Indian Statistical Institute

Master's Thesis

Device Independent Quantum Cryptography For Finite Samples

Submitted by:
Jyotirmoy Basak

Supervisor:
Prof. Subhamoy Maitra

Dissertation submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science

July, 2017

Dedicated to my family

CERTIFICATE

This is to certify that the dissertation entitled **"Device Independent Quantum Cryptography For Finite Samples"** submitted by **Jyotirmoy Basak** to Indian Statistical Institute, Kolkata, in partial fulfillment for the award of the degree of **Master of Technology** in **Computer Science** is a bonafide record of work carried out by him under my supervision and guidance. The dissertation has fulfilled all the requirements as per the regulations of this institute and, in my opinion, has reached the standard needed for submission.

Prof. Subhamoy Maitra
Professor,
Applied Statistics Unit,
Indian Statistical Institute, Kolkata
Dated : July, 2017.

Acknowledgments

I would like to show my highest gratitude to my advisor, *Prof. Subhamoy Maitra*, for his guidance and continuous support and encouragement. He has literally taught me how to do good research, and motivated me with great insights and innovative ideas.

My deepest thanks to Arpita mam, Bappa da, Goutam sir for their constant supports and valuable suggestions and discussions to complete my dissertation. I would like to thank Guruprasad sir, who first introduce me with the subject Quantum Information and Computation. I would also like to thank all the teachers of Indian Statistical Institute, for their valuable suggestions and discussions which added an important dimension to my research work.

Finally, I am very much thankful to my parents, grandmother and all other family members for their everlasting supports. Last but not the least, I would like to thank all of my friends for their help and support.

Jyotirmoy Basak
M.Tech, Computer Science,
Indian Statistical Institute, Kolkata

Abstract

Quantum cryptography promises levels of security that are impossible to replicate in classical world. In all the initial quantum cryptographic protocols, the involving parties trust the measurement devices involved in the protocol.

Later it is shown that the security of the protocol can't be guaranteed when the quantum devices on which the protocol relies are untrusted. This invents the concept of device independent protocols which implies that the security does not rely on trusting that the quantum devices used are truthful. The aim of the device independent approach to cryptography is to do away with this trustful assumption, and, consequently, significantly increase security.

With this aim, several device independent quantum cryptographic protocols are proposed till now. All these existing device independent schemes are perfectly alright for asymptotic limit only. However, none of these protocols have analyzed the scheme for finite sample size i.e all the existing device independent protocols are theoretically correct but none of these are practically implementable.

In this thesis, we overcome this shortcomings by upgrading the existing device independent quantum cryptographic protocols for finite samples. The modified protocols provide an estimation of the sample size in an optimal way. Due to finite sample size, we have to allow some information leakage to the adversary. However, by fixing the accuracy parameter appropriately for all the protocols, we show that the adversary can't perform any fruitful attack due to this information leakage.

Contents

Abstract **1**

Contents **4**

1 Introduction **7**

1.1 Quantum Cryptography - An Overview 7

1.2 Applications of Quantum Cryptography 8

1.3 Related Works and Limitations 9

1.4 Our Contribution 10

1.5 Organization of Thesis 11

2 Preliminaries **12**

2.1 Basics of Quantum Information 12

2.1.1 Qubits and Measurements 12

2.1.2 Entangled States 13

2.1.3 Bloch Sphere Representation 14

2.1.4 Quantum Operators 15

2.2 Basics of Quantum Computation 15

2.2.1 Quantum Gates 16

3 Overview of Quantum Cryptographic Protocols 19

3.1 Quantum Key Distribution 19

3.1.1 BB84 Protocol: 19

3.1.2 Device Independent QKD Protocol: 21

3.2 Quantum Private Query 22

3.2.1 Yang's Quantum Private Query Protocol: 22

3.2.2 Device Independent QPQ Protocol: 23

3.3 Quantum Bit Commitment 24

3.3.1 Quantum Bit Commitment Protocol: 24

3.3.2 Device Independent Quantum Bit Commitment: 24

4 Proposed Scheme For Finite Sample Device Independent Protocols 26

4.1 Expected estimation of sample size 26

4.2 Generalization towards device independent protocols for finite samples . . . 27

4.2.1 Generalized View of CHSH Game 28

4.3 Modification of DI-QKD Towards Finite Number of Entangled States . . . 30

4.3.1 Security bounds against additional information leakage and lower key rate 30

4.3.2 Modified DI-QKD protocol with finite samples and Security Analysis 32

4.3.3 Security Analysis of the Modified Protocol 34

4.4 Modification of DI-QPQ Towards Finite Number of Entangled States 35

4.4.1 Maximization of success probability 35

4.4.2 Security bounds against additional information leakage 37

4.4.3 Modified DI-QPQ protocol with finite samples and Security Analysis 39

4.4.4 Security Analysis of the Modified Protocol 40

4.5 Modification of DI-QBC Towards Finite Number of Entangled States 41

5 Overview Of Quantum Pseudo Telepathy Games 42

5.1 CHSH Game . . . 43

5.1.1 Classical Strategy: . . . 43

5.1.2 Quantum Strategy: . . . 43

5.2 GHZ Game . . . 44

5.2.1 Classical Strategy: . . . 44

5.2.2 Quantum Strategy: . . . 45

5.3 Parity Game . . . 46

5.3.1 Classical Strategy: . . . 46

5.3.2 Quantum Strategy: . . . 47

6 Proposed Strategy For Optimal Sample Device Independent Protocols 48

6.1 Modification of DI-QKD Towards Optimal Number of Entangled States . . 48

6.1.1 Transformation of two qubit state into three qubit . . . 49

6.1.2 Comparative Study Between Two Games . . . 49

6.1.3 Modified DI-QKD protocol with optimal samples . . . 50

6.2 Modification of DI-QPQ Towards Optimal Number of Entangled States . . 52

6.2.1 Transformation of two qubit state into three qubit . . . 52

6.2.2 Comparative Study Between Two Games . . . 53

6.2.3 Modified DI-QPQ protocol with optimal samples . . . 54

6.3 Modification of DI-QBC Towards Optimal Number of Entangled States . . 55

6.3.1 Modified DI-QBC protocol with optimal samples . . . 55

7 Conclusion and Future Work 57

Bibliography 60

List of Figures

2.1 Bloch sphere representation of a qubit 15

2.2 Two qubit quantum gates 18

2.3 Three qubit quantum gates 18

4.1 Plot of CHSH correlation value as a function of eavesdropper's deviation value ϵ_E 31

4.2 Plot of p_{QPQ} as a function of θ 36

4.3 Plot of m_{QPQ} (vertical axis) as a function of ϵ (left) and p_{QPQ} (right) with $\gamma = 0.01$ 37

6.1 Comparative study of success probabilities between CHSH and parity game for DI-QKD protocol 50

6.2 Comparative study of success probabilities between CHSH and parity game for DI-QPQ protocol 53

List of Tables

2.1 Summary of some quantum mechanical notations 14

3.1 Procedure of BB84 Protocol 20

Chapter 1

Introduction

1.1 Quantum Cryptography - An Overview

Historically, the term “cryptography” has been associated with the study and design of techniques for secure communication in the presence of third parties called adversaries or eavesdroppers. In 1976, Diffie and Hellman in their paper “New Directions in Cryptography”[13], identified the requirement of data integrity, authentication and non-repudiation in cryptographic protocols. The real breakthrough in cryptography came when Rivest, Shamir and Adlemann discovered an amazingly simple scheme for encryption, popularly known as RSA. The basic principle they used is the hardness assumption of factorization problem i.e, given a large number, there was no polynomial time algorithm to find it’s prime factors.

It was known that Quantum computers offer enormous computation power which is not possible in the classical domain. Using this concept, Peter Shor came with a polynomial time quantum algorithm for factoring large number in 1994. The algorithm shows that if quantum computer can be made in reality then all the RSA based crypto system will be evacuated in a moment.

Another important question in classical crypto system is to establish some common key between distant separated parties. The widely used schemes that is used mainly in classical crypto system is based on famous Discrete Log Problem. But it has been also shown that with the help of a quantum computer, Discrete Log Problem can be easily broken. All these results show that the existing classical cryptographic protocols are no longer secure under the enormous computation power of quantum computers. This short comings of classical cryptographic protocols lead people to develop the idea of cryptography in quantum paradigm.

Quantum cryptography[19][8] aims to make data secure using fundamental physical principles, such as the quantum mechanical phenomena of entanglement and Heisenberg’s uncertainty principle. The idea behind quantum cryptography is that two people communicating using a quantum channel can be absolutely sure no one is eavesdropping. Heisenbergs uncertainty principle requires anyone measuring a quantum system to disturb it, and that disturbance alerts legitimate users as to the eavesdroppers presence. For this reason quantum cryptography is completely secure.

The main challenge now in quantum cryptographic domain is to implement secure quantum cryptographic protocols for practical purpose. In practice, quantum cryptography has been demonstrated in the laboratory by IBM and others, but over relatively short distances. Recently, over longer distances, fiber optic cables with incredibly pure optic properties have successfully transmitted photon bits up to 60 kilometers. Beyond that, BERs (bit error rates) caused by a combination of the Heisenberg Uncertainty Principle and microscopic impurities in the fiber make the system unworkable. Some research has seen successful transmission through the air, but this has been over short distances in ideal weather conditions. It remains to be seen how much further technology can push forward the distances at which quantum cryptography is practical.

1.2 Applications of Quantum Cryptography

Several quantum cryptographic protocols are developed since the first application of quantum cryptography by Bennet and Brassard[6]($BB84$ protocol). Quantum cryptographic protocols offer more security than that can be achieved in classical scenario. The well known applications of quantum cryptography is as follows-

Quantum Key Distribution: The most well known and developed application of quantum cryptography is quantum key distribution, which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, key establishment will fail causing Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques.

Quantum Private Query: Quantum private query is a two party mistrustful cryptographic protocol where one of the two legitimate party, say Bob, owns a database. His job is to protect the entire database from the client's(Alice's) knowledge along with providing the element asked by client. On the other hand, the client's motivation is to extract more elements from the database beside her query. If the owner of the database tries to obtain information on the query, the person querying the database can find it out.

Quantum Coin Flipping: Quantum coin flipping is a protocol that is used between two participants who do not trust each other. The participants communicate via a quantum channel and exchange information through the transmission of qubits. Alice will determine a random basis and sequence of qubits and then transmit them to Bob. Bob then detects and records the qubits. Once Bob has recorded the qubits sent by Alice, he makes a guess to Alice on what basis she chose. Alice reports whether he won or lost to Bob and then sends Bob her entire original qubit sequence. Since the two parties do not trust each other, cheating is likely to occur at any step in the process.

Quantum Bit Commitment: Quantum bit commitment(QBC) is a two-party cryptography including the following phases. In the commit phase, Alice (the sender of the commitment) decides the value of the bit b(b = 0 or 1) that she wants to commit, and sends Bob(the receiver of the commitment) a piece of evidence, e.g., some quantum states. Later, in the reveal phase, Alice announces the value of b, and Bob checks it with the evidence. The interval between the commit and reveal phases is sometimes called the holding phase. A QBC protocol is called unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1. Here Alice's cheating means that she wants to change the value of b after the commit phase, while Bob's cheating means that he tries to learn b before the reveal phase.

All these quantum cryptographic protocols provide better security than the corresponding protocol in classical paradigm. But if the protocols are not implemented perfectly or the devices involving in the protocols are imperfect then the security of the protocols may be violated. So, this protocols are considered as "probably secure" protocol whose security assumption are based on the perfect working of the involved devices.

In all the cases, the initial protocol was proposed assuming that the devices are perfect i.e, all the initial versions of the protocols are device dependent. Now quantum researchers are interested in the device independent versions of these protocols where security does not rely on trusting that the quantum devices used are truthful. Thus the security analysis of such a protocol needs to consider scenarios of imperfect or even malicious devices.

1.3 Related Works and Limitations

In 1984, Bennett et. al.[6] proposed first quantum key distribution(QKD) protocol which is also the first protocol in quantum cryptographic paradigm. Thereafter, many QKD protocols were proposed but all these were device dependent. Mayers et. al.[24] proposed first device independent QKD protocol. Later on Ekert[15], Barrett[3], Vazirani et. al.[32] and many others proposed device independent QKD protocols.

The first protocol in quantum private query(QPQ) domain had been proposed by Giovannetti et al.[17] followed by [16] and [28]. However, those scheme are highly theoretical and difficult for implementation. For implementation purpose, Jakobi et al.[21] came out with a QPQ protocol based on SARG04 quantum key distribution protocol[29]. Later Yang et al. came out with a flexible QPQ protocol[33] which was based on B92 quantum key distribution scheme[7]. Maitra et. al.[23] proposed a device independent QPQ protocol which is probably the first device independent QPQ protocol.

In distrustful quantum cryptographic paradigm, Mochon[26] proposed a weak quantum coin flipping protocol with arbitrary small bias. Mayers[25], Lo and Chau[22] proposed quantum bit commitment protocol. Later on many other bit commitment and coin flipping protocol was proposed but Silman et. al.[30] first came out with an interesting bit commitment and coin flipping protocol where the device dependent protocol is indeed device independent one. Recently, Adlam et. al.[1] came out with a device independent bit commitment protocol followed by Aharon et al.[2].

The limitation of all these device independent protocols are that they are theoretically alright but not practically implementable as they proposed the test of device independence property for infinite number of samples. This motivates us to introduce the device independent protocols for finite number of samples so that it can be practically implementable.

1.4 Our Contribution

In this thesis, the focus is to propose device independent quantum protocols for finite samples by keeping the security intact so that it can be practically implementable. The contributions of our work are summarized as follows:

- We have improved the device independent protocols of QKD, QPQ and bit commitment for finite samples(which was not introduced previously) i.e, the testing of the measurement device involves finite number of samples so that it can be practically implementable.
- We have to allow some deviation from the actual intended value while testing for finite samples. Here, we give a bound on the the value of deviation that eavesdropper can choose in terms of the chosen accuracy parameter.
- By choosing appropriate value of accuracy parameter, we have shown that the modified protocol will not generate any security loop-hole for this amount of deviation.
- We perform rigorous security analysis for the modified protocol and show that the security remains intact as compared to the previous device independent protocols(which are theoretically correct but not practically implementable) and security increased compared to existing device dependent protocols.

- We analyze the performance of different pseudo telepathy games in terms of their success probability in quantum paradigm by drawing graphs from our calculated value and choose the most suitable game(or games) in terms of optimal sample size for different scenario.
- Finally we propose a modified approach based on the analysis of different quantum pseudo telepathy games for the testing of device independence property(which was not introduced previously) to further reduce the sample size for finite sample device independent protocols.

1.5 Organization of Thesis

The rest of the thesis is organized as follows.

- In chapter 2, we discuss about the necessary mathematical background and basic overview of quantum information and computation.
- In chapter 3, we propose the detailed overview of some quantum crytpographic protocols and discuss about their existing device independent versions.
- In chapter 4, we introduce a general setup for all these protocols and propose our modified device independent protocol for finite samples.
- In chapter 5, we propose an overview of different quantum pseudo telepathy games and discuss about their classical and quantum strategy along with their success probability in different paradigm.
- In chapter 6, we propose a modified strategy for testing the device independence property to further reduce the sample size and also propose further modified protocols by applying this strategy.
- In chapter 7, we conclude the thesis by providing a summary of our work and give a brief discussion on future course of research.

Chapter 2

Preliminaries

"Quantum mechanics: Real black magic calculus" - Albert Einstein.

Quantum computing is an interdisciplinary field, encompassing physics, mathematics and computer science. The basic introductory knowledge which is required to work on the field of quantum information and quantum computation is mentioned here.

2.1 Basics of Quantum Information

To study about different aspects of quantum information, some basic knowledge about quantum mechanics is necessary which is described here. More details about this topic can be found in [27].

2.1.1 Qubits and Measurements

The fundamental concept of classical computation and classical information is the bit, which can be in two states - 0 or 1. Analogously, the simplest quantum mechanical system is the qubit, which has a $2-D$ state space and is represented by a unit state vector. Let $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in that state space can be written as :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{where } \alpha \text{ and } \beta \text{ are complex numbers} \tag{2.1}$$

For $|\psi\rangle$ to be a unit vector, $\langle\psi|\psi\rangle = 1$, where $\langle\alpha|\beta\rangle$ represents inner product of two vectors α and β. This implies that this α and β should also satisfy the property

$|\alpha|^2 + |\beta|^2 = 1$. Similarly an n - qubit system has 2^n computational basis states and can have a state which is a linear combination of these basis states. This gives rise to the continuum of quantum states.

This way a qubit differs from a classical bit is that, it can exist in superposition of states which is not possible in classical scenario. Any linear combination $\sum_i \alpha_i|\psi_i\rangle$ is a superposition of the states $|\psi_i\rangle$ with amplitude α_i. The probability that the state of the qubit after measurement happens to be $|\psi_i\rangle$ is $|\alpha_i|^2$. The condition that the probabilities sum to 1 is expressed by the normalization condition $\sum_i |\alpha_i|^2 = 1$.

The simplest measurement is in the standard basis, and measuring $|\psi\rangle$ in $\{|0\rangle, |1\rangle\}$ basis yields 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.More generally, we may choose any orthogonal basis $|v\rangle, |w\rangle$ and measure the qubit in that basis.To do this, we rewrite our state in that basis:$|\psi\rangle = \alpha'|v\rangle + \beta'|w\rangle$. The outcome is $|v\rangle$ with probability $|\alpha'|^2$ and $|w\rangle$ with probability $|\beta'|^2$.

Similarly, according to superposition principle, any quantum state of the two electrons can be written as a linear combination of four states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ in the following way:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{2.2}$$

where each $\alpha_{ij} \in \mathbb{C}$ and $\sum_{ij} |\alpha_{ij}|^2 = 1$.

2.1.2 Entangled States

Tensor product between two one qubit states $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$ is defined as $(\alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle)$.

Most of the two qubit states can be decomposed into two one qubit states like above where the tensor product of two resulting one qubit state produces the original two qubit state. The states which can't be written as a tensor product of two other lower dimensional states are called entangled states.

The concept of maximal entanglement can be defined as follows: if we consider the set of all non entangled states then the entangled state which has maximum distance from this set is called maximally entangled state. This is one way of viewing maximally entangled states though there are various other concepts.

The two qubit entangled states

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

$$|\phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}},$$
$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

are called two qubit maximally entangled states. They are also known as **Bell states**[4][5] or **EPR pairs**[14].

Here are some notations of quantum information and their description listed in the table 2.1 which are used throughout the thesis.

Notation	Description
z^*	Complex conjugate of the complex number z.
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as *bra*.
$\langle\phi\|\psi\rangle$	Inner product between the vectors $\|\phi\rangle$ and $\|\psi\rangle$.
$\|\phi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\phi\rangle$ and $\|\psi\rangle$.
$\|\phi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\phi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = (A^T)^*$
$\langle\phi\|A\|\psi\rangle$	Inner product between $\|\phi\rangle$ and $A\|\psi\rangle$. Equivalently inner product between $A^\dagger\|\psi\rangle$ and $\|\psi\rangle$.

Table 2.1: Summary of some quantum mechanical notations

2.1.3 Bloch Sphere Representation

An useful way of thinking about qubits is the geometric representation of Bloch sphere. Since normalization conditions hold in equation (2.1), $|\alpha|^2+|\beta|^2 = 1$ and it maybe rewritten as:

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle) \quad \text{where } \theta, \phi, \gamma \in \mathbb{R} \tag{2.3}$$

The factor $e^{i\gamma}$ can be ignored because it has no observable effects. Thus equation(2.3) can be effectively written as:

$$|\psi\rangle = (\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle) \tag{2.4}$$

The parameters θ and ϕ define a point on an unit 3-D sphere, called the Bloch sphere(figure 2.1). It offers an useful way of visualizing the state of a single qubit. But the intuition is limited because there is no simple generalization of the Bloch sphere for multiple qubits.

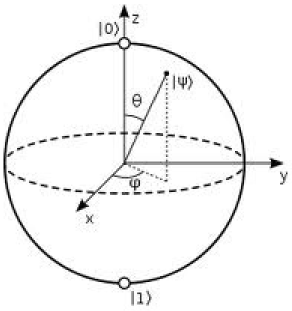

Figure 2.1: Bloch sphere representation of a qubit

2.1.4 Quantum Operators

An operator A whose adjoint is also A is known as **hermitian** or self adjoint operator. An important class of hermitian operators are projectors. Let P be an operator which is defined as,

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i|$$

where $|1\rangle, ..., |k\rangle$ is an orthonormal basis and P satisfies $P^{\dagger} = P$. Here P is hermitian.

Suppose a quantum system is in one of a number of states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i. $\{p_i, |\psi_i\rangle\}$ is called an ensemble of pure states. The **density operator** for the system is defined by the equation

$$\rho = \sum_{i} p_i |\psi_i\rangle\langle\psi_i|$$

This representation is often known as **density matrix** representation. Density operator satisfies the property hermitian, positive(i.e, all eigen values are positive) and $trace(operator) = 1$.

An operator U is called an **unitary operator** if it satisfies the property

$$UU^{\dagger} = U^{\dagger}U = I$$

where $U^{\dagger}$ is the conjugate transpose of U.

2.2 Basics of Quantum Computation

Changes occurring to a quantum state can be described using the language of quantum computation. All valid quantum operations are unitary. The evolution of an isolated quantum system with a finite number of states can be described by a unitary matrix and thus is reversible. Reversibility is a necessary condition for quantum computing.

Quantum circuits can be represented by space-time diagrams. In these diagrams, time usually progresses from left to right. The circuit comprises of a sequence of quantum gates, either in series or parallel. An n - qubit gate or operation is represented by a $2^n \times 2^n$ unitary matrix. The overall unitary transformation performed is computed by composing the unitary matrices of the corresponding quantum gates. If several gates act on the same subset of qubits, then they must be applied in series and their overall effect is computed by the dot product. If adjacent gates within a quantum circuit act on independent subset of qubits, then they can be applied in parallel and the overall effect is the tensor product of the unitary matrices.

2.2.1 Quantum Gates

In this subsection we discuss about basic properties of some fundamental one-qubit, two-qubit and three-qubit operations and the corresponding quantum gates, that are used to build quantum circuits for information processing. It must be borne in mind, that due to no-cloning principle quantum circuits do not have any fanout or feedback mechanism and thus can be represented by an acyclic graph.

One-qubit Gates

A one-qubit gate can be represented by a 2×2 unitary matrix. Some one-qubit gates and their operations are listed below-

- **Global Phase Gate:** The global phase gate, P, is defined as:

  $$P(\theta) = e^{i\theta} I \tag{2.5}$$

  where I denotes the identity matrix, which indicates that no operation is performed.

  Remark: The global phase gate is physically indistinguishable and hence is not physically implemented. But it is useful to match circuit identities.

- **Pauli Gates:** The Pauli spin matrices for the x, y and z axes, corresponding to the Pauli Gates X, Y and Z are respectively:

  $$\sigma_x \equiv X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  $$\sigma_y \equiv Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z \equiv Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- **Rotation Gates:** The evolution of a quantum operation depends on the exponentiation of the Hermitian matrix. This leads to the definition of rotation gates, which represent rotation around different axes.

  $$R_x(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$$

  $$R_y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & \sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$$

  $$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

  X, Y and Z can be regarded as special cases of R_x, R_y, R_z respectively with rotation angles of π. The periods of R_x, R_y and R_z are 4π. The rotation gates can be defined in terms of the Pauli gates as follows:

  $$R_j(\theta) = e^{(\frac{-i\theta A}{2})} = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})A, \quad j \in \{x, y, z\}, \quad A \in \{X, Y, Z\}$$

- **Hadamard Gate:** The Hadamard gate or Hadamard operator denoted by H is defined as follows:

  $$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

  Hadamard operator is an unitary operator which acts as the following-

  $$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

  $$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Two Qubit Gates

The physical interactions available within different types of quantum systems can give rise to different two-qubit operations and corresponding gates. These are described by 4×4 unitary matrices.

One of the most useful operations for both classical and quantum computing are the controlled operations. They act on two qubits - a control qubit and a target qubit. Suppose U is an arbitrary single-qubit operation. For the **controlled-U (CU)** operation, if the control qubit c is set, then U is applied to the target qubit t, else the target qubit t is left alone. That is,

$$|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$$

- **CNOT Gate:** CNOT gate is a specific type of CU gate with $U = X$ gate and is also an unitary operator which acts on two qubits(figure 2.2). The first qubit is called control bit and the second qubit is called target bit. The operation of CNOT gate is defined as follows-

$$U|0\rangle_1|0\rangle_2 = |0\rangle_1|0\rangle_2$$

$$U|0\rangle_1|1\rangle_2 = |0\rangle_1|1\rangle_2$$

$$U|1\rangle_1|0\rangle_2 = |1\rangle_1|1\rangle_2$$

$$U|1\rangle_1|1\rangle_2 = |1\rangle_1|0\rangle_2$$

  where unitary operator U acts as a CNOT gate.

  In terms of computational basis, the action of the CNOT is given by $|c\rangle|t\rangle \rightarrow |c\rangle|t \otimes c\rangle$.

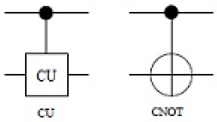

Figure 2.2: Two qubit quantum gates

Three Qubit Gates

Three-qubit reversible gates provide a higher level of abstraction for circuit description because interactions among more than two qubits are difficult to implement. The three qubit gates must be decomposed into two-qubit and one-qubit gates. Some commonly used three-qubit gates are **Toffoli**, **Fredkin** and **Peres** gates(figure 2.3).

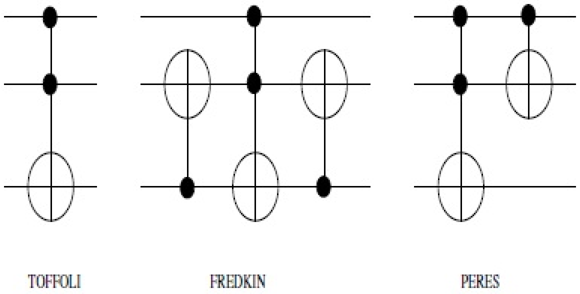

Figure 2.3: Three qubit quantum gates

Chapter 3

Overview of Quantum Cryptographic Protocols

3.1 Quantum Key Distribution

Quantum key distribution(QKD) is a provably secure protocol by which private key bits can be created between two parties over a public channel. This protocol is based on no cloning theorem and proof comes from the quantum property that information gain is only possible at the expense of disturbing the signal. There are many quantum key distribution protocols but the protocol proposed by Bennett and Brassard (commonly known as BB84 protocol) is the most popular one.

3.1.1 BB84 Protocol:

The BB84 protocol[6] is the most popular QKD protocol. It is named after its inventors, Bennett and Brassard. The procedure of BB84 is as follows -

- **Quantum communication phase:**
- In BB84, Alice sends Bob a sequence of photons, each independently chosen from one of the four polarizations - vertical, horizontal, 45-degrees and 135-degrees.
- For each photon, Bob randomly chooses one of the two measurement bases(rectilinear and diagonal) to perform a measurement.
- Bob records his measurement bases and results. Bob publicly acknowledges his receipt of signals.

Alice's bit sequence	1	0	1	1	0	1	0	0	0	1
Alice's basis	$\times$	$+$	$+$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$\times$
Alice's photon polarization	$\nwarrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\nearrow$	$\updownarrow$	$\nearrow$	$\nearrow$	$\leftrightarrow$	$\nwarrow$
Bob's basis	$+$	$+$	$\times$	$+$	$+$	$\times$	$\times$	$+$	$+$	$\times$
Bob's measured polarization	$\updownarrow$	$\leftrightarrow$	$\nwarrow$	$\updownarrow$	$\leftrightarrow$	$\nearrow$	$\nearrow$	$\updownarrow$	$\leftrightarrow$	$\nwarrow$
Bob's shifted measured polarization		$\leftrightarrow$		$\updownarrow$			$\nearrow$		$\leftrightarrow$	$\nwarrow$
Bob's data sequence		0		1			0		0	1

Table 3.1: Procedure of BB84 Protocol

- **Public discussion phase:**
- Alice broadcasts her bases of measurements. Bob broadcasts his bases of measurements.
- Alice and Bob discard all events where they use different bases for a signal. The remaining bits are defined as "sifted bits".
- To test for tampering, Alice randomly chooses a fraction, p, of all remaining events as test events. For those test events, she publicly broadcasts their positions and polarizations.
- Bob broadcasts the polarizations of the test events.
- Alice and Bob compute the error rate of the test events (i.e., the fraction of data for which their values disagree). If the computed error rate is larger than some prescribed threshold value, say 11%, they abort. Otherwise, they proceed to the next step.
- Alice and Bob each convert the polarization data of all remaining data into a binary string called a raw key (by, for example, mapping a vertical or 45- degrees photon to "0" and a horizontal or 135-degrees photon to "1"). They can perform classical post-processing such as error correction and privacy amplification to generate a final key.

Rigorous security proof of BB84 protocol shows that this protocol for quantum key distribution (QKD) is unconditionally secure i.e., the security of the protocol based solely on the validity of quantum mechanics and the behavior of measurement devices. There are some attacks which shows that if the devices involved are untrusted then the protocol will no longer remain secure. So, in device dependent case, the security of the protocol solely depends on the behavior of the devices.

3.1.2 Device Independent QKD Protocol:

Mayers and Yao[24] were the first to put forth a challenge now known as device independence: Except for a necessary assumption of spatial separation, the quantum devices used would be treated as completely uncharacterized entities, and security would be guaranteed based solely on simple tests performed on the devices.

Such a scheme for restoring unconditional security would even be possible relies on a unique feature of quantum entanglement, called monogamy[31]. Indeed, a hint of this approach can already be seen in Ekerts entanglement-based proposal for key distribution[15], which advocated tests based on the violation of Bell inequalities.

Vidick and Vazirani[32] resolve the challenge of device independent quantum key distribution(DIQKD) by showing a variant of Ekerts original protocol that has all the desirable features of DI-QKD.

The security proof of their protocol requires no independence assumptions it only assumes that the devices can be modeled by the laws of quantum mechanics, and are spatially isolated from each other and from any adversarys laboratory.

Vidick and Vazirani's proposed DI-QKD protocol requires the users, Alice and Bob, to make n uses of their devices. From the n pairs of output bits collected they are able to extract a shared key of length κn, where κ is a constant depending on the noise rate η that the users wish to tolerate. The main idea of their DI-QKD protocol is presented in algorithm 1.

- **Inputs:** n = number of rounds, η = noise tolerance
- For rounds $i \in \{1, \cdots, n\}$, Alice picks $x_i \in \{0, 1, 2\}$, and Bob picks $y_i \in \{0, 1\}$, uniformly at random. They input x_i, y_i into their respective devices, obtaining outputs $a_i, b_i \in \{0, 1\}$ respectively.
- **Testing:** Alice chooses a random subset $\mathbf{B} \subset \{1, \cdots, n\}$ of size γn, where γ is a small constant, and shares it publicly with Bob(rounds in **B** are called test rounds). Alice and Bob announce their input/output pairs in **B**. They compute the fraction of inputs in **B** that satisfy the CHSH condition $a_i \oplus b_i = x_i \wedge y_i$. If this fraction is smaller than $\cos^2 \pi/8 - \eta$ they abort the protocol.
- **Extraction:** Alice and Bob publicly reveal their choices of inputs. Let **C** be the set of rounds i in which $(x_i, y_i) = (2, 1)$ (rounds in **C** are called key rounds). The users compute the fraction of rounds in $B \cap C$ for which $a_i = b_i$. If it is less than $1 - \eta$ they abort the protocol. Otherwise, they perform information reconciliation on the remaining rounds in **C**, followed by privacy amplification using, e.g., two-universal hashing.

Algorithm 1: Overview of device independent QKD protocol

The protocol presented by Vazirani and Vidick (algorithm 1) is the first major example of a purely classical tester for untrusted quantum devices that is provably robust against noise.

3.2 Quantum Private Query

In Quantum Private Query (QPQ), Bob owns a database and Alice as a client places a query regarding a specific element of that database. The protocols have been designed in such a way so that Bob never knows which element is asked by Alice and Alice can't extract a single element of the database expect her query.

Giovannetti et al.[17] first proposed the idea of QPQ protocol followed by[28] but these are not practically implementable. Jakobi et al.[21] first came out with a practically implementable QPQ proposal. Later on many practically implementable QPQ protocol was proposed. Among those, the protocol proposed by Yang et al.[33] is one of the most popular one.

3.2.1 Yang's Quantum Private Query Protocol:

In this section we revisit the protocol for quantum private query proposed by Yang et. al.[33]. The protocol exploits the idea of B92 quantum key distribution scheme. There are two phases in this protocol, namely, key generation phase and private query phase. The basic idea of the protocol is presented here.

- **Key Generation Phase:**
- Bob and Alice share entangled states of the form $\frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$, where, $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$. Here, subscript B stands for Bob and subscript A stands for Alice. θ may vary from 0 to $\frac{\pi}{2}$.
- After receiving the qubits from Bob, Alice announces the position of the qubits that have ultimately reached at the end of Alice. Bob discards the lost photons.
- After post selection, Bob measures his qubits in $\{|0\rangle_B, |1\rangle_B\}$ basis, whereas Alice measures her qubits either in $\{|\phi_0\rangle_A, |\phi_0^{\perp}\rangle_A\}$ basis or in $\{|\phi_1\rangle_A, |\phi_1^{\perp}\rangle_A\}$ basis randomly.
- If the measurement result of Alice gives $|\phi_0^{\perp}\rangle$, she concludes that the raw key bit at Bob's end must be 1. If it would be $|\phi_1^{\perp}\rangle$, the raw key bit must be 0.
- Bob and Alice execute classical post-processing so that Alice's information on the key reduces to one bit or more. Bob knows the whole key, whereas Alice generally knows several bits of the key.
- **Private Query Phase:**
- If Alice knows the jth bit of the key K and wants to know the ith element of the database, she declares the integer $s = j - i$.

- Bob shifts K by s and hence gets a new key, say K_0. Bob encrypts his database by this new key K_0 with one-time pad and sends the encrypted database to Alice.
- Alice decrypts the value with her jth key bit and gets the required element of the database.

3.2.2 Device Independent QPQ Protocol:

Recently, Maitra et. al.[23] showed that, in Yang's protocol (described in section 3.2.1), if the measurement devices are not trusted and the shared states are not in exact form then Alice can extract extra information equals to $2\epsilon^2 \sin^2\theta$. To resist against this attack, they proposed a device independent approach of Yang's protocol. This is probably the first device independent approach of Quantum Private Query protocol. The overview of their protocol is described in algorithm 2.

1. Bob starts with n number of entangled states.
2. Bob divides the given entangled pairs into two sets. One is Γ_{CHSH} and another is Γ_{QPQ}. The set Γ_{CHSH} contains γn number of entangled states, whereas Γ_{QPQ} contains $(1-\gamma)n$ number of the entangled states for $0 < \gamma < 1$.
3. For rounds $i \in \{1, \cdots, \gamma n\}$

   (a) Bob chooses $x_i \in \{0,1\}$ and $y_i \in \{0,1\}$ uniformly at random.

   (b) If $x_i = 0$, he measures the first particle of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, he measures that in $\{|+\rangle, |-\rangle\}$ basis.

   (c) Similarly, if $y_i = 0$, Bob measures the second particle of the entangled state in $\{|\psi_1\rangle, |\psi_1^\perp\rangle\}$ basis and if $y_i = 1$, he measures that in $\{|\psi_2\rangle, |\psi_2^\perp\rangle\}$ basis.

   (d) The output is recorded as $a_i(b_i) \in \{0,1\}$ for the first (second) particle. The encoding for $a_i(b_i)$ is as follows.

   - For the first particle of each pair, $a_i = 0$ if the measurement result is $|0\rangle$ or $|+\rangle$; it is 1 if the result would be $|1\rangle$ or $|-\rangle$.
   - For the second particle of each pair, $b_i = 0$ if the measurement result is $|\psi_1\rangle$ or $|\psi_2\rangle$; it is 1 if the measurement result would be $|\psi_1^\perp\rangle$ or $|\psi_2^\perp\rangle$, then $b_i = 1$.

   (e) Testing: For the test round $i \in \Gamma_{CHSH}$, define

   $$Y_i = \begin{cases} 1 & \text{if } a_i \oplus b_i = x_i \wedge y_i \\ 0 & \text{if } \textit{otherwise.} \end{cases}$$

4. If $\frac{1}{\gamma n}\sum_i Y_i < \frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$, Bob aborts the protocol.
5. Conditioning on the event that the local CHSH test at Bob's end has been successful, Bob proceeds for the subset Γ_{QPQ} and sends one halves of the remaining $(1-\gamma)n$ number of entangled pairs to Alice.
6. Alice performs the private query phase as described in Yang's protocol (described in section 3.2.1).

Algorithm 2: Overview of Device Independent QPQ Protocol

3.3 Quantum Bit Commitment

Bit commitment is a protocol between two mistrusting parties, Alice and Bob, which is supposed to provide the following functionality: In a commit phase, Alice gives as input a value(i.e, a bit) and Bob gets a confirmation that Alice has committed to a value (without learning the actual value). Later, in an opening reveal phase, Alice can decide to reveal the value to Bob.

Bennett and Brassard[6] proposed first quantum bit commitment protocol in their famous BB84 paper (actually, the protocol they describe is only claimed to implement coin tossing, but it is obvious how to modify it in order to implement bit commitment). Later on, many quantum bit commitment protocols were proposed till now. Although the protocol proposed in BB84 paper has some flaws, most of the protocols proposed after that are based on this concept.

3.3.1 Quantum Bit Commitment Protocol:

The simplified bit commitment protocol proposed in BB84 paper[6] is described here.

- **Commit Phase:**
- Alice decides to send either b_0 or b_1 to Bob, where b_i is a classical bit.
- Alice encodes her classical bit in either the $|0\rangle, |1\rangle$ basis or $|+\rangle, |-\rangle$ basis. For b_0, she transmits one qubit from the first basis. For b_1, she sends one qubit from the second basis.
- **Reveal Phase:**
- Alice reveals her commitment to Bob via a classical channel. She sends a classical string 00 to indicate $|0\rangle$, 01 to indicate $|1\rangle$, 10 to indicate $|+\rangle$, and 11 to indicate $|-\rangle$. The first bit represents the bit Alice has committed. The second bit represents the basis element, corresponding to the qubit she has sent.
- Bob measures his qubit in a basis that corresponds to the classical communication he has received.
- If his measurements agree with what Alice revealed to him, the commitment is successful. Otherwise, Bob catches a lying Alice.

3.3.2 Device Independent Quantum Bit Commitment:

Most of the bit commitment protocols proposed till now does not involve the sharing of an entangled state between two distrustful parties as a part of the protocol. Silman et.

al.[30] first proposed a bit commitment protocol which involves the sharing of a three qubit entangled state (GHZ state) between two parties. Later on Adlam et. al.[1] and Aharon et. al.[2] also proposed device independent bit commitment protocols which involve sharing of two qubit entangled states.

Though the later two protocols are recent ones, the protocol proposed by Silman et. al.[30] has the curious property that its device dependent version is essentially device independent, in the sense that its security is not compromised in the event that an honest party cannot trust its measurement devices. We describe the overview of their proposed protocol in algorithm 3.

The protocol is based on GHZ paradox which involves three boxes with binary inputs s_A, s_B and s_C, and outputs r_A, r_B and r_C respectively. The **GHZ paradox** consists of the fact that if the inputs satisfy $s_A \oplus s_B \oplus s_C = 1$, we can always have the outputs satisfy $r_A \oplus r_B \oplus r_C = s_A s_B s_C \oplus 1$.

Alice has a box, A, and Bob has a pair of boxes, B and C. The three boxes are supposed to satisfy the GHZ paradox.

- **Commit Phase:**
- Alice inputs into her box the value of the bit she wishes to commit to. Denote the input and output of her box by s_A and r_A.
- She then selects a classical bit a uniformly at random. If $a = 0 (a = 1)$, she sends Bob a classical bit $c = r_A (c = r_A \oplus s_A)$ as her commitment.
- **Reveal Phase:**
- Alice sends Bob s_A and r_A.
- Bob first checks whether $c = r_A$ or $c = r_A \oplus s_A$. He then randomly chooses a pair of inputs s_B and s_C, satisfying $s_B \oplus s_C = 1 \oplus s_A$, inputs them into his two boxes and checks whether the GHZ paradox is satisfied.
- If any of these tests fails then he aborts.

Algorithm 3: Overview of device independent Bit Commitment protocol

Note that if the parties are honest here(and the boxes satisfy the GHZ paradox), then the protocol never aborts.

Chapter 4

Proposed Scheme For Finite Sample Device Independent Protocols

In previous chapter, we have discussed about several quantum cryptographic protocols and their device independent approach. In all device independent protocols described in previous chapter(except the device independent bit commitment protocol where the device dependent protocol is indeed device independent), the basic idea is to perform CHSH test (local or non local) to certify the given state.

However, the existing device independent protocols work perfectly for the asymptotic case when we have infinite number of qubits but these are not practically implementable. In this chapter, we describe modified device independent protocols for finite number of qubits and connect the sample size to the success probability of CHSH test. We also perform a rigorous security analysis for each of the proposed protocols.

4.1 Expected estimation of sample size

We recall the Chernoff-Hoeffding[20] bound here.

Proposition 1. *Let* $X = \frac{1}{m}\sum_i X_i$ *be the average of* m *independent random variables* $X_1, X_2, \cdots, X_m$ *with values* $[0,1]$*, and let* $\mathbb{E}[X] = \frac{1}{m}\sum_i \mathbb{E}[X_i]$ *be the expected value of* X*, then for any* $\delta > 0$*, we have* $\Pr\left[|X - \mathbb{E}[X]| \geq \delta\right] \leq \exp(-2\delta^2 m)$.

In our case, if the i-th run of the CHSH test succeeds, we set $X_i = 1$; otherwise $X_i = 0$. Note that $\mathbb{E}[X] = \mathbb{E}[X_i] = p$ (say), the expected success probability of the CHSH test. The variable X denotes the actual success probability p'.

Now the question is how large should "the number of samples" be so that we get a good "accuracy" of the given state with high "confidence"? More precisely, suppose we want to estimate the success probability p within an error margin of ϵp and confidence $1-\gamma$, meaning,

$$\Pr[|p' - p| \leq \epsilon p] \geq 1 - \gamma, \tag{4.1}$$

where p' and p are the estimated and the expected values respectively. Comparing Equation (4.1) with Proposition 1, we want, for given ϵ, p and γ,

$$\exp(-2\epsilon^2 p^2 m) \leq \gamma, \qquad \text{i.e., } m \geq \tfrac{1}{2\epsilon^2 p^2} \ln \tfrac{1}{\gamma}.$$

This implies that as the value of the success probability increases, the required sample size decreases. Denoting the maximum success probability for a specific θ by p_{max}, we can write,

$$m_{opt} = \frac{1}{2\epsilon^2 p_{max}^2} \ln \frac{1}{\gamma} \tag{4.2}$$

This m_{opt} gives the optimal value of the sample size required to certify a given state where the value of θ corresponding to this state is already known.

4.2 Generalization towards device independent protocols for finite samples

Since the core of any device independent protocol is to test whether the entangled states shared between the parties are of specific form or not, we can extend the analysis for all device independent protocols.

Without loss of generality, let the generalized form of the state shared in different protocols is

$$\sqrt{q}|0\rangle|\phi_0\rangle + \sqrt{1-q}|1\rangle|\phi_1\rangle$$

where $|\phi_0\rangle = \cos\theta_1|0\rangle + \sin\theta_1|1\rangle$ and $|\phi_1\rangle = \cos\theta_2|0\rangle - \sin\theta_2|1\rangle$.

So the state can be written as,

$$\sqrt{q}(\cos\theta_1|00\rangle + \sin\theta_1|01\rangle) + \sqrt{1-q}(\cos\theta_2|10\rangle - \sin\theta_2|11\rangle). \tag{4.3}$$

Let $\{|\psi_1\rangle, |\psi_2\rangle\}$ be the generalized form of a measurement basis, where

$$|\psi_1\rangle = \cos\psi_1|0\rangle + \sin\psi_1|1\rangle, \qquad |\psi_1^{\perp}\rangle = \sin\psi_1|0\rangle - \cos\psi_1|1\rangle,$$

$$|\psi_2\rangle = \cos\psi_2|0\rangle + \sin\psi_2|1\rangle, \qquad |\psi_2^{\perp}\rangle = \sin\psi_2|0\rangle - \cos\psi_2|1\rangle.$$

4.2.1 Generalized View of CHSH Game

As in all the device independent protocol, the idea of the CHSH game[12] to test the measurement device is same, we can view this in a generalized form which can be applicable for all the device independent protocols.

In CHSH game there are two players having two black boxes and one referee. Each boxes can take one input bit and provides one output bit. The referee supplies the inputs $x_i \in \{0, 1\}$ to Alice and $y_i \in \{0, 1\}$ to Bob for each round $i \in \{1, \cdots, n\}$.

At the beginning of the game, Alice and Bob share n number of entangled pairs between themselves. For $i \in \{1, \cdots, n\}$, if $x_i = 0$, Alice measures her qubit in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, it is measured in $\{|+\rangle, |-\rangle\}$ i.e., in Hadamard basis. Similarly, if $y_i = 0$, Bob measures his part in $\{|\psi_1\rangle, |\psi_1^{\perp}\rangle\}$ basis and if $y_i = 1$, it is measured in $\{|\psi_2\rangle, |\psi_2^{\perp}\rangle\}$ basis. The outputs are recorded as a bit a_i (for Alice) and b_i (for Bob). The encoding for $a_i(b_i)$ is as follows.

- For Alice's particle, if the measurement result would be $|0\rangle$ or $|+\rangle$, then $a_i = 0$.
- If the measurement result would be $|1\rangle$ or $|-\rangle$, then $a_i = 1$.
- For Bob's particle, if the measurement result would be $|\psi_1\rangle$ or $|\psi_2\rangle$, then $b_i = 0$.
- If the measurement result would be $|\psi_1^{\perp}\rangle$ or $|\psi_2^{\perp}\rangle$, then $b_i = 1$.

The players win in the round $i \in \{1, \cdots, n\}$ if the CHSH condition $a_i \oplus b_i = x_i \wedge y_i$ holds. The game is described in more formalized form in Algorithm 4.

According to this generalized view of CHSH game, the overall success probability (p) of the generalized shared state (as given in equation (4.3)) when all the four inputs are equally likely will be,

$$\begin{aligned} p &= \frac{1}{4} + \frac{q}{4}\left(\cos^2(\theta_1 - \psi_1) + \cos^2(\theta_1 - \psi_2)\right) \\ &\quad + \frac{(1-q)}{4}\left(\sin^2(\theta_2 + \psi_1) + \sin^2(\theta_2 + \psi_2)\right) \\ &\quad + \frac{\sqrt{q(1-q)}}{4}\left(\cos(\theta_1 - \theta_2 - 2\psi_1) - \cos(\theta_1 - \theta_2 - 2\psi_2)\right). \end{aligned} \tag{4.4}$$

Now for device independent setting, we have to perform CHSH test to check the given state. But when we want to perform the CHSH test for finitely many samples, we have to

1. Alice and Bob each possesses one black box which can take one input bit and provides one output bit.
2. Referee R supplies the inputs x_i to Alice and y_i to Bob for $i \in \{0, \cdots, n\}$.
3. At the beginning of the game Alice and Bob share n number of entangled states between themselves.
4. For round $i \in \{1, \cdots, n\}$
    - If $x_i = 0$, Alice measures her particle in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, she measures that in $\{|+\rangle, |-\rangle\}$ basis.
    - Similarly, if $y_i = 0$, Bob measures his particle in $\{|\psi_1\rangle, |\psi_1^\perp\rangle\}$ basis and if $y_i = 1$, he measures that in $\{|\psi_2\rangle, |\psi_2^\perp\rangle\}$ basis.
    - The output is recorded as $a_i(b_i) \in \{0, 1\}$ for the Alice's (Bob's) particle.
5. For the round $i \in \{0, \cdots, n\}$, if $a_i \oplus b_i = x_i \wedge y_i$, Alice and Bob win the game, otherwise they fail.

Algorithm 4: Generalized CHSH game for device independent protocols

allow some deviation from the actual success probability. Let p_{max} be the maximum value of p in equation (4.4).

From Chernoff-Hoeffding bound, we get that if the optimal sample size to test a given state with certain accuracy and confidence is m_{opt} then

$$m_{opt} = \frac{1}{2\epsilon^2 p_{max}^2} \ln \frac{1}{\gamma}$$

where ϵ and γ are respective accuracy and confidence parameter and p_{max} is the corresponding maximum success probability.

So, for the states of the above general form, we will check for m_{opt} number of samples whether the success probability of CHSH game for this specified number of samples lies within the interval,

$$[p_{max} - \epsilon p_{max},\ p_{max} + \epsilon p_{max}]$$

If the value lies within the specified range then we will proceed the protocol, otherwise we will abort the protocol.

Next, we discuss how this general calculation can be applied to specific protocols.

4.3 Modification of DI-QKD Towards Finite Number of Entangled States

In case of QKD[32], the shared state between two parties is of the form

$$|\psi_{QKD}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

which is a special form of the above mentioned general state (equation (4.3)) when $\theta_1 = 0$, $\theta_2 = \frac{3\pi}{2}$, $q = \frac{1}{2}$. From the equation of the estimated sample size (equation (4.2)), we can see that as the success probability increases, the required sample size decreases.

For this state which is of the form $|\psi_{QKD}\rangle$, the success probability will be maximum for $\psi_1 = \frac{\pi}{8}$ and $\psi_2 = -\frac{\pi}{8}$.

Now, by putting this specific values into the above generalized success probability expression (equation (4.4)), we get the success probability of this state for CHSH game which is,

$$p_{QKD} = (\frac{1}{2} + \frac{1}{2\sqrt{2}}) = \cos^2 \frac{\pi}{8} \approx 0.85$$

This success probability is maximum for this specific state and also for two qubit entangled states in CHSH game.

By putting the value p_{QKD} in equation (4.2), we can get the optimal sample size m_{QKD} required for a specific accuracy and confidence. So, for m_{QKD} number of states of the form $|\psi_{QKD}\rangle$, the success probability will never exceed the value p_{QKD} as this is the maximum success probability for two qubit entangled states in CHSH game.

So we will check here whether the success probability value of CHSH test for this many samples lies within the range $[p_{QKD} - \epsilon p_{QKD}\ ,\ p_{QKD}]$ or not. If this success probability value lies within this range then we will proceed the protocol, otherwise we will abort the protocol.

So, from the above condition, it is clear that we have to allow ϵp_{QKD} amount of deviation from the original success probability value p_{QKD}. Now if this deviation is very large (i.e, the value of ϵ is very large), then it may create security loop-hole for eavesdropper. So, we have to give a proper bound on the value of ϵ so that eavesdropper can't earn anything from this deviation.

4.3.1 Security bounds against additional information leakage and lower key rate

Here we will propose a bound on the value of ϵ so that exploiting this deviation, eavesdropper can not extract significant amount of information about the key shared between Bob and herself.

In our modified version of the local CHSH test, we suggest that if the maximum success probability of the given state lies within the specified interval then Bob accepts the state and proceeds the protocol otherwise Bob aborts the protocol.

It may happen that for some other state (for example, $(\alpha|00\rangle + \beta|11\rangle$, where $|\alpha|^2 = (\frac{1}{2} + \epsilon_E)$ and $|\beta|^2 = (\frac{1}{2} - \epsilon_E))$ the success probability value lies within the specified interval. Now to cheat the parties involved in QKD protocol, eavesdropper may supplies a state of the above form. In this case, the CHSH correlation value will be $(1 + \sqrt{1 - 4\epsilon_E^2})(\sqrt{\frac{1}{2} + \epsilon_E} + \sqrt{\frac{1}{2} - \epsilon_E})$ instead of the maximum correlation value $2\sqrt{2}$[11], which can be achieved for states of the form $|\psi_{QKD}\rangle$. The relation between CHSH correlation value and ϵ_E is shown in figure 4.1.

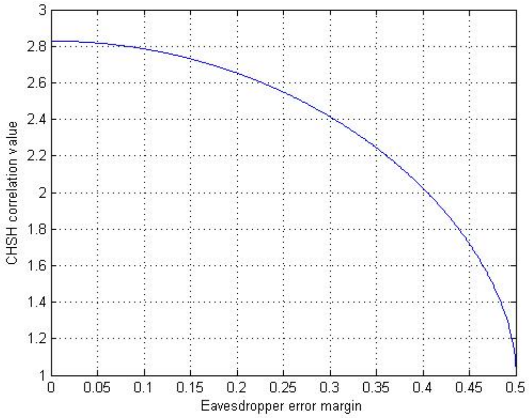

Figure 4.1: Plot of CHSH correlation value as a function of eavesdropper's deviation value ϵ_E

From the relation between eavesdropper's information and CHSH correlation value[18], we can see that $I_E(S) \leq h(\frac{1+\sqrt{(\frac{s}{2})^2-1}}{2})$ where $I_E(S)$ is the information leaked to the eavesdropper and $h(x) = -x\log(x) - (1-x)\log(1-x)$ is binary entropy. Achievable key rate ‘k' between communicating parties in QKD after error correction and privacy amplification is given by, $k \geq 1 - h(Q) - I_E(S)$[18]. From the above relations it can be concluded that as the value of ϵ_E increases for the given state, the difference between actual CHSH correlation value and maximum CHSH correlation value(i.e, $2\sqrt{2}$) will increase until CHSH correlation value 2 which is the maximum value that can be achieved classically. Now this increasing difference between actual and maximum CHSH correlation value will increase the information leakage to eavesdropper and decrease the achievable key rate.

To close such type of security loop-hole (which arises due to the finite sample size) we bound the value of ϵ_E so that the additional information which is leaked to Alice should be infinitesimally small.

Let, in spite of the claimed state, Bob is provided the states of the form $(\alpha|00\rangle + \beta|11\rangle)$. Rigorous calculations show that the success probability for these states merges to $\frac{1}{2}+\frac{1}{4\sqrt{2}}(1+\sqrt{1-4\epsilon^2})$ where $0 \leq \epsilon \leq \frac{1}{2}$. We denote this success probability value by p'. Now for the given state to be successfully verified, this success probability value (p') must lie within the interval $[p_{QKD} - \epsilon p_{QKD}, p_{QKD} + \epsilon p_{QKD}]$, where p_{QKD} is the maximum success probability of the original claimed state and ϵ is the accuracy parameter chosen by the communicating parties.

So, p' must satisfy

$$p_{QKD} - \epsilon p_{QKD} \leq p' \leq p_{QKD} + \epsilon p_{QKD}$$

Now from the left and right inequalities, we get $\epsilon_E^2 \geq -\epsilon(\sqrt{2}+1)$ and $\epsilon_E^2 \leq \epsilon(\sqrt{2}+1)$ respectively. Since negative ϵ_E is not meaningful, we have the solution as

$$\epsilon_E \leq \sqrt{\epsilon(\sqrt{2}+1)}. \tag{4.5}$$

So, to deceive communicating parties, the states are prepared in such a way such that the value of ϵ_E must satisfy the condition $\epsilon_E \leq \sqrt{\epsilon(\sqrt{2}+1)}$. Otherwise, with a high probability the success probability of the given state will not lie within the specified interval and communicating parties will abort the protocol.

So, we can write $\epsilon_E \leq \sqrt{k\epsilon}$, where $k = (\sqrt{2}+1)$ is a constant. In this case, eavesdropper will get the additional information which equals to $I_E(S) \leq h(\frac{1+\sqrt{(\frac{s}{2})^2-1}}{2})$[18] where s is the CHSH correlation value for the given state. Thus, the information leaked to eavesdropper remains in order of ϵ. If we choose the value of ϵ sufficiently small, say 10^{-10}, then we can bound the leakage in the order of 10^{-10}.

4.3.2 Modified DI-QKD protocol with finite samples and Security Analysis

Now, we are in the state to propose our modified protocol for finite sample size. Any one of the communicating parties first calculates the value of the success probability for the claimed state. Then from the calculated success probability p_{QKD}, the party calculates the required optimal sample size m_{QKD} for the CHSH test to certify the states with certain accuracy and confidence. Communicating parties start with $n = 2m_{QKD}$ number of entangled states (see Section 4.3.3 for explanation). Let Γ_{CHSH} denote the set which contains the states for CHSH test, where $|\Gamma_{CHSH}| = m_{QKD}$ and Γ_{QKD} denote the set which contains the remaining states, i.e., $|\Gamma_{QKD}| = n - m_{QKD} = m_{QKD}$. Communicating parties choose the states for each of Γ_{CHSH} and Γ_{QKD} uniformly at random from the given set of n states. Our modified protocol has been described in algorithm 5.

1. For rounds $i \in \{1, \cdots, |\Gamma_{CHSH}|\}$

   (a) Alice chooses input $x_i \in \{0, 1\}$ and Bob chooses input $y_i \in \{0, 1\}$ uniformly at random.

   (b) If $x_i = 0$, Alice measures the first qubit of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, she measures that in $\{|+\rangle, |-\rangle\}$ basis.

   (c) Similarly, if $y_i = 0$, Bob performs a rotation by $\frac{\pi}{8}$ on his qubit and measure in $\{|0\rangle, |1\rangle\}$ basis and if $y_i = 1$, Bob performs a rotation by $-\frac{\pi}{8}$ on his qubit and measure in $\{|0\rangle, |1\rangle\}$ basis.
   (d) The output is recorded as $a_i(b_i) \in \{0, 1\}$ for the first and second particle respectively. The encoding for $a_i(b_i)$ is performed as follows.

   - For the first qubit of each pair, if the measurement result is $|0\rangle$ or $|+\rangle$ then $a_i = 0$; if the result is $|1\rangle$ or $|-\rangle$ then it would be 1.
   - For the second qubit of each pair, if the measurement result is $|1\rangle$ or $|-\rangle$ then $a_i = 0$; if the result is $|0\rangle$ or $|+\rangle$ then it would be 1.

   (e) Testing: For the test round $i \in \Gamma_{CHSH}$, define

$$Y_i = \begin{cases} 1 & \text{if } a_i \oplus b_i = x_i \wedge y_i \\ 0 & \text{if } \textit{otherwise}. \end{cases}$$

2. If the value of $\frac{1}{|\Gamma_{CHSH}|} \sum_i Y_i$ lies within the range $[p_{QKD} - \epsilon p_{QKD}, p_{QKD}]$, where p_{QKD} equals $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ and ϵ is the accuracy parameter chosen by the communicating parties, they proceed the protocol otherwise they abort the protocol.

3. When the CHSH test is successful, communicating parties proceed for the subset Γ_{QKD}.

4. Alice and Bob perform the key distribution phase as described in [6].

Algorithm 5: Modified DI-QKD protocol for finite sample

Explicitly, here, we assume i) the inherent correctness of the quantum mechanics, ii) no information leakage from the legitimate parties' laboratories, iii) devices are memoryless i.e., each use of the devices is independent and iv) the detectors have unit efficiencies.

4.3.3 Security Analysis of the Modified Protocol

The security analysis of the modified protocol follows from the following result.

Theorem 1. *If for a subset Γ_{CHSH} of size m, the fraction of the inputs (x_i, y_i), $i \in \Gamma_{CHSH}$, which satisfy the CHSH condition i.e., $(a_i \oplus b_i = x_i \wedge y_i)$ is equal to $\frac{1}{2} + \frac{1}{2\sqrt{2}} - \delta$, then for the remaining subset Γ_{QKD} of size $n - m$, a fraction of inputs (x_i, y_i), $i \in \Gamma_{QKD}$, which satisfy the CHSH condition, is also equal to $\frac{1}{2} + \frac{1}{2\sqrt{2}} - \delta$ with a statistical deviation ν.*

Here, $\delta = \sqrt{\frac{1}{2m} \ln \frac{1}{\epsilon_{CHSH}}}$ and $\nu = \sqrt{\frac{(m+1)}{2(1-\frac{m}{n})m^2} \ln \frac{1}{\epsilon_{QKD}}}$, ϵ_{CHSH} and ϵ_{QKD} are negligibly small value.

Essentially, the result means that if the success probability of the local CHSH game for the set Γ_{CHSH} varies in the range $[p_{QKD} - \epsilon p_{QKD}, p_{QKD}]$, where p_{QKD} equals $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ and ϵ is the accuracy parameter, then the success probability of the game for the set Γ_{QKD} would vary in the range $[p_{QKD} - \epsilon p_{QKD} - \nu, p_{QKD}]$.

Note that in Theorem 1, if n is close to m, then ν is no longer guaranteed to be negligible. On the other hand, the choice $n \geq 2m$ makes the coefficient of $\frac{(m+1)}{m^2} \ln \frac{1}{\epsilon_{QKD}}$ less than 1 and thus is practically a good choice.

So far, the entire security analysis, including that of QKD[6] and DI-QKD[32], is performed under the assumption that the states provided by Alice are all identical. Indeed, when n is infinitely large, eavesdropper cannot have any advantage in non-uniformly biasing the states, as Alice and Bob selects the subset Γ_{CHSH} uniformly randomly. However, when $n \gg 2m$, but finite, then eavesdropper could inject more bias in the choice of her basis than the threshold $\sqrt{\epsilon(\sqrt{2}+1)}$ (from equation (4.5)) for a few states and no bias for the remaining states and still she could pass the CHSH test by Alice and Bob. More formally, if eavesdropper injects a bias ϵ'_E in r out of n states uniformly at random, then it can be easily shown that to pass the CHSH test, the following condition is required.

$$\epsilon'_E \leq \sqrt{\frac{n}{r}\epsilon(\sqrt{2}+1)}. \tag{4.6}$$

Thus, by choosing $r \ll n$, eavesdropper can lift the threshold of ϵ'_E much higher than that of ϵ_E and can also retrieve more information and reduce key rate if the corresponding states are selected for QKD.

To resist this attack, Alice and Bob have to choose the minimum possible n, i.e., $n =$

$2m_{QKD}$. Since communicating parties will take $m = m_{QKD}$ as per our analysis, we have $n = 2m_{QKD}$.

One may think that the restriction on n would limit Alice and Bob to set a secret key of large length between them. Although the length of the secret key is usually small, if they wish to set a large secret key between them then this can be easily taken care of by allowing Alice and Bob to play the game repeatedly, and finally combine all the keys generate from different rounds and set a large secret key.

4.4 Modification of DI-QPQ Towards Finite Number of Entangled States

In case of QPQ[33], the shared state between two party is of the form

$$|\psi_{QPQ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$$

where $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$, which is a special form of the above mentioned general state(equation (4.3)) when $\theta_1 = \frac{\theta}{2}$, $\theta_2 = \frac{\theta}{2}$, $q = \frac{1}{2}$. From the equation of the estimated sample size, we can see that as the success probability increases, the required sample size decreases. So, we have to find maximum success probability corresponding to a particular θ to reduce the sample size.

4.4.1 Maximization of success probability

In DI-QPQ protocol[23], Bob and Alice share entangled states of the form $\frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$, where $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$. The value of θ is known to all. Bob chooses two measurement bases namely $\{|\psi_1\rangle, |\psi_1^{\perp}\rangle\}$ and $\{|\psi_2\rangle, |\psi_2^{\perp}\rangle\}$, to play the local CHSH game. Here, $|\psi_1\rangle = \cos\frac{\psi_1}{2}|0\rangle + \sin\frac{\psi_1}{2}|1\rangle$ and $|\psi_2\rangle = \cos\frac{\psi_2}{2}|0\rangle + \sin\frac{\psi_2}{2}|1\rangle$. Now, for a particular value of the angles ψ_1, ψ_2 and θ, only Bob can calculate the success probability value of the local CHSH game, hence, preventing Alice to manipulate the states and the measurement devices. Here we propose a modification of the scheme proposed by Maitra et. al.[23].

In the DI-QPQ protocol[23], Bob gets the success probability in terms of θ, ψ_1 and ψ_2 which is equal to $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$. To maximize the quantity, we have to maximize $\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2$.

Now, we can write,

$$\begin{aligned} & \sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2 \\ = \; & \sin\theta\sin\psi_1 + \sin\theta\sin\psi_2 + \cos\psi_1 - \cos\psi_2 \\ = \; & (\sin\theta\sin\psi_1 + \cos\psi_1) + (\sin\theta\sin\psi_2 - \cos\psi_2) \end{aligned}$$

Setting $\sin\theta = r\cos\phi$ and $1 = r\sin\phi$, we get

$$\begin{aligned} & (r\cos\phi\sin\psi_1 + r\sin\phi\cos\psi_1) \\ & +(r\cos\phi\sin\psi_2 - r\sin\phi\cos\psi_2) \\ = \; & r(\sin(\psi_1 + \phi) + \sin(\psi_2 - \phi)), \end{aligned}$$

where $r^2 = 1 + \sin^2\theta$, $r\cos\phi = \sin\theta$ and $r\sin\phi = 1$. Thus we get, $\tan\phi = \text{cosec }\theta$ i.e, $\phi = \tan^{-1}(\text{cosec }\theta\ )$.

Again, the value $r(\sin(\psi_1+\phi)+\sin(\psi_2-\phi))$ will be maximum when both $\sin(\psi_1+\phi) = 1$ and $\sin(\psi_2-\phi) = 1$ i.e, when $(\psi_1+\phi) = \frac{\pi}{2}$ and $(\psi_2-\phi) = \frac{\pi}{2}$. From that we get, $\psi_1 = (\frac{\pi}{2}-\phi)$ and $\psi_2 = (\frac{\pi}{2}+\phi)$.

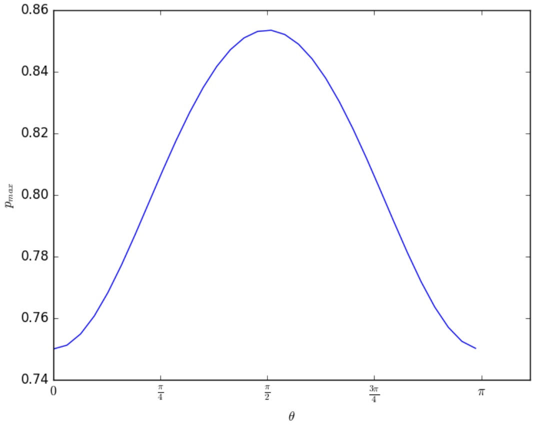

Figure 4.2: Plot of p_{QPQ} as a function of θ

As we know the value of θ, we can easily calculate the value of ψ_1 and ψ_2 from the above equations and play the local CHSH game for these ψ_1 and ψ_2. For these values of ψ_1 and ψ_2, the success probability value corresponding to that θ will be maximum. Figure 4.2 shows how p_{QPQ} varies as θ varies between 0 to π, taking the maximum value of $cos^2\pi/8$ at $\theta = \pi/2$.

By putting the value p_{QPQ} in equation (4.2), we can get the optimal sample size m_{QPQ} required for a specific accuracy and confidence. So, for m_{QPQ} number of states of the form $|\psi_{QPQ}\rangle$, we will check whether the success probability value of CHSH test for this many samples lies within the range $[p_{QPQ} - \epsilon p_{QPQ}\ ,\ p_{QPQ} + \epsilon p_{QPQ}]$ or not. If this success probability value lies within this range then we will proceed the protocol, otherwise we will abort the protocol.

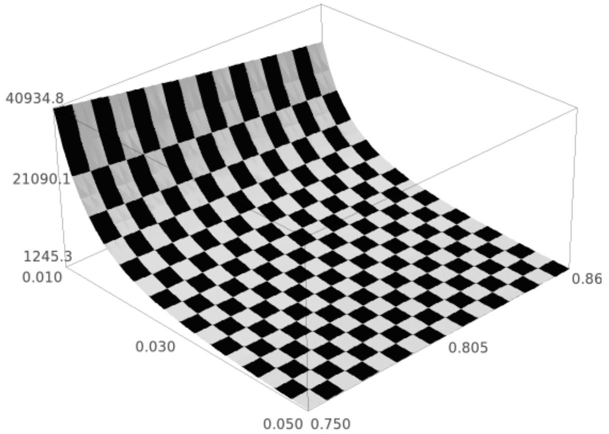

Figure 4.3: Plot of m_{QPQ} (vertical axis) as a function of ϵ (left) and p_{QPQ} (right) with $\gamma = 0.01$

Figure 4.3 shows how m_{QPQ} varies with ϵ and p_{QPQ}, when we fix the confidence at 99%. As expected, we see that as we decrease the values of ϵ or p_{QPQ}, the value of m_{QPQ} increases.

So, from the above condition, it is clear that we have to allow ϵp_{QPQ} amount of deviation from the original success probability value p_{QPQ}. Now if this deviation is very large (i.e, the value of ϵ is very large), then it may create security loop-hole for eavesdropper. So, we have to give a proper bound on the value of ϵ so that eavesdropper can't earn anything from this deviation.

4.4.2 Security bounds against additional information leakage

Now, we will propose a bound on the value of ϵ so that exploiting this deviation, Alice can not extract significant amount of information about the key shared between Bob and herself.

In our modified version of the local CHSH test, we suggest that if the maximum success probability of the given state lies within the specified interval then Bob accepts the state and proceeds the protocol otherwise Bob aborts the protocol.

It may happen that for some other state (for example, $(\alpha|0\rangle_B|\phi_0\rangle_A+\beta|1\rangle_B|\phi_1\rangle_A)$, where $|\alpha|^2 = (\frac{1}{2}+\epsilon_A)$ and $|\beta|^2 = (\frac{1}{2}-\epsilon_A)$) the success probability value lies within this interval. Now to cheat Bob, Alice may supplies a state of the above form. In this case, if Alice chooses the basis $\{|\phi_0\rangle_A, |\phi_0^{\perp}\rangle_A\}$ with probability $\frac{1}{2}-\epsilon_A$ and $\{|\phi_1\rangle_A, |\phi_1^{\perp}\rangle_A\}$ with probability $\frac{1}{2}+\epsilon_A$, she can extract $(\frac{1}{2}+2\epsilon_A^2)\sin^2\theta$ fraction of entire key stream[23] which is prohibited by the protocol.

To close such type of security loop-hole (which arises due to the finite sample size) we bound the value of ϵ_A so that the additional information which is leaked to Alice should be infinitesimally small.

Let, in spite of the claimed state, Bob is provided the states of the form $(\alpha|0\rangle_B|\phi_0\rangle_A + \beta|1\rangle_B|\phi_1\rangle_A)$. Rigorous calculations show that the success probability for these states merges to $\frac{1}{2}+\frac{1}{8}\sin\theta(\sin\psi_1+\sin\psi_2)+\frac{1}{4}\sqrt{\frac{1}{4}-\epsilon_A^2}(\cos\psi_1-\cos\psi_2)+\frac{1}{4}\epsilon_A\cos\theta(\cos\psi_1+\cos\psi_2)$. We denote this success probability value by p''. Now for the given state to be successfully verified, this success probability value (p'') must lie within the interval $[p_{QPQ}-\epsilon p_{QPQ}, p_{QPQ}+\epsilon p_{QPQ}]$, where p_{QPQ} is the maximum success probability of the original claimed state for a given θ and ϵ is the accuracy parameter chosen by Bob.

So, p'' must satisfy

$$p_{QPQ} - \epsilon p_{QPQ} \leq p'' \leq p_{QPQ} + \epsilon p_{QPQ}.$$

Now from the left and right inequalities, we get $\epsilon_A^2 \geq -\frac{2\epsilon p_{QPQ}}{\cos\psi_1}$ and $\epsilon_A^2 \leq \frac{2\epsilon p_{QPQ}}{\cos\psi_1}$ respectively. Since negative ϵ_A is not meaningful, we have the solution as

$$\epsilon_A \leq \sqrt{\frac{2\epsilon p_{QPQ}}{\cos\psi_1}}. \tag{4.7}$$

Here, we consider only the situation when $\psi_1 \in [0, \frac{\pi}{2})$. This is because from the previous calculation we get that the value of ψ_1 always lies within $[0, \frac{\pi}{2})$ whenever $\theta \in [0, \frac{\pi}{2}]$.

So, to deceive Bob the states are prepared in such a way such that the value of ϵ_A must satisfy the condition $\epsilon_A \leq \sqrt{\frac{2\epsilon p_{QPQ}}{\cos\psi_1}}$. Otherwise, with a high probability the success probability of the given state will not lie within the specified interval and Bob will abort the protocol.

From the earlier section we get that for a given θ, the values of p_{QPQ}, ψ_1 and ψ_2 are fixed. So, we can write $\epsilon_A \leq k\sqrt{\epsilon}$, where $k = \sqrt{\frac{2p_{QPQ}}{cos\psi_1}}$ is a constant for a given θ. In this case, Alice will get the additional information which equals to $\epsilon_A^2\sin^2\theta$[23]. Thus, the information leaked to Alice remains in order of ϵ. If we choose the value of ϵ sufficiently small, say 10^{-10}, then we can bound the leakage in the order of 10^{-10}.

4.4.3 Modified DI-QPQ protocol with finite samples and Security Analysis

Now, we are in the state to propose our modified protocol for finite sample size. Bob first calculates the value of ψ_1 and ψ_2 for which the claimed state attains the maximum success probability. Then from the calculated maximum success probability p_{QPQ}, Bob calculates the required optimal sample size m_{QPQ} for the local CHSH test to certify the states with certain accuracy and confidence. Bob starts with $n = 2m_{QPQ}$ number of entangled states (see Section 4.4.4 for explanation). Let Γ_{CHSH} denote the set which contains the states for local CHSH test, where $|\Gamma_{CHSH}| = m_{QPQ}$ and Γ_{QPQ} denote the set which contains the remaining states, i.e., $|\Gamma_{QPQ}| = n - m_{QPQ} = m_{QPQ}$. Bob chooses the states for each of Γ_{CHSH} and Γ_{QPQ} uniformly at random from the given set of n states. Our modified protocol has been described in algorithm 6.

Explicitly, here, we assume i) the inherent correctness of the quantum mechanics, ii) no information leakage from the legitimate parties' laboratories, iii) devices are memoryless i.e., each use of the devices is independent and iv) the detectors have unit efficiencies.

1. For rounds $i \in \{1, \cdots, |\Gamma_{CHSH}|\}$

   (a) Bob chooses input $x_i \in \{0,1\}$ and $y_i \in \{0,1\}$ uniformly at random.

   (b) If $x_i = 0$, he measures the first qubit of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, he measures that in $\{|+\rangle, |-\rangle\}$ basis.

   (c) Similarly, if $y_i = 0$, Bob measures the second qubit of the entangled state in $\{|\psi_1\rangle, |\psi_1^{\perp}\rangle\}$ basis and if $y_i = 1$, he measures that in $\{|\psi_2\rangle, |\psi_2^{\perp}\rangle\}$ basis, where the values of ψ_1 and ψ_2 have been calculated previously.
   (d) The output is recorded as $a_i(b_i) \in \{0,1\}$ for the first and second particle respectively. The encoding for $a_i(b_i)$ is performed as follows.

   - For the first qubit of each pair, if the measurement result is $|0\rangle$ or $|+\rangle$ then $a_i = 0$; if the result is $|1\rangle$ or $|-\rangle$ then it would be 1.
   - For the second qubit of each pair, if the measurement result is $|\psi_1\rangle$ or $|\psi_2\rangle$ then $b_i = 0$; and if the measurement result is $|\psi_1^{\perp}\rangle$ or $|\psi_2^{\perp}\rangle$, then $b_i = 1$.

   (e) Testing: For the test round $i \in \Gamma_{CHSH}$, define

$$Y_i = \begin{cases} 1 & \text{if } a_i \oplus b_i = x_i \wedge y_i \\ 0 & \text{if } \textit{otherwise}. \end{cases}$$

2. If the value of $\frac{1}{|\Gamma_{CHSH}|}\sum_i Y_i$ lies within the range $[p_{QPQ_{max}} - \epsilon p_{QPQ_{max}}, p_{QPQ_{max}} + \epsilon p_{QPQ_{max}}]$, where $p_{QPQ_{max}}$ equals $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$ and ϵ is the accuracy parameter chosen by Bob, Bob proceeds the protocol otherwise Bob aborts the protocol.

3. When the local CHSH test at Bob's end is successful, Bob proceeds for the subset Γ_{QPQ} and sends one halves of the remaining entangled pairs to Alice.

4. Alice performs the private query phase as described in [33].

Algorithm 6: Modified DI-QPQ protocol for finite sample

4.4.4 Security Analysis of the Modified Protocol

The security analysis of the modified protocol follows from the following result.

Theorem 2. *If for a subset Γ_{CHSH} of size m, the fraction of the inputs $(x_i,\ y_i)$, $i \in \Gamma_{CHSH}$, which satisfy the CHSH condition i.e., $(a_i \oplus b_i = x_i \wedge y_i)$ is equal to $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2} - \delta$, then for the remaining subset Γ_{QPQ} of size $n - m$, a fraction of inputs (x_i, y_i), $i \in \Gamma_{QPQ}$, which satisfy the CHSH condition, is also equal to $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2} - \delta$ with a statistical deviation ν.*

Here, $\delta = \sqrt{\frac{1}{2m}\ln\frac{1}{\epsilon_{CHSH}}}$ and $\nu = \sqrt{\frac{(m+1)}{2(1-\frac{m}{n})m^2}\ln\frac{1}{\epsilon_{QPQ}}}$, ϵ_{CHSH} and ϵ_{QPQ} are negligibly small value.

Essentially, the result means that if the success probability of the local CHSH game for the set Γ_{CHSH} varies in the range $[p_{QPQ} - \epsilon p_{QPQ}, p_{QPQ} + \epsilon p_{QPQ}]$, where p_{QPQ} equals $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$ and ϵ is the accuracy parameter, then the success probability of the game for the set Γ_{QPQ} would vary in the range $[p_{QPQ} - \epsilon p_{QPQ} - \nu, p_{QPQ} + \epsilon p_{QPQ} + \nu]$.

Note that in Theorem 2, if n is close to m, then ν is no longer guarranteed to be negligible. On the other hand, the choice $n \geq 2m$ makes the coefficient of $\frac{(m+1)}{m^2}\ln\frac{1}{\epsilon_{QPQ}}$ less than 1 and thus is practically a good choice.

So far, the entire security analysis, including that of QPQ[33] and DI-QPQ[23], is performed under the assumption that the states provided by Alice are all identical. Indeed, when n is infinitely large, Alice cannot have any advantage in non-uniformly biasing the states, as Bob selects the subset Γ_{CHSH} uniformly randomly. However, when $n \gg 2m$, but finite, then Alice could inject more bias in the choice of her basis than the threshold $\sqrt{\frac{2\epsilon p_{QPQ}}{\cos\psi_1}}$ (from Eq. (4.7)) for a few states and no bias for the remaining states and still she could pass the CHSH test by Bob. More formally, if she injects a bias ϵ'_A in r out of n states uniformly at random, then it can be easily shown that to pass the CHSH test, the following condition is required.

$$\epsilon'_A \leq \sqrt{\frac{2n\epsilon p_{QPQ}}{r\cos\psi_1}}. \tag{4.8}$$

Thus, by choosing $r \ll n$, Alice can lift the threshold of ϵ'_A much higher than that of ϵ_A and can also retrieve more number of keys if the corresponding states are selected for QPQ.

To resist this attack, Bob has to choose the minimum possible n, i.e., $n = 2m$. Since Bob will take $m = m_{QPQ}$ as per our analysis in Section 4.4.1, we have $n = 2m_{QPQ}$.

One may think that the restriction on n would limit Bob to know the key bits for all the positions of the database. This can be easily taken care of by allowing Alice and Bob to play the game repeatedly, each time corresponding to new sets of positions in the database, so as to cover all the positions for Bob.

4.5 Modification of DI-QBC Towards Finite Number of Entangled States

In case of Bit Commitment[1], the shared state between two party is the Bell state

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},$$

which is a special form of the above mentioned general state with $\theta_1 = \frac{\pi}{2}$, $\theta_2 = \pi$, $q = \frac{1}{2}$. From the equation of the estimated sample size, we can see that as the success probability increases, the required sample size decreases. For this state which is of the form $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$, the success probability will be maximum for $\psi_1 = -\frac{3\pi}{8}$ and $\psi_2 = \frac{3\pi}{8}$.

Now, by putting this specific values into the above success probability expression we get the success probability of this state which is $p_{BC} = (\frac{1}{2} + \frac{1}{2\sqrt{2}})$. This success probability is maximum for this specific state and also for two qubit entangled states in CHSH game.

So, for m_{QBC} number of states of the form $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$, the success probability will never exceed the value p_{BC} as this is the maximum success probability for two qubit entangled states in CHSH game and so we will check here whether the success probability value of CHSH test for this many samples lies within the range $[p_{BC} - \epsilon p_{BC}\ ,\ p_{BC}]$ or not. If this success probability value lies within this range then we will proceed the protocol, otherwise we will abort the protocol.

The modified protocol of device independent quantum bit commitment for finite samples will be same like the protocol proposed in case of quantum key distribution.

Chapter 5

Overview Of Quantum Pseudo Telepathy Games

Quantum pseudo-telepathy[10] is a phenomenon in quantum game theory resulting in anomalously high success rates in coordination games between separated players. These high success rates would require communication between the players in a purely classical (non-quantum) world; however, the game is set up such that during the game, communication is physically impossible. This means that for quantum pseudo-telepathy to occur, prior to the game the participants need to share a physical system in an entangled quantum state, and during the game have to execute measurements on this entangled state as part of their game strategy. Games in which the application of such a quantum strategy leads to pseudo-telepathy are also referred to as quantum non-locality games.

A two-party game is defined as a sextuple $G = \langle X, Y, A, B, P, W \rangle$, where X, Y , A and B are sets, $P \subset X \times Y$ and $W \subset X \times Y \times A \times B$. It is convenient to think of X and Y as the input sets, A and B as the output sets, P as a predicate on $X \times Y$ known as the promise, and W as the winning condition, which is a relation between inputs and outputs that has to be satisfied by Alice and Bob whenever the promise is fulfilled i.e, formally it can be said that Alice and Bob win when asked (x, y) and answer (a, b) if $(x, y) \notin P$ or $(x, y, a, b) \in W$.

The effect of quantum pseudo telepathy can be observed in many games. The use of the quantum pseudo telepathic effects enables players better results than they would achieve in the classical game without sharing any information at all. Here we define some of this games.

5.1 CHSH Game

The CHSH game[12] is played by two players, Alice and Bob which are far away from each other and they are not able to communicate in the classical manner at all. The game judge gives one random binary digit x to Alice and one random binary digit y to Bob. Alice must correspond to a game judge with a binary digit a and Bob must correspond with a binary digit b. Game Judge takes a look at all binary digits x, y, a, b and declares Alice and Bob winners if $a \oplus b = x \wedge y$, otherwise Alice and Bob lose the game. Symbol $\oplus$ denotes the XOR operation (addition modulo 2).

5.1.1 Classical Strategy:

If Alice and Bob play the classical version of the CHSH game without exchanging any information in the classical manner then the maximum probability for Alice and Bob to win is $\frac{3}{4}$. They can achieve such probability by using the following strategy:

- Bob will always correspond with $b = 0$.
- If Alice receives $x = 0$, she will correspond with $a = 0$. The game is won by Alice and Bob with the probability 1.
- If Alice receives $x = 1$ then she has to gamble because she does not know binary digit y which Bob received. Game is won by Alice and Bob with the probability $\frac{1}{2}$.

Overall probability for Alice and Bob to win the game if they use the above mentioned strategy is:

$$= (\frac{1}{2} \times 1) + (\frac{1}{2} \times \frac{1}{2}) = \frac{3}{4}$$

5.1.2 Quantum Strategy:

In quantum strategy of CHSH game, Alice and Bob share two qubit system which is initialized in the Bell state

$$|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

For a given angle $\theta \in [0, 2\pi)$, define

$$|\phi_0(\theta)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,$$

$$|\phi_1(\theta)\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$$

They can gain maximum success using the following strategy:

- Alice takes the first qubit and Bob takes the second qubit from the shared quantum state.
- If Alice receives $x = 0$ then she will measure her qubit with respect to the basis $\{|\phi_0(0)\rangle, |\phi_1(0)\rangle\}$.
- If Alice receives $x = 1$ then she will measure her qubit with respect to the basis $\{|\phi_0(\pi/4)\rangle, |\phi_1(\pi/4)\rangle\}$.
- If Bob receives $y = 0$ then he will measure his qubit with respect to the basis $\{|\phi_0(\pi/8)\rangle, |\phi_1(\pi/8)\rangle\}$.
- If Bob receives $y = 1$ then he will measure his qubit with respect to the basis $\{|\phi_0(-\pi/8)\rangle, |\phi_1(-\pi/8)\rangle\}$.

Alice and Bob will answer correctly with probability $\cos^2 \pi/8 \approx 0.85$ by following the above strategy, which is better than an optimal classical strategy that wins with probability $\frac{3}{4}$.

5.2 GHZ Game

In GHZ game[10], Alice, Bob and Charles have each one bit as an input with the promise that the parity of the input bits is 0. We denote the input bits x_1, x_2 and x_3. The task for each player is to produce one bit so that the parity of the output bits is equal to the disjunction of the input bits. Thus, if a_1, a_2 and a_3 are the outputs, then the equation $a_1 \oplus a_2 \oplus a_3 = x_1 \vee x_2 \vee x_3$ must hold.

5.2.1 Classical Strategy:

First consider a deterministic strategy, where each answer is a function of the question received and no randomness is used by the players. Let us write a_r, b_s and c_t to denote the answers that would be given for each choice of r, s and t. For example, if $a_0 = 1$ and $a_1 = 0$, then Alice always answers the question 0 with 1 and the question 1 with 0. The winning conditions can be expressed by the four equations -

$$a_0 \oplus b_0 \oplus c_0 = 0$$

$$a_0 \oplus b_1 \oplus c_1 = 1$$

$$a_1 \oplus b_0 \oplus c_1 = 1$$

$$a_1 \oplus b_1 \oplus c_0 = 1$$

Adding the four equations modulo 2 gives $0 = 1$, a contradiction. This means it is not possible for a deterministic strategy to win every time. Like CHSH game(section 5.1) the maximum success probability achieved in this case is also equals to 3/4, which can be achieved classically using the following strategy-

- Alice, Bob and Charlie all corresponds with $a_i = 1$, $b_i = 1$ and $c_i = 1$ irrespective of the input they receive.
- For input 000, output will be $a_0 \oplus b_0 \oplus c_0 = 1$ for their strategy. So, for this input they will always loose according to this strategy.
- For input $\in \{110, 101, 011\}$, output will be always 1 for their strategy. So, for this input combination they will always win according to this strategy.

Overall probability for Alice, Bob and Charlie to win the game if they use the above mentioned strategy is:

$$= (\frac{1}{4} \times 0) + (\frac{3}{4} \times 1) = \frac{3}{4}$$

5.2.2 Quantum Strategy:

In quantum strategy, the three players share the entangled state

$$|\psi\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

This is sometimes called a GHZ state - but also the term GHZ state sometimes refers to the state-

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

which is equivalent to $|\psi\rangle$ up to local unitary operations. Each player will use the same strategy:

- If the question is $q = 1$, then the player performs a Hadamard transform on their respective qubit of the above state. If $q = 0$, the player does not perform a Hadamard transform.
- The player measures their qubit in the standard basis(means $\{|0\rangle, |1\rangle\}$ basis) and returns the answer to the referee.
- Alternately, the players measure with respect to the basis $\{|0\rangle, |1\rangle\}$ when they receive $q = 0$ and measure with respect to the basis $\{|+\rangle, |-\rangle\}$ when they receive $q = 1$.

Three players will answer correctly with probability 1 by following the above strategy, which is better than an optimal classical strategy that wins with probability $\frac{3}{4}$.

5.3 Parity Game

For any $n \geq 3$, the parity game G_n consists of n players. This game is also known as multi party pseudo telepathy game[9]. Each player A_i receives a single input bit x_i and is requested to produce a single output bit y_i. The players are promised that there is an even number of $1s$ among their inputs. Without being allowed to communicate after receiving their inputs, the players are challenged to produce a collective output that contains an even number of $1s$ if and only if the number of $1s$ in the input is divisible by 4. More formally, we require that -

$$\sum_{i}^{n} y_i \equiv \frac{1}{2}\sum_{i}^{n} x_i \ (mod\ 2)$$

provided $\sum_i^n x_i \equiv 0\ (mod\ 2)$. We say that $x = x_1 x_2 \cdots x_n$ is the question and $y = y_1 y_2 \cdots y_n$ is the answer.

5.3.1 Classical Strategy:

Here also we consider a deterministic strategy (like GHZ game described in section 5.2), where each answer is a function of the question received and no randomness is used by the players. Let us consider three players and write a_r, b_s and c_t to denote the answers that would be given for each choice of r, s and t. The four winning conditions for four possible inputs can be listed as follows -

For input 000, output must belongs to set $\{000, 110, 101, 011\}$

For input $\in \{110, 101, 011\}$, output must belongs to set $\{100, 010, 001, 111\}$

Here also it can be proved that it is not possible for a deterministic strategy to win every time. Like CHSH game and GHZ game(section 5.1 and 5.2) the maximum success probability achieved in classical case is also equals to 3/4, which can be achieved using the following strategy -

- Alice, Bob and Charlie all corresponds with output $a_i = 1$, $b_i = 1$ and $c_i = 1$ irrespective of the input they receive.
- For input 000, output will be $a_0 b_0 c_0 = 111$ for their strategy. So, for this input they will always loose according to this strategy.
- For input $\in \{110, 101, 011\}$, output will be always 111 for their strategy. So, for this input combination they will always win according to this strategy.

Overall probability for Alice, Bob and Charlie to win the game if they use the above mentioned strategy is:

$$= (\frac{1}{4} \times 0) + (\frac{3}{4} \times 1) = \frac{3}{4}$$

5.3.2 Quantum Strategy:

In quantum strategy, n players will share n-qubit entangled state $|\phi_n^+\rangle$ which is of the form -

$$|\phi_n^+\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$$

Let S denote the unitary transformation defined by,

$$S|0\rangle \rightarrow |0\rangle$$

$$S|1\rangle \rightarrow i|1\rangle$$

The quantum strategy followed by each of the player is described here -

Each player A_i receives input bit x_i and does the following.

- If $x_i = 1$, A_i applies transformation S to his qubit; otherwise he does nothing.
- He applies Hadamard transform (H) to his qubit irrespective of the input.
- He measures his qubit in standard basis (i.e, in $\{|0\rangle, |1\rangle\}$ basis) in order to obtain y_i. Then he produces y_i as his output.

Here in this protocol for n players, they will answer correctly with probability 1 by following the above strategy, which is better than an optimal classical strategy that wins with probability $\frac{3}{4}$.

Parity game is also famously known as Multiparty Pseudo Telepathy game. There also exists other games[10] like Deutsch-Jozsa game, Magic Square game, Matching game etc.

Of course, it would be interesting to find new pseudo-telepathy games or families of games. It would be equally interesting to show how they relate to one another. Just like three party parity game and GHZ game discussed above are almost of same kind. We can also see the application of theses pseudo telepathy games to several quantum cryptographic protocols.

Chapter 6

Proposed Strategy For Optimal Sample Device Independent Protocols

In previous chapter, we have discussed about several pseudo telepathy games and their classical and quantum winning strategy. Among these games, CHSH game[12] is used in most of the device independent quantum cryptographic protocols in the form of CHSH test[12] to test the measurement devices involved in the protocol. In this chapter, we propose a new strategy for testing measurement devices so that we can use optimal number of samples while testing the measurement devices in finite sample scenario.

6.1 Modification of DI-QKD Towards Optimal Number of Entangled States

Let us consider a generalized form $|\psi_{gen}\rangle$ of the two qubit entangled state involved in Quantum Key Distribution (QKD) protocol where

$$|\psi_{gen}\rangle = \cos\theta|00\rangle + e^{i\phi}\sin\theta|11\rangle$$

In the above state if we put $\theta = \frac{\pi}{4}$ and $\phi = 0$, we will get the state $(|00\rangle + |11\rangle)/\sqrt{2}$, which is originally shared in QKD protocol.

The success probability of the CHSH game[12] with this general state $|\psi_{gen}\rangle$ will be $\frac{1}{2} + \frac{1}{4\sqrt{2}}(1 + cos\phi sin2\theta)$ which equals $\frac{1}{2} + \frac{1}{2\sqrt{2}}$ for the state shared in QKD protocol.

6.1.1 Transformation of two qubit state into three qubit

Now we will transform the above general state $|\psi_{gen}\rangle$ into equivalent three qubit entangled state as follows:

- In QKD, Alice and Bob each holds one qubit of the shared two qubit entangled state. Now either Alice or Bob adds an ancilla qubit $|0\rangle$ to his end.
- The party who adds the ancilla qubit in his end will perform CNOT operation on the target ancilla qubit $|0\rangle$ by considering the other qubit in his end of the shared entangled state as control qubit.
- After performing this operation, the resulting state between two parties will be of the form
$$\cos\theta|000\rangle + e^{i\phi}\sin\theta|111\rangle$$
- This state will be the resulting three qubit entangled state shared between two parties.

Now the success probability of the parity game[9] with this transformed state $\cos\theta|000\rangle + e^{i\phi}\sin\theta|111\rangle$ will be $\frac{1}{2}(1 + sin2\theta cos\phi)$ which equals 1 for the three qubit state $(|000\rangle + |111\rangle)/\sqrt{2}$ which can be obtained by applying the above transformation when the shared state between two party is $(|00\rangle + |11\rangle)/\sqrt{2}$ i.e, the state shared in QKD protocol.

6.1.2 Comparative Study Between Two Games

Let y_1 denote the success probability of the parity game for the transformed three qubit state of the form $cos\theta|000\rangle + e^{i\phi}sin\theta|111\rangle$. Then $y_1 = \frac{1}{2}(1 + sin2\theta cos\phi)$

Again, let y_2 denote the success probability of the CHSH game for the initial two qubit shared entangled state of the form $cos\theta|00\rangle + e^{i\phi}sin\theta|11\rangle$. Then $y_2 = \frac{1}{2} + \frac{1}{4\sqrt{2}}(1 + cos\phi sin2\theta)$

The success probability values of two games corresponding to different values of θ from 0 to $\frac{\pi}{4}$ is shown in figure 6.1.

Here in the graph, blue line represents the success probability of the parity game and green line represents the success probability of CHSH game. From the graph, it can be seen that for CHSH game, the value of success probability varies between 0.67 to 0.85 whereas for parity game, the value of the success probability varies between 0.5 to 1. So, the deviation range of success probability values for parity game is more as compared to the deviation for CHSH game.

It is also clear from the graph that in both the cases maximum success probability can be achieved when $\phi = 0$ and $\theta = \frac{\pi}{4}$. The maximum success probability in CHSH game

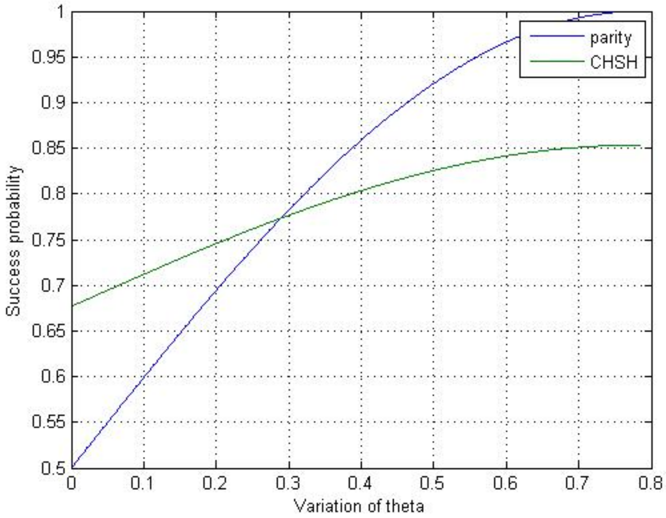

Figure 6.1: Comparative study of success probabilities between CHSH and parity game for DI-QKD protocol

corresponds to the two qubit state $(|00\rangle + |11\rangle)/\sqrt{2}$ shared in QKD protocol. Similarly, the maximum success probability in parity game corresponds to the three qubit state $(|000\rangle + |111\rangle)/\sqrt{2}$ which can be obtained from the two qubit state shared in QKD protocol by applying the above transformation (described in section 6.1.1).

6.1.3 Modified DI-QKD protocol with optimal samples

From the discussion of previous section, we can see that the success probability of the transformed three qubit state is higher compared to success probability of the shared two qubit state in QKD protocol.

The expression of the estimated sample size (as discussed in chapter 4) implies that as the success probability increases, the required sample size to estimate a state decreases. In case of QKD, as the success probability of the transformed three qubit state is higher compared to the actual two qubit state, we will perform parity game test with the transformed state instead of CHSH test to reduce the sample size needed to test measurement devices.

In previous case, while discussing about device independent protocols for finite samples, we only consider the maximum success probability corresponding to a fixed θ but not consider any variation of CHSH test[14] to reduce sample size. Here we focus on this issue and propose our modified protocol for optimal number of samples.

At first, any one of the communicating parties calculates the value of success probability for the transformed state. Then from the calculated success probability $p_{QKD_{max}}$, the party calculates the required optimal sample size $m_{QKD_{opt}}$ for the parity game to certify the states with certain accuracy and confidence. Communicating parties start with $n = 2m_{QKD_{opt}}$ number of entangled states (as described in security analysis of chapter 4).

Let Γ_{parity} denote the set which contains the states for parity test, where $|\Gamma_{parity}| = m_{QKD_{opt}}$ and Γ_{QKD} denote the set which contains the remaining states, i.e., $|\Gamma_{QKD}| = n - m_{QKD_{opt}} = m_{QKD_{opt}}$. Communicating parties choose the states for each of Γ_{parity} and Γ_{QKD} uniformly at random from the given set of n states. We consider here that Alice adds extra ancilla qubit to her end i.e, for the shared three qubit state, Alice has two qubits and Bob has one qubit. Our modified protocol has been described in algorithm 7.

1. Let the inputs are x_i, y_i, z_i where it satisfies the condition $x_i \oplus y_i \oplus z_i = 0$. For rounds $i \in \{1, \cdots, |\Gamma_{parity}|\}$

   (a) Alice chooses input $x_i y_i \in \{0,1\}^2$ and Bob chooses input $z_i \in \{0,1\}$ where inputs x_i, y_i, z_i satisfies the condition $x_i \oplus y_i \oplus z_i = 0$.

   (b) If $x_i = 0 (y_i = 0)$, Alice measures the first (second) qubit of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1 (y_i = 1)$, she first applies unitary operator S (see chapter 5 section 5.3) to first (second) qubit and then measure in $\{|0\rangle, |1\rangle\}$ basis.

   (c) Similarly, if $z_i = 0$, Bob measures his qubit in $\{|0\rangle, |1\rangle\}$ basis and if $z_i = 1$, Bob first applies unitary operator S to his qubit and then measure in $\{|0\rangle, |1\rangle\}$ basis. (d) The output is recorded as $a_i, b_i, c_i \in \{0,1\}$ for the first, second and third particle respectively. The encoding for a_i, b_i, c_i is performed as follows.

   - For each of the qubit shared between Alice and Bob, if the measurement result is $|0\rangle$ then output will be 0; if the result is $|1\rangle$ then it would be 1.

   (e) Testing: For the test round $i \in \Gamma_{parity}$, define

$$Y_i = \begin{cases} 1 & \text{if for input } 000, \text{ output} \in \{110, 101, 011, 000\} \text{ or for input} \in \\ & \{110, 101, 011\}, \text{output} \in \{100, 010, 001, 111\} \\ 0 & \text{if } \textit{otherwise}. \end{cases}$$

2. If the value of $\frac{1}{|\Gamma_{parity}|} \sum_i Y_i$ lies within the range $[p_{QKD_{max}} - \epsilon p_{QKD_{max}}, p_{QKD_{max}}]$, where $p_{QKD_{max}}$ equals 1 and ϵ is the accuracy parameter chosen by the communicating parties, they proceed the protocol otherwise they abort the protocol.

3. When the parity test is successful, communicating parties proceed for the subset Γ_{QKD}.

4. Alice and Bob perform the key distribution phase as described in [32].

Algorithm 7: Modified DI-QKD protocol for optimal sample

6.2 Modification of DI-QPQ Towards Optimal Number of Entangled States

The two qubit entangled state involved in Quantum Private Query (QPQ) protocol is of the form

$$|\psi_{QPQ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$$

where $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$.

The success probability of the CHSH game for this state $|\psi_{QPQ}\rangle$ will be $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$ where $|\psi_1\rangle$ and $|\psi_2\rangle$ are the chosen measurement basis and this success probability value can be maximized by choosing appropriate measurement basis $|\psi_1\rangle$ and $|\psi_2\rangle$ for a particular θ.

From the discussion of chapter 4, it is clear that the optimal value of $|\psi_1\rangle$ and $|\psi_2\rangle$ corresponding to a particular θ will be $|\psi_1\rangle = (\frac{\pi}{2} - \tan^{-1}(\text{cosec } \theta\ ))$ and $|\psi_2\rangle = (\frac{\pi}{2} + \tan^{-1}(\text{cosec } \theta\ ))$

6.2.1 Transformation of two qubit state into three qubit

In DI-QPQ[23], Bob holds the entangled state and perform local CHSH test before the protocol starts and Alice acts as an adversary in this case. Now we will transform the state $|\psi_{QPQ}\rangle$ into equivalent three qubit entangled state as follows:

- Bob first perform the CNOT operation over the two qubit entangled state to be shared by considering first qubit as a control bit and second qubit as a target bit.
- After performing the CNOT operation, Bob will add an ancilla qubit $|0\rangle$ in his end and perform Toffoli operation by considering first two qubit of the modified entangled state as control bit and the ancilla qubit as a target bit.
- After performing this operations, the resulting state will be of the form

$$\frac{1}{2}(\cos\frac{\theta}{2}|000\rangle + \sin\frac{\theta}{2}|010\rangle + \cos\frac{\theta}{2}|111\rangle - \sin\frac{\theta}{2}|100\rangle)$$

- This state will be the resulting three qubit entangled state at Bob's end.

Now the success probability of the parity game with this transformed three qubit state will be $\frac{1}{2}(1 + \cos\theta)$ which equals 1 for $\theta = 0$.

6.2.2 Comparative Study Between Two Games

Let z_1 denote the success probability of the parity game for the transformed three qubit state of the form $\frac{1}{2}(\cos\frac{\theta}{2}|000\rangle + \sin\frac{\theta}{2}|010\rangle + \cos\frac{\theta}{2}|111\rangle - \sin\frac{\theta}{2}|100\rangle)$. Then $z_1 = \frac{1}{2}(1 + \cos\theta)$

Again, let z_2 denote the success probability of the CHSH game for the initial two qubit entangled state of the form $\frac{1}{2}(\cos\frac{\theta}{2}|00\rangle + \sin\frac{\theta}{2}|01\rangle + \cos\frac{\theta}{2}|10\rangle - \sin\frac{\theta}{2}|11\rangle)$. Then $z_2 = \frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$ where $|\psi_1\rangle = (\frac{\pi}{2} - \tan^{-1}(\text{cosec }\theta\ ))$ and $|\psi_2\rangle = (\frac{\pi}{2} + \tan^{-1}(\text{cosec }\theta\ ))$

The success probability values of two games corresponding to different values of θ from 0 to $\frac{\pi}{2}$ is shown in figure 6.2.

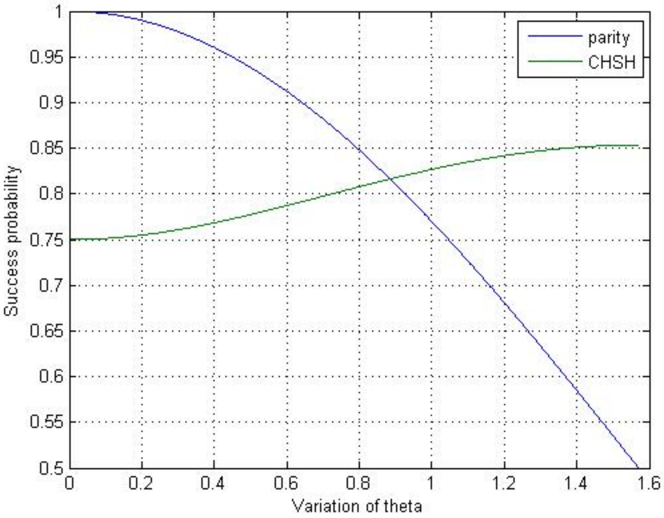

Figure 6.2: Comparative study of success probabilities between CHSH and parity game for DI-QPQ protocol

Here in this graph, blue line represents the success probability of parity game and green line represents the success probability of CHSH game. From the graph it can be seen that for CHSH game, the value of success probability varies between 0.75 to 0.85 whereas for parity game, the value of the success probability varies between 1 to 0.5. So, the deviation range of success probability values for parity game is more as compared to the deviation for CHSH game.

From the graph, it is clear that at $\theta \approx 0.9$, two lines intersect each other. So, for all the given states where the values of $\theta \leq 0.9$, the success probability of parity game for transformed three qubit state is higher compared to the success probability of CHSH game for original two qubit state. Again, for $\theta > 0.9$, the success probability of CHSH game for original two qubit state is higher compared to the success probability of parity game for transformed three qubit state.

6.2.3 Modified DI-QPQ protocol with optimal samples

From the discussion of previous section, we can conclude that for $\theta \leq 0.9$, the success probability of parity game is higher and for $\theta > 0.9$, the success probability of CHSH game is higher.

The expression of the estimated sample size (as discussed in chapter 4) implies that as the success probability increases, the required sample size to estimate a state decreases.

1. First we will check whether the value of $\theta > 0.9$ or not. If $\theta > 0.9$, then we will perform CHSH test as described in chapter 4 subsection 4.2.1, else we will perform the following steps.
2. Let the inputs are x_i, y_i, z_i where it satisfies the condition $x_i \oplus y_i \oplus z_i = 0$. For rounds $i \in \{1, \cdots, |\Gamma_{parity}|\}$

   (a) Bob chooses input $x_i y_i z_i \in \{0,1\}^3$ where inputs x_i, y_i, z_i satisfies the condition $x_i \oplus y_i \oplus z_i = 0$.

   (b) If $x_i = 0$, Bob measures the first qubit of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, he first applies unitary operator S (see chapter 5 section 5.3) to first qubit and then measure in $\{|0\rangle, |1\rangle\}$ basis.

   (c) Similarly, he will perform on second and third qubit based on the value of y_i and z_i respectively. (d) The output is recorded as $a_i b_i c_i \in \{0,1\}$ for the first, second, third particle respectively. The encoding for a_i, b_i, c_i is performed as follows.

   - For each of the qubit, if the measurement result is $|0\rangle$ then output will be 0; if the result is $|1\rangle$ then it would be 1.

   (e) Testing: For the test round $i \in \Gamma_{parity}$, define

   $$Y_i = \begin{cases} 1 & \text{if for input } 000, \text{ output } \in \{110, 101, 011, 000\} \text{ or for input } \in \\ & \{110, 101, 011\}, \text{ output} \in \{100, 010, 001, 111\} \\ 0 & \text{if } \textit{otherwise.} \end{cases}$$

3. If the value of $\frac{1}{|\Gamma_{parity}|} \sum_i Y_i$ lies within the range $[p_{QPQ_{max}} - \epsilon p_{QPQ_{max}}, p_{QPQ_{max}} + \epsilon p_{QPQ_{max}}]$ (for the cases where the values of $p_{QPQ_{max}} + \epsilon p_{QPQ_{max}}$ is greater than 1, consider the range as $[p_{QPQ_{max}} - \epsilon p_{QPQ_{max}}, 1]$) where $p_{QPQ_{max}}$ equals the maximum success probability corresponding to transformed three qubit state and ϵ is the accuracy parameter chosen by the communicating parties, they proceed the protocol otherwise they abort the protocol.
4. When the parity test is successful, communicating parties proceed for the subset Γ_{QPQ}.
5. Alice and Bob perform the private query phase as described in [33].

Algorithm 8: Modified DI-QPQ protocol for optimal sample

In previous case, while discussing about device independent protocols for finite samples, we only consider the maximum success probability corresponding to a fixed θ but not consider any variation of CHSH test to reduce sample size. Here we focus on this issue and propose our modified protocol for optimal number of samples.

Here from this analysis, we come to the conclusion that to reduce the sample size, we will perform parity test when $\theta \leq 0.9$ and will perform CHSH test[14] when $\theta > 0.9$.

At first, depending upon the value of θ, we will decide whether we have to perform CHSH test or parity test and calculate the success probability accordingly. Then from the calculated success probability $p_{QPQ_{max}}$, the party calculates the required optimal sample size $m_{QPQ_{opt}}$ for the parity game/CHSH game to certify the states with certain accuracy and confidence. Communicating parties start with $n = 2m_{QPQ_{opt}}$ number of entangled states (as described in security analysis of chapter 4).

Let Γ_{parity} denote the set which contains the states for parity test, where $|\Gamma_{parity}| = m_{QPQ_{opt}}$ and Γ_{QPQ} denote the set which contains the remaining states, i.e., $|\Gamma_{QPQ}| = n - m_{QPQ_{opt}} = m_{QPQ_{opt}}$. Communicating parties choose the states for each of Γ_{parity} and Γ_{QPQ} uniformly at random from the given set of n states. Our modified protocol has been described in algorithm 8.

6.3 Modification of DI-QBC Towards Optimal Number of Entangled States

In device independent Quantum Bit Commitment (QBC) protocol proposed by Aharon et. al[2], they used the entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$ for bit commitment. In device independent setting, they perform the device independence testing based on the violation of CHSH correlation. Now this testing procedure is equivalent to the CHSH test.

We have already shown in section 6.1 that for this specific form of state, the success probability of parity check game for transformed three qubit state is higher compared to the success probability of CHSH game for actual two qubit state.

So, like modified device independent QKD protocol, we will also use the same strategy here i.e, we will perform the parity game instead of CHSH game to test the measurement devices.

6.3.1 Modified DI-QBC protocol with optimal samples

At first, any one of the communicating parties calculates the value of the success probability for the transformed state. Then from the calculated success probability $p_{QBC_{max}}$, the party calculates the required optimal sample size $m_{QBC_{opt}}$ for the parity game to certify the states with certain accuracy and confidence. Communicating parties start with $n = 2m_{QBC_{opt}}$ number of entangled states (as described in security analysis of chapter 4).

Let Γ_{parity} denote the set which contains the states for parity test, where $|\Gamma_{parity}| = m_{QBC_{opt}}$ and Γ_{QBC} denote the set which contains the remaining states, i.e., $|\Gamma_{QBC}| =$

$n - m_{QBC_{opt}} = m_{QBC_{opt}}$. Communicating parties choose the states for each of Γ_{parity} and Γ_{QBC} uniformly at random from the given set of n states. We consider here that Alice adds extra ancilla qubit to her end i.e, for the shared three qubit state, Alice has two qubits and Bob has one qubit. Our modified protocol has been described in algorithm 9.

1. Let the inputs are x_i, y_i, z_i where it satisfies the condition $x_i \oplus y_i \oplus z_i = 0$. For rounds $i \in \{1, \cdots, |\Gamma_{parity}|\}$

   (a) Alice chooses input $x_i y_i \in \{0,1\}^2$ and Bob chooses input $z_i \in \{0,1\}$ uniformly at random.

   (b) If $x_i = 0 (y_i = 0)$, Alice measures the first (second) qubit of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1 (y_i = 1)$, she first applies unitary operator S (see chapter 5 section 5.3) to first (second) qubit and then measure in $\{|0\rangle, |1\rangle\}$ basis.

   (c) Similarly, if $z_i = 0$, Bob measures his qubit in $\{|0\rangle, |1\rangle\}$ basis and if $z_i = 1$, Bob first applies unitary operator S to his qubit and then measure in $\{|0\rangle, |1\rangle\}$ basis. (d) The output is recorded as $a_i b_i c_i \in \{0,1\}$ for the first, second, third particle respectively. The encoding for a_i, b_i, c_i is performed as follows.

   - For each of the qubit shared between Alice and Bob, if the measurement result is $|0\rangle$ then output will be 0; if the result is $|1\rangle$ then it would be 1.

   (e) Testing: For the test round $i \in \Gamma_{parity}$, define

   $$Y_i = \begin{cases} 1 & \text{if for input } 000, \text{ output} \in \{110, 101, 011, 000\} \text{ or for input} \in \\ & \{110, 101, 011\}, \text{ output} \in \{100, 010, 001, 111\} \\ 0 & \text{if } \textit{otherwise}. \end{cases}$$

2. If the value of $\frac{1}{|\Gamma_{parity}|} \sum_i Y_i$ lies within the range $[p_{QBC_{max}} - \epsilon p_{QBC_{max}}, p_{QBC_{max}}]$, where $p_{QBC_{max}}$ equals 1 and ϵ is the accuracy parameter chosen by the communicating parties, they proceed the protocol otherwise they abort the protocol.

3. When the parity test is successful, communicating parties proceed for the subset Γ_{QBC}.

4. Alice and Bob perform the bit commitment phase as described in [6].

Algorithm 9: Modified DI-QBC protocol for optimal sample

Chapter 7

Conclusion and Future Work

In this thesis, we have proposed modified device independent quantum cryptographic protocols for finite samples with the aim of practical implementation. We have approximated the required sample size for certain accuracy and confidence by using Chernoff-Hoeffding bound because among all the well known formulas and inequalities for calculating sample size, this provides the most optimal bound on sample size compared to others.

We propose a bound over eavesdropper's choice on the deviation value from the actual intended state in terms of our choice for the value of accuracy parameter and show that though we have allowed some sort of deviation for finite samples, eavesdropper can't get any extra information. Also, to test the measurement devices, we have proposed an optimal strategy(without using only CHSH test) to further reduce the sample size.

To the best of our knowledge, this is the first approach towards device independent quantum cryptographic protocols for finite samples. We have discussed here about only three protocols(quantum key distribution, quantum private query and quantum bit commitment). Use this idea or some variation of this idea to propose finite sample device independent approach for other existing quantum cryptographic protocols will be our future scope of work. As soon as the dream of the quantum computer becomes true, all these approaches will be implemented practically for the advancement of technology and security.

Bibliography

[1] Emily Adlam and Adrian Kent. Device-independent relativistic quantum bit commitment. *Phys. Rev. A*, 92:022315, Aug 2015.

[2] N Aharon, S Massar, S Pironio, and J Silman. Device-independent bit commitment based on the chsh inequality. *New Journal of Physics*, 18(2):025014, 2016.

[3] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.

[4] John S Bell. On the einstein podolsky rosen paradox. 1964.

[5] John S Bell. Physics 1, 195 (1964). *Google Scholar*, 1966.

[6] C. H. BENNETT. Quantum cryptography : Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Comp., Syst. and Signal Proc., Bangalore, India, Dec. 10-12, 1984*, 1984.

[7] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[8] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, Jan 1992.

[9] Gilles Brassard, Anne Broadbent, and Alain Tapp. *Multi-party Pseudo-Telepathy*, pages 1–11. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[10] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, Nov 2005.

[11] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, Mar 1980.

[12] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[13] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, September 2006.

[14] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[15] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[16] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum private queries: Security analysis. *IEEE Transactions on Information Theory*, 56(7):3465–3477, July 2010.

[17] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum private queries. *Phys. Rev. Lett.*, 100:230502, Jun 2008.

[18] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, Aug 2010.

[19] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[20] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[21] Markus Jakobi, Christoph Simon, Nicolas Gisin, Jean-Daniel Bancal, Cyril Branciard, Nino Walenta, and Hugo Zbinden. Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A*, 83:022301, Feb 2011.

[22] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410–3413, Apr 1997.

[23] Arpita Maitra, Goutam Paul, and Sarbani Roy. Device-independent quantum private query. *Phys. Rev. A*, 95:042344, Apr 2017.

[24] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 503–509, Nov 1998.

[25] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, Apr 1997.

[26] C. Mochon. Quantum weak coin flipping with arbitrarily small bias. *ArXiv e-prints*, November 2007.

[27] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[28] Lukasz Olejnik. Secure quantum private information retrieval using phase-encoded queries. *Phys. Rev. A*, 84:022313, Aug 2011.

[29] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[30] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Phys. Rev. Lett.*, 106:220501, Jun 2011.

[31] B. M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, Jan 2004.

[32] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[33] Yu-Guang Yang, Si-Jia Sun, Peng Xu, and Ju Tian. Flexible protocol for quantum private query based on b92 protocol. *Quantum Information Processing*, 13(3):805–813, Mar 2014.