample space of the function,* $\boldsymbol{\pi} : \mathsf{Perm}(\mathscr{X}) \times \mathscr{X} \to \mathscr{X}$, *such that* $\boldsymbol{\pi}(p, x) = p(x)$.

We can similarly define a strong random permutation, $\boldsymbol{\pi}^{\pm}$ *as the challenge function inducing the following distributions: for* $(\delta^q, x^q, y^q) \in \{-1, +1\}^q \times \mathscr{X}^q \times \mathscr{X}^q$,

$$\Pr\left(\boldsymbol{\pi}^{\pm}(\delta^q, x^q) = y^q\right) = \begin{cases} 1/(|\mathscr{Y}|)_d & \text{if } a^q \leftrightarrow b^q \\ 0 & \text{otherwise} \end{cases}$$

where (δ^q, a^q, b^q) *is the undirected representation of* (δ^q, x^q, y^q) *and* $d = |\{()a^q)|$.

Definition 2.8 (tweakable random permutation). *A* $(\mathscr{T} \times \mathscr{X}, \mathscr{X})$ *challenge function* $\widetilde{\boldsymbol{\pi}}$ *is called a* tweakable random permutation *if for* $(t^q, x^q, y^q) \in \mathscr{T}^q \times \mathscr{X}^q \times \mathscr{Y}^q$,

$$\Pr\left(\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q\right) = \begin{cases} \displaystyle\prod_{i=1}^{r} \frac{1}{(|\mathscr{Y}|)_{d_i}} & \text{if } x^q \overset{t^q}{\leftrightarrow} y^q \\ 0 & \text{otherwise} \end{cases}$$

where $r = |t^{\{q\}}|$ *and for* $t'_1, \ldots, t'_r$ *being the distinct elements in* t^q, $d_i = |\{x_j : t_j = t'_i\}|$.

The direct way of describing a tweakable random permutation as a challenge function is to take $\widetilde{\mathsf{Perm}}(\mathscr{T} \times \mathscr{X}, \mathscr{X}) := \mathsf{Func}(\mathscr{T}, \mathsf{Perm}(\mathscr{X}))$ *as the sample space of the function,* $\widetilde{\boldsymbol{\pi}} : \mathsf{Func}(\mathscr{T}, \mathsf{Perm}(\mathscr{X})) \times \mathscr{T} \times \mathscr{X} \to \mathscr{X}$, *such that* $\widetilde{\boldsymbol{\pi}}(\widetilde{p}, t, x) = \widetilde{p}(t)(x)$.

2.2 DISTINGUISHERS AND DISTINGUISHING ADVANTAGE

A *distinguisher* of two $(\mathscr{X}, \mathscr{Y})$ challenge functions $\mathcal{O}_1$ and $\mathcal{O}_2$, is defined as the tuple $(\mathscr{A}, \boldsymbol{\mathscr{C}})$, and denoted as $\mathscr{A}_{\boldsymbol{\mathscr{C}}}$, where

- $\mathscr{A}$ is a $(\mathscr{X}, \mathscr{Y})$ adversarial function drawing its random coins from Ω, and
- $\boldsymbol{\mathscr{C}} : \Omega \times \mathscr{X}^q \times \mathscr{Y}^q \to \{0, 1\}$ is a decision predicate,

such that output of $\mathscr{A}^{\mathcal{O}_i}_{\boldsymbol{\mathscr{C}}}$, with random coins $\mathsf{W} \xleftarrow{*} \Omega$, is $\boldsymbol{\mathscr{C}}(\mathsf{W}, \tau(\mathscr{A}^{\mathcal{O}_i}))$. Now we define the *advantage* of $\mathscr{A}_{\boldsymbol{\mathscr{C}}}$ in distinguishing between the challenge functions $\mathcal{O}_1$ and $\mathcal{O}_2$ as

$$\Delta_{\mathscr{A}_{\boldsymbol{\mathscr{C}}}}(\mathcal{O}_1;\mathcal{O}_2) = \left|\Pr\left(\mathscr{A}_{\boldsymbol{\mathscr{C}}}^{\mathcal{O}_1} \to 1\right) - \Pr\left(\mathscr{A}_{\boldsymbol{\mathscr{C}}}^{\mathcal{O}_2} \to 1\right)\right|$$

Let

$$A = \boldsymbol{\mathscr{C}}^{-1}(1) = \{(\omega, x^q, y^q) \in \Omega \times \mathscr{X}^q \times \mathscr{Y}^q : \boldsymbol{\mathscr{C}}(\omega, x^q, y^q) = 1\}$$

Then by Lemma A.2 we have

$$\Delta_{\mathscr{A}_{\boldsymbol{\mathscr{C}}}}(\mathcal{O}_1;\mathcal{O}_2) \leq \Delta((\mathsf{W}, \tau(\mathscr{A}_{\boldsymbol{\mathscr{C}}}{}^{\mathcal{O}_1})), (\mathsf{W}, \tau(\mathscr{A}_{\boldsymbol{\mathscr{C}}}{}^{\mathcal{O}_2}))) \tag{2.1}$$

ASSUMPTIONS ON DISTINGUISHERS. In the method of analysis pursued in this dissertation we make certain assumptions about the nature of distinguishers we would consider in our security definitions. These assumptions, instead of being restrictive, actually increase the distinguishing advantage of the distinguishers considered. Hence the security proofs can be looked upon as a kind of worst-case analysis.

1. TIME UNBOUNDED: We assume the decision predicate is $\boldsymbol{\mathscr{C}}_{\text{opt}}$ defined as:

$$\boldsymbol{\mathscr{C}}_{\text{opt}}(\omega, x^q, y^q) = \begin{cases} 1 & \text{if } \Pr\left(\mathsf{W} = \omega, \tau(\mathscr{A}^{\mathcal{O}_1}) = (x^q, y^q)\right) \geq \Pr\left(\mathsf{W} = \omega, \tau(\mathscr{A}^{\mathcal{O}_2}) = (x^q, y^q)\right) \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{\mathscr{C}}_{\text{opt}}$ is the optimum decision predicate in the sense that it achieves equality in (2.1). $\boldsymbol{\mathscr{C}}_{\text{opt}}$ may not be efficiently computable. However, since we are interested in information-theoretic security analysis we will consider time/memory-unbounded distinguishers. To measure the distinguisher efficiency we will only consider its *oracle query complexity*. Since we have fixed the decision predicate, here onwards we abuse notation to simply denote a distinguisher by its adversarial function $\mathscr{A}$, omitting $\boldsymbol{\mathscr{C}}_{\text{opt}}$ from the suffix.

2. DETERMINISTIC: For any adversarial function we can find a deterministic adversarial function that is a better distinguisher than the former. Suppose the adversarial function $\mathscr{A}$ has a sample space Ω. Fix $\omega \in \Omega$. Let $\mathscr{A}^{\omega}$ be a deterministic adversarial function that just executes $\mathscr{A}$ with the random coin ω. Then we have $\Delta_{\mathscr{A}}(\mathcal{O}_1;\mathcal{O}_2) = \mathbb{E}_{\mathsf{W}}\left(\Delta_{\mathscr{A}^{\mathsf{W}}}(\mathcal{O}_1;\mathcal{O}_2)\right)$. Since there must exist $\omega_0 \in \Omega$ such that $\mathbb{E}_{\mathsf{W}}\left(\Delta_{\mathscr{A}^{\mathsf{W}}}(\mathcal{O}_1;\mathcal{O}_2)\right) \leq \Delta_{\mathscr{A}^{\omega_0}}(\mathcal{O}_1;\mathcal{O}_2)$, we obtain a deterministic distinguisher $\mathscr{A}^{\omega_0}$ such that

$$\Delta_{\mathscr{A}}(\mathcal{O}_1;\mathcal{O}_2) \leq \Delta_{\mathscr{A}^{\omega_0}}(\mathcal{O}_1;\mathcal{O}_2)$$

Hence, without loss of generality, we consider only deterministic distinguishers.

3. NO REDUNDANCY: Depending on the challenge function our distinguisher is interacting with, we declare the following queries redundant. We will call the i-th query *redundant*:

- *Keyed function:* $\exists j < i : x_i = x_j$
- *Keyed strong permutation:* $\exists j < i : (\delta_i, x_i) = (\delta_j, x_j) \vee (\delta_i, x_i) = (-\delta_j, y_j)$, where y_j is the j-th response by the challenge function.
- *Tweakable keyed permutation:* $\exists j < i : (t_i = t_j) \wedge ((\delta_i, x_i) = (\delta_j, x_j) \vee (\delta_i, x_i) = (-\delta_j, y_j))$, where y_j is the j-th response by the challenge function.

In all these cases the response to the i-th query by the respective challenge function is completely determined by the j-th query-response pair, and hence the distinguisher is better off not making a redundant query. Thus we only consider those distinguishers that never make redundant queries.

QUERY COMPLEXITY IN DIFFERENT SECURITY GAMES. In the formulation above we consider a high-level adversary that has query complexity q, which in simpler terms means the adversary can make q oracle queries. However, the nature of the queries varies with the underlying examples. We consider two such important cases because they are relevant to this dissertation:

- Consider a construction where the underlying primitive, although still assumed to be random, can be public, e. g., in the PRF construction, the sum of Even Mansour, the underlying primitives are public random permutations. In this scenario, the adversary can be stateful: in the *offline phase* it queries the public permutation and in the *online phase* it queries the construction. We typically denote the bound on such an adversary's offline queries by p and the bound on online queries by q, as usual. An adversary with query complexity (p, q) is called a (p, q)*-adversary*.
- Consider variable input length construction where the underlying primitives have n-bit inputs. If a message of length m comes, it is typically broken into $\ell = \lceil m/n \rceil$ blocks and then processed by the underlying primitives. In this case it becomes necessary to parameterize the query complexity by the 3-tuple $\rho = (q, \ell, \sigma)$, where q is the number of queries, ℓ is the maximum length in blocks of any query, and σ is the total number of blocks queried. In such security games, the adversary having query complexity ρ, is called a ρ*-adversary*.

2.3 SECURITY DEFINITIONS

Let $\mathcal{O}$ be a q-bounded $(\mathscr{X}, \mathscr{Y})$ challenge function, and let $\mathscr{A}(q)$ be the space of all q-bounded $(\mathscr{X}, \mathscr{Y})$ adversarial functions. Then we define the following distinguishing advantages against $\mathcal{O}$:

PRF/(S)PRP/T(S)PRP distinguishing advantages

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{O}}(q) = \max_{\mathscr{A} \in \mathscr{A}(q)} \Delta_{\mathscr{A}}(\mathcal{O}; \boldsymbol{\rho})$$

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathcal{O}}(q) = \max_{\mathscr{A} \in \mathscr{A}(q)} \Delta_{\mathscr{A}}(\mathcal{O}; \boldsymbol{\pi}) \qquad \mathbf{Adv}^{\mathrm{sprp}}_{\mathcal{O}}(q) = \max_{\mathscr{A} \in \mathscr{A}(q)} \Delta_{\mathscr{A}}(\mathcal{O}^{\pm}; \boldsymbol{\pi}^{\pm})$$

$$\mathbf{Adv}^{\mathrm{tprp}}_{\mathcal{O}}(q) = \max_{\mathscr{A} \in \mathscr{A}(q)} \Delta_{\mathscr{A}}(\mathcal{O}; \widetilde{\boldsymbol{\pi}}) \qquad \mathbf{Adv}^{\mathrm{tsprp}}_{\mathcal{O}}(q) = \max_{\mathscr{A} \in \mathscr{A}(q)} \Delta_{\mathscr{A}}(\mathcal{O}^{\pm}; \widetilde{\boldsymbol{\pi}}^{\pm})$$

This completes the discussion on security notions.

3

H-TECHNIQUE

In this chapter, we explore the H-coefficient technique, introduced by Patarin [Pat09], and its extensions, and how they bound the distinguishing advantage of an adversary.

3.1 BOUNDING DISTINGUISHER ADVANTAGE

The assumptions on the distinguishers imply that

$$\begin{aligned}\Delta_{\mathscr{A}}(\mathscr{O}_1;\mathscr{O}_2) &= \Delta((\mathsf{W},\tau(\mathscr{A}^{\mathscr{O}_1})),(\mathsf{W},\tau(\mathscr{A}^{\mathscr{O}_2}))) && \text{by definition of } \boldsymbol{\mathscr{C}}_{\text{opt}}\\ &= \Delta(\tau(\mathscr{A}^{\mathscr{O}_1}),\tau(\mathscr{A}^{\mathscr{O}_2})) && \text{since } \mathscr{A} \text{ is deterministic}\end{aligned}$$

Thus to bound the advantage of a distinguisher, $\mathscr{A}$, in distinguishing between the two challenge functions $\mathscr{O}_1$, $\mathscr{O}_2$, we have to bound the statistical distance between the transcript random variables corresponding to the interaction of $\mathscr{A}$ with either $\mathscr{O}_1$ or $\mathscr{O}_2$.

We first present a version of the *expectation method* proposed by Hoang et al [HT16], that takes into consideration extended challenge functions. A similar version can be found in [JN22] too. The reason why we present this theorem first is because the classic coefficients H-technique exposed by Patarin in [Pat09] and even the extended version of it [JN22], can be derived from this generalized theorem.

expectation method

Theorem 3.1. *Let $\mathscr{O}_1$ and $\mathscr{O}_2$ be two $(\mathscr{X},\mathscr{Y})$ challenge functions and $\overline{\mathscr{O}}_1 = (\mathscr{O}_1,\mathscr{S}_1), \overline{\mathscr{O}}_2 = (\mathscr{O}_2,\mathscr{S}_2)$ be $\mathscr{S}$-extended version of them, respectively. Consider the random variables $\Theta_1 = \tau(\mathscr{A}^{\overline{\mathscr{O}}_1})$ and $\Theta_2 = \tau(\mathscr{A}^{\overline{\mathscr{O}}_2})$. Let $\Omega = \mathsf{Supp}(\boldsymbol{p}_{\Theta_1})$, and fix any subset $\Omega_{\text{bad}} \subseteq \Omega$. Let $\epsilon : \Omega \to [0,1]$ be a function satisfying:*

- $\epsilon(t) = 1$ *for all* $t \in \Omega_{\text{bad}}$
- $\epsilon(t) \geq \max\{0, 1 - \boldsymbol{p}_{\Theta_2}(t)/\boldsymbol{p}_{\Theta_2}(t)\}$ *for all* $t \in \Omega \setminus \Omega_{\text{bad}}$.

Then

$$\Delta_{\mathscr{A}}(\overline{\mathscr{O}}_1;\overline{\mathscr{O}}_2) \leq \mathbb{E}_{\Theta_1}\left(\epsilon(\Theta_1)\right). \tag{3.1}$$

The theorem statement follows from Lemma A.3.

In the above theorem if the function taken is such that $\epsilon(t) = \varepsilon$ for all $t \in \Omega \setminus \Omega_{\text{bad}}$, where $\varepsilon \in [0,1]$ is a constant, then the right-hand side of the inequality Eq. (3.1) becomes $\boldsymbol{p}_{\Theta_1}(\Omega_{\text{bad}}) + \varepsilon$. Thus we have the extended H-technique [JN22], given as follows:

extended H-technique

Corollary 3.0.1. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two $(\mathcal{X}, \mathcal{Y})$ challenge functions and $\overline{\mathcal{O}}_1 = (\mathcal{O}_1, \mathcal{S}_1), \overline{\mathcal{O}}_2 = (\mathcal{O}_2, \mathcal{S}_2)$ be $\mathcal{S}$-extended version of them, respectively. Consider the random variables $\Theta_1 = \tau(\mathcal{A}^{\overline{\mathcal{O}}_1})$ and $\Theta_2 = \tau(\mathcal{A}^{\overline{\mathcal{O}}_2})$. Let $\Omega = \mathsf{Supp}(\boldsymbol{p}_{\Theta_1})$, and fix any subset $\Omega_{\text{bad}} \subseteq \Omega$. If*

$$\frac{\boldsymbol{p}_{\Theta_2}(t)}{\boldsymbol{p}_{\Theta_1}(t)} \geq 1 - \varepsilon, \qquad \forall t \in \Omega \setminus \Omega_{\text{bad}}$$

then

$$\Delta_{\mathcal{A}}(\overline{\mathcal{O}}_1; \overline{\mathcal{O}}_2) \leq \boldsymbol{p}_{\Theta_1}(\Omega_{\text{bad}}) + \varepsilon. \tag{3.2}$$

All the distinguishers above were implicitly equipped with the optimal decision function $\boldsymbol{\mathcal{E}}_{\text{opt}} : \Omega \times \mathcal{X}^q \times \mathcal{Y}^q \times \mathcal{S} \to \{0,1\}$ defined as

$$\boldsymbol{\mathcal{E}}_{\text{opt}}(\omega, x^q, y^q, s) = \begin{cases} 1 & \text{if } \Pr\left(\tau(\mathcal{A}^{\mathcal{O}_1}) = (x^q, y^q), \mathcal{S}(x^q) = s\right) \\ & \quad \geq \Pr\left(\tau(\mathcal{A}^{\mathcal{O}_2}) = (x^q, y^q), \mathcal{S}'(x^q) = s\right) \\ 0 & \text{otherwise.} \end{cases}$$

Now let us consider a distinguisher that instead uses the decision predicate

$$\boldsymbol{\mathcal{E}}(\omega, x^q, y^q, s) = \begin{cases} 1 & \text{if } \Pr\left(\tau(\mathcal{A}^{\mathcal{O}_1}) = (x^q, y^q)\right) \geq \Pr\left(\tau(\mathcal{A}^{\mathcal{O}_2}) = (x^q, y^q)\right) \\ 0 & \text{otherwise.} \end{cases}$$

which, as one can see, is functionally independent of $\mathcal{S}$, i. e., the distinguisher ignores the supplements in the extended transcripts. Note that we have $\Delta_{\mathcal{A}}(\mathcal{O}_1; \mathcal{O}_2) = \Delta_{\mathcal{A}_{\boldsymbol{\mathcal{E}}}}(\overline{\mathcal{O}}_1; \overline{\mathcal{O}}_2) \leq \Delta_{\mathcal{A}_{\boldsymbol{\mathcal{E}}_{\text{opt}}}}(\overline{\mathcal{O}}_1; \overline{\mathcal{O}}_2)$. This observation leads to the coefficient H-technique [Pato9].

coefficient H-technique

Corollary 3.0.2. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two $(\mathcal{X}, \mathcal{Y})$ challenge functions. Consider the random variables $\Theta_1 = \tau(\mathcal{A}^{\mathcal{O}_1})$ and $\Theta_2 = \tau(\mathcal{A}^{\mathcal{O}_2})$. Let $\Omega = \mathsf{Supp}(\boldsymbol{p}_{\Theta_1})$, and fix any subset $\Omega_{\text{bad}} \subseteq \Omega$. If*

$$\frac{\boldsymbol{p}_{\Theta_2}(t)}{\boldsymbol{p}_{\Theta_1}(t)} \geq 1 - \varepsilon, \qquad \forall t \in \Omega \setminus \Omega_{\text{bad}}$$

then

$$\Delta_{\mathscr{A}}(\mathscr{O}_1;\mathscr{O}_2) \leq \boldsymbol{p}_{\Theta_1}(\Omega_{\text{bad}}) + \varepsilon. \tag{3.3}$$

We present here a more fine-grained version of the expectation method as follows:

Fine-grained Expectation Method

Theorem 3.2. *Let Ω be the set of all transcripts. For some $\epsilon_{\text{bad}} \geq 0$ and $\epsilon_{\text{ratio}} : \Omega \to \mathbb{R}$, suppose there is a set $\Omega_{\text{bad}} \subseteq \Omega$ satisfying the following conditions:*

- $\Pr(\Theta_0 \in \Omega_{\text{bad}}) \leq \epsilon_{\text{bad}}$,
- ϵ_{ratio} *is non-negative on* $\Omega \setminus \Omega_{\text{bad}}$,
- *for any* $\omega \notin \Omega_{\text{bad}}$, ω *is attainable and* $\dfrac{\Pr(\Theta_1 = \omega)}{\Pr(\Theta_0 = \omega)} \geq 1 - \epsilon_{\text{ratio}}(\omega)$.

Then for any distinguisher $\mathscr{A}$ trying to distinguish between $\mathscr{O}_1$ and $\mathscr{O}_0$, we have the following bound on its distinguishing advantage:

$$\Delta_{\mathscr{A}}(\mathscr{O}_1;\mathscr{O}_2) \leq \epsilon_{\text{bad}} + \mathbb{E}_{\Theta_0}\left(\chi_{\mathit{good}}\epsilon_{\text{ratio}}\right),$$

where χ_{good} denotes the indicator function for $\Omega \setminus \Omega_{\text{bad}}$.

H-technique is the umbrella term that applies for all three methods (Theorem 3.1, Corollaries 3.0.1 and 3.0.2) defined above, and although the latter two methods are derivatives of the expectation method, we will use them in security proofs of different cryptographic constructions, according to suitability.

3.2 MIRROR THEORY AS A CONSEQUENCE OF H-TECHNIQUE: A TOY EXAMPLE

OPTIMAL PRF SECURITY OF THE XOR_1 CONSTRUCTION. Consider the $(\{0,1\}^{n-1}, \{0,1\}^n)$ challenge function $\mathscr{O}$ defined as $\mathscr{O}(x) = \pi(0\|x) \oplus \pi(1\|x)$ where π is a $\{0,1\}^n$ random permutation, i. e., $\pi \xleftarrow{\$} \text{Perm}(\{0,1\}^n)$. We want to find out the PRF security of the above construction, i. e., we want to calculate $\mathbf{Adv}^{\text{prf}}_{\mathscr{O}}(q) = \max_{\mathscr{A}\in\mathscr{A}(q)} \Delta_{\mathscr{A}}(\mathscr{O};\rho)$, where ρ is a $(\{0,1\}^{n-1}, \{0,1\}^n)$ random function. To bound $\Delta_{\mathscr{A}}(\mathscr{O};\rho)$ via the coefficient H-technique (Corollary 3.0.2). Consider the naive decision predicate, $\boldsymbol{\mathscr{d}} : (\{0,1\}^{n-1})^q \times (\{0,1\}^n)^q \to \{0,1\}$, defined as

$$\boldsymbol{\mathscr{d}}(x^q, y^q) = \begin{cases} 1, & \text{if } \exists i \in [q] : y_i = 0. \\ 0, & \text{otherwise.} \end{cases}$$

Note that for any adversarial function $\mathscr{A} \in \boldsymbol{\mathscr{A}}(q)$, we have $\Pr\left(\boldsymbol{\mathscr{E}}(\tau(\mathscr{A}^{\mathcal{O}})) = 1\right) = 0$, while $\Pr\left(\boldsymbol{\mathscr{E}}(\tau(\mathscr{A}^{\boldsymbol{\rho}})) = 1\right) = q/2^n$. Thus $\Delta_{\mathscr{A}_{\boldsymbol{\mathscr{E}}}}(\mathcal{O}; \boldsymbol{\rho}) = q/2^n$. We will show soon enough that no distinguisher can do any better than this naive distinguisher.

In this distinguishability scenario, all transcripts are attainable, in the sense that $\Omega = \mathsf{Supp}(\tau(\mathscr{A}^{\boldsymbol{\rho}})) = (\{0,1\}^{n-1})^q \times (\{0,1\}^n)^q$. We define the subset of bad transcripts as $\Omega_{\mathrm{bad}} = \{(x^q, y^q) : y_i = 0 \text{ for some } i \in [q]\} = \mathsf{Supp}(\tau(\mathscr{A}^{\boldsymbol{\rho}})) \setminus \mathsf{Supp}(\tau(\mathscr{A}^{\mathcal{O}}))$, where due to the last equality $\mathcal{O}$ and $\boldsymbol{\rho}$ are obviously distinguishable, as is also seen with above naive distinguisher. Letting $\Theta_1 := \tau(\mathscr{A}^{\boldsymbol{\rho}})$ and $\Theta_2 := \tau(\mathscr{A}^{\mathcal{O}})$, we have $\boldsymbol{p}_{\Theta_1}(\Omega_{\mathrm{bad}}) = q/2^n$ and $\boldsymbol{p}_{\Theta_1}(x^q, y^q) = 2^{-nq}$, by definition of the random function (Definition 2.6). If we could prove $\boldsymbol{p}_{\Theta_2}(x^q, y^q) \geq 2^{-nq}$ for all $(x^q, y^q) \in \Omega \setminus \Omega_{\mathrm{bad}}$, then by the coefficient H-technique (here $\varepsilon = 0$, see Corollary 3.0.2), we have $\Delta_{\mathscr{A}}(\mathcal{O}; \boldsymbol{\rho}) \leq q/2^n$, for any adversarial function $\mathscr{A} \in \boldsymbol{\mathscr{A}}(q)$, thus implying n-bit PRF security of $\mathcal{O}$.

Now, let us define the $2q$ random variables: $\mathsf{V}_{2i-1} := \boldsymbol{\pi}(0\|x_i)$ and $\mathsf{V}_{2i} := \boldsymbol{\pi}(1\|x_i)$ for $i \in [q]$. Consider the system of equations and non-equations given below, which must be satisfied for the event, $\mathcal{O}(x^q) = y^q$, to hold:

(EQUATIONS). $\mathsf{V}_{2i-1} \oplus \mathsf{V}_{2i} = y_i$ for $i \in [q]$.

(NON-EQUATIONS). $\mathsf{V}_i \neq \mathsf{V}_j$, which can be equivalently written as $\mathsf{V}_i \oplus \mathsf{V}_j \neq 0$, for $i, j \in [q]$, $i \neq j$.

If the number of solutions to the above system of equations and non-equations i. e., the number of $2q$-tuples of n-bit numbers satisfying the above system, is at least N, then we have $\boldsymbol{p}_{\Theta_2}(x^q, y^q) \geq N/(2^n)_{2q}$. Thus to show n-bit PRF security of $\mathcal{O}$, we need to show that *the number of solutions to the above system of equations and non-equations is at least* $(2^n)_{2q}/2^{nq}$. The italicized statement is in fact a particular case of Mirror theory, as we will introduce next.

Part II

RESULTS AND PROOFS

In the second part of the dissertation, we introduce the Mirror Theory Problem in general, discuss some of its variants, claim lower bounds to the number of solutions corresponding to each variant, and prove them using combinatorial arguments.

4

THE MIRROR THEORY PROBLEM

The Mirror Theory Problem is a combinatorial optimization problem, specifically a *lower-bound analysis of the number of solutions to a system of equations and non-equations over a field*. A system of equations over a field is a well-defined algebraic notion, and the number of solutions to such a system on discrete fields can be counted straightforwardly, by just keeping in mind that given a solution, all other solutions can be found by translating the kernel, of the coefficient matrix of the system, by the given solution. The size of the kernel itself is determined by the rank of the coefficient matrix. However, when you throw *non-equations*, like $X_1 + \cdots + X_j \neq \lambda$, in the mix, the number of solutions is not yet determined.

The Mirror Theory Problem

A particular problem in $\texttt{MTP}^{(v,e,n)}$, the class of Mirror Theory problems with parameters $v, e, n \in \mathbb{N}$, representing the number of variables, equations and non-equations, respectively, is instantiated by

- A vector space $\mathbb{V}$ over a finite field $(\mathbb{F}, +, \cdot)$.
- $\boldsymbol{a}^e = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_e)$, with $\boldsymbol{a}_i \in \mathbb{F}^v$, denoting the coefficients of the i-th equation, for all $i \in [e]$.
- $\boldsymbol{b}^n = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, with $\boldsymbol{b}_i \in \mathbb{F}^v$, denoting the coefficients of the i-th non-equation, for all $i \in [n]$.
- $\lambda^e = (\lambda_1, \ldots, \lambda_e) \in \mathbb{V}^e$, where λ_i is the constants of the i-th equation, for $i \in [e]$.
- $\theta^n = (\theta_1, \ldots, \theta_n) \in \mathbb{V}^n$, where θ_i is the constants of the i-th non-equation, for $i \in [n]$.
- $\mathbb{V}^* \subseteq \mathbb{V}$, the set where the v variables can take values from.

This particular problem, denoted as $\texttt{MTP}(\boldsymbol{a}^e, \boldsymbol{b}^n, \lambda^e, \theta^n, \mathbb{V}^*)$, is to *find the number of solutions to the following system of equations and non-equations*:

(EQUATIONS). $\boldsymbol{a}_{i,1} \cdot \mathsf{X}_1 + \cdots + \boldsymbol{a}_{i,v} \cdot \mathsf{X}_v = \lambda_i$, $i \in [e]$.

(NON-EQUATIONS). $\boldsymbol{b}_{i,1} \cdot \mathsf{X}_1 + \cdots + \boldsymbol{b}_{i,v} \cdot \mathsf{X}_v \neq \theta_i$, $i \in [n]$.

where $\mathsf{X}_1, \ldots, \mathsf{X}_v$ are $\mathbb{V}^*$-valued variables . $\boldsymbol{x}^v = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_v) \in (\mathbb{V}^*)^v$ is called a solution to the above system of equations and non-equations, if assigning the values $\mathsf{X}_i = \boldsymbol{x}_i$ the left-hand side and right-hand side of the equations match, and the left-hand side and right-hand side of the non-equations do not match.

SIMPLIFICATIONS. Due to the challenging nature of the mirror theory problem in its current state, we mitigate its complexity through substantial simplifications for the scope of this dissertation:

- Since the dissertation is cryptographically motivated, we restrict ourselves to the vector space $\mathbb{F}_2^m$ over the binary field $(\mathbb{F}_2, \oplus, \bullet)$, where $\oplus$ is the *bitwise-xor operation* (involutive), and $\bullet$ is bitwise scalar multiplication.
- The Mirror Theory Problem with non-homogenous system of non-equations is out of the scope of this dissertation. Here we are only concerned with non-equations, with 0^m as constants. A bivariate non-equation with constant 0^m, $\mathsf{X}_i \oplus \mathsf{X}_j \neq 0^m$ can be alternatively written as $\mathsf{X}_i \neq \mathsf{X}_j$.

4.1 MIRROR THEORY WITH BIVARIATE SYSTEM OF EQUATIONS

Since xor-ing is essentially sequential in the summands, in this section we restrict ourselves to *bivariate systems of equations and non-equations*, where every equation or non-equation has exactly two variables that have to be xor-ed just once. This means that in the problems we will consider $\mathrm{wt}(\boldsymbol{a}_i) = 2$, $i \in [e]$ and $\mathrm{wt}(\boldsymbol{b}_i) = 2$, $i \in [n]$.

Complete Homogeneous Bivariate Mirror Theory Problem

The *complete homogeneous bivariate Mirror Theory Problem* instantiated by

- $\boldsymbol{a}^e = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_e)$, with $\boldsymbol{a}_i \in \mathbb{F}_2^v$, $\mathrm{wt}(\boldsymbol{a}_i) = 2$, for all $i \in [e]$.
- $\lambda^e = (\lambda_1, \ldots, \lambda_e) \in (\mathbb{F}_2^m)^e$.

also denoted as $\texttt{CMTP}(\boldsymbol{a}^e, \lambda^e)$, is to find the number of solutions to the system of equations and non-equations:

(EQUATIONS). $\boldsymbol{a}_{i,1}\mathsf{X}_1 \oplus \cdots \oplus \boldsymbol{a}_{i,v}\mathsf{X}_v = \lambda_i$, $i \in [e]$.

(NON-EQUATIONS). $\mathsf{X}_i \neq \mathsf{X}_j$ for all $i, j \in [v], i \neq j$.

If the variables are restricted to take values from $\mathbb{V}^* \subseteq \mathbb{F}_2^m$, then the problem is called *restricted complete homogeneous bivariate Mirror Theory Problem*, denoted as $\texttt{RCMTP}(\boldsymbol{a}^e, \lambda^e, \mathbb{V}^*)$. Of course, $\texttt{CMTP}(\boldsymbol{a}^e, \lambda^e) = \texttt{RCMTP}(\boldsymbol{a}^e, \lambda^e, \mathbb{F}_2^m)$.

Bipartite Homogeneous Bivariate Mirror Theory Problem

The *bipartite homogeneous bivariate Mirror Theory Problem* instantiated by

- A bipartition (A, B) of $[v]$, i.e. $[v] = A \sqcup B$.
- $\boldsymbol{a}^e = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_e)$, with $\boldsymbol{a}_i \in \mathbb{F}_2^v$, $\mathrm{wt}(\boldsymbol{a}_i|_A) = 1$, $\mathrm{wt}(\boldsymbol{a}_i|_B) = 1$, for all $i \in [e]$.
- $\lambda^e = (\lambda_1, \ldots, \lambda_e) \in (\mathbb{F}_2^m)^e$.

also denoted as $\texttt{BMTP}((A, B), \boldsymbol{a}^e, \lambda^e)$, is to find the number of solutions to the system of equations and non-equations:

(EQUATIONS). $\boldsymbol{a}_{i,1}\mathsf{X}_1 \oplus \cdots \oplus \boldsymbol{a}_{i,v}\mathsf{X}_v = \lambda_i$, $i \in [e]$.

(NON-EQUATIONS). $\begin{array}{l} \mathsf{X}_i \neq \mathsf{X}_j \text{ for all } i, j \in A, i \neq j \\ \mathsf{X}_i \neq \mathsf{X}_j \text{ for all } i, j \in B, i \neq j \end{array}$.

4.1.1 *Graphical representation of a system of bivariate equations*

Given $\boldsymbol{a}^e = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_e)$, with $\boldsymbol{a}_i \in \mathbb{F}_2^v$, $\mathrm{wt}(\boldsymbol{a}_i) = 2$, $i \in [e]$, and $\lambda^e = (\lambda_1, \ldots, \lambda_e) \in (\mathbb{F}_2^m)^e$, we denote the system of equations

$$\boldsymbol{a}_{i,1}\mathsf{X}_1 \oplus \cdots \oplus \boldsymbol{a}_{i,v}\mathsf{X}_v = \lambda_i, \ i \in [e] \tag{4.1}$$

as $\mathscr{E}(\boldsymbol{a}^e, \lambda^e)$. For any permutation σ on $[e]$, the set of all solutions to $\mathscr{E}(\boldsymbol{a}^e, \lambda^e)$, denoted as $\mathcal{S}(\boldsymbol{a}^e, \lambda^e) \subset (\mathbb{V}^*)^v$, is exactly same as $\mathcal{S}(\boldsymbol{a}^{\sigma[e]}, \lambda^{\sigma[e]})$, the set of all solutions to $\mathscr{E}(\boldsymbol{a}^{\sigma[e]}, \lambda^{\sigma[e]})$, where $\boldsymbol{a}^{\sigma[e]} = (\boldsymbol{a}_{\sigma 1}, \boldsymbol{a}_{\sigma 2}, \ldots, \boldsymbol{a}_{\sigma v})$, and $\lambda^{\sigma[e]} = (\lambda_{\sigma 1}, \lambda_{\sigma 2}, \ldots, \lambda_{\sigma v})$. In other words, the order of the equations does not affect the solution set, and hence we are going to ignore it. Let us define an equivalence relation between the system of equations (as defined in Eq. (4.1)), as follows: we say $\mathscr{E}(\boldsymbol{a}^e, \lambda^e) \sim \mathscr{E}(\boldsymbol{b}^e, \gamma^e)$ if $\boldsymbol{b}^e = \boldsymbol{a}^{\sigma[e]}$ and $\gamma^e = \lambda^{\sigma[e]}$ for some permutation σ over $[e]$. Let us denote the equivalence class of $\mathscr{E}(\boldsymbol{a}^e, \lambda^e)$ under $\sim$, as $\mathscr{E}[\boldsymbol{a}^e, \lambda^e]$. This equivalence class can be thought of as an unordered system of equations, depending only on the multiset of coefficient-constant pairs, $\{\!\{(\boldsymbol{a}_1, \lambda_1), \ldots, (\boldsymbol{a}_e, \lambda_e)\}\!\}$. Let us denote the collection of all these equivalence classes, each having v m-bit variables and e bivariate equations, as $\texttt{EQC}^{(v,e,\mathbb{F}_2^m)}$.

Now consider the following collection of graphs:

$$\texttt{GC}^{(v,e,\mathbb{F}_2^m)} := \{([v], E, L) : |E| = e, L : E \to \mathbb{F}_2^m\}$$

There is a one-to-one correspondence between $\texttt{EQC}^{(v,e,\mathbb{F}_2^m)}$ and $\texttt{GC}^{(v,e,\mathbb{F}_2^m)}$ defined as follows: For an unordered system of equations $\mathscr{E} := \mathscr{E}[\boldsymbol{a}^e, \lambda^e] \in \texttt{EQC}^{(v,e,\mathbb{F}_2^m)}$, let

$$\mathscr{G}(\mathscr{E}) := \left\{ j_1 \xrightarrow{\lambda_i} j_2 : \boldsymbol{a}_{i,j_1} = \boldsymbol{a}_{i,j_2} = 1, i \in [e] \right\} \in \texttt{GC}^{(v,e,\mathbb{F}_2^m)}$$

Conversely, for any graph $\mathscr{G} = ([v], E, L) \in \texttt{GC}^{(v,e,\mathbb{F}_2^m)}$, we define $\mathscr{E}(\mathscr{G}) := \mathscr{E}[\boldsymbol{a}^e, \lambda^e]$, where for any ordering of the edges in E, say $E_1 = \{j_1, k_1\}, \ldots, E_e = \{j_e, k_e\}$,

$$\boldsymbol{a}_i = \mathbb{1}_v(j_1, j_2); \text{ and } \lambda_i = L(E_i), \qquad i \in [e].$$

We recall that $\mathbb{1}_v(j_1, j_2) \in \mathbb{F}_2^v$ has only two non-zero bits, the j_1-th and j_2-th bits.

$$\begin{aligned}
\mathsf{X}_1 \oplus \mathsf{X}_2 &= \lambda_1 \\
\mathsf{X}_1 \oplus \mathsf{X}_3 &= \lambda_2 \\
\mathsf{X}_4 \oplus \mathsf{X}_5 &= \lambda_3 \\
\mathsf{X}_3 \oplus \mathsf{X}_6 &= \lambda_4 \\
\mathsf{X}_6 \oplus \mathsf{X}_1 &= \lambda_5 \\
\mathsf{X}_4 \oplus \mathsf{X}_7 &= \lambda_6
\end{aligned}$$

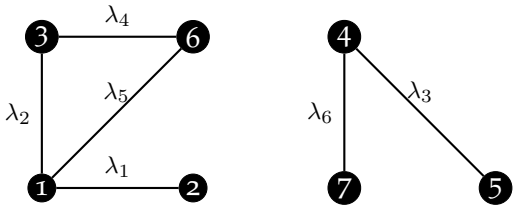


Figure 4.1: The system of equations on the left is equivalent to the labeled undirected graph on the right.

4.1.2 *Consistency conditions for* CMTP *and* BMTP

CYCLES. Suppose $\boldsymbol{x}^v = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_v) \in (\mathbb{V}^*)^v$ satisfies the unordered system of equations $\mathscr{E}$. If, $\mathscr{G}(\mathscr{E})$, the corresponding undirected edge-labeled graph, has a cycle

$$j_1 \xrightarrow{\lambda_1} j_2 \xrightarrow{\lambda_2} \cdots \xrightarrow{\lambda_{p-1}} j_p \xrightarrow{\lambda_p} j_1,$$

then adding up the following equalities (which hold since $\boldsymbol{x}^v$ is a solution to $\mathscr{E}$),

$$\boldsymbol{x}_{j_1} \oplus \boldsymbol{x}_{j_2} = \lambda_1, \boldsymbol{x}_{j_2} \oplus \boldsymbol{x}_{j_3} = \lambda_2, \ldots, \boldsymbol{x}_{j_p} \oplus \boldsymbol{x}_{j_1} = \lambda_p$$

we get $\bigoplus_{i \in [p]} \lambda_i = 0^m$. Thus we have established that *for a system of equations $\mathscr{E}$ to have a solution, any cycle in the corresponding graph $\mathscr{G}(\mathscr{E})$ must have label-sum 0^m.*

The above observation can be alternatively stated as follows: *if some linear combination of the coefficient vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_e$ is null, then the same linear combination of the constants $\lambda_1, \ldots, \lambda_e$ is also null,* i. e., $\boldsymbol{a}_{i_1} \oplus \cdots \oplus \boldsymbol{a}_{i_p} = 0^v \implies \lambda_{i_1} \oplus \cdots \oplus \lambda_{i_p} = 0^m$. This is because if $\boldsymbol{a}_{i_1}, \ldots, \boldsymbol{a}_{i_p}$ sum to zero, then the edges corresponding to $\boldsymbol{a}_{i_j}$, $j \in [p]$ (i. e., the edge $\{k_1, k_2\}$ if $\boldsymbol{a}_{i_j} = \mathbb{1}_v(k_1, k_2)$), form a cycle (or a disjoint union of cycles) in $\mathscr{G}(\mathscr{E})$.

PATHS. Now let $\boldsymbol{x}^v$ be a solution to the system of equations $\mathscr{E}$ that also satisfy the non-equation $\mathsf{X}_i \neq \mathsf{X}_j$. Now if there is a path between the vertices i and j, say $i \xrightarrow{\lambda_1} i_1 \xrightarrow{\lambda_2} \cdots \xrightarrow{\lambda_{p-1}} i_{p-1} \xrightarrow{\lambda_p} j$, then summing the equalities $\boldsymbol{x}_i \oplus \boldsymbol{x}_{i_1} = \lambda_1, \boldsymbol{x}_{i_1} \oplus \boldsymbol{x}_{i_2} = \lambda_2, \ldots, \boldsymbol{x}_{i_{p-1}} \oplus \boldsymbol{x}_j = \lambda_p$, we get $\boldsymbol{x}_i \oplus \boldsymbol{x}_j = \bigoplus_{i\in[p]} \lambda_i$, and hence, since $\boldsymbol{x}_i \neq \boldsymbol{x}_j$, we must have $\bigoplus_{i\in[p]} \lambda_i \neq 0^m$. This establishes that *a system of equations has a solution satisfying the non-equation $\mathsf{X}_i \neq \mathsf{X}_j$ if and only any path between the vertices i and j in $\mathscr{G}(\mathscr{E})$ has non non-zero label-sum.*

Definition 4.1 (consistent system). *A system of equations and non-equations is called* consistent *if it has at least one solution.*

Lemma 4.1 (consistency conditions). *The system of equations and non-equations in* $\texttt{CMTP}(\boldsymbol{a}^e, \lambda^e)$ *is consistent if:*

- *Every cycle in $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$ must have label-sum 0^m.*
- *Every path in $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$ must have non-zero label-sum.*

The system of equations and non-equations in $\texttt{BMTP}((A, B), \boldsymbol{a}^e, \lambda^e)$ *is consistent if:*

- *Every cycle in $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$ must have label-sum 0^m.*
- *Every even-length path in $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$ must have non-zero label-sum.*

The proof of this consistency lemma follows from the discussion above. For the second part of the lemma, one should note that the graph, $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$, for the $\texttt{BMTP}((A, B), \boldsymbol{a}^e, \lambda^e)$ problem, is a bipartite graph with shores A and B, and the non-equations are between variables indexed by the same shore, implying that any path between them would be of even length.

4.1.3 *Standard Form of a System of Equations*

Note that, if indeed for some m-bit numbers $\lambda_1, \ldots, \lambda_p$, we have $\bigoplus_{i\in[p]} \lambda_i = 0^m$, then for any m-bit numbers, $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_p$,

$$\boldsymbol{x}_i \oplus \boldsymbol{x}_{i+1} = \lambda_i \; \forall i \in [p-1] \implies \boldsymbol{x}_p \oplus \boldsymbol{x}_1 = \lambda_p.$$

This implies that, given $\mathscr{E}$ has at least one solution, for any cycle, $j_1 \xrightarrow{\lambda_1} j_2 \xrightarrow{\lambda_2} \cdots \xrightarrow{\lambda_{p-1}} j_p \xrightarrow{\lambda_p} j_1$ in $\mathscr{G}(\mathscr{E})$, one can simply drop one of the edges, say e. g., the edge $j_p \xrightarrow{\lambda_p} j_1$, or alternatively remove the equation corresponding to the edge, i. e., remove the coefficient-constant pair $(\mathbb{1}_v(j_1, j_2), \lambda_p)$ from the multiset of coefficient-constant pairs of $\mathscr{E} \in \texttt{EQC}^{(v,e,\mathbb{F}_2^m)}$, and obtain the reduced system of equations $\mathscr{E}' \in \texttt{EQC}^{(v,e-1,\mathbb{F}_2^m)}$, such that set of all solutions to $\mathscr{E}$ is exactly same as the set of all solutions of $\mathscr{E}'$. In other words,

$$\begin{aligned}
\mathsf{X}_1 \oplus \mathsf{X}_2 &= \lambda_1 \\
\mathsf{X}_1 \oplus \mathsf{X}_3 &= \lambda_2 \\
\mathsf{X}_4 \oplus \mathsf{X}_5 &= \lambda_3 \\
\mathsf{X}_3 \oplus \mathsf{X}_6 &= \lambda_4 \\
\cancel{\mathsf{X}_6 \oplus \mathsf{X}_1 = \lambda_5} & \\
\mathsf{X}_4 \oplus \mathsf{X}_7 &= \lambda_6
\end{aligned}$$

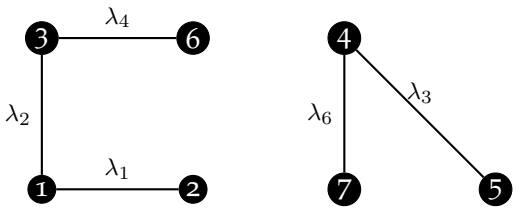


Figure 4.2: One can check in Fig. 4.1, that the graph has the cycle $1 \xrightarrow{\lambda_2} 3 \xrightarrow{\lambda_4} 6 \xrightarrow{\lambda_5} 1$, which implies that for this system of equations to have a solution we must have $\lambda_2 \oplus \lambda_4 \oplus \lambda_5 = 0^m$, in which case the equation $\mathsf{X}_6 \oplus \mathsf{X}_1 = \lambda_5$ becomes redundant.

linear dependency among the coefficient vectors leads to redundant equations. Thus we can assume without of loss of generality that our *collection of coefficient vectors is linearly independent*, or equivalently assume that $\mathscr{G}(\mathscr{E})$ *is acyclic*.

Given an undirected graph $\mathscr{G}$, consider the equivalence relation $\rightsquigarrow$ on the vertex set of $\mathscr{G}$, where $u \rightsquigarrow v$ is there if a path from u to v. Then the equivalence classes are called the components of the graph. Let $\mathtt{GC}^{(v,e,\mathbb{F}_2^m,c)}$ be the class of graphs having vertex set $[v]$, e edges and an m-bit edge-labeling function, such that the graph has c components. We define a transformation $\mathrm{Star} : \mathtt{GC}^{(v,e,\mathbb{F}_2^m,c)} \to \mathtt{GC}^{(v,v-c,\mathbb{F}_2^m,c)}$, under which a graph $\mathscr{G} \in \mathtt{GC}^{(v,e,\mathbb{F}_2^m,c)}$ is mapped to a graph $\mathscr{S} := \mathrm{Star}(\mathscr{G}) \in \mathtt{GC}^{(v,v-c,\mathbb{F}_2^m,c)}$, such that each of the c components of $\mathscr{S}$ is a *star*[1], and the set of all solutions to $\mathscr{E}(\mathscr{G})$ is exactly same as the set of all solutions to $\mathscr{E}(\mathscr{S})$. The transformation Star is defined as follows: For a graph $\mathscr{G} = ([v], E, L) \in \mathtt{GC}^{(v,e,\mathbb{F}_2^m,c)}$, let $[v]/\rightsquigarrow = \{[\![v_i]\!] : i \in c\}$, where v_i is the representative of the i-th equivalence class, or, in other words, v_i is some arbitrary vertex of the i-th component, denoted as $[\![v_i]\!]$. Then

$$\mathrm{Star}(\mathscr{G}) := \bigsqcup_{i \in [c]} \left\{ v_i \xrightarrow{L(P_{u \rightsquigarrow v})} u : \forall u \in [\![v_i]\!], u \neq v_i \right\}$$

where $P_{u \rightsquigarrow v}$ is any path from u to v, and $L(P_{u \rightsquigarrow v})$ is the sum of the labels of the edges of the said path. Note that, if a system of equations has at least one solution, then any two paths between vertices u and v will have the same label sum, and hence the above transformation is well-defined.

Also, note that the transformation depends on the particular choice of the vertices v_i, one from each component. Different choices of such representative vertices would have led to isomorphic graphs having star components, albeit with different edge labels. The choice of the representative vertices does not matter because the system of equations, corresponding to each such graph, will have the same set of solutions.

1 A *star* of v vertices, contains a vertex with degree $v - 1$ (also called the *center* of the star), and all the other vertices have degree 1.

$$
\begin{aligned}
\mathsf{X}_2 \oplus \mathsf{X}_1 &= \lambda_1 \\
\mathsf{X}_2 \oplus \mathsf{X}_3 &= \lambda_1 \oplus \lambda_2 \\
\mathsf{X}_2 \oplus \mathsf{X}_6 &= \lambda_1 \oplus \lambda_2 \oplus \lambda_4 \\
\mathsf{X}_4 \oplus \mathsf{X}_5 &= \lambda_3 \\
\mathsf{X}_4 \oplus \mathsf{X}_7 &= \lambda_6
\end{aligned}
$$

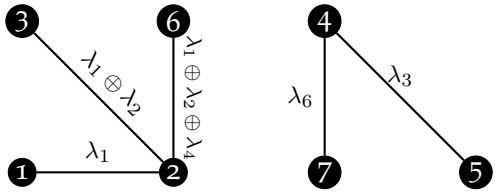


Figure 4.3: The system of equations given here is in the standard form and is equivalent to the system of equations given in Fig. 4.1

Definition 4.2 (standard form). *We say that a system of equations, $\mathscr{E}$, is in* standard form *if every component of $\mathscr{G}(\mathscr{E})$ is a star. For any system of equations $\mathscr{E}$, we say that $\mathscr{E}(\mathrm{Star}(\mathscr{G}(\mathscr{E})))$ is a* standardized version *of $\mathscr{E}$.*

As any system of equations, that has at least one solution, can be standardized, we reformulate our Mirror Theory problems assuming that the corresponding system of equations *is* in standard form. Since a system of equations has the exact same set of solutions as its standardized version, such an assumption is without loss of generality.

4.2 MIRROR THEORY WITH GENERAL SYSTEM OF EQUATIONS

A general system of equations over $\mathbb{F}_2^m$ can be represented as $\mathbf{A}\mathsf{X}^v = \boldsymbol{\lambda}^e$, where $\mathbf{A} \in \mathbb{F}_2^{e \times v}$ is a $e \times v$ binary matrix, with i-th row the coefficient vector of the i-th equation, $\boldsymbol{a}_i$, $\mathsf{X}^v = (\mathsf{X}_1, \ldots, \mathsf{X}_v)$ is the vector of v variables, and $\boldsymbol{\lambda}^e = (\lambda_1, \ldots, \lambda_e)$ is the vector of constant of the equations, as mentioned in the definition of the MTP problem. Note that if $\mathbf{A}$ has a zero column then the variable corresponding to this column does not appear in the system of equations and hence can be ignored. Thus we assume that $\mathbf{A}$ has no zero column.

Of course, an equation having more than two variables cannot be represented by a graph edge, but we can still borrow the ideas from the graphical representation of bivariate systems and adapt it to the general case:

COMPONENTS. Consider the augmented matrix $\mathbf{A}|\boldsymbol{\lambda}$ corresponding to a system of equations. We say that two rows $\boldsymbol{a}_i|\lambda_i$ and $\boldsymbol{a}_j|\lambda_j$ are *adjacent*, denoted $\boldsymbol{a}_i|\lambda_i \sim \boldsymbol{a}_j|\lambda_j$ if and only if $\boldsymbol{a}_i$ and $\boldsymbol{a}_j$ share a common column index with non-zero entry. We say that two rows $\boldsymbol{a}_i|\lambda_i$ and $\boldsymbol{a}_j$ are *connected*, denoted $\boldsymbol{a}_i|\lambda_i \rightsquigarrow \boldsymbol{a}_j|\lambda_j$, if and only if there exists a (possibly empty) sequence of rows $(\boldsymbol{a}_{k_1}, \ldots, \boldsymbol{a}_{k_u})$ such that $\boldsymbol{a}_i \sim \boldsymbol{a}_{k_1} \sim \cdots \sim \boldsymbol{a}_{k_u} \sim \boldsymbol{a}_j$. Then, $\rightsquigarrow$ is an equivalence relation on $\mathrm{row}(\mathbf{A}|\boldsymbol{\lambda})$, effectively partitioning $\mathrm{row}(\mathbf{A}|\boldsymbol{\lambda}) = \mathbf{A}_1|\boldsymbol{\lambda}_1 \sqcup \cdots \sqcup \mathbf{A}_c|\boldsymbol{\lambda}_c$. With a slight abuse of notations, we also write $\mathbf{A}_i|\boldsymbol{\lambda}_i$ to

denote the $e_i \times (v+1)$ submatrix (also referred as a *component*) of $\mathbf{A}|\boldsymbol{\lambda}$ corresponding to the equivalence class $\mathbf{A}_i|\boldsymbol{\lambda}_i = \{\boldsymbol{a}_{j_1}|\lambda_{j_1}, \ldots, \boldsymbol{a}_{j_{q_i}}|\lambda_{j_{q_i}}\}$, i.e.

$$\mathbf{A}_i|\boldsymbol{\lambda}_i = \begin{pmatrix} \boldsymbol{a}_{j_1}|\lambda_{j_1} \\ \vdots \\ \boldsymbol{a}_{j_{q_i}}|\lambda_{j_{q_i}} \end{pmatrix},$$

where $\sum_i e_i = e$. For each component $\mathbf{A}_i|\boldsymbol{\lambda}_i$ of $\mathbf{A}|\boldsymbol{\lambda}$, let $\overline{\mathbf{A}}_i$ denote the *column-reduced form* of $\mathbf{A}_i$, which is obtained by simply dropping all the zero columns from $\mathbf{A}_i$. The rank of $\overline{\mathbf{A}}_i$ is the same as the rank of $\mathbf{A}_i$. Let $v_i := |\mathrm{col}(\overline{\mathbf{A}}_i)|$ and $\sum_i v_i = v$. For any $i \in [c]$, we say that $\mathbf{A}_i|\boldsymbol{\lambda}_i$ is *isolated* if $q_i = 1$. By extension, $\mathbf{A}|\boldsymbol{\lambda}$ is said to be isolated if $\mathbf{A}_i|\boldsymbol{\lambda}_i$ is isolated for all $i \in [c]$.

Note that, both the relations, $\sim$ and $\sim\!\!\sim$, are independent of $\boldsymbol{\lambda}$. Accordingly, we often view them as relations on $\mathrm{row}(\mathbf{A})$.

Definition 4.3 (Acyclic matrix). *Any matrix $\mathbf{A}|\boldsymbol{\lambda}$ is said to be cyclic if and only if there exists:*

- *two rows $\boldsymbol{a}_i$ and $\boldsymbol{a}_j$ that share at least two non-zero column indices; or*
- *a sequence of three or more distinct rows $\boldsymbol{a}_{i_1}|\lambda_{i_1}, \boldsymbol{a}_{i_2}|\lambda_{i_2}, \boldsymbol{a}_{i_3}|\lambda_{i_3}, \ldots, \boldsymbol{a}_{j_k}|\lambda_{j_k}$ such that $\boldsymbol{a}_{i_1}|\lambda_{i_1} \sim \boldsymbol{a}_{i_2}|\lambda_{i_2} \sim \boldsymbol{a}_{i_3}|\lambda_{i_3} \sim \ldots \sim \boldsymbol{a}_{j_k}|\lambda_{j_k} \sim \boldsymbol{a}_{i_1}\lambda_{i_1}$.*

All other systems are called acyclic.

Definition 4.4 (Canonical Component Form). *Let $\mathbf{A}_1|\boldsymbol{\lambda}_1 \sqcup \cdots \sqcup \mathbf{A}_c|\boldsymbol{\lambda}_c$ be the partitioning of $\mathrm{row}(\mathbf{A}|\boldsymbol{\lambda})$ with respect to $\sim\!\!\sim$. The component form (CF) of $\mathbf{A}|\boldsymbol{\lambda}$ with respect to an arbitrary ordering $(\mathbf{A}_{i_1}|\boldsymbol{\lambda}_{i_1}, \ldots, \mathbf{A}_{i_c}|\boldsymbol{\lambda}_{i_c})$ is defined as the block matrix*

$$\mathrm{CF}(\mathbf{A}|\boldsymbol{\lambda}) := \begin{pmatrix} \overline{\mathbf{A}}_{i_1} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_{i_1} \\ \mathbf{0} & \overline{\mathbf{A}}_{i_2} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_{i_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_{i_c} & \boldsymbol{\lambda}_{i_c} \end{pmatrix}$$

$\mathbf{A}|\boldsymbol{\lambda}$ can have several component forms. Unless stated otherwise, we always assume that the system $\mathbf{A}|\boldsymbol{\lambda}$ is in some component form, for if not, it can be placed in CF by swapping of rows and columns.

CLIQUES OF NON-EQUATIONS. Note that a system of bivariate non-equations can also be viewed as a labeled undirected graph, with one edge corresponding to each non-equation. In CMTP we have dealt with non-equations with the corresponding graph being complete, while in BMTP, the graph of the non-equations consists of exactly two cliques. Here we generalize this notion so that the graph of the system of non-equations contains k cliques.

Restricted Mirror Theory Problem

The *restricted Mirror Theory problem* instantiated by

- An acyclic matrix in component form

$$\mathbf{A}|\boldsymbol{\lambda} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_c & \boldsymbol{\lambda}_c \end{pmatrix} \in \mathbb{F}_2^{e\times(v+1)}.$$

  with $\overline{\mathbf{A}}_i \in \mathbb{F}_2^{e_i\times v_i}, \boldsymbol{\lambda}_i \in (\mathbb{F}_2^m)^{e_i\times 1}; \sum_i r_i = e, \sum_i v_i = v$.

- An equivalence relation $\simeq$ inducing the partition $\mathscr{P} := (P_1, \ldots, P_k)$ of $[v]$, i.e., $[v] = P_1 \sqcup \cdots \sqcup P_k$.

- A family of sets $\mathscr{R} = \{R_i \subseteq \mathbb{F}_2^m\}_{i\in[k]}$

also denoted as $\texttt{RMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$, is to find the number of solutions to the system of equations and non-equations:

(EQUATIONS). $\mathbf{A}\mathsf{X}^v = \boldsymbol{\lambda}$

(NON-EQUATIONS). $\begin{array}{ll} \mathsf{X}_i \neq \mathsf{X}_j & \text{for } i, j \in P_{k'}, k' \in [k], \\ \mathsf{X}_i \notin R_{k'} & \text{for } i \in P_{k'}, k' \in [k]. \end{array}$

We will denote the number of solutions to $\texttt{RMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$ as $N(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$

We are particularly interested in the following two cases:

- $k = 1$, i. e., for all $i, j \in [v]$, $i \simeq j$. In this case we call the RMTP problem *complete*, also denoted as $\texttt{CRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \mathscr{R})$, where $\mathscr{R} = \{R\}$ just contains a single set.

- For each row $\boldsymbol{a}_i = (a_1, \ldots, a_v)$ of $\mathbf{A}$, if $a_j, a_{j'} \neq 0$, then $j \not\simeq j'$. In this case we call the RMTP problem *partite*. Moreover, it is called w-*regular* if each row of $\mathbf{A}$ has weight w, i. e., $\boldsymbol{a}_i = w$ for $i \in [e]$. We denote a regular partite RMTP problem as a $\texttt{RPRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R}, w)$.

In the following chapters, we will study these different variants of the Mirror Theory problem, give different lower bounds to the number of solutions to the different variants, and apply the lower bounds in security analyses of various constructions using the H-technique.

5

TOYING WITH CMTP: SOME BASIC RESULTS

In this chapter we rearrange the system of equations of the CMTP problem, so that they can be simply parameterized by a *set-system*. We present a probabilistic treatmeant of the CMTP problem that will greatly help in proving the lower bounds. Since our basic proof strategy will be inductive, we then toy around with the CMTP instance, by comparing the number of solutions of the original instance with that of the reduced instance obtained by removing a component or an edge.

We will recall certain notations first to smoothen the presentation of our proofs.

NOTATIONS. Consider a centered set-system Γ. We ignore the exponent, for the time being, which denotes the number of sets in the set-system. We can alternatively denote this as $|\Gamma|$. We denote by $\|\Gamma\| := \sum_{\gamma\in\Gamma} |\gamma|$ the total number of elements in all the sets of the set-system Γ combined. $\|\Gamma\|_{\max} := \max_{\gamma\in\Gamma} |\gamma|$ denotes the size of the set in Γ that has the maximum number of elements. For $\gamma \in \Gamma$ we denote by $\Gamma_{-\gamma}$ the set-system formed by removing the set γ from Γ. For any set, γ containing 0^m, we denote by $\Gamma_{+\gamma}$, the set-system formed by adding the set γ to the set-system Γ. Finally for any set $\gamma \in \Gamma$ and any other set γ' containing 0^m we will denote by $\Gamma_{-\gamma+\gamma'}$ the set-system formed by removing the set γ from and adding the set γ' to Γ. For $x \in \gamma \in \Gamma$, we denote by $\Gamma_{-x|\gamma}$, the set-system $\Gamma_{-\gamma+(\gamma\setminus\{x\})}$, i. e., the set-system formed by replacing γ by $\gamma \setminus \{x\}$. For two set-systems Γ and Λ, we say that $\Gamma \subseteq \Lambda$ if every set in Γ is also in Λ. For $\Gamma \subseteq \Lambda$ we denote by $\Lambda \setminus \Gamma$ the set-system obtained by removing all the sets of Γ from the set-system Λ.

5.1 REFORMULATION OF CMTP

For a system of equations, $\mathscr{E}[\boldsymbol{a}^e, \lambda^e]$, in standard form, the graph property that every component of $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$ is a star imposes a definite structure on the coefficient vectors $\boldsymbol{a}^e$, which can be embedded into a rearrangement of the constants λ^e, such that given such structured collection of the constants, one can deduce the coefficient vectors, thus lending $\boldsymbol{a}^e$ redundant.

Let the size of the c components of $\mathscr{G}(\mathscr{E})$ be $\xi_1, \ldots, \xi_c$, respectively. Instead of presenting the constants as an ordered tuple λ^e, we reorder and group them according as they appear as edge-labels in the star components of $\mathscr{G}(\mathscr{E})$. Consider the multisets $\boldsymbol{\lambda}_i := \{\!\{\lambda_{i,1}, \ldots, \lambda_{i,\xi_i-1}\}\!\}$, $i \in [c]$, denoting the collection of edge-labels of the i-th component. As it does not matter how the components are enumerated, we consider the multiset of

multisets $\Lambda^{\{\!\{c\}\!\}} = \{\!\{\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_c\}\!\}$. Instead of characterizing the system of equations in terms of the multiset $\{\!\{(\boldsymbol{a}_1, \lambda_1), \ldots, (\boldsymbol{a}_e, \lambda_e)\}\!\}$, we characterize a system of equations in standard form by $\Lambda^{\{\!\{c\}\!\}}$. Thus we will denote a system of equations in standard form as $\mathscr{E}[\Lambda^{\{\!\{c\}\!\}}]$.

SET-SYSTEM. Note that if the system of equations, $\mathscr{E}$ of a CMTP problem is in standard form, the non-equations force that (1) every edge-label of $\mathscr{G}(\mathscr{E})$ is non-zero, i. e., $\lambda_{i,j} \neq 0^m$, $j \in [\xi_i], i \in [c]$, (2) edge-labels of the same component of $\mathscr{G}(\mathscr{E})$ are distinct, i. e., $\lambda_{i,j} \neq \lambda_{i,j'}$, $j, j' \in [\xi_i], j \neq j', i \in [c]$. Thus in this case $\boldsymbol{\lambda}_i$ is a set (since it is a multiset with all elements distinct). We will call a multiset of sets a *set-system*. If the system of equations corresponding to a CMTP problem is in standard form then the problem, like its system of equations, can be characterized by a set-system.

Reformulation of CMTP

NOTATION. $\eta_i := \xi_i - 1$, denotes the number of edges in the i-th component.

The *complete homogeneous bivariate Mirror Theory Problem* instantiated by the set-system

$$\Lambda^{\{\!\{c\}\!\}} = \{\!\{\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_c\}\!\} : \boldsymbol{\lambda}_i = \{\lambda_{i,1}, \ldots, \lambda_{i,\xi_i - 1}\}, \lambda_{i,j} \neq 0^m, j \in [\eta_i], i \in [c],$$

also denoted as $\texttt{CMTP}(\Lambda^{\{\!\{c\}\!\}})$, is to find the number of solutions to the system of equations and non-equations:
(EQUATIONS). $\mathsf{X}_{i,0} \oplus \mathsf{X}_{i,j} = \lambda_{i,j}$, $j \in [\eta_i], i \in [c]$.

(NON-EQUATIONS). $\mathsf{X}_{i,j} \neq \mathsf{X}_{i',j'}$ for all $j \in [0..\eta_i], j' \in [0..\eta_{i'}], i, i' \in [c], i \neq i'$.

5.2 PROBABILISTIC TREATMENT OF THE COMBINATORIAL PROBLEM

We can generate solutions to any system of equations $\mathscr{E}$ as follows: Let $\mathscr{G}(\mathscr{E}) = ([v], E, L) \in \texttt{GC}^{(v,e,\mathbb{F}_2^m,c)}$, i. e., it has c components, and let $[v]/\rightsquigarrow = \{v_i : i \in [c]\}$ be a collection of representative vertices, one from each of the components, then, for every $i \in [c]$, we uniformly and independently sample $\mathsf{S}_{v_i} \xleftarrow{\$} \{0,1\}^m$ and set $\mathsf{S}_u := \mathsf{S}_{v_i} \oplus L(P_{u \rightsquigarrow v_i})$ for any $u \in [\![v_i]\!], u \neq v_i$. Note that $\mathsf{S}^v = (\mathsf{S}_1, \ldots, \mathsf{S}_v)$, as defined above, is a solution to $\mathscr{E}$. However this random solution may not satisfy any arbitrary system of non-equations. In fact, as we define below, the system of non-equations specify an event subset of the sample space (which is basically the set of all solutions to $\mathscr{E}$) of the random variable S^v.

Recall that the system of equations and non-equations corresponding to $\texttt{CMTP}(\Lambda^{\{\!\{c\}\!\}})$ is consistent if (1) $\lambda_{i,j} \neq 0^m$ for $j \in [\eta_i], i \in [c]$, and (2) $\lambda_{i,j} \neq \lambda_{i,j'}$ for $j, j' \in [\eta_i], j \neq j', i \in [c]$. While easy to manipulate, both conditions have to be handled in a different way, leading to unnecessary complications. The simplest fix is to introduce an additional element 0^m to each of the sets $\boldsymbol{\lambda}_i$. Thus instead of considering the multiset, $\boldsymbol{\lambda}_i$, of only the edge-labels

of the i-th component, if we consider the multiset $(\boldsymbol{\lambda}_i)_{+0^m} := \{\!\{0^m, \lambda_{i,1}, \ldots, \lambda_{i,\eta_i}\}\!\}$ then we can combine the two consistency conditions above and just say that $(\boldsymbol{\lambda}_i)_{+0^m}$ is a set for all $i \in [c]$. If every set in a set-system contains 0^m we call the set-system a *centered set-system*. Thus if the system of equations and non-equations of $\mathtt{CMTP}(\Lambda^{\{\!\{c\}\!\}})$ is consistent, then $\Lambda^{\{\!\{c\}\!\}}_{+0^m} := \{\!\{(\boldsymbol{\lambda}_1)_{+0^m}, \ldots, (\boldsymbol{\lambda}_c)_{+0^m}\}\!\}$ is a centered set-system.

Complete Disjointness Event for a Set-System

Given a centered set-system $\Lambda^{\{\!\{c\}\!\}}$, we say that the *complete disjointness event*, $\mathsf{CDE}(\Lambda^{\{\!\{c\}\!\}})$, holds, if for a random vector $\mathsf{S}^c = (\mathsf{S}_1, \ldots, \mathsf{S}_c)$, where $\mathsf{S}_i \xleftarrow{\$} \{0,1\}^m$ independently for each $i \in [c]$, the translated sets, $\mathsf{S}_1 \oplus \boldsymbol{\lambda}_1, \ldots, \mathsf{S}_c \oplus \boldsymbol{\lambda}_c$ are disjoint. We define the probability of the complete disjointness event as

$$\boldsymbol{p}(\Lambda^{\{\!\{c\}\!\}}) := \boldsymbol{p}_{\mathsf{S}^c}(\mathsf{CDE}(\Lambda^{\{\!\{c\}\!\}})).$$

Note that, every set in a centered set-system is non-empty because they at least contain the element 0^m.

5.3 SOME RESULTS ON THE PROBABILITY OF CDE EVENT

As a first step we will compare the events $\mathsf{CDE}(\Lambda)$ and $\mathsf{CDE}(\Lambda_{-\boldsymbol{\lambda}})$, thus obtaining a lower bound on the ratio of $\boldsymbol{p}(\Lambda)$ and $\boldsymbol{p}(\Lambda_{-\boldsymbol{\lambda}})$, so that iterating this bound we can prove the lower bounds via induction on $c := |\Lambda|$, the number of sets in Λ.

Lemma 5.1. *For $\boldsymbol{\gamma} \in \Gamma$, we have*

$$\boldsymbol{p}(\Gamma) = \boldsymbol{p}(\Gamma_{-\boldsymbol{\gamma}}) \left(1 - \frac{\|\Gamma\| - 1}{2^m}\right) \qquad \text{if } |\boldsymbol{\gamma}| = 1 \tag{5.1}$$

$$\boldsymbol{p}(\Gamma) \geq \boldsymbol{p}(\Gamma_{-\boldsymbol{\gamma}}) \left(1 - \frac{|\boldsymbol{\gamma}| \cdot \|\Gamma_{-\boldsymbol{\gamma}}\|}{2^m}\right) \qquad \text{if } |\boldsymbol{\gamma}| \geq 2 \tag{5.2}$$

Proof. These relations are easy to verify by looking at the restriction imposed on S which translates the set $\boldsymbol{\gamma}$. Indeed let us assume $\Gamma = \{\!\{\gamma_1, \ldots, \gamma_c\}\!\}$ is a centered set-system containing $c := |\Lambda|$ sets, and say $\boldsymbol{\gamma} = \boldsymbol{\gamma}_1$. If $\mathsf{S}_2, \ldots, \mathsf{S}_c$ already satisfies $\mathsf{CDE}(\Gamma_{-\boldsymbol{\gamma}})$, then to satisfy the event $\mathsf{CDE}(\Gamma)$, we have to choose S_1 in such a way that $\mathsf{S}_1 \oplus \boldsymbol{\gamma}_1$ is disjoint from the sets $\mathsf{S}_2 \oplus \boldsymbol{\gamma}_2, \ldots, \mathsf{S}_c \oplus \boldsymbol{\gamma}_c$, or in other words, we should have,

$$\mathsf{S}_1 \oplus \gamma \neq \mathsf{S}_i \oplus \gamma' \qquad \forall\, \gamma \in \boldsymbol{\gamma}, \gamma' \in \boldsymbol{\gamma}_i, i \neq 1.$$

Hence, if $|\boldsymbol{\gamma}| = 1$, S_1 has to be different from exactly $\|\Gamma\| - 1$ values, while, if $|\boldsymbol{\gamma}| > 1$, it has to avoid at most $|\boldsymbol{\gamma}| \cdot \|\Gamma_{-\boldsymbol{\gamma}}\|$ elements. The result now follows from the fact that $\mathsf{S}_1 \xleftarrow{\$} \{0,1\}^m$ and is independent of the random variables $\mathsf{S}_2, \ldots, \mathsf{S}_c$. □

Note that for two centered set-systems Λ and Γ with $\Gamma \subseteq \Lambda$, we can apply the inequality (5.2) repeatedly to obtain the following result:

Corollary 5.1.1. *For centered set-systems $\Gamma \subseteq \Lambda$, we have*

$$\frac{\boldsymbol{p}(\Lambda)}{\boldsymbol{p}(\Gamma)} \geq \left(1 - \frac{|\Lambda| \cdot \|\Lambda\|_{\max}^2}{2^m}\right)^{|\Lambda \setminus \Gamma|}$$

The result follows directly from the observation that for any $\boldsymbol{\lambda} \in \Lambda$, $|\boldsymbol{\lambda}| \leq \|\Lambda\|_{\max}$ and hence $\|\Lambda\| \leq |\Lambda| \cdot \|\Lambda\|_{\max}$.

5.3.1 *Link Deletion Equation*

Now instead of removing an entire set from the set-system, let us just remove one element from a set at a time.

Note that, for any set-system Λ, $\mathsf{CDE}(\Lambda) \implies \mathsf{CDE}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$. Now, for a centered set system, Λ, let uniform random vector of m-bit numbers, $\mathsf{S}^{|\Lambda|} = (\mathsf{S}_{\boldsymbol{\lambda}} : \boldsymbol{\lambda} \in \Lambda)$, satisfy the event $\mathsf{CDE}(\Lambda_{-\lambda|\boldsymbol{\lambda}_1}) \wedge \neg\mathsf{CDE}(\Lambda)$, where let us denote by $\mathsf{S}_{\boldsymbol{\lambda}}$ the uniformly drawn m-bit number corresponding to the set $\boldsymbol{\lambda}$. Then there must exist $\lambda' \in \boldsymbol{\lambda}' \in \Lambda_{-\boldsymbol{\lambda}}$, such that $\mathsf{S}_{\boldsymbol{\lambda}} = \lambda \oplus \lambda' \oplus \mathsf{S}_{\boldsymbol{\lambda}'}$. Now $\mathsf{CDE}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$ implies that $\mathsf{S}_{\boldsymbol{\lambda}} \oplus (\boldsymbol{\lambda} \setminus \lambda)$ is disjoint from $\mathsf{S}_{\boldsymbol{\lambda}'} \oplus \boldsymbol{\lambda}'$. Thus to have $\mathsf{S}_{\boldsymbol{\lambda}} = \lambda \oplus \lambda' \oplus \mathsf{S}_{\boldsymbol{\lambda}'}$, we must have $\boldsymbol{\lambda} \setminus \lambda$ is disjoint from $\boldsymbol{\lambda}' \oplus \lambda \oplus \lambda'$. Thus if we define

$$I(\lambda, \boldsymbol{\lambda}) := \{(\lambda \oplus \lambda', \boldsymbol{\lambda}') : \lambda' \in \boldsymbol{\lambda}' \in \Lambda_{-\boldsymbol{\lambda}}, (\boldsymbol{\lambda}' \oplus \lambda \oplus \lambda') \cap (\boldsymbol{\lambda} \setminus \lambda) = \emptyset\}$$

then we have for $(\delta, \boldsymbol{\lambda}') \in I(\lambda, \boldsymbol{\lambda})$, the following events are equivalent:

$$\mathsf{CDE}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \wedge (\mathsf{S}_{\boldsymbol{\lambda}} = \delta \oplus \mathsf{S}_{\boldsymbol{\lambda}'}) \equiv \mathsf{CDE}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) \wedge (\mathsf{S}_{\boldsymbol{\lambda}} = \delta \oplus \mathsf{S}_{\boldsymbol{\lambda}'}),$$

where

$$\Lambda_{(\delta,\boldsymbol{\lambda}')} := \Lambda_{-\boldsymbol{\lambda}-\boldsymbol{\lambda}'+\boldsymbol{\lambda}''}, \text{ with } \boldsymbol{\lambda}'' := (\delta \oplus \boldsymbol{\lambda}') \sqcup (\boldsymbol{\lambda} \setminus \lambda)$$

Combining we have

$$\begin{aligned}\mathsf{CDE}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) &\equiv \mathsf{CDE}(\Lambda) \vee (\mathsf{CDE}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \wedge \neg\mathsf{CDE}(\Lambda)) \\ &\equiv \mathsf{CDE}(\Lambda) \vee \bigvee_{(\delta,\boldsymbol{\lambda}') \in I(\lambda,\boldsymbol{\lambda})} (\mathsf{CDE}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) \wedge (\mathsf{S}_{\boldsymbol{\lambda}} = \delta \oplus \mathsf{S}_{\boldsymbol{\lambda}'}))\end{aligned}$$

Note that the event $(\mathsf{S}_{\boldsymbol{\lambda}} = \delta \oplus \mathsf{S}_{\boldsymbol{\lambda}'})$ occurs with probability 2^{-n} and is independent of the event $\mathsf{CDE}(\Lambda_{(\delta,\boldsymbol{\lambda}')})$. Also the events $(\mathsf{S}_{\boldsymbol{\lambda}} = \delta^* \oplus \mathsf{S}_{\boldsymbol{\lambda}^*})$ and $(\mathsf{S}_{\boldsymbol{\lambda}} = \delta^{**} \oplus \mathsf{S}_{\boldsymbol{\lambda}^{**}})$ for distinct $(\delta^*, \boldsymbol{\lambda}^*), (\delta^{**}, \boldsymbol{\lambda}^{**}) \in I(\lambda, \boldsymbol{\lambda})$ are mutually exclusive. Hence, we have the *link-deletion equation* for any centered set-system:

Lemma 5.2 (Link-deletion lemma). *Let Λ be a centered set-system, and $\lambda \in \boldsymbol{\lambda} \in \Lambda$, then*

$$\boldsymbol{\rho}(\Lambda) = \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) - \frac{1}{2^m} \sum_{(\delta,\boldsymbol{\lambda}')\in I(\lambda,\boldsymbol{\lambda})} \boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) \tag{5.3}$$

where $I(\lambda,\boldsymbol{\lambda})$ and $\Lambda_{(\delta,\boldsymbol{\lambda}')}$, for $(\delta,\boldsymbol{\lambda}') \in I(\lambda,\boldsymbol{\lambda})$, are defined as above.

Remark 5.1. The link-deletion lemma, Lemma 5.3.1, holds for all centered set-systems, and not only for paired set-systems.

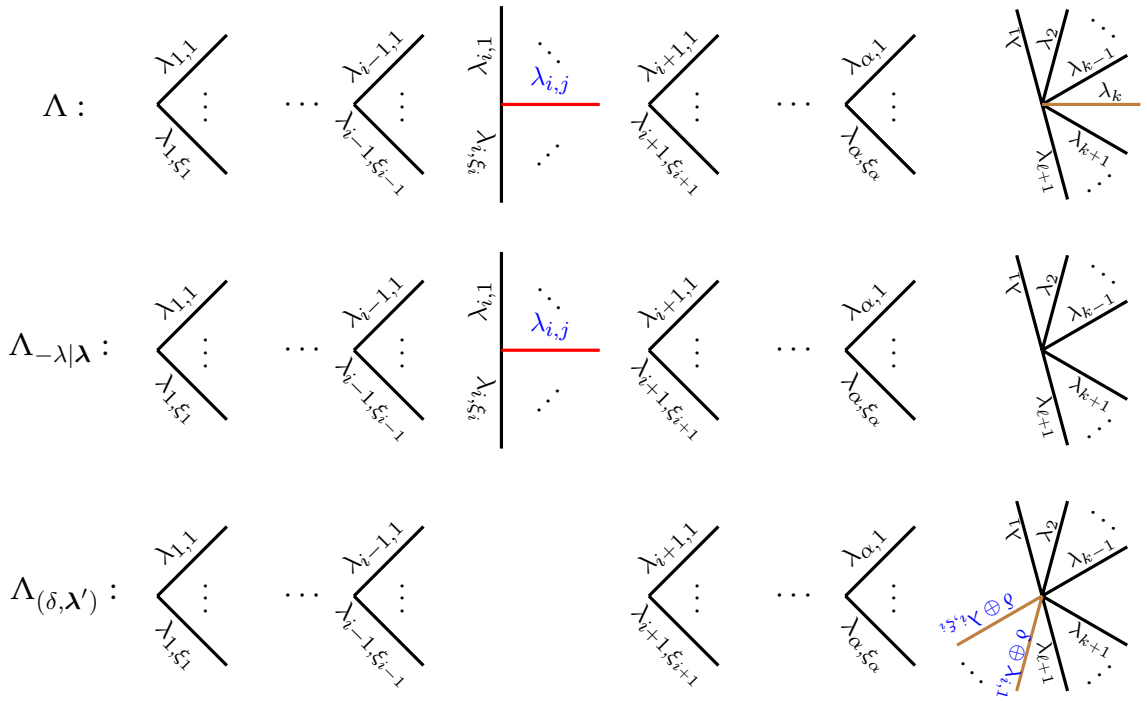


Figure 5.1: Graphical depiction of the link-deletion operation. Here, we have represented graphs corresponding to the three types of terms appearing in the link-deletion equation, with $x = \lambda_k$, $y = \lambda_{i,j}$, $\delta = \lambda_k \oplus \lambda_{i,j}$, $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_{\ell+1}\}$, and $\boldsymbol{\lambda}' = \boldsymbol{\lambda}_i$. Central vertices correspond to the $\mathsf{R}_1, \ldots, \mathsf{R}_\alpha, \mathsf{R}$ random variables.

To get a bound on the ratio $\boldsymbol{\rho}(\Lambda)/\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$, our obvious next step will be to compare $\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$ and $\boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')})$ for $(\delta,\boldsymbol{\lambda}') \in I(\lambda,\boldsymbol{\lambda})$. Note that for any centered set-system translating one of the component sets will not alter the probability of the corresponding complete disjointness event, i. e., $\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Gamma_{-\boldsymbol{\gamma}+(c\oplus\boldsymbol{\gamma})})$ for any $c \in \{0,1\}^m$, Then denoting $\Lambda' := \Lambda_{-\lambda|\boldsymbol{\lambda}}$, $\boldsymbol{\gamma} := \boldsymbol{\lambda} \setminus \lambda$, $\boldsymbol{\gamma}' := \delta \oplus \boldsymbol{\lambda}'$ and $\Gamma := \Lambda'_{-\boldsymbol{\lambda}'+\boldsymbol{\gamma}'}$, we have $\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$ and

$\boldsymbol{p}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}) = \boldsymbol{p}(\Lambda_{(\delta,\boldsymbol{\lambda}')})$, where $\boldsymbol{\gamma}$ and $\boldsymbol{\gamma}'$ are disjoint because $(\delta, \boldsymbol{\lambda}') \in I(\lambda, \boldsymbol{\lambda})$. Thus our task will be to compare $\boldsymbol{p}(\Gamma)$ and $\boldsymbol{p}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'})$ for any set-system Γ and disjoint component sets $\boldsymbol{\gamma}, \boldsymbol{\gamma}' \in \Gamma$.

To show that $\boldsymbol{p}(\Gamma)$ and $\boldsymbol{p}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'})$ are indeed very close we bound the 'maximum distance' between the two probabilities, by first proving an inequality between the distance terms that is recursive in the size of the sets and set-systems involved, and showing that particular terms of any sequence of numbers satisfying the inequality will be very small. First we define the what we mean by maximum distance in this case.

D-terms

Definition 5.1. *For a particular set-system Λ let us define the* differential term *(in short, D-term):*

$$D(\alpha, \ell) = \max_{\Gamma, \boldsymbol{\gamma}, \boldsymbol{\gamma}'} |\boldsymbol{p}(\Gamma) - \boldsymbol{p}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'})|$$

where the maximum is taken over all sets $\boldsymbol{\gamma}$ with $|\boldsymbol{\gamma}| = \ell + 1$, $\boldsymbol{\gamma}' \in \Gamma_{-\boldsymbol{\gamma}} \subseteq \Lambda$ disjoint from $\boldsymbol{\gamma}$, where $|\Gamma_{-\boldsymbol{\gamma}}| = \alpha$.
For all $\ell < 0$, we define $D(\alpha, \ell) = 0$.

The above results and definitions will come in handy in proving optimal lower bounds for the CMTP problem. We will adopt the proof strategy discussed above, and first do an warm up exercise in proving a lower bound to the number of solutions to CMTP in the $\xi_{max} = 2$ case in Chapter 6 and then move on to proving a lower bound for the general $\xi_{\max}$ case in Chapter 7. In both cases we will find out a recursive inequality in the D-terms and give a recursive inequality bound.

6

WARM UP : CMTP FOR $\xi_{max} = 2$

In this chapter we prove an optimal lower bound for $\boldsymbol{\rho}(\Lambda)$ when $\|\Lambda\|_{\max} = 2$. This is a warm-up exercise before we move on to our next task of obtaining a lower bound for more general set-systems. Specifically, we are going to prove the following theorem:

Main Result for $\xi_{\max} = 2$

Theorem 6.1. [DNS22, Lemma 2] *Consider any natural number $m \geq 12$. Then for a cenetered set-system Λ with $\|\Lambda\|_{\max} = 2$ and $1 \leq |\Lambda| \leq 2^m/58$, we have*

$$\boldsymbol{\rho}(\Lambda) \geq \frac{(2^m)_{\|\Lambda\|}}{2^{m\cdot\|\Lambda\|}}$$

This result, that we prove in the next section, Section 6.1, although seems to be for the most rudimentary case, has merits of its own, as we explore in Section 13.1.

6.1 PROOF OF THEOREM 6.1

Recall Lemma 5.1. Note that, if $\Gamma' \subseteq \Gamma$ be the collection of all singletons in Γ, i. e., every set in Γ' is $\{0^m\}$ and every set in $\Gamma \setminus \Gamma'$ has size 2, then by applying Eq. (5.1) repeatedly, we have

$$\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Gamma \setminus \Gamma') \cdot \frac{(2^m - \|\Gamma \setminus \Gamma'\|)_{\|\Gamma'\|}}{2^{m\cdot\|\Gamma'\|}} \tag{6.1}$$

If all the sets in a centered set-system has size 2, let us call it a *paired* set-system. Now if we prove the following statement, then from Eq. (6.1) we will have Theorem 6.1.

Main Result for Paired Set-Systems

Theorem 6.1.A. *Consider any natural number $m \geq 12$. Then for a paired set-system Λ with $1 \leq |\Lambda| \leq 2^m/58$, we have*

$$\boldsymbol{\rho}(\Lambda) \geq \frac{(2^m)_{2|\Lambda|}}{2^{2m|\Lambda|}}$$

Proof. We prove Theorem 6.1.A, subdividing it into two cases: (1) $|\Lambda| < 2^{\frac{m}{2}-1} - 1$, in which case it can be proven via induction on $|\Lambda|$, using inequality (5.2); and (2) $|\Lambda| > 2^{\frac{m}{2}-1} - 1$, for which case, as we will find out, inequality (5.2) is no longer enough to achieve the promised bound. In this case we will need a more sophisticated result, Lemma 6.1, where instead of removing a set from the set-system as in Lemma 5.1, we remove a well-chosen element from a set of the set-system. Thus here the induction is carried on $\|\Lambda\|$.

$|\Lambda| < 2^{\frac{m}{2}-1} - 1$. For a paired system Λ, we have $\|\Lambda\| = 2|\Lambda|$ since any set in Λ has two elements. Then inequality (5.2) implies that

$$\boldsymbol{\rho}(\Lambda) \geq \boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}}) \left(1 - \frac{4|\Lambda| - 4}{2^m}\right) \tag{6.2}$$

Note that if $|\Lambda| < 2^{\frac{n}{2}-1} - 1$, then the inequality $(\star)$ holds in the following calculation

$$\begin{aligned}\left(1 - \frac{2|\Lambda| - 2}{2^m}\right)\left(1 - \frac{2|\Lambda| - 1}{2^m}\right) &= 1 - \frac{4|\Lambda| - 3}{2^m} + \frac{(2|\Lambda| - 2)(2|\Lambda| - 1)}{2^{2m}} \\ &= 1 - \frac{4|\Lambda| - 4}{2^m} - \underbrace{\frac{2^m - (2|\Lambda| - 2)(2|\Lambda| - 1)}{2^{2m}}}_{\geq 0\ (\star)} \\ &\leq 1 - \frac{4|\Lambda| - 4}{2^m} \end{aligned} \tag{6.3}$$

Thus, the inequalities (6.2) and (6.3), along with the fact that for any centered set-system, Γ, containing just one set, i. e., with $|\Gamma| = 1$, we have $\boldsymbol{\rho}(\Gamma) = 1$, results in the follwoing lower bound

$$\boldsymbol{\rho}(\Lambda) \geq \left(1 - \frac{2|\Lambda| - 1}{2^m}\right)\left(1 - \frac{2|\Lambda| - 2}{2^m}\right) \cdots \left(1 - \frac{2}{2^m}\right)\left(1 - \frac{1}{2^m}\right) = \frac{(2^m)_{2|\Lambda|}}{2^{2n|\Lambda|}}$$

as claimed in Theorem 6.1.A.

$|\Lambda| \geq 2^{\frac{m}{2}-1} - 1$. Unfortunately, in this case, the inequality $(\star)$, used to derive (6.3), will not hold, and similar algebraic trickery will not work. Thus instead of removing a set, $\boldsymbol{\lambda} = \{0^m, \lambda\}$, at once, from a paired set-system Λ, we remove the elements λ and 0^m successively. This implies that the task of comparing $\boldsymbol{\rho}(\Lambda)$ and $\boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}})$ will now be done in two steps : (1) comparing $\boldsymbol{\rho}(\Lambda)$ and $\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$, and then (2) comparing $\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$ and $\boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}})$. The second step is to simply paraphrase Eq. (5.1) for paired set-systems,

$$\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) = \boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}}) \left(1 - \frac{2|\Lambda| - 2}{2^m}\right) \tag{6.4}$$

Now to solve the first step we will present a crucial lemma, Lemma 6.1, the proof of which will be deferred to the next section, Section 6.2. As a prerequisite, we will define the *multiplicity* of m-bit numbers in a paired set-system as follows:

Multiplicity of sets in a paired set-system

Definition 6.1. *For a paired set-system Λ and a m-bit number λ, we define the* multiplicity *of λ in Λ as*

$$\mu_\Lambda(\lambda) := |\{\boldsymbol{\gamma} \in \Lambda : \boldsymbol{\gamma} = \{0^m, \lambda\}\}|$$

We define the maximum multiplicity *of a paired set-system Λ as*

$$M(\Lambda) := \max_{\lambda \in \{0,1\}^m} \mu_\Lambda(\lambda)$$

Lemma 6.1 (Core Lemma for paired set-systems). *Consider a paired set-system Λ with $|\Lambda| \geq 2m$. Let $\lambda \in \{0,1\}^m$ be such that $\mu_\Lambda(\lambda) = M(\Lambda)$ and consider any arbitrary $\boldsymbol{\lambda} \in \Lambda$ such that $\lambda \in \boldsymbol{\lambda}$. Then we have*

$$\boldsymbol{\rho}(\Lambda) \geq \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \left(1 - \frac{2|\Lambda| - 1}{2^m}\right)$$

Note that for $m \geq 12$, we have $2^{\frac{m}{2}-1} - 1 > 2m$, and hence Lemma 6.1 is applicable in the case $|\Lambda| \geq 2^{\frac{m}{2}-1} - 1$.

We take one possible ordering of the sets in the set-system Λ, according to their multiplicity, say $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{|\Lambda|}$, such that $\boldsymbol{\lambda}_i = \{0^m, \lambda_i\}$ and $\mu_\Lambda(\lambda_i) \geq \mu_\Lambda(\lambda_j)$ for all $i \leq j$. Note that this implies $\mu_\Lambda(\lambda_1) = M(\Lambda)$. Also, the removal of the set with the highest multiplicity preserves the ordering of the remaining sets, i. e., the ordering $\boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_{|\Lambda|}$, of the sets in the set-system $\Lambda_{-\boldsymbol{\lambda}_1}$, has non-increasing multiplicity. Thus from Lemma 6.1 and Eq. (6.4), we have

$$\begin{aligned}
\boldsymbol{\rho}(\Lambda) &\geq \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}_1}) \left(1 - \frac{2|\Lambda| - 1}{2^m}\right) \\
&= \boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}_1}) \left(1 - \frac{2|\Lambda| - 2}{2^m}\right) \left(1 - \frac{2|\Lambda| - 1}{2^m}\right)
\end{aligned}$$

Thus we remove sets, $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_s$, until the size of the resulting set-system, $\Lambda' := \Lambda_{-\boldsymbol{\lambda}_1 - \cdots - \boldsymbol{\lambda}_s}$, reduces it to the previous case, i. e., $|\Lambda'| \leq 2^{m/2-1} - 1$. Of course, we should have $s = |\Lambda| - 2^{m/2-1} + 1$. Thus we have

$$\begin{aligned}
\boldsymbol{\rho}(\Lambda) &\geq \boldsymbol{\rho}(\Lambda') \frac{(2^m - 2|\Lambda'|)_{2s}}{2^{2ms}} \\
&\geq \frac{(2^m)_{2|\Lambda'|}}{2^{2m|\Lambda'|}} \cdot \frac{(2^m - 2|\Lambda'|)_s}{2^{2ms}} = \frac{(2^m)_{2|\Lambda|}}{2^{2m|\Lambda|}}
\end{aligned}$$

Thus modulo the proof of Lemma 6.1 we are done. □

6.2 PROOF OF CORE LEMMA FOR PAIRED SET-SYSTEMS

Now we will present a recursive inequality for the D-terms (Def. 5.1):

Lemma 6.2 (Recursive inequality for D-terms.). *Let $\alpha \le |\Lambda| \le \frac{2^m}{58}$, $\ell \ge 0$. Then for a paired set-system Λ,*

$$D(\alpha,\ell) \le D(\alpha,\ell-1) + \frac{2|\Lambda|}{2^m} D(\alpha-1,\ell+1) + \frac{4\cdot M(\Lambda)\cdot \boldsymbol{\rho}(\Lambda)}{2^m(1-4|\Lambda|/2^m)^{|\Lambda|-\alpha}} \tag{6.5}$$

Proof. We fix a set $\boldsymbol{\gamma}$ with $|\boldsymbol{\gamma}| = \ell+1$, a set-system $\Gamma = \Lambda'_{+\boldsymbol{\gamma}}$ for some sub-set-system $\Lambda' \subseteq \Lambda$ with $|\Lambda'| = \alpha$, and another set $\boldsymbol{\gamma}' \in \Lambda'$ such that $\boldsymbol{\gamma} \cap \boldsymbol{\gamma}' = \emptyset$. We assume that these are made in such a manner such that $D(\alpha,\ell) = |\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'})|$. In the following proof, let us denote $\Gamma' := \Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}$. Now we prove the inequality in two cases:

CASE $|\boldsymbol{\gamma}| = 1$. In this case let $\boldsymbol{\gamma} = \{\gamma\}$. Then $\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Lambda')\cdot(1-2\alpha/2^m)$, from Eq. (5.1). Also $\Gamma'_{-\gamma|\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'} = \Lambda'$. Hence from link-deletion equation Eq. (5.3),

$$\boldsymbol{\rho}(\Gamma') = \boldsymbol{\rho}(\Lambda') - \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda})\in I(\gamma)} \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})$$

where $I(\gamma) := \{(\gamma\oplus x,\boldsymbol{\lambda}) : x\in\boldsymbol{\lambda}\in\Gamma'_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}, (\boldsymbol{\lambda}\oplus\gamma\oplus x)\cap(\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'\setminus\gamma) = \emptyset\}$. Note that $\Gamma'_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'} = \Lambda'_{-\boldsymbol{\gamma}'} \subseteq \Lambda$ is a paired set-system, implying that any $\boldsymbol{\lambda}\in\Gamma_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}$ will be of the form $\boldsymbol{\lambda} = \{0^m,\lambda\}$. Similarly, $\boldsymbol{\gamma}'\in\Lambda'$ will also be of the form $\boldsymbol{\gamma}' = \{0^m,\gamma'\}$. For $x\in\boldsymbol{\lambda}\in\Gamma'_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}$, $(\gamma\oplus x,\boldsymbol{\lambda})\notin I(\gamma)$ if and only if there exists $z\in\boldsymbol{\gamma}'$ and $x\oplus\lambda\in\boldsymbol{\lambda}$ such that $\gamma\oplus z = \lambda$. The total number of such tuples $(\gamma\oplus x,\boldsymbol{\lambda})$ is $2|\Gamma'_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}| = 2(\alpha-1)$, and those that do not belong to $I(\gamma)$ is $2\mu_{\Lambda'_{-\boldsymbol{\gamma}'}}(\gamma) + 2\mu_{\Lambda'_{-\boldsymbol{\gamma}'}}(\gamma\oplus\gamma') \le 2\mu_{\Lambda'}(\gamma) + 2\mu_{\Lambda'}(\gamma\oplus\gamma') - 2$. Thus $|I(\gamma)| \ge 2\alpha - 4M(\Lambda)$. Hence

$$\begin{aligned}
D(\alpha,0) = |\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma')| &= \left|\frac{2\alpha}{2^m}\boldsymbol{\rho}(\Lambda') - \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda})\in I(\gamma)}\boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})\right| \\
&\le \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda})\in I(\gamma)}\left|\boldsymbol{\rho}(\Lambda') - \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})\right| + \frac{4M(\Lambda)}{2^m}\boldsymbol{\rho}(\Lambda') \\
&\overset{(\star)}{\le} \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda})\in I(\gamma)}\left|\boldsymbol{\rho}(\Lambda') - \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})\right| + \frac{4M(\Lambda)\boldsymbol{\rho}(\Lambda)}{2^m\,(1-4|\Lambda|/2^m)^{|\Lambda|-\alpha}} \\
&\overset{(\star\star)}{\le} \frac{2\alpha}{2^m}D(\alpha-1,1) + \frac{4M(\Lambda)\boldsymbol{\rho}(\Lambda)}{2^m\,(1-4|\Lambda|/2^m)^{|\Lambda|-\alpha}}
\end{aligned}$$

where $(\star)$ follows from repeatedly applying Eq. (6.2), and $(\star\star)$ follows from the fact that $\Gamma'_{(\delta,\boldsymbol{\lambda})} = \Gamma'_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'-\boldsymbol{\lambda}+(\delta\oplus\boldsymbol{\lambda})\sqcup(\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'\setminus\gamma)} = \Lambda'_{-\boldsymbol{\gamma}'-\boldsymbol{\lambda}+(\delta\oplus\boldsymbol{\lambda})\sqcup\boldsymbol{\gamma}'}$.

CASE $|\boldsymbol{\gamma}| > 1$. Fix $\gamma \in \boldsymbol{\gamma}$. By link-deletion equation Eq. (5.3), we have

$$\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Gamma_{-\gamma|\boldsymbol{\gamma}}) - \frac{1}{2^m} \sum_{(\delta,\boldsymbol{\lambda})\in I(\gamma)} \boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda})})$$
$$\boldsymbol{\rho}(\Gamma') = \boldsymbol{\rho}(\Gamma'_{-\gamma|\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}) - \frac{1}{2^m} \sum_{(\delta,\boldsymbol{\lambda})\in I'(\gamma)} \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})$$

where

$$I(\gamma) = \{(\gamma \oplus x, \boldsymbol{\lambda}) : x \in \boldsymbol{\lambda} \in \Gamma_{-\boldsymbol{\gamma}}, (\boldsymbol{\lambda} \oplus \gamma \oplus x) \cap (\boldsymbol{\gamma} \setminus \gamma) = \emptyset\}$$
$$I'(\gamma) = \{(\gamma \oplus x, \boldsymbol{\lambda}) : x \in \boldsymbol{\lambda} \in \Gamma'_{-\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}, (\boldsymbol{\lambda} \oplus \gamma \oplus x) \cap (\boldsymbol{\gamma} \sqcup \boldsymbol{\gamma}' \setminus \gamma) = \emptyset\}$$

It is easy to see that $I'(\gamma) \subseteq I(\gamma)$. If $(\delta, \boldsymbol{\lambda}) \in I(\gamma) \setminus I'(\gamma)$, then

- either $(\delta, \boldsymbol{\lambda}) = (\gamma \oplus x, \boldsymbol{\gamma}')$ for some $x \in \boldsymbol{\gamma}'$ such that $(\boldsymbol{\gamma}' \oplus \gamma) \cap (\boldsymbol{\gamma} \setminus \gamma) = \emptyset$.[1] The number of such tuples $(\delta, \boldsymbol{\gamma}')$ will be at most 2.
- or $\boldsymbol{\lambda} \in \Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'}$, $\delta = \gamma \oplus x$, for $x \in \boldsymbol{\lambda}$, such that $(\boldsymbol{\lambda} \oplus \gamma) \cap (\boldsymbol{\gamma} \setminus \gamma) = \emptyset$ and $(\boldsymbol{\lambda} \oplus \gamma) \cap \boldsymbol{\gamma}' \neq \emptyset$. The number of such tuples $(\delta, \boldsymbol{\lambda})$ will be $2\mu_{\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'}}(\gamma) + 2\mu_{\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'}}(\gamma \oplus \gamma')$.

Thus very similar to the previous case it turns out that $|I(\gamma) \setminus I'(\gamma)| \leq 4M(\Lambda)$. Thus we have

$$\begin{aligned} D(\alpha, \ell) &= |\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma')| \\ &\leq |\boldsymbol{\rho}(\Gamma_{-\gamma|\boldsymbol{\gamma}}) - \boldsymbol{\rho}(\Gamma'_{-\gamma|\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'})| + \frac{1}{2^m} \sum_{(\delta,\boldsymbol{\lambda})\in I'(\gamma)} |\boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda})}) - \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})| \\ &\quad + \frac{4M(\Lambda)}{2^m} \boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda})}) \\ &\overset{(\star)}{\leq} D(\alpha, \ell-1) + \frac{2|\Lambda|}{2^m} D(\alpha-1, \ell+1) + \frac{4M(\Lambda)\boldsymbol{\rho}(\Lambda)}{2^m(1-4|\Lambda|/2^m)^{|\Lambda|-\alpha}} \end{aligned}$$

where $(\star)$ follows from the following observations:

- $|I'(\gamma)| \leq 2|\Lambda|$ (because each set $\boldsymbol{\lambda}$) corresponds to the two tuples $(\gamma, \boldsymbol{\lambda})$ and $(\gamma \oplus \lambda, \boldsymbol{\lambda})$, which may or may not be in $I'(\gamma)$.
- Repeated application of Eq. (6.2) to the last term.
- Considering $\Gamma = \Lambda'_{+\boldsymbol{\gamma}}$ for $\Lambda' \subseteq \Lambda$. So $\Gamma_{-\gamma|\boldsymbol{\gamma}} = \Lambda'_{+\boldsymbol{\gamma}\setminus\gamma}$ and $\Gamma'_{-\gamma|\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'} = \Lambda'_{-\boldsymbol{\gamma}'+\boldsymbol{\gamma}'\sqcup\boldsymbol{\gamma}\setminus\gamma} = (\Gamma_{-\gamma|\boldsymbol{\gamma}})_{-\boldsymbol{\gamma}\setminus\gamma-\boldsymbol{\gamma}'+\boldsymbol{\gamma}'\sqcup\boldsymbol{\gamma}\setminus\gamma}$, implying that $|\boldsymbol{\rho}(\Gamma_{-\gamma|\boldsymbol{\gamma}}) - \boldsymbol{\rho}(\Gamma'_{-\gamma|\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}})| \leq D(\alpha, \ell-1)$. Similarly one can show $|\boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda})}) - \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda})})| \leq D(\alpha-1, \ell+1)$.

This completes the proof of the recursive inequality. □

1 Note that for any set $\boldsymbol{\lambda} = \{0^m, \lambda\}$, $\boldsymbol{\lambda} \oplus x = \boldsymbol{\lambda}$ if and only if $x \in \boldsymbol{\lambda}$.

To make things look less tedious we define the double sequence $\{a_{d,\ell}\}_{0\le d\le|\Lambda|,\ell\le 2d-1}$ as follows

$$a_{d,\ell} := \frac{\beta^d}{2\boldsymbol{\rho}(\Lambda)} \times D(|\Lambda| - d, \ell) \tag{6.6}$$

where $\beta = 2|\Lambda|/2^m$. This double sequence satisfies the following properties:

- Multiplying both sides of the recursive inequality for D-terms, Eq. (6.5), by $\beta^d/2\boldsymbol{\rho}(\Lambda)$, we have

$$a_{d,\ell} \le a_{d,\ell-1} + a_{d+1,\ell+1} + \frac{2M(\Lambda)}{2^m}\left(\frac{\beta}{1-2\beta}\right)^d$$

- Also assuming $\Gamma, \boldsymbol{\gamma}, \boldsymbol{\gamma}'$ are chosen as in the proof of the above lemma, we have $\boldsymbol{\rho}(\Gamma) \le \boldsymbol{\rho}(\Lambda')$ since $\Gamma = \Lambda'_{+\boldsymbol{\gamma}}$ and $\boldsymbol{\rho}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}) \le \boldsymbol{\rho}(\Lambda')$ since $\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'} = \Lambda'_{-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}$, implying that $D(\alpha,\ell) = |\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'})| \le 2\boldsymbol{\rho}(\Lambda') \le 2\boldsymbol{\rho}(\Lambda)/(1-4|\Lambda|/2^m)^{|\Lambda|-\alpha}$, from Eq. 6.2. This reduces to the following inequality for the $a_{d,\ell}$-terms:

$$a_{d,\ell} \le \left(\frac{\beta}{1-2\beta}\right)^d$$

Now noting from the definition of β and the condition that $|\Lambda| \le 2^m/58$, we have that that $\beta/(1-2\beta) \le 1/4e$, we see that our double sequence exactly fits into the criteria for the following result, for $C = 2M(\Lambda)$:

Lemma 6.3 (Recursive Inequality Bound I). *Suppose $a_{d,\ell} \ge 0$ such that $a_{d,k} := 0$ for all $k < 0$ and for all $0 \le d \le 2n$ we have*

$$a_{d,\ell} \le \left(\frac{1}{4e}\right)^d \tag{6.7}$$

$$a_{d,\ell} \le a_{d,\ell-1} + a_{d+1,\ell+1} + \frac{C}{2^m}\cdot\left(\frac{1}{4e}\right)^d \tag{6.8}$$

for some $C > 0$. Then

$$a_{0,0} \le \frac{4C+2}{2^m}.$$

We prove this result in the following subsection, Subsect. 6.2.1. But first let us understand the implication of this result for our double sequence, $\{a_{d,\ell}\}_{0\le d\le|\Lambda|,\ell\le 2d-1}$, defined in Eq. 6.6. Let Λ be a paired set-system, and let $\boldsymbol{\lambda} = \{0^m, \lambda\} \in \Lambda$. Then by the link-deletion lemma, Lemma 5.3.1, we have that

$$\boldsymbol{\rho}(\Lambda) = \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) - \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda}')\in I(\lambda,\boldsymbol{\lambda})}\boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')})$$

As observed earlier, denoting $\Lambda' := \Lambda_{-\lambda|\boldsymbol{\lambda}}$, $\boldsymbol{\gamma} := \boldsymbol{\lambda} \setminus \lambda$, $\boldsymbol{\gamma}' := \delta \oplus \boldsymbol{\lambda}'$ and $\Gamma := \Lambda'_{-\boldsymbol{\lambda}'+\boldsymbol{\gamma}'}$, we have $\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$ and $\boldsymbol{\rho}(\Gamma_{-\boldsymbol{\gamma}-\boldsymbol{\gamma}'+\boldsymbol{\gamma}\sqcup\boldsymbol{\gamma}'}) = \boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')})$, where $\boldsymbol{\gamma}$ and $\boldsymbol{\gamma}'$ are disjoint because $(\delta, \boldsymbol{\lambda}') \in I(\lambda, \boldsymbol{\lambda})$. Then

$$\begin{aligned}
|\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) - \boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')})| \le D(|\Lambda_{-\boldsymbol{\lambda}}|, 0) &\overset{(\S)}{\le} \frac{2\boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}})(8M(\Lambda_{-\boldsymbol{\lambda}})+2)}{2^m} \\
&\overset{(\star)}{\le} \frac{20M(\Lambda)\boldsymbol{\rho}(\Lambda_{-\boldsymbol{\lambda}})}{2^m} \\
&\overset{(\dagger)}{\le} \frac{20M(\Lambda)\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})}{2^m(1-2|\Lambda_{-\boldsymbol{\lambda}}|/2^m)} \\
&\overset{(\ddagger)}{\le} \frac{21M(\Lambda)\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})}{2^m}
\end{aligned}$$

where $(\S)$ follows from the recursive bound, Lemma 6.3, $(\star)$ follows from the fact that $M(\lambda) \ge 1$, $(\dagger)$ follows from Eq. (6.4), and $(\ddagger)$ follows from the fact that $|\Lambda| \le 2^m/58$. Rearranging terms we have that

$$\boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) \ge \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \left(1 + \frac{21M(\Lambda)}{2^m}\right)$$

6.2.1 *Proof of Recursive Inequality Bound I*

PROOF IDEA. The *initial bound*, i.e., Eq. (6.7) of $a_{d,\ell}$ says that $a_{0,0} \le 1$. However, due to the *recursive inequality*, i.e., Eq. (6.8), we show that $a_{0,0}$ has to be very small. The recursive inequality gives us $a_{0,0} = a_{1,1} + O(2^{-n})$. However, the initial bound ensures $a_{1,1} \le 1/4e$. Therefore, a single application of recursive inequality is not sufficient to conclude the desired bound. However, if we apply the recursive inequality twice before applying the initial bound, we have

$$\begin{aligned}
a_{0,0} &= a_{1,0} + a_{2,2} + O(2^{-n}) \\
&= a_{2,1} + a_{2,2} + O(2^{-n}) = 2(1/4e)^2 + O(2^{-n}).
\end{aligned}$$

So, we apply the recursive inequality several times before applying the bounds on a terms and we get an upper bound of $a_{0,0}$ of the form $M_d/(4e)^d + O(2^{-n})$ for some M_d. In the detailed proof, we show that the constant term present in $O(2^{-n})$ do not blow up and the value of $M_d/(4e)^d = O(2^{-n})$ for $d = 2n$.

PROOF OF LEMMA 6.3. We first state the following claim, which follows from iterated applications of the recursive inequality. A proof of the claim is deferred to the end of this section.

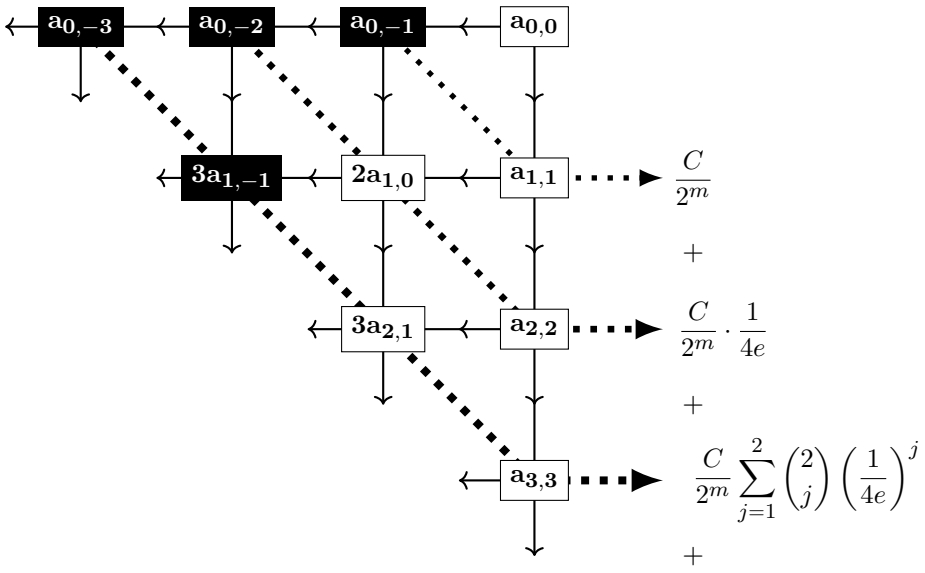


Figure 6.1: The proof idea of the Recursive Inequality Lemma. The white terms in the black squares, in this pascal tree-like structure, are equal to zero. However, we keep them to achieve a compact coefficient $\binom{d_0}{i}$ due to our condition on the double sequence.

Claim 1. *For any* $0 \leq d_0 \leq 2n$, *we have*

$$a_{0,0} \leq \sum_{i=\lceil \frac{d_0}{2} \rceil}^{d_0} \binom{d_0}{i} a_{i,2i-d_0} + \frac{C}{2^m} \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \binom{i}{j} \left(\frac{1}{4e}\right)^j. \tag{6.9}$$

By plugging in the bound of each a-term from Eq. (6.7) into the right hand side of Eq. (6.9) and bounding each of the binomial coefficients as $\binom{m}{j} \leq m^j/j! \leq (em/j)^j \leq (2e)^j$, for $j \geq m/2$, we get the following bound for all $d \leq 2n$.

$$a_{0,0} \leq \sum_{i=\lceil \frac{d}{2} \rceil}^{d} \left(2e \cdot \frac{1}{4e}\right)^i + \frac{C}{2^m} \sum_{i=0}^{d-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \left(2e \cdot \frac{1}{4e}\right)^j.$$

Now by using the inequality $\sum_{a \geq i} r^a \leq \frac{r^i}{1-r}$, we obtain

$$a_{0,0} \leq 2 \cdot 2^{-d/2} + \frac{2C}{2^m} \sum_{i=0}^{d-1} 2^{-i/2} \leq 2 \cdot 2^{-d/2} + \frac{4C}{2^m}.$$

By replacing $d = 2n$, we complete the proof of the lemma. □

PROOF OF THE CLAIM : We prove the claim by induction on d_0. The result holds trivially for $d_0 = 1$ (by applying $d = \ell = 0$ in Eq. (6.8)). Now we prove the statement for $d_0 + 1$, assuming it is true for d_0. Therefore, we have

$$\begin{aligned} a_{0,0} &\leq \sum_{i=\lceil \frac{d_0}{2} \rceil}^{d_0} \binom{d_0}{i} a_{i,2i-d_0} + \frac{C}{2^m} \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \binom{i}{j} \left(\frac{1}{4e}\right)^j \\ &\leq \sum_{i=\lceil \frac{d_0}{2} \rceil}^{d_0} \binom{d_0}{i} \left(a_{i,2i-d_0-1} + a_{i+1,2i-d_0+1} + \frac{C}{2^m} \cdot \left(\frac{1}{4e}\right)^i \right) \\ &\quad + \frac{C}{2^m} \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \binom{i}{j} \left(\frac{1}{4e}\right)^j . \end{aligned} \tag{6.10}$$

For $i < \lceil (d_0+1)/2 \rceil$, $2i - (d_0+1) < 0$, and hence $a_{i,2i-(d_0+1)} = 0$. For $i > \lceil (d_0+1)/2 \rceil$, the coefficient of $a_{i,2i-(d_0+1)}$ in the above sum will be $\binom{d_0}{i-1} + \binom{d_0}{i}$, which is same as $\binom{d_0+1}{i}$ (see Fig. 6.1 for the recursive growth of coefficients). For $i = \left\lceil \frac{d_0+1}{2} \right\rceil$, the coefficient of $a_{i,2i-d_0-1}$ will be

$$\begin{cases} \binom{d_0}{i} & \text{if } d_0 \equiv 1 \pmod 2 \\ \binom{d_0}{i-1} + \binom{d_0}{i} & \text{if } d_0 \equiv 0 \pmod 2. \end{cases}$$

In both cases, the coefficient of $a_{i,2i-d_0-1}$ for $i = \left\lceil \frac{d_0+1}{2} \right\rceil$ is at most $\binom{d_0+1}{i}$. Using the above observation in Eq. 6.10 the inductive step is proved. □

Remark 6.1. The similar result is also achieved when the initial bound (i.e., Eq. (6.7)) is replaced by $a_{d,\ell} \leq \beta^d$ for any constant $0 < \beta < 1$. However, we need that Eq. (6.7) and Eq. (6.8) hold for all $d \leq 2n/\log(\frac{1}{2e\beta})$.

7

CMTP FOR GENERAL ξ_{max}

In this chapter we prove the following result, which is a generalization of Theorem 6.1 for a system of equations with a wider range of $\xi_{\max}$.

Main Result for general $\xi_{\max}$

Theorem 7.1. [CDNPS23, Theorem 1'] *Let Λ be a centered set-system of elements of $\{0,1\}^m$ such that $\xi_{\max} = \|\Lambda\|_{\max}$. If $\|\Lambda\| \leq 2^{m/2}$ or $2^{m/2} \geq \xi_{\max}^2 m + \xi_{\max}$, and $1 \leq \|\Lambda\| \leq 2^m/12\xi_{\max}^2$, then*

$$\boldsymbol{\rho}(\Lambda) \geq \frac{(2^m)_{\|\Lambda\|}}{2^{m\|\Lambda\|}}.$$

The proof technique for Theorem 7.1 is very similar to the technique for proving Theorem 6.1. From a high level, the proof works in two steps:

1. if Λ is small ($\|\Lambda\| \leq 2^{m/2}$), then simple calculations show that Theorem 7.1 holds;
2. otherwise, we prove that, for a well-chosen $\lambda \in \boldsymbol{\lambda} \in \Lambda$, one has

$$\boldsymbol{\rho}(\Lambda) \geq \left(1 - \frac{\|\Lambda\| - 1}{2^m}\right) \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}),$$

   Clearly, applying point 2 repeatedly until $\|\Lambda\| \leq 2^{m/2}$ allows us to conclude the proof of Theorem 7.1.

Intuitively, the element that we remove from one of the sets of Λ is the one that appears, in the associated system of equations, with maximum multiplicity.

The notion of multiplicity of an element in any centered system, needs to be generalized from the corresponding definition, Defn. 6.1, for paired systems.

Multiplicity of sets in a general set-system

Definition 7.1. *Given $z \in \{0,1\}^m \setminus \{0^m\}$, and a set $\boldsymbol{\lambda}$, we define $\mu_{\boldsymbol{\lambda}}(z)$ as the number of 2-subsets $\{\lambda, \lambda'\}$ of $\boldsymbol{\lambda}$ with $\lambda \oplus \lambda' = z$. For a set-system Λ, we define*

$$\mu_\Lambda(z) := \sum_{\boldsymbol{\lambda} \in \Lambda} \mu_{\boldsymbol{\lambda}}(z), \quad M(\Lambda) := \max_{z \in \{0,1\}^m} \mu_\Lambda(z).$$

Clearly, for any set-system Λ, $M(\Lambda) \geq 1$. Note that Defn. 7.1 reduces to Defn. 6.1 when $\xi_{\max} = 2$.

The underlying core lemma behind the second point of our proof strategy is the following one.

Lemma 7.1 (Core lemma for centered set-systems). *Let Λ be a centered set-system with $2^{m/2} \leq \|\Lambda\| \leq 2^m/12\xi_{\max}^2$ where $\xi_{\max} = \|\Lambda\|_{\max}$ satisfies the bound given in Theorem 7.1, i.e., $2^{m/2} \geq \xi_{\max}^2 m + \xi_{\max}$. Suppose the maximum $M(\Lambda)$ is attained for $\lambda \oplus \lambda'$ with $\{\lambda, \lambda'\} \subseteq \boldsymbol{\lambda} \in \Lambda$. Then,*

$$\boldsymbol{p}(\Lambda) \geq \left(1 - \frac{\|\Lambda\| - 1}{2^m}\right) \cdot \boldsymbol{p}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$$

Remark 7.1. Recall that, the crude bounds, Lemma 5.1, Corollary 5.1.1; and the link deletion equation, Lemma 5.3.1, presented in the previous warm-up chapter, holds for all centered set systems, and not only paired set-systems. So these results will be reused in the present proof.

PROOF OF THEOREM 7.1. Let us write $W_i := (1 - \frac{i}{2^m})$, so that $\prod_{i=1}^{k-1} W_i = (2^m)_k / 2^{mk}$. Now we claim that, for $\|\Lambda\| \leq 2^{m/2}$,

$$\left(1 - \frac{|S| \times \|\Lambda_{-S}\|}{N}\right) \geq \prod_{i=\|\Lambda_{-S}\|}^{\|\Lambda\|-1} W_i \tag{7.1}$$

and hence $\boldsymbol{p}(\Lambda) \geq \boldsymbol{p}(\Lambda_{-S}) \times \prod_{i=\|\Lambda_{-S}\|}^{\|\Lambda\|-1} W_i$. After repeatedly removing an element one by one, we have $\boldsymbol{p}(\Lambda) \geq \prod_{i=1}^{\|\Lambda\|-1} W_i$ which proves the theorem. Now we prove Eq. (7.1). It is sufficient to show that

$$1 - \frac{ar}{2^m} \geq \left(1 - \frac{a}{2^m}\right) \cdots \left(1 - \frac{a+r-1}{2^m}\right)$$

where $a + r \leq 2^{m/2}$. This can be easily shown by induction on r. For $r = 1$, it is obvious. Now by applying induction hypothesis for r, we obtain

$$\begin{aligned}\left(1 - \frac{a}{2^m}\right) \cdots \left(1 - \frac{a+r-1}{2^m}\right)\left(1 - \frac{a+r}{2^m}\right) &\leq \left(1 - \frac{ar}{2^m}\right)\left(1 - \frac{a+r}{2^m}\right) \\ &\leq 1 - \frac{ar+a}{2^m} - \frac{r}{2^m}\left(1 - \frac{a(a+r)}{2^m}\right) \leq 1 - \frac{ar+a}{2^m}.\end{aligned}$$

For the last inequality we use the fact that $a + r + 1 \leq 2^{m/2}$.

For the next case, we assume that $2^{m/2} \leq \|\Lambda\| \leq 2^m/12\xi_{\max}^2$, i.e. $\|\Lambda\|$ is within the required bounds for which Lemma 7.1 holds. We can create a sequence of nested set-systems $\{\Lambda^{(i)}\}_{i=0}^{\sigma}$, with

$$\Lambda^{(0)} := \Lambda, \quad \|\Lambda^{(i+1)}\| = \|\Lambda^{(i)}\| - 1, \ \forall i \in [\sigma - 1], \quad \|\Lambda^{(\sigma)}\| \leq 2^{m/2},$$

in the following manner: Let $\lambda_i, \lambda_i'\} \subseteq \boldsymbol{\lambda}_i \in \Lambda^{(i)}$ such that $\lambda_i \oplus \lambda_i'$ attains the highest multiplicity in $\Lambda^{(i)}$, $M(\Lambda^{(i)})$. We choose one arbitrarily if there exists more than one choice. We define $\Lambda^{(i+1)} := \Lambda^{(i)}_{-\lambda_i|\boldsymbol{\lambda}_i}$. Now for every $i \in [\sigma - 1]$, if $|\boldsymbol{\lambda}_i| = 1$ we apply Eq. (5.1), and if $|\boldsymbol{\lambda}_i| \geq 2$, we apply Lemma 7.1, to obtain

$$\boldsymbol{\rho}(\Lambda) \geq \boldsymbol{\rho}(\Lambda^{(\sigma)}) \prod_{i=1}^{\sigma} \left(1 - \frac{\|\Lambda\| - i}{2^m}\right).$$

We already have shown the result for $\Lambda^{(\sigma)}$ that $\boldsymbol{\rho}(\Lambda^{(\sigma)}) \geq (2^m)_{\|\Lambda^{(\sigma)}\|}/2^{m\|\Lambda^{(\sigma)}\|}$, which completes the proof. □

7.1 PROOF OF CORE LEMMA FOR CENTERED SET-SYSTEMS

PROOF STRATEGY. In order to prove Lemma 7.1, we will prove that $|\boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) - \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})|$ is small enough in front of $\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})$, for all $(\delta, \boldsymbol{\lambda}') \in I(\lambda, \boldsymbol{\lambda})$. This will be done in the following steps.

1. Upper bound the size of the set $I(\lambda, \boldsymbol{\lambda})$ of the link deletion equation, Lemma 5.3.1 (in Lemma 7.2).
2. Establish a recursive inequality between the maximum difference between terms of the form $\boldsymbol{\rho}(\Gamma_{-\gamma|\boldsymbol{\gamma}})$, and terms of the form $\boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\gamma}')})$, with $\Gamma_{-\boldsymbol{\gamma}} \subset \Lambda$, and $\boldsymbol{\gamma}$ an arbitrary set of some fixed size (in Lemma 7.3). This will be done by applying the link-deletion equation to the two probabilities that maximize the difference term, thus introducing new difference terms and an error term.
3. After applying this inequality a logarithmic number of times along with simple bounds on the probability ratios, prove that remaining terms become sufficiently small thanks to the geometric reduction offered by the recursive inequality bound II (Lemma 7.4).

7.1.1 *Size Lemma*

Clearly, for all $\lambda \in \boldsymbol{\lambda} \in \Lambda$, $|I(\lambda, \boldsymbol{\lambda})| \leq \|\Lambda\|$. However, we establish an improved upper bound for the size of $I(\lambda, \boldsymbol{\lambda})$ where λ and $\boldsymbol{\lambda}$ are described in the statement of the Core Lemma, Lemma 7.1.

Lemma 7.2 (size lemma). *For a given $\lambda \in \boldsymbol{\lambda} \in \Lambda$ as described in the Lemma 7.1, we have $|I(\lambda, \boldsymbol{\lambda}))| \leq \|\Lambda\| - M(\Lambda) - |\boldsymbol{\lambda}|/2$.*

Proof. Take any $\boldsymbol{\gamma} \in \Lambda_{-\boldsymbol{\lambda}}$. Note that there are $\mu_{\boldsymbol{\gamma}}(a \oplus b)$ many 2-sets $\{\gamma, \gamma'\} \subseteq \boldsymbol{\gamma}$ such that $\gamma \oplus \gamma' = a \oplus b$ and hence $b = \gamma' \oplus (a \oplus \gamma) \in \boldsymbol{\gamma} \oplus (a \oplus \gamma)$. So, $(a \oplus \gamma, \boldsymbol{\gamma}) \notin I(\lambda, \boldsymbol{\lambda})$. So, $|I(\lambda, \boldsymbol{\lambda})| \leq \sum_{\boldsymbol{\gamma} \in \Lambda_{-\boldsymbol{\lambda}}} (|\boldsymbol{\gamma}| - \mu_{\boldsymbol{\gamma}}(a \oplus b)) = (\|\Lambda\| - |\boldsymbol{\lambda}|) - M(\Lambda) + \mu_{\boldsymbol{\lambda}}(a \oplus b) \leq \|\Lambda\| - M(\Lambda) - |\boldsymbol{\lambda}|/2$, as $\mu_{\boldsymbol{\lambda}}(a \oplus b) \leq |\boldsymbol{\lambda}|/2$. Indeed, for every element, $\lambda \in \boldsymbol{\lambda}$, there exists at most one element λ' in $\boldsymbol{\lambda}$ such that $\lambda \oplus \lambda' = a \oplus b$. In the case where it exists, then neither λ nor λ' can be part of a different 2-set. □

Remark 7.2. Note that this is where we use the hypothesis that underlying group is of exponent 2. We exhibit a simple counter-example when this is not the case. Take for example $\mathcal{G} = \mathbb{Z}/6\mathbb{Z}$, and $\boldsymbol{\lambda} = \{0, 2, 4\}$. Then one has $\mu_{\boldsymbol{\lambda}}(2) = 3 = |\boldsymbol{\lambda}|$. Note that, as we will see later, that the condition $\mu_{\boldsymbol{\lambda}}(a - b) \leq |\boldsymbol{\lambda}| - 1$ is required to conclude the proof of Lemma 7.1. This hints that either the case where the exponent of $\mathcal{G}$ is greater than 3 is fundamentally different from our case, or that our current proof strategy can still be tightened.

7.1.2 *Recursive Inequality of the D-terms*

The definition of D-terms, $D(\alpha, \ell)$ for $\alpha \leq \|\Lambda\|, \ell \geq 0$, Defn. 5.1, holds for any centered set-system. Let us generalize the recursive inequality of D-terms to any centered set-system:

Lemma 7.3 (Recursive Inequality for the D-terms). *Let $\alpha \leq |\Lambda| \leq \frac{2^m}{12\xi_{\max}^2}$, $\ell \geq 0$. Then,*

$$D(\alpha, \ell) \leq D(\alpha, \ell - 1) + \frac{\xi_{\max}}{2^m} \sum_{i=1}^{|\Lambda|} D(\alpha - 1, \ell + \xi_i - 1) + \frac{2M(\Lambda)\xi_{\max} \cdot \boldsymbol{\rho}(\Lambda)}{2^m \left(1 - |\Lambda|\xi_{\max}^2/2^m\right)^{|\Lambda| - \alpha}}. \tag{7.2}$$

Note, for $q \leq \|\Lambda\| \leq 2^m/12\xi_{\max}^2$, $\frac{\xi_{\max}}{2^m(1 - |\Lambda|\xi_{\max}^2/2^m)} \leq (4\xi e q)^{-1}$. Denoting $\beta := \xi_{\max}/2^m$, and $a_{d,\ell} = \frac{\beta^d}{2\boldsymbol{\rho}(\Lambda)} D(q - d, \ell)$ we have,

$$a_{d,\ell} \leq a_{d,\ell-1} + \sum_{i=1}^{q} a_{d+1,\ell+\ell_i} + \beta M(\Lambda) \left(4e\xi_{\max} q\right)^{-d},$$

where $\ell_i = \xi_i - 1$.

Proof. We fix $\boldsymbol{\lambda} \in \Lambda' \subseteq \Lambda$ where $|\Lambda'| = \alpha$ and a set $\boldsymbol{\gamma}$ with $|\boldsymbol{\gamma}| = \ell + 1$ disjoint with $\boldsymbol{\lambda}$. Let $\Gamma := \Lambda_{+\boldsymbol{\gamma}}$ and $\Gamma' := \Gamma_{-\boldsymbol{\lambda}-\boldsymbol{\gamma}+(\boldsymbol{\lambda}\sqcup\boldsymbol{\gamma})}$. Looking back at Fig. 5.1, τ and τ' would correspond respectively to the second and third graphs. We assume that $\Lambda', \boldsymbol{\gamma}, \boldsymbol{\lambda}$ are chosen in such a manner that $|\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma')| = D(\alpha, \ell)$. Now we prove the inequality in two cases.
Case $|\boldsymbol{\gamma}| = 1$. In this case, let $\boldsymbol{\gamma} = \{\gamma\}$. Then $\boldsymbol{\rho}(\Gamma) = \boldsymbol{\rho}(\Lambda') \cdot (1 - \|\Lambda'\|/2^n)$ from Eq. (5.1). Also $\Gamma'_{-\gamma|\boldsymbol{\lambda}\sqcup\boldsymbol{\gamma}} = \Lambda'$. Hence from link deletion lemma, Eq. 5.3,

$$\boldsymbol{\rho}(\Gamma') = \boldsymbol{\rho}(\Lambda') - 2^{-m} \sum_{(\delta,\boldsymbol{\lambda}')\in I} \boldsymbol{\rho}(\Gamma'_{\delta,\boldsymbol{\lambda}'})$$

where $I := I(\gamma, \boldsymbol{\lambda}) = \{(\delta, \boldsymbol{\lambda}') : \gamma \oplus \delta \in \boldsymbol{\lambda}' \in \Lambda'_{-\boldsymbol{\lambda}}, \boldsymbol{\lambda}' \oplus \delta \text{ is disjoint with } \boldsymbol{\lambda}\}$. For $z' \in \boldsymbol{\lambda}' \in \Lambda'_{-\boldsymbol{\lambda}}$, $(\gamma \oplus z, \boldsymbol{\lambda}') \notin I$ if and only if there exists $y \in \boldsymbol{\lambda}$ and $w \in \boldsymbol{\lambda}'$ such that $\gamma \oplus y = z \oplus w$. Thus $|I| \geq \sum_{\boldsymbol{\lambda}'\in\Lambda'_{-\boldsymbol{\lambda}}} \left(|\boldsymbol{\lambda}'| - \sum_{y\in\boldsymbol{\lambda}} 2\mu_{\boldsymbol{\lambda}'}(\gamma \oplus y)\right) = \|\Lambda'\| - |\boldsymbol{\lambda}| - \sum_{y\in\boldsymbol{\lambda}} 2\mu_{\Lambda'_{-\boldsymbol{\lambda}}}(\gamma \oplus y) \geq \|\Lambda'\| - \|\Lambda'\|_{\max} \cdot 2M(\Lambda')$. Hence

$$\begin{aligned}
D(\alpha, 0) = |\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma')| &= \left| \frac{\|\Lambda'\|}{2^m} \boldsymbol{\rho}(\Lambda') - 2^{-m} \sum_{(\delta,\boldsymbol{\lambda}')\in I} \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda}')}) \right| \\
&\overset{(\star)}{\leq} 2^{-m} \sum_{(\delta,\boldsymbol{\lambda}')\in I} |\boldsymbol{\rho}(\Lambda') - \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda}')})| + \frac{2M(\Lambda')\|\Lambda'\|_{\max} \cdot \boldsymbol{\rho}(\Lambda)}{2^m \left(1 - \frac{\|\Lambda\setminus\Lambda'\|_{\max} \times \|\Lambda'\|}{2^m}\right)^{|\Lambda\setminus\Lambda'|}} \\
&\leq \frac{\|\Lambda'_{-\boldsymbol{\lambda}}\|_{\max}}{2^m} \sum_{\boldsymbol{\lambda}'\in\Lambda'\setminus\boldsymbol{\lambda}} D(\alpha - 1, |\boldsymbol{\lambda}'| - 1) + \frac{2M(\Lambda')\|\Lambda'\|_{\max} \cdot \boldsymbol{\rho}(\Lambda)}{2^m \left(1 - \frac{\|\Lambda\setminus\Lambda'\|_{\max} \times \|\Lambda'\|}{2^m}\right)^{|\Lambda\setminus\Lambda'|}},
\end{aligned}$$

where the last term in $(\star)$ is obtained from the initial condition, Cor. (5.1.1).
Case $|\boldsymbol{\gamma}| \geq 2$. Fix $\boldsymbol{\gamma} \in \boldsymbol{\gamma}$. By link-deletion equation, we have

$$\begin{aligned}
\boldsymbol{\rho}(\Gamma) &= \boldsymbol{\rho}(\Gamma_{-\gamma|\boldsymbol{\gamma}}) - \frac{1}{2^m} \sum_{(\delta,\boldsymbol{\lambda}')\in I} \boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda}')}) \\
\boldsymbol{\rho}(\Gamma') &= \boldsymbol{\rho}(\Gamma'_{-\gamma|\boldsymbol{\lambda}\sqcup\boldsymbol{\gamma}}) - \frac{1}{2^m} \sum_{(\delta,\boldsymbol{\lambda}')\in I'} \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda}')}),
\end{aligned}$$

where

$$\begin{aligned}
I &:= I(\gamma, \boldsymbol{\gamma}) = \{(\delta, \boldsymbol{\lambda}') : \gamma \oplus \delta \in \boldsymbol{\lambda}' \in \Lambda', \ \ \boldsymbol{\lambda}' \oplus \delta \text{ is disjoint with } \boldsymbol{\gamma} \setminus \gamma\}, \\
I' &:= I(\gamma, \boldsymbol{\lambda} \sqcup \boldsymbol{\gamma}) = \{(\delta, \boldsymbol{\lambda}') : \gamma \oplus \delta \in \boldsymbol{\lambda}' \in \Lambda'_{-\boldsymbol{\lambda}}, \ \ \boldsymbol{\lambda}' \oplus \delta \text{ is disjoint with } \boldsymbol{\lambda} \sqcup \boldsymbol{\gamma} \setminus \gamma\}.
\end{aligned}$$

It is easy to see that $I' \subseteq I$. If $(\delta, \boldsymbol{\lambda}') \in I \setminus I'$, then,

- either $\boldsymbol{\lambda}' = \boldsymbol{\lambda}$ and $\delta = \gamma \oplus y$ for some $y \in \boldsymbol{\lambda}$, such that $\boldsymbol{\lambda} \oplus (\gamma \oplus y)$ is disjoint with $\boldsymbol{\gamma} \setminus \gamma$ or

- $\boldsymbol{\lambda}' \in \Lambda' \setminus \boldsymbol{\lambda}$ and $\delta = \gamma \oplus z$ for some $z \in \boldsymbol{\lambda}'$, such that $\boldsymbol{\lambda}' \oplus (\gamma \oplus z)$ is disjoint with $\boldsymbol{\gamma} \setminus \gamma$ but not disjoint with $\boldsymbol{\lambda} \sqcup (\gamma \setminus \gamma)$.

The first case can contribute at most $|\boldsymbol{\lambda}|$. The second case will happen if for some $z, w \in \boldsymbol{\lambda}'$, and $y \in \boldsymbol{\lambda}$, $z \oplus w = \boldsymbol{\gamma} \oplus y$. Thus

$$|I \setminus I'| \leq |\boldsymbol{\lambda}| + \sum_{y \in \boldsymbol{\lambda}} \mu_{\Lambda'_{-\boldsymbol{\lambda}}}(\gamma \oplus y) \leq \|\Lambda'\|_{\max} \cdot 2M(\Lambda').$$

Hence, we have the following:

$$\begin{aligned}
&D(\alpha, \ell) = |\boldsymbol{\rho}(\Gamma) - \boldsymbol{\rho}(\Gamma')| \\
&\leq \left|\boldsymbol{\rho}(\Gamma_{-\gamma|\boldsymbol{\gamma}}) - \boldsymbol{\rho}(\Gamma'_{-\gamma|\boldsymbol{\lambda}\sqcup\boldsymbol{\gamma}})\right| + 2^{-m} \sum_{(\delta,\boldsymbol{\lambda}') \in I'} \left|\boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda}')}) - \boldsymbol{\rho}(\Gamma'_{(\delta,\boldsymbol{\lambda}')})\right| + \sum_{(\delta,\boldsymbol{\lambda}') \in I \setminus I'} \boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda}')})/2^m \\
&\leq D(\alpha, \ell - 1) + \frac{\|\Lambda'_{-\boldsymbol{\lambda}}\|_{\max}}{2^m} \sum_{\boldsymbol{\lambda}' \in \Lambda'_{-\boldsymbol{\lambda}}} D(\alpha - 1, \ell + |\boldsymbol{\lambda}'| - 1) + \frac{2M(\Lambda')\|\Lambda'\|_{\max} \cdot \boldsymbol{\rho}(\Lambda)}{2^m \left(1 - \frac{\|\Lambda \setminus \Lambda'\|_{\max} \times \|\Lambda'\|}{2^m}\right)^{|\Lambda \setminus \Lambda'|}}.
\end{aligned} \tag{7.3}$$

The last inequality follows from the observation that $\Gamma_{(\delta,\boldsymbol{\lambda}')}$ and $\Gamma'_{(\delta,\boldsymbol{\lambda}')}$ are considered when we take maximum to compute $D(\alpha - 1, \ell + |\boldsymbol{\lambda}'| - 1)$. Moreover, from our initial condition Cor. 5.1.1,

$$\boldsymbol{\rho}(\Gamma_{(\delta,\boldsymbol{\lambda}')}) \leq \boldsymbol{\rho}(\Lambda') \leq \boldsymbol{\rho}(\Lambda) / \left(1 - \frac{\|\Lambda \setminus \Lambda'\|_{\max} \times \|\Lambda'\|}{2^m}\right)^{|\Lambda \setminus \Lambda'|}$$

Now, taking upper bounds of the total size terms, and adding some positive terms in the middle sum, and noting that $M(\Lambda') \leq M(\Lambda)$ [1], the inequality, Eq. (7.3) can be easily modified to the recursive inequality, Eq. (7.2). □

7.1.3 *Final Wrap up of Proof*

We can conclude the proof of the core lemma, Lemma 7.1, using Lemmas 7.2, 7.3, along with the following result that will be proven in Subsect. 7.1.4.

Lemma 7.4 (Recursive Inequality Bound II). *Suppose $a_{d,\ell} \geq 0$ such that: (i) $a_{d,k} := 0$ for all $k < 0$, and (ii) for all $0 \leq d \leq \xi m$ and $0 \leq \ell_i \leq \xi - 1$ for $i \in [q]$, we have*

$$a_{d,\ell} \leq (4\xi e q)^{-d} \qquad \text{(initial bound)} \tag{7.4}$$

1 Since $\Lambda' \subseteq \Lambda$, we have $\sum_{\boldsymbol{\lambda} \in \Lambda'} \mu_{\boldsymbol{\lambda}}(z) \leq \sum_{\boldsymbol{\lambda}' \in \Lambda} \mu_{\boldsymbol{\lambda}'}(z)$ for every $z \in \{0,1\}^n$, since every $\boldsymbol{\lambda} \in \Lambda'$ is subset of some $\boldsymbol{\lambda}' \in \Lambda$. So taking maximum over all $z \in \{0,1\}^n$, on both sides would give us $M(\Lambda') \leq M(\Lambda)$.

$$a_{d,\ell} \leq a_{d,\ell-1} + \sum_{i=1}^{q} a_{d+1,\ell+\ell_i} + C \cdot (4\xi eq)^{-d} \quad \text{(recursive inequality)} \tag{7.5}$$

for some $C > 0$. Then, for every $\ell \in [\xi - 2]$,

$$a_{0,\ell} \leq \frac{4}{2^m} + 4C\xi.$$

Remark 7.3. Note that the initial bound ensures only that $a_{0,\ell} \leq 1$. However, the presence of recursive inequality forces the value of $a_{0,\ell}$ to be very small.

Let $\lambda, \lambda', \boldsymbol{\lambda}, \Lambda$ be as in the statement of core lemma, Lemma 7.1, and let $\Lambda_0 = \Lambda_{-\boldsymbol{\lambda}}$. Note that one has $\xi_{\max}^2 m \leq 2^{m/2} - \xi_{\max} \leq \|\Lambda_0\| \leq 2^m/12\xi_{\max}^2$. Moreover, let $q = |\Lambda_0|$. Similarly, one has $\xi_{\max} q \geq \|\Lambda_0\| \geq \xi_{\max}^2 m$, which means that $q \geq \xi_{\max} m$. We are going to apply Lemma 7.4 to Λ_0 as follows.

Let us take, $\xi = \xi_{\max}$, $C = \beta M(\Lambda) = M(\Lambda)\xi_{\max}/2^m$ in the statement of the above Lemma 7.3. From the definition of $a_{d,\ell} = \frac{\beta^d}{2\boldsymbol{\rho}(\Lambda_0)} D(q-d,\ell)$, we must ensure that $q \geq d$ in order to apply Lemma 7.3. This can easily be seen to be true as $q \geq \xi m$ and $d \leq \xi m$. Then, for $(\delta, \boldsymbol{\lambda}') \in I(\lambda, \boldsymbol{\lambda})$, we have

$$|\boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) - \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})| \leq D(q, |\boldsymbol{\lambda}| - 2) \leq 2\boldsymbol{\rho}(\Lambda_0) a_{0,|\boldsymbol{\lambda}|-2} \leq \frac{8\boldsymbol{\rho}(\Lambda_0)}{2^m}(\Delta\xi_{\max}^2 + 1).$$

Note that one has

$$\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \geq \boldsymbol{\rho}(\Lambda_0)\left(1 - \frac{\|\Lambda_0\|\xi_{\max}}{2^m}\right) \geq \boldsymbol{\rho}(\Lambda_0)\left(1 - \frac{1}{12\xi_{\max}}\right) \geq \boldsymbol{\rho}(\Lambda_0)\frac{23}{24}.$$

Thus, one has

$$\begin{aligned}
\boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) &\leq \frac{8\boldsymbol{\rho}(\Lambda_0)}{2^m}(M(\Lambda)\xi_{\max}^2 + 1) + \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \leq \left(\frac{8\boldsymbol{\rho}(\Lambda_0)(M(\Lambda)\xi_{\max}^2+1)}{2^m \cdot \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})} + 1\right)\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \\
&\leq \left(\frac{24\cdot 8}{23\cdot 2^m}(M(\Lambda)\xi_{\max}^2+1) + 1\right)\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \leq \left(\frac{C'M(\Lambda)}{2^m} + 1\right)\boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}),
\end{aligned}$$

where $C' = 9(\xi_{\max}^2 + 1)$, as $M(\Lambda) \geq 1$. Using this bound in the appropriate link deletion equation we have:

$$\begin{aligned}
\boldsymbol{\rho}(\Lambda) &= \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) - \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda}')\in I(\lambda|\boldsymbol{\lambda})} \boldsymbol{\rho}(\Lambda_{(\delta,\boldsymbol{\lambda}')}) \quad \text{(From Eq. (5.3))} \\
&\geq \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) - \frac{1}{2^m}\sum_{(\delta,\boldsymbol{\lambda}')\in I(\lambda,\boldsymbol{\lambda})} \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})(1 + C'M(\Lambda)/2^m) \\
&\geq \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}})\left(1 - \frac{\|\Lambda\| - M(\Lambda) - |\boldsymbol{\lambda}|/2}{2^m}\left(1 + \frac{C'M(\Lambda)}{2^m}\right)\right) \quad \text{(From Lemma 7.2)}
\end{aligned}$$

$$\geq \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \left(1 - \frac{\|\Lambda\| - 1}{2^m} + \frac{M(\Lambda)}{2^m}\left(1 - \frac{C'(\|\Lambda\| - M(\Lambda) - 1)}{2^m}\right)\right)$$
$$\geq \boldsymbol{\rho}(\Lambda_{-\lambda|\boldsymbol{\lambda}}) \left(1 - \frac{\|\Lambda\| - 1}{2^m}\right).$$

The last inequality follows as $C'\|\Lambda\| \leq 2^m$, for $\|\Lambda\| \leq 2^m/12\xi_{\max}^2$, which concludes our proof of Lemma 7.1. □

7.1.4 *Proof of Recursive Inequality Bound II, Lemma 7.4*

Let us denote by an ordered tuple of integers from $[q]$, as $i^k := (i_1, \cdots, i_k) \in [q]^k$. Note that, for all positive integer j, $e^j \geq \frac{j^j}{j!}$ and so $1/j! \leq (e/j)^j$, and we have

$$\binom{t}{j} \leq \frac{t^j}{j!} \leq (et/j)^j. \tag{7.6}$$

This inequality will be frequently used for the proof of this lemma. We also use the following fact extensively: for $r < 1$, $\sum_{j \geq i} r^j \leq \frac{r^i}{1-r}$.

We state the following claim, which follows from iterated applications of the recursive inequality.

Claim 7.4.1. For any $0 \leq d \leq \xi m$, and $0 \leq \ell < \xi - 1$ we have

$$a_{0,\ell} \leq \sum_{k=\left\lceil \frac{d-\ell}{\xi} \right\rceil}^{d} \binom{d}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^k \ell_{i_j} - d} + C \sum_{i=0}^{d-1} \sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j} (4\xi e)^{-j}. \tag{7.7}$$

PROOF OF THE CLAIM. We prove the claim by induction on d. The result holds trivially for $d = 1$ (by applying $d = \ell = 0$ in Eqn. (7.5)). Now we prove the statement for $d_0 + 1$, assuming it is true for d_0. Therefore, we have

$$\begin{aligned} a_{0,\ell} &\leq \sum_{k=\left\lceil \frac{d_0-\ell}{\xi} \right\rceil}^{d_0} \binom{d_0}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^k \ell_{i_j} - d_0} + C \sum_{i=0}^{d_0-1} \sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j} (4\xi e)^{-j} \\ &\leq \sum_{k=\left\lceil \frac{d_0-\ell}{\xi} \right\rceil}^{d_0} \binom{d_0}{k} \sum_{i^k \in [q]^k} \left(\sum_{i_{k+1} \in [q]} a_{k+1,k+1+\sum_{j=1}^{k+1} \ell_{i_j} - (d_0+1)} + C \cdot (4\xi e q)^{-k} \right) \\ &\quad + \sum_{k=\left\lceil \frac{d_0-\ell}{\xi} \right\rceil}^{d_0} \binom{d_0}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^k \ell_{i_j} - (d_0+1)} + C \sum_{i=0}^{d_0-1} \sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j} (4\xi e)^{-j} \end{aligned}$$

$$\leq \sum_{k=\left\lceil \frac{d_0+1-\ell}{\xi} \right\rceil}^{d_0+1} \binom{d_0}{k-1} \sum_{i^{k-1}\in[q]^{k-1}} \sum_{i_k\in[q]} a_{k,k+\sum_{j=1}^{k}\ell_{i_j}-(d_0+1)}$$
$$+ \sum_{k=\left\lceil \frac{d_0+1-\ell}{\xi} \right\rceil}^{d_0+1} \binom{d_0}{k} \sum_{i^{k}\in[q]^{k}} a_{k,k+\sum_{j=1}^{k}\ell_{i_j}-(d_0+1)} + C\sum_{i=0}^{d_0}\sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j}(4\xi e)^{-j}.$$

The range of the first and second summations has deliberately been taken to start from $\lceil (d_0+1-\ell)/\xi \rceil \leq \lceil (d_0-\ell)/\xi \rceil + 1$, because if $k < \lceil (d_0+1-\ell)/\xi \rceil$, then $k + \sum_{j=1}^{k}\ell_{i_j} - (d_0+1) \leq k\xi - (d_0+1) < 0$ and hence $a_{k,k+\sum_{j=1}^{k}\ell_{i_j}-(d_0+1)} = 0$. Now we can see that the coefficient of $\sum_{i^k\in[q]^k} a_{k,k+\sum_{j=1}^{k}-(d_0+1)}$ in the above summation is bounded by $\binom{d_0}{k-1} + \binom{d_0}{k} = \binom{d_0+1}{k}$. This concludes the proof of the claim. □

PROOF OF LEMMA 7.4. Let us take $d = \xi m$. In that case, Claim 1 becomes

$$a_{0,\ell} \leq \sum_{k=\left\lceil \frac{\xi m-\ell}{\xi} \right\rceil}^{\xi m} \binom{\xi m}{k} \sum_{i^{k}\in[q]^{k}} a_{k,k+\sum_{j=1}^{k}\ell_{i_j}-\xi m} + C\sum_{i=0}^{\xi m-1}\sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j}(4\xi e)^{-j}.$$

We are going to upper bound both terms of the sum in subsequent turns. For the first term, note that one has $k \geq m - \frac{\ell}{\xi} > m-1$ since $\ell < \xi - 1$ by definition. This implies that

$$\binom{\xi m}{k} \leq \left(\frac{e\xi m}{k}\right)^{k} \leq \left(\frac{e\xi m}{m-1}\right)^{k} \leq (2e\xi)^{k}.$$

Hence, using the initial bound, one has

$$\sum_{k=\left\lceil \frac{\xi m-\ell}{\xi} \right\rceil}^{\xi m} \binom{\xi m}{k} \sum_{i^{k}\in[q]^{k}} a_{k,k+\sum_{j=1}^{k}\ell_{i_j}-\xi m} \leq \sum_{k=\left\lceil \frac{\xi m-\ell}{\xi} \right\rceil}^{\xi m} (2e\xi)^{k} q^{k} (4\xi eq)^{-k} \leq \frac{4}{2^m} \leq \frac{4}{2^m}$$

As for the second term, we make the following observation: For $\xi k < i \leq \xi(k+1)$, $k \in (n-1]$, $j \geq \lceil \frac{i-\ell}{\xi} \rceil \geq k$, and hence

$$\binom{i}{j} \leq \left(\frac{ei}{j}\right)^{j} \leq \left(\frac{e\xi(k+1)}{k}\right)^{j} \leq (2e\xi)^{j}.$$

For $0 \leq i \leq \xi$ and $j \geq 1$, $\binom{i}{j} \leq \left(\frac{ei}{j}\right)^{j} \leq (e\xi)^{j}$. Thus, we are going to break the sum into two parts:

$$\sum_{i=0}^{\xi m-1}\sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j}(4\xi e)^{-j} = \sum_{i=0}^{\xi}\sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j}(4\xi e)^{-j} + \sum_{i=\xi+1}^{\xi m-1}\sum_{j=\left\lceil \frac{i-\ell}{\xi} \right\rceil}^{i} \binom{i}{j}(4\xi e)^{-j}$$

$$
\begin{aligned}
&\leq \xi + 1 + \sum_{i=0}^{\xi} \sum_{j=1}^{i} (e\xi)^j (4e\xi)^{-j} + \sum_{i=\xi+1}^{\xi m-1} \sum_{j=\lceil i/\xi \rceil - 1}^{i} (2e\xi)^j (4e\xi)^{-j} \\
&\leq \xi + 1 + \frac{\xi+1}{3} + 4 \sum_{i=\xi+1}^{\xi m-1} \frac{1}{2^{\lceil i/\xi \rceil}} \\
&\overset{(1)}{\leq} \frac{4}{3}(\xi+1) + 2\xi \overset{(2)}{\leq} 4\xi,
\end{aligned}
$$

where the last inequality follows from the fact that $\xi \geq 2$. □

8

BMTP FOR $\xi_{\max} = 2$

In this chapter we analyse the simplest version of the BMTP$((A, B), \boldsymbol{a}^q, \lambda^q)$ problem, where any pair of coefficient vectors $\boldsymbol{a}_i$ and $\boldsymbol{a}_j$ are orthogonal. In this case the graph $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^q, \lambda^q])$ consists just of isolated edges. Of course, the size of each component of this graph is 2, hence $\xi_{\max} = 2$.

However, first we present a reformulation of the general BMTP problem. The main reason to do this is because this formulation will facilitate the proof of the $\xi_{\max} = 2$ subcase. Moreover, this formulation might motivate future direction and open problems that are not in the scope of this thesis.

The graph, $\mathscr{G}(\mathscr{E})$, associated with the system of equations, $\mathscr{E}$, of a BMTP$((A, B), \boldsymbol{a}^e, \lambda^e)$ problem, is a bipartite graph between shores A and B. While standardizing $\mathscr{E}$, as $\mathscr{E}[\Lambda^{\{\!\{c\}\!\}}] := \mathscr{E}(\mathrm{Star}(\mathscr{G}(\mathscr{E})))$, let us assume the convention that all the representative vertices, one from each component of $\mathscr{G}(\mathscr{E})$, used in the Star transformation (recall from Chapter 4), are chosen from shore A. Then the collection of edge-labels of the i-th component can be alternatively viewed as a pair of multisets, $\{\boldsymbol{\lambda}_{i,A} := \{\lambda_j : j \in [\![v_i]\!] \cap A\}, \boldsymbol{\lambda}_{i,B} := \{\lambda_j : j \in [\![v_i]\!] \cap B\}\}$, where $\boldsymbol{\lambda}_{i,A}$ (resp., $\boldsymbol{\lambda}_{i,B}$) denotes the collection of labels of the edges from the center of the star to vertices in A (resp., B). For simplicity of notation we can relabel the elements so that $\boldsymbol{\lambda}_{i,A} = \{\lambda^A_{i,1}, \ldots, \lambda^A_{i,\xi^A_i} - 1\}$ and $\boldsymbol{\lambda}_{i,B} = \{\lambda^B_{i,1}, \ldots, \lambda^B_{i,\xi^B_i}\}$, where ξ^A_i (resp., ξ^B_i) are the number of A-vertices (resp. B-vertices) in $[\![v_i]\!]$.

BISET-SYSTEM. Note that if the system of equations, $\mathscr{E}$, of a BMTP problem is in standard form, then the non-equations of the BMTP problem force the following two conditions on the edge-labels of $\mathscr{G}(\mathscr{E})$: (1) label of any edge between two vertices in A is non-zero, i. e., $\lambda^A_{i,j} \neq 0^m$ for all $j \in [\xi^A_i - 1], i \in [c]$, (2) label-sum of a path between any two vertices in A (resp. any two vertices in B) is non-zero, i. e., $\lambda^A_{i,j} \neq \lambda^A_{i,j'}$ and $\lambda^B_{i,k} \neq \lambda^B_{i,k'}$ for all $j, j' \in [\xi^A_i - 1], k, k' \in [\xi^B_i], i \in [c]$. This implies both $\boldsymbol{\lambda}_{i,A}$ and $\boldsymbol{\lambda}_{i,B}$ are sets for $i \in [c]$. We call an ordered pair of set-systems, both containing equal number of sets, a *biset-system*. If the system of equations corresponding to a BMTP problem is in standard form, then the problem, like its system of equations, can be characterized by a biset system, $(\Lambda^{\{\!\{c\}\!\}}_A, \Lambda^{\{\!\{c\}\!\}}_B)$, where $\Lambda^{\{\!\{c\}\!\}}_A = \{\!\{\boldsymbol{\lambda}_{1,A}, \ldots, \boldsymbol{\lambda}_{c,A}\}\!\}$ and $\Lambda^{\{\!\{c\}\!\}}_B = \{\!\{\boldsymbol{\lambda}_{1,B}, \ldots, \boldsymbol{\lambda}_{c,B}\}\!\}$.

Reformulation of BMTP

NOTATION. $\eta_i^A := \xi_i^A - 1$, denote the number of edges between A-vertices in the i-th component.

The *bipartite homogeneous bivariate Mirror Theory Problem* instantiated by the biset-system

$$(\Lambda_A^{\{\!\{c\}\!\}}, \Lambda_B^{\{\!\{c\}\!\}}) = (\{\!\{\boldsymbol{\lambda}_{1,A}, \ldots, \boldsymbol{\lambda}_{c,A}\}\!\}, \{\!\{\boldsymbol{\lambda}_{1,B}, \ldots, \boldsymbol{\lambda}_{c,B})\}\!\}) :$$

$$\begin{aligned} \boldsymbol{\lambda}_{i,A} &= \{\lambda_{i,1}^A, \ldots, \lambda_{i,\eta_i^A}\}, \quad \lambda_{i,j}^A \neq 0^m, j \in [\eta_i^A] && i \in [c] \\ \boldsymbol{\lambda}_{i,B} &= \{\lambda_{i,1}^B, \ldots, \lambda_{i,\xi_i^B}\}, && i \in [c] \end{aligned}$$

also denoted as $\texttt{BMTP}(\Lambda_A^{\{\!\{c\}\!\}}, \Lambda_B^{\{\!\{c\}\!\}})$, is to find the number of solutions to the system of equations and non-equations:
(EQUATIONS).

$$\begin{aligned} \mathsf{X}_{i,0} \oplus \mathsf{X}_{i,j} &= \lambda_{i,j}^A, \quad j \in [\eta_i^A], i \in [c]. \\ \mathsf{X}_{i,0} \oplus \mathsf{Y}_{i,j} &= \lambda_{i,j}^B, \quad j \in [\xi_i^B], i \in [c]. \end{aligned}$$

(NON-EQUATIONS).

$$\begin{aligned} \mathsf{X}_{i,j} &\neq \mathsf{X}_{i',j'} \quad \text{for all } j \in [0..\eta_i^A], j' \in [0..\eta_{i'}^A], i, i' \in [c], i \neq i'. \\ \mathsf{Y}_{i,j} &\neq \mathsf{Y}_{i',j'} \quad \text{for all } j \in [\xi_i^B], j' \in [\xi_{i'}^B], i, i' \in [c], i \neq i'. \end{aligned}$$

Notation: We denote a the biset-system $(\Lambda_A^{\{\!\{c\}\!\}}, \Lambda_B^{\{\!\{c\}\!\}})$ as $\Lambda_{AB}^{\{\!\{c\}\!\}}$. An element of Λ_{AB} is a pair of sets $(\boldsymbol{\lambda}_A, \boldsymbol{\lambda}_B)$, which will be denoted as $\boldsymbol{\lambda}_{AB}$. An element in $\boldsymbol{\lambda}_A$ will be typically denoted as λ_A, whereas an element in $\boldsymbol{\lambda}_B$ will be typically denoted as λ_B.

Recall that the system of equations and non-equations corresponding to $\texttt{BMTP}(\Lambda_{AB}^{\{\!\{c\}\!\}})$ is consistent if (1) $\lambda_{i,j}^A \neq 0^m$ for $j \in [\eta_{i,A}], i \in [c]$, and (2) $\lambda_{i,j}^A \neq \lambda_{i,j'}^A$ for $j, j' \in [\eta_{i,A}], j \neq j', i \in [c]$, and $\lambda_B \ell \neq \lambda_B \ell'$ for $j, j' \in [\eta_{i,B}], j \neq j', i \in [c]$. While easy to manipulate, both conditions have to be handled in a different way, leading to unnecessary complications. The simplest fix is to introduce an additional element 0^m to each of the sets $\boldsymbol{\lambda}_{i,A}$. Thus instead of considering the multiset, $\boldsymbol{\lambda}_{i,A}$, of only the edge-labels of the i-th component, if we consider the multiset $(\boldsymbol{\lambda}_{i,A})_{+0^m} := \{\!\{0^m, \lambda_{i,1}, \ldots, \lambda_{i,\eta_{i,A}}\}\!\}$ then we can combine the two consistency conditions above and just say that $(\boldsymbol{\lambda}_{i,A})_{+0^m}$ is a set for all $i \in [c]$. If every A-set in a biset-system contains 0^m we call the set-system a *centered biset-system*.

Thus if the system of equations and non-equations of $\texttt{BMTP}(\Lambda_{AB}^{\{\!\{c\}\!\}})$ is consistent, then $(\Lambda_{AB}^{\{\!\{c\}\!\}})_{+0^m|A} := \{\!\{((\boldsymbol{\lambda}_{1,A})_{+0^m}, \boldsymbol{\lambda}_{1,B}), \ldots, ((\boldsymbol{\lambda}_{c,A})_{+0^m}, \boldsymbol{\lambda}_{c,B})\}\!\}$ is a centered biset-system.

Bipartite Disjointness Event for a Biset-System

Given a centered biset-system $\Lambda_{AB}^{\{\!\{c\}\!\}}$, we say that the *bipartite disjointness event*, $\mathsf{BDE}(\Lambda_{AB}^{\{\!\{c\}\!\}})$, holds, if for a random vector $\mathsf{S}^c = (\mathsf{S}_1, \ldots, \mathsf{S}_c)$, where $\mathsf{S}_i \xleftarrow{\$} \{0,1\}^m$ independently for each $i \in [c]$, the translated sets, $\mathsf{S}_1 \oplus \boldsymbol{\lambda}_{1,A}, \ldots, \mathsf{S}_c \oplus \boldsymbol{\lambda}_{c,A}$ are disjoint, and $\mathsf{S}_1 \oplus \boldsymbol{\lambda}_{1,B}, \ldots, \mathsf{S}_c \oplus \boldsymbol{\lambda}_{c,B}$ are disjoint.
We define the probability of the bipartite disjointness event as

$$\boldsymbol{\mathcal{p}}(\Lambda_{AB}^{\{\!\{c\}\!\}}) := \boldsymbol{\mathcal{p}}_{\mathsf{S}^c}(\mathsf{BDE}(\Lambda_{AB}^{\{\!\{c\}\!\}})).$$

Note that, every A-set in a centered biset-system is non-empty because they at least contain the element 0^m.

THE $\xi_{\max} = 2$ CASE. Now we present the particular type of biset-systems that we will come across the proof for the $\xi_{\max} = 2$ subcase of the BMTP problem.

Unistar and paired biset-systems

Consider a biset-system $\Lambda_{AB}^{\{\!\{q\}\!\}}$ with $\boldsymbol{\lambda}_{i,A} = \{0^m\}$, $\boldsymbol{\lambda}_{i,B} = \{\lambda_i\}$, for $i \in [q-1]$ and $0 \geq |\boldsymbol{\lambda}_{q,B}| - |\boldsymbol{\lambda}_{q,A}| \leq 1$. A biset-system with this property is called a *unistar* biset-system. If $|\boldsymbol{\lambda}_{q,A}| + |\boldsymbol{\lambda}_{q,B}| = \ell$, we say Λ_{AB} is a unistar biset-system with a *ℓ-star*. Moreover if $\boldsymbol{\lambda}_{q,A} = \{0^m\}$ and $\boldsymbol{\lambda}_{q,B} = \{\lambda_q\}$, then $\Lambda_{AB}^{\{\!\{c\}\!\}}$ will be called a *paired* biset-system.

Now we present our main result for paired biset-systems:

Main result for BMTP with $\xi_{\max} = 2$

Theorem 8.1. *For $m \geq 7$ and any paired biset-system $\Lambda_{AB}^{\{\!\{q\}\!\}}$ with $1 \leq q \leq 2^m/17$, we have*

$$\boldsymbol{\mathcal{p}}(\Lambda_{AB}^{\{\!\{q\}\!\}}) \geq \frac{((2^m)_q)^2}{2^{2mq}}\left(1 - \frac{8m^3}{2^{2m}} - \frac{19q^2}{2^{2m}}\right).$$

We first exploit the properties of the probabilities of the distinctness event between related labels for independent permutations case through Lemma 8.1 and Lemma 8.2. Similar to our CMTP proofs, we introduce the notion of the link-deletion operation and the Link-Deletion Lemma (i.e., Lemma 8.3). These results together will allow us to state the Core-Lemma (i.e., Lemma 8.4), which allows us to prove Lemma 8.1.

Lemma 8.1. *For a unistar biset-system $\Lambda_{AB}^{\{\!\{q\}\!\}}$ with $\boldsymbol{\lambda}_{q,A} = \{0^m\}$ and $\boldsymbol{\lambda}_{q,B} = \emptyset$, we have*

$$\boldsymbol{\rho}(\Lambda_{AB}) = \boldsymbol{\rho}(\Lambda_{AB} \setminus \boldsymbol{\lambda}_{q,AB}) \cdot \left(1 - \frac{q-1}{2^m}\right)$$

Proof. The result follows from the fact that

$$\mathsf{BDE}(\Lambda_{AB}^{\{\!\{q\}\!\}}) = \underbrace{\mathsf{BDE}(\Lambda_{AB} \setminus \boldsymbol{\lambda}_{q),AB}}_{\mathsf{E}} \wedge \underbrace{\left(\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} \in \{0,1\}^m \setminus \{\mathsf{S}_{\boldsymbol{\lambda}_{1,AB}}, \ldots, \mathsf{S}_{\boldsymbol{\lambda}_{q-1,AB}}\}\right)}_{\mathsf{E}'}$$

and the fact that the events E and E' above are independent. □

Lemma 8.2. *For a paired biset-system, $\Lambda_{AB}^{\{\!\{q\}\!\}}$ and any of its paired biset-subsystem $\Gamma_{AB}^{\{\!\{q-d\}\!\}} \subseteq \Lambda_{AB}$, we have*

$$\boldsymbol{\rho}(\Gamma_{AB}) \leq \boldsymbol{\rho}(\Lambda_{AB}) / \left(1 - \frac{2q}{2^m}\right)^d$$

Proof. $\mathsf{BDE}(\Gamma_{AB}) \wedge \neg\mathsf{BDE}(\Lambda_{AB}) \equiv$ For each $\boldsymbol{\lambda}_{AB} = (\{0^m\}, \{\lambda\}) \in \Lambda_{AB} \setminus \Gamma_{AB}$ $(\# = d)$,

$$\mathsf{S}_{\boldsymbol{\lambda}_{AB}} \notin \underbrace{\{\mathsf{S}_{\boldsymbol{\lambda}'_{AB}} : \boldsymbol{\lambda}'_{AB} \in \Gamma_{AB}\}}_{\#=q-d\leq q} \cup \underbrace{\{\mathsf{S}_{\boldsymbol{\lambda}'_{AB}} \oplus \lambda' \oplus \lambda : \boldsymbol{\lambda}'_{AB} = (\{0^m\}, \{\lambda'\}) \in \Gamma_{AB}\}}_{\#=q-d\leq q}$$

The lemma follows by union bound and the independence of $\mathsf{BDE}(\Gamma_{AB})$ and $\mathsf{S}_{\boldsymbol{\lambda}_{AB}}$ for $\boldsymbol{\lambda}_{AB} \in \Lambda_{AB} \setminus \Gamma_{AB}$. □

ALTERNATE LINK DELETION. Let $\Lambda_{AB}^{\{\!\{q\}\!\}}$ be a unistar biset-system with $|\boldsymbol{\lambda}_{q,A}| + |\boldsymbol{\lambda}_{q,B}| = \ell \geq 1$. We remove the elements alternately from $\boldsymbol{\lambda}_{q,A}$ and $\boldsymbol{\lambda}_{q,B}$ in the following manner: If $\ell \equiv 0 \pmod 2$, then we remove a link element $\lambda \in \boldsymbol{\lambda}_{q,A}$, otherwise, we remove a link element $\lambda \in \boldsymbol{\lambda}_{q,B}$.

For every $\lambda \in \boldsymbol{\lambda}_{q,A}$, we define the following set:

$$I_A(\lambda) := \{[\boldsymbol{\lambda}'_{AB}] = (\{0^m\}, \{\lambda'\}) \in \Lambda_{AB}^{\{\!\{q\}\!\}} \setminus \boldsymbol{\lambda}_{q,AB} : \lambda \oplus \lambda' \notin \boldsymbol{\lambda}_{q,B}\}$$

and for every $\lambda \in \boldsymbol{\lambda}_{q,B}$, we define the following set:

$$I_B(\lambda) := \{[\boldsymbol{\lambda}'_{AB}] = (\{0^m\}, \{\lambda'\}) \in \Lambda_{AB}^{\{\!\{q\}\!\}} \setminus \boldsymbol{\lambda}_{q,AB} : \lambda \oplus \lambda' \notin \boldsymbol{\lambda}_{q,A}\}$$

Now for every $\lambda \in \boldsymbol{\lambda}_{q,A}$, and $[\boldsymbol{\lambda}'_{AB}] \in I_A(\lambda)$, we define

$$(\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]} := (\Lambda_{AB})_{-\boldsymbol{\lambda}'_{AB}-\boldsymbol{\lambda}_{q,AB}+\boldsymbol{\lambda}''_{q,AB}} \text{ where } \boldsymbol{\lambda}''_{q,AB} = (\boldsymbol{\lambda}_{q,A}, \boldsymbol{\lambda}_{q,B} \cup \{\delta\})$$

and for every $\lambda \in \boldsymbol{\lambda}_{q,B}$, and $(\delta, \boldsymbol{\lambda}'_{AB}) \in I_B(\lambda)$, we define

$$(\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]} := (\Lambda_{AB})_{-\boldsymbol{\lambda}'_{AB}-\boldsymbol{\lambda}_{q,AB}+\boldsymbol{\lambda}''_{q,AB}} \text{ where } \boldsymbol{\lambda}''_{q,AB} = (\boldsymbol{\lambda}_{q,A} \cup \{\delta\}, \boldsymbol{\lambda}_{q,B})$$

Note that if Λ_{AB} is unistar biset-system with a ℓ-star, then $(\Lambda_B)_{[\boldsymbol{\lambda}'_{AB}]}$ is a unistar system with a $(\ell+1)$-star, for $[\boldsymbol{\lambda}'_{AB}] \in I_{A/B}(\lambda)$.

Now we state our alternate link deletion lemma for unistar biset-systems.

Lemma 8.3 (Alternate link deletion lemma). *Let $\Lambda_{AB}^{\{\!\{q\}\!\}}$ be a unistar biset-system with $|\boldsymbol{\lambda}_{q,A}| + |\boldsymbol{\lambda}_{q,B}| = \ell \geq 1$. Then using the above notations:*

$$\boldsymbol{\rho}(\Lambda_{AB}) = \boldsymbol{\rho}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,A}}) - \frac{1}{2^m} \sum_{[\boldsymbol{\lambda}'_{AB}] \in I_A(\lambda)} \boldsymbol{\rho}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_B]}), \text{ if } \ell \equiv 0 \pmod 2$$

$$\boldsymbol{\rho}(\Lambda_{AB}) = \boldsymbol{\rho}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,B}}) - \frac{1}{2^m} \sum_{[\boldsymbol{\lambda}'_{AB}] \in I_B(\lambda)} \boldsymbol{\rho}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_B]}), \text{ if } \ell \equiv 1 \pmod 2$$

Proof. For $(\delta, \boldsymbol{\lambda}'_{AB}) \in I_A(\lambda)$, the following events are equivalent:

$$\mathsf{BDE}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,A}}) \wedge (\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} = \lambda \oplus \mathsf{S}_{\boldsymbol{\lambda}'_{AB}}) \equiv \mathsf{BDE}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]}) \wedge (\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} = \lambda \oplus \mathsf{S}_{\boldsymbol{\lambda}'_{AB}}),$$

So it follows that,

$$\begin{aligned}\mathsf{BDE}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,AB}}) &\equiv \mathsf{BDE}(\Lambda_{AB}) \vee (\mathsf{BDE}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,AB}}) \wedge \neg\mathsf{BDE}(\Lambda_{AB})) \\ &\equiv \mathsf{BDE}(\Lambda_{AB}) \vee \bigvee_{[\boldsymbol{\lambda}'_{AB}] \in I_A(\lambda)} (\mathsf{BDE}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]}) \wedge (\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} = \lambda \oplus \mathsf{S}_{\boldsymbol{\lambda}'_{AB}}))\end{aligned}$$

Note that the event $(\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} = \lambda \oplus \mathsf{S}_{\boldsymbol{\lambda}'_{AB}})$ occurs with probability 2^{-m} and is independent of the event $\mathsf{BDE}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]})$. Also the events $(\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} = \lambda \oplus \mathsf{S}_{\boldsymbol{\lambda}^*_{AB}})$ and $(\mathsf{S}_{\boldsymbol{\lambda}_{q,AB}} = \lambda \oplus \mathsf{S}_{\boldsymbol{\lambda}^{**}_{AB}})$ for distinct $[\boldsymbol{\lambda}^*_{AB}], [\boldsymbol{\lambda}^{**}_{AB}] \in I_A(\lambda)$ are mutually exclusive. This proves our result. □

Multiplicity of B-elements

Given a paired biset-system, Λ_{AB} and $x \in \{0,1\}^m$, we define

$$\mu_{\Lambda_{AB}}(x) = \#\{\boldsymbol{\lambda}_{AB} \in \Lambda_{AB} : \boldsymbol{\lambda}_B = \{x\}\}, \quad M(\Lambda_{AB}) := \max_{x \in \{0,1\}^m} \mu_{\Lambda_{AB}}(x)$$

The core lemma for paired biset-systems goes as follows:

Lemma 8.4 (Core lemma for paired biset-systems). *For $q > 2m$, and a paired biset-system $\Lambda_{AB}^{\{\!\{q\}\!\}}$, with $\boldsymbol{\lambda}_{q,AB} = (\{0^m\}, \{\lambda\})$, where $\lambda = \arg\max_{x\in\{0,1\}^m} \mu_{\Lambda_{AB}}(x)$. Then for all $[\boldsymbol{\lambda}'_{AB}] \in I_B(\lambda)$,*

$$\boldsymbol{\rho}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]}) \leq \boldsymbol{\rho}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,B}}) \cdot \left(1 + \frac{17M(\Lambda_B)}{2^m}\right).$$

We prove the core lemma in Sect. **??**. But first we prove our main result, Theorem 8.1, putting to use the above core lemma.

PROOF OF THEOREM 8.1. We prove the result in two steps. In the first step, we prove that

$$\boldsymbol{\rho}(\Lambda_{AB}^{\{\!\{2m\}\!\}}) \geq \frac{((2^m)_{2m})^2}{(2^m)^{4n}} \left(1 - \frac{8m^3}{2^{2m}}\right), \tag{8.1}$$

and in the second step we prove that

$$\boldsymbol{\rho}(\Lambda_{AB}^{\{\!\{q\}\!\}}) \geq \boldsymbol{\rho}(\Lambda_{AB}^{\{\!\{2m\}\!\}}) \cdot \frac{((2^m - 2m)_{q-2m})^2}{(2^{2m})^{q-2m}} \left(1 - \frac{19q^2}{2^{2m}}\right) \tag{8.2}$$

holds. Combining Eqn. (8.1) and Eqn. (8.2), we have our result,

$$\begin{aligned} \boldsymbol{\rho}(\Lambda_{AB}^{\{\!\{q\}\!\}}) &\geq \frac{((2^m)_q)^2}{2^{2mq}} \cdot \left(1 - \frac{19q^2}{2^{2m}}\right)\left(1 - \frac{8m^3}{2^{2m}}\right) \\ &\geq \frac{((2^m)_q)^2}{2^{2mq}} \cdot \left(1 - \frac{19q^2}{2^{2m}} - \frac{8m^3}{2^{2m}}\right). \end{aligned}$$

First Step. For any $q \leq 2^{m-1}$, we take an arbitrary paired biset-system $\Lambda_{AB}^{\{\!\{q\}\!\}}$. So

$$\begin{aligned} \boldsymbol{\rho}(\Lambda_{AB}) &\geq \boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}}) \cdot \left(1 - \frac{2q}{2^m}\right) \\ &= \boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}}) \cdot \left(1 - \frac{q}{2^m}\right)^2 \left(1 - \frac{q^2/2^{2m}}{(1 - q/2^m)^2}\right). \end{aligned} \tag{8.3}$$

Let us denote $\zeta(q) = \frac{q^2/2^{2m}}{(1-q/2^m)^2}$. Note that, $\zeta(q)$ is an increasing function and $(1 - \zeta(q))^q \geq 1 - q \cdot \zeta(q)$. Therefore, by multiplying Eqn. (8.3) for $1 \leq q \leq 2m - 1$, we get

$$\begin{aligned} \boldsymbol{\rho}(\Lambda_{AB}^{\{\!\{2m\}\!\}}) &\geq \frac{((2^m)_{2m})^2}{2^{4mn}} \left(1 - \frac{(2m-1)^3/2^{2m}}{(1 - (2m-1)/2^m)^2}\right) \\ &\geq \frac{((2^m)_{2m})^2}{(2^m)^{4m}} \left(1 - \frac{8m^3}{2^{2m}}\right), \end{aligned}$$

where the last inequality holds because $1 - \frac{(2m-1)^3/2^{2m}}{(1-(2m-1)/2^m)^2} \geq 1 - 8m^3/2^{2m}$ for $n \geq 7$.

Second Step. Now, let $2m \leq \alpha \leq 2^m/17$, and let $\Gamma_{AB}^{\{\!\{\alpha+1\}\!\}}$ be a paired biset-system with $\boldsymbol{\gamma}_{\alpha+1,AB} = (\{0^m\}, \{\gamma\})$, such that $\mu_{\Gamma_{AB}}(\gamma) = M(\Gamma_{AB})$. Let $\Gamma'_{AB} = (\Gamma_{AB})_{-\boldsymbol{\gamma}_{\alpha+1,AB}}$. Then

$$\frac{\boldsymbol{\rho}(\Gamma_{AB})}{\boldsymbol{\rho}(\Gamma'_{AB})} \geq \frac{(2^m-\alpha)^2}{2^{2m}}(1-\eta(\alpha)) \tag{8.4}$$

holds, where $\eta(\alpha) := \frac{17\alpha/2^{2m}}{1-\alpha/2^m}$. Note that, $\eta(\alpha)$ is a non-decreasing function, and $(1-\eta(q-1))^q \geq 1-(q-1)\eta(q-1) \geq 1 - q\cdot\eta(q)$. Moreover, for all $q \leq 2^m/17$, we have $17/(1-q/2^m) \leq 19$. Therefore, by multiplying Eqn. (8.4) for all $2m \leq \alpha \leq q-1$, we have Eqn. (8.2).

Let $I_B(\gamma) := \{[\boldsymbol{\gamma}'_{AB}] : \boldsymbol{\gamma}'_{AB} = (\{0^m\}, \{\gamma'\}) \in \Gamma'_{AB} : \gamma \neq \gamma'\}$ be the set of all bisets $\boldsymbol{\gamma}'_{AB}$ for which γ' does not collide with γ. It is easy to see that $|I_B(\gamma)| = \alpha - M(\Gamma_{AB}) + 1$. By applying Lemma 8.3 and Lemma 8.4, we can bound $\boldsymbol{\rho}(\Gamma_{AB})$ from below as follows:

$$\begin{aligned}
\boldsymbol{\rho}(\Gamma_{AB}) &= \boldsymbol{\rho}((\Gamma_{AB})_{-\gamma|\boldsymbol{\gamma}_{\alpha+1,B}}) - \frac{1}{2^m}\sum_{[\boldsymbol{\lambda}'_{AB}]\in I_B(\gamma)} \boldsymbol{\rho}((\Gamma_{AB})_{[\boldsymbol{\lambda}'_{AB}]}) \\
&\overset{(\star)}{\geq} \boldsymbol{\rho}((\Gamma_{AB})_{-\gamma|\boldsymbol{\gamma}_{\alpha+1,B}}) - \frac{1}{2^m}\sum_{[\boldsymbol{\lambda}'_{AB}]\in I_B(\gamma)} \boldsymbol{\rho}((\Gamma_{AB})_{-\gamma|\boldsymbol{\gamma}_{\alpha+1,B}})\left(1+17\frac{M(\Gamma_{AB})}{2^m}\right) \\
&\geq \boldsymbol{\rho}((\Gamma_{AB})_{-\gamma|\boldsymbol{\gamma}_{\alpha+1,B}})\left(1-\frac{\alpha-M(\Gamma_{AB})+1}{2^m}\left(1+\frac{17M(\Gamma_{AB})}{2^m}\right)\right) \\
&\overset{(\star\star)}{\geq} \boldsymbol{\rho}((\Gamma_{AB})_{-\gamma|\boldsymbol{\gamma}_{\alpha+1,B}})\left(1-\frac{\alpha}{2^m}-\frac{17\alpha}{2^{2m}}\right) \\
&\overset{(\star\star\star)}{\geq} \boldsymbol{\rho}(\Gamma'_{AB})\cdot\frac{(2^m-\alpha)^2}{2^{2m}}(1-\eta(\alpha))
\end{aligned}$$

where $(\star)$ follows from the core lemma, Lemma 8.4, $(\star\star)$ follows from the calculation

$$\begin{aligned}
\frac{\alpha-M(\Gamma_{AB})+1}{2^n}\left(1+\frac{17M(\Gamma_{AB})}{2^m}\right) &\leq \frac{\alpha}{2^n}+\frac{17\alpha}{2^{2m}}-\frac{M(\Gamma_{AB})-1}{2^m}\left(1-\frac{17\alpha}{2^m}\right) \\
&\leq \frac{\alpha}{2^n}+\frac{17\alpha}{2^{2m}},
\end{aligned}$$

and $(\star\star)$ follows from Lemma 8.1. □

Thus modulo the proof of the core lemma, Lemma 8.4, we are done.

8.1 PROOF OF THE CORE LEMMA, LEMMA 8.4

For a paired biset-system $\Lambda_{AB}^{\{\!\{q\}\!\}}$, we need compare $\boldsymbol{\rho}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,B}})$ and $\boldsymbol{\rho}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]})$, where $[\boldsymbol{\lambda}'_{AB}] \in I_B(\lambda)$. We define an operation on unistar biset-systems, so that when it

is applied to $(\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]}$ it yields the biset-system $(\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,B}}$. Our operation, denoted as Op, is defined as follows: Let $\Gamma_{AB}^{\{\!\{\alpha\}\!\}}$ be a unistar system and $x \in \boldsymbol{\lambda}_{q,A}, y \in \boldsymbol{\lambda}_{q,B}$, then $\mathrm{Op}(\Gamma_{AB}, x, y) = (\Gamma'_{AB})^{\{\!\{\alpha+1\}\!\}}$, where $\boldsymbol{\gamma}'_{\alpha,AB} := (\{0^m\}, x \oplus y)$, and $\boldsymbol{\gamma}'_{\alpha+1,AB} := (\boldsymbol{\gamma}_{\alpha,A} \setminus \{x\}, \boldsymbol{\gamma}_{\alpha,B} \setminus \{y\})$.

Now we define the D-terms:

D-terms for unistar biset-systems

For a positive integer q, for all $\ell \geq 0$ and $1 \leq \alpha \leq q$, we define

$$D(\alpha, \ell) := \max_{\Gamma_{AB}, x, y} |\boldsymbol{\rho}(\Gamma_{AB}) - \boldsymbol{\rho}(\mathrm{Op}(\Gamma_{AB}, x, y))|$$

where the maximum is taken over all unistar biset-systems $\Gamma_{AB}^{\{\!\{\alpha\}\!\}}$ with a $(\ell+2)$-star, and $x \in \boldsymbol{\lambda}_{\alpha,A}, y \in \boldsymbol{\lambda}_{\alpha,B}$, such that $(\mathrm{Op}(\Gamma_{AB}, x, y))_{-\boldsymbol{\gamma}'_{\alpha+1,AB}} \subseteq (\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}}$.

Next we prove a recursive inequality for D-terms:

Lemma 8.5 (Recursive inequality of D-terms). *For any $\alpha \leq q$ and $\ell \geq 0$,*

$$D(\alpha, \ell) \leq D(\alpha, \ell-1) + \frac{q}{2^m} \cdot D(\alpha-1, \ell+1) + \frac{3M(\Lambda_{AB})}{2^m} \cdot \frac{\boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}})}{(1-2q/2^m)^{q-\alpha}}$$

Proof sketch. We will give the proof sketch for $\ell \equiv 0 \pmod 2$, The other case can be proved using similar arguments. Take the unistar biset-system $\Gamma_{AB}^{\{\!\{\alpha\}\!\}}$ with a $(\ell+2)$-star, and $x \in \boldsymbol{\lambda}_{\alpha,A}, y \in \boldsymbol{\lambda}_{\alpha,B}$, such that $(\mathrm{Op}(\Gamma_{AB}, x, y))_{-\boldsymbol{\gamma}'_{\alpha+1,AB}} \subseteq (\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}}$, and such that $D(\alpha, \ell) = |\boldsymbol{\rho}(\Gamma_{AB}) - \boldsymbol{\rho}(\mathrm{Op}(\Gamma_{AB}, x, y))|$. Let $\Gamma^*_{AB} = \mathrm{Op}(\Gamma_{AB}, x, y)$. We fix any $\gamma \in \boldsymbol{\gamma}_{\alpha,A} \setminus \{x\}$. Then by the alternate link deletion lemma, Lemma 8.3, we have

$$\boldsymbol{\rho}(\Gamma_{AB}) = \boldsymbol{\rho}((\Gamma_{AB})_{-\gamma|\boldsymbol{\gamma}_{q,A}}) - \frac{1}{2^m} \sum_{[\boldsymbol{\gamma}'_{AB}] \in I_A(\gamma)} \boldsymbol{\rho}((\Gamma_{AB})_{[\boldsymbol{\gamma}'_B]})$$

$$\boldsymbol{\rho}(\Gamma^*_{AB}) = \boldsymbol{\rho}((\Gamma^*_{AB})_{-\gamma|\boldsymbol{\gamma}^*_{q,A}}) - \frac{1}{2^m} \sum_{[\boldsymbol{\gamma}'_{AB}] \in I^*_A(\gamma)} \boldsymbol{\rho}((\Gamma^*_{AB})_{[\boldsymbol{\gamma}'_B]})$$

where

$$I_A(\gamma) := \{[\boldsymbol{\gamma}'_{AB}] : \boldsymbol{\gamma}'_{AB} = (\{0^m\}, \{\gamma'\}) \in \Gamma_{AB} \setminus \boldsymbol{\gamma}_{\alpha,AB}, \gamma \oplus \gamma' \notin \boldsymbol{\gamma}_{\alpha,B}\}$$
$$I^*_A(\gamma) := \{[\boldsymbol{\gamma}'_{AB}] : \boldsymbol{\gamma}'_{AB} = (\{0^m\}, \{\gamma'\}) \in \Gamma^*_{AB} \setminus \boldsymbol{\gamma}^*_{AB}[\alpha+1], \gamma \oplus \gamma' \notin \boldsymbol{\gamma}^*_B[\alpha+1]\}$$

Subtracting this and using $|I^*_A(\gamma) \setminus I_A(\gamma)| \leq 3M(\Lambda_{AB})$, we obtain the result. □

Also note that, from Lemma 8.2, we can deduce

$$D(\alpha, \ell) \leq \frac{2\boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}})}{(1-2q/2^m)^{q-\alpha}}$$

Now let $\beta = q/2^m$ and define the double sequence $\{a_{d,\ell}\}_{0\le d\le q, \ell\le 2d-1}$ as:

$$a_{d\ell} := \frac{\beta^d D(\alpha,\ell)}{2\boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}})}$$

Also for $q \le 2^m/17$, we have $(\beta/(1-2\beta))^d \le (1/4e)^d$. Recalling that $q \ge 2m$, we see that the double sequence defined above satisfies all the conditions of Lemma 6.3, and hence we have

$$a_{0,0} \le \frac{8M(\Lambda_{AB})}{2^m}$$

The core lemma statement now follows:

$$\begin{aligned}|\boldsymbol{\rho}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,B}}) - \boldsymbol{\rho}((\Lambda_{AB})_{[\boldsymbol{\lambda}'_{AB}]})| &\overset{(\star)}{\le} \frac{16M(\Lambda_B)\cdot\boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}})}{2^m} \\ &\overset{(\star\star)}{\le} \frac{17M(\Lambda_{AB})}{2^m}\cdot\boldsymbol{\rho}((\Lambda_{AB})_{-\lambda|\boldsymbol{\lambda}_{q,B}})\end{aligned}$$

where $(\star)$ follows from the fact that $D(q,0) = a_{0,0}\cdot 2\boldsymbol{\rho}((\Lambda_{AB})_{-\boldsymbol{\lambda}_{q,AB}})$, and $(\star\star)$ follows from using Lemma 8.1 and noting that $1 - q/2^m \ge 16/17$ for $q/2^m \le 1/17$.

9

BMTP IN TWEAKABLE PERMUTATION SETTING

In this chapter we consider the $\texttt{BMTP}((A, B), \boldsymbol{a}^e, \lambda^e)$ problem, for which the corresponding graph, $\mathscr{G}(\mathscr{E}[\boldsymbol{a}^e, \lambda^e])$ is of a particular structure.

Bipartite Star Graph

A bipartite graph $(A \sqcup B, E)$ is called a *bipartite star graph* if every component of the graph is a star. Thus every component of a graph is of one of the following categories:

- the component consists of an isolated edge
- the component consists of more than one edges all incident at an A-vertex, we call these components *A-stars*.
- the component consists of more than one edges all incident at a B-vertex, we call these components *B-stars*.

A bipartite star graph is parameterized by $(c_1, c_A, c_B, q_A, q_B, \xi_{\max})$, where

- c_1, c_A, c_B are the number of isolated edges, A-stars and B-stars, respectively,
- q_A, q_B are the total number of edges in the A-stars and B-stars
- $\xi_{\max}$ is the size of the largest component.

Remark 9.1. Although the graph $\mathscr{G}$, corresponding to a BMTP problem, is a bipartite graph, $\mathrm{Star}(\mathscr{G})$, which contains only star components (see Chapter 4), may not be bipartite. So even if the above graph structure might look quite general, all BMTP problems cannot be reduced to one, the corresponding graph of which will be a bipartite star graph.

Suppose the graph $\mathscr{G}$ corresponding to a BMTP problem be a bipartite star graph parameterized by $(c_1, c_A, c_B, q_A, q_B, \xi_{\max})$. Since the ordering of the components of the graph does not affect the number of solutions to the corresponding BMTP problem, for the rest of the paper we fix a particular ordering of the components, in which the isolated edges occur first, then the A-stars and then the B-stars. Let the number of vertices and edges in the i-th component be denoted as ξ_i and $\eta_i := \xi_i - 1$, respectively. Here, again the collection of labels of the edges of the i-th component can be viewed as a

multiset $\boldsymbol{\lambda}_i := \{\!\{\lambda_{i,1}, \ldots, \lambda_{i,\eta_i}\}\!\}$. Now the non-equations of the BMTP problem force the following two conditions on the edge-labels of $\mathscr{G}$: label-sum of a path between any two vertices in A (resp. any two vertices in B) is non-zero, i.e., $\lambda_{i,j} \neq \lambda_{i,j'}$ for all $j, j' \in [\eta_i], i \in [c], c := c_1 + c_A + c_B$. This implies $\boldsymbol{\lambda}_i$ is a set for $i \in [c]$. Thus in this case the BMTP problem is instantiated by an ordered tuple of sets $\Lambda^c = (\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_c)$, where $\boldsymbol{\lambda}_i$ is a singleton for $i \in [c_1]$, correspond to the edge-labels of an A-star for $i \in [c_1 + 1, c_1 + c_A]$, and correspond to the edge-labels of an B-star for $i \in [c_1 + c_A + 1, c]$. Also, $\sum_{i=c_1+1}^{c_A} |\boldsymbol{\lambda}_i| = q_A$, $\sum_{i=c_1+c_A+1}^{c} |\boldsymbol{\lambda}_i| = q_B$ and $\max_{i\in[c]} |\boldsymbol{\lambda}_i| + 1 = \xi_{\max}$. We say that such a set-tuple is parameterized by $(c, c_A, c_B, q_A, q_B, \xi_{\max})$.

Reformulation of BMTP with bipartite star graph

NOTATION. The *bipartite homogeneous bivariate Mirror Theory Problem* instantiated by the set-tuple

$$\Lambda^c = (\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_c) :$$

$$\boldsymbol{\lambda}_i = \{\lambda_{i,1}, \ldots, \lambda_{i,\eta_i}\} \quad i \in [c]$$

parameterized by $(c, c_A, c_B, q_A, q_B, \xi_{\max})$,
also denoted as $\texttt{BMTP}(\Lambda^c)$, is to find the number of solutions to the system of equations and non-equations
(EQUATIONS).

$$\begin{aligned}
&\mathsf{X}_{i,1} \oplus \mathsf{Y}_{i,1} = \lambda_{i,1}, \quad i \in [c_1].\\
&\mathsf{X}_{i,1} \oplus \mathsf{Y}_{i,j} = \lambda_{i,j}, \quad j \in [\eta_i], i \in [c_1 + 1, c_A].\\
&\mathsf{X}_{i,j} \oplus \mathsf{Y}_{i,1} = \lambda_{i,j}, \quad j \in [\eta_i], i \in [c_1 + c_A + 1, c].
\end{aligned}$$

(NON-EQUATIONS).

$$\begin{aligned}
&\mathsf{X}_{i,j} \neq \mathsf{X}_{i',j'} \quad \text{for all } (i,j),(i',j') \in \begin{array}{l}([c_1 + c_A] \times \{1\})\\ \cup([c_1 + c_A + 1, c] \times [\eta_i])\end{array}, i \neq i'\\
&\mathsf{Y}_{i,j} \neq \mathsf{Y}_{i',j'} \quad \text{for all } (i,j),(i',j') \in \begin{array}{l}([c_1] \times \{1\}) \cup ([c_1 + 1, c_A] \times [\eta_i])\\ \cup([c_1 + c_A + 1, c] \times \{1\}), \quad i \neq i'\end{array}
\end{aligned}$$

We denote the system of equations and non-equations corresponding to $\texttt{BMTP}(\Lambda^c)$ problem as $\mathscr{EN}[\Lambda^c]$.

Now we define the multiplicity of the equation constants in a way that suits our purpose.

Multiplicity of BMTP constants

Definition 9.1. *For a set-tuple $\Lambda^c = (\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_c)$, and an m-bit number λ, we denote the multiplicity of λ in Λ^c as*

$$\mu_{\Lambda^c}(\lambda) := \#\{i \in [c] : \lambda \in \boldsymbol{\lambda}_i\}$$

Moreover if $\bigcup_{i\in[c]} \boldsymbol{\lambda}_i = \{\lambda_1, \ldots, \lambda_d\}$, then we define

$$\mu_i := \mu_{\Lambda^c}(\lambda_i)$$

to be the frequency of the i-th distinct element in Λ^c. We associate the multiplicity vector $(\mu_1, \ldots, \mu_d)$ with the set-tuple Λ^c.

Equipped with this definitions, we are now going to present the BMTP result for the tweakable permutation setting.

Main result for BMTP in tweakable permutation setting

Theorem 9.1 ([JN20]). *Consider the set-tuple $\Lambda^c = (\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_c)$ parameterized by $(c_1, c_A, c_B, q_A, q_B, \xi_{\max})$, with multiplicity vector $(\mu_1, \ldots, \mu_d)$. Also let $\eta_i := |\boldsymbol{\lambda}_i|$, $i \in [c]$ and $q := c_1 + q_A + q_B$.*
If $q \le 2^m/4$ and $q \cdot \xi_{\max} \le 2^m/2$, then the number of solutions to the $\mathtt{BMTP}(\Lambda^c)$ problem is at least

$$\left(1 - \frac{13q^4}{2^{3m}} - \frac{2q^2}{2^{2m}} - \frac{4q^2}{2^{2m}}\left(\sum_{i=1}^{c_A+c_B} \eta_{c_1+i}^2\right)\right) \times \frac{(2^m)_{c_1+c_A+q_B}\,(2^m)_{c_1+q_A+c_B}}{\prod_{i=1}^{d}(2^m)_{\mu_i}}.$$

Theorem 9.1 has already been proved in [JN20], but for sake of completeness we redo the proof below in our own terminology.

ADDITIONAL NOTATIONS. We introduce some additional notations to facilitate the presentation of the proof. For $i \in [c + c_A + c_B]$:

- $\eta_{<i}$ denotes the number of edges in the first $i-1$ components.
- $\xi_{A,<i}$ denotes the number of A-vertices in the first $i-1$ components.
- $\xi_{B,<i}$ denotes the number of B-vertices in the first $i-1$ components.
- N_i denotes the number of solutions to $\mathtt{BMTP}(\Lambda^i)$, that is the number of solutions to the sub-system of equations and non-equations instantiated by the sub-tuple

$\Lambda^i = (\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_i)$. The graph corresponding to this sub-system consists of the first i components of the graph corresponding to $\texttt{BMTP}(\Lambda^c)$. Note that we want a lower bound for $N_{c_1+c_A+c_B}$.

- $H_i := N_i \cdot \prod_{j=1}^{d_i} (2^m)_{\mu^i_j}$, where $(\mu^i_1, \ldots, \mu^i_{d_i})$ is the multiplicity vector of Λ^i. Note that $H_{c_1+c_A+c_B}/N_{c_1+c_A+c_B}$ is precisely the denominator of the lower bound in Theorem 9.1.
- $J_i := (2^m)_{\xi_{A,<i+1}} \cdot (2^m)_{\xi_{B,<i+1}}$. Note that $J_{c+c_A+c_B}$ is precisely the numerator of the lower bound in Theorem 9.1.
- We denote the system of equations and non-equations, consisting of $\mathscr{EC}[\Lambda^c]$ and an additional equation $\mathsf{X}_{i,j} \oplus \mathsf{Y}_{i',j'} = \lambda$, as $\mathscr{EN}[\Lambda^c]_{+(\mathsf{X}_{i,j} \oplus \mathsf{Y}_{i',j'} = \lambda)}$.
- For $i \in [c_1]$ and $j, k \in [i]$, let $N_i(j, k, \lambda)$ denotes the number of solutions satisfying an additional equation $\mathsf{X}_{j,1} \oplus \mathsf{Y}_{k,1} = \lambda$ along with the system of equations and non-equations of $\texttt{BMTP}(\Lambda^i)$, i.e., $N_i(j, k, \lambda)$ is the number of solutions to $\mathscr{EN}[\Lambda^i]_{+(\mathsf{X}_{j,1} \oplus \mathsf{Y}_{k,1} = \lambda)}$. Note that

$$N_i(j, j, \lambda) = \begin{cases} N_i & \text{if } \lambda = \lambda_{j,1} \\ 0 & \text{otherwise} \end{cases}$$

  That is for $\mu_{\Lambda^i}(\lambda)$ many j's, $N_i(j, j, \lambda) = N_i$. Moreover for $j \neq k$,

  $N_i(j, k, \lambda) = 0$ if $\lambda \in \{\lambda_{j,1}, \lambda_{k,1}\}$.

- For $i \in [c_1]$ and $k \in [i]$, we denote the number of solutions to $\texttt{BMTP}(\Lambda^{[i]\setminus k})$ by $N_{[i]\setminus k}$.
- For $i \in [c_1]$, $k \in [i]$ and $j, \ell \in [i] \setminus \{k\}$, let $N_{[i]\setminus k}(j, \ell, \lambda)$ denote the number of solutions satisfying an additional equation $\mathsf{X}_{j,1} \oplus \mathsf{Y}_{\ell,1} = \lambda$ along with the system of equations and non-equations of $\texttt{BMTP}(\Lambda^{[i]\setminus k})$.

Lemma 9.1 (Isolated edge deletion). *For $i \in [c_1 - 1]$,*

$$N_{i+1} = N_i \cdot (2^m - 2i + \mu_{\Lambda^i}(\lambda_{i+1,1})) + \sum_{(j,k)\in I} N_i(j, k, \lambda_{i+1,1})$$

where $I = I(\lambda_{i+1,1}) := \{(j, k) \in [i]^{2*} : \lambda_{i+1,1} \notin \{\lambda_{j,1}, \lambda_{k,1}\}\}$.

Proof. Let S_i denote the set of all solutions to the system of equations and non-equations corresponding to $\texttt{BMTP}(\Lambda^i)$. We take any $(x^i, y^i) \in S_i$. For any $x \in \{0,1\}^m$, we have $(x^i \| x, y^i \| x \oplus \lambda_{i+1,1}) \in S_{i+1}$ if and only if $x \notin x^{\{i\}} \cup (y^{\{i\}} \oplus \lambda_{i+1,1})$. Thus

$$|S_{i+1}| = |S_i| \cdot \left| \{0,1\}^m \setminus (x^{\{i\}} \cup (y^{\{i\}} \oplus \lambda_{i+1,1})) \right|$$

Now since $(x^i, y^i) \in S_i$, we have $x_j \neq x_k$ and $y_j \neq y_k$ for $j \neq k \in [i]$. Hence $|x^{\{i\}}| = |y^{\{i\}} \oplus \lambda_{i+1,1}| = i$. Now suppose $x_j = y_k \oplus \lambda_{i+1,1}$. Then (x^i, y^i), besides satisfying the system of equations and non-equations corresponding to $\mathtt{BMTP}(\Lambda^i)$, also satisfies the additional equation $\mathsf{X}_j \oplus \mathsf{X}_k = \lambda_{i+1,1}$. Thus

$$|x^{\{i\}} \cap (y^{\{i\}} \oplus \lambda_{i+1,1})| = \sum_{j,k \in [i]} N_i(j, k, \lambda - i + 1, 1) = \mu_{\Lambda^i}(\lambda_{i+1,1}) + \sum_{(j,k) \in I} N_i(j, k, \lambda_{i+1,1})$$

using the properties of $N_i(j, k, \lambda)$. Combining the above arguments, we have our result. □

Remark 9.2. In the above proof, note that there is no special significance to which particular isolated edge is removed. The same argument would imply that for $i \in [c_1]$ and $k \in [i]$,

$$N_i = N_{[i]\setminus k} \cdot (2^m - 2(i-1) + \mu_{\Lambda^i \setminus \boldsymbol{\lambda}_k}(\lambda_{k,1})) + \sum_{(j,\ell) \in I} N_{[i]\setminus k}(j, \ell, \lambda_{k,1})$$

where $I = I(\lambda_{k,1}) := \{(j, \ell) \in ([i] \setminus k)^{2*} : \lambda_{k,1} \notin \{\lambda_{j,1}, \lambda_{\ell,1}\}\}$. As a consequence, we have the following corollary.

Corollary 9.1.1. *For $i \in [c_1]$ and $k \in [i]$,*

$$(2^m - 2(i-1))N_{[i]\setminus k} \leq N_i \leq (2^m - (i-1))N_{[i]\setminus k}.$$

Next we lower bound the $N_i(j, k, \lambda)$-term.

Lemma 9.2. *For all $\lambda \in \{0,1\}^m$ and $(j, k) \in I(\lambda)$,*

$$N_i(j, k, \lambda) \geq \frac{N_i}{2^m - i + 1} \cdot \left(1 - \frac{2(i-2)}{2^m - 2(i-2)}\right).$$

Proof. Suppose $(x^{[i]\setminus k}, y^{[i]\setminus k})$ satisfies $\mathscr{EN}[\Lambda^{[i]\setminus k}]$. Then $(x'^{[i]}, y'^{[i]})$, with $(x'^{[i]\setminus k}, y'^{[i]\setminus k}) = (x^{[i]\setminus k}, y^{[i]\setminus k})$ and $x'_k = x_j \oplus \lambda \oplus \lambda_{k,1}$ and $y'_k = x_j \oplus \lambda$, will not satisfy $\mathscr{EN}[\Lambda^i]_{+(\mathsf{X}_{j,1} \oplus \mathsf{Y}_{k,1} = \lambda)}$, if and only if, for some $\ell \in [i] \setminus \{j, k\}$, either $x'_k = x_\ell$ or $y'_k = y_\ell$, or in other words if

$$x_j \oplus y_\ell = \lambda \oplus \lambda_{k,1} \oplus \lambda_{\ell,1} \text{ or } x_j \oplus y_\ell = \lambda.$$

In the first case $(x^{[i]\setminus k}, y^{[i]\setminus k})$ satisfies $\mathscr{EN}[\Lambda^{[i]\setminus k}]_{+(\mathsf{X}_{j,1} \oplus \mathsf{Y}_{\ell,1} = \lambda \oplus \lambda_{k,1} \oplus \lambda_{\ell,1})}$, and in the second case it satisfies $\mathscr{EN}[\Lambda^{[i]\setminus k}]_{+(\mathsf{X}_{j,1} \oplus \mathsf{Y}_{\ell,1} = \lambda)}$.

Consider the system of equations $\mathscr{EN}[\Lambda^{[i]\setminus k}]_{+(\mathsf{X}_{j,1} \oplus \mathsf{Y}_{\ell,1} = \lambda)}$. If we fix $\mathsf{X}_{j,1} = x_j$, then the variables $\mathsf{Y}_{j,1}, \mathsf{Y}_{\ell,1}$ and $\mathsf{X}_{\ell,1}$ will get determined. Thus the number of solutions satisfying $\mathscr{EN}[\Lambda^{[i]\setminus k}]_{+(\mathsf{X}_{j,1} \oplus \mathsf{Y}_{\ell,1} = \lambda)}$ is at most the number of solutions satisfying $\mathscr{EN}[\Lambda^{[i]\setminus\{k,\ell\}}]$, i. e., we have $N_{[i]\setminus k}(j, \ell, \lambda) \leq N_{[i]\setminus\{k,\ell\}}$. Similarly, $N_{[i]\setminus k}(j, \ell, \lambda \oplus \lambda_{k,1} \oplus \lambda_{\ell,1}) \leq N_{[i]\setminus\{k,\ell\}}$.

Thus, combining, we have

$$\begin{aligned}
N_i(j,k,\lambda) &\geq N_{[i]\setminus k} - \sum_{\ell\in[i]\setminus\{j,k\}} N_{[i]\setminus k}(j,\ell,\lambda) - \sum_{\ell''\in[i]\setminus\{j,k\}} N_{[i]\setminus k}(j,\ell',\lambda\oplus\lambda_{k,1}\oplus\lambda_{\ell',1}) \\
&\geq N_{[i]\setminus k} - \sum_{\ell\in[i]\setminus\{j,k\}} N_{[i]\setminus\{k,\ell\}} - \sum_{\ell'\in[i]\setminus\{j,k\}} N_{[i]\setminus\{k,\ell'\}} \\
&\geq N_{[i]\setminus k} - (i-2)N_{[i]\setminus\{k,\ell\}} - (i-2)N_{[i]\setminus\{k,\ell'\}} \\
&\overset{(\star)}{\geq} N_{[i]\setminus k}\cdot\left(1-\frac{2(i-2)}{2^m-2(i-2)}\right) \\
&\overset{(\star\star)}{\geq} \frac{N_i}{2^m-i+1}\cdot\left(1-\frac{2(i-2)}{2^m-2(i-2)}\right)
\end{aligned}$$

where $(\star)$ and $(\star\star)$ follows from Cor. 9.1.1. □

Lemma 9.3 (A-star deletion). *For $i \in [c_A]$ and $i' := c_1 + i$, we have*

$$N_{i'} \geq \left(2^m - \xi_{A,<i'} - \eta_{i'}\xi_{B,<i'} + \sum_{j=1}^{\eta_{i'}} \mu_{\Lambda^{i'-1}}(\lambda_{i',j})\right)\cdot N_{i'-1}.$$

Proof. Let $S_{i'}$ and $S_{i'-1}$ be the sets of solutions of $\texttt{BMTP}(\Lambda^{i'})$ and $\texttt{BMTP}(\Lambda^{i'-1})$, respectively. For any $x \in \{0,1\}^n$, let $y^{\eta_{i'}} := (x\oplus\lambda_{i',1},\ldots,x\oplus\lambda_{i',\eta_{i'}})$. If $(x^{\xi_{A,<i'}}, y^{\xi_{B,<i'}}) \in S_{i'-1}$, then $(x^{\xi_{A,<i'}}\|x, y^{\xi_{B,<i'}}\|y^{\eta_{i'}}) \notin S_{i'}$, if and only if, either $x \in x^{\{\xi_{A,<i'}\}}$ or $y^{\{\xi_{B,<i'}\}} \cap y^{\{\eta_{i'}\}} \neq \emptyset$. Thus

$$|S_{i'}| = |S_{i'-1}|\cdot\left|\{0,1\}^m \setminus \left(x^{\{\xi_{A,<i'}\}} \cup \bigcup_{j=1}^{\eta_{i'}} (y^{\{\xi_{B,<i'}\}}\oplus\lambda_{i',j})\right)\right|$$

Now noting that

- $|x^{\{\xi_{A,<i'}\}}| = \xi_{A,<i'}$
- $\left|\bigcup_{j=1}^{\eta_{i'}}(y^{\{\xi_{B,<i'}\}}\oplus\lambda_{i',j})\right| \leq \eta_{i'}\xi_{B,<i'}$
- $\left|x^{\{\xi_{A,<i'}\}} \cap \bigcup_{j=1}^{\eta_{i'}}(y^{\{\xi_{B,<i'}\}}\oplus\lambda_{i',j})\right| \geq \sum_{j=1}^{\eta_{i'}}\mu_{\Lambda^{i'-1}}(\lambda_{i',j})$, since for each $j\in[\eta_{i'}]$ there exists $\mu_{\Lambda^{i'-1}}(\lambda_{i',j})$ equations in $\mathscr{EM}[\Lambda^{i'-1}]$ with constant $\lambda_{i',j}$.

we have our result. □

Similar arguments yield

Lemma 9.4 (B-star deletion). *For $i \in [c_B]$ and $i' := c_1 + c_A + i$, we have*

$$N_{i'} \geq \left(2^m - \xi_{B,<i'} - \eta_{i'}\xi_{A,<i'} + \sum_{j=1}^{\eta_{i'}} \mu_{\Lambda^{i'-1}}(\lambda_{i',j})\right) \cdot N_{i'-1}.$$

Now we prove a lower bound on the ratio of the H and J-terms. Theorem 9.1 directly follows from this and the definition of the H and J-terms.

Lemma 9.5 (Ratio of H and J-terms). *For $q \leq 2^m/4$ and $q \cdot \xi_{\max} \leq 2^m/2$, we have*

$$\frac{H_{c_1+c_A+c_B}}{J_{c_1+c_A+c_B}} \geq 1 - \frac{13q^4}{2^{3m}} - \frac{2q^2}{2^{2m}} - \frac{4q^2}{2^{2m}}\left(\sum_{i=c_1+1}^{c} \eta_i^2\right)$$

Proof. We prove this in two steps:

STEP 1. We show that, for $i \in [c_1 - 1]$,

$$\frac{H_{i+1}}{J_{i+1}} \geq 1 - \frac{13i^3}{2^{3m}} - \frac{2i}{2^{2m}} \tag{9.1}$$

STEP 2. Next we show that for $i' \in [c_1 + 1, c]$,

$$\frac{H_{i'}}{J_{i'}} \geq \left(1 - \frac{4q^2\eta_{i'}^2}{2^{2m}}\right) \cdot \frac{H_{i'-1}}{J_{i'-1}} \tag{9.2}$$

Now Lemma 9.5 follows by multiplying Eq. (9.1) for all $i \in [c_1 - 1]$ and Eq. (9.2) for all $i' \in [c_1 + 1, c]$, and noting that $H_1 = J_1 = 2^{2m}$.

PROOF OF EQ. (9.1). From Lemma 9.1 and Lemma 9.2, we have that for $i \in [c_1 - 1]$,

$$N_{i+1} \geq N_i \cdot \left(2^m - 2i + \mu_{\Lambda^i}(\lambda_{i+1,1}) + \frac{|I(\lambda_{i+1,1})|}{2^m - i + 1}\left(1 - \frac{2(i-2)}{2^m - 2(i-2)}\right)\right)$$

Recalling that $I(\Lambda_{i+1,1}) = \{(j,k) \in [i]^{2*} : \lambda_{i+1,1} \notin \{\lambda_{j,1}, \lambda_{k,1}\}\}$, we have $|I(\lambda_{i+1,1})| = (i - \mu_{\Lambda^i}(\lambda_{i+1,1}))(i - \mu_{\Lambda^i}(\lambda_{i+1,1}) - 1)$.

In the following equations we abbreviate $\mu_{\Lambda^i}(\lambda_{i+1,1})$ as μ, for the sake of presentation. Now, for $i \in [c_1 - 1]$, we have

$$\frac{H_{i+1}}{J_{i+1}} \geq \frac{(2^m - \mu) \cdot \frac{N_{i+1}}{N_i}}{(2^m - i)^2} \cdot \frac{H_i}{J_i}$$

$$
\begin{aligned}
&\geq \frac{(2^m-\mu)\left(2^m-2i+\mu+\frac{(i-\mu)(i-\mu-1)}{2^m-i+1}\left(1-\frac{2(i-2)}{2^m-2(i-2)}\right)\right)}{(2^m-i)^2}\cdot\frac{H_i}{J_i}\\
&\overset{(\star)}{\geq} \frac{(2^m-\mu)(2^m-2i+\mu)\frac{(2^m-\mu)(i-\mu)(i-\mu-1)}{2^m-i+1}-\frac{16i^3}{3\cdot 2^m}}{(2^m-i)^2}\cdot\frac{H_i}{J_i}\\
&\overset{(\star\star)}{\geq} \left(1-\frac{(i-\mu)+\frac{(i-\mu)^2\mu}{2^m}-\frac{(i-\mu)\mu}{2^m}+\frac{16i^3}{3\cdot 2^m}}{(2^m-i)^2}\right)\cdot\frac{H_i}{J_i}\\
&\overset{(\star\star\star)}{\geq} \left(1-\frac{13i^3}{2^{3m}}-\frac{2i}{2^{2m}}\right)\cdot\frac{H_i}{J_i}
\end{aligned}
$$

For $(\star)$, we have used that $i \leq c_1 \leq q \leq 2^m/2$, $(i-2), (i-\mu) < i$ and $(2^m-\mu), (2^m-i+1) < 2^m$. $(\star\star)$ is obtained just by simplifying $(\star)$. For $(\star\star\star)$ we have used that $(i-\mu), \mu \leq i$ and $(2^m-i)^2 \leq 2^{2n}$.

PROOF OF EQ. (9.2). We prove Eq. (9.2) only for $i' = c_1 + i$ for $i \in [c_A]$. The same arguments hold for $i' \in [c_1 + c_A + 1, c]$, and hence the proof for those i' is omitted.

From Lemma 9.3 we have

$$
\frac{N_{i'}}{N_{i'-1}} \geq 2^m - \xi_{A,<i'} - \eta_{i'}\xi_{B,<i'} + \sum_{j=1}^{\eta_{i'}} \mu_{\Lambda^{i'-1}}(\lambda_{i',j})
$$

In the following calculations we abbreviate $\mu_{\Lambda^{i'-1}}(\lambda_{i',j})$ as μ'_j for $j \in [\eta_{i'}]$. Then we have

$$
\begin{aligned}
\frac{H_{i'}}{J_{i'}} &\geq \frac{\prod_{j=1}^{\eta_{i'}}(2^m-\mu'_j)\cdot\frac{N_{i'}}{N_{i'-1}}}{\left(2^m-\xi_{A,<i'}\right)\left(2^m-\xi_{B,<i'}\right)_{\eta_{i'}}}\cdot\frac{H_{i'-1}}{J_{i'-1}}\\
&\geq \frac{\overbrace{\prod_{j=1}^{\eta_{i'}}(2^m-\mu'_j)\cdot\left(2^m-\xi_{A,<i'}-\eta_{i'}\xi_{B,<i'}+\sum_{k=1}^{\eta_{i'}}\mu'_k\right)}^{A}}{\underbrace{\left(2^m-\xi_{A,<i'}\right)\left(2^m-\xi_{B,<i'}\right)_{\eta_{i'}}}_{B}}\cdot\frac{H_{i'-1}}{J_{i'-1}}
\end{aligned}
$$

We bound the two terms A and B as follows:

$$
\begin{aligned}
A &= \prod_{j=1}^{\eta_{i'}}(2^m-\mu'_j)\cdot\left(2^m-\xi_{A,<i'}-\eta_{i'}\xi_{B,<i'}+\sum_{k=1}^{\eta_{i'}}\mu'_k\right)\\
&\geq \left(2^{m\eta_{i'}}-\sum_{j=1}^{\eta_{i'}}\mu'_j 2^{m(\eta_{i'}-1)}\right)\cdot\left(2^m-\xi_{A,<i'}-\eta_{i'}\xi_{B,<i'}+\sum_{k=1}^{\eta_{i'}}\mu'_k\right)
\end{aligned}
$$

$$\geq 2^{m(\eta_{i'}+1)} - \xi_{A,<i'}2^{m\eta_{i'}} - \eta_{i'}\xi_{B,<i'}2^{m\eta_{i'}} - \left(\sum_{j=1}^{\eta_{i'}} \mu'_j\right)^2 2^{m(\eta_{i'}-1)}$$

Since $\xi_{A,<i'}, \xi_{B,<i'} + \eta_{i'} < q$, and $\xi_{\max} q < 2^m/2$, we have $B \geq 2^{m(\eta_{i'}+1)-1}$. Also

$$\begin{aligned}
B &= (2^m - \xi_{A,<i'})\,(2^m - \xi_{B,<i'})_{\eta_{i'}} \\
&\leq (2^m - \xi_{A,<i'})(2^m - \xi_{B,<i'})^{\eta_{i'}} \\
&\leq (2^m - \xi_{A,<i'})\left(2^{m\eta_{i'}} - \eta_{i'}\xi_{B,<i'}2^{m(\eta_{i'}-1)} + \eta_{i'}^2\xi_{B,<i'}^2 w^{m(\eta_{i'}-2)}\right) \\
&\leq 2^{m(\eta_{i'}+1)} - \eta_{i'}\xi_{B,<i'}2^{m\eta_{i'}} + \eta_{i'}^2\xi_{B,<i'}^2 2^{m(\eta_{i'}-1)} - \xi_{A,<i'}2^{m\eta_{i'}} + \eta_{i'}\xi_{A,<i'}\xi_{B,<i'}2^{m(\eta_{i'}-1)}
\end{aligned}$$

Combining the bounds,

$$\begin{aligned}
\frac{A}{B} &= 1 - \frac{B-A}{B} \\
&\geq 1 - \frac{\eta_{i'}^2\xi_{B,<i'}^2 2^{m(\eta_{i'}-1)} + \eta_{i'}\xi_{A,<i'}\xi_{B,<i'}2^{m(\eta_{i'}-1)} + \left(\sum_{j=1}^{\eta_{i'}} \mu'_j\right)^2 2^{m(\eta_{i'}-1)}}{2^{m(\eta_{i'}+1)-1}} \\
&\overset{(\star)}{\geq} 1 - \frac{\eta_{i'}^2 q^2 2^{m(\eta_{i'}-1)} + \eta_{i'} q^2 2^{m(\eta_{i'}-1)} + q^2 2^{m(\eta_{i'}-1)}}{2^{m(\eta_{i'}+1)-1}} \\
&\overset{(\star\star)}{\geq} 1 - \frac{4\eta_{i'}^2 q^2}{2^{2m}}
\end{aligned}$$

$(\star)$ follows from the fact that $\xi_{A,<i'}, \xi_{B,<i'}, \sum_{j=1}^{\eta_{i'}} \mu'_j \leq q$. $(\star\star)$ follows from the fact that $\eta_{i'}^2 > \eta_{i'} + 1$ as $\eta_{i'} > 2$. □

10

PRELIMINARIES FOR THE RMTP PROBLEM

NOTATIONS. Recall that the $\texttt{RMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$ problem is parameterized by an acyclic augmented matrix

$$\mathbf{A}|\boldsymbol{\lambda} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_c & \boldsymbol{\lambda}_c \end{pmatrix} \in \mathbb{F}_2^{e \times (v+1)}.$$

with $\overline{\mathbf{A}}_i \in \mathbb{F}_2^{e_i \times v_i}, \boldsymbol{\lambda}_i \in (\mathbb{F}_2^m)^{e_i \times 1}; \sum_i e_i = e, \sum_i v_i = v$. Let us denote by $e_{\leq i} := \sum_{j=1}^{i} e_j$ and $v_{\leq i} := \sum_{j=1}^{i} v_j$ the number of equations and variables involved in the first i components, respectively. Let us denote the system of equations corresponding to the i-th component as

$$\mathscr{E}_i : \overline{\mathbf{A}}_i \mathsf{X}^{[e_{\leq i-1}+1, e_{\leq i}]} = \boldsymbol{\lambda}_i$$

Denoting the first i components as the submatrix

$$\mathbf{A}_{\leq i}|\boldsymbol{\lambda}_{\leq i} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_i & \boldsymbol{\lambda}_i \end{pmatrix} \in \mathbb{F}_2^{e_{\leq i} \times (v_{\leq i}+1)}.$$

we can express the system of equations corresponding to the first i components as

$$\mathscr{E}_{\leq i} : \overline{\mathbf{A}}_{\leq i} \mathsf{X}^{[e_{\leq i}]} = \boldsymbol{\lambda}_{\leq i}$$

Consider a solution $\mathbf{x}^v = (x_1, \ldots, x_v)$ to the $\texttt{RMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$, then $\mathbf{x}^{v_{\leq i}} = (x_1, \ldots, x_{v_{\leq i}})$ is a solution to $\texttt{RMTP}(\mathbf{A}_{\leq i}, \boldsymbol{\lambda}_{\leq i}, \simeq, \mathscr{R})$, where by a slight abuse of notation, the relation $\simeq$ is actually the restriction of the equivalence relation $\simeq$ on $[v]$ to its subset $[v_{\leq i}]$. We use the shorthand $\mathbf{x}_{\leq i}$ to denote the vector $\mathbf{x}^{v_{\leq i}}$. Now given the partial solution $\mathbf{x}_{\leq i}$ to $\texttt{RMTP}(\mathbf{A}_{\leq i}, \boldsymbol{\lambda}_{\leq i}, \simeq, \mathscr{R})$, let us define two new families of sets $\mathscr{P}(\mathbf{x}_{\leq i}) := \{P_j(\mathbf{x}_{\leq i})\}_{j \in [k]}$ and $\mathscr{F}_{\leq i} := \mathscr{F}(\mathbf{x}_{\leq i}) := \{F_j(\mathbf{x}_{\leq i})\}_{j \in [k]}$, where k is the number of equivalence classes of $\simeq$:

$$P_j(\mathbf{x}_{\leq i}) := \{x_{j'} \in \mathbf{x}_{\leq i} : j' \in P_j\}, \quad F_{\leq i-1}^{[j]} := F_j(\mathbf{x}_{\leq i}) = R_j \sqcup P_j(\mathbf{x}_{\leq i}) \tag{10.1}$$

Let $r^j_{\leq i} := |P_j(\mathbf{x}_{\leq i})|$, $r_j := |R_j|$ for $j \in [k]$, which implies $|F_j(\mathbf{x}_{\leq i})| = r_j + r^{(j)}_{\leq i} =: f^{(j)}_{\leq i}$. We assume the convention that $\mathbf{x}_{\leq 0}$ is the empty vector, implying $P_j(\mathbf{x}_{\leq 0}) = \emptyset$ and $F_j(\mathbf{x}_{\leq 0}) = R_j$.

If a component $\mathbf{A}_i|\boldsymbol{\lambda}_i$ contains just one row, we call the component is *isolated*, otherwise it is called *non-isolated*. We analyze the isolated and non-isolated components separately. For that purpose, we assume that all the isolated components appear before the non-isolated ones in the CF representation of $\mathbf{A}|\boldsymbol{\lambda}$. In particular we denote by i^* the largest index of an isolated component.

We denote the maximal multiplicity among the equations constants as

$$\Delta_{\boldsymbol{\lambda}_i} := \max_{\lambda} |\{j \in |\boldsymbol{\lambda}_i| : \lambda_{i,j} = \lambda\}|, \quad \Delta_{\boldsymbol{\lambda}} := \max_{\boldsymbol{\lambda}_i \in \boldsymbol{\lambda}} \Delta_{\boldsymbol{\lambda}_i}$$

EXPECTED NUMBER OF SOLUTIONS. Under the assumption that $\boldsymbol{\lambda}$ is chosen uniformly at random, one would expect that the number of solutions to $\texttt{RMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$ will be approximately

$$\mathbb{E}\left(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R}\right) := 2^{-me} \cdot \prod_{i=1}^{k} \left(2^m - |R_i|\right)_{|P_i|}$$

We want to show that the class of RMTP problems we consider the actual number of solutions is very close to this value, $\mathbb{E}\left(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R}\right)$.

10.1 CERTAIN LINEAR ALGEBRA RESULTS

In this section we state certain results that establish the acyclic and regularity assumptions on our coefficient matrix in linear algebraic grounds, that is in terms of its rank and weight.

Weight of a matrix

Definition 10.1. *The* weight *of any* $\mathbf{A} \in \mathbb{F}_2^{e \times v}$ *is defined as*

$$\mathrm{wt}(\mathbf{A}) := \min\{\mathrm{wt}(\boldsymbol{a}) : \boldsymbol{a} \in \mathrm{rowsp}^+(\mathbf{A})\}$$

where $\mathrm{rowsp}^+(\mathbf{A}) := \{a_1\mathbf{A}_1. \oplus \cdots \oplus a_e\mathbf{A}_e. : (a_1, \ldots, a_e) \in \mathbb{F}_2^e \setminus \mathbf{0}\}$, $\mathbf{A}_i.$ *denoting the* i*-th row of* $\mathbf{A}$.

The following fact relates the weight of a matrix and its components with its row rank.

Proposition 10.1. *Suppose* $\mathbf{A} \in \mathbb{F}_2^{e \times v}$ *with weight* $\mathrm{wt}(\mathbf{A}) \geq w > 0$. *Then,*

1. $\mathbf{A}$ *has full row rank.*

2. *For every* $v' \geq v - w + 1$ *and* $1 \leq i_1 < \cdots < i_{v'} \leq v$, *the matrix* $\mathbf{A}' = (\mathbf{A}_{\cdot i_1} | \ldots | \mathbf{A}_{\cdot i_{v'}})$ *has full row rank, where* $\mathbf{A}_{\cdot i}$ *denotes the* i*-th column of* $\mathbf{A}$.

3. $v - w + 1 \geq e$.

Proof. 1 follows from the definition. For 2, suppose to the contrary that $\mathbf{A}'$ does not have full rank, i.e., there exists $(a_1, \ldots, a_e) \in \mathbb{F}_2^e \setminus \mathbf{0}$ such that $a_1 \mathbf{A}'_{1\cdot} \oplus \cdots \oplus a_e \mathbf{A}'_{e\cdot} = \mathbf{0}$. Then the vector $\boldsymbol{a} = a_1 \mathbf{A}_{1\cdot} \oplus \cdots \oplus a_e \mathbf{A}_{e\cdot} \in \mathrm{rowsp}^+(\mathbf{A})$ has weight $\mathrm{wt}(\boldsymbol{a}) \leq v - v' \leq w - 1$, which implies $\mathrm{wt}(\mathbf{A}) < w$, and we have arrived at a contradiction. Finally, 3 follows from 2. □

The following results provide an easy-to-check condition for determining the weight of a matrix.

Proposition 10.2. *For any* $w \geq 2$, *any* w*-regular and acyclic* $\mathbf{A} \in \mathbb{F}_2^{e \times v}$ *has* $\mathrm{wt}(\mathbf{A}) = w$.

Proof. The result trivially holds for a $1 \times v$ matrix. Suppose the result holds for any $(e-1) \times v$ acyclic matrix. Then we show that the result also holds for a $e \times v$ acyclic matrix $\mathbf{A}$. Since $\mathbf{A}$ is acyclic, any row, say $\mathbf{A}_{e\cdot}$, shares at most one non-zero column index with any other row[1]. Consider the matrix $\mathbf{A}'$, that is obtained from $\mathbf{A}$ by deleting the row $\mathbf{A}_{e\cdot}$. Since $\mathbf{A}'$ will also be acyclic and w-regular by induction hypothesis we have that $\mathrm{wt}(\mathbf{A}') = w$. Now assume to the contrary that $\mathrm{wt}(\mathbf{A}) < w$. Then by Proposition 10.1 there exists a $e \times (v - w + 1)$ submatrix of $\mathbf{A}$, say $\mathbf{A}''$, that does not have full row rank, i.e., there exists an non-zero vector $(a_1, \ldots, a_e) \in \mathbb{F}_2^e$ such that $\boldsymbol{a} = a_1 \mathbf{A}''_{1\cdot} \oplus \cdots \oplus a_e \mathbf{A}''_{e\cdot} = \mathbf{0}$. If $a_e = 0$, then we have $\mathbf{A}'''$, obtained from $\mathbf{A}''$ by removing the e-th row, $\mathbf{A}''_{e\cdot}$, is a $(e-1) \times (v - w + 1)$ submatrix of $\mathbf{A}'$ that does not have full row rank, which contradicts the fact that $\mathrm{wt}(\mathbf{A}') = w$. So suppose $a_e \neq 0$. If $\mathbf{A}''$ has a column, that has only one non-zero entry, and that entry is in the e-th row then it contradicts the fact that $\boldsymbol{a} = 0$. Otherwise, suppose that the column with non-zero entry at the e-th row, also has another non-zero entry at, say the j-th row (there can be exactly one such $j \neq e$). Then again $a_j = 0$, would contradict the fact that $\boldsymbol{a} = 0$. So in this case we must have $a_j \neq 0$. Note that, by choice of $\mathbf{A}_{e\cdot}$, every other column in $\mathbf{A}''$ has a zero entry in their e-th row. Let $\mathbf{A}^{(4)}$ be the matrix obtained from $\mathbf{A}''$ by removing the said column, and the e-th row. Then again $\mathbf{A}^{(4)}$ constitutes a $(e-1) \times (v - w)$ submatrix of $\mathbf{A}'$ that does not have full row rank, contradicting the fact that $\mathrm{wt}(\mathbf{A}') = w$. □

Proposition 10.3. *For any* $e \geq 2$ *and any* $w \geq 3$, *let* $\mathbf{A} \in \mathbb{F}_2^{e \times v}$ *be acyclic and* w*-regular. Then for any* $e \times (v - w)$ *submatrix,* $\mathbf{A}'$, *of* $\mathbf{A}$, *we have*

$$\mathrm{rank}(\mathbf{A}') = \begin{cases} e - 1, & \text{if } \exists^* j \in [e] : \mathbf{A}'_{j\cdot} = \mathbf{0} \\ e, & \text{otherwise} \end{cases}$$

1 This is because if every vertex of a graph has degree at least two, then the graph has a cycle.

Proof. Let us consider the case when $\mathbf{A}'_{j\cdot} = \mathbf{0}$. Let $\mathbf{A}''$ be the matrix obtained from $\mathbf{A}'$ by removing the j-th row, then $\mathrm{rank}(\mathbf{A}') = \mathrm{rank}(\mathbf{A}'') \leq e-1$. Also $\mathbf{A}'_{j\cdot} = \mathbf{0}$ implies that $\mathbf{A}_{j\cdot}$ have non-zero entries only at column indices not included in $\mathbf{A}'$. Also any other row can share at most one non-zero column index with $\mathbf{A}_{j\cdot}$. Hence $\mathbf{A}''$ is also acyclic and at least $(w-1)$-regular. Thus by Proposition 10.2 we have $\mathrm{wt}(\mathbf{A}'') \geq w-1$, which by Proposition 10.1 implies $\mathrm{rank}(\mathbf{A}') = \mathrm{rank}(\mathbf{A}'') \geq e-1$, which proves the first part.

In the other case every row of $\mathbf{A}'$ is non-zero. Assume to the contrary that $\mathrm{rank}(\mathbf{A}') < e$. Then there exists $(a_1, \ldots, a_e) \in \mathbb{F}_2^e$ such that $\boldsymbol{a} = a_1\mathbf{A}'_{1\cdot} \oplus \cdots \oplus a_e\mathbf{A}'_{e\cdot} = \mathbf{0}$. Let $\mathbf{A}''$ be the matrix consisting of those rows of $\mathbf{A}$, $\mathbf{A}_{j\cdot}$, such that $a_j \neq 0$. Take a longest path in $\mathbf{A}''$, i. e., choose distinct row indices, $j_1, j_2, \ldots, j_\ell$ such that $\mathbf{A}''_{j_1\cdot} \sim \mathbf{A}''_{j_2\cdot} \sim \cdots \sim \mathbf{A}''_{j_\ell\cdot}$, and no other row is adjacent to either $\mathbf{A}''_{j_1\cdot}$ or $\mathbf{A}''_{j_1\cdot}$. Such a longest path will exist because $\mathbf{A}$ is acyclic. Moreover, since $\mathbf{A}$ is w-regular there will be $w-1$ columns, such that the only non-zero entry in those columns occur at row index j_1 and there will be $w-1$ more columns such that the only non-zero entry in those columns occur at row index j_ℓ (since the first and last row in the path each have degree 1). Thus even if we remove w rows from $\mathbf{A}''$, we will still be left with $w-2 \geq 1$ columns that have exactly one non-zero entry. However this implies $\boldsymbol{a} \neq \mathbf{0}$, contradicting our previous assumption. □

10.2 SUM-CAPTURE LEMMA

For some $w \geq 2$, let $\alpha \in \mathbb{F}_2^w$, and $\mathscr{A}, \mathscr{B}_1, \ldots, \mathscr{B}_w \subseteq \mathbb{F}_2^m$, define

$$\mu_\alpha(\mathscr{A}, \{\mathscr{B}_1, \ldots, \mathscr{B}_w\}) := \left\{ \mathbf{b} = (b_1, \ldots, b_w) \in \mathscr{B}_1 \times \cdots \times \mathscr{B}_w : \bigoplus_{i=1}^{w} \alpha_i \cdot b_i \in \mathscr{A} \right\}$$

In addition, for any $p \geq 0$, we define

$$\mu_\alpha^k(\mathscr{A}, p) := \max_{\substack{\mathscr{B}_1, \ldots, \mathscr{B}_k \subseteq \mathbb{F}_2^m \\ |\mathscr{B}_i| \leq p}} \left| \left\{ \mathbf{b} = (b_1, \ldots, b_k) \in \mathscr{B}_1 \times \cdots \times \mathscr{B}_k : \bigoplus_{i=1}^{k} \alpha_i \cdot b_i \in \mathscr{A} \right\} \right|,$$

The following lemma is from [Jha24]. A similar result is also shown in [TZ21].

Lemma 10.1. *Let G be a finite abelian group, and let $0 \leq q \leq N/2$. For all but an $O(N^{-1})$ fraction of subsets $\mathscr{A} \subseteq G$ such that $|\mathscr{A}| = q$ and any non-zero $\alpha \in (\mathbb{F}_2^m)^k$, we have*

$$\mu_\alpha^k(\mathscr{A}, p) \leq \left(\frac{qp^{\mathrm{wt}(\alpha)}}{N} + 4p^{\mathrm{wt}(\alpha)-1}\sqrt{\ln(N)q} \right),$$

For $\alpha = (1, 1, \ldots, 1)$, we use the shorthand $\mu(\mathscr{A}, \mathscr{B})$ for $\mu_\alpha(\mathscr{A}, \mathscr{B})$.

11 REGULAR PARTITE RMTP

In this section, we are going to prove the following lower bound to the number of solutions to $\texttt{RPRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$ problem:

Main result for regular partite RMTP

Theorem 11.1. *Let $w \geq 2$ and $w(q+r) \leq 2^m/2$. Then the RMTP problem, instantiated by*

- *an acyclic w-regular $\mathbf{A}$ with component form*

$$\mathbf{A}|\boldsymbol{\lambda} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_c & \boldsymbol{\lambda}_c \end{pmatrix} \in \mathbb{F}_2^{q \times (v+1)}.$$

  with $\overline{\mathbf{A}}_i \in \mathbb{F}_2^{q_i \times v_i}, \boldsymbol{\lambda}_i \in (\mathbb{F}_2^m)^{q_i \times 1}; \sum_i q_i = q, \sum_i v_i = v$.

- *An equivalence relation $\simeq$ over $[v]$ that induces a partition $(P_1, \ldots, P_w)$ of $[v]$, with respect to which $\mathbf{A}$ is partite.*

- *family of restricted sets $\mathscr{R} = \{R_j\}_{j \in [w]}$, with $|R_j| \leq r$ for all $j \in [w]$.*

has number of solutions $N(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R}) \geq (1-\epsilon) \cdot \mathbb{E}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$, where

$$\epsilon \leq \frac{2\mu(\boldsymbol{\lambda}, \mathscr{R})}{2^{m(w-1)}} + \frac{2q\Delta_{\boldsymbol{\lambda}}}{2^{m(w-1)}} + \frac{6q(q+r)^w}{2^{mw}} + \sum_{i=i^*+1}^{c} \left(\frac{2v_i^w (q+r)^w}{2^{mw}} + \frac{q_i (q+r)^{w-1}}{2^{(w-1)}} \right)$$

Observe that

$$N(\mathbf{A}_{\leq i}, \boldsymbol{\lambda}_{\leq i}, \simeq, \mathscr{R}) = \sum_{\mathbf{x}^{v_{\leq i-1}}} N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}^{v_{\leq i-1}})) \tag{11.1}$$

where the summation is over all possible partial solutions $\mathbf{x}^{v_{\leq i-1}}$ of the sub-problem $\texttt{RMTP}(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R})$. Now let us fix $\mathbf{x}^{v_{\leq i-1}}$. We define

$$\mathscr{S}(\mathbf{x}^{v_{\leq i-1}}) := \{\mathbf{y} = (y_{v_{\leq i-1}+1}, \ldots, y_{v_{\leq i}}) \in F_{[1]}^c \times \cdots \times F_{[v_i]}^c : \overline{\mathbf{A}}_i \mathbf{y} = \boldsymbol{\lambda}_i\}$$

where for all $j \in [v_i]$, $F_{[j]} := F_{j'}(\mathbf{x}^{v_{\le i-1}})$ for the unique j' such that $v_{\le i-1} + j \in P_{j'}$ (uniqueness follows from partiteness). $\mathcal{S}(\mathbf{x}^{v_{\le i-1}})$ is the set of all solutions to $\texttt{RMTP}(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}^{v_{\le i-1}}))$, or equivalently, all tuples $\mathbf{y}$ such that $\mathbf{x}^{v_{\le i-1}} \| \mathbf{y}$ is a solution to $\texttt{RMTP}(\mathbf{A}_{\le i}, \boldsymbol{\lambda}_{\le i}, \simeq, \mathscr{R})$. Also let $f_{[j]} := |F_{[j]}|$.

CRUDE BOUND. Since the $\overline{\mathbf{A}}_i$ is a $q_i \times v_i$ acyclic matrix having full row rank, implying that the dimension of its null space is $v_i - q_i$, and noting that $|F_j(\mathbf{x}^{v_{\le i-1}})| \le r + q$ for all $j \in [v_i]$ we have

$$2^{(v_i - q_i - 1)m}(2^m - v_i(r+q)) \le |\mathcal{S}(\mathbf{x}^{v_{\le i-1}})| \le 2^{(v_i - q_i)m}$$

This inequality along with Eq. (11.1) implies

$$2^{(v_i - q_i - 1)m}(2^m - v_i(r+q)) \le \frac{N(\mathbf{A}_{\le i}, \boldsymbol{\lambda}_{\le i}, \simeq, \mathscr{R})}{N(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R})} \le 2^{(v_i - q_i)m} \tag{11.2}$$

Now we give a finer analysis. We define

$$\mathcal{S}_\emptyset := \{\mathbf{y} \in (\mathbb{F}_2^m)^{v_i} : \overline{\mathbf{A}}_i \mathbf{y} = \boldsymbol{\lambda}_i\}$$

Moreover, for each $j \in [v_i]$, we define

$$\mathcal{S}_{\{j\}} := \mathcal{S}_{\{j\}}(\mathbf{x}^{v_{\le i-1}}) := \mathcal{S}_\emptyset \cap \left((\mathbb{F}_2^m)^{j-1} \times F_{[j]} \times (\mathbb{F}_2^m)^{w-j}\right)$$

Then we have

$$\mathcal{S}(\mathbf{x}^{v_{\le i-1}}) = \mathcal{S}_\emptyset \setminus \bigcup_{j \in [v_i]} \mathcal{S}_{\{j\}}$$

Thus defining $\mathcal{S}_J := \cap_{j \in J} \mathcal{S}_{\{j\}}$ for $J \subseteq [v_i]$, we have principle of inclusion and exclusion

$$N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}^{v_{\le i-1}})) = |\mathcal{S}(\mathbf{x}^{v_{\le i-1}})| = \sum_{\substack{J \subseteq [v_i] \\ J \neq \emptyset}} (-1)^{|J|} |\mathcal{S}_J|$$

Choose any nonempty subset $J \subseteq [v_i]$ with $|J| \le w - 1$. Then the $q_i \times (v_i - |J|)$ submatrix, $\mathbf{A}_{i,J}$, of $\overline{\mathbf{A}}_i$ obtained by removing the columns with indices $v_{\le i-1} + j : j \in J$, has full row rank, q_i, by Propositions 10.2 and 10.1. Thus if we fix the $v_{\le i-1} + J$ indexed variables to be $\mathbf{y}^J = (y_j : j \in J) \in \bigtimes_{j \in J} F_{[j]}$, we get a system of equations with coefficient matrix $\mathbf{A}_{i,J}$, which will have exactly $2^{(v_i - |J| - q_i)m}$ solutions. Thus, denoting $f_{[J]} = \prod_{j \in J} f_{[j]}$, we have $|\mathcal{S}_J| = f_{[J]} \cdot 2^{(v_i - |J| - q_i)m}$ for all $J \subseteq [v_i]$, with $|J| \le w - 1$.

First we prove the lower bound for isolated components.

Lemma 11.1. *Take $i \in [i^*]$, which means that the i-th component is isolated. Then for any solution, $\boldsymbol{x}^{i-1}$, to $\texttt{RMTP}(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R})$, we have*

$$|\mathscr{S}(\boldsymbol{x}^{i-1})| \ge 2^{-m} \cdot \prod_{j=1}^{w} (2^m - f_{\le i-1}^{(j)}) \cdot \left(1 - \frac{2}{2^{m(w-1)}} \left| \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\boldsymbol{x}^{i-1})) - \frac{\prod_{j=1}^{w} f_{\le i-1}^{(j)}}{2^m} \right| \right)$$

Proof. In this case we have $v_i = w$ and $q_i = 1$. Then we have

$$\begin{aligned}
|\mathscr{S}(\mathbf{x}^{i-1})| &= \sum_{\substack{J \subseteq [w] \\ J \neq \emptyset}} (-1)^{|J|} |\mathscr{S}_J| = \sum_{\substack{J \subset [w] \\ J \neq \emptyset}} (-1)^{|J|} f_{[J]} 2^{m(w-|J|-1)} + (-1)^w \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) \\
&= 2^{-m} \left(\sum_{\substack{J \subset [w] \\ J \neq \emptyset}} (-1)^{|J|} f_{[J]} 2^{m(w-|J|)} + \prod_{j=1}^{w} f_{\le i-1}^{(j)} - \prod_{j=1}^{w} f_{\le i-1}^{(j)} + (-1)^w 2^m \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) \right) \\
&= 2^{-m} \left(\prod_{j=1}^{w} (2^m - f_{\le i-1}^{(j)}) + (-1)^w 2^m \left(\mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) - \frac{\prod_{j=1}^{w} f_{\le i-1}^{(j)}}{2^m} \right) \right) \\
&\ge \frac{\prod_{j=1}^{w} (2^m - f_{\le i-1}^{(j)})}{2^m} \left(1 - \frac{2^m}{\prod_{j=1}^{w} (2^m - f_{\le i-1}^{(j)})} \left| \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) - \frac{\prod_{j=1}^{w} f_{\le i-1}^{(j)}}{2^m} \right| \right) \\
&\ge \frac{\prod_{j=1}^{w} (2^m - f_{\le i-1}^{(j)})}{2^m} \left(1 - \frac{2}{2^{m(w-1)}} \left| \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) - \frac{\prod_{j=1}^{w} f_{\le i-1}^{(j)}}{2^m} \right| \right)
\end{aligned}$$

where the second equality follows from the definition of μ, and the last inequality follows from the fact that $f_{\le i-1}^{(j)} \le r + q \le 2^n/2$. □

Lemma 11.2. *Take $i \in [i^*]$. Then*

$$N(\mathbf{A}_{\le i}, \boldsymbol{\lambda}_{\le i}, \simeq, \mathscr{R}) \ge \frac{\prod_{j=1}^{w} (2^m - f_{\le i-1}^{(j)})}{2^m} \left(1 - \frac{2\mu(\boldsymbol{\lambda}_i, \mathscr{R})}{2^{m(w-1)}} - \frac{2\Delta_{\boldsymbol{\lambda}_{\le i}}}{2^{m(w-1)}} - \frac{6(q+r)^w}{2^{mw}} \right) \times N(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R})$$

Proof. From Eq. (11.1) and Lemma 11.1, we have

$$N(\mathbf{A}_{\le i}, \boldsymbol{\lambda}_{\le i}, \simeq, \mathscr{R}) = \sum_{\mathbf{x}^{i-1}} N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}^{i-1}))$$

$$\geq \sum_{\mathbf{x}^{i-1}} \frac{\prod_{j=1}^{w}(2^m - f_{\leq i-1}^{(j)})}{2^m} \left(1 - \frac{2}{2^{m(w-1)}} \left| \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) - \frac{\prod_{j=1}^{w} f_{\leq i-1}^{(j)}}{2^m} \right| \right)$$

$$\geq \frac{\prod_{j=1}^{w}(2^m - f_{\leq i-1}^{(j)})}{2^m} \left(N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R}) - \frac{2\prod_{j=1}^{w} f_{\leq i-1}^{(j)}}{2^{mw}} N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R}) \right.$$

$$\left. - \frac{2}{2^{m(w-1)}} \sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) \right)$$

Lemma 11.2 then follows by noting that $f_{\leq i-1}^{(j)} \leq r + q$ and the following claim.

Claim 11.2.1.

$$\sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) \leq \left(\mu(\boldsymbol{\lambda}_i, \mathscr{R}) + \Delta_{\boldsymbol{\lambda}_{\leq i-1}} + \frac{2(r+q)^w}{2^m} \right) N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R})$$

□

PROOF OF CLAIM 11.2.1. We have

$$\sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, \mathscr{F}(\mathbf{x}^{i-1})) = \sum_{\mathbf{x}^{i-1}} \sum_{I \subseteq [w]} \mu(\boldsymbol{\lambda}_i, \{P_I, R_{[w]\setminus I}\})$$

$$= \sum_{I \subseteq [w]} \sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, \{P_I, R_{[w]\setminus I}\})$$

where $P_I = \bigtimes_{j \in I} P_j$ and $R_{[w]\setminus I} = \bigtimes_{j \in [w]\setminus I} R_j$.

CASE 1. $I = \emptyset$. In this case:

$$\sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, R_{[w]}) = \mu(\boldsymbol{\lambda}_i, \mathscr{R}) \cdot N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R})$$

CASE 2. $I \neq \emptyset$. Fix some $\mathbf{a}^{[w]\setminus I} \in R_{[w]\setminus I}$ and define $\mathbf{a}^{\oplus} := \bigoplus_{j \in [w]\setminus I} a_j$, with $\mathbf{a}^{\oplus} = 0^m$ whenever $I = [w]$. Fix some $\mathbf{b}^I \in P_I$. Then we have

$$\sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, \mathbf{x}^{\mathbf{b}^I}, \mathbf{a}^{[w]\setminus I}\}) = \sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i \oplus \mathbf{a}^{\oplus}, \mathbf{x}^{\mathbf{b}^I}\})$$

The r.h.s. is the number of solutions of $\texttt{RMTP}(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R})$ that additionally satisfies the equation $\bigoplus_{b \in \mathbf{b}^I} x_b = \boldsymbol{\lambda}_i \oplus \mathbf{b}^{\oplus}$. Let $\boldsymbol{\alpha}$ be a $1 \times v_{\leq i-1}$ binary vector, which have non-zero entries only at the indices $b \in \mathbf{b}^I$. If $\mathbf{A}'$ is the matrix obtained by adjoining the row $\boldsymbol{\alpha}$ to $\mathbf{A}_{\leq i-1}$, and $\boldsymbol{\lambda}'$ is the vector obtained by adjoining the element $\boldsymbol{\lambda}_i \oplus \mathbf{a}^{\oplus}$ to $\boldsymbol{\lambda}_{\leq i-1}$, then the r.h.s. is basically $N(\mathbf{A}', \boldsymbol{\lambda}', \simeq, \mathscr{R})$.

CASE 2.1. $\mathbf{A}'$ has full row rank. Suppose for some $j \in [i-1]$, $\mathbf{A}_j$ has a non-zero entry at the index $b \in \mathbf{b}^I$. Let $\mathbf{A}_{[i]\setminus j}|\boldsymbol{\lambda}_{[i-1]\setminus j}$ be the matrix obtained from $\mathbf{A}_{\le i-1}|\boldsymbol{\lambda}_{\le i-1}$ by removing the row $\mathbf{A}_j|\boldsymbol{\lambda}_j$. Then using the fact that $\mathbf{A}''$ has full row rank, we have

$$N(\mathbf{A}', \boldsymbol{\lambda}', \simeq, \mathscr{R}) \le 2^{m(w-2)} N(\mathbf{A}_{[i]\setminus j}, \boldsymbol{\lambda}_{[i]\setminus j}, \simeq, \mathscr{R})$$

Moreover using the crude bound Eq. 11.2, we have

$$N(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R}) \ge (2^{m(w-1)} - w(r+q)2^{m(w-2)}) \cdot N(\mathbf{A}_{[i]\setminus j}, \boldsymbol{\lambda}_{[i]\setminus j}, \simeq, \mathscr{R})$$

Combining, we have

$$N(\mathbf{A}', \boldsymbol{\lambda}', \simeq, \mathscr{R}) \le \frac{2}{2^m} N(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R})$$

where we use the fact $w(r+q) \le 2^m/2$. There are at most $\binom{w}{|I|}$ choices of I with size $|I|$, and for each such choice there are at most $q^{|I|}r^{w-|I|}$ choices for $\mathbf{b}^I, \mathbf{a}^{[w]\setminus I}$, which finally gives

$$\sum_{I\subseteq[w]} \sum_{\mathbf{x}^{i-1}} \mu(\boldsymbol{\lambda}_i, \{P_I, R_{[w]\setminus I}\}) \le \frac{2(r+q)^w}{2^m} N(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R})$$

CASE 2.2. $\mathbf{A}'$ does not have full row rank. In this case, the adjoined row, $\boldsymbol{\alpha}$, must be linearly dependent on the rows of $\mathbf{A}_{\le i-1}$. But since all the rows of $\mathbf{A}_{\le i-1}$ have weight w and their non-zero entries are at disjoint column indices. So we must have, $I = [w]$, and $\boldsymbol{\alpha} = \mathbf{A}_j$ for some $j \in [i-1]$, which also necessitates that $\boldsymbol{\lambda}_j = \boldsymbol{\lambda}_i$. Since there are at most $\Delta_{\boldsymbol{\lambda}_{\le i-1}}$ choices for such a j, $N(\mathbf{A}', \boldsymbol{\lambda}', \simeq, \mathscr{R}) \le \Delta_{\boldsymbol{\lambda}_i} \cdot N(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \simeq, \mathscr{R})$.

The claim then follows by combining all these cases. □

Finally, we move on to give a lower bound for the non-isolated components.

Lemma 11.3. *Suppose $i > i^*$, that is the i-th component is non-isolated. Then*

$$|\mathcal{S}(\boldsymbol{x}^{v_{\le i-1}})| \ge \frac{\prod_{j=1}^{w}(2^m - f^{(j)}_{\le i-1})}{2^{mq_i}} \left(1 - \frac{2v_i^w(q+r)^w}{2^{mw}} - \epsilon(q,r,w)\right)$$

where

$$\epsilon(q,r,w) = \begin{cases} \frac{2q_i(r+q)^{w-1}}{2^{m(w-1)}} & \text{for odd } w \\ 0 & \text{for even } w \end{cases}$$

Proof. Recall that $|\mathcal{S}(\mathbf{x}^{v_{\le i-1}})| = \sum_{\substack{J\subseteq[v_i]\\ J\neq\emptyset}}(-1)^{|J|}|\mathcal{S}_J|$. First we consider the case when w is even. Then by using Bonferroni's inequality, we have

$$
\begin{aligned}
|\mathcal{S}(\mathbf{x}^{v_{\le i-1}})| &\ge \sum_{\substack{J\subseteq[v_i]\\ 0<|J|\le w-1}}(-1)^{|J|}|\mathcal{S}_J| = \sum_{\substack{J\subseteq[v_i]\\ 0<|J|\le w-1}}(-1)^{|J|}f_{[J]}2^{m(v_i-|J|-q_i)}\\
&\ge \frac{1}{2^{mq_i}}\left(\sum_{\substack{J\subseteq[v_i]\\ 0<|J|\le w-1}}(-1)^{|J|}f_{[J]}2^{m(v_i-|J|)} + \sum_{\substack{J\subseteq[v_i]\\ |J|=w}} f_{[J]}2^{m(v_i-w)} - \sum_{\substack{J\subseteq[v_i]\\ |J|=w}} f_{[J]}2^{m(v_i-w)}\right)\\
&\ge \frac{1}{2^{mq_i}}\left(\prod_{j=1}^{v_i}(2^m - f^{(j)}_{\le i-1}) - v_i^w(r+q)^w 2^{m(v_i-w)}\right)\\
&\ge \frac{\prod_{j=1}^{v_i}(2^m - f^{(j)}_{\le i-1})}{2^{mq_i}}\left(1 - \frac{2v_i^w(r+q)^w}{2^{mw}}\right)
\end{aligned}
$$

where the second last inequality follows from the fact that $f_{[J]} \le (r+q)^w$ for any J with size w.

Now for odd w, again using Bonferroni's inequality we have

$$
\begin{aligned}
|\mathcal{S}(\mathbf{x}^{v_{\le i-1}})| &\ge \sum_{\substack{J\subseteq[v_i]\\ 0<|J|\le w}}(-1)^{|J|}|\mathcal{S}_J| = \sum_{\substack{J\subseteq[v_i]\\ 0<|J|\le w-1}}(-1)^{|J|}f_{[J]}2^{m(v_i-|J|-q_i)} - \sum_{\substack{J\subseteq[v_i]\\ |J|=w}}|\mathcal{S}_J|\\
&\ge \frac{1}{2^{mq_i}}\left(\sum_{\substack{J\subseteq[v_i]\\ 0<|J|\le w}}(-1)^{|J|}f_{[J]}2^{m(v_i-|J|)} - 2^{mq_i}\sum_{\substack{J\subseteq[v_i]\\ |J|=w}}|\mathcal{S}_J|\right)\\
&\ge \frac{1}{2^{mq_i}}\left(\prod_{j=1}^{v_i}(2^m - f^{(j)}_{\le i-1}) - 2^{mq_i}\sum_{\substack{J\subseteq[v_i]\\ |J|=w}}|\mathcal{S}_J|\right)\\
&\ge \frac{\prod_{j=1}^{v_i}(2^m - f^{(j)}_{\le i-1})}{2^{mq_i}}\left(1 - \frac{2}{2^{m(v_i-q_i)}}\sum_{\substack{J\subseteq[v_i]\\ |J|=w}}|\mathcal{S}_J|\right)
\end{aligned}
$$

Now we make the following claim:

Claim 11.3.1.

$$\sum_{\substack{J\subseteq[v_i]\\|J|=w}} |\mathcal{S}_J| \leq q_i(r+q)^{w-1}2^{m(v_i-w-q_i+1)} + v_i^w(r+q)^w 2^{m(v_i-w-q_i)}$$

The lemma now follows from the above claim. □

PROOF OF CLAIM 11.3.1. Take any $J \subseteq [v_i]$ with $|J| = w$. Let $\mathbf{A}'$ be the matrix obtained by removing the J-indexed columns from $\overline{\mathbf{A}}_i$. Now using Proposition 10.3 we have two cases:

CASE 1. For some row $(\overline{\mathbf{A}}_i)_{j\cdot}$, all the non-zero entries of the row are exactly in the J-column indices. Then by Proposition 10.3 we have $\mathrm{rank}(\mathbf{A}') = q_i - 1$. Let us denote the collection of all J's satisfying Case 1 as mcj, then we have

$$\sum_{J\in\mathcal{J}} |\mathcal{S}_J| \leq q_i(r+q)^{w-1}2^{m(v_i-w-q_i+1)}$$

CASE 2. This is the complementary case. From Proposition 10.3, we know that in this case $\mathrm{rank}(\mathbf{A}') = q_i$, and hence we have

$$\sum_{\substack{J\subseteq[v_i]\\|J|=w, J\notin\mathcal{J}}} |\mathcal{S}_j| \leq v_i^w(r+q)^w 2^{m(v_i-w-q_i)}$$

The sum of these two cases yeilds the claim. □

Since the bound in Lemma 11.3 is independent of $\mathbf{x}^{v_{\leq i-1}}$, we have the following corollary.

Corollary 11.3.1. *For $i > i^*$,*

$$N(\mathbf{A}_{\leq i}, \boldsymbol{\lambda}_{\leq i}, \simeq, \mathscr{R}) \geq \frac{\prod_{j=1}^{w}(2^m - f_{\leq i-1}^{(j)})}{2^{mq_i}}\left(1 - \frac{2v_i^w(q+r)^w}{2^{mw}} - \epsilon(q,r,w)\right) \times N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \simeq, \mathscr{R})$$

where $\epsilon(q,r,w)$ is defined as in Lemma 11.3.

Theorem 11.1 now follows from the recursive application of Corollary 11.3.1 for all i from c down to i^*+1 and then Lemma 11.2 from i^* down to 1.

12 COMPLETE RMTP

In this chapter we consider the $\texttt{CRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \{R\})$ problem. Note that if $\mathbf{a}|0^m \in \mathrm{rowsp}^+(\mathbf{A}|\boldsymbol{\lambda})$ with $\mathrm{wt}(\mathbf{a}) = 2$, then $N(\mathbf{A}, \boldsymbol{\lambda}, \{R\}) = 0$. In this case we call the CRMTP problem *trivial*, otherwise, we call it *non-trivial*. We will prove the following lower bound to the number of solutions to a nontrivial $\texttt{CRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \{R\})$ problem:

Main result for complete RMTP

Theorem 12.1. *Let $w \geq 2$ and $w(q+r) \leq 2^m/2$. Then the non-trivial* CRMTP *problem instantiated by*

- *an acyclic w-regular $\mathbf{A}$ with component form*

$$\mathbf{A}|\boldsymbol{\lambda} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_c & \boldsymbol{\lambda}_c \end{pmatrix} \in \mathbb{F}_2^{q \times (v+1)}.$$

  with $\overline{\mathbf{A}}_i \in \mathbb{F}_2^{q_i \times v_i}, \boldsymbol{\lambda}_i \in (\mathbb{F}_2^m)^{q_i \times 1}; \sum_i q_i = q, \sum_i v_i = v$.

- *a restricted set R, with size $|R| = r$.*

has number of solutions $N(\mathbf{A}, \boldsymbol{\lambda}, \{R\}) \geq (1-\epsilon) \cdot \mathbb{E}(\mathbf{A}, \boldsymbol{\lambda}, \{R\})$, where

$$\epsilon \leq \frac{2\mu(\boldsymbol{\lambda}, \mathscr{R})}{2^{m(w-1)}} + \frac{2qM}{2^{m(w-1)}} + \frac{6q(q+r)^w}{2^{mw}} + \frac{qw^2}{2^{2m}} + \sum_{i=i^*+1}^{c} \left(\frac{2v_i^w (q+r)^w}{2^{mw}} + \frac{q_i (q+r)^{w-1}}{2^{(w-1)}} + \frac{v_i^2}{2^{2m}} \right)$$

Here $\mathscr{R}$ is a family of sets containing w copies of R. Also, note that the expected number of solutions for random $\boldsymbol{\lambda}$ is defined as

$$\mathbb{E}(\mathbf{A}, \boldsymbol{\lambda}, \{R\}) = 2^{-mq} \cdot (2^m - |R|)_v .$$

Consider an equivalence relation $\simeq$ on $[v]$, inducing a partition $(P_1, \ldots, P_w)$, such that $\mathbf{A}$ is partite with respect to $\simeq$. Also let $\mathscr{R} = \{R_j\}_{j \in [w]}$ be a family of sets containing

w copies of R, i.e., $R_1 = \cdots = R_w = R$, as defined in Theorem 12.1. Then we call the $\texttt{RPRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \simeq, \mathscr{R})$ problem a partite version of the $\texttt{CRMTP}(\mathbf{A}, \boldsymbol{\lambda}, \{R\})$ problem. Adapting Eq. (10.1) of Chapter 10 for the CRMTP case, we define

$$F(\mathbf{x}_{\le i}) := R \cup \mathbf{x}_{\le i}, \qquad f_{\le i} := |F(\mathbf{x}_{\le i})| \tag{12.1}$$

We let $\mathscr{F}(\mathbf{x}_{\le i}) = \{F_j(\mathbf{x}_{\le i})\}_{j=[w]}$ denote the family of sets, with $F_1 = \cdots = F_w = F(\mathbf{x}_{\le i})$ Then CRMTP variant of Eq. (11.1) will then be

$$N(\mathbf{A}_{\le i}, \boldsymbol{\lambda}_{\le i}, \{R\}) = \sum_{\mathbf{x}_{\le i-1}} N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \{F(\mathbf{x}_{\le i-1})\}) \tag{12.2}$$

where the summation is taken over all $\mathbf{x}_{\le i-1}$ satisfying $\texttt{CRMTP}(\mathbf{A}_{\le i-1}, \boldsymbol{\lambda}_{\le i-1}, \{R\})$. Now $N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \{F(\mathbf{x}_{\le i-1})\}) = |\mathscr{S}(\mathbf{x}_{\le i-1})|$, where

$$\mathscr{S}(\mathbf{x}_{\le i-1}) = \{\mathbf{y} \in (\mathbb{F}_2^m \setminus F(\mathbf{x}_{\le i-1}))^{v_i *} : \overline{\mathbf{A}}_i \mathbf{y} = \boldsymbol{\lambda}_i\}$$

As for done for the partite case, we now define

$$\mathscr{S}_\emptyset := \{\mathbf{y} \in (\mathbb{F}_2^m)^{v_i} : \overline{\mathbf{A}}_i \mathbf{y} = \boldsymbol{\lambda}_i\}, \;\; \mathscr{S}_{\{j\}} := \mathscr{S}_\emptyset \cap \left((\mathbb{F}_2^m)^{j-1} \times F(\mathbf{x}_{\le i-1}) \times (\mathbb{F}_2^m)^{v_i - j}\right), \; j \in [v_i]$$

Moreover, for $j_1 < j_2 \in [v_i]$, we define

$$\mathscr{EQ}_{j_1,j_2} := \{\mathbf{y} \in (\mathbb{F}_2^m)^{v_i} : \overline{\mathbf{A}}\mathbf{y} = \boldsymbol{\lambda}_i \wedge y_{j_1} = y_{j_2}\}$$

Then we have

$$\mathscr{S}(\mathbf{x}_{\le i-1}) = \mathscr{S}_\emptyset \setminus \left(\left(\bigcup_{j=1}^{v_i} \mathscr{S}_{\{j\}} \right) \cup \left(\bigcup_{j_1 < j_2 \in [v_i]} \mathscr{EQ}_{j_1,j_2} \right) \right)$$

Thus

$$\begin{aligned} N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \{F(\mathbf{x}_{\le i-1})\}) &= |\mathscr{S}_\emptyset| - \left| \bigcup_{j=1}^{v_i} \mathscr{S}_{\{j\}} \right| - \left| \bigcup_{j_1 < j_2 \in [v_i]} \mathscr{EQ}_{j_1,j_2} \right| \\ &= N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}_{\le i-1})) - \left| \bigcup_{j_1 < j_2 \in [v_i]} \mathscr{EQ}_{j_1,j_2} \right| \\ &\ge N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}_{\le i-1})) - \binom{v_i}{2} 2^{m(v_i - 2 - q_i)} \end{aligned}$$

where in the second equality $N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}_{\le i-1}))$ denotes the number of solutions to $\texttt{RPRMTP}(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}(\mathbf{x}_{\le i-1}))$, the partite version of $\texttt{CRMTP}(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \{F(\mathbf{x}_{\le i-1})\})$, and the last inequality follows from the fact that $|\mathscr{EQ}_{j_1,j_2}| \le 2^{m(v_i - 2 - q_i)}$ as $\mathrm{wt}(\mathbf{A}) \ge w \ge 2$. This gives the following counterparts to Lemma 11.1, 11.2, 11.3 and Corollary 11.3.1, for the CRMTP case:

Lemma 12.1. *Take $i \in [i^*]$, which means that the i-th component is isolated. Then for any solution, $\boldsymbol{x}^{i-1}$, to* CRMTP$(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \{R\})$*, we have*

$$|\mathcal{S}(\boldsymbol{x}^{i-1})| \geq \frac{(2^m - f_{\leq i-1})^w}{2^m} \cdot \left(1 - \frac{2}{2^{m(w-1)}} \left|\mu(\boldsymbol{\lambda}_i, \mathscr{F}(\boldsymbol{x}^{i-1})) - \frac{f^w_{\leq i-1}}{2^m}\right| - \frac{w^2}{2^{2m}}\right)$$

Lemma 12.2. *Take $i \in [i^*]$. Then*

$$N(\mathbf{A}_{\leq i}, \boldsymbol{\lambda}_{\leq i}, \{R\}) \geq \frac{(2^m - f_{\leq i-1})^w}{2^m} \left(1 - \frac{2\mu(\boldsymbol{\lambda}_i, \mathscr{R})}{2^{m(w-1)}} - \frac{2M}{2^{m(w-1)}} - \frac{6(r+wq)^w}{2^{mw}} - \frac{w^2}{2^{2m}}\right) \times N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \{R\})$$

Lemma 12.3. *Suppose $i > i^*$, that is the i-th component is non-isolated. Then*

$$|\mathcal{S}(\boldsymbol{x}_{\leq i-1})| \geq \frac{(2^m - f_{\leq i-1})^{v_i}}{2^{mq_i}} \left(1 - \frac{2v_i^w (r+wq)^w}{2^{mw}} - \epsilon(q,r,w) - \frac{v_i^2}{2^{2m}}\right)$$

where

$$\epsilon(q,r,w) = \begin{cases} \frac{2q_i(r+q)^{w-1}}{2^{m(w-1)}} & \text{for odd } w \\ 0 & \text{for even } w \end{cases}$$

Corollary 12.3.1. *For $i > i^*$,*

$$N(\mathbf{A}_{\leq i}, \boldsymbol{\lambda}_{\leq i}, \{R\}) \geq \frac{(2^m - f_{\leq i-1})^{v_i}}{2^{mq_i}} \left(1 - \frac{2v_i^w (q+r)^w}{2^{mw}} - \epsilon(q,r,w) - \frac{v_i^2}{2^{2m}}\right) \times N(\mathbf{A}_{\leq i-1}, \boldsymbol{\lambda}_{\leq i-1}, \{R\})$$

where $\epsilon(q,r,w)$ is defined as in Lemma 12.3.

Now by recursive application of Corollary 12.3.1 from c to $i^* + 1$, and then applying Lemma 12.2 from i^* down to 1, gives us Theorem 12.1. The distinguishing terms between the results above and their respective partite counterparts are marked in blue. They are contributed by the additional $\mathscr{EQ}$ sets in the CRMTP case.

Part III

MOTIVATIONS AND APPLICATIONS

In the third part of the dissertation we present popular cryptographic constructions whose security analyses gave rise to the need of different variants of the mirror theory problem, and how the lower bounds proved by us result in optimal security bounds for the respective constructions.

13

APPLICATIONS OF COMPLETE AND BIPARTITE MIRROR THEORY FOR $\xi_{max} = 2$

Xor of two pseudorandom permutations, $\mathsf{XOR}_2(x) := \mathsf{E}_{k_1}(x) \oplus \mathsf{E}_{k_2}(x)$ [1] [BI99], and its single-keyed variant $\mathsf{XOR}_1(x) := \mathsf{E}_k(0\|x) \oplus \mathsf{E}_k(1\|x)$, are the most popular candidates among the PRP-based PRF constructions, as discussed in section 1.3.1. Both these constructions result in systems of equations, the corresponding graphs of which have maximum component size 2. In this chapter, we present the security bounds for both of these constructions using Theorem 8.1 and 6.1, respectively.

13.1 XOR_1 CONSTRUCTION: APPLICATIONS OF CMTP FOR $\xi_{\max} = 2$

The security analysis of the XOR_1 construction using the H-coefficient technique is already done in section 3.2. The only thing that remains to prove the n-bit security of XOR_1 construction is to prove that the number of solutions to a bivariate system of q equations having $\xi_{\max} = 2$, is at least $(2^n)_{2q}/2^{nq}$. This is exactly what Theorem 6.1 states for any $n \geq 12$ and $q \leq 2^n/58$. Thus we have,

Theorem 13.1. *For any $n \geq 12$ and $q \leq 2^n/58$,*

$$\boldsymbol{Adv}^{\mathrm{prf}}_{\mathrm{XOR}_1}(q) \leq \frac{q}{2^n}.$$

13.2 XOR_2 CONSTRUCTION: APPLICATION OF BMTP FOR $\xi_{\max} = 2$

Consider the $\{0,1\}^n$-challenge function $\mathcal{O}$ defined as $\mathcal{O}(x) = \boldsymbol{\pi}_1(x) \oplus \boldsymbol{\pi}_2(x)$ where $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2$ are independent $\{0,1\}^n$ random permutations, i. e., $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2 \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n)$. We want to find out the PRF security of the above construction, i. e., we want to calculate $\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{O}}(q) = \max_{\mathscr{A} \in \boldsymbol{\mathscr{A}}(q)} \Delta_{\mathscr{A}}(\mathcal{O}; \boldsymbol{\rho})$, where $\boldsymbol{\rho}$ is a $\{0,1\}^n$-random function. To bound $\Delta_{\mathscr{A}}(\mathcal{O}; \boldsymbol{\rho})$ via the coefficient H-technique (Corollary 3.0.2).

In this distinguishability scenario all transcripts are attainable, in the sense that $\Omega = \mathsf{Supp}(\tau(\mathscr{A}^{\boldsymbol{\rho}})) = (\{0,1\}^n)^q \times (\{0,1\}^n)^q$. Letting $\Theta_1 := \tau(\mathscr{A}^{\boldsymbol{\rho}})$ and $\Theta_2 := \tau(\mathscr{A}^{\mathcal{O}})$, we have

- $\boldsymbol{p}_{\Theta_1}(x^q, y^q) = 2^{-nq}$, by definition of the random function (Definition 2.6).

1 Here, E_{k_1} and E_{k_2} denote two n-bit independent pseudorandom permutations

- $\boldsymbol{p}_{\Theta_1}(x^q, y^q) = N/((2^n)_q)^2$, where N is the number of solutions to the following system of equations and non-equations (recalling from Example 1.2): The internal variables are $\mathsf{X}_i = \pi_1(x_i)$ and $\mathsf{Y}_i = \pi_2(x_i)$, $i \in [q]$.

  (EQUATIONS). $\mathsf{X}_i \oplus \mathsf{Y}_i = y_i$ for $i \in [q]$.

  (NON-EQUATIONS). $\mathsf{X}_i \oplus \mathsf{X}_j \neq 0$, $\mathsf{Y}_i \oplus \mathsf{Y}_j \neq 0$, for $i, j \in [q]$, $i \neq j$.

.

Now using Theorem 8.1, real-to-ideal world probability ratio turns out to be:

$$\frac{\boldsymbol{p}_{\Theta_1}(x^q, y^q)}{\boldsymbol{p}_{\Theta_0}(x^q, y^q)} = 1 - \frac{19q^2}{2^{2n}} - \frac{8n^3}{2^{2n}}$$

for any $n \geq 7$, and $q \leq 2^n/17$. Thus by H-coefficient technique (Corollary 3.0.1) we have:

Theorem 13.2. *For $n \geq 7$ and $q \leq 2^n/17$, we have*

$$\boldsymbol{Adv}^{\mathrm{prf}}_{\mathsf{XOR}_2}(q) \leq \frac{19q^2}{2^{2n}} + \frac{8n^3}{2^{2n}}$$

14

CRYPTOGRAPHIC APPLICATIONS OF LOWER BOUND FOR CMTP PROBLEM, THEOREM 7.1

In order to give an overview of how CMTP can be used, and to illustrate the importance of Theorem 7.1, we provide security proofs for a diverse set of constructions. Note that we focus on the parts of the proof that involve system of bivariate equations and omit the other parts, for which we cite the relevant results in the literature.

14.2 THE XORP CONSTRUCTION

In [Iwa06], Iwata introduced CENC, a beyond-birthday-bound secure mode of operation which uses an underlying permutation-based PRF dubbed XORP which is defined as follows:

$$\begin{aligned}\mathsf{XORP}[w] \,:\, \{0,1\}^{n-s} &\longrightarrow \{0,1\}^{wn}\\ x &\longmapsto \|_{i=1}^{w} \pi\left(\langle 0\rangle_s \| x\right) \oplus \pi\left(\langle i\rangle_s \| x\right),\end{aligned}$$

where $s = \lceil \log_2(w+1) \rceil$, and π is a uniformly random secret n-bit permutation. Later, Iwata, Mennink, and Vizár [IMV16] made the link between XORP and Mirror Theory explicit, and proved optimal security for the construction, using [Pat10a, Theorem 6]. We revisit their proof by applying Theorem 7.1 in order to demonstrate the following result[1].

Theorem 14.1. *Let $\mathscr{A}$ be an adversary against the prf-security of XORP$[w]$, which is allowed at most q queries. If $q \leq 2^n/12(w+1)^2$, one has*

$$\boldsymbol{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[w]}(q) \leq \frac{wq}{2^n} + \frac{w^2 q}{2^{n+1}}.$$

Proof. We are going to rely on the H coefficients technique. Let us fix an adversary $\mathscr{A}$ against the prf-security of XORP$[w]$, which is allowed at most q queries. We assume without loss of generality that $\mathscr{A}$ is deterministic (as it is time-unbounded), never repeats queries, and always makes exactly q queries. The transcript τ of the interaction of $\mathscr{A}$ with its oracle can be written as

$$\tau = \{(X_1, Y_{1,1} \| \ldots \| Y_{1,w}), \ldots, (X_q, Y_{q,1} \| \ldots \| Y_{q,w})\},$$

1 We do not claim novelty for this Theorem, but we present its proof for illustration purpose.

where, for $i = 1, \ldots, q$ and $j = 1, \ldots, w$, one has $|Y_{i,j}| = n$. We say that an attainable transcript τ is bad if at least one of those conditions is satisfied:

- there exists $(i, j) \in (q] \times (w]$ such that $Y_{i,j} = 0^n$;
- there exists $(i, j, j') \in (q] \times (w] \times (w]$ such that $j \neq j'$ and $Y_{i,j} = Y_{i,j'}$.

The set $\Omega \setminus \Omega_{\text{bad}}$ consists of all attainable transcripts that are not bad. Since the $Y_{i,j}$ values are uniformly random and independent in the ideal world, it is easy to see that one has

$$\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{ideal}}}) \in \Omega_{\text{bad}}\right) \leq \frac{wq}{2^n} + \frac{w^2 q}{2^{n+1}}. \tag{14.8}$$

Let us fix any good transcript τ. By taking $X'_{i,j} = \pi\left(\langle j \rangle_s \| X_i\right)$, the event $\tau(\mathscr{A}^{\mathcal{O}_{\text{real}}}) = \tau$ can easily be turned into the following system of bivariate affine equations:

$$\begin{array}{rcl@{\qquad}rcl} X'_{1,0} \oplus X'_{1,1} & = & Y_{1,1} & & X'_{1,0} \oplus X'_{q,1} & = & Y_{q,1} \\ \vdots & & & \cdots & \vdots & & \\ X'_{1,0} \oplus X'_{1,w} & = & Y_{1,w} & & X'_{1,0} \oplus X'_{q,w} & = & Y_{q,w} \end{array}$$

Since τ is a good transcript, the corresponding graph clearly has q components, of size $w + 1$, and the sum of labels of edges of any path in the graph is not 0^n. Let us denote N the number of pairwise distinct solutions of this system. Then the probability that $X'_{i,j} = \pi\left(\langle j \rangle_s \| X_i\right)$ for all pairs (i, j) is exactly $1/\left(2^n\right)_{(w+1)q}$. Hence, one has

$$\frac{\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{real}}}) = \tau\right)}{\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{ideal}}}) = \tau\right)} \geq N \frac{\left(2^n\right)^{wq}}{\left(2^n\right)_{(w+1)q}} \geq 1, \tag{14.9}$$

where the last inequality results from the application of Theorem 7.1. Combining Cor. 3.0.2 with Eqs (14.8) and (14.9) ends the proof of Theorem 14.1. □

14.3 OPTIMALLY SECURE VARIABLE-INPUT-LENGTH PRFS

In [CJN20], Cogliati, Jha and Nandi propose several constructions to build optimally secure variable-input-length (VIL) PRFs from secret random permutations. Those schemes combine a diblock almost collision-free universal hash function with a finalization function based on the Benes construction [AV96]. The most efficient variant, whose representation can be found in Figure 14.1, relies on two independent permutations, and its security proof [CJN20, Theorem 7.3] involves the use of Mirror Theory for a single permutation.

First, let us recall the necessary definition for keyed hash function. A $(\mathscr{K}, \mathscr{X}, \mathscr{Y})$-keyed function H is said to be *ϵ-almost universal (AU) hash function* if for any distinct $X, X' \in \mathscr{X}$, we have

$$\Pr_{\mathsf{K} \xleftarrow{*} \mathscr{K}}\left(H_{\mathsf{K}}(X) = H_{\mathsf{K}}(X')\right) \leq \epsilon. \tag{14.10}$$

Let us fix a non-empty set $\mathcal{X} \subset \{0,1\}^*$, and let H be a $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$-keyed function that processes its inputs in n-bit blocks. H is said to be (q, σ, ϵ)-*Almost θ-Collision-free Universal* (or ACU_θ) if, for every $X^q \in (\mathcal{X})_q$ such that X^q contains at most σ blocks, one has $\Pr_{C \geq \theta}(\leq) \epsilon$, where

$$C := |\{(i,j) \,:\, 1 \leq i < j \leq q,\, H_K(X_i) = H_K(X_j)\}|.$$

Finally, we say that a pair $H = (H_1, H_2)$ of two $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$-keyed hash functions H_1, H_2 is $(q, \sigma, \epsilon_2, \epsilon_1)$-*Diblock ACU$_q$* (or DbACU_q) if H is (q, σ, ϵ_2)-AU and H_1, H_2 are (q, σ, ϵ_1)-ACU_q.

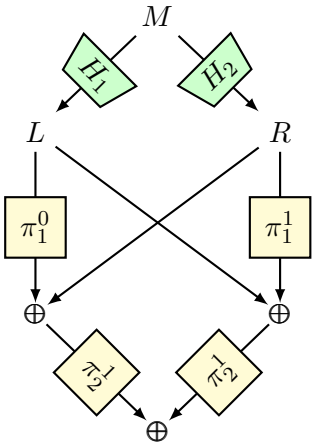


Figure 14.1: Representation of the 2k-HtmB-p2$[H]$ based on two uniformly random and independent n-bit permutations π_1, π_2. In the figure $\pi_i^0(x) := \pi_i(0\|x)$ and $\pi_i^1(x) := \pi_i(1\|x)$, for $i = 1, 2$. An edge (u, v) with label g denotes the mapping $v = g(u)$. Unlabeled edges are identity mapping. The inputs to the functions π_i^j are first truncated before the application of π_i.

Having defined the required security notion for the underlying hash function, the following result holds.

Theorem 14.2. *For $\epsilon_1, \epsilon_2, \sigma \geq 0$, $q \leq 2^n/12n^2$, and $(q, \sigma, \epsilon_2, \epsilon_1)$-DbACU$_q$ hash function H instantiated with key $K \xleftarrow{*} \mathcal{K}$, the prf-advantage of any distinguisher $\mathcal{A}$ that makes at most q queries against* 2k-HtmB-p2$[H]$ *is given by*

$$\boldsymbol{Adv}^{\mathrm{prf}}_{\text{2k-HtmB-p2}}(q) \leq \frac{128q^2}{2^{3n}} + \frac{136q^2}{2^{2n}} + \frac{8q}{2^n} + \epsilon_2 + 2\epsilon_1.$$

The complete proof of this result is exactly the same as the one of [CJN20, Theorem 7.3] where [Pat10a, Theorem 6] is replaced with Theorem 7.1.

PROOF SKETCH. Let us denote with M_i, for $i = 1, \ldots, q$, the inputs from $\mathscr{A}$. We introduce several random variables: $\mathsf{L}_i = \mathsf{H}_1(M_i)$, $\mathsf{R}_i = H_2(M_i)$, $\mathsf{X}_i = \mathsf{trunc}_{n-1}(\pi_1(0\|\mathsf{L}_i) \oplus \mathsf{R}_i)$ and $Y_i = \mathsf{trunc}_{n-1}(\pi_1(1\|\mathsf{R}_i) \oplus \mathsf{L}_i)$, so that

$$\mathsf{S}_i = \pi_2(0\|\mathsf{X}_i) \oplus \pi_2(1\|\mathsf{Y}_i).$$

Additionally, at the end of the interaction of $\mathscr{A}$ with its oracle, we release the values of the L_is, R_is,X_is, and Y_is. In the real world, we release the actual values, while in the ideal world we simply draw uniformly random keys for $\mathbf{H}_1$ and $\mathbf{H}_2$, along with a lazily sampled uniformly random π_1. Note that this can only increase the advantage of an adversary, so this can be done without loss of generality.

In order to apply Theorem 7.1, we need to make sure that the system (S) consisting of the q equations

$$\mathsf{S}_i = \pi_2(0\|\mathsf{X}_i) \oplus \pi_2(1\|\mathsf{Y}_i)$$

satisfies the initial conditions. We recall that an alternating trail of length k is a sequence $(i_1, \ldots, i_{k+1})$ such that either $X_{i_j} = \mathsf{X}_{i_j+1}$ or $Y_{i_j} = \mathsf{Y}_{i_j+1}$ for $j = 1, \ldots, k$, and consecutive equalities do not involve the same family of variables (i.e. an equality in X should be followed with an equality in Y). Moreover, an alternating cycle is a special type of alternating trail of even length, such that $i_{k+1} = i_1$. We say that a transcript τ is bad if at least one of the following conditions hold:

- τ contains an alternating cycle;
- τ contains an alternating trail $(i_1, \ldots, i_{k+1})$ such that $\oplus_{j=1}^{k+1} \mathsf{S}_{i_j} = 0$;
- the largest block of equalities contains at least $n + 1$ variables.[2]

In [CJN20], the authors prove that

$$\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{ideal}}}) \in \Omega_{\text{bad}}\right) \leq \frac{128q^2}{2^{3n}} + \frac{136q^2}{2^{2n}} + \frac{8q}{2^n} + \epsilon_2 + 2\epsilon_1. \tag{14.11}$$

Moreover, for any good transcript τ, one has

$$\frac{\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{real}}}) = \tau\right)}{\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{ideal}}}) = \tau\right)} = \frac{s2^{nq}}{(2^n)_{q_X+q_Y}} \geq 1, \tag{14.12}$$

where s denotes the number of p.d. solutions to the system (S) of equations, and q_X (resp. q_Y) the number of pairwise distinct X_i (resp. Y_i) values, and the last inequality results from the application of Theorem 7.1. Combining Cor. 3.0.2 with Equations (14.11) and (14.12) ends the proof of Theorem 14.2.

2 We say that two variables are in the same block of equalities if there exists an alternating trail involving both variables.

14.4 FEISTEL SCHEMES

In [Pat10b], Patarin introduced the study of beyond-birthday-bound security of balanced and unbalanced Feistel schemes using Mirror Theory. Since our work has improved upon the bounds conjectured by Patarin, we present here the proof sketch of security analysis of six-round balanced Feistel scheme with our new improved bounds.

DEFINTION OF ψ^k. Suppose $\mathsf{Func}(n,n)$ is the collection of all n-bit functions from $\{0,1\}^n$ to itself, and $\mathsf{Perm}(2n)$ be the collection of all permutations on $\{0,1\}^{2n}$. Then for $f \in \mathsf{Func}(n,n)n$ and $L, R \in \{0,1\}^n$, $\psi(f) \in \mathsf{Perm}(2n)$ is defined as follows:

$$\psi(f)[L,R] := [R, L \oplus f(R)]$$

In general, for $f_1, \cdots, f_k \in \mathsf{Func}(n,n)$, $\psi^k(f_1, \cdots, f_k) \in \mathsf{Perm}(2n)$ is defined as,

$$\psi^k(f_1, \cdots, f_k) := \psi(f_k) \circ \cdots \circ \psi(f_1).$$

The permutation $\psi^k(f_1, \cdots, f_k)$ is called a *balanced Feistel scheme with k rounds*. When $f_1, \cdots, f_k$ are randomly and independently chosen in $\mathsf{Func}(n,n)$, $\psi^k(f_1, \cdots, f_k)$ is called a *random Feistel scheme with k rounds*.

To analyze the PRP security of k-round Feistel scheme via the H-coefficient technique, given a transcript containing q query-response pairs

$$\tau := \{([L_i, R_i], [S_i, T_i]) : L_i, R_i, S_i, T_i \in \{0,1\}^n, i \in [q]\},$$

we would like to find out the probability of realizing this transcript in the real world,

$$\Pr\left(\tau(\mathscr{A}^{\mathcal{O}_{\text{real}}}) = \tau\right) = \Pr_{\substack{(f_1,\cdots,f_k) \\ \xleftarrow{*} \mathsf{Func}(n,n)^k}} \left(\psi^k(f_1, \cdots, f_k)[L_i, R_i] = [S_i, T_i]\ \forall i \in [q]\right) = \frac{H_k(\tau)}{|\mathsf{Func}(n,n)|^k}$$

where,

$$H_k(\tau) := \left|\{(f_1, \cdots, f_k) \in \mathsf{Func}(n,n)^k : \psi^k(f_1, \cdots, f_k)[L_i, R_i] = [S_i, T_i]\ \forall i \in [q]\}\right|$$

Note that, here, irrespective of whether the transcript was realized in the real or the ideal world, we will have that $[L_i, R_i], i \in [q]$ are pairwise distinct, and $[S_i, T_i], i \in [q]$ are pairwise distinct. There are no bad transcripts in the following analysis.

In Fig. 14.2 we have denoted the outputs of the successive rounds as follows:

$$[L_i, R_i] \xrightarrow{\psi(f_1)} [R_i, X_i] \xrightarrow{\psi(f_2)} [X_i, Y_i] \xrightarrow{\psi(f_3)} [Y_i, Z_i] \xrightarrow{\psi(f_4)} [Z_i, A_i] \xrightarrow{\psi(f_5)} [A_i, S_i] \xrightarrow{\psi(f_6)} [S_i, T_i]$$

Viewing 6-round Feistel as $\psi^6(f_1, \cdots, f_6) = \psi(f_1) \circ \psi^4(f_2, \cdots, f_5) \circ \psi(f_6)$, we can write

$$H_6(\tau) = \sum_{f_1, f_6 \in \mathsf{Func}(n,n)} H_4(\tau') \tag{14.13}$$

where

$$\tau' = \{([R_i, X_i], [A_i, S_i]) : X_i := L_i \oplus f_1(R_i), A_i := T_i \oplus f_6(S_i), i \in [q]\}$$

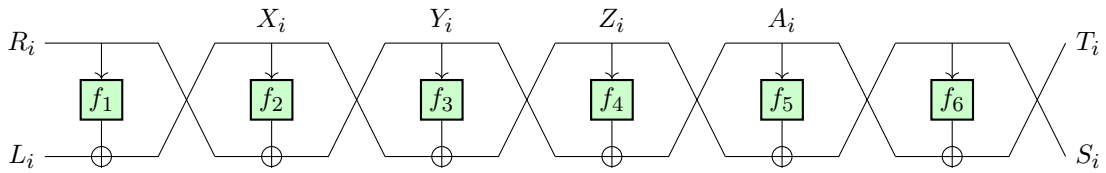


Figure 14.2: Balanced Feistel scheme with 6 rounds

FRAMEWORKS FOR ψ^4. To calculate $H_4(\tau')$ we define a 'framework' as a collection of equations of the form $Y_i = Y_j$ or $Z_i = Z_j$. We will say that two frameworks are equal if they imply exactly the same set of equalities in Y and Z. Let $\mathscr{F}$ be a framework. We will denote by $\mathsf{weight}(\mathscr{F})$ the number of $(Y_i, Z_i) \in (\{0,1\}^n)^2, i \in [q]$ that satisfy $\mathscr{F}$. If we denote $y_{\mathscr{F}}$ (resp., $z_{\mathscr{F}}$) the number of independent equalities of the form $Y_i = Y_j$ (resp., of the form $Z_i = Z_j$) in $\mathscr{F}$, then obviously we have $\mathsf{weight}(\mathscr{F}) = (2^n)_{q-y_{\mathscr{F}}} \cdot (2^n)_{q-z_{\mathscr{F}}}$

Note that, for a given framework $\mathscr{F}$, $Y_i = Y_j \in \mathscr{F} \implies f_3(Y_i) = f_3(Y_j)$, which is equivalent to saying $X_i \oplus Z_i = X_j \oplus Z_j$. Similarly, $Z_i = Z_j \in \mathscr{F} \implies Y_i \oplus A_i = Y_j \oplus A_j$. Moreover, $X_i = X_j \implies f_2(X_i) = f_2(X_j)$ which is equivalent to saying $R_i \oplus Y_i = R_j \oplus Y_j$. Similarly, $A_i = A_j \implies Z_i \oplus S_i = Z_j \oplus S_j$.

Let x be the number of independent equalities of the form $X_i = X_j, i \neq j$ and a be the number of independent equalities of the form $A_i = A_j, i \neq j$. Then by simple alegbraic manipulation we have the following result.

Lemma 14.1 (exact formula for $H_4(\tau')$).

$$H_4(\tau') = |\mathsf{Func}(n,n)|^4 \sum_{\mathscr{F}} \frac{[\#Y^q \textit{ satisfying } (C1)] \cdot [\#Z^q \textit{ satisfying } (C2)]}{2^{n(4q-x-y_{\mathscr{F}}-z_{\mathscr{F}}-a)}} \tag{14.14}$$

where

$$(C1): \begin{cases} X_i = X_j \implies Y_i \oplus Y_j = R_i \oplus R_j \\ Z_i = Z_j \in \mathscr{F} \implies Y_i \oplus Y_j = A_i \oplus A_j \\ \textit{The only equations } Y_i = Y_j, i < j, \textit{ are exactly those implied by } \mathscr{F} \end{cases}$$

$$(C2): \begin{cases} A_i = A_j \implies Z_i \oplus Z_j = S_i \oplus S_j \\ Y_i = Y_j \in \mathscr{F} \implies Z_i \oplus Z_j = X_i \oplus X_j \\ \textit{The only equations } Z_i = Z_j, i < j, \textit{ are exactly those implied by } \mathscr{F} \end{cases}$$

The summation on the r.h.s. of Eq. (14.14) is taken over all possible frameworks $\mathscr{F}$.

A we can see (C_1) yeilds a system of difference equations in the variables Y^q, and $(C2)$ a system of difference equations in Z^q. To find the number of solutions to these systems of equations using Theorem 7.1, we have to ensure: (1) the systems are p.d.-consistent, (2) the

conditions specified in the theorem, like the bound on the maximum component size, and that on the number of variables, is satisfied by the concerned systems.

Now the systems will be p.d. consistent if there is no cycle of non-zero label sum. To be on the safe side, we eliminate the possibility of any cycle whatsoever. Note that, there will be a cycle in the graph representing the system of difference equations in $(C1)$ (resp., $(C2)$) only if there is a 'circle in $X, Z_{\mathscr{F}}$' (resp., 'circle in $A, Y_{\mathscr{F}}$'), by which we mean that, for some $k \geq 3$, there is a cyclic tuple of indices $(i_1, \cdots, i_k)$, with $i_1, \cdots, i_{k-1}$ pairwise distinct and $i_k = i_1$, such that for all $j \in [k-1]$, either we have $X_{i_j} = X_{i_{j+1}}$ or we have $Z_{i_j} = Z_{i_{j+1}} \in \mathscr{F}$. We define a circle in $A, Y_{\mathscr{F}}$ similarly.

Following the same arguments there will be component of size ξ in the graph representing the system of difference equations in $(C1)$ (resp., $(C2)$) only if there is a 'line in $X, Z_{\mathscr{F}}$' (resp., 'line in $A, Y_{\mathscr{F}}$') of length ξ, by which we mean that, there are $\xi + 1$ distinct indices $i_1, \cdots, i_{\xi+1}$ such that for all $j \in [\xi]$, either $X_{i_j} = X_{i_{j+1}}$ or $Z_{i_j} = Z_{i_j} \in \mathscr{F}$. We define a line in $A, Y_{\mathscr{F}}$ similarly.

GOOD FRAMEWORK. We call a framework for ψ^4, $\mathscr{F}$, a *good framework*, if it does not result in any of the following:

1. a circle in $X, Z_{\mathscr{F}}$
2. a circle in $A, Y_{\mathscr{F}}$
3. a line in $X, Z_{\mathscr{F}}$ of length $\geq n$
4. a line in $A, Y_{\mathscr{F}}$ of length $\geq n$

From elaborate probability calculations done in Appendix C of [Pat10b] we have the following result:

Lemma 14.2 ([Pat10b]). *For a realizable transcript $\tau = \{([L_i, R_i], [S_i, T_i]) : i \in [q]\}$, when $f_1, f_6 \xleftarrow{*} \mathsf{Func}(,n)$ and $\mathscr{F}$ is randomly chosen (i.e., with probability proportional to $\mathsf{weight}(\mathscr{F})$), then*

$$\Pr\left(\mathscr{F} \text{ is a good framework}\right) \geq 1 - \frac{8q}{2^n}.$$

If a good framework $\mathscr{F}$ is chosen, then the systems of difference equations in $(C1)$ and $(C2)$ are p.d.-consistent and satisfy the conditions of Theorem 7.1 with $\xi_{\max} \leq n$. Now the system of difference equations in $(C1)$ (resp., $C2$) has $x + z_{\mathscr{F}}$ equations in $q - y_{\mathscr{F}}$ variables (resp., $a + y_{\mathscr{F}}$ equations in $q - z_{\mathscr{F}}$ variables) and hence by Theorem 7.1 has at least $(2^n)_{q-y_{\mathscr{F}}} / 2^{n(x+z_{\mathscr{F}})}$ solutions (resp., $(2^n)_{q-z_{\mathscr{F}}} / 2^{n(a+y_{\mathscr{F}})}$ solutions) if $q \leq N/12(\log_2 N)^2$. Then from Eq. (14.13) and Eq. (14.14) we get that

$$H_6(\tau) \geq \frac{|\mathsf{Func}(n,n)|^4}{2^{4qn}} \sum_{f_1, f_6 \in \mathsf{Func}(n,n)} \sum_{\text{good } \mathscr{F}} \underbrace{(2^n)_{q-y_{\mathscr{F}}} \cdot (2^n)_{q-z_{\mathscr{F}}}}_{\mathsf{weight}(\mathscr{F})} \overset{(\star)}{\geq} \frac{|\mathsf{Func}(n,n)|^6}{2^{2qn}} \left(1 - \frac{8q}{2^n}\right)$$

where $(\star)$ follows from Lemma 14.2 and the fact that $\sum_{\mathscr{F}} \mathsf{weight}(\mathscr{F}) = 2^{2qn}$. Thus, we have a for a realizable transcript τ

$$\frac{\Pr[T_{\text{real}} = \tau]}{\Pr[T_{\text{ideal}} = \tau]} = \frac{\frac{1}{2^{2qn}}\left(1 - \frac{8q}{2^n}\right)}{1/\left(2^{2n}\right)_q} \geq 1 - \frac{8q}{2^n} - \frac{q^2}{2^{2n}}.$$

Summarizing we have the following result.

Theorem 14.3. *If $q \leq \frac{2^n}{12n^2}$, then for every CPCA-2 adversary [a] $\mathscr{A}$ with q adaptive chosen plaintext or chosen ciphertext queries, we have*

$$\boldsymbol{Adv}^{\text{sprp}}_{\psi^6(f_1,\cdots,f_6)}(q) \leq \frac{8q}{2^n} + \frac{q^2}{2^{2n}}.$$

where $f_1, \cdots, f_6 \xleftarrow{*} \mathsf{Func}(n, n)$.

a CPCA-2 adversary here means an adversary that adaptively queries Chosen Plaintexts and Chosen Ciphertexts.

15

THE LRW+ PARADIGM:
APPLICATION OF BMTP, *THEOREM 9.1*

In the seminal paper [LRW02], Liskov et al proposed the LRW1 and LRW2 constructions for tweakable blockciphers. Landecker et al [LST12] were the first to notice that cascading two independent instances of LRW2 results in BBB security. In [BGGS20], Bao et al, proposed that the three round-cascade of LRW1, which they named TNT, is beyond birthday bound CCA secure. In [JKNS24] we presented a birthday bound chosen ciphertext attack on TNT, disproving the claims by [BGGS20]. This motivated our proposal of a generalized view of the cascaded LRW design, in the same work [JKNS24], that encompasses both 4-LRW1 and cascaded 2-LRW2 constructions. In this chapter we prove the IND-CCA security of the LRW+ construction up to $2^{3n/4}$ queries. But first we give the birthday bound attack for TNT, that inspired our investigation into LRW+ [1].

15.1 BIRTHDAY BOUND CCA ATTACK ON TNT

We consider the TNT construction in an information-theoretic setting. Accordingly, we instantiate TNT based on three independent uniform random permutations $\boldsymbol{\pi}_1$, $\boldsymbol{\pi}_2$, and $\boldsymbol{\pi}_3$ of $\{0,1\}^n$. Recall that, the TNT construction is defined by the mapping

$$(t, m) \xmapsto{\mathsf{TNT}} \boldsymbol{\pi}_3(t \oplus \boldsymbol{\pi}_2(t \oplus \boldsymbol{\pi}_1(m))), \tag{15.3}$$

For some non-zero $\delta \in \{0,1\}^n$ and $m \in \{0,1\}^n$, consider the function $\mathcal{O}_{\delta,m} : \{0,1\}^n \to \{0,1\}^n$, associated to each n-bit tweakable permutation $\mathcal{O}$ with n-bit tweak, defined by the mapping

$$t \xmapsto{\mathcal{O}_{\delta,m}} \mathcal{O}^{-1}(t \oplus \delta,\ \mathcal{O}(t,\ m)). \tag{15.4}$$

We are only interested in $\widetilde{\boldsymbol{\pi}}_{\delta,m}$ and $\mathsf{TNT}_{\delta,m}$ where $\widetilde{\boldsymbol{\pi}}$ is a tweakable uniform random permutation of $\{0,1\}^n$ with n-bit tweaks.

Suppose $\widetilde{\boldsymbol{\pi}}_{\delta,m}$ is executed over q distinct inputs $(t_1, \ldots, t_q)$. Observe that, for any valid choice of $(t_1, \ldots, t_q)$, $\widetilde{\boldsymbol{\pi}}$ is executed at most twice for any tweak t_i. Thus, one can expect $\widetilde{\boldsymbol{\pi}}_{\delta,m}(\cdot)$ to be almost uniform and independent, and thus, indistinguishable from a uniform random function $\boldsymbol{\rho} : \{0,1\}^n \to \{0,1\}^n$ for a large range of q. In fact, as long as

$$\widetilde{\boldsymbol{\pi}}(t_i, m) \neq \widetilde{\boldsymbol{\pi}}(t_j, m) \text{ for all } i \neq j \text{ such that } t_j = t_i \oplus \delta,$$

1 This is a bonus result, not directly related to Mirror Theory, and the following section can be skipped.

$\widetilde{\pi}_{\delta,m}$ can be shown to be indistinguishable from $\boldsymbol{\rho}$ up to $O(2^n)$ queries. More importantly, as we show in the following discussion, one can easily show that the $\widetilde{\pi}_{\delta,m}$ is almost identical to $\boldsymbol{\rho}$ in terms of the number of output collisions.

$\mathsf{TNT}_{\delta,m}$, on the other hand, exhibits a rather peculiar and interesting property. Apparently, $\mathsf{TNT}_{\delta,m}$ is more prone to collisions as compared to $\widetilde{\pi}_{\delta,m}$, which results in a direct IND-CCA distinguisher for TNT. A formal distinguisher with complete advantage calculation appears later in section 15.1.2. We first demonstrate the biased behavior by comparing the number of output collisions for $\mathsf{TNT}_{\delta,m}$ and $\widetilde{\pi}_{\delta,m}$.

15.1.1 *Comparing the Number of Collision Pairs in Ideal and Real Worlds*

Fix some non-negative integer $q \leq 2^n$. Fix a set $\mathscr{T} = \{t_1, \ldots, t_q\} \subseteq \{0,1\}^n$ of size q, an $m \in \{0,1\}^n$, and a non-zero $\delta \in \{0,1\}^n$. Let $\mathscr{O}$ be a tweakable permutation (which is either $\widetilde{\pi}$ in the ideal world or TNT in the real world). We compute $\mathsf{M}'_i = \mathscr{O}_{\delta,m}(t_i)$ by making a forward query $\mathscr{O}(t_i, m) := \widehat{\mathsf{C}}_i$, followed by a backward query $\mathsf{M}'_i = \mathscr{O}^{-1}(t_i \oplus \delta, \widehat{\mathsf{C}}_i)$. We write $\mathtt{COLL}(\mathscr{O}_{\delta,m})$ to denote the number of pairs (i,j), $i < j$ such that $\mathsf{M}'_i = \mathsf{M}'_j$.

ANALYZING $\mathrm{COLL}_{\mathrm{id}} := \mathtt{COLL}(\widetilde{\pi}_{\delta,m})$: For any $i \neq j \in [q]$, let $\chi_{i,j}$ denote the indicator random variable corresponding to the event: $\mathsf{M}'_j = \mathsf{M}'_i$. Then, using linearity of expectation, we have

$$\mathbb{E}\left(\mathsf{coll}_{\mathrm{id}}\right) = \sum_{i<j\in[q]} \mathbb{E}\left(\chi_{i,j}\right) = \sum_{i<j\in[q]} \Pr\left(\chi_{i,j}\right), \tag{15.5}$$

where we abused the notation slightly to use $\chi_{i,j}$ to denote the event $\chi_{i,j} = 1$. Let $\sim$ be a relation on $[q]$, such that for all $i \neq j \in [q]$, $i \sim j$ if and only if $t_i = t_j \oplus \delta$. Note that $\sim$ is symmetric. Suppose there are ν pairs (t_i, t_j), $i < j$ such that $t_i \sim t_j$. Clearly, $\nu \leq q/2$. Now, we can split the right-hand side of (15.5) as follows:

$$\sum_{i<j\in[q]} \Pr\left(\chi_{i,j}\right) = \sum_{\substack{i<j\in[q] \\ i\sim j}} \Pr\left(\chi_{i,j}\right) + \sum_{\substack{i<j\in[q] \\ i\not\sim j}} \Pr\left(\chi_{i,j}\right) \tag{15.6}$$

CASE $i \not\sim j$: We must have $\{t_i, t_j\} \cap \{t_i \oplus \delta, t_j \oplus \delta\} = \emptyset$. Thus, the two calls to $\widetilde{\pi}_{\delta,m}$ corresponding to the i-th and j-th queries result in exactly 2 calls to $\widetilde{\pi}$ and 2 calls $\widetilde{\pi}^{-1}$, each with a distinct tweak than others. Hence, the outputs of $\widetilde{\pi}_{\delta,m}$ on inputs t_i and t_j are mutually independent and uniformly distributed in $\{0,1\}^n$. Thus, for any $i \not\sim j$, we have

$$\Pr\left(\chi_{i,j}\right) = \frac{1}{2^n}, \tag{15.7}$$

which results in

$$\sum_{\substack{i<j\in[q]\\ i\not\sim j}} \Pr\left(\chi_{i,j}\right) = \left(\binom{q}{2} - \nu\right)\frac{1}{2^n}, \tag{15.8}$$

CASE $i \sim j$: In this case we have $t_i = t_j \oplus \delta$. Let $\mathsf{F}_{i,j}$ be the event that $\widetilde{\pi}(t_i, m) = \widetilde{\pi}(t_j, m)$. Then, we have $\mathsf{M}'_i = \mathsf{M}'_j = m$. Since, $t_i \neq t_j$, $\Pr\left(\mathsf{F}_{i,j}\right) = 2^{-n}$. So, for any $i \sim j$, we have

$$\begin{aligned}\Pr\left(\chi_{i,j}\right) &= \Pr\left(\chi_{i,j} \wedge \mathsf{F}_{i,j}\right) + \Pr\left(\chi_{i,j} \wedge \neg\mathsf{F}_{i,j}\right)\\ &= \Pr\left(\mathsf{F}_{i,j}\right) + \Pr\left(\chi_{i,j} \wedge \neg\mathsf{F}_{i,j}\right)\\ &= \frac{1}{2^n} + \Pr\left(\chi_{i,j} \wedge \neg\mathsf{F}_{i,j}\right),\end{aligned}$$

which immediately gives

$$\frac{1}{2^n} \leq \Pr\left(\chi_{i,j}\right) \leq \frac{1}{2^n} + \Pr\left(\chi_{i,j} \mid \neg\mathsf{F}_{i,j}\right) \leq \frac{1}{2^n} + \frac{1}{2^n - 1}. \tag{15.9}$$

Note that the last inequality follows from the observation that given $\neg\mathsf{F}_{i,j}$, outputs of $\widetilde{\pi}^{-1}(t_i \oplus \delta)$ and $\widetilde{\pi}^{-1}(t_j \oplus \delta)$ are sampled independently from a set of size exactly $2^n - 1$. This further results in

$$\frac{\nu}{2^n} \leq \sum_{\substack{i<j\in[q]\\ i\sim j}} \Pr\left(\chi_{i,j}\right) \leq \nu\left(\frac{1}{2^n} + \frac{1}{2^n - 1}\right). \tag{15.10}$$

Using (15.5), (15.6), (15.8), (15.10), and $\nu \leq q/2$ we have

$$\binom{q}{2}\frac{1}{2^n} \leq \mathbb{E}\left(\mathsf{coll}_{\mathrm{id}}\right) \leq \binom{q}{2}\frac{1}{2^n} + \frac{q}{2^n}. \tag{15.11}$$

ANALYZING $\mathsf{coll}_{\mathrm{re}} := \mathtt{COLL}(\mathsf{TNT}_{\delta,m})$: The analysis of $\mathtt{COLL}(\mathsf{TNT}_{\delta,m})$ is a bit more subtle and interesting. Fig. 15.1 gives a pictorial view of the i-th execution of $\mathsf{TNT}_{\delta,m}$. Clearly, the respective calls to π_3 and its inverse cancel out each other, resulting in the compressed view illustrated in Fig. 15.2.

Note that for any $i, j \in [q]$, $\mathsf{U}_i \oplus \mathsf{U}_j = t_i \oplus t_j$. Now, fix a pair of inputs (t_i, t_j) such that there is a collision at the output, i.e.,

$$(\mathsf{M}'_i = \mathsf{M}'_j) \iff (\widehat{\mathsf{M}}'_i = \widehat{\mathsf{M}}'_j) \iff (\mathsf{U}'_i \oplus \mathsf{U}'_j = t_i \oplus t_j) \iff (\mathsf{U}'_i \oplus \mathsf{U}'_j = \mathsf{U}_i \oplus \mathsf{U}_j),$$

and let $\chi_{i,j}$ denote the corresponding indicator random variable. Observe that $\mathsf{TNT}_{\delta,m}$, has the following interesting property:

$$(\widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j = \delta) \implies (\mathsf{U}'_i \oplus \mathsf{U}'_j = \mathsf{U}_i \oplus \mathsf{U}_j = t_i \oplus t_j),$$

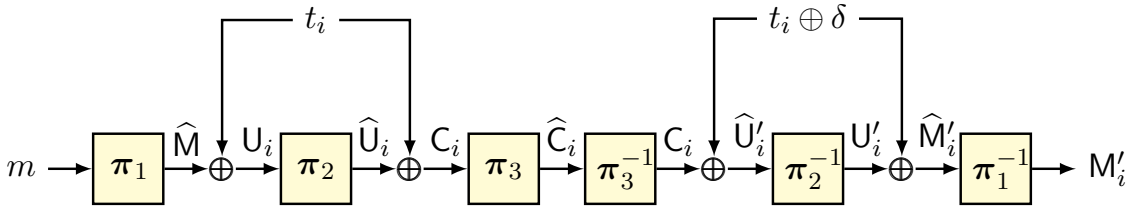


Figure 15.1: The execution trace for $\mathsf{TNT}_{\delta,m}$ on input t_i.

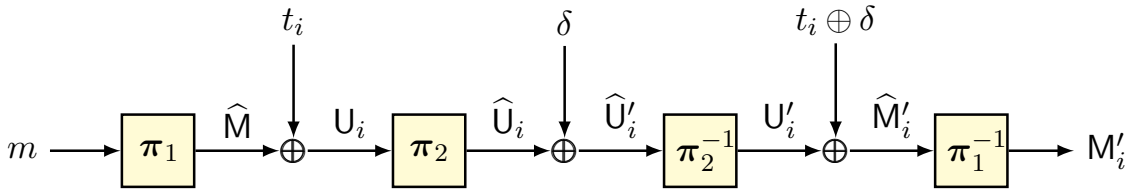


Figure 15.2: The effective execution trace for $\mathsf{TNT}_{\delta,m}$ on input t_i.

which implies that there are two sources of collisions in $\mathsf{TNT}_{\delta,m}$. A collision happens whenever

1. $\widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j = \delta$, or
2. $\widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta$ and $\mathsf{U}'_i \oplus \mathsf{U}'_j = t_i \oplus t_j$.

From this one can easily get a good upper and lower bound on the expected number of collisions in the real world. Using linearity of expectation, we have

$$\mathbb{E}\left(\mathsf{coll}_{\mathrm{re}}\right) = \sum_{i<j\in[q]} \mathbb{E}\left(\chi_{i,j}\right) = \sum_{i<j\in[q]} \Pr\left(\chi_{i,j}\right) \tag{15.12}$$

Further, from the above discussion, we have

$$\begin{aligned}
\Pr\left(\chi_{i,j}\right) &= \Pr\left(\chi_{i,j} \wedge \widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j = \delta\right) + \Pr\left(\chi_{i,j} \wedge \widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta\right) \\
&= \Pr\left(\widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j = \delta\right) + \Pr\left(\widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta\right) \\
&\qquad \times \Pr\left(\mathsf{U}'_i \oplus \mathsf{U}'_j = t_i \oplus t_j \mid \widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta\right) \\
&= \frac{1}{2^n - 1} + \left(1 - \frac{1}{2^n - 1}\right) \\
&\qquad \times \Pr\left(\mathsf{U}'_i \oplus \mathsf{U}'_j = t_i \oplus t_j \mid \widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta\right),
\end{aligned} \tag{15.13}$$

Note that $\widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta$ implies that $\mathsf{U}'_i, \mathsf{U}'_j \notin \{\mathsf{U}_i, \mathsf{U}_j\}$. Now, fix a valid choice for $(\mathsf{U}_i, \mathsf{U}_j, \widehat{\mathsf{U}}_i, \widehat{\mathsf{U}}_j)$, say $(u_i, u_j, \widehat{u}_i, \widehat{u}_j)$. Then, the number of valid choices for $(\mathsf{U}'_i, \mathsf{U}'_j)$ that satisfy the equation $\mathsf{U}'_i \oplus \mathsf{U}'_j = t_i \oplus t_j$, are all $(x, x \oplus t_i \oplus t_j)$ pairs such that

$$x \in \{0,1\}^n \setminus \left(\{u_i, u_j\} \cup \{u_i \oplus t_i \oplus t_j, u_j \oplus t_i \oplus t_j\}\right)$$

But, observe that $\{u_i, u_j\} = \{u_i \oplus t_i \oplus t_j, u_j \oplus t_i \oplus t_j\}$ by definition, for any valid choice of (u_i, u_j). Therefore, the number of valid $(x, x \oplus t_i \oplus t_j)$ is exactly $2^n - 2$. Furthermore, this counting is independent of the choice of $(u_i, u_j, \widehat{u}_i, \widehat{u}_j)$, whence it holds unconditionally. Now, each such choice for $(\mathsf{U}'_i, \mathsf{U}'_j)$ occurs with at most $1/(2^n-2)(2^n-3)$ probability, as they are sampled from $\{0,1\}^n \setminus \{\mathsf{U}_i, \mathsf{U}_j\}$ in a WOR (without replacement) manner. Then, using (15.13), we have

$$\begin{aligned}\Pr\left(\chi_{i,j}\right) &= \frac{1}{2^n-1} + \left(1 - \frac{1}{2^n-1}\right) \times \frac{1}{2^n-3} \\ &= \frac{1}{2^n-1} + \frac{1}{2^n-3} - \frac{1}{(2^n-1)(2^n-3)} \\ &= \frac{2}{2^n} + \frac{1}{2^n(2^n-1)} + \frac{3}{2^n(2^n-3)} - \frac{1}{(2^n-1)(2^n-3)}\end{aligned}$$

Using (15.12), we immediately have

$$\mathbb{E}\left(\mathsf{coll}_{\mathrm{re}}\right) = \binom{q}{2}\left(\frac{1}{2^n-1} + \frac{1}{2^n-3} - \frac{1}{(2^n-1)(2^n-3)}\right) \geq \binom{q}{2}\frac{2}{2^n}, \tag{15.14}$$

and on comparing this with (15.11), we can conclude that

$$\mathbb{E}\left(\mathsf{coll}_{\mathrm{re}}\right) \approx 2\mathbb{E}\left(\mathsf{coll}_{\mathrm{id}}\right).$$

This clearly indicates that the occurrence of collisions in $\mathsf{TNT}_{\delta,m}$ is approximately twice that of $\widetilde{\pi}_{\delta,m}$.

15.1.2 *The Collision Counting Distinguisher*

Based on the observations from the preceding section, we now present a formal distinguisher, called $\mathscr{A}^*$.

Fix a message $m \in \{0,1\}^n$, a set $\mathscr{T} = \{t_1, \ldots, t_q\} \subseteq \{0,1\}^n$ of size q, and a $\delta \neq 0^n$. Let $\theta(q,n)$ be some non-negative function of q and n, which will be defined later in the course of analysis.

Let $\mathcal{O}^{\pm}$ be the oracle $\mathscr{A}^*$ is interacting with. Then, $\mathscr{A}^*$ works by collecting $\mathsf{M}'_i = \mathcal{O}_{\delta,m}(t_i)$ for all $t_i \in \mathscr{T}$ in a multiset $\mathscr{M}$. As shown in the preceding section, this can be easily done by a pair of encryption-decryption queries for each $i \in [q]$. After this, $\mathscr{A}^*$ counts the number of collisions in $\mathscr{M}$ using any mechanism `collCount`, which we do not specify here (see [JKNS24] for details). If the number of collisions is greater than $\theta(q,n)$, the distinguisher returns 1, otherwise, it returns 0.

Note that the exact implementation of `collCount` is not relevant for the forthcoming advantage calculation and hence skipped. However, it is amply evident that the space complexity of the attack is $O(q)$, i.e., dominated by the query complexity. Further, looking ahead momentarily, one can implement `collCount` in such a way that it runs in time

$O(q \log_2 q)$. Other than this, $\mathscr{A}^*$ only makes $2q$ calls to $\mathscr{O}$, thus the overall time complexity is also in $O(q \log_2 q)$.

Define

$$\mu_{\mathrm{re}} := \binom{q}{2}\frac{2}{2^n} \qquad \mu_{\mathrm{id}} := \binom{q}{2}\frac{1}{2^n} + \frac{q}{2^n}.$$

Then, from (15.11) and (15.14), we have that $\mathbb{E}\left(\mathtt{COLL}(\mathsf{TNT}_{\delta,m})\right) \geq \mu_{\mathrm{re}} \geq \mu_{\mathrm{id}} \geq \mathbb{E}\left(\mathtt{COLL}(\widetilde{\pi}_{\delta,m})\right)$, whenever $q \geq 3$.

Theorem 15.2. *For $n \geq 4$, $10 \leq q \leq 2^n$, and $\theta(q,n) = (\mu_{\mathrm{re}} + \mu_{\mathrm{id}})/2$, we have*

$$\boldsymbol{Adv}^{\mathrm{tsprp}}_{\mathit{TNT}}(\mathscr{A}^*) \geq 1 - 371\frac{2^n}{q^2}.$$

Specifically, for $q \geq 28 \times 2^{\frac{n}{2}}$, $\boldsymbol{Adv}^{\mathrm{tsprp}}_{\mathit{TNT}}(\mathscr{A}^*) \geq 0.5$.

Proof. Recall that $\mathsf{coll}_{\mathrm{id}} = \mathtt{COLL}(\widetilde{\pi}_{\delta,m})$ and $\mathsf{coll}_{\mathrm{re}} = \mathtt{COLL}(\widetilde{\pi}_{\delta,m})$. Let $\sigma_s^2 := \mathsf{Var}(\mathsf{coll}_s)$, for all $s \in \{\mathrm{id}, \mathrm{re}\}$. In addition, whenever necessary, we also reuse the notations and definitions from the expectation calculation given in section 15.1.1.
Now, we have

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{TNT}}(\mathscr{A}^*) &= \left|\Pr\left(\mathscr{A}^*(\mathsf{TNT}_{\delta,m}) = 1\right) - \Pr\left(\mathscr{A}^*(\widetilde{\pi}_{\delta,m}) = 1\right)\right| \\
&= \left|\Pr\left(\mathsf{coll}_{\mathrm{re}} > \theta(q,n)\right) - \Pr\left(\mathsf{coll}_{\mathrm{id}} > \theta(q,n)\right)\right| \\
&\geq 1 - \frac{4(\sigma^2_{\mathrm{re}} + \sigma^2_{\mathrm{id}})}{(\mu_{\mathrm{re}} - \mu_{\mathrm{id}})^2}. \qquad (15.15)
\end{aligned}$$

where the last inequality follows from Proposition A.2. We make the following claim on σ^2_{re} and σ^2_{id}.

Claim 15.0.1. *For $n \geq 4$, $10 \leq q \leq 2^n$, we have*

$$\sigma^2_{\mathrm{id}} \leq \frac{4q^2}{2^n} \qquad \sigma^2_{\mathrm{re}} \leq \frac{11q^2}{2^n}$$

A proof of this claim is available in the Appendix A.3. Next, from (15.11) and (15.14), we have

$$\begin{aligned}
(\mu_{\mathrm{re}} - \mu_{\mathrm{id}})^2 &\geq \left(\binom{q}{2}\frac{2}{2^n} - \binom{q}{2}\frac{1}{2^n} - \frac{q}{2^n}\right)^2 \\
&\geq \binom{q}{2}^2 \frac{1}{2^{2n}}\left(1 - \frac{1}{q}\right)^2 \geq 0.162\frac{q^4}{2^{2n}} \qquad (15.16)
\end{aligned}$$

where the last inequality follows from $q \geq 10$. The result then follows from (15.15), Claim 15.0.1, and (15.16). □

15.2 BBB CCA-SECURITY OF LRW+

ALMOST XOR UNIVERSAL HASH FUNCTION: A (τ, n)-hash function family $\mathscr{H}$, is a family of functions $\{h : \{0,1\}^\tau \to \{0,1\}^n\}$, keyed implicitly by the choice of h. A (τ, n)-hash function family $\mathscr{H}$ is called an ϵ-almost XOR universal hash family (AXUHF) if for all $t \neq t' \in \{0,1\}^\tau$, and $\lambda \in \{0,1\}^n$, we have

$$\Pr\left(\mathsf{H} \xleftarrow{*} \mathscr{H} \ : \ \mathsf{H}(t) \oplus \mathsf{H}(t') = \lambda\right) \leq \epsilon. \tag{15.17}$$

For the special case of $\lambda = 0^n$, $\mathscr{H}$ is referred as an ϵ-AUHF.

THE LRW+ CONSTRUCTION: Let $\widetilde{\mathscr{H}}$ be a family of (τ, n)-tweakable permutations, and $\mathscr{H}$ be a (τ, n)-hash function family. Let $\widehat{\mathscr{H}} = (\widetilde{\mathscr{H}}^2 \times \mathscr{H})$, $(\widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}) \leftarrow \mathsf{KG}\left(\widehat{\mathscr{H}}\right)$, and $(\boldsymbol{\pi}_1, \boldsymbol{\pi}_2) \xleftarrow{*} \mathsf{Perm}(n)$, where $\mathsf{KG}\left(\widehat{\mathscr{H}}\right)$ is an efficient probabilistic algorithm that returns a random triple from $\widehat{\mathscr{H}}$.

The LRW+ construction is a (τ, n)- tweakable permutation family, defined by the following mapping (see Figure 15.3 for an illustration):

$$(t, m) \mapsto \widetilde{\mathbf{H}}_2^{-1}\left(t, \boldsymbol{\pi}_2\left(\mathbf{H}(t) \oplus \boldsymbol{\pi}_1\left(\widetilde{\mathbf{H}}_1(t, m)\right)\right)\right). \tag{15.18}$$

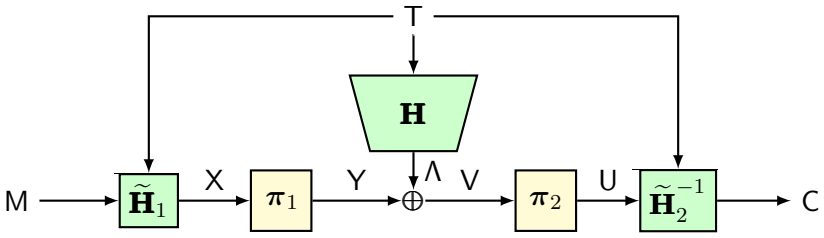


Figure 15.3: The LRW+ construction.

15.2.1 *Security of LRW+*

We say that $\mathsf{KG}\left(\widehat{\mathscr{H}}\right)$ is a pairwise independent sampling mechanism or PISM, if $(\widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}) \leftarrow \mathsf{KG}\left(\widehat{\mathscr{H}}\right)$ is a pairwise independent tuple.

We say that $\widetilde{\mathscr{H}}$ is an ϵ-almost universal tweakable permutation family (AUTPF) if and only if for all distinct $(t, m), (t', m') \in \{0,1\}^\tau \times \{0,1\}^n$,

$$\Pr\left(\widetilde{\mathbf{H}} \xleftarrow{*} \widetilde{\mathscr{H}} \ : \ \widetilde{\mathbf{H}}(t, m) = \widetilde{\mathbf{H}}(t', m')\right) \leq \epsilon.$$

Theorem 15.3. *Let $\tau, n \in \mathbb{N}$, and $\epsilon_1, \epsilon_2 \in [0,1]$. If $\widetilde{\mathscr{H}}$ and $\mathscr{H}$ are respectively ϵ_1-AUTPF and ϵ_2-AUHF, and $\mathsf{KG}\left(\widetilde{\mathscr{H}}\right)$ is a PISM, then, for $q \leq 2^{n-2}$, we have*

$$\boldsymbol{Adv}^{\mathrm{tsprp}}_{\mathsf{LRW+}}(q) \leq \epsilon(q,n),$$

where

$$\epsilon(q,n) = 2q^2\epsilon_1^{1.5} + \frac{4q^4\epsilon_1^2}{2^n} + \frac{32q^4\epsilon_1}{2^{2n}} + \frac{13q^4}{2^{3n}} + q^2\epsilon_1^2 + q^2\epsilon_1\epsilon_2 + \frac{2q^2}{2^{2n}}. \tag{15.19}$$

15.2.2 *Proof of Theorem 15.3*

Note that we are in the information-theoretic setting. In other words, we consider computationally unbounded distinguisher $\mathscr{A}$. Without loss of generality, we assume that $\mathscr{A}$ is deterministic and non-trivial.

15.2.2.1 *Oracle Description*

The two oracles of interest are: $\mathscr{O}_1$, the real oracle, that implements LRW+; and, $\mathscr{O}_0$, the ideal oracle, that implements $\widetilde{\boldsymbol{\pi}} \xleftarrow{*} \widetilde{\mathsf{Perm}}(\tau, n)$. We consider an extended version of these oracles, the one in which they release some additional information. We use notations analogously as given in Figure 15.3 to describe the transcript generated by $\mathscr{A}$'s interaction with its oracle.

Description of the real oracle, $\mathscr{O}_1$. The real oracle $\mathscr{O}_1$ faithfully runs LRW+. We denote the transcript random variable generated by $\mathscr{A}$'s interaction with $\mathscr{O}_1$ by the usual notation Θ_1, which is an 11-ary q-tuple

$$(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q, \mathsf{X}^q, \mathsf{Y}^q, \mathsf{V}^q, \mathsf{U}^q, \Lambda^q, \widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}),$$

defined as follows: The initial transcript consists of $(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q)$, where for all $i \in [q]$:

$$\mathsf{T}_i : \ i\text{-th tweak value} \quad \mathsf{M}_i : \ i\text{-th plaintext value} \quad \mathsf{C}_i : \ i\text{-th ciphertext value},$$

where, $\mathsf{C}^q = \mathsf{LRW+}(\mathsf{T}^q, \mathsf{M}^q)$. At the end of the query-response phase $\mathscr{O}_1$ releases some additional information $(\mathsf{X}^q, \mathsf{Y}^q, \mathsf{V}^q, \mathsf{U}^q, \Lambda^q, \widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H})$, such that for all $i \in [q]$:

- $(\mathsf{X}_i, \mathsf{Y}_i)$: i-th input-output pair for $\boldsymbol{\pi}_1$,
- $(\mathsf{V}_i, \mathsf{U}_i)$: i-th input-output pair for $\boldsymbol{\pi}_2$,
- Λ_i: i-th internal masking, $\widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}$: are the hash keys.

Note that X^q, U^q, and Λ^q are completely determined by the hash keys $\widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}$, and the initial transcript $(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q)$. We include them anyhow for the sake of convenience.

Description of the ideal oracle, $\mathcal{O}_0$. The ideal oracle $\mathcal{O}_0$ has access to $\widetilde{\pi}$. Since $\mathcal{O}_1$ releases some additional information, $\mathcal{O}_0$ must generate these values as well. The ideal transcript random variable Θ_0 is also an 11-ary q-tuple

$$(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q, \mathsf{X}^q, \mathsf{Y}^q, \mathsf{V}^q, \mathsf{U}^q, \Lambda^q, \widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}),$$

defined below. The initial transcript consists of $(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q)$, where for all $i \in [q]$:

$$\mathsf{T}_i: \ i\text{-th tweak value} \quad \mathsf{M}_i: \ i\text{-th plaintext value} \quad \mathsf{C}_i: \ i\text{-th ciphertext value},$$

where $\mathsf{C}^q = \widetilde{\pi}(\mathsf{T}^q, \mathsf{M}^q)$. Once the query-response phase is over $\mathcal{O}_0$ first samples $(\widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H}) \xleftarrow{*} \mathsf{KG}\left(\widehat{\mathscr{H}}\right)$, and then computes $(\mathsf{X}^q, \mathsf{U}^q, \Lambda^q)$, as follows:

$$\mathsf{X}^q := \widetilde{\mathbf{H}}_1(\mathsf{T}^q, \mathsf{M}^q) \qquad \mathsf{U}^q := \widetilde{\mathbf{H}}_2(\mathsf{T}^q, \mathsf{C}^q) \qquad \Lambda^q := \mathbf{H}(\mathsf{T}^q).$$

Note that the conditional distributions of $(\mathsf{X}^q, \mathsf{U}^q, \Lambda^q, \widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H})$, given $(\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q)$ is identical in both the worlds. This means that X^q, U^q, and Λ^q are defined honestly.

Given the partial transcript $\Theta_0' := (\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q, \mathsf{X}^q, \mathsf{U}^q, \Lambda^q, \widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H})$ we wish to characterize the hash key $\widehat{\mathbf{H}} := (\widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H})$ as good or bad. We write $\widehat{\mathscr{H}}_{\mathsf{bad}}$ for the set of bad hash keys, and $\widehat{\mathscr{H}}_{\mathsf{good}} := \widehat{\mathscr{H}} \setminus \widehat{\mathscr{H}}_{\mathsf{bad}}$. We say that the hash key $\widehat{\mathbf{H}} \in \widehat{\mathscr{H}}_{\mathsf{bad}}$ (or $\widehat{\mathbf{H}}$ is bad) if and only if one of the following predicates is true:

1. H_1: $\exists^* i, j \in [q]$ such that $\mathsf{X}_i = \mathsf{X}_j \wedge \mathsf{U}_i = \mathsf{U}_j$.
2. H_2: $\exists^* i, j \in [q]$ such that $\mathsf{X}_i = \mathsf{X}_j \wedge \Lambda_i = \Lambda_j$.
3. H_3: $\exists^* i, j \in [q]$ such that $\mathsf{U}_i = \mathsf{U}_j \wedge \Lambda_i = \Lambda_j$.
4. H_4: $\exists^* i, j, k, \ell \in [q]$ such that $\mathsf{X}_i = \mathsf{X}_j \wedge \mathsf{U}_j = \mathsf{U}_k \wedge \mathsf{X}_k = \mathsf{X}_\ell$.
5. H_5: $\exists^* i, j, k, \ell \in [q]$ such that $\mathsf{U}_i = \mathsf{U}_j \wedge \mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell$.
6. H_6: $\exists k \geq 2^n/2q, \exists^* i_1, i_2, \ldots, i_k \in [q]$ such that $\mathsf{X}_{i_1} = \cdots = \mathsf{X}_{i_k}$.
7. H_7: $\exists k \geq 2^n/2q, \exists^* i_1, i_2, \ldots, i_k \in [q]$ such that $\mathsf{U}_{i_1} = \cdots = \mathsf{U}_{i_k}$.

CASE 1. $\widehat{\mathbf{H}}$ IS BAD: If the hash key $\widehat{\mathbf{H}}$ is bad, then Y^q and V^q values are sampled degenerately as $\mathsf{Y}_i = \mathsf{V}_i = 0$ for all $i \in [q]$. It means that we sample without maintaining any specific conditions, which will almost certainly lead to inconsistencies.

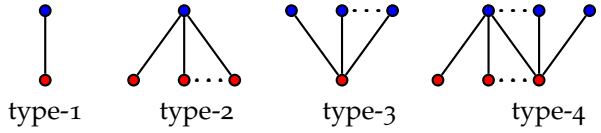


Figure 15.4: Enumerating all possible types of components of a transcript graph corresponding to a good hash key: type-1 is the only possible component of size $= 1$ edge; type-2 and type-3 are star components with center in A and B, respectively; type-4 is the only possible component that is not isolated or star (can have degree 2 vertices in both A and B). Note that the vertex-coloring is only for illustration purposes.

CASE 2. $\widehat{\mathbf{H}}$ IS GOOD: To characterize the transcript corresponding to a good hash key, it will be useful to study a random bipartite edge-labeled graph associated with $(\mathsf{X}^q, \mathsf{U}^q, \Lambda^q)$.

Definition 15.1 (Transcript Graph). *A transcript graph $\mathcal{G} = (A, B, E)$ associated with $(\mathsf{X}^q, \mathsf{U}^q, \Lambda^q)$, denoted $\mathcal{G}(\mathsf{X}^q, \mathsf{U}^q, \Lambda^q)$, is an undirected bipartite graph, where $A := \{(\mathsf{X}_i, 0) : i \in [q]\}$ and $B := \{(\mathsf{U}_i, 1) : i \in [q]\}$ are the two partitions of the vertex-set, and $E := \{((\mathsf{X}_i, 0), (\mathsf{U}_i, 1)) : i \in [q]\}$ denotes the edge-set. We also associate the label Λ_i with edge $((\mathsf{X}_i, 0), (\mathsf{U}_i, 1)) \in E$.*

For all practical purposes we may drop the partition markers 0 and 1, for each vertex $(\mathsf{X}_i, 0) \in A$ and $(\mathsf{U}_i, 1) \in B$, as they can be easily distinguished from the context and notations. Note that the event $\mathsf{X}_i = \mathsf{X}_j$ and $\mathsf{U}_i = \mathsf{U}_j$, although extremely unlikely, will result in a parallel edge in $\mathcal{G}$. Finally, each edge $(\mathsf{X}_i, \mathsf{U}_i) \in E$ corresponds to a query index $i \in [q]$, so we can equivalently view (and call) the edge $(\mathsf{X}_i, \mathsf{U}_i)$ as index (or query) i.

Consider the random transcript graph $\mathcal{G}(\mathsf{X}^q, \mathsf{U}^q)$ arising due to $\widehat{\mathbf{H}} \in \widehat{\mathscr{H}_{\mathsf{good}}}$. Lemma 15.1 and Figure 15.4 characterizes the different types of possible components in $\mathcal{G}(\mathsf{X}^q, \mathsf{U}^q)$.

Lemma 15.1. *The transcript graph $\mathcal{G}(\mathsf{X}^q, \mathsf{U}^q, \Lambda^q)$ generated by a good hash key $\widehat{\mathbf{H}}$ has the following properties:*

1. *$\mathcal{G}$ is simple, acyclic and has no isolated vertices.*
2. *$\mathcal{G}$ has no two adjacent edges i and j such that $\Lambda_i \oplus \Lambda_j = 0$.*
3. *$\mathcal{G}$ has no component of size $\geq 2^n/2q$ edges.*
4. *$\mathcal{G}$ has no component such that it has 2 distinct degree 2 vertices in A or B.*

In fact the all possible types of components in $\mathcal{G}$ are enumerated in Figure 15.4.

It should be noted that in [JN20], the authors do not explicitly address type-4 graphs. Instead, they focus on two specific subclasses, namely, type-4 and type-5 graphs [JN20]. Fortunately, this omission does not significantly impact either the security bound or the subsequent analysis.

In what follows, we describe the sampling of Y^q and V^q conditioned on the fact that $\widehat{\mathbf{H}} \in \widehat{\mathscr{H}_{\mathsf{good}}}$. We collect the indices $i \in [q]$ corresponding to the edges in all type-1, type-2, type-3, and type-4 components, in the index sets $\mathscr{I}_1$, $\mathscr{I}_2$, $\mathscr{I}_3$, and $\mathscr{I}_4$, respectively. Clearly, the five sets are disjoint, and $[q] = \mathscr{I}_1 \sqcup \mathscr{I}_2 \sqcup \mathscr{I}_3 \sqcup \mathscr{I}_4$. Let $\mathscr{I} = \mathscr{I}_1 \sqcup \mathscr{I}_2 \sqcup \mathscr{I}_3$. Consider a constrained system of equations

$$\mathscr{L} = \{Y_i \oplus V_i = \Lambda_i \ : \ i \in \mathscr{I}\},$$

with the constraint

$$\phi : \ \mathsf{X}^q \leftrightarrow Y^q \wedge \mathsf{U}^q \leftrightarrow V^q.$$

The solution space for $\mathscr{L}$, satisfying the constraint ϕ, is precisely the set

$$\mathcal{S} = \{(y^{\mathscr{I}}, v^{\mathscr{I}}) : y^{\mathscr{I}} \leftrightarrow \mathsf{X}^{\mathscr{I}} \wedge v^{\mathscr{I}} \leftrightarrow \mathsf{U}^{\mathscr{I}} \wedge y^{\mathscr{I}} \oplus v^{\mathscr{I}} = \Lambda^{\mathscr{I}}\}.$$

Given these definitions, the ideal oracle $\mathscr{O}_0$ samples $(\mathsf{Y}^q, \mathsf{V}^q)$ as follows:

- $(\mathsf{Y}^{\mathscr{I}}, \mathsf{V}^{\mathscr{I}}) \xleftarrow{*} \mathcal{S}$, i.e., $\mathscr{O}_0$ uniformly samples one valid assignment from the set of all valid assignments for $\mathsf{Y}^{\mathscr{I}}$ and $\mathsf{V}^{\mathscr{I}}$.
- Let $\mathscr{G} \setminus \mathscr{C}_{\mathscr{I}}$ denote the subgraph of $\mathscr{G}$ after the removal of all type-1, type-2, and type-3 components. For each component $\mathscr{C}$ of $\mathscr{G} \setminus \mathscr{C}_{\mathscr{I}}$:
  - Suppose $(\mathsf{X}_i, \mathsf{U}_i) \in \mathscr{C}$ corresponds to an edge in $\mathscr{C}$, where both X_i and U_i have degree ≥ 2. Then, $\mathsf{Y}_i \xleftarrow{*} \{0,1\}^n$ and $\mathsf{V}_i = \mathsf{Y}_i \oplus \Lambda_i$.
  - For each edge $(\mathsf{X}_{i'}, \mathsf{U}_{i'}) \neq (\mathsf{X}_i, \mathsf{U}_i) \in \mathscr{C}$, either $\mathsf{X}_{i'} = \mathsf{X}_i$ or $\mathsf{U}_{i'} = \mathsf{U}_i$. Suppose, $\mathsf{X}_{i'} = \mathsf{X}_i$. Then, $\mathsf{Y}_{i'} = \mathsf{Y}_i$ and $\mathsf{V}_{i'} = \mathsf{Y}_{i'} \oplus \Lambda_{i'}$. Now, suppose $\mathsf{U}_{i'} = \mathsf{U}_i$. Then, $\mathsf{V}_{i'} = \mathsf{V}_i$ and $\mathsf{Y}_{i'} = \mathsf{V}_{i'} \oplus \Lambda_{i'}$.

At this point, $\Theta_0 = (\mathsf{T}^q, \mathsf{M}^q, \mathsf{C}^q, \mathsf{X}^q, \mathsf{Y}^q, \mathsf{V}^q, \mathsf{U}^q, \Lambda^q, \widetilde{\mathbf{H}}_1, \widetilde{\mathbf{H}}_2, \mathbf{H})$ is completely defined. In this way we maintain both the consistency of equations of the form $\mathsf{Y}_i \oplus \mathsf{V}_i = \Lambda_i$ (as in the case of real world), and the permutation consistency within each component, given that $\widehat{\mathbf{H}} \in \widehat{\mathscr{H}_{\mathsf{good}}}$. However, there might be collisions among Y or V values from different components.

15.2.2.2 *Definition and Analysis of Bad Transcripts*

Given the description of the transcript random variable corresponding to the ideal oracle we can define the set of transcripts Ω as the set of all tuples $\omega = (t^q, m^q, c^q, x^q, y^q, v^q, u^q, \lambda^q, \widetilde{h}_1, \widetilde{h}_2, h)$, where $t^q \in (\{0,1\}^\tau)^q$; $m^q, c^q, y^q, v^q \in (\{0,1\}^n)^q$; $\widehat{h} = (\widetilde{h}_1, \widetilde{h}_2, h) \in \widehat{\mathscr{H}}$; $x^q = \widetilde{h}_1(t^q, m^q)$; $u^q = \widetilde{h}_2(t^q, c^q)$; $\lambda^q = h(t^q)$; and $m^q \overset{t^q}{\leftrightarrow} c^q$.

Our bad transcript definition is inspired by two requirements:

1. Eliminate all x^q, u^q, and λ^q tuples such that both y^q and v^q are trivially restricted by way of linear dependence. For example, consider the condition H_2. This leads to $y_i = y_j$, which would imply $v_i = y_i \oplus \lambda_i = y_j \oplus \lambda_j = v_j$. Assuming $i > j$, v_i is trivially restricted ($= v_j$) by way of linear dependence. This may lead to $u^q \not\leftrightarrow v^q$ as u_i may not be equal to u_j.

2. Eliminate all x^q, u^q, y^q, v^q tuples such that $x^q \not\leftrightarrow y^q$ or $u^q \not\leftrightarrow v^q$.

Among the two, requirement 2 is trivial as $x^q \leftrightarrow y^q$ and $u^q \leftrightarrow v^q$ is always true for real world transcript. Requirement 1 is more of a technical one that helps in the ideal world sampling of y^q and v^q.

BAD TRANSCRIPT DEFINITION: Throughout the discussion, we consider the transcript

$$\omega = (t^q, m^q, c^q, x^q, y^q, v^q, u^q, \lambda^q, \widehat{h})$$

to characterize the bad transcripts.

We first designate certain transcripts as bad depending upon the characterization of hash keys. Inspired by the ideal world description, we say that a hash key $\widehat{h} \in \widehat{\mathscr{H}_{\mathsf{bad}}}$ (or $\widehat{h}$ is bad) if and only if the following predicate is true:

$$\mathsf{H}_1 \vee \mathsf{H}_2 \vee \mathsf{H}_3 \vee \mathsf{H}_4 \vee \mathsf{H}_5 \vee \mathsf{H}_6 \vee \mathsf{H}_7.$$

We say that ω is *hash-induced* bad transcript, if $\widehat{h} \in \mathscr{H}_{\mathsf{bad}}$. We write this event as BAD1, and by a slight abuse of notations,[2] we have

$$\mathtt{BAD1} = \bigcup_{i=1}^{7} \mathsf{H}_i. \tag{15.20}$$

This takes care of the first requirement. For the second one we have to enumerate all the conditions which might lead to $x^q \not\leftrightarrow y^q$ or $u^q \not\leftrightarrow v^q$. Since we sample degenerately when the hash key is bad, the transcript is *trivially inconsistent* in this case. For good hash keys, if $x_i = x_j$ (or $u_i = u_j$) then we always have $y_i = y_j$ (res. $v_i = v_j$); hence the inconsistency won't arise. So, given that the hash key is good, we say that ω is *sampling-induced* bad transcript, if one of the following conditions is true:
for some $\alpha \in [4]$ and $\beta \in \{\alpha, \ldots, 4\}$, we have

- $\mathsf{Ycoll}_{\alpha\beta}$: $\exists i \in \mathscr{I}_\alpha, j \in \mathscr{I}_\beta$, such that $x_i \neq x_j \wedge y_i = y_j$, and
- $\mathsf{Vcoll}_{\alpha\beta}$: $\exists i \in \mathscr{I}_\alpha, j \in \mathscr{I}_\beta$, such that $u_i \neq u_j \wedge v_i = v_j$,

2 We use the notation H_i to denote the event that the predicate H_i is true.

where $\mathscr{I}_i$ is defined as before in section 15.2.2.1. By varying α and β over all possible values, we get all 30 conditions which might lead to $x^q \not\leftrightarrow y^q$ or $u^q \not\leftrightarrow v^q$. Here we remark that some of these 30 conditions are never satisfied due to the sampling mechanism prescribed in section 15.2.2.1. These are Ycoll_{11}, Ycoll_{12}, Ycoll_{13}, Ycoll_{22}, Ycoll_{23}, Ycoll_{33}, Vcoll_{11}, Vcoll_{12}, Vcoll_{13}, Vcoll_{22}, Vcoll_{23}, and Vcoll_{33}. We listed them here only for the sake of completeness. We write the combined event that one of the 30 conditions hold as BAD2. Again by an abuse of notations, we have

$$\mathsf{BAD2} = \bigcup_{\alpha\in[4],\beta\in\{\alpha,\ldots,4\}} (\mathsf{Ycoll}_{\alpha\beta} \cup \mathsf{Vcoll}_{\alpha\beta}) \,. \tag{15.21}$$

Finally, a transcript ω is called bad, i.e. $\omega \in \Omega_{\mathsf{bad}}$, if it is either a hash-induced or a sampling-induced bad transcript. All other transcripts are called good. It is easy to see that all good transcripts are attainable (as required in the H-coefficient technique or the expectation method).

BAD TRANSCRIPT ANALYSIS: We analyze the probability of realizing a bad transcript in the ideal world. By definition, this is possible if and only if one of BAD1 or BAD2 occurs. So, we have

$$\begin{aligned}\epsilon_{\mathsf{bad}} = \Pr\left(\Theta_0 \in \Omega_{\mathsf{bad}}\right) &= \Pr_{\Theta_0}\left(\mathsf{BAD1} \cup \mathsf{BAD2}\right) \\ &\leq \underbrace{\Pr_{\Theta_0}\left(\mathsf{BAD1}\right)}_{\epsilon_{\mathsf{h}}} + \underbrace{\Pr_{\Theta_0}\left(\mathsf{BAD2}\right)}_{\epsilon_{\mathsf{s}}} .\end{aligned} \tag{15.22}$$

Lemma 15.2 upper bounds ϵ_{h} to $q^2\epsilon_1^2 + q^2\epsilon_1\epsilon_2 + 2q^2\epsilon_1^{1.5} + 16q^4\epsilon_1 2^{-2n}$ and Lemma 15.3 upper bounds ϵ_{s} to $4q^4\epsilon_1^2 2^{-n}$. Substituting these values in (15.22), we get

$$\epsilon_{\mathsf{bad}} \leq q^2\epsilon_1^2 + q^2\epsilon_1\epsilon_2 + 2q^2\epsilon_1^{1.5} + \frac{16q^4\epsilon_1}{2^{2n}} + \frac{4q^4\epsilon_1^2}{2^n}. \tag{15.23}$$

Lemma 15.2. $\epsilon_{\mathsf{h}} \leq q^2\epsilon_1^2 + q^2\epsilon_1\epsilon_2 + 2q^2\epsilon_1^{1.5} + \dfrac{16q^4\epsilon_1}{2^{2n}}$.

Proof. Using (15.20) and (15.22), we have

$$\epsilon_{\mathsf{h}} = \Pr\left(\mathsf{H}_1 \cup \mathsf{H}_2 \cup \mathsf{H}_3 \cup \mathsf{H}_4 \cup \mathsf{H}_5 \cup \mathsf{H}_6 \cup \mathsf{H}_7\right) \leq \sum_{i=1}^{7} \Pr\left(\mathsf{H}_i\right).$$

H_1 is true if for some distinct i, j both $\mathsf{X}_i = \mathsf{X}_j$, and $\mathsf{U}_i = \mathsf{U}_j$. Now $\mathsf{T}_i = \mathsf{T}_j \implies \mathsf{M}_i \neq \mathsf{M}_j$. Hence $\mathsf{X}_i \neq \mathsf{X}_j$ (since $\widetilde{\mathbf{H}}_1$ is a tweakable permutation) and H_1 is not true. So suppose $\mathsf{T}_i \neq \mathsf{T}_j$. Then, using the fact that $\widetilde{\mathscr{H}}$ is an ϵ-AUHF and KG is a PISM, for a fixed i, j we get an upper bound of ϵ_1^2. Furthermore, we have at most $\binom{q}{2}$ pairs of (i, j). Thus, $\Pr\left(\mathsf{H}_1\right) \leq \binom{q}{2}\epsilon_1^2$.

Following a similar line of argument one can bound $\Pr(\mathsf{H}_2) \leq \binom{q}{2}\epsilon_1\epsilon_2$ and $\Pr(\mathsf{H}_3) \leq \binom{q}{2}\epsilon_1\epsilon_2$.

In the remaining, we bound the probability of H_4 and H_6, while the probability of H_5 and H_7 can be bounded analogously. Now, H_4 is true if for some pairwise distinct i, j, k, ℓ,

$$\widetilde{\mathbf{H}}_1(\mathsf{T}_i, \mathsf{M}_i) = \widetilde{\mathbf{H}}_1(\mathsf{T}_j, \mathsf{M}_j), \;\; \widetilde{\mathbf{H}}_2(\mathsf{T}_j, \mathsf{C}_j) = \widetilde{\mathbf{H}}_2(\mathsf{T}_k, \mathsf{C}_k), \;\; \widetilde{\mathbf{H}}_1(\mathsf{T}_k, \mathsf{M}_k) = \widetilde{\mathbf{H}}_1(\mathsf{T}_\ell, \mathsf{M}_\ell).$$

Again, using the fact that KG is a PISM, we have that the second equation is independent of the other two equations. Using Lemma A.4, we have

$$\Pr(\mathsf{H}_4) \leq q^2\epsilon_1^{1.5}.$$

For H_6, for some $i_1, \ldots, i_k$, we have

$$\mathsf{X}_{i_1} = \mathsf{X}_{i_2} = \cdots = \mathsf{X}_{i_k},$$

where $k \geq 2^n/2q$. Since, $(t_{i_j}, m_{i_j}) \neq (t_{i_l}, m_{i_l})$ for all $j \neq l$, we can apply Corollary A.6.1 to get

$$\Pr(\mathsf{H}_6) \leq \frac{8q^4\epsilon_1}{2^{2n}}.$$

□

Lemma 15.3. $\epsilon_{\mathsf{s}} \leq \dfrac{4q^4\epsilon_1^2}{2^n}$.

Proof. Using (15.21) and (15.22), we have

$$\begin{aligned}\epsilon_{\mathsf{s}} &= \Pr\left(\bigcup_{\alpha\in[4],\beta\in\{\alpha,\ldots,4\}} (\mathsf{Ycoll}_{\alpha\beta} \cup \mathsf{Vcoll}_{\alpha\beta})\right) \\ &\leq \sum_{\alpha\in[4]} \sum_{\beta\in\{\alpha,\ldots,4\}} \left(\Pr(\mathsf{Ycoll}_{\alpha\beta}) + \Pr(\mathsf{Vcoll}_{\alpha\beta})\right).\end{aligned}$$

We bound the probabilities of the events on the right hand side in groups as given below:

1. Bounding $\sum_{\alpha\in[3],\beta\in\{\alpha,\ldots,3\}} \Pr(\mathsf{Ycoll}_{\alpha\beta}) + \Pr(\mathsf{Vcoll}_{\alpha\beta})$: Recall that the sampling of Y and V values is always done consistently for indices belonging to $\mathscr{I} = \mathscr{I}_1 \sqcup \mathscr{I}_2 \sqcup \mathscr{I}_3$. Hence,

$$\sum_{\alpha\in[3],\beta\in\{\alpha,\ldots,3\}} \Pr(\mathsf{Ycoll}_{\alpha\beta}) + \Pr(\mathsf{Vcoll}_{\alpha\beta}) = 0, \tag{15.24}$$

2. Bounding $\sum_{\alpha\in[3]} \Pr(\mathsf{Ycoll}_{\alpha 4}) + \Pr(\mathsf{Vcoll}_{\alpha 4})$: Let's consider the event Ycoll_{14}, which translates to there exist indices $i \in \mathscr{I}_1$ and $j \in \mathscr{I}_4$ such that $\mathsf{X}_i \neq \mathsf{X}_j \wedge \mathsf{Y}_i = \mathsf{Y}_j$. Since $j \in \mathscr{I}_4$, there must exist $k, \ell \in \mathscr{I}_4 \setminus \{j\}$, such that one of the following happens

$$\mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell$$

$$\mathsf{U}_j = \mathsf{U}_k \wedge \mathsf{X}_k = \mathsf{X}_\ell$$
$$\mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_j = \mathsf{U}_\ell.$$

We analyze the first case, while the other two cases can be similarly bounded. To bound the probability of Ycoll_{14}, we can look at the joint event

$$\mathsf{E}: \ \exists i \in \mathscr{I}_1, \exists^* j,k,\ell \in \mathscr{I}_4, \text{ such that } \mathsf{Y}_i = \mathsf{Y}_j \wedge \mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell.$$

Note that the event $\mathsf{Y}_i = \mathsf{Y}_j$ occurs with exactly 2^{-n} probability conditioned on the event $\mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell$. Thus, we get

$$\begin{aligned}\Pr(\mathsf{E}) &= \Pr\left(\exists i \in \mathscr{I}_1, \exists^* j,k,\ell \in \mathscr{I}_4, \text{ such that } \mathsf{Y}_i = \mathsf{Y}_j \wedge \mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell\right) \\ &\le \sum_{i \in \mathscr{I}_1} \sum_{j<k<\ell \in \mathscr{I}_4} \Pr\left(\mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell\right) \times \Pr\left(\mathsf{Y}_i = \mathsf{Y}_j \mid \mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell\right) \\ &\le q\binom{q}{3}\frac{\epsilon_1^2}{2^n},\end{aligned}$$

where the last inequality follows from the AUHF property of $\widetilde{\mathscr{H}}$, the PISM property of KG, and the uniform randomness of Y_j. The probability of the other two cases are identically bounded, whence we get

$$\Pr\left(\mathsf{Ycoll}_{14}\right) \le 3q\binom{q}{3}\frac{\epsilon_1^2}{2^n}.$$

We can bound the probabilities of Ycoll_{24}, Ycoll_{34}, and $\mathsf{Vcoll}_{\alpha 4}$ for all $\alpha \in [3]$ in a similar manner. So, we skip the argumentation for these cases, and summarize the probability for this group as

$$\sum_{\alpha \in [3]} \Pr\left(\mathsf{Ycoll}_{\alpha 4}\right) + \Pr\left(\mathsf{Vcoll}_{\alpha 4}\right) \le \frac{3q^4\epsilon_1^2}{2^n}. \tag{15.25}$$

3. Bounding $\Pr\left(\mathsf{Ycoll}_{44}\right) + \Pr\left(\mathsf{Vcoll}_{44}\right)$: Consider the event Ycoll_{44}, which translates to there exists distinct indices $i, j \in \mathscr{I}_4$ such that $\mathsf{X}_i \neq \mathsf{X}_j \wedge \mathsf{Y}_i = \mathsf{Y}_j$. Here as $i, j \in \mathscr{I}_4$, there must exist $k, \ell \in \mathscr{I}_4 \setminus \{j\}$ such that one of the following happens

$$\mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_k = \mathsf{U}_\ell$$
$$\mathsf{U}_j = \mathsf{U}_k \wedge \mathsf{X}_k = \mathsf{X}_\ell$$
$$\mathsf{X}_j = \mathsf{X}_k \wedge \mathsf{U}_j = \mathsf{U}_\ell.$$

The analysis of these cases is similar to 2 above. So, we skip it and provide the final bound

$$\Pr\left(\mathsf{Ycoll}_{44}\right) \le 3q\binom{q}{3}\frac{\epsilon_1^2}{2^n}.$$

The probability of Vcoll_{44} can be bounded in a similar fashion.

$$\Pr\left(\mathsf{Ycoll}_{44}\right) + \Pr\left(\mathsf{Vcoll}_{44}\right) \leq \frac{q^4\epsilon_1^2}{2^n}. \tag{15.26}$$

The result follows by combining (15.24)-(15.26), followed by some simplifications. □

15.2.2.3 *Good Transcript Analysis*

From section 15.2.2.1, we know the types of components present in the transcript graph corresponding to a good transcript ω are exactly as in Figure 15.4. Let $\omega = (t^q, m^q, c^q, x^q, y^q, v^q, u^q, \lambda^q, \widetilde{h}_1, \widetilde{h}_2, h)$ be the good transcript at hand. From the bad transcript description of section 15.2.2.2, we know that for a good transcript $m^q \overset{t^q}{\leftrightarrow} c^q$, $x^q \leftrightarrow y^q$, $v^q \leftrightarrow u^q$, and $y^q \oplus v^q = \lambda^q$.

First, we add some new parameters with respect to ω to aid the remaining analysis.

For $i \in [4]$, let $c_i(\omega)$ and $q_i(\omega)$ respectively denote the number of components and the number of indices (corresponding to the edges) of type-i in ω. Further, let $z_i^1(\omega)$ and $z_i^2(\omega)$ respectively denote the number of vertices from A and B in type-i components. Note that

- $z_1^1(\omega) = z_1^2(\omega) = q_1(\omega) = c_1(\omega)$;
- $z_2^1(\omega) = c_2(\omega)$, and $z_2^2(\omega) = q_2(\omega) \geq 2c_2(\omega)$;
- $z_3^2(\omega) = c_3(\omega)$, and $z_3^1(\omega) = q_3(\omega) \geq 2c_3(\omega)$; and
- $z_4^b(\omega) \geq 2c_4(\omega)$, for $b \in \{1, 2\}$, and $z_4^1 + z_4^2 = q_4 - c_4$.

In addition, for a good transcript $q = \sum_{i=1}^5 q_i(\omega)$. For notational convenience, let $p_1 := z_1^1 + z_2^1 + z_3^1 = c_1 + c_2 + q_3$ and $p_2 := z_1^2 + z_2^2 + z_3^2 = c_1 + q_2 + c_3$.

Let t^q be associated with the multiplicity vector $(\mu_1, \ldots, \mu_d)$ and $t^{\mathscr{J}}$ be associated with the multiplicity vector $(\mu'_1, \ldots, \mu'_d)$. We must have $d \leq q$ and $\sum_{i=d}^d \mu_i = q$ while $\sum_{i=d}^d \mu'_i = |\mathscr{J}|$.

Let $\Lambda^{\mathscr{J}}$ be associated with the multiplicity vector $(\nu_1, \ldots, \nu_{d'})$. Here we have $d' \leq |\mathscr{J}|$ and $\sum_{i=1}^{d'} \nu_i = |\mathscr{J}|$.

For all these parameters, we will drop the ω qualification whenever it is understood from the context.

INTERPOLATION PROBABILITY FOR THE REAL ORACLE: In the real oracle, $\widehat{\mathbf{H}} \leftarrow \mathsf{KG}\left(\widehat{\mathscr{H}}\right)$, $\boldsymbol{\pi}_1$ is called exactly $p_1 + z_4^1$ times and $\boldsymbol{\pi}_2$ is called exactly $p_2 + z_4^2$ times. Thus, we have

$$\Pr\left(\Theta_1 = \omega\right) = \Pr_{\mathsf{KG}}\left(\widehat{\mathbf{H}} = \widehat{h}\right) \times \frac{1}{(2^n)_{p_1+z_4^1}} \times \frac{1}{(2^n)_{p_2+z_4^2}}. \tag{15.27}$$

INTERPOLATION PROBABILITY FOR THE IDEAL ORACLE: In the ideal oracle, the sampling is done in parts:

I. $\widetilde{\boldsymbol{\pi}}$ *sampling*: We have

$$\Pr\left(\widetilde{\boldsymbol{\pi}}(t^q, m^q) = c^q\right) \leq \frac{1}{\prod_{i=1}^{d}(2^n)_{\mu_i}}.$$

II. *Hash key sampling*: This is identical to the real world, and simply given by $\Pr_{\mathsf{KG}}\left(\widehat{\mathbf{H}} = \widehat{h}\right)$.

III. *Internal variables sampling*: The internal variables Y^q and V^q are sampled in two stages.

(A). *type*-1, *type*-2 *and type*-3 *sampling*: Recall the sets $\mathscr{I}_1$, $\mathscr{I}_2$, and $\mathscr{I}_3$, from section 15.2.2.2. Consider the system of equations,

$$\mathscr{E} = \{\mathsf{Y}_i \oplus \mathsf{V}_i = \lambda_i \ : \ i \in \mathscr{I}\}.$$

From Figure 15.4 we know that the graph corresponding to $\mathscr{E}$ is a bipartite star graph with parameters $(c_1, c_2, c_3, q_2, q_3, \xi_{\max})$, with $\xi_{\max} \leq 2^n/2q$, since the transcript is good. So, we can apply Theorem 9.1 to get a lower bound on the number of valid solutions for $\mathscr{E}$. Using the fact that $(\mathsf{Y}^{\mathscr{I}}, \mathsf{V}^{\mathscr{I}}) \xleftarrow{*} \mathscr{S}(\mathscr{L})$, and Theorem 9.1, we have

$$\Pr\left((\mathsf{Y}^{\mathscr{I}}, \mathsf{V}^{\mathscr{I}}) = (y^{\mathscr{I}}, v^{\mathscr{I}})\right) \leq \frac{\prod_{i=1}^{d'}(2^n)_{\nu_i}}{\zeta(\omega)(2^n)_{p_1}(2^n)_{p_2}},$$

where

$$\zeta(\omega) \geq \left(1 - \frac{13q^4}{2^{3n}} - \frac{2q^2}{2^{2n}} - \left(\sum_{i=1}^{c_2+c_3} \eta_{c_1+i}^2\right)\frac{4q^2}{2^{2n}}\right),$$

and η_i denotes the number of edges in the i-th component for all $i \in [c_1 + c_2 + c_3]$.

(B). *type*-4 *sampling*: For the remaining indices, one value is sampled uniformly for each of the components, i.e., we have

$$\Pr\left(\left(\mathsf{Y}^{[q]\setminus\mathscr{I}}, \mathsf{V}^{[q]\setminus\mathscr{I}}\right) = \left(y^{[q]\setminus\mathscr{I}}, v^{[q]\setminus\mathscr{I}}\right)\right) = \frac{1}{2^{nc_4}}.$$

By combining I, II, III, and rearranging the terms, we have

$$\Pr\left(\mathsf{\Theta}_0 = \omega\right) \leq \Pr_{\mathsf{KG}}\left(\widehat{\mathbf{H}} = \widehat{h}\right) \times \frac{1}{\zeta(\omega)} \times \frac{\prod_{i=1}^{d'}(2^n)_{\nu_i}}{\prod_{i=1}^{d}(2^n)_{\mu_i}(2^n)_{p_1}(2^n)_{p_2}2^{nc_4}}. \tag{15.28}$$

15.2.2.4 *Ratio of Interpolation Probabilities*

On dividing (15.27) by (15.28), and simplifying the expression, we get

$$\begin{aligned}\frac{\Pr\left(\Theta_1=\omega\right)}{\Pr\left(\Theta_0=\omega\right)} &\geq \zeta(\omega)\cdot\frac{\prod_{i=1}^{d}(2^n)_{\mu_i}}{\prod_{i=1}^{d'}(2^n)_{\nu_i}(2^n-p_1-c_4)_{z_4^1-c_4}(2^n-p_2)_{z_4^2}}\\ &\overset{1}{\geq} \zeta(\omega)\cdot\frac{\prod_{i=1}^{d}(2^n)_{\mu'_i}\prod_{i=1}^{d}(2^n-\mu'_i)_{\mu_i-\mu'_i}}{\prod_{i=1}^{d'}(2^n)_{\nu_i}(2^n-p_1-c_4)_{z_4^1-c_4}(2^n-p_2)_{z_4^2}}\\ &\overset{2}{\geq} \zeta(\omega)\cdot\frac{\prod_{i=1}^{d}(2^n-\mu'_i)_{\mu_i-\mu'_i}}{(2^n-p_1-c_4)_{z_4^1-c_4}(2^n-p_2)_{z_4^2}}\Bigg\}A\\ &\overset{3}{\geq} \zeta(\omega).\end{aligned} \tag{15.29}$$

At inequality 1, we simply rewrite the numerator. Further, $r \geq s$, as number of distinct internal masking values is at most the number of distinct tweaks, and $\{t^{\mathcal{J}}\}$ compresses to $\{\lambda^{\mathcal{J}}\}$. So, using Proposition A.3, we can justify inequality 2. At inequality 2, for $i \in \{2,3,4\}$, $c_i(\omega) > 0$ if and only if $r \geq 2$. Also, $\mu'_i \leq c_1+c_2+c_3 \leq p_1 \leq p_1+c_4$ and similarly $\mu'_i \leq p_2$ for all $i \in [r]$. Furthermore, $\mu_i \leq c_1+c_2+c_3+2c_4 \leq p_1+z_4^1$, and similarly $\mu_i \leq p_2+z_4^2$. Also, $\sum_{i=1}^{d}\mu_i-\mu'_i = q_4 = z_4^1+z_4^2-c_4$. Thus, A satisfies the conditions laid out in Proposition A.4, and hence $A \geq 1$. This justifies inequality 3.

We define $\epsilon_{\mathsf{ratio}} : \Omega \to [0,\infty)$ by the mapping

$$\epsilon_{\mathsf{ratio}}(\omega) = 1-\zeta(\omega).$$

Clearly $\epsilon_{\mathsf{ratio}}$ is non-negative and the ratio of real to ideal interpolation probabilities is at least $1-\epsilon_{\mathsf{ratio}}(\omega)$ (using (15.29)). Thus, we can use the expectation method (Theorem 3.1) to get

$$\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{LRW+}}(q)(q) \leq \frac{2q^2}{2^{2n}}+\frac{13q^4}{2^{3n}}+\frac{4q^2}{2^{2n}}\mathbb{E}\left(\sum_{i=1}^{c_2+c_3}\eta^2_{c_1+i}\right)+\epsilon_{\mathsf{bad}}. \tag{15.30}$$

Let $\sim_1$ (res. $\sim_2$) be an equivalence relation over $[q]$, such that $\alpha \sim_1 \beta$ (res. $\alpha \sim_2 \beta$) if and only if $\mathsf{X}_\alpha = \mathsf{X}_\beta$ (res. $\mathsf{U}_\alpha = \mathsf{U}_\beta$). Now, each η_i random variable denotes the cardinality of some non-singleton equivalence class of $[q]$ with respect to either $\sim_1$ or $\sim_2$. Let $\mathscr{P}^1_1,\ldots,\mathscr{P}^1_k$ and $\mathscr{P}^2_1,\ldots,\mathscr{P}^2_{k'}$ denote the non-singleton equivalence classes of $[q]$ with respect to $\sim_1$ and $\sim_2$, respectively. Further, for $j \in [k]$ and $j' \in [k']$, let $\mathtt{n}_j = |\mathscr{P}^1_j|$ and $\mathtt{m}_{j'} = |\mathscr{P}^2_{j'}|$. Then, we have

$$\begin{aligned}\mathbb{E}\left(\sum_{i=1}^{c_2+c_3}\eta^2_{c_1+i}\right) &\leq \mathbb{E}\left(\sum_{j=1}^{k}\mathtt{n}_j^2\right)+\mathbb{E}\left(\sum_{j'=1}^{k'}\mathtt{m}^2_{k'}\right)\\ &\leq 4q^2\epsilon_1.\end{aligned} \tag{15.31}$$

where the first inequality follows from linearity, and the second inequality follows from Lemma A.6. Theorem 15.3 then follows from (15.23), (15.30), and (15.31). □

16

SUM OF r EVEN-MANSOUR:
APPLICATION OF RPRMTP*, THEOREM 11.1*

In thus chapter, we consider the sum of r Even-Mansour ciphers, defined as $\mathsf{SOEM}^r_{\boldsymbol{\pi}_1,\ldots,\boldsymbol{\pi}_r}(\mathsf{K}_1,\ldots,\mathsf{K}_r,m) := \bigoplus_{i\in[r]} \boldsymbol{\pi}_i(\mathsf{K}_i \oplus m)$, where $\boldsymbol{\pi}_i$ are independent random permutations. We show using Theorem 11.1 that this public permutation-based construction achieves $rn/(r+1)$-bit PRF security in the presence of adversaries making total p queries to the public permutations in the offline phase, and q queries to the construction oracle in the online phase.

SUM OF r EVEN-MANSOUR. For any $r \geq 2$, let $(\pi_1,\ldots,\pi_r) \xleftarrow{*} \mathsf{Perm}(n)^r$ be a tuple of r permutations of $\{0,1\}^n$ and let $(K_1,\ldots,K_r) \in (\{0,1\}^n)^r$ be a r-tuple of n-bit strings.

One-round Even-Mansour construction is a keyed permutation of $\{0,1\}^n$ defined by the mapping

$$x \longmapsto \pi_1(x \oplus K_1) \oplus K_1,$$

where K_1 denotes the key.

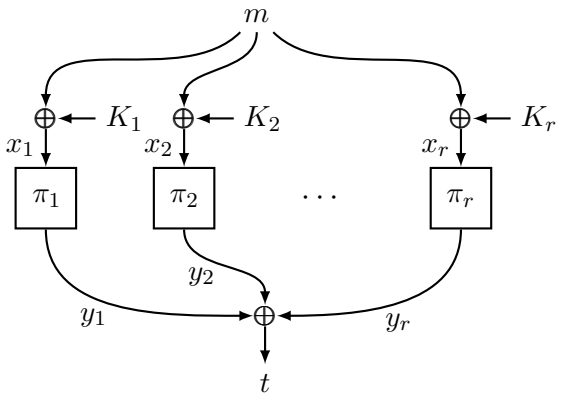


Figure 16.1: The π-SOEM^r construction instantiated with key $K = (K_1,\ldots,K_r)$.

The r-sum of Even-Mansour construction, π-SOEM^r is a length-preserving keyed function of $\{0,1\}^n$ defined by the mapping

$$x \longmapsto \bigoplus_{i=1}^{r} \pi_i(x \oplus K_i),$$

where $K = (K_1, \ldots, K_r)$ denotes the key. See Figure 16.1 for a pictorial illustration. Notice that we skipped the post-permutation key masking. This is motivated by a similar simplification [ST23] by Sibleyras and Todo who studied the $r = 2$ case. Thus, we study the same problem for any arbitrary $r \geq 2$.

Theorem 16.2. *Fix some $r \geq 2$, $q + p \leq 2^{\frac{r}{r+1}n - \log_2(n)}$, and $\boldsymbol{\pi} = (\boldsymbol{\pi}_1, \ldots, \boldsymbol{\pi}_r) \xleftarrow{*} \mathsf{Perm}(n)^r$. Then*

$$\boldsymbol{Adv}^{\mathrm{prf}}_{\boldsymbol{\pi}\text{-}\mathsf{SOEM}^r}(p, q) \leq \frac{1}{2^n} + \frac{16nq(2p)^{r-2}}{2^{n(r-1)}} + \frac{20\sqrt{nq}(2p+2q)^{r-1}}{2^{n(r-1)}} + \frac{10q(2p+2q)^r}{2^{nr}}.$$

Proof. For the purpose of this proof let $\mathsf{F}_{\mathsf{K}}(\cdot) = \boldsymbol{\pi}\text{-}\mathsf{SOEM}^r_{\mathsf{K}}(\cdot)$, and let $\boldsymbol{\rho} \xleftarrow{*} \{0,1\}^n$. $\mathscr{A}$'s goal is to distinguish between the *real* oracle $(\mathsf{F}_{\mathsf{K}}, \boldsymbol{\pi}^{\pm})$ and the *ideal* oracle $(\boldsymbol{\rho}, \boldsymbol{\pi}^{\pm})$, where F_{K} and $\boldsymbol{\rho}$ are referred as the construction oracle and $\boldsymbol{\pi}^{\pm}$ is referred as the primitive oracle. Fix a (q, p)-distinguisher $\mathscr{A}$. Let

- $(\mathsf{M}^i, \mathsf{T}^i)$ denote the i-th query-response tuple corresponding to the construction oracle. Let $\mathsf{M} := \{\mathsf{M}^i : i \in [q]\}$ and $\mathsf{T} := \{\mathsf{T}^i : i \in [q]\}$.
- $(\mathsf{U}^i_j, \mathsf{V}^i_j)$ denote the i-th query-response tuple corresponding to the permutation $\boldsymbol{\pi}_j$. Unless stated otherwise, we assume that all these queries are in the forward direction. Let $\mathsf{U}_j := \{\mathsf{U}^i_j : i \in [p]\}$, $\mathsf{V}_j := \{\mathsf{V}^i_j : i \in [p]\}$, $\mathsf{U} := (\mathsf{U}_1, \ldots, \mathsf{U}_r)$, and $\mathsf{V} := (\mathsf{V}_1, \ldots, \mathsf{V}_r)$.
- $(\mathsf{X}^i_j, \mathsf{Y}^i_j)$ denote the input-output tuple to the j-th permutation, for all $j \in [r]$, within the i-th construction query in the real world, i.e., $\mathsf{X}^i_j = \mathsf{M}^i \oplus \mathsf{K}_j$. Let $\mathsf{X}^i := (\mathsf{X}^i_j : j \in [r])$ and $\mathsf{Y}^i := (\mathsf{Y}^i_j : j \in [r])$. Let $\mathsf{X} := \{\mathsf{X}^i : i \in [q]\}$ and $\mathsf{Y} := \{\mathsf{Y}^i : i \in [q]\}$.

We study a modified game where the real oracle releases (X, Y) to $\mathscr{A}$ once the query-response phase is over, but before $\mathscr{A}$ outputs. This obviously does not decrease $\mathscr{A}$'s advantage.

IDEAL WORLD TRANSCRIPT EXTENSION: Naturally, in the ideal world, the sampling is extended to generate this additional information. Let us define the set

$$\mathscr{SC}(\mathsf{T}, \mathsf{V}) := \left\{ (i, j_1, j_2 \ldots, j_r) \in [q] \times [p]^r : \bigoplus_{k=1}^{r} \mathsf{V}^{j_k}_k = \mathsf{T}^i \right\}$$

such that $\mu(\mathsf{T}, \mathsf{V}) = |\mathscr{SC}(\mathsf{T}, \mathsf{V})|$. We define the predicate

$$\mathsf{LSC}(\mathsf{T}, \mathsf{V}) := \left(\mu(\mathsf{T}, \mathsf{V}) > \frac{q(ep)^r}{2^n} + 12(ep)^{r-1}\sqrt{nq} \right).$$

The subsequent two-step sampling mechanism for (X, Y) in the ideal world is defined under the condition that $\neg\mathsf{LSC}(\mathsf{T}, \mathsf{V})$ holds:

1. In the first step, a dummy key tuple is sampled uniformly at random, i.e., $\mathsf{K} \xleftarrow{*} (\{0,1\}^n)^r$, which determines $\mathsf{X}^i_j := \mathsf{M}^i \oplus \mathsf{K}_j$. Consider the following predicates:

$$\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K}) : \exists\, i \in [q],\, j_1,\ldots,j_r \in [p] \text{ such that } \left(\forall k \in [r],\, \mathsf{X}^i_k = \mathsf{U}^{j_k}_k\right)$$
$$\mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}) : \exists\, (i,j_1,j_2,\ldots,j_r) \in \mathscr{SC}(\mathsf{T},\mathsf{V}),\, k \in [r], \text{ such that}$$
$$(\mathsf{X}^i_k \neq \mathsf{U}^{j_k}_k) \text{ and } \left(\forall k' \neq k,\, \mathsf{X}^i_{k'} = \mathsf{U}^{j_{k'}}_{k'}\right)$$

   Going forward we assume that $\neg(\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K}) \vee \mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}))$ holds. For each $i \in [q]$:

   a) if there exists $j \in [p]$ and $k \in [r]$, such that $\mathsf{X}^i_k = \mathsf{U}^j_k$, then define $\mathsf{Y}^i_k := \mathsf{V}^j_k$;

   b) let $\mathscr{I}_i = \{j \in [r] : \mathsf{X}^i_j \notin \mathsf{U}_j\}$ to be the set of permutation indices with fresh input for the i-th construction query.

   c) let $\sim$ be a relation on $[q]$ defined as: $i_1 \sim i_2 \iff \mathscr{I}_{i_1} = \mathscr{I}_{i_2}$. Clearly, $\sim$ is an equivalence relation. Let $\mathscr{Q}^{(1)}_{(0)} \sqcup \ldots \mathscr{Q}^{(r)}_{(0)} \sqcup \mathscr{Q}_{(1)} \sqcup \ldots \sqcup \mathscr{Q}_{(c)}$ denote the corresponding partitioning of $[q]$, where $\mathscr{Q}^{(j)}_{(0)} = \{i \in [q] : \mathscr{I}_i = \{j\}\}$, i. e., all queries for which exactly one of the permutations have fresh input. Let $|\mathscr{Q}^{(j)}_{(0)}| = q^{(j)}_0$, $q_0 := \sum_{j\in[r]} q^{(j)}_0$ and $|\mathscr{Q}_{(i)}| = q_i$. Then $q_0 + \sum_{i\in[c]} q_i = q$.

   d) for all $j \in [r]$ and $i \in \mathscr{Q}^{(j)}_{(0)}$, define $\mathsf{Y}^i_j := \bigoplus_{l\in[r]\setminus j} \mathsf{Y}^i_l \oplus \mathsf{T}^i$ and

$$\mathsf{Y}^{(0)} = \left\{ \mathsf{Y}^i_j \oplus \bigoplus_{l\in[r]\setminus j} \mathsf{Y}^i_l \oplus \mathsf{T}^i \;:\; j \in [r], i \in \mathscr{Q}^{(j)}_{(0)} \right\}.$$

   This concludes the first step. We encourage the readers to verify that at the end of this step Y^i_j is undefined for exactly the indices in $\mathscr{I}_i$ and $|\mathscr{I}_i| \geq 2$. Furthermore, due to $\neg(\mathsf{KG}(\mathsf{MU},\mathsf{K}) \vee \mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}))$, the partially defined (X,Y) is permutation-consistent.

2. In the second step we formulate a RPRMTP problem with the yet unsampled input-output variables of the random permutations and sample from the solution space of this problem.

   RPRMTP *formulation:* For each $i \in [c]$, let $\mathscr{I}_{(i)} = \{j_1,\ldots,j_{t_i}\}$ denote the set of permutation indices with fresh input for the i-th equivalence class $\mathscr{Q}_{(i)}$. Let $r_i = q_i t_i$.

   Now we define the RPRMTP problem instantiated by

- an acyclic $\mathbf{A}$ with component form

$$\mathbf{A}|\boldsymbol{\lambda} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_c & \boldsymbol{\lambda}_c \end{pmatrix}.$$

  with $\overline{\mathbf{A}}_i \in \mathbb{F}_2^{q_i \times r_i}, \boldsymbol{\lambda}_i \in (\mathbb{F}_2^m)^{q_i \times 1}$. Where the i-th component $\overline{\mathbf{A}}_i|\boldsymbol{\lambda}_i$ is the augmented coefficient-constant matrix of the system of equations:

$$\mathscr{E}_i = \left\{ \bigoplus_{k \in \mathscr{J}_{(i)}} \mathsf{Y}_k^j = \mathsf{T}^j \bigoplus_{k' \in [r] \setminus \mathscr{J}_{(i)}} \mathsf{Y}_{k'}^j \right\}_{j \in \mathscr{Q}_{(i)}}$$

  In particular, $\overline{\mathbf{A}}_i$ is t_i-regular, isolated.
- The equivalence relation $\simeq$ over $[r]$ that induces a partition $(P_1, \ldots, P_r)$ of $[r]$, with respect to which $\mathbf{A}$ is partite.
- family of restricted sets $\mathsf{V} = \{\mathsf{V}_j\}_{j \in [r]}$, with $|\mathsf{V}_j| = p$ for all $j \in [r]$.

3. In the second step, we sample a solution for each of the c constrained systems. Now, for the i-th component:
   - let $F_{\le i-1}^{[j]} = \mathsf{V}_j \cup \{\mathsf{Y}_j^k \ : \ k \in \mathscr{Q}_{(0)}^{(j)}\} \cup \{\mathsf{Y}_j^k \ : \ k \in \mathscr{Q}_{(1)} \sqcup \ldots \sqcup \mathscr{Q}_{(i-1)}\}$, for all $j \in [r]$, and let $|F_{\le i-1}^{[j]}| = f_{\le i-1}^{(j)} \le p + q$,
   - let $\mathscr{F}_{\le i-1} = \{F_{\le i-1}^{[j]} \ : \ j \in \mathscr{J}_{(i)}\}$, and $\widehat{\mathscr{F}}_{\le i-1} = (F_{\le i-1}^{[j]} \ : \ j \in \mathscr{J}_{(i)})$
   - let $\mathsf{T}^{(i)} = (\mathsf{T}^k \bigoplus_{j \in [r] \setminus \mathscr{J}_{(i)}} \mathsf{Y}_j^k \ : \ k \in \mathscr{Q}_{(i)})$. Then, $|\mathsf{T}^{(i)}| \le q_i$.
   - let $\mathsf{Y}^{(i)} = \{\mathsf{Y}_j^k \ : \ k \in \mathscr{Q}_{(i)}, j \in \mathscr{J}_{(i)}\}$. Then, $|\mathsf{Y}^{(i)}| = r_i$.

   We sample $\mathsf{Y}^{(i)} \xleftarrow{*} \mathscr{S}(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}_{\le i-1})$, where using Theorem 11.1, we have

$$N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}_{\le i-1}) \ge \frac{\prod_{j \in \mathscr{J}_{(i)}} (2^n - f_{\le i-1}^{(j)})_{q_i}}{2^{nq_i}} \left(1 - \varepsilon^{(i)}\right) \tag{16.1}$$

$$\varepsilon^{(i)} \le \frac{2\mu(\mathsf{T}^{(i)}, \mathscr{F}_{\le i-1})}{2^{n(t_i-1)}} + \frac{2q_i \Delta_{\boldsymbol{\lambda}_{\le i-1}}}{2^{n(t_i-1)}} + \frac{6q_i(p+q)^{t_i}}{2^{nt_i}} \tag{16.2}$$

   Since the solution for each system is sampled in a consistent manner given a consistent solution for the previous system, the cumulative sampling is also permutation-compatible. This completes the second step.

At this stage the full transcript in the ideal world, i.e., $\mathtt{\Theta}_0 = (\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}, \mathsf{Y})$ is fully determined.

Some Notations on Transcripts: For any $\mathrm{wo} \in \{\mathrm{re}, \mathrm{id}\}$, and $\mathtt{\Theta}_{\mathrm{wo}} = (\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}, \mathsf{Y})$, let:

- $\Theta_{\mathrm{wo}}^{\mathsf{key}}$ denote the restriction of Θ_{wo} to the key K,
- $\Theta_{\mathrm{wo}}^{\mathsf{con}}$ denote the restriction of Θ_{wo} to the construction query-response tuple (M, T),
- $\Theta_{\mathrm{wo}}^{\mathsf{prim}}$ denote the restriction of Θ_{wo} to the key (U, V),
- $\Theta_{\mathrm{wo}}^{\mathsf{int}}$ denote the restriction of Θ_{wo} to the construction-specific primitive query-response (X, Y).

BAD TRANSCRIPT DEFINITION AND ANALYSIS: A transcript $\omega = (M, T, U, V, K, Y) \in \Omega$ is said to be *bad* if and only if $\mathsf{LSC}(T, V) \vee \mathsf{KG}(M, U, K) \vee \mathsf{SC}(M, T, U, V, K)$ holds.

Lemma 16.4.

$$\Pr\left(\Theta_0 \in \Omega_{\mathrm{bad}}\right) \leq \frac{1}{2^n} + \frac{4\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}} + \frac{2q(p+q)^r}{2^{nr}}$$

Proof. We have

$$\begin{aligned}\Pr\left(\Theta_0 \in \Omega_{\mathrm{bad}}\right) &= \Pr\left(\mathsf{LSC}(\mathsf{T}, p+q) \vee \mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K}) \vee \mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K})\right) \\ &\leq \Pr\left(\mathsf{LSC}(\mathsf{T}, p+q)\right) + \Pr\left(\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K})\right) + \Pr\left(\mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) \mid \neg\mathsf{LSC}(\mathsf{T}, p+q)\right) \\ &\leq \frac{1}{2^n} + \frac{qp^r}{2^{nr}} + \frac{q(p+q)^r}{2^{nr}} + \frac{4(p+q)^{r-1}\sqrt{nq}}{2^{n(r-1)}},\end{aligned}$$

where the first term on the right-hand side corresponds to $\Pr\left(\mathsf{LSC}(\mathsf{T}, p+q)\right)$ and follows from Lemma 10.1, the second term corresponds to $\Pr\left(\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K})\right)$ and follows from the uniformity of K. The last two terms correspond to $\Pr\left(\mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) \mid \neg\mathsf{LSC}(\mathsf{T}, p+q)\right)$. To argue this, first notice that given $\neg\mathsf{LSC}(\mathsf{T}, p+q)$, we have

$$\mu(\mathsf{T}, \mathsf{V}) \leq \frac{q(p+q)^r}{2^n} + 4(p+q)^{r-1}\sqrt{nq}.$$

For each choice of $k \in [r]$, the predicate $\forall k' \neq k$, $\mathsf{X}_{k'}^i = \mathsf{U}_{k'}^{j_{k'}}$ is satisfied with at most $2^{-n(r-1)}$ probability. Now, we get the desired terms using union bound. □

Lemma 16.5.

$$\Pr\left(\Theta_0 \in \Omega_{\mathrm{bad}}\right) \leq \frac{1}{2^n} + \frac{2qp^r}{2^{rn}} + \frac{4p^{r-1}\sqrt{nq}}{2^{n(r-1)}}$$

Proof. We have

$$\begin{aligned}\Pr\left(\Theta_0 \in \Omega_{\mathrm{bad}}\right) &= \Pr\left(\mathsf{LSC}(\mathsf{T}, \mathsf{V}) \vee \mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K}) \vee \mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K})\right) \\ &\leq \Pr\left(\mathsf{LSC}(\mathsf{T}, \mathsf{V})\right) + \Pr\left(\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K})\right) + \Pr\left(\mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) \mid \neg\mathsf{LSC}(\mathsf{T}, \mathsf{V})\right)\end{aligned}$$

$$\leq \frac{1}{2^n} + \frac{qp^r}{2^{nr}} + \frac{qp^r}{2^{nr}} + \frac{4p^{r-1}\sqrt{nq}}{2^{n(r-1)}},$$

where the first term on the right hand side corresponds to $\Pr(\mathsf{LSC}(\mathsf{T},\mathsf{V}))$ and follows from Lemma 10.1, the second term corresponds to $\Pr(\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K}))$ and follows from the uniformity of K. The last two terms correspond to $\Pr(\mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}) \mid \neg\mathsf{LSC})$. To argue this, first notice that given $\neg\mathsf{LSC}(\mathsf{T},\mathsf{V})$, we have

$$\mu(\mathsf{T},\mathsf{V}) \leq \frac{qp^r}{2^n} + 12p^{r-1}\sqrt{nq}.$$

For each choice of $k \in [r]$, the predicate $\forall k' \neq k, \mathsf{X}^i_{k'} = \mathsf{U}^{j_{k'}}_{k'}$ is satisfied with at most $2^{-n(r-1)}$ probability. Now, we get the desired terms using union bound. □

GOOD TRANSCRIPT ANALYSIS: Let $\omega = (M,T,U,V,K,Y)$ be a good transcript. Since the transcript is good, $\neg(\mathsf{LSC}(T,V) \vee \mathsf{KG}(M,U,K) \vee \mathsf{SC}(M,T,U,V,K))$ holds.

Before moving forward, recall the notations introduced while discussing the sampling in the ideal world. We assume analogous notations for any arbitrary transcript.

We also ignore the probability computation of obvious events, such as: the message tuple being realized.

Real World: In the real world, we have

$$\begin{aligned}\Pr(\mathtt{\Theta}_1 = \omega) &= \Pr\left(\mathtt{\Theta}_1^{\mathrm{key}} = K, \mathtt{\Theta}_1^{\mathrm{prim}} = (U,V), \mathtt{\Theta}_1^{\mathrm{int}} = (X,Y), \mathtt{\Theta}_1^{\mathrm{con}} = (M,T)\right)\\ &= \Pr\left(\mathtt{\Theta}_1^{\mathrm{key}} = K\right) \times \Pr\left(\mathtt{\Theta}_1^{\mathrm{prim}} = (U,V)\right) \times \Pr\left(\mathtt{\Theta}_1^{\mathrm{int}} = (X,Y) \mid \mathtt{\Theta}_1^{\mathrm{key}}, \mathtt{\Theta}_1^{\mathrm{prim}}\right)\\ &= \frac{1}{2^{nr}} \times \frac{1}{(2^n)^r_p} \times \Pr\left(\mathtt{\Theta}_1^{\mathrm{int}} = (X,Y) \mid \mathtt{\Theta}_1^{\mathrm{key}}, \mathtt{\Theta}_1^{\mathrm{prim}}\right),\end{aligned}$$

where the first term on the right hand side follows from the uniformity of K, the second term follows from the uniformity of $\boldsymbol{\pi} = (\boldsymbol{\pi}_1, \ldots, \boldsymbol{\pi}_r)$.

As for the last term, consider the partition imposed by $\sim$ in an arbitrary order, and also the associated notations introduced earlier. Then, conditioned on $(\mathtt{\Theta}_1^{\mathrm{key}}, \mathtt{\Theta}_1^{\mathrm{prim}})$, we have

$$\Pr\left(\mathtt{\Theta}_1^{\mathrm{int}} = (X,Y) \mid \mathtt{\Theta}_1^{\mathrm{key}}, \mathtt{\Theta}_1^{\mathrm{prim}}\right) = \prod_{j=1}^{r} \frac{1}{(2^n - p)_{q_0^{(j)}}} \times \prod_{\substack{i \in [c]\\ j' \in \mathcal{J}_{(i)}}} \frac{1}{(2^n - f^{(j')}_{\leq i-1})_{q_i}}.$$

Indeed, the first product term corresponds to the query indices with exactly one fresh primitive input, i.e. the ones in $\mathcal{Q}^{(j)}_{(0)}$ for some $j \in [r]$, and the second product correspond to the query indices with at least two fresh primitive inputs, computed using a simple

application of chain rule over the partitions $\mathcal{Q}_{(1)}, \ldots, \mathcal{Q}_{(c)}$. By combining everything, we have

$$\Pr\left(\mathtt{\Theta}_1 = \omega\right) = \frac{1}{2^{nr}} \times \frac{1}{(2^n)_p^r} \times \prod_{j=1}^{r} \frac{1}{(2^n - p)_{q_0^{(j)}}} \times \prod_{\substack{i\in[c] \\ j'\in\mathcal{J}_{(i)}}} \frac{1}{(2^n - f_{\le i-1}^{(j')})_{q_i}}, \tag{16.3}$$

Ideal World: In the ideal world, we have

$$\begin{aligned}
\Pr\left(\mathtt{\Theta}_0 = \omega\right) &= \Pr\left(\mathtt{\Theta}_0^{\mathrm{key}} = K, \mathtt{\Theta}_0^{\mathrm{prim}} = (U,V), \mathtt{\Theta}_0^{\mathrm{int}} = (X,Y), \mathtt{\Theta}_0^{\mathrm{con}} = (M,T)\right) \\
&= \Pr\left(\mathtt{\Theta}_0^{\mathrm{key}} = K\right) \times \Pr\left(\mathtt{\Theta}_0^{\mathrm{con}} = (M,T)\right) \times \Pr\left(\mathtt{\Theta}_0^{\mathrm{prim}} = (U,V)\right) \\
&\qquad \times \Pr\left(\mathtt{\Theta}_0^{\mathrm{int}} = (X,Y) \mid \mathtt{\Theta}_0^{\mathrm{key}}, \mathtt{\Theta}_0^{\mathrm{prim}}, \mathtt{\Theta}_0^{\mathrm{con}}\right) \\
&= \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{(2^n)_p^r} \times \Pr\left(\mathtt{\Theta}_0^{\mathrm{int}} = (X,Y) \mid \mathtt{\Theta}_0^{\mathrm{key}}, \mathtt{\Theta}_0^{\mathrm{prim}}, \mathtt{\Theta}_0^{\mathrm{con}}\right) \\
&= \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{(2^n)_p^r} \times \prod_{i\in[c]} \Pr\left(\mathtt{Y}^{(i)} = Y^{(i)} \mid \mathscr{F}_{\le i-1}\right) \\
&= \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{(2^n)_p^r} \times \prod_{i\in[c]} \frac{1}{N(\overline{\mathbf{A}}_i, \boldsymbol{\lambda}_i, \simeq, \mathscr{F}_{\le i-1})}
\end{aligned}$$

where the first three terms are obvious. The fourth term corresponds to the indices in $\mathcal{Q}_{(i)}$ for all $i \in [c]$. Further, using (16.1), we have

$$\begin{aligned}
\Pr\left(\mathtt{\Theta}_0 = \omega\right) &\ge \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{(2^n)_p^r} \times \prod_{\substack{i\in[c] \\ j'\in[r]}} \frac{2^{nq_i}}{\left(1 - \varepsilon^{(i)}\right)(2^n - f_{\le i-1}^{(j')})_{q_i}} \\
&= \frac{1}{2^{nr}} \times \frac{1}{2^{nq_0}} \times \frac{1}{(2^n)_p^r} \times \prod_{\substack{i\in[c] \\ j'\in[r]}} \frac{1}{\left(1 - \varepsilon^{(i)}\right)(2^n - f_{\le i-1}^{(j')})_{q_i}},
\end{aligned} \tag{16.4}$$

where the equality follows from the fact that $q = q_0 \sum_{i\in[c]} q_i$.

The Ratio: On dividing (16.3) by (16.4), we have

$$\frac{\Pr\left(\mathtt{\Theta}_1 = \omega\right)}{\Pr\left(\mathtt{\Theta}_0 = \omega\right)} \ge \prod_{i\in[c]} \left(1 - \varepsilon^{(i)}\right) \tag{16.5}$$

$$\ge 1 - \sum_{i\in[c]} \varepsilon^{(i)}$$

$$\ge 1 - \underbrace{\sum_{i\in[c]} \left(\frac{2\mu(\mathsf{T}^{(i)}, \mathscr{F}_{\le i-1})}{2^{n(t_i-1)}} + \frac{2q_i \Delta_{\boldsymbol{\lambda}_{\le i-1}}}{2^{n(t_i-1)}} + \frac{6q_i(p+q)^{t_i}}{2^{nt_i}} \right)}_{\epsilon_{\mathsf{ratio}}(\omega)} \tag{16.6}$$

Now, we have

$$\mathbb{E}\left(\chi_{\mathsf{good}}\epsilon_{\mathsf{ratio}}\right) = \sum_{i\in[c]} \mathbb{E}\left(\chi_{\mathsf{good}}(\Theta_0)\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathscr{F}}_{\le(i-1)})}{2^{n(t_i-1)}}\right) + \sum_{i\in[c]} \frac{2\mathbb{E}\left(q_i\right)\mathbb{E}\left(\Delta_{\boldsymbol{\lambda}_{\le i-1}}\right)}{2^{n(t_i-1)}} \tag{16.7}$$

$$+ \sum_{i\in[c]} \frac{6\mathbb{E}\left(q_i\right)(p+q)^{t_i}}{2^{nt_i}}$$

$$\le \sum_{i\in[c]} \mathbb{E}\left(\chi_{\mathsf{good}}(\Theta_0)\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathscr{F}}_{\le(i-1)})}{2^{n(t_i-1)}}\right) + \frac{16nq(2p)^{r-2}}{2^{n(r-1)}} + \frac{6q(2(p+q))^r}{2^{nr}} \tag{16.8}$$

where the first equality follows from the linearity of expectation and the fact that $\mathbb{E}\left(\chi\mathtt{R}\right) \le \mathbb{E}\left(\mathtt{R}\right)$ for any non-negative random variable $\mathtt{R}$ and indicator random variable χ. The second/third term in the second inequality follows from $\mathbb{E}\left(q_i\right) \le qp^{r-t_i}/2^{n(r-t_i)} \le q(p+q)^{r-t_i}/2^{n(r-t_i)}$, $t_i \ge 2$ and $c \le 2^r$.Additionally, due to the uniformity of T and $q < 2^n$, $\mathbb{E}\left(\Delta_{\boldsymbol{\lambda}_{\le i-1}}\right) \le 4n$. Now, for the first term, when $t_i = r$, we have

$$\begin{aligned}\mathbb{E}\left(\chi_{\mathsf{good}}(\Theta_0)\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathscr{F}}_{\le i-1})}{2^{n(r-1)}}\right) &\le \frac{2\mu(\mathsf{T},\mathsf{V})}{2^{n(r-1)}} \\ &\le \frac{2\mu^r(\mathsf{T}, p+q)}{2^{n(r-1)}} \\ &\le \frac{2q(p+q)^r}{2^{nr}} + \frac{8\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}},\end{aligned} \tag{16.9}$$

where the last inequality follows from $\chi_{\mathsf{good}}(\Theta_0) = 1$. For, $t_i < r$, let $\mathscr{J}_{(i)} = \{j_1, \ldots, j_{t_i}\}$, $[r] \setminus \mathscr{J}_{(i)} = \{j'_1, \ldots, j'_{r-t_i}\}$, and

$$\mathscr{KSC}_{(i)} := \left\{(\mathsf{T}^{i'}, \mathsf{V}^{k_1}_{j'_1}, \ldots, \mathsf{V}^{k_{r-t_i}}_{j'_{r-t_i}}, \mathsf{Z}_{\mathscr{J}_{(i)}}) \in \mathsf{T} \times \mathsf{V}_{[r]\setminus\mathscr{J}_{(i)}} \times \mathscr{F}^{[\mathscr{J}_{(i)}]}_{\le(i-1)} \;:\; \mathsf{X}^{i'}_{j'_l} = \mathsf{U}^{k_l}_{j'_l}\right\}$$

Then, $|\mathscr{KSC}_{(i)}| = \mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathscr{F}}_{\le i-1})$, and thus

$$\begin{aligned}\mathbb{E}\left(\chi_{\mathsf{good}}(\Theta_0)\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathscr{F}}_{\le i-1})}{2^{n(t_i-1)}}\right) &\le \frac{2}{2^{n(t_i-1)}}\mathbb{E}\left(\chi_{\mathsf{good}}(\Theta_0)|\mathscr{KSC}_{(i)}|\right) \\ &\le \frac{2}{2^{n(t_i-1)}} \times \frac{\mu^r(\mathsf{T}, p+q)}{2^{n(r-t_i)}} \\ &\le \frac{2q(p+q)^r}{2^{nr}} + \frac{8\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}}\end{aligned} \tag{16.10}$$

where the second inequality follows from the uniformity of K, and the last inequality follows from $\chi_{\mathsf{good}}(\Theta_0) = 1$. Using (16.9) and (16.10) in (16.8), we have

$$\mathbb{E}\left(\chi_{\mathsf{good}}\epsilon_{\mathsf{ratio}}\right) \leq \frac{16nq(2p)^{r-2}}{2^{n(r-1)}} + \frac{16\sqrt{nq}(2(p+q))^{r-1}}{2^{n(r-1)}} + \frac{8q(2(p+q))^r}{2^{nr}} \tag{16.11}$$

Finally, using the fine-grained variant of the Expectation method (see Theorem 3.2) along with Lemma 16.4 and (16.11), we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\boldsymbol{\pi}\text{-}\mathsf{SOEM}^r}(p,q) \leq \frac{1}{2^n} + \frac{16nq(2p)^{r-2}}{2^{n(r-1)}} + \frac{20\sqrt{nq}(2p+2q)^{r-1}}{2^{n(r-1)}} + \frac{10q(2p+2q)^r}{2^{nr}},$$

which completes the proof. □

17

1K-DBHTS AND INSTANTIATIONS: *APPLICATION OF* CRMTP*, THEOREM 12.1*

Here we investigate the diblock hash-then-sum MAC construction, where a diblock hash function outputs two blocks, such that each block behaves like the output of a universal hash function and then apply the sum-of-permutations PRF on the blocks, i. e., passing each block through a blockcipher, and the resulting pair of outputs being xored to get the tag. We are particularly interested in the single-keyed instantiations of 1k-DBHtS , like 1k-PMAC+ and 1k-LightMAC+ , where all the underlying blockciphers used to instantiate the diblock hash and the ones applied to its output blocks are keyed by the same key. We prove that these are optimally secure MACs using Theorem 12.1.

UNIVERSAL HASH FUNCTIONS. For some $\delta > 0$, a $(\mathscr{K}, \{0,1\}^*, \mathscr{Y})$-keyed function H is called *δ-almost universal* if and only if for all $m \neq m' \in \{0,1\}^*$, we have

$$\Pr\left(H_{\mathsf{K}}(m) = H_{\mathsf{K}}(m')\right) \leq \delta,$$

where the probability is computed over $\mathsf{K} \xleftarrow{*} \mathscr{K}$.

We often call the hash function H a *diblock* hash function, if we can write $\mathscr{Y}$ as $\mathscr{Z}^2$ for some $\mathscr{Z}$. For any diblock hash function H, we write $(H_K^1(m), H_K^2(m)) := (z_1, z_2)$, where $z_1, z_2 \in \mathscr{Z}$, and $H_K(m) = y = (z_1, z_2)$.

PERMUTATION-BASED HASH FUNCTIONS. A $(\mathscr{K}, \{0,1\}^*, \mathscr{Y})$-hash function is said to be permutation-based if $\mathscr{K} \subseteq \mathsf{Perm}(n)^r$ for some $r \in \mathbb{N}$. For any such hash function H, the *block function*, $\beta_H : \mathsf{Perm}(n) \times \{0,1\}^* \to \mathbb{N}$, is defined by the mapping:

$$(\boldsymbol{\pi}^r, m) \mapsto \beta_{(\boldsymbol{\pi}^r, m)},$$

where $\boldsymbol{\pi}^r = (\boldsymbol{\pi}_1, \ldots, \boldsymbol{\pi}_r)$ and $\beta_{(\boldsymbol{\pi}^r, m)}$ denotes the minimum number of invocations[1] of $\boldsymbol{\pi}$ needed to compute $H_{\boldsymbol{\pi}}(m)$.

In this section, we fix $r = 1$, and make the following two plausible assumptions on β_H:

1. β_H is functionally independent of the permutation, whence we drop the permutation from the parameters.
2. $\beta_H(m) = O\left(\lceil |m|/n \rceil\right)$ for any $m \in \{0,1\}^*$. In particular, we assume that there exists a constant $c \in \mathbb{N}$, such that $\beta_H(m) \leq c\lceil |m|/n \rceil$ for any $m \in \{0,1\}^*$. We refer to such an H as a *rate-c^{-1}* hash function.

1 Note that, there exists a circuit for H such that on every input, H makes (possibly) a large but bounded number of black-box calls to $\boldsymbol{\pi}^r$. Thus, $\beta_{\boldsymbol{\pi}^r, m}$ is well-defined for any $\boldsymbol{\pi}^r$ and m.

Note that, 1 follows from 2. We state it explicitly for brevity.

We remark that the underlying hash functions in almost all the popular constructions, including LightMAC , PMAC , LightMAC+ , PMAC+ , 3kf9, etc. are rate-1, and SUM-ECBC is rate-2^{-1}. Thus, the above assumption is indeed plausible, and $c \leq 2$ in most applications.

17.0.1 *Coverfree Hash Functions.*

For any $(\mathscr{K}, \{0,1\}^*, \mathscr{Y}^2)$-diblock hash function H, any $r, s \in \mathbb{N}$, and any $\boldsymbol{m} := (m_1, \ldots, m_q) \in (\{0,1\}^*)_q$, we define the following events

$\mathsf{COLL1}_H(\boldsymbol{m})$: $\exists^* i, j \in [q]$ such that $H^1_{\mathsf{K}}(m_i) = H^1_{\mathsf{K}}(m_j)$;

$\mathsf{COLL2}_H(\boldsymbol{m})$: $\exists^* i, j \in [q]$ such that $H^2_{\mathsf{K}}(m_i) = H^2_{\mathsf{K}}(m_j)$;

$\mathsf{AP1}^r_H(\boldsymbol{m})$: $\exists^* i_1, \ldots, i_r \in [q]$ such that
$H^1_{\mathsf{K}}(m_{i_1}) = H^1_{\mathsf{K}}(m_{i_2}), H^2_{\mathsf{K}}(m_{i_2}) = H^2_{\mathsf{K}}(m_{i_3}), \ldots, H^1_{\mathsf{K}}(m_{i_{r-1}}) = H^1_{\mathsf{K}}(m_{i_r})$;

$\mathsf{AP2}^r_H(\boldsymbol{m})$: $\exists^* i_1, \ldots, i_r \in [q]$ such that
$H^2_{\mathsf{K}}(m_{i_1}) = H^2_{\mathsf{K}}(m_{i_2}), H^1_{\mathsf{K}}(m_{i_2}) = H^1_{\mathsf{K}}(m_{i_3}), \ldots, H^2_{\mathsf{K}}(m_{i_{r-1}}) = H^2_{\mathsf{K}}(m_{i_r})$;

$\mathsf{MC1}^s_H(\boldsymbol{m})$: $\exists^* i_1, \ldots, i_s \in [q]$ such that
$H^1_{\mathsf{K}}(m_{i_1}) = H^1_{\mathsf{K}}(m_{i_2}) = \cdots = H^1_{\mathsf{K}}(m_{i_s})$;

$\mathsf{MC2}^s_H(\boldsymbol{m})$: $\exists^* i_1, \ldots, i_s \in [q]$ such that
$H^2_{\mathsf{K}}(m_{i_1}) = H^2_{\mathsf{K}}(m_{i_2}) = \cdots = H^2_{\mathsf{K}}(m_{i_s})$,

$\mathsf{COLL}_H(\boldsymbol{m})$: $\exists^* i, j \in [q]$ such that $H_{\mathsf{K}}(m_i) = H_{\mathsf{K}}(m_j)$.

where the randomness is induced by $\mathsf{K} \xleftarrow{*} \mathscr{K}$.

Definition 17.1. *For some $\epsilon_1, \delta : \mathbb{N}^3 \to [0,1]$ and $\epsilon_2, \epsilon_3 : \mathbb{N}^4 \to [0,1]$, a $(\mathscr{K}, \{0,1\}^*, \mathscr{Y})$-diblock hash function H is said to be an $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-Coverfree Hash or CfH if and only if for any $\rho = (q, \ell, \sigma) \in \mathbb{N}^3$, any $\boldsymbol{m} = (m_1, \ldots, m_q) \in (\{0,1\}^{n\ell})_q$ containing at most σ blocks and any $r, s \in \mathbb{N}$, it satisfies*

$$\Pr\left(\mathsf{COLL1}_H(\boldsymbol{m})\right) \leq \epsilon_1(\rho), \quad \Pr\left(\mathsf{AP1}^r_H(\boldsymbol{m})\right) \leq \epsilon_2(\rho, r), \quad \Pr\left(\mathsf{MC1}^s_H(\boldsymbol{m})\right) \leq \epsilon_3(\rho, s),$$

$$\Pr\left(\mathsf{COLL2}_H(\boldsymbol{m})\right) \leq \epsilon_1(\rho), \quad \Pr\left(\mathsf{AP2}^r_H(\boldsymbol{m})\right) \leq \epsilon_2(\rho, r), \quad \Pr\left(\mathsf{MC2}^s_H(\boldsymbol{m})\right) \leq \epsilon_3(\rho, s),$$

and $\Pr\left(\mathsf{COLL}_H(\boldsymbol{m})\right) \leq \delta(\rho)$.

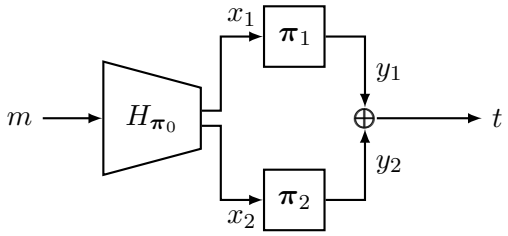


Figure 17.1: The 1k-DBHtS $_{\pi,H}$ construction.

17.1 SECURITY OF SINGLE-KEYED DOUBLE-BLOCK HASH-THEN-SUM

Let π be a permutation of $\{0,1\}^n$. We define three injective functions $\pi_0, \pi_1, \pi_2 : \{0,1\}^{n-2} \to \{0,1\}^n$ as follows:

$$\pi_0(\cdot) := \pi(00\|\cdot) \qquad \pi_1(\cdot) := \pi(01\|\cdot) \qquad \pi_2(\cdot) := \pi(10\|\cdot)$$

For $0 \le j \le 2$, we define $\mathscr{I}_j(n) := \{\pi_j : \pi \in \mathsf{Perm}(n)\}$.

Definition 17.2 (Single-keyed Permutation-based DBHtS). *For some permutation π of $\{0,1\}^n$ and a permutation-based rate-c^{-1} diblock hash function $H : \mathscr{I}_0(n) \times \{0,1\}^* \to \{0,1\}^{n-2} \times \{0,1\}^{n-2}$, we define the single-keyed* DBHtS *, denoted* 1k-DBHtS $_{\pi,H}$ *construction by the mapping:*

$$m \mapsto \pi_1(H_{\pi_0}(m)) \oplus \pi_2(H_{\pi_0}(m)). \tag{17.1}$$

The construction is illustrated in Fig. 17.1.

We drop the parameters π and H whenever they are clear from the context. We reemphasize here that the π_0,π_1,π_2 are all domain-separated versions of the same permutation π.

Theorem 17.2. *Let $c, q, \ell, \sigma \ge 0$ satisfying $q\ell < \sigma$ and $\overline{\sigma} = c\sigma + 2q \le 2^{n-3}$. Suppose $H : \mathscr{I}_0(n) \times \{0,1\}^* \to \{0,1\}^{2n-4}$ is a rate-c^{-1} $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-CFH. Then, for $\rho = (q, \ell, \sigma)$ and $\rho' = (2, \ell, 2\ell)$, the PRF advantage of any ρ-distinguisher $\mathscr{A}$ against 1k-DBHtS $_{\pi,H}$ satisfies*

$$\boldsymbol{Adv}^{\mathrm{prf}}_{\text{1k-DBHtS }_{\pi,H}}(\mathscr{A}) \le \epsilon_1 + \epsilon_2,$$

where

$$\epsilon_1 := 2\epsilon_2(\rho, 4) + \delta(\rho) + \frac{q + 2\epsilon_1(\rho) + \epsilon_2(\rho, 3)}{2^n} + 2\epsilon_3\left(\rho, 2^n/4\overline{\sigma}\right).$$

$$\epsilon_2 := \frac{16q^2\overline{\sigma}^2\epsilon_1(\rho')}{2^{2n}} + \frac{8q^2\epsilon_1(\rho')}{2^n} + \frac{3q\overline{\sigma}}{2^{3n/2}} + \frac{40q\overline{\sigma}^{5/2}}{2^{5n/2}} + \frac{4q\overline{\sigma} + 16q\overline{\sigma}^2 + 16q^3\overline{\sigma}}{2^{3n}}.$$

Proof. Without loss of generality assume that $\mathscr{A}$ is deterministic. Let

- $\mathsf{M}^i := (\mathsf{M}^i_1, \ldots, \mathsf{M}^i_{\ell_i})$, denote the i-th query of the distinguisher, containing $\ell_i \leq \ell$ blocks.
- T^i, denote the i-th response of the oracle.

In addition, the oracle releases additional information to the distinguisher, once the distinguisher is done querying the oracle, but before it outputs its decision bit.
In the real world, the oracle releases:

- $\mathsf{X}^i := (\mathsf{X}^i_1, \mathsf{X}^i_2) = H_{\boldsymbol{\pi}_0}(\mathsf{M}^i)$, the $(2n-2)$-bit internal hash output, or *finalization input* corresponding to the i-th query.
- $\mathsf{Y}^i := (\mathsf{Y}^i_1, \mathsf{Y}^i_2) = (\boldsymbol{\pi}_1(\mathsf{X}^i_1), \boldsymbol{\pi}_2(\mathsf{X}^i_2))$, the $2n$-bit *finalization output* corresponding to the i-th query.
- R, the set of all image points sampled during the computation of $H_{\boldsymbol{\pi}_0}(\mathsf{M}^i)$ for all $i \in [q]$. Since H is a rate-c^{-1} hash function, $r = |R| = c\sigma$.

Thus, the full real world transcript can be described as

$$\Theta_1 := ((\mathsf{M}^i, \mathsf{T}^i, \mathsf{X}^i, \mathsf{Y}^i : i \in [q]), R).$$

In the ideal world, the oracle first samples a dummy random permutation $\boldsymbol{\pi}'$, and then computes $\mathsf{X}^i := H_{\boldsymbol{\pi}'_0}(\mathsf{M}^i)$ for all $i \in [q]$. In other words, X^i is generated faithfully for all $i \in [q]$. Note that, R can be derived here as well, as the ideal oracle is faithfully generating the hash outputs.

SAMPLING Y IN THE IDEAL WORLD: The sampling mechanism for Y^i is on the other hand a bit more sophisticated. The goal is to sample Y^i's in such a way that

$$\mathsf{X}^i_1 \leftrightarrow \mathsf{Y}^i_1, \qquad \mathsf{X}^i_2 \leftrightarrow \mathsf{Y}^i_2,$$

is satisfied for all $i \neq j \in [q]$. We refer to this predicate as the *permutation compatibility condition*.

For any $i \in [q]$, let $(i)_1 := \min\{j < i \ : \ \mathsf{X}^i_1 = \mathsf{X}^j_1\}$ and $(i)_2 := \min\{j < i \ : \ \mathsf{X}^i_2 = \mathsf{X}^j_2\}$. Let $v = |\{(i)_1, (i)_2 \ : \ i \in [q]\}|$. The system of equations $\{\mathsf{Y}^{(i)_1}_1 \oplus \mathsf{Y}^{(i)_2}_2 = \mathsf{T}^i : i \in [q]\}$, can be treated as the system of equations in an instance of the the non-trivial $\texttt{CRMTP}(\mathbf{A}_{q\times v}, \mathbf{T}, \{R\})$ problem, where

$$\mathbf{A}|\mathbf{T} := \begin{pmatrix} \overline{\mathbf{A}}_1 & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{T}_1 \\ \mathbf{0} & \overline{\mathbf{A}}_2 & \cdots & \mathbf{0} & \mathbf{T}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{\mathbf{A}}_c & \mathbf{T}_c \end{pmatrix} \in \mathbb{F}_2^{q\times(v+1)}.$$

is the 2-regular, acyclic augmented coefficient-constant matrix of the system. Without loss of generality we assume $\mathbf{A}$ has a component form (since any matrix can be transformed into the component form by permuting the rows, which preserves the set of solutions), such that all the isolated components appear before the non-isolated ones.

As long as the system is acyclic and non-trivial and satisfies the bound $\xi_{\mathbf{A}}(2q + c\sigma) \leq 2^n/2$, we can use the results developed in the previous section. Here Keeping this in mind, we now define some bad predicates on the partial transcript $((\mathsf{M}^i, \mathsf{T}^i, \mathsf{X}^i : i \in [q]), R)$:

$$
\begin{aligned}
\mathsf{A}_1 &: \exists^* i,j,k,l \in [q], && \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{X}_2^j = \mathsf{X}_2^k \wedge \mathsf{X}_1^k = \mathsf{X}_1^l.\\
\mathsf{A}_2 &: \exists^* i,j \in [q], && \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{T}^i \oplus \mathsf{T}^j = 0^n.\\
\mathsf{A}_3 &: \exists^* k \geq 2^{n-2}/(c\sigma + 2q), i_1, \ldots, i_k \in [q], && \mathsf{X}_1^{i_1} = \mathsf{X}_1^{i_2} = \ldots = \mathsf{X}_1^{i_k}.\\
\mathsf{B}_1 &: \exists^* i,j,k,l \in [q], && \mathsf{X}_2^i = \mathsf{X}_2^j \wedge \mathsf{X}_1^j = \mathsf{X}_1^k \wedge \mathsf{X}_2^k = \mathsf{X}_2^l.\\
\mathsf{B}_2 &: \exists^* i,j \in [q], && \mathsf{X}_2^i = \mathsf{X}_2^j \wedge \mathsf{T}^i \oplus \mathsf{T}^j = 0^n.\\
\mathsf{B}_3 &: \exists^* k \geq 2^{n-2}/(c\sigma + 2q), i_1, \ldots, i_k \in [q], && \mathsf{X}_2^{i_1} = \mathsf{X}_2^{i_2} = \ldots = \mathsf{X}_2^{i_k}.\\
\mathsf{C} &: \exists^* i \in [q], && \mathsf{T}^i = 0^n.\\
\mathsf{D} &: \exists^* i,j \in [q], && \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{X}_2^i = \mathsf{X}_2^j.\\
\mathsf{E} &: \exists^* i,j,k \in [q], && \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{X}_2^j = \mathsf{X}_2^k \wedge \mathsf{T}^i \oplus \mathsf{T}^j \oplus \mathsf{T}^k = 0^n.
\end{aligned}
$$

Define $\mathsf{Cyclic} := \mathsf{A}_1 \vee \mathsf{B}_1 \vee \mathsf{D}$, $\mathsf{Trivial} := \mathsf{A}_2 \vee \mathsf{B}_2 \vee \mathsf{C} \wedge \mathsf{E}$, and $\mathsf{Giant} := \mathsf{A}_3 \vee \mathsf{B}_3$. It is not difficult to see that as long as Cyclic, Trivial, and Giant are false, $\mathbf{A}$ is acyclic and satisfies $\xi_{\mathbf{A}}(c\sigma + 2q) \leq 2^{n-1}$ for $(c\sigma + 2q) < 2^{3n/4}$, and $\mathtt{CRMTP}(\mathbf{A}, \mathbf{T}, \{R\})$ problem is non-trivial.

Onwards we describe the sampling of Y conditioned on the fact that $\neg(\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant})$ holds.

SAMPLING Y^i IN ISOLATED CASE: For the i-th isolated component, using Lemma 12.2, the number of solutions conditioned on the forbidden set R and a compatible solution $\mathsf{Y}^{\leq(i-1)}$ of $\mathtt{CRMTP}(\mathbf{A}_{\leq i-1}, \mathbf{T}^{\leq i-1}, \{R\})$ is given by

$$
N(\overline{\mathbf{A}}_i, \mathbf{T}_i, \{F\}) \geq \frac{(2^n - r - 2i + 2)^2}{2^n} \left(1 - \frac{2}{2^n}\left|\mu(\mathbf{T}_i, \mathscr{F}) - \frac{(r + 2i - 2)^2}{2^n}\right| - \frac{4}{2^{2n}}\right).
$$

We sample $\mathsf{Y}^i \xleftarrow{*} \mathcal{S}(\overline{\mathbf{A}}_i, \mathbf{T}_i, \{F\})$, where $F := F(\mathsf{Y}^{\leq i-1}) = R \sqcup \mathsf{Y}^{\{\leq i-1\}}$, is defined analogously as in Eq. 12.1, with $|F| = r + 2(i-1)$.

SAMPLING Y^i IN NON-ISOLATED CASE: For the i-th non-isolated component, using Lemma 12.3, the number of solutions conditioned on the forbidden set R and a compatible solution $\mathsf{Y}^{\leq i-1}$ of $\mathtt{CRMTP}(\mathbf{A}_{\leq i-1}, \mathbf{T}^{\leq i-1}, R)$ is given by

$$
N(\overline{\mathbf{A}}_i, \mathbf{T}_i, \{F\}) \geq \frac{(2^n - f_{\leq i-1})^{v_i}}{2^{nq_i}} \left(1 - \frac{2r_i^2(r + 2q)^2}{2^{2n}} - \frac{r_i^2}{2^{2n}}\right).
$$

We sample $\mathsf{Y}^i \xleftarrow{*} \mathcal{S}(\overline{\mathbf{A}}_i, \mathbf{T}_i, \{F\})$, where again $F := F(\mathsf{Y}^{i-1}) = R \sqcup \mathsf{Y}^{\{\le i-1\}}$ and $f_{\le i-1} := |F| < r + 2q$.

This concludes the sampling in the ideal world, and finally the ideal world transcript is given by

$$\Theta_0 := ((\mathsf{M}^i, \mathsf{T}^i, \mathsf{X}^i, \mathsf{Y}^i : i \in [q]), R).$$

where the permutation compatibility condition is satisfied as long as $\neg(\mathsf{Cyclic} \vee \mathsf{Trivial})$ holds; otherwise the transcript is defined arbitrarily.

(BAD) TRANSCRIPT DEFINITION AND ANALYSIS: The set of transcripts Ω is the set of all tuples $\omega = ((m^i, t^i, x^i, y^i : i \in [q]), R)$, where $m^i \in \{0,1\}^*$, $t^i \in \{0,1\}^n$, $x^i \in \{0,1\}^{2n-2}$, $y^i \in \{0,1\}^{2n}$ and $R \subseteq (\{0,1\}^n)^{c\sigma}$, where $\sigma = \sum_{i=1}^{q} \lceil |m^i|/n \rceil$.

A transcript ω is said to be *bad*, i.e. $\omega \in \Omega_{\mathrm{bad}}$ if and only if it satisfies $\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant}$, and *good* otherwise.

Lemma 17.4. *Suppose H is an $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-coverfree hash function. Then*

$$\Pr\left(\Theta_0 \in \Omega_{\mathrm{bad}}\right) \le 2\epsilon_2(\rho, 4) + \delta(\rho) + \frac{q + 2\epsilon_1(\rho) + \epsilon_2(\rho, 3)}{2^n} + 2\epsilon_3\left(\rho, \frac{2^{n-2}}{c\sigma + 2q}\right).$$

Proof. Let $s' = 2^{n-2}/(c\sigma + 2q)$. We have

$$\begin{aligned}
\Pr\left(\Theta_0 \in \Omega_{\mathrm{bad}}\right) &= \Pr\left(\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant}\right) \\
&\le \Pr\left(\mathsf{Cyclic}\right) + \Pr\left(\mathsf{Trivial}\right) + \Pr\left(\mathsf{Giant}\right) \\
&\le \Pr\left(\mathsf{A}_1\right) + \Pr\left(\mathsf{B}_1\right) + \Pr\left(\mathsf{D}\right) + \Pr\left(\mathsf{A}_2\right) + \Pr\left(\mathsf{B}_2\right) + \Pr\left(\mathsf{C}\right) + \Pr\left(\mathsf{E}\right) \\
&\qquad + \Pr\left(\mathsf{A}_3\right) + \Pr\left(\mathsf{B}_3\right) \\
&\le \Pr\left(\mathsf{AP1}^4_H(\mathsf{M})\right) + \Pr\left(\mathsf{AP2}^4_H(\mathsf{M})\right) + \Pr\left(\mathsf{COLL}_H(\mathsf{M})\right) + \frac{\Pr\left(\mathsf{COLL1}_H(\mathsf{M})\right)}{2^n} \\
&\qquad + \frac{\Pr\left(\mathsf{COLL2}_H(\mathsf{M})\right)}{2^n} + \frac{q}{2^n} + \frac{\Pr\left(\mathsf{AP1}^3_H(\mathsf{M})\right)}{2^n} \\
&\qquad + \Pr\left(\mathsf{MC1}^{s'}_H(\mathsf{M})\right) + \Pr\left(\mathsf{MC2}^{s'}_H(\mathsf{M})\right) \\
&\le 2\epsilon_2(\rho, 4) + \delta + \frac{q + 2\epsilon_1(\rho) + \epsilon_2(\rho, 3)}{2^n} + 2\epsilon_3(\rho, s'),
\end{aligned}$$

where the the first three (in)equalities follow from the definition and a trivial application of union bound, the fourth inequality just maps the bad predicates to corresponding coverfree hash events, and finally the fifth inequality follows from the coverfree bound of H. □

GOOD TRANSCRIPT ANALYSIS: Fix a good transcript $\omega \in \Omega \setminus \Omega_{\mathrm{bad}}$. We will recycle notations from the sampling phase.

In the real world, $\boldsymbol{\pi}$ is sampled exactly $r+v$ times ($|R| = r$ and $|\{(i)_1, (i)_2 \ : \ i \in [q]\}| = v$). Thus, we have

$$\Pr\left(\mathtt{\Theta}_1 = \omega\right) = \frac{1}{(2^n)_{r+v}} \tag{17.2}$$

In the ideal world, first $\mathbf{T}$ is sampled uniformly from a set of size 2^{nq}, followed by R which is sampled faithfully via $\boldsymbol{\pi}$. Finally, Y is sampled. Let the first i^* components of $\mathbf{A}|\mathbf{T}$ be isolated and the rest be non-isolated.

$$\begin{aligned}\Pr\left(\mathtt{\Theta}_0 = \omega\right) &= \frac{1}{2^{nq}} \times \frac{1}{(2^n)_r} \times \prod_{i=1}^{i^*} \frac{1}{N(\overline{\mathbf{A}}_i, \mathbf{T}_i, \{F(\mathsf{Y}^{\le i-1})\})} \times \prod_{i'=i^*+1}^{c} \frac{1}{N(\overline{\mathbf{A}}_i, \mathbf{T}_i, \{F(\mathsf{Y}^{\le i-1})\})} \\ &\le \frac{1}{2^{nq}} \times \frac{1}{(2^n)_r} \times \prod_{i=1}^{i^*} \frac{2^n}{(1-\mu_i)(2^n - f_{\le i-1})^2} \times \prod_{i'=i^*+1}^{c} \frac{2^{nq_{i'}}}{(1-\nu_{i'})(2^n - f_{\le i'-1})^{v_{i'}}}\end{aligned}$$

where

$$\mu_i = \frac{2}{2^n}\left|\mu(\mathbf{T}_i, \mathscr{F}) - \frac{f_{\le i-1}^2}{2^n}\right| + \frac{4}{2^n}, \tag{17.3}$$

$$\nu_{i'} = \frac{2v_{i'}^2(r+2q)^2}{2^{2n}} + \frac{v_{i'}^2}{2^n}. \tag{17.4}$$

Continuing on we have

$$\begin{aligned}\Pr\left(\mathtt{\Theta}_0 = \omega\right) &\le \frac{1}{(2^n)_r} \times \prod_{i=1}^{i^*} \frac{1}{(1-\mu_i)(2^n - f_{\le i-1})^2} \times \prod_{i'=i^*+1}^{c} \frac{1}{(1-\nu_{i'})(2^n - f_{\le i'-1})^{v_{i'}}} \\ &\le \frac{1}{\left(1 - \sum_{i=1}^{i^*} \mu_i\right)} \times \frac{1}{\left(1 - \sum_{i'=i^*+1}^{c} \nu_{i'}\right)} \times \prod_{i=1}^{c} \frac{1}{(2^n - f_{\le i-1})^{v_i}}\end{aligned} \tag{17.5}$$

On dividing (17.2) by (17.5), we have

$$\begin{aligned}\frac{\Pr\left(\mathtt{\Theta}_1 = \omega\right)}{\Pr\left(\mathtt{\Theta}_0 = \omega\right)} &\ge \left(1 - \sum_{i=1}^{i^*} \mu_i - \sum_{i'=i^*+1}^{c} \nu_{i'}\right) \times \frac{\prod_{i=1}^{c}(2^n - f_{\le i-1})^{v_i}}{(2^n)_{r+v}} \\ &\ge \left(1 - \sum_{i=1}^{i^*} \mu_i - \sum_{i'=i^*+1}^{c} \nu_{i'}\right).\end{aligned} \tag{17.6}$$

To apply the Expectation Method, Theorem 3.1, we have to compute

$$\mathbb{E}\left(\sum_{i=1}^{i^*} \mu_i\right) \qquad \text{and} \qquad \mathbb{E}\left(\sum_{i'=i^*+1}^{c} \nu_{i'}\right)$$

First, let $\sim_1$ (res. $\sim_2$) be equivalence relations on $[q]$, such that $i \sim_1 j$ (res. $i \sim_2 j$) if and only if $\mathsf{X}_1^i = \mathsf{X}_1^j$ (res. $\mathsf{X}_2^i = \mathsf{X}_2^j$). Let $\mathscr{C}_1^1, \ldots, \mathscr{C}_{t_1}^1$ and $\mathscr{C}_1^2, \ldots, \mathscr{C}_{t_2}^2$ denote the non-singleton equivalence classes of $[q]$ with respect to $\sim_1$ and $\sim_2$, respectively. For $i \in [t_1]$ and $j \in [t_2]$, let $\mathtt{mc}_i^{(1)} = |\mathscr{C}_i^1|$ and $\mathtt{mc}_j^{(2)} = |\mathscr{C}_j^2|$.

$$\begin{aligned}
\mathbb{E}\left(\sum_{i'=i^*+1}^{c} \nu_{i'}\right) &= \left(\frac{2(r+2q)^2}{2^{2n}} + \frac{1}{2^n}\right) \mathbb{E}\left(\sum_{i'=i^*+1}^{c} v_{i'}^2\right) \\
&\leq \left(\frac{2(r+2q)^2}{2^{2n}} + \frac{1}{2^n}\right) \times 2 \left(\sum_{j=1}^{t_1} \mathbb{E}\left(\mathtt{mc}_j^{(1)}\right) + \sum_{j'=1}^{t_2} \mathbb{E}\left(\mathtt{mc}_{j'}^{(2)}\right)\right) \\
&\leq \frac{16q^2(r+2q)^2\epsilon_1(2,\ell,2\ell)}{2^{2n}} + \frac{8q^2\epsilon_1(2,\ell,2\ell)}{2^n}. \qquad (17.7)
\end{aligned}$$

where the last inequality follows from Lemma A.6.
Second, using Proposition A.1, we have

$$\begin{aligned}
\mathbb{E}\left(\sum_{i=1}^{i^*} \mu_i\right) &= \mathbb{E}\left(\frac{2}{2^n}\sum_{i=1}^{i^*}\left|\mu(\mathbf{T}_i, \mathscr{F}) - \frac{f_{\leq i-1}^2}{2^n}\right| + \sum_{i=1}^{i^*}\frac{4}{2^n}\right) \\
&= \frac{2}{2^n}\sum_{i=1}^{i^*}\mathbb{E}\left(\left|\mu(\mathbf{T}_i, \mathscr{F}) - \frac{f_{\leq i-1}^2}{2^n}\right|\right) + \frac{4q}{2^n} \\
&\leq \frac{2}{2^n}\sum_{i=1}^{i^*}\sqrt{\mathsf{Var}(\mu(\mathbf{T}_i, \mathscr{F}))} + \frac{2}{2^n}\sum_{i=1}^{i^*}\left|\mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right) - \frac{f_{\leq i-1}^2}{2^n}\right| + \frac{4q}{2^n} \qquad (17.8)
\end{aligned}$$

We claim:

Claim 17.4.1.

$$\left|\mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right) - \frac{f_{\leq i-1}^2}{2^n}\right| \leq \frac{2r^2 + 8q(r+2q)^2 + 8q^2(r+2q)}{2^{2n}} \qquad (17.9)$$

$$\sqrt{\mathsf{Var}(\mu(\mathbf{T}_i, \mathscr{F}))} \leq \frac{\sqrt{2}(r+2q)}{2^{n/2}} + \frac{20(r+2q)^{5/2}}{2^{3n/2}} \qquad (17.10)$$

Theorem 17.2 then follows from Lemma 17.4 and Eq. (17.7)-(17.10). □

PROOF OF CLAIM 17.4.1. First consider $\left|\mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right) - \frac{f_{\leq i-1}^2}{2^n}\right|$. We need both lower and upper bounds on $\mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right)$. Let $\mathscr{I} = \{i_1, \ldots, i_r\}$ be an arbitrary indexing of R and $\mathscr{J} = \{j_1, \ldots, j_{v_{\leq i-1}}\}$ denote the indexing corresponding to $\mathsf{Y}^{\leq i-1}$. Then, $\mathscr{I} \sqcup \mathscr{J}$ gives an indexing of $F := F(\mathsf{Y}^{\leq i-1})$.

For all $j, j' \in \mathscr{I} \sqcup \mathscr{J}$, let $\chi_{j,j'}$ denote the indicator random variable corresponding to the event $\mathsf{A}_j \oplus \mathsf{B}_{j'} = \mathbf{T}_i$, where $\mathsf{A}_j, \mathsf{B}_{j'} \in F$. Then, we have

$$\mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right) = \sum_{j \neq j' \in \mathscr{I} \sqcup \mathscr{J}} \Pr\left(\chi_{j,j'}\right). \tag{17.11}$$

Now, we can have four cases depending upon where j and j' come from:

Case A: $j, j' \in \mathscr{I}$. In this case, for any pair of (j, j'), $\Pr\left(\chi_{j,j'}\right) = 1/(2^n - 1)$ and there are at most $r(r-1)$ such pairs, which results in

$$\sum_{j \neq j' \in \mathscr{I}} \Pr\left(\chi_{j,j'}\right) = \frac{r(r-1)}{2^n - 1}. \tag{17.12}$$

Case B: $j \in \mathscr{I} \wedge j' \in \mathscr{J}$. In this case, using the fact that there are at least $(2^n - r - 2q)$ and at most 2^n solutions for any equation, we have

$$\frac{2r(i-1)}{2^n} \leq \sum_{j \in \mathscr{I}, j' \in \mathscr{J}} \Pr\left(\chi_{j,j'}\right) \leq \frac{2r(i-1)}{2^n - r - 2q} \tag{17.13}$$

Case C: $j \in \mathscr{I} \wedge j' \in \mathscr{J}$. This case is symmetrical to Case B above.

$$\frac{2r(i-1)}{2^n} \leq \sum_{j' \in \mathscr{I}, j \in \mathscr{J}} \Pr\left(\chi_{j,j'}\right) \leq \frac{2r(i-1)}{2^n - r - 2q} \tag{17.14}$$

Case D: $j, j' \in \mathscr{J}$. Using similar argumentation as above, we have

$$\frac{4(i-1)^2 - 2(i-1)}{2^n} \leq \sum_{j, j' \in \mathscr{J}} \Pr\left(\chi_{j,j'}\right) \leq \frac{4(i-1)^2 - 2(i-1)}{2^n - r - 2q} \tag{17.15}$$

Recall that

$$\frac{f^2_{\leq i-1}}{2^n} = \frac{(r + 2(i-1))^2}{2^n}.$$

Then, (17.9) follows from (17.11)-(17.15).

Now, consider the second claim. We have to compute the variance of $\mu(\mathbf{T}_i, \mathscr{F})$. First, using the above formulation, we have

$$\begin{aligned}
\mathsf{Var}(\mu(\mathbf{T}_i, \mathscr{F})) &= \mathsf{Var}\Big(\sum_{j,j' \in \mathscr{I} \sqcup \mathscr{J}} \chi_{j,j'}\Big) \\
&= \sum_{j,j' \in \mathscr{I} \sqcup \mathscr{J}} \mathsf{Var}(\chi_{j,j'}) + \sum_{\substack{j_1,j_2,j_3,j_4 \in \mathscr{I} \sqcup \mathscr{J} \\ \{j_1,j_2\} \neq \{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4})
\end{aligned}$$

$$\leq \sum_{j,j' \in \mathscr{I} \sqcup \mathscr{J}} \mathbb{E}\left(\chi_{j,j'}\right) + \sum_{\substack{j_1,j_2,j_3,j_4 \in \mathscr{I} \sqcup \mathscr{J} \\ \{j_1,j_2\} \neq \{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4})$$

$$\leq \mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right) + \sum_{\substack{j_1,j_2,j_3,j_4 \in \mathscr{I} \sqcup \mathscr{J} \\ \{j_1,j_2\} \neq \{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4}) \tag{17.16}$$

Now, from (17.11)-(17.15), we have

$$\mathbb{E}\left(\mu(\mathbf{T}_i, \mathscr{F})\right) \leq \frac{2(r+2q)^2}{2^n}. \tag{17.17}$$

All that remains is to bound the covariances for every choice of $(j_1, j_2) \neq (j_3, j_4)$. First, we have

$$\mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4}) = \Pr\left(\chi_{j_1,j_2}, \chi_{j_3,j_4}\right) - \Pr\left(\chi_{j_1,j_2}\right) \Pr\left(\chi_{j_3,j_4}\right)$$

Given the above discussion on $\Pr\left(\chi_{j,j'}\right)$ for arbitrary j, j', it is sufficient to upper bound $\Pr\left(\chi_{j_1,j_2}, \chi_{j_3,j_4}\right)$, and use lower bound on $\Pr\left(\chi_{j_1,j_2}\right)$ (and $\Pr\left(\chi_{j_3,j_4}\right)$) from the above discussion. Depending upon $j_k \in \mathscr{I}$ or $j_k \in \mathscr{J}$, for all $k \in [4]$, we can have 16 cases, that we group into 5 supercases depending upon the size of $\{j_1, j_2, j_3, j_4\} \cap \mathscr{I}$. We will skip most of the details of computation for each case, and instead discuss the most important subcases.

Case A: $|\{j_1, j_2, j_3, j_4\} \cap \mathscr{I}| = 4$: In this case it is easy to see that $\Pr\left(\chi_{j_1,j_2}, \chi_{j_3,j_4}\right) \leq 1/(2^n - 1)(2^n - 3)$, and thus

$$\sum_{\substack{j_1,j_2,j_3,j_4 \in \mathscr{I} \\ \{j_1,j_2\} \neq \{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4}) \leq r^4 \left(\frac{1}{(2^n-1)(2^n-3)} - \frac{1}{(2^n-1)^2} \right)$$

$$\leq \frac{16r^4}{2^{3n}}. \tag{17.18}$$

Case B: $|\{j_1, j_2, j_3, j_4\} \cap \mathscr{I}| = 3$: Wlog assume $j_1 \notin \mathscr{I}$. Then, first $\Pr\left(\chi_{j_3,j_4}\right) = 1/(2^n - 1)$ and $\Pr\left(\chi_{j_1,j_2} \mid \chi_{j_3,j_4}\right) \leq 1/(2^n - r - 2q)$ (since the j_1 variable is sampled out of a set of size at least $(2^n - r - 2q)$). Thus, in this case, we have

$$\sum_{\substack{|\{j_1,j_2,j_3,j_4\} \cap \mathscr{I}| = 3 \\ \{j_1,j_2\} \neq \{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4}) \leq 8r^3 q \left(\frac{1}{(2^n-1)(2^n-r-2q)} - \frac{1}{2^n(2^n-1)} \right)$$

$$\leq \frac{32(r+2q)^4 q}{2^{3n}}. \tag{17.19}$$

Case C: $|\{j_1, j_2, j_3, j_4\} \cap \mathscr{I}| = 2$: The most interesting subcase here is $|\{j_1, j_2\} \cap \mathscr{I}| = 1$, $|\{j_3, j_4\} \cap \mathscr{I}| = 1$. Wlog assume $j_1, j_3 \in \mathscr{I}$ and $j_2, j_4 \in \mathscr{J}$. Let $\mathsf{R}_1, \mathsf{R}_3, \mathsf{Y}_2, \mathsf{Y}_4$ denote the corresponding values in $\mathscr{F}$. We have two equations:

$$\mathsf{R}_1 \oplus \mathsf{Y}_2 = \mathbf{T}_i$$

$$\mathsf{R}_3 \oplus \mathsf{Y}_4 = \mathbf{T}_i$$

Now, if Y_2 and Y_4 come from different equations, then the above holds with at most $1/(2^n - r - 2q)^2$ probability as each of Y_2 and Y_4 are sampled from a set of size at least $(2^n - r - 2q)$. The interesting case arises when they are from the same equation, say (k). In this case the above equation holds if and only if $\mathsf{R}_1 \oplus \mathsf{R}_3 = \mathbf{T}_i \oplus \mathsf{T}^{(k)}$. Thus, we have a modified system

$$\begin{aligned}\mathsf{R}_1 \oplus \mathsf{R}_3 &= \mathbf{T}_i \oplus \mathsf{T}^{(k)}\\ \mathsf{R}_1 \oplus \mathsf{Y}_2 &= \mathbf{T}_i\end{aligned}$$

Now, once we fix j_1, j_3 and (k) all other indices are fixed (remember, (i) is fixed throughout). Thus, we have at most $2r^2q$ choices and each choice holds with at most $1/(2^n-1)(2^n - r - 2q)$ probability, which is less than the probability in other cases. All in all, by taking the maximum probability, in this case we have

$$\begin{aligned}\sum_{\substack{|\{j_1,j_2,j_3,j_4\}\cap\mathscr{I}|=2\\ \{j_1,j_2\}\neq\{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2},\chi_{j_3,j_4}) &\leq 24r^2q^2\left(\frac{1}{(2^n-r-2q)^2} - \frac{1}{2^{2n}}\right)\\ &\leq \frac{96(r+2q)^3q^2}{2^{3n}}. \end{aligned} \tag{17.20}$$

Case D: $|\{j_1, j_2, j_3, j_4\} \cap \mathscr{I}| = 1$: W.l.o.g. assume $j_1 \in \mathscr{I}$. The most interesting case here would be if j_3 and j_4 correspond to the same equation index say (k), in which case χ_{j_3,j_4} happens if and only if $\mathbf{T}_i = \mathsf{T}^{(k)}$. But since $\mathbf{T}_i$ is uniform and independent of $\mathsf{T}^{(k)}$, the overall probability in this subcase is still $1/2^n(2^n - r - 2q) \leq 1/(2^n - r - 2q)(2^n - r - 2q)$. Again by taking the maximum probability across all subcases, we have

$$\begin{aligned}\sum_{\substack{|\{j_1,j_2,j_3,j_4\}\cap\mathscr{I}|=1\\ \{j_1,j_2\}\neq\{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2},\chi_{j_3,j_4}) &\leq 48rq^3\left(\frac{1}{(2^n-r-2q)^2} - \frac{1}{2^{2n}}\right)\\ &\leq \frac{192(r+2q)^2q^3}{2^{3n}}. \end{aligned} \tag{17.21}$$

Case E: $|\{j_1, j_2, j_3, j_4\} \cap \mathscr{I}| = 0$: Using a similar argumentation as above, we have

$$\begin{aligned}\sum_{\substack{|\{j_1,j_2,j_3,j_4\}\cap\mathscr{I}|=0\\ \{j_1,j_2\}\neq\{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2},\chi_{j_3,j_4}) &\leq 16q^4\left(\frac{1}{(2^n-r-2q)^2} - \frac{1}{2^{2n}}\right)\\ &\leq \frac{64(r+2q)q^4}{2^{3n}}. \end{aligned} \tag{17.22}$$

A cursory look shows that the covariance across all the cases is in $O((r+2q)^5/2^{3n})$. In particular, after appropriate simplifications, we have

$$\sum_{\substack{j_1,j_2,j_3,j_4 \in \mathcal{J} \sqcup \mathcal{J} \\ \{j_1,j_2\} \neq \{j_3,j_4\}}} \mathsf{Cov}(\chi_{j_1,j_2}, \chi_{j_3,j_4}) \leq \frac{400(r+2q)^5}{2^{3n}} \tag{17.23}$$

Then, (17.10) follows by taking square root on both sides of (17.16) after appropriate substitutions from (17.17) and (17.23). □

17.2 INSTANTIATIONS OF COVER-FREE HASH FUNCTIONS.

For a diblock hash function $H : \mathcal{J}_0(n) \times \{0,1\}^* \to \{0,1\}^n \times \{0,1\}^n$ we can construct the truncated diblock hash $\mathsf{T}H : \mathcal{J}_0(n) \times \{0,1\}^* \to \{0,1\}^{n-2} \times \{0,1\}^{n-2}$ as $\mathsf{T}H(x) := (\mathsf{Trunc}(H_1(x)), \mathsf{Trunc}(H_2(x)))$, where $\mathsf{Trunc} : \{0,1\}^n \to \{0,1\}^{n-2}$ truncates the first two bits of its n-bit input.

Now let us define the functions $\mathsf{PHash} : \mathcal{J}_0(n) \times \{0,1\}^* \to \{0,1\}^n \times \{0,1\}^n$ and $\mathsf{LightHash} : \mathcal{J}_0(n) \times \{0,1\}^* \to \{0,1\}^n \times \{0,1\}^n$, as follows:

$\mathsf{PHash}_{\boldsymbol{\pi}_0}$	$\mathsf{LightHash}_{\boldsymbol{\pi}_0}$
Input: $m = m[1] \| \cdots \| m[k] \in (\{0,1\}^{n-2})^k$	Input: $m = m[1] \| \cdots \| m[k] \in (\{0,1\}^{n-s})^k$
$\Delta_0 \leftarrow \mathsf{Trunc}(\boldsymbol{\pi}_0(0))$	for $i \in [k]$,
$\Delta_1 \leftarrow \mathsf{Trunc}(\boldsymbol{\pi}_0(1))$	$\quad Z[i] \leftarrow \boldsymbol{\pi}_0(\langle i \rangle_{s-2} \| m[i])$
for $i \in [k]$,	$x[1] \leftarrow Z[1] \oplus Z[2] \oplus \cdots \oplus Z[k]$
$\quad W[i] \leftarrow m[i] \oplus 2^i \cdot \Delta_0 \oplus 2^{2i} \cdot \Delta_1$	$x[2] \leftarrow 2^{k-1} \cdot Z[1] \oplus 2^{k-2} \cdot Z[2] \cdots \oplus Z[k]$
$\quad Z[i] \leftarrow \boldsymbol{\pi}_0(W[i])$	return $x := (x[1] \| x[2])$
$x[1] \leftarrow Z[1] \oplus Z[2] \cdots \oplus Z[k]$	
$x[2] \leftarrow Z[1] \oplus 2 \cdot Z[2] \cdots \oplus 2^{k-1} \cdot Z[k]$	
return $x := (x[1] \| x[2])$	

Two instances of CfHs will be the truncated versions of the above hash functions, TPHash and TLightHash, respectively. In fact, we have that 1k-PMAC+ $= 1k\text{-DBHtS}_{\mathsf{TPHash}}$ and 1k-LightMAC+ $= 1k\text{-DBHtS}_{\mathsf{TLightHash}}$.

17.2.1 *Affine bad events.*

For a diblock hash function H, any $\mathbf{x} = (x_1, \ldots, x_q) \in (\mathcal{X})_q$, and $c, c_1, c_2, c_3 \in \{0,1\}^2$, we define:

$$\mathsf{COLL}_H^{c_1,c_2}(\mathbf{x}): \ \exists^* i,j \in [q] \text{ such that } H_K(x_i) \oplus H_K(x_j) = (c_1\|0^{n-2}, c_2\|0^{n-2})$$

$$\mathsf{COLL1}_H^{c}(\mathbf{x}): \ \exists^* i,j \in [q] \text{ such that } H^1_K(x_i) \oplus H^1_K(x_j) = c\|0^{n-2}.$$

$$\mathsf{COLL2}_H^{c}(\mathbf{x}): \ \exists^* i,j \in [q] \text{ such that } H^2_K(x_i) \oplus H^2_K(x_j) = c\|0^{n-2}.$$

$$\mathsf{AP1}_H^{c_1,c_2,c_3}(\mathbf{x}): \ \exists^* i,j,k,l \in [q] \text{ such that } H^1_K(x_i) \oplus H^1_K(x_j) = c_1\|0^{n-2} \wedge H^2_K(x_j) \oplus H^2_K(x_k) = c_2\|0^{n-2} \wedge H^1_K(x_k) \oplus H^1_K(x_l) = c_3\|0^{n-2}.$$

$$\mathsf{AP2}_H^{c_1,c_2,c_3}(\mathbf{x}): \ \exists^* i,j,k,l \in [q] \text{ such that } H^2_K(x_i) \oplus H^2_K(x_j) = c_1\|0^{n-2} \wedge H^1_K(x_j) \oplus H^1_K(x_k) = c_2\|0^{n-2} \wedge H^2_K(x_k) \oplus H^2_K(x_l) = c_3\|0^{n-2}.$$

$$\mathsf{AP2}_H^{c_1,c_2}(\mathbf{x}): \ \exists^* i,j,k \in [q] \text{ such that } H^2_K(x_i) \oplus H^2_K(x_j) = c_1\|0^{n-2} \wedge H^1_K(x_j) \oplus H^1_K(x_k) = c_2\|0^{n-2}$$

$$\mathsf{MC1}_H^{c_1,\ldots,c_s}(\mathbf{x}): \ \exists^* i,j,k,l \in [q] \text{ such that } H^1_K(x_i) \oplus H^1_K(x_j) = c_1\|0^{n-2} \wedge \cdots \wedge H^1_K(x_{i_{s-1}}) \oplus H^1_K(x_{i_s}) = c_s\|0^{n-2}$$

$$\mathsf{MC2}_H^{c_1,\ldots,c_s}(\mathbf{x}): \ \exists^* i,j,k,l \in [q] \text{ such that } H^2_K(x_i) \oplus H^2_K(x_j) = c_1\|0^{n-2} \wedge \cdots \wedge H^2_K(x_{i_{s-1}}) \oplus H^2_K(x_{i_s}) = c_s\|0^{n-2}$$

One can readily check that

$$\mathsf{COLL1}_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{c\in\{0,1\}^2} \mathsf{COLL1}_H^{c}(\mathbf{x}) \qquad \mathsf{COLL2}_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{c\in\{0,1\}^2} \mathsf{COLL2}_H^{c}(\mathbf{x})$$

$$\mathsf{AP1}^4_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{\substack{(c_1,c_2,c_3)\\ \in(\{0,1\}^2)^3}} \mathsf{AP1}_H^{c_1,c_2,c_3}(\mathbf{x}) \qquad \mathsf{AP2}^4_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{\substack{(c_1,c_2,c_3)\\ \in(\{0,1\}^2)^3}} \mathsf{AP2}_H^{c_1,c_2,c_3}(\mathbf{x})$$

$$\mathsf{COLL}_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{\substack{(c_1,c_2)\\ \in(\{0,1\}^2)^2}} \mathsf{COLL}_H^{c_1,c_2}(\mathbf{x}) \qquad \mathsf{AP1}^3_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{\substack{(c_1,c_2)\\ \in(\{0,1\}^2)^3}} \mathsf{AP1}_H^{c_1,c_2,c_3}(\mathbf{x})$$

$$\mathsf{MC1}^s_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{\substack{c^s\\ \in(\{0,1\}^2)^s}} \mathsf{MC1}_H^{c_1,\cdots,c_s}(\mathbf{x}) \qquad \mathsf{MC2}^s_{\mathsf{T}H}(\mathbf{x}) = \bigvee_{\substack{c^s\\ \in(\{0,1\}^2)^s}} \mathsf{MC2}_H^{c_1,\cdots,c_s}(\mathbf{x})$$

(17.24)

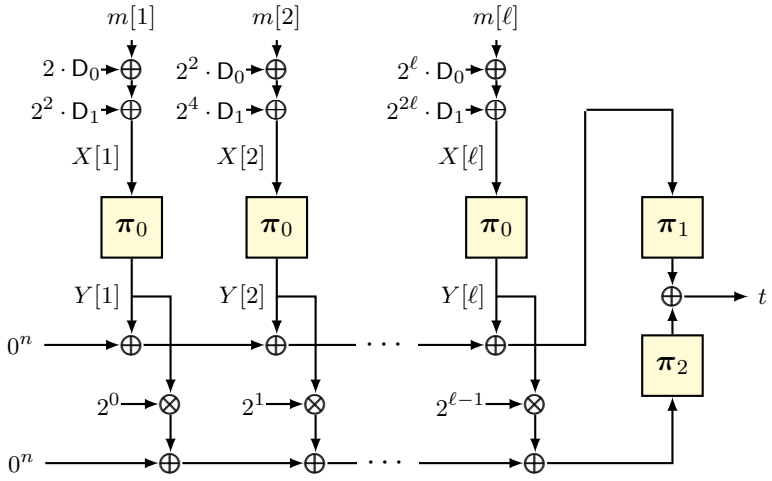


Figure 17.2: 1k-PMAC+

17.2.2 *TPHash.*

Our bad event analysis heavily depends on the one presented in [KLL20]. We tailor their bounds according to our needs while highlighting the main aspects of similarity and departure between their results and ours.

Similar to the PMAC+ analysis in [KLL20] we define analogous auxiliary events as follows: Let the i-th message be $m^i = m^i[1] \| \cdots \| m^i[\ell_i] \in (\{0,1\}^{n-2})^{\ell_i}$, $i \in [q]$. For $i \neq j \in [q]$, let $\ell = \min\{\ell_i, \ell_j\}$ and $\ell' = \max\{\ell_i, \ell_j\}$, then we can define the index set for which $m^i[k] \neq m^j[k]$ as

$$I_{ij} := \{k \in [\ell] : m^i[k] \neq m^j[k]\} \sqcup [\ell + 1..\ell']$$

We define the following random variables: $\mathsf{D}_0 := \mathsf{Trunc}(\boldsymbol{\pi}_0(0))$, $\mathsf{D}_1 := \mathsf{Trunc}(\boldsymbol{\pi}_0(1))$, and $\mathsf{W}^i = \mathsf{W}^i[1] \| \cdots \| \mathsf{W}^i[\ell_i]$, where $\mathsf{W}^i[k] = m^i[k] \oplus 2^k \cdot \mathsf{D}_0 \oplus 2^{2k} \cdot \mathsf{D}_1$. We further define the random index sets where W^i and W^j collide as follows:

$$\mathtt{I}_{\mathsf{col}} = \{(i,j) \in ([q])_2 : \exists^* k, k' \text{ such that } \mathsf{W}^i[k] = \mathsf{W}^j[k']\}$$
$$\mathtt{J}_{\mathsf{col}} = \{(i,j) \in ([q])_2 : \min\{I_{ij}\} \leq \ell_i \text{ and } \exists k \text{ such that } \mathsf{W}^i[\min\{I_{ij}\}] = \mathsf{W}^j[k]\}$$

Then the auxiliary events are:

Aux_1 : $\mathsf{D}_0 = 0 \vee \mathsf{D}_1 = 0$

Aux_2 : $\exists i \in [q], \exists^* k, k'$ such that $\mathsf{W}^i[k] = \mathsf{W}^i[k']$.

Aux_3 : $\exists i \in [q], k \in [\ell_i]$ such that $\mathsf{W}^i[k] \in \{0, 1, \boldsymbol{\pi}_0^{-1}(0)\}$.

Aux_4 : $|\mathtt{I}_{\mathsf{col}}| > s$, where $s = 2^n/4\overline{\sigma}$.

$\mathsf{Aux}_5 : |\mathsf{J}_{\mathsf{col}}| > s'$ where $s' = \ell q$

and let $\mathsf{Aux} = \bigvee_{i\in[5]} \mathsf{Aux}_i$.

Lemma 17.5. *For $\boldsymbol{m} = (m^i : i \in [q])$ and $c, c_1, c_2, c_3 \in \{0,1\}^2$,*

$$\Pr\left(\mathsf{COLL}^{c_1,c_2}_{\mathit{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}) \wedge \neg\mathsf{Aux}\right) \le \frac{4\ell q^2}{2^{2n}}$$
$$\Pr\left(\mathsf{AP1}^{c_1,c_2,c_3}_{\mathit{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}) \wedge \neg\mathsf{Aux}\right) \le \frac{2s'^2}{2^{2n}} + \frac{4s}{2^n} + \frac{2}{2^n} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{8sq^2}{2^{2n}} + \frac{96q^2}{2^{2n}} + \frac{8q^4}{2^{3n}}$$

Proof Sketch: First we note that, the following pairs of events, the left defined in [KLL20] and the right defined in this paper, are equivalent in the single-key scenario:

$$\mathsf{Bad}_1 \equiv \mathsf{COLL}^{0,0}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}), \qquad \mathsf{Bad}_2 \equiv \mathsf{AP1}^{0,0,0}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})$$

Analogous to Eq. (10) and (11) of [KLL20], we can write, for any $c \in \{0,1\}^2$,

$$\mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m^i) \oplus \mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m^j) = c\|0^{n-2} \iff A_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus A_t \cdot \mathsf{Z}[t] = c\|0^{n-2}$$
$$\mathsf{PHash}^2_{\boldsymbol{\pi}_0}(m^i) \oplus \mathsf{PHash}^2_{\boldsymbol{\pi}_0}(m^j) = c\|0^{n-2} \iff B_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus B_t \cdot \mathsf{Z}[t] = c\|0^{n-2}$$

where, for $(i,j) \in ([q])_2$, $\{\mathsf{W}[1], \ldots, \mathsf{W}[t]\} := \{\mathsf{W}^i[1], \ldots, \mathsf{W}^i[\ell_i]\} \cup \{\mathsf{W}^j[1], \ldots, \mathsf{W}^j[\ell_j]\}$, and for $k \in [t]$, $\mathsf{Z}[k] := \boldsymbol{\pi}_0(\mathsf{W}[k])$.

Thus, borrowing from the analysis of [KLL20], each of the events in the statement of this lemma can be written as an event that a system of equations $\boldsymbol{AZ} = \boldsymbol{c}$ holds, where $\boldsymbol{Z}$ is a vector with k-th component $\mathsf{Z}[k]$, and $\boldsymbol{c}$ depends on the indices c, c_1, c_2, c_3 of the corresponding event. If $\boldsymbol{c} \notin \mathscr{C}(\boldsymbol{A})$, then this system of equations will hold with 0 probability. If $\boldsymbol{c} \in \mathscr{C}(\boldsymbol{A})$ then the probability that this system of equations holds, depends on the rank of $\boldsymbol{A}$ and not on $\boldsymbol{c}$. So we have that

$$\Pr\left(\mathsf{COLL}^{c_1,c_2}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}) \wedge \neg\mathsf{Aux}\right) \le \Pr\left(\mathsf{COLL}^{0,0}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}) \wedge \neg\mathsf{Aux}\right) = \Pr\left(\mathsf{Bad}_1 \wedge \neg\mathsf{Aux}\right)$$
$$\Pr\left(\mathsf{AP1}^{c_1,c_2,c_3}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}) \wedge \neg\mathsf{Aux}\right) \le \Pr\left(\mathsf{AP1}^{0,0,0}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m}) \wedge \neg\mathsf{Aux}\right) = \Pr\left(\mathsf{Bad}_2 \wedge \neg\mathsf{Aux}\right)$$

Thus we can use the bounds on the corresponding bad events from [KLL20] to get our result. □

The probability analysis of the events $\mathsf{AP2}^{c_1,c_2,c_3}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})$ and $\mathsf{AP1}^{c_1,c_2}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})$ are similar to the analysis of the events $\mathsf{AP1}^{c_1,c_2,c_3}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})$ and $\mathsf{COLL}^{c_1,c_2}_{\mathsf{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})$, respectively.

Lemma 17.6. *For $\ell \le 2^{n-2}$, $m \ne m' \in (\{0,1\}^{n-2})^{\le\ell}$, and $c \in \{0,1\}^2$, we have*

$$\Pr\left(\mathit{PHash}^1_{\boldsymbol{\pi}_0}(m) \oplus \mathit{PHash}^1_{\boldsymbol{\pi}_0}(m') = c\|0^{n-2}\right) \le \frac{26\ell}{2^n}$$
$$\Pr\left(\mathit{PHash}^2_{\boldsymbol{\pi}_0}(m) \oplus \mathit{PHash}^2_{\boldsymbol{\pi}_0}(m') = c\|0^{n-2}\right) \le \frac{26\ell}{2^n}$$

Proof. Let $m \in (\{0,1\}^{n-2})^{\ell}$ and $m' \in (\{0,1\}^{n-2})^{\ell'}$. Note that the claim is trivial $\ell = 1$ and we ignore this case.

Let i be the maximum block-index where m and m' are distinct, precisely,

$$i = \begin{cases} \ell, & \text{if } \ell > \ell' \\ \max\{j \le \ell : m[j] \neq m'[j]\}, & \text{if } \ell = \ell' \end{cases}$$

Consider the random variables:

$$\begin{aligned} &\mathsf{D}_0 = \mathsf{trunc}(\boldsymbol{\pi}(0)), && \mathsf{D}_1 = \mathsf{trunc}(\boldsymbol{\pi}(1)), && \\ &\mathsf{W}[i] = m[i] \oplus 2^i \cdot \mathsf{D}_0 \oplus 2^{2i} \cdot \mathsf{D}_1, && \mathsf{Z}[i] = \boldsymbol{\pi}_0(\mathsf{W}[i]), && i \in [\ell] \\ &\mathsf{W}'[i] = m'[i] \oplus 2^i \cdot \mathsf{D}_0 \oplus 2^{2i} \cdot \mathsf{D}_1, && \mathsf{Z}'[i] := \boldsymbol{\pi}_0(\mathsf{W}'[i]), && i \in [\ell'] \end{aligned}$$

Let us define the following events:

$$\begin{aligned} &\mathsf{E}_1 : \mathsf{D}_0 = 0 \\ &\mathsf{E}_2 : \bigvee_{j \in [\ell]} (\mathsf{W}[j] = 0 \vee \mathsf{W}[j] = 1) \vee \bigvee_{j \in [\ell']} (\mathsf{W}'[j] = 0 \vee \mathsf{W}'[j] = 1) \\ &\mathsf{E}_3 : \bigvee_{\substack{j \in [\ell] \\ j \neq i}} (\mathsf{W}[i] = \mathsf{W}[j]) \vee \bigvee_{j \in [\ell']} (\mathsf{W}[i] = \mathsf{W}'[j]) \end{aligned}$$

Note that $\Pr\left(c \cdot \mathsf{Trunc}(\boldsymbol{\pi}(a)) = b\right) = 4/2^n$ for any $a \in \{0,1\}^n$ and $b, c \in \{0,1\}^{n-2}$ with $c \neq 0$. Hence, for any $a_1, \ldots, a_r \in \{0,1\}^n$ and $b, c_1, \ldots, c_r \in \{0,1\}^{n-2}$ with $c_r \neq 0$, we have

$$\begin{aligned} &\Pr\left(c_1 \cdot \mathsf{Trunc}(\boldsymbol{\pi}(a_1)) \oplus \cdots \oplus c_r \cdot \mathsf{Trunc}(\boldsymbol{\pi}(a_r)) = b\right) \\ &= \sum_{\substack{b'_1, \ldots, b'_{r_1} \\ \in \{0,1\}^n \\ \text{all distinct}}} \Pr\left(\mathsf{Trunc}(\boldsymbol{\pi}(a_r)) = b'\right) \Pr\left(\boldsymbol{\pi}(a_i) = b'_i \; \forall i \in [r-1]\right) \\ &\le \frac{4}{2^n - r + 1} \end{aligned}$$

where $b_i = \mathsf{trunc}(b'_i)$ and $b' = c_r^{-1} \cdot (b \oplus c_1 \cdot b_1 \oplus \cdots \oplus c_{r-1} \cdot b_{r-1})$. Similarly for any $a_1, \ldots, a_r \in \{0,1\}^n$ and $b, c_1, \ldots, c_r \in \{0,1\}^{n-2}$ with at least one $c_i \neq 0$, we have

$$\Pr\left(c_1 \cdot \boldsymbol{\pi}(a_1) \oplus \cdots \oplus c_r \cdot \boldsymbol{\pi}(a_r) = b\right) \le \frac{1}{2^n - r + 1}. \tag{17.25}$$

This implies $\Pr\left(\mathsf{E}_1\right) = \Pr\left(\mathsf{trunc}(\boldsymbol{\pi}(0)) = 0\right) = 4/2^n$, $\Pr\left(\mathsf{E}_2 \mid \mathsf{E}_1^c\right) \le 4\ell \cdot 4/2^n$, and $\Pr\left(\mathsf{E}_3 \mid \mathsf{E}_1^c \wedge \mathsf{E}_2^c\right) \le (2\ell - 1) \cdot 4/2^n$.

Now the event $\mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m) \oplus \mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m') = c \| 0^{n-2}$, is equivalent to $\mathsf{Z}[1] \oplus \cdots \oplus \mathsf{Z}[\ell] \oplus \mathsf{Z}'[1] \oplus \cdots \oplus \mathsf{Z}'[\ell'] = c \| 0^{n-2}$. Of course, if any two Z-random variables are identically equal

then they cancel out. However, conditional on $\mathsf{E}_1^c \wedge \mathsf{E}_2^c \wedge \mathsf{E}_3^c$ we have $\mathsf{Z}[i] \neq \mathsf{Z}[j], \mathsf{Z}'[j']$ for any $j \in [m] \setminus \{i\}, j' \in [m']$ and $\mathsf{Z}[i] \neq 0, \boldsymbol{\pi}(0), \boldsymbol{\pi}(1)$. Hence from Eq. (17.25), we have

$$\Pr\left(\mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m) \oplus \mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m') = c\|0^{n-2} \mid \mathsf{E}_1^c \wedge \mathsf{E}_2^c \wedge \mathsf{E}_3^c\right) \leq \frac{1}{2^n - (m-1) - m' - 2} \leq \frac{1}{2^n - 2\ell} \leq 2/2^n$$

assuming $\ell \leq 2^{n-2}$.

Since for any two events A and B, we have $\Pr(\mathsf{A}) = \Pr(\mathsf{A} \wedge \mathsf{B}) + \Pr(\mathsf{A} \wedge \mathsf{B}^c)$ and $\Pr(\mathsf{A} \wedge \mathsf{B}) \leq \Pr(\mathsf{A})$ and $\Pr(\mathsf{A} \wedge \mathsf{B}) \leq \Pr(\mathsf{A} \mid \mathsf{B})$, we have

$$\begin{aligned}
&\Pr\left(\mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m) \oplus \mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m') = c\|0^{n-2}\right) \\
&\leq \Pr(\mathsf{E}_1) + \Pr(\mathsf{E}_2 \mid \mathsf{E}_1^c) + \Pr(\mathsf{E}_3 \mid \mathsf{E}_1^c \wedge \mathsf{E}_2^c) \\
&\quad + \Pr\left(\mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m) \oplus \mathsf{PHash}^1_{\boldsymbol{\pi}_0}(m') = c\|0^{n-2} \mid \mathsf{E}_1^c \wedge \mathsf{E}_2^c \wedge \mathsf{E}_3^c\right) \\
&\leq \frac{4}{2^n} + \frac{16\ell}{2^n} + \frac{8\ell - 4}{2^n} + \frac{2}{2^n} \leq \frac{26\ell}{2^n}
\end{aligned}$$

Same argument shows that $\Pr\left(\mathsf{PHash}^2_{\boldsymbol{\pi}_0}(m) \oplus \mathsf{PHash}^2_{\boldsymbol{\pi}_0}(m') = c\|0^{n-2}\right) \leq 26\ell/2^n$. □

Corollary 17.6.1.

$$\Pr\left(\mathsf{COLL1}^c_{\mathit{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{13\ell q^2}{2^n} \qquad \Pr\left(\mathsf{COLL2}^c_{\mathit{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{13\ell q^2}{2^n}$$

$$\Pr\left(\mathsf{MC1}^{c_1,\ldots,c_s}_{\mathit{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{13\ell q^2}{s \cdot 2^n} \qquad \Pr\left(\mathsf{MC2}^{c_1,\ldots,c_s}_{\mathit{PHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{13\ell q^2}{s \cdot 2^n}$$

The Corollary 17.6.1 follows from Lemma 17.6 by simple application of the Markov's inequality.

Finally, we bound the auxiliary events

Lemma 17.7. *We have*

$$\Pr(\mathsf{Aux}_1 \vee \mathsf{Aux}_3) \leq \frac{3\ell q}{2^n - 2} + \frac{2}{2^n} \qquad \Pr(\mathsf{Aux}_2) \leq \frac{\ell^2 q}{2^{n+1}}$$

$$\Pr(\mathsf{Aux}_4) \leq \frac{\ell^2 q^2}{s \cdot 2^n} \qquad \Pr(\mathsf{Aux}_5) \leq \frac{\ell q^2}{s' \cdot 2^n}$$

Combining these bounds we have

$$\Pr(\mathsf{Aux}) \leq \frac{(\ell^2 + 8\ell)q}{2^{n+1}} + \frac{\ell^2 q^2}{s \cdot 2^n} + \frac{\ell q^2}{s' \cdot 2^n}$$

Combining Eq. (17.24), Lemma 17.5, Corollary 17.6.1 and Lemma 17.7 we have the following result:

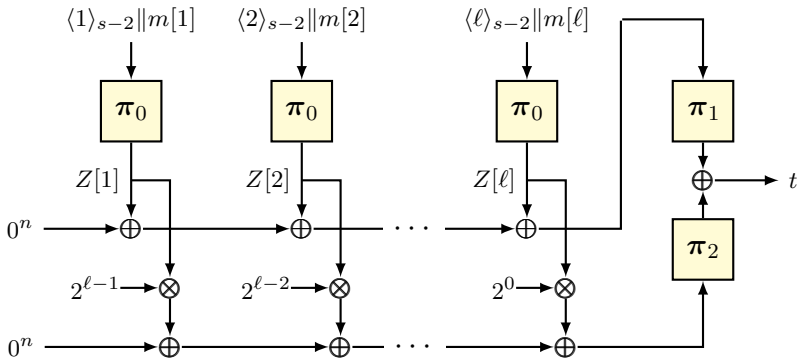


Figure 17.3: 1k-LightMAC+

Lemma 17.8. *TPHash$_{\pi_0}$ is a $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-CfH where*

$$\epsilon_1(\rho) = \frac{26\ell q^2}{2^n}, \qquad \epsilon_2(\rho, 3) = \frac{16\ell q^2}{2^{2n}}, \qquad \epsilon_3(\rho, s) = \frac{2^s \cdot 13\ell q^2}{s \cdot 2^n}, \qquad \delta(\rho) = \frac{16\ell q^2}{2^{2n}}$$
$$\epsilon_2(\rho, 4) = 8 \cdot \left(\frac{2s'^2}{2^{2n}} + \frac{4s}{2^n} + \frac{2}{2^n} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{8sq^2}{2^{2n}} + \frac{96q^2}{2^{2n}} + \frac{8q^4}{2^{3n}} \right)$$

17.2.3 *TLightHash.*

As before, we let the i-th message be $m^i = m^i[1]\| \cdots \|m^i[\ell_i] \in (\{0,1\}^{n-s})^{\ell_i}$, $i \in [q]$. Note that, $m^i[k] \neq m^j[k] \iff \mathsf{Z}^i[k] \neq \mathsf{Z}^j[k]$ for any $k \in [\max\{\ell_i, \ell_j\}]$, where $\mathsf{Z}^i[k] := \pi_0(\langle k\rangle_{s-2}\|m^i[k])$. Moreover, $\mathsf{Z}^i[k] \neq \mathsf{Z}^j[k']$ for any $k \neq k'$, $i, j \in [q]$. Let us fix $(i, j) \in ([q])_2$, define $\{\mathsf{Z}[1], \ldots, \mathsf{Z}[t]\} := \{\mathsf{Z}^i[k] : k \in [\ell_i]\} \cup \{\mathsf{Z}^j[k] : k \in [\ell_j]\}$ and partition $[t] := \mathtt{I}_{ij}^{=} \sqcup \mathtt{I}_{\bar{i}\bar{j}}^{=} \sqcup \mathtt{I}_{i\bar{j}}^{=}$, where

$$\mathtt{I}_{ij}^{=} := \{k \in [t] : \mathsf{Z}[k] = \mathsf{Z}^i[k'] \neq \mathsf{Z}^j[k'], k' \in [\max\{\ell_i, \ell_j\}]\}$$
$$\mathtt{I}_{\bar{i}\bar{j}}^{=} := \{k \in [t] : \mathsf{Z}[k] = \mathsf{Z}^i[k'] = \mathsf{Z}^j[k'], k' \in [\max\{\ell_i, \ell_j\}]\}$$
$$\mathtt{I}_{i\bar{j}}^{=} := \{k \in [t] : \mathsf{Z}[k] = \mathsf{Z}^j[k'] \neq \mathsf{Z}^i[k'], k' \in [\max\{\ell_i, \ell_j\}]\}$$

Then we have

$$\begin{aligned} &\mathsf{LightHash}^1_{\pi_0}(m^i) \oplus \mathsf{LightHash}^1_{\pi_0}(m^j) = c\|0^{n-2} \\ &\qquad \iff A_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus A_t \cdot \mathsf{Z}[t] = c\|0^{n-2} \\ &\mathsf{LightHash}^2_{\pi_0}(m^i) \oplus \mathsf{LightHash}^2_{\pi_0}(m^j) = c\|0^{n-2} \\ &\qquad \iff B_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus B_t \cdot \mathsf{Z}[t] = c\|0^{n-2} \end{aligned}$$

where

- $A_k = 1$ for $k \in \mathtt{I}_{\bar{i}j} \sqcup \mathtt{I}_{i\bar{j}}$, $A_k = 0$, otherwise.
- $B_k = 2^\beta$ for some β, if $k \in \mathtt{I}_{\bar{i}j} \sqcup \mathtt{I}_{i\bar{j}}$, otherwise $B_k = 2^\beta \oplus 2^\gamma$ for some β, γ.

Due to this similarity with PHash, the argument given in Lemma 17.5 also holds here, giving us

$$\Pr\left(\mathsf{COLL}^{c_1,c_2}_{\mathsf{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \Pr\left(\mathsf{COLL}^{0,0}_{\mathsf{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right)$$
$$\Pr\left(\mathsf{AP1}^{c_1,c_2,c_3}_{\mathsf{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \Pr\left(\mathsf{AP1}^{0,0,0}_{\mathsf{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right)$$
$$\Pr\left(\mathsf{AP2}^{c_1,c_2,c_3}_{\mathsf{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \Pr\left(\mathsf{AP2}^{0,0,0}_{\mathsf{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right)$$

Lemma 17.9. *Assume $\ell \leq 2^n/4$. Then in the ideal world,*

$$\Pr\left(\mathsf{COLL}^{0,0}_{\mathit{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{2q^2}{2^{2n}}$$

Proof. We fix $(i,j) \in ([q])_2$ as above, thus fixing $\{\mathsf{Z}[1], \ldots, \mathsf{Z}[t]\}$ and partitioning $[t] = \mathtt{I}_{\bar{i}j} \sqcup \mathtt{I}_{\bar{i}\bar{j}} \sqcup \mathtt{I}_{i\bar{j}}$. We can make the following observations about the index sets:

- $\mathtt{I}_{\bar{i}j} \sqcup \mathtt{I}_{i\bar{j}} \neq \emptyset$ since otherwise m^i and m^j will not be distinct.
- $|\mathtt{I}_{\bar{i}j} \sqcup \mathtt{I}_{i\bar{j}}| \geq 2$ because otherwise $\mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^i) \neq \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^j)$.

If we consider the system of linear equations representing the events $\mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^i) = \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^j)$ and $\mathsf{LightHash}^2_{\boldsymbol{\pi}_0}(m^i) = \mathsf{LightHash}^2_{\boldsymbol{\pi}_0}(m^j)$, respectively:

$$A_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus A_t \cdot \mathsf{Z}[t] = 0^n$$
$$B_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus B_t \cdot \mathsf{Z}[t] = 0^n$$

then the above observations about the index sets imply that there are two distinct indices $k, k' \in \mathtt{I}_{\bar{i}j} \sqcup \mathtt{I}_{i\bar{j}}$ such that $A_k = A_{k'} = 1$ and $B_k = 2^\beta$, $B_{k'} = 2^\gamma$ for distinct β and γ. This implies that the above system of linear equations has rank 2, and hence will be satisfied with probability $(2^n)_{t-2}/(2^n)_t = 1/(2^n - t + 2)(2^n - t + 1) \leq (2^n - 2\ell + 2)(2^n - 2\ell + 1) \leq 4/2^{2n}$ for $\ell \leq 2^n/4$. Since there are $q(q-1)/2$ tuples $(i,j) \in ([q])_2$, we have our result. □

Lemma 17.10. *Assume that $\ell \leq 2^n/8$. Then in the ideal world, one has,*

$$\Pr\left(\mathsf{AP1}^{0,0,0}_{\mathit{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{q^4}{3 \cdot 2^{3n}} + \frac{q^2}{2 \cdot 2^{3n/2}} + \frac{2}{2^n} + \frac{96q^2}{2^{2n}}$$

Proof. Let us fix $(i,j,r,s) \in ([q])_4$. We want to find the probability of the event

$$\begin{aligned}\mathsf{E}(i,j,r,s) : \big(\mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^i) = \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^j)\big) \\ \wedge \big(\mathsf{LightHash}^2_{\boldsymbol{\pi}_0}(m^j) = \mathsf{LightHash}^2_{\boldsymbol{\pi}_0}(m^r)\big) \\ \wedge \big(\mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^r) = \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^s)\big)\end{aligned}$$

Let $\{\mathsf{Z}[1],\ldots,\mathsf{Z}[t]\} = \{\mathsf{Z}^i[k] : k \in [\ell_i]\} \cup \{\mathsf{Z}^j[k] : k \in [\ell_j]\} \cup \{\mathsf{Z}^r[k] : k \in [\ell_r]\} \cup \{\mathsf{Z}^s[k] : k \in [\ell_s]\}$. Also let us partition $[t]$ in three ways as $[t] = \mathtt{I}_{\bar{i}\bar{j}} \sqcup \mathtt{I}_{i\bar{j}} \sqcup \mathtt{I}_{\bar{i}\bar{j}} \sqcup \mathtt{I}_{ij} = \mathtt{I}_{\bar{j}\bar{r}} \sqcup \mathtt{I}_{j\bar{r}} \sqcup \mathtt{I}_{\bar{j}\bar{r}} \sqcup \mathtt{I}_{jr} = \mathtt{I}_{\bar{r}s} \sqcup \mathtt{I}_{r\bar{s}} \sqcup \mathtt{I}_{\bar{r}\bar{s}} \sqcup \mathtt{I}_{rs}$ where

$$\begin{aligned}\mathtt{I}_{\bar{i}\bar{j}} &:= \{k : \mathsf{Z}[k] = \mathsf{Z}^i[k'] \neq \mathsf{Z}^j[k'], k' \in [\max\{\ell_i,\ell_j,\ell_r,\ell_s\}]\} \\ \mathtt{I}_{i\bar{j}} &:= \{k : \mathsf{Z}[k] = \mathsf{Z}^j[k'] \neq \mathsf{Z}^i[k'], k' \in [\max\{\ell_i,\ell_j,\ell_r,\ell_s\}]\} \\ \mathtt{I}_{\bar{i}\bar{j}} &:= \{k : \mathsf{Z}[k] = \mathsf{Z}^i[k'] = \mathsf{Z}^j[k'], k' \in [\max\{\ell_i,\ell_j,\ell_r,\ell_s\}]\} \\ \mathtt{I}_{ij} &:= \{k : \mathsf{Z}[k] \neq \mathsf{Z}^i[k'], \mathsf{Z}[k] \neq \mathsf{Z}^j[k'], k' \in [\max\{\ell_i,\ell_j,\ell_r,\ell_s\}]\}\end{aligned}$$

and the rest of the index sets are defined analogously.

Then the above event can be represented by the following system of equations

$$\begin{aligned}A_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus A_t \cdot \mathsf{Z}[t] &= 0^n \\ B_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus B_t \cdot \mathsf{Z}[t] &= 0^n \\ C_1 \cdot \mathsf{Z}[1] \oplus \cdots \oplus C_t \cdot \mathsf{Z}[t] &= 0^n\end{aligned}$$

where

- $A_k = 1$ if $k \in \mathtt{I}_{\bar{i}\bar{j}} \sqcup \mathtt{I}_{i\bar{j}}$, and $A_k = 0$ otherwise.
- $B_k = 2^\beta$ for some β if $k \in \mathtt{I}_{\bar{j}r} \sqcup \mathtt{I}_{j\bar{r}}$, $B_k = 2^\beta \oplus 2^\gamma$ for some β,γ if $k \in \mathtt{I}_{\bar{j}\bar{r}}$, and $B_k = 0$ otherwise.
- $C_k = 1$ if $k \in \mathtt{I}_{\bar{r}s} \sqcup \mathtt{I}_{r\bar{s}}$, and $C_k = 0$ otherwise.

As observed in the proof of Lemma 17.9, $|\mathtt{I}_{\bar{i}\bar{j}} \sqcup \mathtt{I}_{i\bar{j}}| \geq 2$ and $|\mathtt{I}_{\bar{r}s} \sqcup \mathtt{I}_{r\bar{s}}| \geq 2$. Let us call the coefficient matrix of the above system of equations $M^{(i,j,r,s)}$, its first row as $A^{(i,j,r,s)}$, second row as $B^{(i,j,r,s)}$ and third row as $C^{(i,j,r,s)}$. Let us write $([q])_4$ as union of three index sets, $([q])_4 = \mathtt{J}_1 \sqcup \mathtt{J}_2 \sqcup \mathtt{J}_3$, where $\mathtt{J}_i$ are defined as follows:

$$\begin{aligned}\mathtt{J}_1 &:= \{(i,j,r,s) : \mathrm{rank}(M^{(i,j,r,s)}) = 3\} \\ \mathtt{J}_2 &:= \{(i,j,r,s) : A^{(i,j,r,s)} = C^{(i,j,r,s)}\}\} \\ \mathtt{J}_2 &:= \{(i,j,r,s) : B^{(i,j,r,s)} = c_1 A^{(i,j,r,s)} \oplus c_2 C^{(i,j,r,s)} \text{ for } c_1,c_2 \neq 0\}\end{aligned}$$

For $(i,j,r,s) \in \mathsf{J}_1$, the probability of the Z-variables satisfying the system of equations is $(2^n)_{t-3}/(2^n)_t \le 8/2^{3n}$ for $\ell \le 2^n/8$, since $t \le 4\ell$. Thus we have

$$\Pr\left[\bigvee_{(i,j,r,s)\in\mathsf{J}_1} \mathsf{E}(i,j,r,s)\right] \le \frac{q^4}{3\cdot 2^{3n}} \tag{17.26}$$

Now let us define the equivalence relation over $([q])_2$ as $(i,j) \sim (r,s)$ if $\mathtt{I}_{\overline{ij}} \sqcup \mathtt{I}_{i\overline{j}} = \mathtt{I}_{\overline{r}s} \sqcup \mathtt{I}_{r\overline{s}}$. If $(i,j) \sim (r,s)$, then $A^{(i,j,r,s)} = C^{(i,j,r,s)}$, which implies $\mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^i) = \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^j) \iff \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^r) = \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^s)$. Suppose the above relations partitions $([q])_2$ into c equivalence classes $([q])_2 = C_1 \sqcup \cdots \sqcup C_c$. For $a = 1,\ldots,c$, consider the events E_a that $\mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^i) = \mathsf{LightHash}^1_{\boldsymbol{\pi}_0}(m^j)$ for every $(i,j) \in C_a$. Thus from Eq. (17.25) we have that

$$\Pr[\mathsf{E}_a] \le \frac{1}{2^n - 2\ell + 1}$$

since $|\mathtt{I}_{\overline{ij}} \sqcup \mathtt{I}_{i\overline{j}}| \le 2\ell$ for all $(i,j) \in C_a$. Now we have

$$\begin{aligned}
&\Pr\left[\bigvee_{(i,j,r,s)\in\mathsf{J}_2} \mathsf{E}(i,j,r,s)\right] = \Pr\left[\bigvee_{a\in[c]}\ \bigvee_{(i,j),(r,s)\in C_a} \mathsf{E}(i,j,r,s)\right] \\
&\le \sum_{a=1}^{c} \Pr\left[\bigvee_{(i,j),(r,s)\in C_a} \mathsf{E}(i,j,r,s)\right] \\
&= \sum_{a=1}^{c} \Pr[\mathsf{E}_a] \cdot \Pr\left(\bigvee_{(i,j),(r,s)\in C_a} \mathsf{LightHash}^2_{\boldsymbol{\pi}_0}(m^j) = \mathsf{LightHash}^2_{\boldsymbol{\pi}_0}(m^r) \mid \mathsf{E}_a\right) \\
&\le \sum_{a=1}^{c} \frac{1}{2^n - 2\ell + 1} \cdot \min\left\{\frac{|C_a|^2}{2(2^n - 2\ell + 1)}, 1\right\}
\end{aligned}$$

where the last inequality follows from Eq. (17.25) and the facts that $A^{(i,j,r,s)}$ and $B^{(i,j,r,s)}$ are linearly independent, and that $|\mathtt{I}_{\overline{j}r} \sqcup \mathtt{I}_{j\overline{r}} \sqcup \mathtt{I}_{\overline{j}\overline{r}}| \le 2\ell$ for all $(j,r) \in C_a$. Note that $1/(2^n - 2\ell + 1) \le 2/2^n$ for $\ell \le 2^n/8$. Subject to the condition that $\sum_{a=1}^{c} |C_a| = \binom{q}{2}$, the sum $\sum_{a=1}^{c} \min\{|C_a|^2/(2(2^n - 2\ell + 1)), 1\}$ is maximized when $c = \lfloor \binom{q}{2}/2^{n/2} \rfloor + 1$, $|C_a| = 2^{n/2}$ for $a \in [c-1]$ and $|C_c| = \binom{q}{2} - (c-1)2^{n/2}$, in which case we have

$$\sum_{c=1}^{a} \frac{2}{2^n} \cdot \min\left\{\frac{|C_a|^2}{2^n}, 1\right\} \le \frac{q^2}{2\cdot 2^{3n/2}} + \frac{2}{2^n}.$$

Thus we have

$$\Pr\left[\bigvee_{(i,j,r,s)\in\mathsf{J}_1} \mathsf{E}(i,j,r,s)\right] \le \frac{q^2}{2\cdot 2^{3n/2}} + \frac{2}{2^n} \tag{17.27}$$

Finally we consider $(i,j,r,s) \in \mathsf{J}_3$. In this case $B^{(i,j,r,s)} = c_1 A^{(i,j,r,s)} + c_2 C^{(i,j,r,s)}$. This linear dependence implies the following:

- $c_1 = 2^\beta$ and $c_2 = 2^\gamma$ for some β, γ.
- $(\mathtt{I}_{\overline{ij}} \sqcup \mathtt{I}_{i\overline{j}}) \triangle (\mathtt{I}_{\overline{r}s} \sqcup \mathtt{I}_{r\overline{s}}) = \mathtt{I}_{\overline{jr}} \sqcup \mathtt{I}_{j\overline{r}}$.[2] Also $B_k, k \in \mathtt{I}_{\overline{jr}}$ are all distinct, and similarly, $B_k, k \in \mathtt{I}_{j\overline{r}}$ are all distinct
- $(\mathtt{I}_{\overline{ij}} \sqcup \mathtt{I}_{i\overline{j}}) \cap (\mathtt{I}_{\overline{r}s} \sqcup \mathtt{I}_{r\overline{s}}) = \mathtt{I}_{\overline{j}\overline{r}}$. From the definition of the index sets, this reduces to $\mathtt{I}_{i\overline{j}} \cap \mathtt{I}_{\overline{r}s} = \mathtt{I}_{\overline{j}\overline{r}}$. If for $k \in \mathtt{I}_{\overline{j}\overline{r}}$, $\mathsf{Z}[k] = \mathsf{Z}^j[k'] = \mathsf{Z}^r[k']$, then $B_k = 2^{\ell_j - k'} + 2^{\ell_r - k'}$. Since $2^a + 2^b = 2^c + 2^d$ implies either $(a,b) = (c,d)$ or $(a,b) = (d,c)$, and since in this case for every $k \in \mathtt{I}_{\overline{j}\overline{r}}$, $B_k = 2^\beta + 2^\gamma$, we have $|\mathtt{I}_{\overline{j}\overline{r}}| = 1$.

Thus the following assumptions made in proof of Lemma 4 of [KLL20] holds true:

- $B^{(i,j,r,s)}$ does not contain the same entry more than twice.
- $B^{(i,j,r,s)}$ contains at least two different non-zero entries.
- Each of $A^{(i,j,r,s)}$ and $C^{(i,j,r,s)}$ contains at least three ones.

The rest of the analysis is exactly the one presented in the proof of Lemma 4 of [KLL20], except the ignorable fact that the coefficient of $\mathsf{Z}^j[k']$ is $2^{\ell_j - k'}$ (instead of $2^{k'}$ as in the [KLL20]), which however makes no changes in the argument presented. Thus following the proof of Lemma 4 of [KLL20], we have

$$\Pr\left[\bigvee_{(i,j,r,s)\in \mathsf{J}_3} (i,j,r,s)\right] \leq \frac{24q^2}{(2^n - 4\ell + 1)(2^n - 4\ell + 2)} \leq \frac{96q^2}{2^{2n}} \tag{17.28}$$

for $\ell \leq 2^n/8$.

Combining Eqs. (17.26), (17.27) and (17.28) we have our result. □

The probability analysis of the events $\mathsf{AP2}^{c_1,c_2,c_3}_{\mathsf{LightHash}_{\pi_0}}(\boldsymbol{m})$ and $\mathsf{AP1}^{c_1,c_2}_{\mathsf{LightHash}_{\pi_0}}(\boldsymbol{m})$ are similar to the analysis of the events $\mathsf{AP1}^{c_1,c_2,c_3}_{\mathsf{LightHash}_{\pi_0}}(\boldsymbol{m})$ and $\mathsf{COLL}^{c_1,c_2}_{\mathsf{LightHash}_{\pi_0}}(\boldsymbol{m})$, respectively, and we get the same probability bounds.

The exact same arguments given to prove Lemma 17.6 can be used to prove the following statement, keeping in mind that we do not need to consider the events E_1 and E_2, described in the proof of Lemma 17.6, for LightHash:

Lemma 17.11. *For $\ell \leq 2^{n-2}$, $m \neq m' \in (\{0,1\}^{n-2})^{\leq \ell}$, and $c \in \{0,1\}^2$, we have*

$$\Pr\left(\mathit{LightHash}^1_{\pi_0}(m) \oplus \mathit{LightHash}^1_{\pi_0}(m') = c \| 0^{n-2}\right) \leq \frac{8\ell}{2^n}$$

$$\Pr\left(\mathit{LightHash}^2_{\pi_0}(m) \oplus \mathit{LightHash}^2_{\pi_0}(m') = c \| 0^{n-2}\right) \leq \frac{8\ell}{2^n}$$

2 For two sets A, B, we denote their symmetric difference as $A \triangle B := (A \setminus B) \cup (B \setminus A)$

Corollary 17.11.1.

$$\Pr\left(\mathsf{COLL1}^{c}_{\mathit{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{4\ell q^2}{2^n} \qquad \Pr\left(\mathsf{COLL2}^{c}_{\mathit{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{4\ell q^2}{2^n}$$
$$\Pr\left(\mathsf{MC1}^{c_1,\ldots,c_s}_{\mathit{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{4\ell q^2}{s\cdot 2^n} \qquad \Pr\left(\mathsf{MC2}^{c_1,\ldots,c_s}_{\mathit{LightHash}_{\boldsymbol{\pi}_0}}(\boldsymbol{m})\right) \leq \frac{4\ell q^2}{s\cdot 2^n}$$

Thus we get our desired result:

Lemma 17.12. *$\mathit{TLightHash}_{\boldsymbol{\pi}_0}$ is a $(\epsilon_1,\epsilon_2,\epsilon_3,\delta)$-CfH, where*

$$\epsilon_1(\rho) = \frac{8\ell q^2}{2^n}, \qquad \epsilon_2(\rho,3) = \frac{8q^2}{2^{2n}}, \qquad \epsilon_3(\rho,s) = \frac{2^s\cdot 4\ell q^2}{s\cdot 3^n}, \qquad \delta(\rho) = \frac{8q^2}{2^{2n}}$$
$$\epsilon_2(\rho,4) = 8\cdot\left(\frac{q^4}{3\cdot 2^{3n}} + \frac{q^2}{2\cdot 2^{3n/2}} + \frac{2}{2^n} + \frac{96q^2}{2^{2n}}\right)$$

Part IV

REFLECTIONS

In this final part we summarize the dissertation and explore the possible future directions that our works inspire.

18 CONCLUSION AND FUTURE DIRECTIONS

In this thesis we have explored different variants of the Mirror Theory problem, CMTP, BMTP, CRMTP and RPRMTP, achieving optimal or near-optimal lower bounds on the number of solutions in each of the cases, backing them up by mathematically rigorous and verifiable proofs. We have also applied the respective bounds for beyond-birthday-bound security analyses (tight in most cases) of different constructions, that have their own rich history and importance in the symmetric cryptography landscape: PRP-to-PRF constructions, like XOR_1, XOR_2, XORP, 2k-HtmB-p2, sum of Even-Mansour, MACs like 1k-PMAC+ and 1k-LightMAC+ , the PRF-to PRP-construction six-round Feistel, and the TBC construction like 4-LRW1 and 2-LRW2. In this dissertation, we have tried to paint an elaborate picture of the variety and depth of the Mirror Theory problems, both as a theoretical pursuit and a practical tool for tackling provable security analyses.

However, it is always good from a research perspective if you have more questions than answers. Indeed, the works presented above opens up many unexplored alleyways and unclosed gaps.

OPEN VARIANTS OF MIRROR THEORY. The Mirror Theory problem is a very general one, and we have only dealt with very few very structured subclasses of it. So of course, there remains many more problems to cover:

- In this dissertation we have only considered mirror theory problems where the system of non-equations is both bivariate and homogeneous, i. e., the non-equations are of the form $\mathsf{X} \oplus \mathsf{X} \neq 0^n$. However there are cryptographic constructions like the Feistel network with permutations as underlying primitives (used for domain extension of permutations), whose security analyses lead to a systems of non-equations that are not homogeneous. Thus to find a tight lower bound to system of equations and non-homogeneous system of non-equations is an important open problem.
- We have also restricted our attention to the binary field $\mathbb{F}_2^n$ with its involutory operation $\oplus$. Also our proof strategy for CMTP inherently depends on the underlying field being of characteristic 2. It will be interesting to extend the results to a different field, where the binary operation is not involutory.

OTHER OPEN PROBLEMS. In this dissertation we have presented a birthday-bound attack on TNT and a $3n/4$-bit security of the LRW+ paradigm. This leaves us with two important research directions:

- Is there any TBC construction using only three blockcipher calls, like TNT, that achieves BBB security? We believe this will have a negative answer.
- The security bound for 4-LRW1 is not tight. So either we need to look for a matching attack, or a tighter security analysis that results in more than $3n/4$-bit security. It is worthwhile to note that the the lower bound analysis for BMTP in tweakable permutation setting, is not tight enough, since unlike the CMTP case, we have not probed beyond the link deletion equation. We hope a tighter lower bound analysis of BMTP in tweakable permutation setting would lead to better security bound for 4-LRW1.

BEYOND MIRROR THEORY. We would also like to note that we have proved n-bit security of the XOR_2, whereas the only attack against it, proposed by Patarin, requires $O(2^{3n/2})$ queries. However the lower bound analysis of the corresponding BMTP problem for $\xi_{\max} = 2$ seems to be tight enough and might not lead to better bounds. However, in a recent work [Din24] by Itai Dinur, awarded the best paper in EUROCRYPT 2024, has proved $3n/2$-bit tight security of the XOR_2 construction, introducing the novel strategy of bounding (sums of) Fourier coefficients of the transcript distribution function. In fact they proved that the xor of r independent permutations leads to $q/2^{(r-1/2)n}$ single-user security and $\sqrt{u}q_{\max}/2^{(r-1/2)n}$ multi-user security. The results imply that this methodology might be quite powerful, and worth looking into.

Part V

APPENDIX

APPENDIX

A

A.1 PROBABILITY THEORY

We present here a general overview of probability measures on any measurable space, and then tailor it according to needs of this dissertation.

Definition A.1 (σ-field). *For a set Ω, we call $\mathscr{F} \subseteq 2^{\Omega}$ a σ-field if the following conditions are satisfied:*

- $\Omega \in \mathscr{F}$
- $A \in \mathscr{F} \iff A^c \in \mathscr{F}$
- *For any countable collection of sets, $\{A_i : i \in \mathscr{I}\}$, such that $A_i \in \mathscr{F}$, $\forall i \in \mathscr{I}$, we have $\bigcup_{i\in\mathscr{I}} A_i \in \mathscr{F}$.*

Definition A.2 (probability measure). *Given a set Ω and a σ-field $\mathscr{F}$ over Ω, we call $\boldsymbol{\mu} : \mathscr{F} \to [0,1]$ a* probability measure *over $\mathscr{F}$, if the following conditions are satisfied:*

- $\boldsymbol{\mu}(\emptyset) = 0$.
- $\boldsymbol{\mu}(\Omega) = 1$.
- *For a countable collection of mutually disjoint sets in $\mathscr{F}$, $\{A_i : i \in \mathscr{I}\}$, we have, $\boldsymbol{\mu}\left(\bigcup_{i\in\mathscr{I}} A_i\right) = \sum_{i\in\mathscr{I}} \boldsymbol{\mu}(A_i)$.*

For a σ-field $\mathscr{F}$ over Ω and a probability measure $\boldsymbol{\mu}$ over $\mathscr{F}$, we call the triplet $(\Omega, \mathscr{F}, \boldsymbol{\mu})$ a *probability space*.

Definition A.3 (random variables/measurable functions). *A function $\mathsf{X} : \Omega \to \Omega'$ is called* $(\mathscr{F}, \mathscr{F}')$-measurable, *where $\mathscr{F}$ and $\mathscr{F}'$ are σ-fields over Ω and Ω', respectively, if $\mathsf{X}^{-1}(A) \in \mathscr{F}$, $\forall A \in \mathscr{F}'$. In probability theory we alternatively refer to a measurable function as a* random variable.

Definition A.4 (probability measure induced by a random variable). *Let $(\Omega, \mathscr{F}, \boldsymbol{\mu})$ be a probability space, and let $\mathscr{F}'$ be a σ-field over Ω'. A $(\mathscr{F}, \mathscr{F}')$-measurable function (random variable) $\mathsf{X} : \Omega \to \Omega'$* induces a probability measure, *denoted $\boldsymbol{\mu}_{\mathsf{X}}$, on $\mathscr{F}'$, which is defined as*

$$\boldsymbol{\mu}_{\mathsf{X}}(A) := \boldsymbol{\mu}(\mathsf{X}^{-1}(A)),\ \forall A \in \mathscr{F}'.$$

In this dissertation we will only consider finite sample spaces, more specifically the most commonly used one will be the space of all n-bit strings, i. e., $\Omega = \{0,1\}^n$ for some $n \in \mathbb{N}$, or some structured subset of it. Now if a σ-field $\mathscr{F}$ over Ω contains every singleton subset of Ω, i. e., $\{\omega\} \in \mathscr{F},\ \forall \omega \in \Omega$, then $\mathscr{F} = 2^{\Omega}$. We most commonly use the probability space $(\{0,1\}^n, 2^{\{0,1\}^n}, \boldsymbol{u}_n)$, where the *uniform probability measure* $\boldsymbol{u}_n$ is defined on the singleton sets (also called *atoms*) as $\boldsymbol{u}_n(\{\omega\}) = 2^{-n},\ \forall \omega \in \Omega$.

All random variables considered in this paper maps n-bit strings to m-bit strings for some $n, m \in \mathbb{N}$. Since we assume the convention that the respective power sets will be considered as σ-fields over the respective sample spaces, we stop mentioning the σ-fields with respect to which a function $\mathsf{X} : \Omega \to \Omega'$ is measurable, since in this case any such function will be trivially measurable.

Now consider the probability space $(\{0,1\}^n, 2^{\{0,1\}^n}, \boldsymbol{u}_n)$, and a random variable $\mathsf{X} : \{0,1\}^n \to \{0,1\}^m$, then the probabilty measure induced by X will be defined on the atoms as $\boldsymbol{p}_{\mathsf{X}}(\{\omega'\}) = |\{\omega \in \{0,1\}^n : \mathsf{X}(\omega) = \omega'\}| \cdot 2^{-n}$ for all $\omega' \in \{0,1\}^m$. We also denote the quantity $\boldsymbol{p}_{\mathsf{X}}(\{\omega'\})$ as $\Pr(\mathsf{X} = \omega')$.

For any probability measure $\boldsymbol{p}$ defined over $(\Omega, 2^{\Omega})$, we define the corresponding *probability distribution*, denoted by $f_{\boldsymbol{p}} : \Omega \to [0,1]$, as the function that maps $\omega \mapsto \boldsymbol{p}(\{\omega\})$. We abuse notation and denote $f_{\boldsymbol{p}}$ by $\boldsymbol{p}$ itself. This is because one is complete determined by the other, due to the additive property of the probability measure. We define the *support of a probability distribution* $\boldsymbol{p}$ as $\mathsf{Supp}(\boldsymbol{p}) := \{\omega \in \Omega : \boldsymbol{p}(\omega) > 0\}$.

Definition A.5 (expected value). *Let $\mathsf{X} : \Omega \to \Omega'$ be a random variable over a discrete probability space $(\Omega, 2^{\Omega}, \boldsymbol{p})$, and $f : \Omega' \to \Omega''$ be a function. Then the* expected value of $f(\mathsf{X})$*, denoted as $\mathbb{E}_{\mathsf{X}}(f(\mathsf{X}))$, will be defined as*

$$\mathbb{E}_{\mathsf{X}}(f(\mathsf{X})) := \sum_{x \in \Omega'} f(x)\boldsymbol{p}_{\mathsf{X}}(x)$$

Definition A.6 (variance). *Let $\mathsf{X} : \Omega \to \Omega'$ be a random variable over a discrete probability space $(\Omega, 2^{\Omega}, \boldsymbol{p})$, and $f : \Omega' \to \Omega''$ be a function. Then the* variance of $f(\mathsf{X})$*, denoted as $\mathsf{Var}_{\mathsf{X}}(f(\mathsf{X}))$, will be defined as*

$$\mathsf{Var}_{\mathsf{X}}(f(\mathsf{X})) := \mathbb{E}_{\mathsf{X}}\left(f^2(\mathsf{X})\right) - \left(\mathbb{E}_{\mathsf{X}}(f(\mathsf{X}))\right)^2 = \sum_{x \in \Omega'} f(x)^2 \boldsymbol{p}_{\mathsf{X}}(x) - \left(\sum_{x \in \Omega'} f(x)^2 \boldsymbol{p}_{\mathsf{X}}(x)\right)^2$$

The last equality may not hold in general for any real valued random variable X, $\mathsf{Var}_{\mathsf{X}}(f(\mathsf{X})) := \mathbb{E}_{\mathsf{X}}\left(f^2(\mathsf{X})\right) - \left(\mathbb{E}_{\mathsf{X}}(f(\mathsf{X}))\right)^2$.

A.1.1 *Statistical Distance*

Statistical distance is a metric defined over the space of probability distributions on a finite sample space Ω. It is called the total variation in the statistics community. It is used to define the distinguishing advantage and hence is the primary metric in cryptography.

Definition A.7 (statistical distance). *The* statistical distance *between two probability distributions $\boldsymbol{p}_0$ and $\boldsymbol{p}_1$ on a finite sample space Ω as*

$$\Delta(\boldsymbol{p}_0, \boldsymbol{p}_1) := \frac{1}{2} \sum_{\omega \in \Omega} |\boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega)|$$

For two random variables X and Y, we abuse notaiton and define the statistical distnace between them, as $\Delta(\mathsf{X}, \mathsf{Y}) := \Delta(\boldsymbol{p}_{\mathsf{X}}, \boldsymbol{p}_{\mathsf{Y}})$.

We state the metric properties of statistical distance in the following lemma, which follows quite easily from the definition, and hence we skip proving it explicitly.

Lemma A.1. *For any $\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3 \in \mathscr{P}(\Omega)$, we have*

- $\Delta(\boldsymbol{p}_1, \boldsymbol{p}_2) \geq 0$, *the equality holds if and only if $\boldsymbol{p}_1(\omega) = \boldsymbol{p}_2(\omega)$ for all $\omega \in \Omega$*
- $\Delta(\boldsymbol{p}_1, \boldsymbol{p}_2) = \Delta(\boldsymbol{p}_2, \boldsymbol{p}_1)$
- $\Delta(\boldsymbol{p}_1, \boldsymbol{p}_3) \leq \Delta(\boldsymbol{p}_1, \boldsymbol{p}_2) + \Delta(\boldsymbol{p}_2, \boldsymbol{p}_3)$.
- $\Delta(\boldsymbol{p}_1, \boldsymbol{p}_2) \leq 1$, *the equality holds if and only if $\mathsf{Supp}(\boldsymbol{p}_1) \cap \mathsf{Supp}(\boldsymbol{p}_2) = \emptyset$.*

The following lemma gives an alternate definition for the statistical distance:

Lemma A.2. *For $\boldsymbol{p}_0, \boldsymbol{p}_1 \in \mathscr{P}(\Omega)$, then*

$$\max_{A \subseteq \Omega} (\boldsymbol{p}_0(A) - \boldsymbol{p}_1(A)) = \sum_{\omega \in \Omega} \max\{0, \boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega)\} = \Delta(\boldsymbol{p}_0, \boldsymbol{p}_1)$$

The maximum is achieved when $\Omega_> \subseteq A \subseteq \Omega_\geq$, where

$$\Omega_> := \{\omega \in \Omega : \boldsymbol{p}_0(\omega) > \boldsymbol{p}_1(\omega)\}$$
$$\Omega_\geq := \{\omega \in \Omega : \boldsymbol{p}_0(\omega) \geq \boldsymbol{p}_1(\omega)\}$$

Proof. Since for any $\omega \notin \Omega_\geq$, $\boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega) < 0$, and hence obviously $\max_{A \subseteq \Omega}(\boldsymbol{p}_0(A) - \boldsymbol{p}_1(A))$ is acheieved for $\Omega_> \subseteq A \subseteq \Omega_\geq$. Now

$$\begin{aligned}
\Delta(\boldsymbol{p}_0, \boldsymbol{p}_1) &= \frac{1}{2} \sum_{\omega \in \Omega} |\boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega)| \\
&= \frac{1}{2} \sum_{\omega \in \Omega_>} (\boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega)) + \frac{1}{2} \sum_{\omega \in \Omega_>^c} (\boldsymbol{p}_1(\omega) - \boldsymbol{p}_0(\omega)) \\
&= \frac{1}{2} (\boldsymbol{p}_0(\Omega_>) - \boldsymbol{p}_0(\Omega_>^c) - (\boldsymbol{p}_1(\Omega_>) - \boldsymbol{p}_1(\Omega_>^c)) \\
&= \boldsymbol{p}_0(\Omega_>) - \boldsymbol{p}_1(\Omega_>) \\
&= \sum_{\omega \in \Omega_>} (\boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega)) = \sum_{\omega \in \Omega} \max\{0, \boldsymbol{p}_0(\omega) - \boldsymbol{p}_1(\omega)\}
\end{aligned}$$

□

Lemma A.3. *Let $\mathsf{X}, \mathsf{Y} : \Omega \to \Omega'$ be two random variables defined over the same discrete probability space $(\Omega, 2^{\Omega}, \boldsymbol{p})$. Consider the function $\epsilon_{\text{opt}} : \Omega' \to [0,1]$ defined as $\epsilon_{\text{opt}}(x) = \max\{0, 1 - \boldsymbol{p}_{\mathsf{Y}}(x)/\boldsymbol{p}_{\mathsf{X}}(x)\}$, and let $\epsilon : \Omega \to [0,1]$ be any function such that $\epsilon(x) \geq \epsilon_{\text{opt}}(x)$, $\forall x \in \Omega'$. Then we can alternatively express the statistical distance as the expected value of $\epsilon_{\text{opt}}(\mathsf{X})$, and hence bound it by the expected value of $\epsilon(\mathsf{X})$:*

$$\Delta(\boldsymbol{p}_{\mathsf{X}}, \boldsymbol{p}_{\mathsf{Y}}) = \mathbb{E}_{\mathsf{X}}\left(\epsilon_{\text{opt}}(\mathsf{X})\right) \leq \mathbb{E}_{\mathsf{X}}\left(\epsilon(x)\right)$$

Proof.

$$\begin{aligned}\Delta(\boldsymbol{p}_{\mathsf{X}}, \boldsymbol{p}_{\mathsf{Y}}) &= \sum_{x \in \Omega'_{>}} \boldsymbol{p}_{\mathsf{X}}(x) - \boldsymbol{p}_{\mathsf{Y}}(x) \qquad [\Omega'_{>} = \{x \in \Omega' : \boldsymbol{p}_{\mathsf{X}}(x) > \boldsymbol{p}_{\mathsf{Y}}(x)\}] \\ &= \sum_{x \in \Omega'_{>}} \boldsymbol{p}_{\mathsf{X}}(x) \cdot (1 - \boldsymbol{p}_{\mathsf{Y}}(x)/\boldsymbol{p}_{\mathsf{X}}(x)) = \mathbb{E}_{\mathsf{X}}\left(\epsilon(\mathsf{X})\right)\end{aligned}$$

the last equality following from the fact that

$$\epsilon(x) = \begin{cases} 1 - \frac{\boldsymbol{p}_{\mathsf{Y}}(x)}{\boldsymbol{p}_{\mathsf{X}}(x)}, & \text{if } x \in \Omega'_{>} \\ 0, & \text{otherwise.} \end{cases}$$

the inequality follows from the definition of expected value. □

Proposition A.1. *For any real-valued random variable X, we have*

$$\mathbb{E}\left(|\mathsf{X} - \mathbb{E}\left(\mathsf{X}\right)|\right) \leq \sqrt{\mathsf{Var}(\mathsf{X})}.$$

Proof. We have

$$\begin{aligned}\mathbb{E}\left(|\mathsf{X} - \mathbb{E}\left(\mathsf{X}\right)|\right) &= \sqrt{\mathbb{E}\left(|\mathsf{X} - \mathbb{E}\left(\mathsf{X}\right)|\right)^2} \\ &\leq \sqrt{\mathbb{E}\left((\mathsf{X} - \mathbb{E}\left(\mathsf{X}\right))^2\right)} = \sqrt{\mathsf{Var}(\mathsf{X})},\end{aligned}$$

where the inequality also follows from Jensen's inequality among others. □

Proposition A.2. *Let R_0 and R_1 be two random variables with variances σ_0^2 and σ_1^2, respectively, and suppose their expectations follow the relation $\mathbb{E}\left(\mathsf{R}_0\right) \geq \mu_0 \geq \mu_1 \geq \mathbb{E}\left(\mathsf{R}_1\right)$, for some $\mu_0 \geq \mu_1 \geq 0$. Then, for $\mu = (\mu_0 + \mu_1)/2$, we have*

$$\left|\Pr\left(\mathsf{R}_0 > \mu\right) - \Pr\left(\mathsf{R}_1 > \mu\right)\right| \geq 1 - \frac{4(\sigma_0^2 + \sigma_1^2)}{(\mu_0 - \mu_1)^2}.$$

Proof. Let $\overline{\mu} := (\mu_0 - \mu_1)/2$. Then, we have

$$\mu = \mu_0 - \overline{\mu} = \overline{\mu} + \mu_1.$$

Using Bienaymé-Chebyshev inequality, we have

$$\begin{aligned}\Pr(\mathsf{R}_0 > \mu) &= 1 - \Pr(\mathsf{R}_0 \le \mu)\\ &\ge 1 - \Pr(\mathsf{R}_0 - \mu_0 \le -\overline{\mu})\\ &\ge 1 - \Pr(\mathsf{R}_0 - \mathbb{E}(\mathsf{R}_0) \le -\overline{\mu})\\ &\ge 1 - \Pr(|\mathsf{R}_0 - \mathbb{E}(\mathsf{R}_0)| \ge \overline{\mu}) \ge 1 - \frac{\sigma_0^2}{\overline{\mu}^2} \end{aligned} \tag{A.1}$$

and

$$\begin{aligned}\Pr(\mathsf{R}_1 > \mu) &\le \Pr(\mathsf{R}_1 \ge \mu)\\ &\le \Pr(\mathsf{R}_1 - \mu_1 \ge \overline{\mu})\\ &\le \Pr(\mathsf{R}_1 - \mathbb{E}(\mathsf{R}_1) \ge \overline{\mu})\\ &\le \Pr(|\mathsf{R}_1 - \mathbb{E}(\mathsf{R}_1)| \ge \overline{\mu}) \le \frac{\sigma_1^2}{\overline{\mu}^2} \end{aligned} \tag{A.2}$$

The result then follows by subtracting (A.2) from (A.1). □

A.2 RESULTS USED IN THE SECURITY ANALYSIS OF LRW+ (SECT. 15.2)

A.2.1 *Some Results From [JN20] on Hash Functions*

Throughout this section, we fix $t^q = (t_1, \ldots, t_q) \in (\mathcal{T})_q$. Let $\mathscr{H}$ be a (τ, n)-hash function family with ϵ-AUHF property. A pair of distinct elements $t_i, t_j \in t^{\{q\}}$ is said to be *colliding* for a function $h \in \mathscr{H}$, if $h(t_i) = h(t_j)$. Then, for a randomly chosen hash function $\mathsf{H} \xleftarrow{*} \mathscr{H}$, the probability of having at least one colliding pair in t^q is at most $\binom{q}{2} \cdot \epsilon$. This is straightforward from the union bound.

Independence of the hash functions implies the independence of the ϵ-probability events $\mathsf{H}_1(t_i) = \mathsf{H}_1(t_j)$ and $\mathsf{H}_2(t_j) = \mathsf{H}_2(t_k)$. Taking the union bound over $(q)_3$ pairwise distinct tuples (i, j, k), we get

$$\Pr(\exists^* i, j, k \in [q],\ \mathsf{H}_1(t_i) = \mathsf{H}_1(t_j) \ \wedge\ \mathsf{H}_2(t_j) = \mathsf{H}_2(t_k)) \le q(q-1)(q-2) \cdot \epsilon^2.$$

Lemma A.4 (Alternating Collisions Lemma [JN20]). *Suppose H_1, H_2 are two uniformly and independently drawn functions from an ϵ-AUHF $\mathscr{H}$ and $t^q \in (\mathcal{T})_q$. Then,*

$$\Pr(\exists^* i, j, k, l \in [q], H_1(t_i) = H_1(t_j) \wedge H_1(t_k) = H_1(t_l) \wedge H_2(t_j) = H_2(t_k)) \le q^2 \epsilon^{1.5}.$$

Lemma A.5 (Alternating Events Lemma [JN20]). *Let $X^q = (X_1, \ldots, X_q)$ be a q-tuple of random variables. Suppose for all $i < j \in [q]$, $\mathsf{E}_{i,j}$ are events associated with X_i and X_j, possibly dependent. Each event holds with probability at most ϵ. Moreover, for any distinct $i, j, k, l \in [q]$, $\mathsf{F}_{i,j,k,l}$ are*

events associated with X_i, X_j, X_k and X_l, which holds with probability at most ϵ'. Moreover, the collection of events $(\mathsf{F}_{i,j,k,l})_{i,j,k,l}$ is independent with the collection of event $(\mathsf{E}_{i,j})_{i,j}$. Then,

$$\Pr\left(\exists^* i,j,k,l \in [q], \mathsf{E}_{i,j} \ \wedge\ \mathsf{E}_{k,l} \ \wedge\ \mathsf{F}_{i,j,k,l}\right) \leq q^2 \cdot \epsilon \cdot \sqrt{\epsilon'}$$

Let $\mathsf{X}^q = \mathsf{H}(t^q)$. We define an equivalence relation $\sim$ on $[q]$ as: $\alpha \sim \beta$ if and only if $\mathsf{X}_\alpha = \mathsf{X}_\beta$ (i.e. $\sim$ is simply the multicollision relation). Let $\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_r$ denote those equivalence classes of $[q]$ corresponding to $\sim$, such that $\nu_i = |\mathscr{P}_i| \geq 2$ for all $i \in [r]$.

Lemma A.6 ([JN20]). $\mathbb{E}\left(\sum_{i=1}^r {\nu_i}^2\right) \leq 2q^2\epsilon$.

Corollary A.6.1 ([ML19; JN20]). *Let $\nu_{\max} = \max\{\nu_i : i \in [r]\}$. Then, for some $a \geq 2$, we have*

$$\Pr\left(\nu_{\max} \geq a\right) \leq \frac{2q^2\epsilon}{a^2}.$$

A.2.2 *Two Useful Inequalities From JN20*

Definition A.8 ([JN20]). *For $r \geq s$, let $a = (a_i)_{i\in[r]}$ and $b = (b_j)_{j\in[s]}$ be two sequences over $\mathbb{N}$. We say that a compresses to b, if there exists a partition $\mathscr{P}$ of $[r]$ such that $\mathscr{P}$ contains exactly s cells, say $\mathscr{P}_1, \ldots, \mathscr{P}_s$, and $\forall i \in [s],\ \ b_i = \sum_{j\in\mathscr{P}_i} a_j$.*

Proposition A.3 ([JN20]). *For $r \geq s$, let $a = (a_i)_{i\in[r]}$ and $b = (b_j)_{j\in[s]}$ be sequences over $\mathbb{N}$, such that a compresses to b. Then for any $n \in \mathbb{N}$, such that $2^n \geq \sum_{i=1}^r a_i$, we have $\prod_{i=1}^r (2^n)_{a_i} \geq \prod_{j=1}^s (2^n)_{b_j}$.*

Proposition A.4 ([JN20]). *For $r \geq 2$, let $c = (c_i)_{i\in[r]}$ and $d = (d_i)_{i\in[r]}$ be two sequences over $\mathbb{N}$. Let $a_1, a_2, b_1, b_2 \in \mathbb{N}$, such that $c_i \leq a_j$, $c_i + d_i \leq a_j + b_j$ for all $i \in [r]$ and $j \in [2]$, and $\sum_{i=1}^r d_i = b_1 + b_2$. Then, for any $n \in \mathbb{N}$, such that $a_j + b_j \leq 2^n$ for $j \in [2]$, we have $\prod_{i=1}^r (2^n - c_i)_{d_i} \geq (2^n - a_1)_{b_1}(2^n - a_2)_{b_2}$.*

A.3 PROOF OF CLAIM 15.0.1 USED FOR BIRTHDAY BOUND ATTACK ON TNT

PRELIMINARIES ON VARIANCE AND COVARIANCE: Recall that for any two indicator random variables χ and χ', the variance $\mathsf{Var}(\chi)$ and covariance $\mathsf{Cov}(\chi, \chi')$ are defined as:

$$\mathsf{Var}(\chi) = \Pr(\chi) - \Pr(\chi)^2, \qquad \mathsf{Cov}(\chi, \chi') = \Pr(\chi \cdot \chi') - \Pr(\chi) \cdot \Pr(\chi'),$$

and for any random variable X that can be be written as a sum of indicator random variables $\sum_i \chi_i$, we have

$$\mathsf{Var}(\mathsf{X}) = \sum_i \mathsf{Var}(\chi_i) + \sum_{i\neq j} \mathsf{Cov}(\chi_i, \chi_j).$$

A.3.1 *Upper Bounding Var($coll_{id}$)*

Using the fact that $\mathsf{coll}_{\mathsf{id}} = \sum_{i<j} \chi_{i,j}$, we have

$$\mathsf{Var}(\mathsf{coll}_{\mathsf{id}}) = \sum_{i<j} \mathsf{Var}(\chi_{i,j}) + \sum_{i,j,k,\ell} \mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \tag{A.3}$$

where the summation is taken over $i < j, k < \ell, \{i,j\} \neq \{k,\ell\}$ Suppose there are ν pairs $i < j$ satisfying $i \sim j$, where we recall that $i \sim j$ if and only if $t_i = t_j \oplus \delta$.

COMPUTING $\mathrm{VAR}(\chi_{i,j})$. Recall that $\mathsf{Var}(\chi_{i,j}) = \Pr(\chi_{i,j}) - \Pr(\chi_{i,j})^2$. We can have two cases, depending upon $i \sim j$, or not:

A. $i \not\sim j$: In this case, using (15.7), we have

$$\mathsf{Var}(\chi_{i,j}) = \frac{1}{2^n} - \frac{1}{2^{2n}}.$$

B. $i \sim j$: In this case, using (15.9), we have

$$\mathsf{Var}(\chi_{i,j}) \leq \frac{1}{2^n} + \frac{1}{2^n - 1} - \frac{1}{2^{2n}}.$$

By combining the two cases, we have

$$\sum_{i<j} \mathsf{Var}(\chi_{i,j}) \leq \binom{q}{2}\frac{1}{2^n} + \frac{q}{2^n} - \binom{q}{2}\frac{1}{2^{2n}} \tag{A.4}$$

COMPUTING $\mathrm{COV}(\chi_{i,j}, \chi_{k,\ell})$. Recall that $\mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) = \Pr(\chi_{i,j} \cdot \chi_{k,\ell}) - \Pr(\chi_{i,j}) \cdot \Pr(\chi_{k,\ell})$. We can have two cases, depending upon the size of $|\{i,j\} \cap \{k,\ell\}|$:

A. $|\{i,j\} \cap \{k,\ell\}| = 1$: Without loss of generality assume $j = k$, and consider the following subcases:

1. $\exists\, i'_1, i'_2 \in \{i,j,\ell\}$ such that $i'_1 \sim i'_2$: Note that there can be only one such (i'_1, i'_2) pair. We consider the case $i \sim \ell$, as the other two cases are relatively simpler (due to the independence of $\chi_{i,j}$ and $\chi_{j,\ell}$). Note that the event $\chi_{i,j} \cdot \chi_{j,\ell}$ is equivalent to $\chi_{j,i} \cdot \chi_{i,\ell}$, where of course we have abused the definition a bit as $j > i$. However, the meaning is still clear from the context. Now the events $\chi_{j,i}$ and $\chi_{i,\ell}$ are independent, since the j-th query uses distinct tweaks $(t_j, t_j + \delta)$. Thus, using (15.7) and (15.9), we have

$$\mathsf{Cov}(\chi_{i,j}, \chi_{j,\ell}) \leq \frac{1}{2^n(2^n - 1)}.$$

2. $\forall i'_1, i'_2 \in \{i, j, k\}$, $i'_1 \not\sim i'_2$: The two events are independent and identically distributed, as all six tweaks are different. Thus, using (15.7), we have

$$\mathsf{Cov}(\chi_{i,j}, \chi_{j,\ell}) \leq 0.$$

Now, there are at most $\nu(q-2) \leq q^2/2$ triples (i, j, ℓ) that can satisfy case **A.1.**. Thus, we have

$$\sum_{\substack{i<j \\ k<\ell \\ |\{i,j\}\cap\{k,\ell\}|=1}} \mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq \frac{q^2}{2^{2n}} \tag{A.5}$$

B. $|\{i, j\} \cap \{k, \ell\}| = 0$: We handle this case depending upon the number of $(i'_1, i'_2) \in \{i, j, k, \ell\}$ such that $i'_1 \sim i'_2$. Let r be the number of such pairs. Note that r cannot be greater than 2. Thus, we have the following subcases:

1. $r = 0$: In this case, the two events are independent and identically distributed, as all eight tweaks are distinct. Thus, using (15.7), we have

$$\mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq 0.$$

2. $r = 1$: First, suppose $(i'_1, i'_2) \in \{(i, j), (k, \ell)\}$. Without loss of generality let $(i'_1, i'_2) = (i, j)$. Since $\{t_k, t_\ell, t_k \oplus \delta, t_\ell \oplus \delta\} \cap \{t_i, t_j\} = \emptyset$ and $k \not\sim \ell$, using (15.7) and (15.9), we get

$$\mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq \frac{1}{2^n(2^n-1)} \leq \frac{2}{2^{2n}}.$$

Next, suppose $(i'_1, i'_2) \notin \{(i, j), (k, \ell)\}$. Without loss of generality, let $(i'_1, i'_2) = (i, k)$. Note that $\{t_j, t_\ell, t_j \oplus \delta, t_\ell \oplus \delta\} \cap \{t_i, t_k\} = \emptyset$. Then, by conditioning on the value of $(\mathsf{M}'_i, \mathsf{M}'_k)$, the event $\chi_{i,j} \cdot \chi_{k,\ell}$ holds with probability 2^{-2n}, whence using (15.7), we get

$$\mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq 0.$$

3. $r = 2$: Since there are at most $\nu^2 \leq q^2/4$ choices for such quadruples, even a loose bound on the probability of $\Pr(\chi_{i,j} \cdot \chi_{k,\ell})$ will suffice. In particular, we simply use $\Pr(\chi_{i,j})$. Using (15.9), we have

$$\mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq \frac{1}{2^n} + \frac{1}{2^n - 1} - \frac{1}{2^{2n}}.$$

Finally, since there are $\nu q^2 \leq q^3/2$ quadruples that satisfy **B.2.** and $\nu^2 \leq q^2/4$ quadruples that satisfy **B.3.**, we get

$$\sum_{\substack{i<j \\ k<\ell \\ |\{i,j\}\cap\{k,\ell\}|=0}} \mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq \frac{3q^2}{2^{n+2}} + \frac{q^3}{2^{2n}} - \frac{q^2}{2^{2n+2}} \tag{A.6}$$

From (A.3)-(A.6) and $2 \leq q \leq 2^n$, we have

$$\mathsf{Var}(\mathsf{coll}_{\mathsf{id}}) \leq \frac{4q^2}{2^n}. \tag{A.7}$$

A.3.2 *Upper Bounding* $\mathsf{Var}(\mathsf{coll}_{\mathsf{re}})$

The internal variables arising in the execution of $\mathsf{TNT}_{\delta,m}$ are represented by the notations from Fig. 15.2. In particular, we have $\widehat{\mathsf{M}} = \boldsymbol{\pi}_1(m)$, $\mathsf{U}_{i'} = \widehat{\mathsf{M}} \oplus t_{i'}$, $\widehat{\mathsf{U}}_{i'} = \boldsymbol{\pi}_2(\mathsf{U}_{i'})$, $\widehat{\mathsf{U}}'_{i'} = \widehat{\mathsf{U}}_{i'} \oplus \delta$, $\mathsf{U}'_{i'} = \boldsymbol{\pi}_2^{-1}(\widehat{\mathsf{U}}'_{i'})$, $\widehat{\mathsf{M}}'_{i'} = \mathsf{U}'_{i'} \oplus t_{i'}$, and $\mathsf{M}'_{i'} = \boldsymbol{\pi}_1^{-1}(\widehat{\mathsf{M}}'_{i'})$, for all $i' \in [q]$.

We have $\mathsf{coll}_{\mathsf{re}} = \sum_{i<j\in[q]} \chi_{i,j}$, where $\chi_{i,j}$ is the indicator random variable corresponding to the event $\mathsf{M}'_i = \mathsf{M}'_j$ in the real world. Recall that, for any $i \neq j \in [q]$, we have

$$\begin{aligned}\Pr(\chi_{i,j}) &= \frac{1}{2^n-1} + \frac{1}{2^n-3} - \frac{1}{(2^n-1)(2^n-3)} \\ &= \frac{2}{2^n} - \frac{1}{2^n(2^n-1)} - \frac{3}{2^n(2^n-3)} - \frac{1}{(2^n-1)(2^n-3)}\end{aligned}$$

For simplicity we write $p := \Pr(\chi_{i,j})$. We will often employ the following inequalities

$$\frac{2}{2^n} \leq p \leq \frac{2}{2^n} + \frac{7}{2^{2n}}. \tag{A.8}$$

Now, we have

$$\mathsf{Var}(\mathsf{coll}_{\mathsf{re}}) = \sum_{i<j} \mathsf{Var}(\chi_{i,j}) + \sum_{\substack{i<j \\ k<\ell \\ \{i,j\}\neq\{k,\ell\}}} \mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \tag{A.9}$$

COMPUTING $\mathrm{VAR}(\chi_{i,j})$. By definition, we have $\mathsf{Var}(\chi_{i,j}) = p - p^2$, for any $i < j \in [q]$. Thus, using (A.8), we have

$$\sum_{i<j} \mathsf{Var}(\chi_{i,j}) \leq \frac{q^2}{2^n} + \frac{2q^2}{2^{2n}} \tag{A.10}$$

COMPUTING $\mathrm{COV}(\chi_{i,j}, \chi_{k,\ell})$. We have

$$\begin{aligned}\mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) &= \Pr(\chi_{i,j} \cdot \chi_{k,\ell}) - \Pr(\chi_{i,j}) \cdot \Pr(\chi_{k,\ell}) \\ &= \Pr(\chi_{i,j} \cdot \chi_{k,\ell}) - p^2 \leq \Pr(\chi_{i,j} \cdot \chi_{k,\ell}) - \frac{4}{2^{2n}}\end{aligned} \tag{A.11}$$

where the last inequality follows from (A.8). So, from now on, we only have to handle the joint event $\chi_{i,j,k,\ell} = \chi_{i,j} \cdot \chi_{k,\ell}$.

For the sake of simplicity, we perform the analysis, by conditioning on some arbitrary value of $\boldsymbol{\pi}_1(m)$, say $\widehat{m}$. Looking ahead, the final bounds will be independent of this choice,

so the bounds hold unconditionally, and we take this fact for granted. Let $u_{i'} = \widehat{m} \oplus t_{i'}$, for all $i' \in [q]$. Then, $\mathsf{U}_{i'} = u_{i'}$.
As has been established before, the event $\chi_{i,j}$ occurs, if and only if:

$$\mathsf{E}_{i,j} : \widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j = \delta, \text{ or}$$

$$\mathsf{F}_{i,j} : \widehat{\mathsf{U}}_i \oplus \widehat{\mathsf{U}}_j \neq \delta \text{ and } \mathsf{U}'_i \oplus \mathsf{U}'_j = t_i \oplus t_j.$$

Let $\mathsf{E}^2_{i,j,k,\ell}$, $\mathsf{EF}_{i,j,k,\ell}$, $\mathsf{FE}_{i,j,k,\ell}$, and $\mathsf{F}^2_{i,j,k,\ell}$ denote the joint events $(\mathsf{E}_{i,j} \cap \mathsf{E}_{k,\ell})$, $(\mathsf{E}_{i,j} \cap \mathsf{F}_{k,\ell})$, $(\mathsf{F}_{i,j} \cap \mathsf{E}_{k,\ell})$, and $(\mathsf{F}_{i,j} \cap \mathsf{F}_{k,\ell})$, respectively. Then, it is clear that $\chi_{i,j,k,\ell}$ is a union of these four events.

The way we move forward is to count the number of all valid choices (or assignments), denoted by $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell, u'_i, u'_j, u'_k, u'_\ell)$ for $(\widehat{\mathsf{U}}_i, \widehat{\mathsf{U}}_j, \widehat{\mathsf{U}}_k, \widehat{\mathsf{U}}_\ell, \mathsf{U}'_i, \mathsf{U}'_j, \mathsf{U}'_k, \mathsf{U}'_\ell)$ that satisfy the event in focus. Then, the probability of the event is simply this count times $1/(2^n)_\alpha$, where α will denote a lower bound on the number of distinct elements in $\{u_i, u_j, u_k, u_\ell, u'_i, u'_j, u'_k, u'_\ell\}$ for the event in focus.

Now, we can have two cases depending upon $r := |\{i, j\} \cap \{k, \ell\}|$:

A. $r = 1$: Without loss of generality assume $j = k$. Then,

$$\begin{aligned}\Pr\left(\chi_{i,j,j,\ell}\right) &= \Pr\left(\mathsf{E}^2_{i,j,j,\ell} \cup \mathsf{EF}_{i,j,j,\ell} \cup \mathsf{FE}_{i,j,j,\ell} \cup \mathsf{F}^2_{i,j,j,\ell}\right) \\ &\leq \Pr\left(\mathsf{E}^2_{i,j,j,\ell}\right) + \Pr\left(\mathsf{EF}_{i,j,j,\ell}\right) + \Pr\left(\mathsf{FE}_{i,j,j,\ell}\right) + \Pr\left(\mathsf{F}^2_{i,j,j,\ell}\right) \\ &= \Pr\left(\mathsf{EF}_{i,j,j,\ell}\right) + \Pr\left(\mathsf{FE}_{i,j,j,\ell}\right) + \Pr\left(\mathsf{F}^2_{i,j,j,\ell}\right) \qquad \text{(A.12)}\end{aligned}$$

where the last equality follows from the fact that $t_i \oplus \delta = t_j = t_\ell \oplus \delta$ if and only if $t_i = t_\ell$, which is impossible. We handle the three summands one by one:

1. Probability of $\mathsf{EF}_{i,j,j,\ell}$: Any valid choice $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_\ell, u'_i, u'_j, u'_j, u'_\ell)$ must satisfy
   - $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_\ell)$ is pairwise distinct,
   - $\widehat{u}_i \oplus \widehat{u}_j = \delta$ and $\widehat{u}_\ell \notin \{\widehat{u}_i, \widehat{u}_j\}$,
   - $(u'_i, u'_j) = (u_j, u_i)$,
   - $u'_\ell = u'_j \oplus t_j \oplus t_\ell \notin \{u'_i, u'_j, u_\ell\} = \{u_i, u_j, u_\ell\}$,
   - (u'_i, u'_j, u'_ℓ) is pairwise distinct.

   The first three conditions are obvious. In the fourth condition, $u'_\ell \neq u_\ell$ follows from $\delta \neq 0^n$. Now, $\widehat{u}_i$ has 2^n choices, $\widehat{u}_j = \widehat{u}_i \oplus \delta$, and $\widehat{u}_\ell \notin \{\widehat{u}_i, \widehat{u}_j\}$ has obviously $(2^n - 2)$ choices. Once we fix $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_\ell)$, u'_ℓ is fixed. Thus, there are at most $2^n(2^n - 2)$ choices. Further, from condition 3, we have $|\{u_i, u_j, u_\ell, u'_\ell\}| = 4$. Thus, each valid choice occurs with at most $1/(2^n)_4$ probability, as at least 4 variables are sampled in a WOR manner from $\{0,1\}^n$. Thus, we have

$$\Pr\left(\mathsf{EF}_{i,j,j,\ell}\right) \leq \frac{1}{(2^n - 1)(2^n - 3)}$$

$$\leq \frac{1}{2^{2n}}\left(1+\frac{1}{2^n-1}\right)\left(1+\frac{3}{2^n-3}\right)$$
$$\leq \frac{1}{2^{2n}}+\frac{8}{2^{3n}}+\frac{12}{2^{4n}} \tag{A.13}$$

2. Probability of $\mathsf{FE}_{i,j,j,\ell}$: By symmetry, we have

$$\Pr\left(\mathsf{FE}_{i,j,j,\ell}\right) \leq \frac{1}{2^{2n}}+\frac{8}{2^{3n}}+\frac{12}{2^{4n}} \tag{A.14}$$

3. Probability of $\mathsf{F}^2_{i,j,j,\ell}$: Any valid choice $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_j, \widehat{u}_\ell, u'_i, u'_j, u'_j, u'_\ell)$ must satisfy

- $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_\ell)$ is pairwise distinct,
- $\widehat{u}_i \oplus \widehat{u}_j \neq \delta$ and $\widehat{u}_j \oplus \widehat{u}_\ell \neq \delta$,
- $u'_i = u'_j \oplus t_i \oplus t_j \notin \{u_i, u_j\}$,
- $u'_\ell = u'_j \oplus t_j \oplus t_\ell \notin \{u_j, u_\ell\}$,
- (u'_i, u'_j, u'_ℓ) is pairwise distinct.

Now, $\widehat{u}_i \oplus \widehat{u}_\ell = \delta$ (which is possible) a valid assignment would have $(u'_i, u'_\ell) = (u_\ell, u_i)$. But, this implies that this assignment also satisfies $\mathsf{E}_{i,\ell}$. Accordingly, we refine the objective as

$$\Pr\left(\mathsf{F}^2_{i,j,j,\ell}\right) \leq \Pr\left(\mathsf{F}^2_{i,j,j,\ell} \cap \mathsf{E}_{i,\ell}\right) + \Pr\left(\mathsf{F}^2_{i,j,j,\ell} \mid \neg\mathsf{E}_{i,\ell}\right)$$

For the first summand we have at most $2^n(2^n-2)$ valid assignments, each occurring with at most $1/(2^n)_4$ probability, and for the second summand we have at most $2^n(2^n-1)(2^n-3)(2^n-4)$ valid assignments, each occurring with at most $1/(2^n)_6$ probability. Thus, we have

$$\Pr\left(\mathsf{F}^2_{i,j,j,\ell}\right) \leq \frac{2}{2^{2n}}+\frac{26}{2^{3n}}+\frac{92}{2^{4n}} \tag{A.15}$$

On combining (A.11)-(A.15), we get

$$\sum_{\substack{i<j\\k<\ell\\r=1}} \mathsf{Cov}(\chi_{i,j}, \chi_{k,\ell}) \leq \frac{7q^3}{2^{3n}}+\frac{20q^3}{2^{4n}} \tag{A.16}$$

B. $r = 0$: In this case we have

$$\Pr\left(\chi_{i,j,k,\ell}\right) = \Pr\left(\mathsf{E}^2_{i,j,k,\ell} \cup \mathsf{EF}_{i,j,k,\ell} \cup \mathsf{FE}_{i,j,k,\ell} \cup \mathsf{F}^2_{i,j,k,\ell}\right)$$
$$\leq \Pr\left(\mathsf{E}^2_{i,j,k,\ell}\right) + \Pr\left(\mathsf{EF}_{i,j,k,\ell}\right) + \Pr\left(\mathsf{FE}_{i,j,k,\ell}\right) + \Pr\left(\mathsf{F}^2_{i,j,k,\ell}\right) \tag{A.17}$$

We handle the four summands one by one:

1. Probability of $\mathsf{E}^2_{i,j,k,\ell}$: Any valid choice $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell, u'_i, u'_j, u'_k, u'_\ell)$ must satisfy

- $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell)$ is pairwise distinct,
- $\widehat{u}_i \oplus \widehat{u}_j = \delta$ and $\widehat{u}_k \oplus \widehat{u}_\ell = \delta$,
- $(u'_i, u'_j, u'_k, u'_\ell) = (u_j, u_i, u_\ell, u_k)$,

Now, $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell)$ can be fixed in at most $2^n(2^n - 2)$ ways, as fixing $\widehat{u}_i$ fixes $\widehat{u}_j$, and fixing $(\widehat{u}_i, \widehat{u}_j)$ leaves $(2^n - 2)$ choices for $\widehat{u}_k$ and this fixes $\widehat{u}_\ell$. With this the full assignment is fixed. Further, each such assignment holds with at most $1/(2^n)_4$ probability. Thus, we have

$$\Pr\left(\mathsf{E}^2_{i,j,k,\ell}\right) \leq \frac{1}{2^{2n}} + \frac{8}{2^{3n}} + \frac{12}{2^{4n}} \tag{A.18}$$

2. Probability of $\mathsf{EF}_{i,j,k,\ell}$: Any valid choice $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell, u'_i, u'_j, u'_k, u'_\ell)$ must satisfy

- $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell)$ is pairwise distinct,
- $\widehat{u}_i \oplus \widehat{u}_j = \delta$ and $\widehat{u}_k \oplus \widehat{u}_\ell \neq \delta$,
- $(u'_i, u'_j) = (u_j, u_i)$,
- $u'_\ell = u'_k \oplus t_k \oplus t_\ell \notin \{u_i, u_j, u_k, u_\ell\}$,
- $u'_k \notin \{u_i, u_j, u_k, u_\ell\}$,
- $(u'_i, u'_j, u'_k, u'_\ell)$ is pairwise distinct.

The fourth condition follows from $\delta \neq 0^n$, $\widehat{u}_\ell \neq \delta \oplus \widehat{u}_k$, and the fact that $u'_\ell = u_j$ (res. $u'_\ell = u_i$) would imply $\widehat{u}_\ell \oplus \delta = \widehat{u}_j = \widehat{u}_i \oplus \delta$ (res. $\widehat{u}_\ell \oplus \delta = \widehat{u}_i = \widehat{u}_j \oplus \delta$), which is impossible. Similar argument holds for condition 5. Thus, in this case, 6 distinct values are sampled in a WOR manner from $\{0,1\}^n$. There are at most $2^n(2^n - 2)(2^n - 3)(2^n - 4)$ valid choices, each holding with at most $1/(2^n)_6$ probability. Thus, we have

$$\Pr\left(\mathsf{EF}_{i,j,k,\ell}\right) \leq \frac{1}{2^{2n}} + \frac{12}{2^{3n}} + \frac{20}{2^{4n}} \tag{A.19}$$

3. Probability of $\mathsf{FE}_{i,j,k,\ell}$: By symmetry, we have

$$\Pr\left(\mathsf{FE}_{i,j,k,\ell}\right) \leq \frac{1}{2^{2n}} + \frac{12}{2^{3n}} + \frac{20}{2^{4n}} \tag{A.20}$$

4. Probability of $\mathsf{F}^2_{i,j,k,\ell}$: Any valid choice $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_\ell, u'_i, u'_j, u'_j, u'_\ell)$ must satisfy

- $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell)$ is pairwise distinct,
- $\widehat{u}_i \oplus \widehat{u}_j \neq \delta$ and $\widehat{u}_k \oplus \widehat{u}_\ell \neq \delta$,
- $u'_i = u'_j \oplus t_i \oplus t_j \notin \{u_i, u_j\}$,

- $u'_j \notin \{u_i, u_j\}$,
- $u'_\ell = u'_j \oplus t_j \oplus t_\ell \notin \{u_j, u_\ell\}$,
- $u'_k \notin \{u_k, u_\ell\}$,
- $(u'_i, u'_j, u'_k, u'_\ell)$ is pairwise distinct.

Further, a valid choice also satisfies one of the following seven conditions:

i. $\widehat{u}_i \oplus \delta = \widehat{u}_k$, $\widehat{u}_j \oplus \delta = \widehat{u}_\ell$,

ii. $\widehat{u}_i \oplus \delta = \widehat{u}_\ell$, $\widehat{u}_j \oplus \delta = \widehat{u}_k$,

iii. $\widehat{u}_i \oplus \delta = \widehat{u}_k$, $\widehat{u}_j \oplus \delta \neq \widehat{u}_\ell$,

iv. $\widehat{u}_i \oplus \delta \neq \widehat{u}_k$, $\widehat{u}_j \oplus \delta = \widehat{u}_\ell$,

v. $\widehat{u}_i \oplus \delta = \widehat{u}_\ell$, $\widehat{u}_j \oplus \delta \neq \widehat{u}_k$,

vi. $\widehat{u}_i \oplus \delta \neq \widehat{u}_\ell$, $\widehat{u}_j \oplus \delta = \widehat{u}_k$,

vii. $\{\widehat{u}_i \oplus \delta, \widehat{u}_j \oplus \delta\} \cap \{\widehat{u}_k, \widehat{u}_\ell\}$.

Now, we can have one of the two subcases based on whether $\lambda := t_i \oplus t_j \oplus t_k \oplus t_\ell = 0^n$, or not:

a. $\lambda = 0^n$: Observe that, in this case, conditions iii-vi are not satisfiable. For instance, suppose $\widehat{u}_i \oplus \delta = \widehat{u}_k$. Then, $u'_j = u'_i \oplus t_i \oplus t_j = u_k \oplus t_k \oplus t_\ell = u_\ell$ which implies $\widehat{u}_j \oplus \delta = \widehat{u}_\ell$. Thus, only conditions i, ii, and vii are possible. Now, if condition i (res. condition ii) satisfies then we must have $u'_i = u_k$ (res. $u'_i = u_\ell$), $u'_j = u_\ell$ (res. $u'_j = u_k$). Thus, in both the cases fixing $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell)$ fixes the whole assignment. Further, $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell)$ can be fixed in at most $2^n(2^n - 2)$ ways, and each such assignment holds with at most $1/(2^n)_4$ probability. On the other hand, if condition vii satisfies then fixing $(\widehat{u}_i, \widehat{u}_j, \widehat{u}_k, \widehat{u}_\ell, u'_i, u'_k)$ fixes the full assignment. So, in this case we have at most $(2^n)_6$ choices, and each such choice holds with at most $1/(2^n)_8$ probability. Thus, when $t_i \oplus t_j = t_k \oplus t_\ell$, we have

$$\Pr\left(\mathsf{F}^2_{i,j,k,\ell}\right) \leq \frac{12}{2^{2n}} \tag{A.21}$$

b. $\lambda \neq 0^n$: Contrary to case **a.**, it can be easily verified that condition i and ii are not satisfiable in this case. Now, if condition iii-vi is satisfied, then there are at most $2^n(2^n - 2)(2^n - 3)$ valid choices, each holding with at most $1/(2^n)_6$ probability. On the other hand, if condition vii is satisfied, then there are at most $(2^n)_6$ valid choices and each choice occurs with $1/(2^n)_8$ probability. Thus, when $t_i \oplus t_j \neq t_k \oplus t_\ell$, we have

$$\Pr\left(\mathsf{F}^2_{i,j,k,\ell}\right) \leq \frac{1}{2^{2n}} + \frac{58}{2^{3n}} + \frac{168}{2^{4n}} \tag{A.22}$$

To summarize the above computations, we have

$$\sum_{\substack{i<j\\k<\ell\\r=0}} \mathsf{Cov}(\chi_{i,j},\chi_{k,\ell}) = \sum_{\substack{i<j\\k<\ell\\r=0\\\lambda=0}} \mathsf{Cov}(\chi_{i,j},\chi_{k,\ell}) + \sum_{\substack{i<j\\k<\ell\\r=0\\\lambda\neq 0}} \mathsf{Cov}(\chi_{i,j},\chi_{k,\ell}) \tag{A.23}$$

Using (A.11), (A.17)-(A.20), and (A.21), we have

$$\sum_{\substack{i<j\\k<\ell\\r=0\\\lambda=0}} \mathsf{Cov}(\chi_{i,j},\chi_{k,\ell}) \leq \frac{2q^3}{2^{2n}} + \frac{6q^3}{2^{3n}} + \frac{9q^3}{2^{4n}} \tag{A.24}$$

and using (A.11), (A.17)-(A.20) and (A.22), we have

$$\sum_{\substack{i<j\\k<\ell\\r=0\\\lambda\neq 0}} \mathsf{Cov}(\chi_{i,j},\chi_{k,\ell}) \leq \frac{4q^4}{2^{3n}} + \frac{10q^4}{2^{4n}} \tag{A.25}$$

On combining (A.9), (A.10), (A.16), and (A.23)-(A.25), we have

$$\mathsf{Var}(\mathsf{coll}_{\mathsf{re}}) \leq \frac{q^2}{2^n} + \frac{2q^2}{2^{2n}} + \frac{13q^3}{2^{3n}} + \frac{29q^3}{2^{4n}} + \frac{2q^3}{2^{2n}} + \frac{4q^4}{2^{3n}} + \frac{10q^4}{2^{4n}} \tag{A.26}$$

The result follows from $q \leq 2^n$, and $n \geq 4$. □

BIBLIOGRAPHY

[AV96] William Aiello and Ramarathnam Venkatesan. "Foiling Birthday Attacks in Length-Doubling Transformations - Benes: A Non-Reversible Alternative to Feistel." In: *Advances in Cryptology - EUROCRYPT '96. Proceeding*. 1996, pp. 307–320. DOI: 10.1007/3-540-68339-9_27.

[ADMA15] Elena Andreeva, Joan Daemen, Bart Mennink, and Gilles Van Assche. "Security of Keyed Sponge Constructions Using a Modular Proof Approach." In: *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*. Ed. by Gregor Leander. Vol. 9054. Lecture Notes in Computer Science. Springer, 2015, pp. 364–384. DOI: 10.1007/978-3-662-48116-5_18. URL: https://doi.org/10.1007/978-3-662-48116-5_18.

[Ava17] Roberto Avanzi. "The QARMA Block Cipher Family. Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes." In: *IACR Trans. Symmetric Cryptol.* 2017.1 (2017), pp. 4–44.

[BPPSST17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. "GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption." In: *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017, pp. 321–345. DOI: 10.1007/978-3-319-66787-4_16. URL: https://doi.org/10.1007/978-3-319-66787-4_16.

[BGGS20] Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song. "TNT: How to Tweak a Block Cipher." In: *Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part II*. 2020, pp. 641–673.

[BJKLMPSSS16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS." In: *Advances in Cryptology - CRYPTO 2016, Proceedings, Part II*. 2016, pp. 123–153.

[BCK96] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. "Keying Hash Functions for Message Authentication." In: *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*. Ed. by Neal Koblitz. Vol. 1109. Lecture Notes in Computer Science. Springer, 1996, pp. 1–15. DOI: 10.1007/3-540-68697-5_1. URL: https://doi.org/10.1007/3-540-68697-5_1.

[BDJR97] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. "A Concrete Security Treatment of Symmetric Encryption." In: *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*. IEEE Computer Society, 1997, pp. 394–403. DOI: 10.1109/SFCS.1997.646128. URL: https://doi.org/10.1109/SFCS.1997.646128.

[BI99] Mihir Bellare and Russell Impagliazzo. "A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion." In: *IACR Cryptol. ePrint Arch.* 1999 (1999), p. 24.

[BKR00] Mihir Bellare, Joe Kilian, and Phillip Rogaway. "The Security of the Cipher Block Chaining Message Authentication Code." In: *J. Comput. Syst. Sci.* 61.3 (2000), pp. 362–399. DOI: 10.1006/JCSS.1999.1694. URL: https://doi.org/10.1006/jcss.1999.1694.

[BKR98] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. "Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible." In: *Advances in Cryptology - EUROCRYPT '98, Proceeding*. 1998, pp. 266–280. DOI: 10.1007/BFb0054132.

[BR06] Mihir Bellare and Phillip Rogaway. "The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs." In: *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*. Ed. by Serge Vaudenay. Vol. 4004. Lecture Notes in Computer Science. Springer, 2006, pp. 409–426. DOI: 10.1007/11761679_25. URL: https://doi.org/10.1007/11761679_25.

[BM09] Till Stegers Ben Morris Phillip Rogaway. "How to encipher messages on a small domain." In: *Advances in Cryptology - CRYPTO 2009*. Ed. by Shai Halevi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 286–302. ISBN: 978-3-642-03356-8. DOI: 10.1007/978-3-642-03356-8_17.

[Ber99] Daniel J. Bernstein. "How to Stretch Random Functions: The Security of Protected Counter Sums." In: *J. Cryptol.* 12.3 (1999), pp. 185–192. DOI: 10.1007/S001459900051. URL: https://doi.org/10.1007/s001459900051.

[BKLMM+17] Daniel J. Bernstein, Stefan Kölbl, Stefan Lucks, Pedro Maat Costa Massolino, Florian Mendel, et al. "Gimli : A Cross-Platform Permutation." In: *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017, pp. 299–320. DOI: 10.1007/978-3-319-66787-4_15. URL: https://doi.org/10.1007/978-3-319-66787-4_15.

[BDHPAK17] Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. "Farfalle: parallel permutation-based cryptography." In: *IACR Trans. Symmetric Cryptol.* 2017.4 (2017), pp. 1–38. URL: https://tosc.iacr.org/index.php/ToSC/article/view/801.

[BDPVA13] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. "Keccak." In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 313–314. ISBN: 978-3-642-38348-9.

[BLN18] Ritam Bhaumik, Eik List, and Mridul Nandi. "ZCZ - Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls." In: *Advances in Cryptology - ASIACRYPT 2018, Proceedings, Part I*. 2018, pp. 336–366.

[BJKS93] Jürgen Bierbrauer, Thomas Johansson, Gregory Kabatianskii, and Ben J. M. Smeets. "On Families of Hash Functions via Geometric Codes and Concatenation." In: *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*. Ed. by Douglas R. Stinson. Vol. 773. Lecture Notes in Computer Science. Springer, 1993, pp. 331–342. DOI: 10.1007/3-540-48329-2_28. URL: https://doi.org/10.1007/3-540-48329-2_28.

[BR02] John Black and Phillip Rogaway. "A Block-Cipher Mode of Operation for Parallelizable Message Authentication." In: *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*. Ed. by Lars R. Knudsen. Vol. 2332. Lecture Notes in Computer Science. Springer, 2002, pp. 384–397. DOI: 10.1007/3-540-46035-7_25. URL: https://doi.org/10.1007/3-540-46035-7_25.

[Boe93] Bert den Boer. "A Simple and Key-Economical Unconditional Authentication Scheme." In: *J. Comput. Secur.* 2 (1993), pp. 65–72.

[BKLTVV11] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. "spongent: A Lightweight Hash Function." In: *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*. Ed. by Bart Preneel and Tsuyoshi Takagi. Vol. 6917. Lecture Notes in Computer Science. Springer, 2011, pp. 312–325. DOI: 10.1007/978-3-642-23951-9_21. URL: https://doi.org/10.1007/978-3-642-23951-9_21.

[BKLPPRSV07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. "PRESENT: An Ultra-Lightweight Block Cipher." In: *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*. Ed. by Pascal Paillier and Ingrid Verbauwhede. Vol. 4727. Lecture Notes in Computer Science. Springer, 2007, pp. 450–466. DOI: 10.1007/978-3-540-74735-2_31. URL: https://doi.org/10.1007/978-3-540-74735-2_31.

[CS08] Debrup Chakraborty and Palash Sarkar. "A General Construction of Tweakable Block Ciphers and Different Modes of Operations." In: *IEEE Trans. Information Theory* 54.5 (2008), pp. 1991–2006.

[CS14] Shan Chen and John P. Steinberger. "Tight Security Bounds for Key-Alternating Ciphers." In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 327–350. DOI: 10.1007/978-3-642-55220-5_19. URL: https://doi.org/10.1007/978-3-642-55220-5_19.

[CLM19] Yu Long Chen, Eran Lambooij, and Bart Mennink. "How to Build Pseudorandom Functions from Public Random Permutations." In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11692. Lecture Notes in Computer Science. Springer, 2019, pp. 266–293. DOI: 10.1007/978-3-030-26948-7_10. URL: https://doi.org/10.1007/978-3-030-26948-7_10.

[CDNPS23] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and **Abishanka Saha**. "Proof of Mirror Theory for a Wide Range of $\xi _{\max }$." In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Tech-*

niques, Lyon, France, April 23-27, 2023, Proceedings, Part IV. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 470–501. DOI: 10.1007/978-3-031-30634-1_16. URL: https://doi.org/10.1007/978-3-031-30634-1_16.

[CJN20] Benoît Cogliati, Ashwin Jha, and Mridul Nandi. "How to Build Optimally Secure PRFs Using Block Ciphers." In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. Lecture Notes in Computer Science. Springer, 2020, pp. 754–784. DOI: 10.1007/978-3-030-64837-4_25.

[CS16] Benoît Cogliati and Yannick Seurin. "EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC." In: *CRYPTO 2016, Proceedings, Part I*. 2016, pp. 121–149. DOI: 10.1007/978-3-662-53018-4_5.

[CEJNS24] Benoît Cogliati, Jordan Ethan, Ashwin Jha, Mridul Nandi, and **Abishanka Saha**. *On the Number of Restricted Solutions to Constrained Systems and their Applications*. Cryptology ePrint Archive, Paper 2024/1163. https://eprint.iacr.org/2024/1163. 2024. URL: https://eprint.iacr.org/2024/1163.

[DHT17] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. "Information-Theoretic Indistinguishability via the Chi-Squared Method." In: *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*. 2017, pp. 497–523.

[Des] "Data encryption standard." In: *Federal Information Processing Standards Publication* 112 (1999).

[DDNP18] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. "Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF." In: *IACR Trans. Symmetric Cryptol.* 2018.3 (2018), pp. 36–92. DOI: 10.13154/tosc.v2018.i3.36-92.

[DDNPZ17] Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. "Single Key Variant of PMAC_Plus." In: *IACR Trans. Symmetric Cryptol.* 2017.4 (2017), pp. 268–305. DOI: 10.13154/tosc.v2017.i4.268-305.

[DH76] W. Diffie and M. Hellman. "New directions in cryptography." In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[Din24] Itai Dinur. "Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis." In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I*. Ed. by Marc Joye and Gregor Leander. Vol. 14651. Lecture Notes in Computer Science. Springer, 2024, pp. 33–62. DOI: 10.1007/978-3-031-58716-0_2. URL: https://doi.org/10.1007/978-3-031-58716-0_2.

[DNS22] Avijit Dutta, Mridul Nandi, and **Abishanka Saha**. "Proof of Mirror Theory for $\xi_{max} = 2$." In: *IEEE Trans. Inf. Theory* 68.9 (2022), pp. 6218–6232. DOI: 10.1109/TIT.2022.3171178. URL: https://doi.org/10.1109/TIT.2022.3171178.

[GM82] Shafi Goldwasser and Silvio Micali. "Probabilistic encryption & how to play mental poker keeping secret all partial information." In: *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*. STOC '82. San Francisco, California, USA: Association for Computing Machinery, 1982, 365–377. ISBN: 0897910702. DOI: 10.1145/800070.802212. URL: https://doi.org/10.1145/800070.802212.

[GM84] Shafi Goldwasser and Silvio Micali. "Probabilistic encryption." In: *Journal of Computer and System Sciences* 28.2 (1984), pp. 270–299. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(84)90070-9. URL: https://www.sciencedirect.com/science/article/pii/0022000084900709.

[GJMN16] Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves. "Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption." In: *Advances in Cryptology - EUROCRYPT 2016, Proceedings, Part I*. 2016, pp. 263–293.

[GSWG19] Chun Guo, Yaobin Shen, Lei Wang, and Dawu Gu. "Beyond-birthday secure domain-preserving PRFs from a single permutation." In: *Des. Codes Cryptogr.* 87.6 (2019), pp. 1297–1322. DOI: 10.1007/s10623-018-0528-8.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. "The LED Block Cipher." In: *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*. Ed. by Bart Preneel and Tsuyoshi Takagi. Vol. 6917. Lecture Notes in Computer Science. Springer, 2011, pp. 326–341. DOI: 10.1007/978-3-642-23951-9_22. URL: https://doi.org/10.1007/978-3-642-23951-9_22.

[HWKS98] Chris Hall, David A. Wagner, John Kelsey, and Bruce Schneier. "Building PRFs from PRPs." In: *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*. Ed. by Hugo Krawczyk. Vol. 1462. Lecture Notes in Computer Science. Springer, 1998, pp. 370–389. DOI: 10.1007/BFb0055742.

[HT16] Viet Tung Hoang and Stefano Tessaro. "Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security." In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. Lecture Notes in Computer Science. Springer, 2016, pp. 3–32. DOI: 10.1007/978-3-662-53018-4_1. URL: https://doi.org/10.1007/978-3-662-53018-4_1.

[Iwa06] Tetsu Iwata. "New Blockcipher Modes of Operation with Beyond the Birthday Bound Security." In: *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*. 2006, pp. 310–327. DOI: 10.1007/11799313_20.

[IK03] Tetsu Iwata and Kaoru Kurosawa. "OMAC: One-Key CBC MAC." In: *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*. Ed. by Thomas Johansson. Vol. 2887. Lecture Notes in Computer Science. Springer, 2003, pp. 129–153. DOI: 10.1007/978-3-540-39887-5_11. URL: https://doi.org/10.1007/978-3-540-39887-5_11.

[IMV16] Tetsu Iwata, Bart Mennink, and Damian Vizár. "CENC is Optimally Secure." In: *Cryptology ePrint Archive, Report 2016/1087* (2016). https://eprint.iacr.org/2016/1087.

[IM16] Tetsu Iwata and Kazuhiko Minematsu. "Stronger Security Variants of GCM-SIV." In: *IACR Trans. Symmetric Cryptol.* 2016.1 (2016), pp. 134–157. DOI: 10.13154/tosc.v2016.i1.134-157.

[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. "ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication." In: *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*. 2017, pp. 34–65. DOI: 10.1007/978-3-319-63697-9_2.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. "Tweaks and Keys for Block Ciphers: The TWEAKEY Framework." In: *Advances in Cryptology - ASIACRYPT 2014, Proceedings, Part II*. 2014, pp. 274–288.

[JNPS21] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. "The Deoxys AEAD Family." In: *J. Cryptol.* 34.3 (2021), p. 31.

[Jha24] Ashwin Jha. *The generalized sum-capture problem for abelian groups*. 2024.

[JKNS24] Ashwin Jha, Mustafa Khairallah, Mridul Nandi, and **Abishanka Saha**. "Tight Security of TNT and Beyond - Attacks, Proofs and Possibilities for the Cascaded LRW Paradigm." In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I*. Ed. by Marc Joye and Gregor Leander. Vol. 14651. Lecture Notes in Computer Science. Springer, 2024, pp. 249–279. DOI: 10.1007/978-3-031-58716-0_9. URL: https://doi.org/10.1007/978-3-031-58716-0_9.

[JN20] Ashwin Jha and Mridul Nandi. "Tight Security of Cascaded LRW2." In: *J. Cryptol.* 33.3 (2020), pp. 1272–1317.

[JN22] Ashwin Jha and Mridul Nandi. "A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF." In: *Entropy* 24.4 (2022), p. 462. DOI: 10.3390/E24040462. URL: https://doi.org/10.3390/e24040462.

[KLL20] Seongkwang Kim, ByeongHak Lee, and Jooyoung Lee. "Tight Security Bounds for Double-Block Hash-then-Sum MACs." In: *Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part I*. 2020, pp. 435–465. DOI: 10.1007/978-3-030-45721-1_16.

[KR11] Ted Krovetz and Phillip Rogaway. "The Software Performance of Authenticated-Encryption Modes." In: *Fast Software Encryption - FSE 2011. Revised Selected Papers*. 2011, pp. 306–327.

[LS13] Rodolphe Lampe and Yannick Seurin. "Tweakable Blockciphers with Asymptotically Optimal Security." In: *Fast Software Encryption - FSE 2013, Revised Selected Papers*. 2013, pp. 133–151.

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. "Tweakable Blockciphers with Beyond Birthday-Bound Security." In: *Advances in Cryptology - CRYPTO 2012, Proceedings*. 2012, pp. 14–30.

[LNS18] Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras. "Generic Attacks Against Beyond-Birthday-Bound MACs." In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10991. Lecture Notes in Computer Science. Springer, 2018, pp. 306–336. DOI: 10.1007/978-3-319-96884-1_11. URL: https://doi.org/10.1007/978-3-319-96884-1_11.

[LRW02] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. "Tweakable Block Ciphers." In: *Advances in Cryptology - CRYPTO 2002, Proceedings*. 2002, pp. 31–46.

[Luc00] Stefan Lucks. "The Sum of PRPs Is a Secure PRF." In: *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*. Ed. by Bart Preneel. Vol. 1807. Lecture Notes in Computer Science. Springer, 2000, pp. 470–484. DOI: 10.1007/3-540-45539-6_34. URL: https://doi.org/10.1007/3-540-45539-6_34.

[LPTY16] Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. "A MAC Mode for Lightweight Block Ciphers." In: *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*. Ed. by Thomas Peyrin. Vol. 9783. Lecture Notes in Computer Science. Springer, 2016, pp. 43–59. DOI: 10.1007/978-3-662-52993-5_3. URL: https://doi.org/10.1007/978-3-662-52993-5_3.

[Men18] Bart Mennink. "Towards Tight Security of Cascaded LRW2." In: *Theory of Cryptography - TCC 2018, Proceedings, Part II*. 2018, pp. 192–222.

[MRV15] Bart Mennink, Reza Reyhanitabar, and Damian Vizár. "Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption." In: *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9453. Lecture Notes in Computer Science. Springer, 2015, pp. 465–489. DOI: 10.1007/978-3-662-48800-3_19. URL: https://doi.org/10.1007/978-3-662-48800-3_19.

[Min06] Kazuhiko Minematsu. "Improved Security Analysis of XEX and LRW Modes." In: *Selected Areas in Cryptography - SAC 2006, Revised Selected Papers*. 2006, pp. 96–113.

[ML19] Alexander Moch and Eik List. "Parallelizable MACs Based on the Sum of PRPs with Security Beyond the Birthday Bound." In: *Applied Cryptography and Network Security - ACNS 2019, Proceedings*. 2019, pp. 131–151.

[Nai17a] Yusuke Naito. "Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length." In: *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*. 2017, pp. 446–470. DOI: 10.1007/978-3-319-70700-6_16.

[Nai17b] Yusuke Naito. "Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length." In: *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10626. Lecture Notes in Computer Science. Springer, 2017, pp. 446–470. DOI: 10.1007/978-3-319-70700-6_16. URL: https://doi.org/10.1007/978-3-319-70700-6_16.

[Nan06] Mridul Nandi. "A Simple and Unified Method of Proving Indistinguishability." In: *Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings*. Ed. by Rana Barua and Tanja Lange. Vol. 4329. Lecture Notes in Computer Science. Springer, 2006, pp. 317–334. DOI: 10.1007/11941378_23. URL: https://doi.org/10.1007/11941378_23.

[Nat01] National Institute of Standards and Technology. *Announcing the Advanced Encryption Standard (AES)*. FIPS PUB 197. Accessed: 2024-07-10. U.S. Department of Commerce, 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[Pat91a] Jacques Patarin. "Etude des generateurs de permutations pseudo-aleatoires bases sur le schema du D. E. S." Thèse de doctorat dirigée par Camion, Paul Sciences appliquées Paris 6 1991. PhD thesis. 1991. URL: http://www.theses.fr/1991PA066601.

[Pat91b] Jacques Patarin. "Pseudorandom permutations based on the D.E.S. scheme." In: *EUROCODE '90*. Ed. by Gérard Cohen and Pascale Charpin. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 193–204. ISBN: 978-3-540-47546-0.

[Pat98] Jacques Patarin. "About Feistel Schemes with Six (or More) Rounds." In: *Fast Software Encryption*. Ed. by Serge Vaudenay. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 103–121. ISBN: 978-3-540-69710-7.

[Pat03] Jacques Patarin. "Luby-Rackoff: 7 Rounds Are Enough for $2^n(1-\epsilon)$ Security." In: *Advances in Cryptology - CRYPTO 2003*. Ed. by Dan Boneh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 513–529. ISBN: 978-3-540-45146-4.

[Pat05] Jacques Patarin. "On Linear Systems of Equations with Distinct Variables and Small Block Size." In: *Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers*. 2005, pp. 299–321. DOI: 10.1007/11734727_25.

[Pato8a] Jacques Patarin. "A Proof of Security in $O(2^n)$ for the Benes Scheme." In: *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*. Ed. by Serge Vaudenay. Vol. 5023. Lecture Notes in Computer Science. Springer, 2008, pp. 209–220. DOI: 10.1007/978-3-540-68164-9_14. URL: https://doi.org/10.1007/978-3-540-68164-9_14.

[Pato8b] Jacques Patarin. "A Proof of Security in O(2n) for the Xor of Two Random Permutations." In: *Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings*. 2008, pp. 232–248. DOI: 10.1007/978-3-540-85093-9_22.

[Pato9] Jacques Patarin. "The "Coefficients H" Technique." In: *Selected Areas in Cryptography*. Ed. by Roberto Maria Avanzi, Liam Keliher, and Francesco Sica. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 328–345. ISBN: 978-3-642-04159-4.

[Pat10a] Jacques Patarin. "Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography." In: *Cryptology ePrint Archive, Report 2010/287* (2010). https://eprint.iacr.org/2010/287.

[Pat10b] Jacques Patarin. *Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities*. Cryptology ePrint Archive, Paper 2010/293. https://eprint.iacr.org/2010/293. 2010.

[Pat13] Jacques Patarin. "Security in $O(2^n)$ for the Xor of Two Random Permutations - Proof with the standard H technique." In: *Cryptology ePrint Archive, Report 2013/368* (2013). https://eprint.iacr.org/2013/368.

[PS16] Thomas Peyrin and Yannick Seurin. "Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers." In: *Advances in Cryptology - CRYPTO 2016, Proceedings, Part I*. 2016, pp. 33–63.

[Pro14] Gordon Procter. "A Note on the CLRW2 Tweakable Block Cipher Construction." In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 111.

[Rog04] Phillip Rogaway. "Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC." In: *Advances in Cryptology - ASIACRYPT 2004, Proceedings*. 2004, pp. 16–31.

[SK96] Bruce Schneier and John Kelsey. "Unbalanced Feistel networks and block cipher design." In: *FSE*. Vol. 96. 1996, pp. 121–144.

[Sha49] C. E. Shannon. "Communication theory of secrecy systems." In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[SPSCV22] Yaobin Shen, Thomas Peters, François-Xavier Standaert, Gaëtan Cassiers, and Corentin Verhamme. "Triplex: an Efficient and One-Pass Leakage-Resistant Mode of Operation." In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 135–162.

[ST23] Ferdinand Sibleyras and Yosuke Todo. "Keyed Sum of Permutations: A Simpler RP-Based PRF." In: *Topics in Cryptology - CT-RSA 2023, Proceedings*. Ed. by Mike Rosulek. Vol. 13871. Lecture Notes in Computer Science. Springer, 2023, pp. 573–593.

[Sor84] Arthur Sorkin. "Lucifer, a cryptographic algorithm." In: *Cryptologia* 8.1 (1984), pp. 22–42. DOI: 10.1080/0161-118491858746.

[Tay93] Richard Taylor. "An Integrity Check Value Algorithm for Stream Ciphers." In: *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*. Ed. by Douglas R. Stinson. Vol. 773. Lecture Notes in Computer Science. Springer, 1993, pp. 40–48. DOI: 10.1007/3-540-48329-2_4. URL: https://doi.org/10.1007/3-540-48329-2_4.

[TZ21] Stefano Tessaro and Xihu Zhang. "Tight Security for Key-Alternating Ciphers with Correlated Sub-keys." In: *Advances in Cryptology - ASIACRYPT 2021, Proceedings, Part III*. Vol. 13092. Lecture Notes in Computer Science. Springer, 2021, pp. 435–464. DOI: 10.1007/978-3-030-92078-4_15.

[Vau03] Serge Vaudenay. "Decorrelation: A Theory for Block Cipher Security." In: *J. Cryptol.* 16.4 (2003), pp. 249–286. DOI: 10.1007/S00145-003-0220-6. URL: https://doi.org/10.1007/s00145-003-0220-6.

[Yas10a] Kan Yasuda. "The Sum of CBC MACs Is a Secure PRF." In: *CT-RSA 2010*. 2010, pp. 366–381. DOI: 10.1007/978-3-642-11925-5_25.

[Yas10b] Kan Yasuda. "The Sum of CBC MACs Is a Secure PRF." In: *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*. Ed. by Josef Pieprzyk. Vol. 5985. Lecture Notes in Computer Science. Springer, 2010, pp. 366–381. DOI: 10.1007/978-3-642-11925-5_25. URL: https://doi.org/10.1007/978-3-642-11925-5_25.

[Yas11a] Kan Yasuda. "A New Variant of PMAC: Beyond the Birthday Bound." In: *Advances in Cryptology - CRYPTO 2011. Proceedings*. 2011, pp. 596–609. DOI: 10.1007/978-3-642-22792-9_34.

[Yas11b] Kan Yasuda. "A New Variant of PMAC: Beyond the Birthday Bound." In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. Ed. by Phillip Rogaway. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 596–609. DOI: 10.1007/978-3-642-22792-9_34. URL: https://doi.org/10.1007/978-3-642-22792-9_34.

[ZWSW12] Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. "3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound." In: *ASIACRYPT 2012*. 2012, pp. 296–312. DOI: 10.1007/978-3-642-34961-4_19.

[ZQG23] Zhongliang Zhang, Zhen Qin, and Chun Guo. "Just tweak! Asymptotically optimal security for the cascaded LRW1 tweakable blockcipher." In: *Des. Codes Cryptogr.* 91.3 (2023), pp. 1035–1052.

DECLARATION

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification.

Kolkata, July 2024

Abishanka Saha