Investigating Applications of The Target Difference Algorithm in Keccak & Ascon

thesis submitted to the

Indian Statistical Institute, Kolkata

For award of the degree

of

Masters of Technology in Cryptology and Security

by

Asim Manna

[Roll No: CrS1908]

Under the guidance of

Dr. Dhiman Saha

Department of Electrical Engineering and Computer Science
Indian Institute of Technology, Bhilai

Institute Supervisor

Dr. Goutam Paul

Cryptology & Security Research Unit (CSRU)
Indian Statistical Institute, Kolkata

Cryptology and Security Research Unit

INDIAN STATISTICAL INSTITUTE, KOLKATA

JULY 2021

Certificate

This is to certify that the thesis entitled **"Investigating Applications of The Target Difference Algorithm in Keccak & Ascon"** submitted by **Asim Manna (CrS1908)** to the Indian Statistical Institute, Kolkata, is a record of bonafide research work carried under my supervision and is worthy of consideration for the award of Masters of Technology in Cryptology and Security of the Institute.

Date: 09.07.2021

Place: IIT Bhilai

Dr. Dhiman Saha

Acknowledgements

I would like to thank the following people, without whom I would not have been able to complete this research, and without whom I would not have made it through my masters degree.

I would first like to thank my supervisor, Professor Dhiman Saha, whose expertise was invaluable in formulating the research questions and methodology. His insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I would like to acknowledge Sahiba Suryawanshi for her suggestion and help. I want to thank her for all of the opportunities I was given during my project.

I would also like to thank Dr. Pabitra Pal for his valuable guidance throughout my studies. He provided me with the tools that I needed to choose the right direction and successfully complete my dissertation.

In addition, I would like to thank my parents for their wise counsel and for all the unconditional support during my intership.

Asim Manna

ISI Kolkata.

Contents

1 Introduction

Hash functions, particularly *Cryptographic Hash Functions (CHF)* are called the Swiss-army knife of crypto primitives. This is due to the multitude of applications that these functions contribute to. They are ubiquitous in today's digital world and are a part of almost all crypto constructions. The basic aim of a CHF is to ensure data integrity (which is why they have been referred to in coding theory literature as Modification Detection Codes) due to their ability to detect (un-)intentional modifications in data. However, they are widely deployed as the cores of Message Authentication Codes (MAC), Key Derivation Functions (KDF), Password storages, Data immutability applications like Blockchains and so on and so forth. Formally, CHF is a mathematical algorithm that maps data of arbitrary size ("message") to a bit array of a fixed size referred to as *hash* or *digest*. Recently, the notion of fixed size hash has been relaxed and the research community has witnessed constructions (SPONGE [BDPVA07]) that allow for variable (or arbitrary) length hash values. The most recent addition to the globally accepted CHF algorithms is KECCAK [BDPVA09] which won the SHA-3 competition [GJMG11] by NIST in 2012 after 5-years of intense worldwide public cryptanalysis.

This work aims to analyze KECCAK/SHA-3 and look at the differential properties of the construction. In particular, this thesis concentrates on the Target Difference Algorithm (TDA) [DDS12] introduced by Dinur *et al.* in FSE 2012. The algorithm is heuristic in nature and is used to generate a pair of input states of KECCAK/SHA-3 which after one round produce the desired target difference. The strategy was later extended to two rounds by Qiao *et al.* in Eurocrypt 2017 and three rounds by Guo *et al.* in Journal of Cryptology 2020 to find new collision attacks on KECCAK. This algorithm combines basic algebraic techniques with differential cryptanalysis. The input of this algorithm is the target output difference. Depending upon the output difference a system of linear equations is constructed based on the linear and non-linear layers of KECCAK. If the system of equations consistent then it is stored for the next step where the conforming message pairs are computed. The current work aims to understand and implement TDA on KECCAK. In addition, the work also finds and enumerates the affine subspaces of KECCAK and ASCON corresponding to all output differences. In doing so a new property of the ASCON S-box is also reported.

2 Preliminaries

Here we will discuss the description of KECCAK and ASCON in this section. Section 2.1 and 2.2 illustrates the description of KECCAK and ASCON respectively.

We will give the details of the round functions of Keccak and Ascon permutation.

2.1 Keccak Description

The Keccak family of hash functions is based on the Sponge construction [BDPVA09]. The function f, in the sponge construction, is denoted by Keccak-f [b], where b is the length of the input string. Keccak$-f[b]$ function is specialization of Keccak $-\ p[b, n_r]$ family where $n_r = 12 + 2l$ and $l = log_2(b/25) = log_2(w)$ i.e.,

$$\text{Keccak} - f[b] = \text{Keccak} - p[b, 12 + 2l]$$

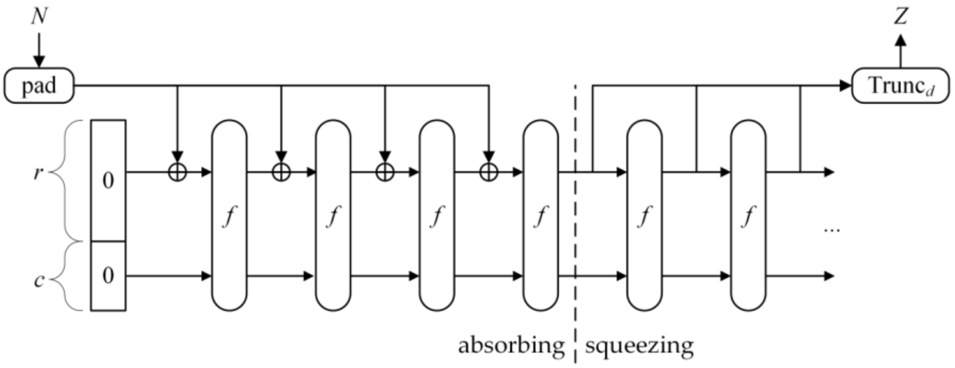

Figure 1.1: The sponge construction [Dwo15]

A state S, which is a b-bit string, in Keccak is usually denoted by a three-dimensional grid of size $5 \times 5 \times w$, w is the lanesize. For example, in the case of Keccak$-f[1600]$, w is equal to 64. The value of b is 1600, so we have $l = 6$. Thus the f function in SHA-3 is Keccak$-p[1600, 24]$. The hash function with output length d is denoted by

$$\text{Keccak} - d = \text{Keccak}[r := 1600 - 2d, c := 2d].$$

For example Keccak-384 means, the capacity $c = 768$ and $r = 832 = 13 \times 64$ i.e in the output state there are 13 lanes are active.

The round function f in Keccak consists of five steps. The step mapping specifies each state transformations. These step mappings are $\theta, \rho, \pi, \chi, \iota$. Let A and B respectively denote input and output states of a step mappings.

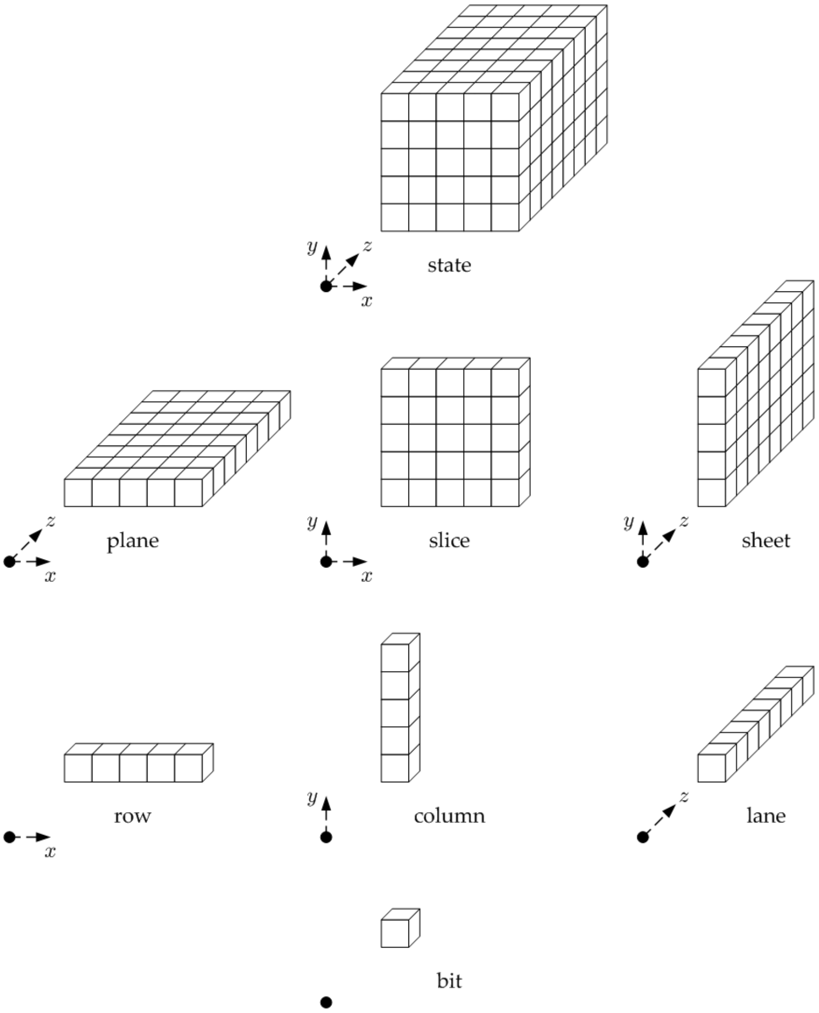

Figure 1.2: Parts of the State Array [Dwo15]

- θ **(Theta)** XOR to each bit of two columns. The first column in the same slice as the updated bit, the second column in the slice before the updated bit. From Figure 1.3, we can see the θ operation. $B[x,y,z] = A[x,y,z] \oplus P[(x-1) \bmod 5, z] \oplus P[(x+1) \bmod 5, (z-1) \bmod w]$ where, $P[x,z] = \oplus_{y=0}^{4} A[x,y,z]$.

- ρ **(Rho)** Translate bits in z-direction. From Figure 1.4, we can see the ρ operation.

$$B[x,y,z] = A[x,y,z+\rho(x,y) \mod w]$$

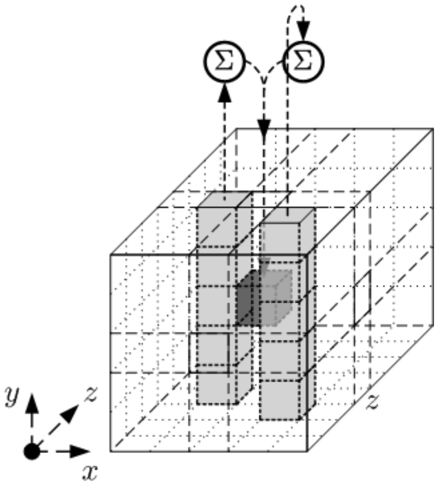

Figure 1.3: Illustration of θ applied to a single bit [Dwo15]

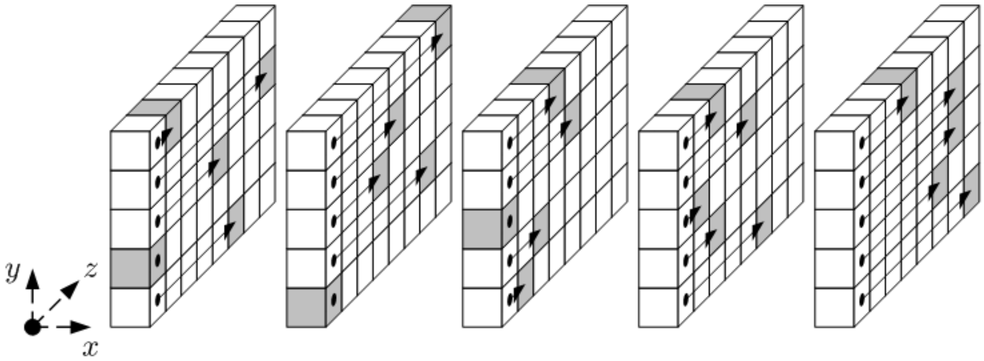

Figure 1.4: Illustration of ρ for b = 200 [Dwo15]

- π **(Pi)** Permute bits within a slice. From Figure 1.5, we can see the π operation

$$B[y][2x+3y][z] = A[x][y][z]$$

- χ **(Chi)** This is a non-linear operation, where each bit in the original, state is XOR-ed with a non-linear function of the next two bits in the same row. From Figure 1.6, we can see the χ operation

$$B[x,y,z] = A[x,y,z] \oplus ((A[(x+1) \bmod 5, y, z] \oplus 1) * (A[(x+2) \bmod 5, y, z]))$$

- ι **(iota)** $B[0,0,z] = A[0,0,z] + RC[z]$

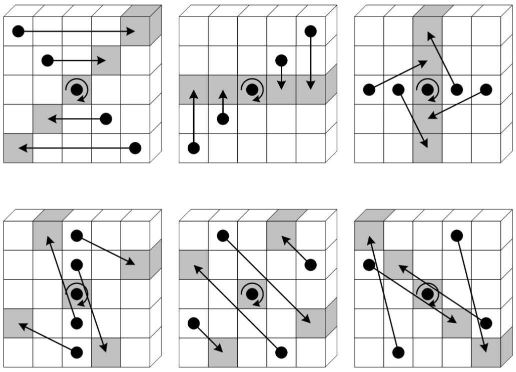

Figure 1.5: Illustration of π applied to a single slice [Dwo15]

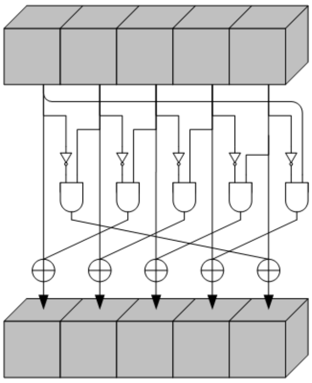

Figure 1.6: Illustration of χ applied to a single row [Dwo15]

Thus one round in KECCAK is given by $Round(A) = \iota(\chi(\pi(\rho(\theta(A)))))$, where A is the initial state. The χ operation of KECCAK takes five-bit in one S-box. Also, we know that the χ operation is non-linear of degree two.

2.2 Ascon Description

ASCON is a submission by Dobraunig et al. [DEMS16] to the CAESAR competition. Ascon is based on a sponge construction with a state size of 320 bits. The three parts- ASCON's Authenticated Encryption Modes, ASCON's Hashing Modes, ASCON's Permutation are specifies the ASCON family.

The ASCON's modes of operations are based on sponge construction. There are two type hash function ASCON-Hash with fixed output size and the extendable output function ASCON-XOF with variable output size internally use the same hashing algorithm. The $320-$bit initial state of ASCON-Xof and ASCON-Hash is given by

$$IV||0^{256} = 0^8||r||a||0^8||h||0^{256},$$
$$S = p^a(IV||0^{256}).$$

where round number a, rate r, the maximal output length of h bits as a 32-bit integer.

Ascon Permutation

All Ascon family members use the same lightweight permutation. The following three permutations iteratively applies an SPN-based round transformation $a = 12$ times (for p^a) or $b \in \{6, 8\}$ times (for p^b). The main variants of the schemes Ascon, Ascon-Xof, and Ascon-Hash are the two 320-bit permutations p^a and p^b . The round transformation consists of the following three steps which operate on a 320-bit state S divided into 5 words x_0, x_1, x_2, x_3, x_4 of 64 bits each:

$$p = p_L \circ p_S \circ p_C$$
$$S = S_r||S_c = x_0||x_1||x_2||x_3||x_4$$

- **Addition of Round Constants(p_C):** Xors a round specific 1-byte constant to word x_2.

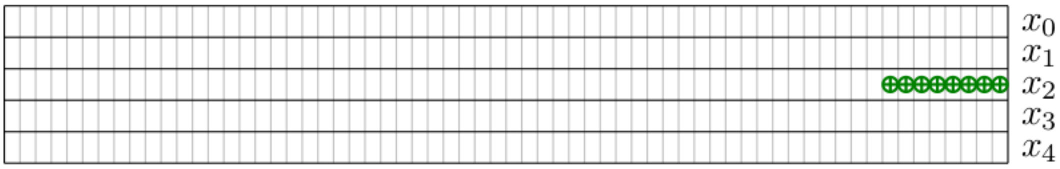

Figure 1.7: The constants are added to word x_2 of the state. [DEMS16]

- **Nonlinear Substitution Layer(p_S):**Applies a 5-bit S-box 64 times in parallel in a bit-sliced. Let $x_{0,i}, x_{1,i}, ..., x_{4,i}$ denote the bits in column $i, 0 \leq i < 64$, where $x_{0,0}$ is the least significant (rightmost) bit of the first register word (outer part) of the state. Let $y_{0,i}, y_{1,i}, ..., y_{4,i}$ denote the same bit position after application of the S-box layer.

$$y_{0,i} = x_{4,i}.x_{1,i} \oplus x_{3,i} \oplus x_{2,i}.x_{1,i} \oplus x_{2,i} \oplus x_{1,i}.x_{0,i} \oplus x_{1,i} \oplus x_{0,i} \ ,$$
$$y_{1,i} = x_{4,i} \oplus x_{3,i}.x_{2,i} \oplus x_{3,i}.x_{1,i} \oplus x_{3,i} \oplus x_{2,i}.x_{1,i} \oplus x_{2,i} \oplus x_{1,i} \oplus x_{0,i} \ ,$$
$$y_{2,i} = x_{4,i}.x_{3,i} \oplus x_{4,i} \oplus x_{2,i} \oplus x_{1,i} \oplus 1,$$
$$y_{3,i} = x_{4,i}.x_{0,i} \oplus x_{4,i} \oplus x_{3,i}.x_{0,i} \oplus x_{3,i}.x_{2,i} \oplus x_{1,i} \oplus x_{0,i} \ ,$$
$$y_{4,i} = x_{4,i}.x_{1,i} \oplus x_{4,i} \oplus x_{3,i} \oplus x_{1,i}.x_{0,i} \oplus x_{1,i} \ .$$

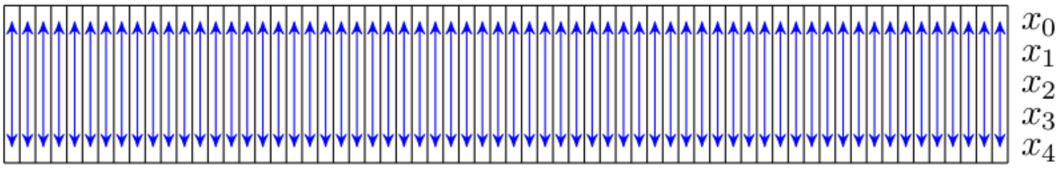

Figure 1.8: The substitution layer of Ascon applies a 5-bit S-box to the state. [DEMS16]

We can see that the the algebraic degree of S-box of Ascon is 2. Consider one S-box $[y_{0,i}, y_{1,i}, ..., y_{4,i}]$. If we fix three values $x_{4,i}, x_{1,i}, x_{3,i}$ then the S-box becomes linear.

- **Linear Diffusion Layer(p_L):** The following index computations are under mod 64.
  $y_{0,i} = x_{0,i} \oplus x_{0,i+19} \oplus x_{0,i+28}$,
  $y_{1,i} = x_{1,i} \oplus x_{1,i+61} \oplus x_{1,i+39}$
  $y_{2,i} = x_{2,i} \oplus x_{2,i+1} \oplus x_{2,i+6}$,
  $y_{3,i} = x_{3,i} \oplus x_{3,i+10} \oplus x_{3,i+17}$,
  $y_{4,i} = x_{4,i} \oplus x_{4,i+7} \oplus x_{4,i+41}$.
  The linear layer can be represented by a 320×320 matrix.

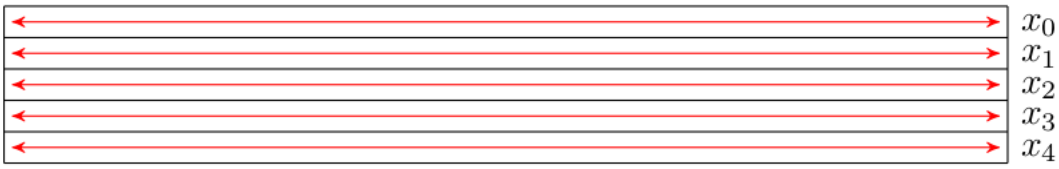

Figure 1.9: The linear diffusion layer of Ascon . [DEMS16]

3 Literature Survey

Target difference algorithm (TDA) is a technique to link a differential characteristic to the initial state of the Keccak permutation, using one round permutation. TDA is basically used for building connectors and achieve new collision attacks up to 6-round. Here we will discuss briefly the works on TDA. Dinur *et al.* first proposed the TDA [DDS12] which illustrates in Section 3.1. Then

Qiao *et al.* [QSLG17] developed another strategy to build a 2-round connector. Then in Section 3.2, we will discuss the extension of TDA to three rounds by Guo *et al.* [GLL+20].

3.1 Introduction of the TDA explained by Dinur *et al.* [DDS12]

Dinur *et al.* [DDS12] used the TDA algorithm in the first part of their 4-round collision attack on Keccak-224 and Keccak-256 to obtain a sufficiently large set of message pairs that satisfy the target difference after the first round of Keccak. They were combining 3-round differential trails and 1-round connectors and found 4-rounds collisions. The main idea to use the target difference algorithm is to find collisions and near-collisions in Keccak. The main challenge is to find the input of this algorithm. Thus they had to find such high probability the target differences such that after one round Keccak, gives this target difference. After finding a high probability differential characteristic with a low Hamming weight , they extended it backwards to obtain the target difference Δ_T. Then the target difference algorithm to link the extended characteristic backwards to the initial state of Keccak permutation, with an additional round. Given a low Hamming weight starting state difference of a characteristic, they extended it backwards by one round, and maintain its high probability [DGPW12]. Thus, any low Hamming weight characteristic for r rounds of Keccak permutation can be used to obtain results on a round-reduced version of Keccak. Also, they tried how to use 2 rounds characteristics to find collision for 4 rounds of Keccak-224 and Keccak-256, and how to use 3 rounds characteristics to find near-collision for 5 rounds of these Keccak versions. The main idea to use the target difference algorithm is to extend the initial characteristic by two additional rounds:

- Extend the characteristic backwards by one round to obtain the target difference with high characteristic's probability.

- Used the target difference algorithm to link the characteristic to the initial state of Keccak's permutation, through an additional round.

3.2 Extension of TDA to Two Rounds by Qiao *et al.* [QSLG17]

Qiao *et al.* [QSLG17] extends the above connector one round further and hence achieves collision attacks for up to 5 rounds. By linearization of all S-boxes of the first round, the problem of finding solutions of 2 rounds connectors is converted to that of solving a system of linear equations. They develop an algebraic and differential hybrid method to launch collision attacks on KECCAK with complexities below the birthday bound, against 5 rounds KECCAK-224 and 6 round KECCAK collision challenges are also achieved. Also they used the result that the KECCAK S-box can be expressed as linear transformations, when the input is restricted to some affine subspaces. Dinur *et al.*. [DDS12] and Bertoni *et al.*. [BDPA11] stated that when the input and output differences are fixed, the solution set of the KECCAK S-box contains affine subspaces of dimension up to 3. In this paper, Qiao *et al.* [QSLG17] showed that the number of 2-dimensional subspaces of S-box linearization is maximum and for those of dimension 3, six 2-dimensional affine subspaces out of it could allow the linearization. Using these result, they converted the problem to of finding 2 rounds connectors into that of solving a system of linear equations. Previously, Dinur *et al.*. [DDS12] found M and M' such that $R^1(\bar{M}||0^c) + R^1(\bar{M'}||0^c) = \Delta S_I$. Then Qiao *et al.* were bulding two rounds connnector i.e $R^2(\bar{M}||0^c) + R^2(\bar{M'}||0^c) = \Delta S_I$.

$$\alpha_0 \xrightarrow{L_0} \beta_0 \xrightarrow{\chi_0} \alpha_1 \xrightarrow{L_1} \beta_1 \xrightarrow{\chi_1} \alpha_2 = \Delta S_I \text{ (given)}.$$

α_i : Input difference of the i-th round function, i = 0, 1, 2,...
β_i : Input difference of χ in the i-th round, i = 0, 1, 2,...
Choosing β_1 in the 2 rounds connector:

- Randomly choose compatible input differences (those δ^{in}'s such that $DDT(\delta^{in}, \delta^{out}) > 0$) β_1 according to ΔS_I until the 2 rounds connectors.

- We can only choose those β_1 such that $\beta_1 \xrightarrow{\chi_1} \alpha_2$ is of the best probability for the given α_2.

α_1 can be uniquely determined by the relation $\alpha_1 = L^{-1}(\beta_1)$.
From Target difference algorithm, we can find β_0 from α_1.
Then, they were building an algorithm to construct a system of equations with these above differences and able to find to an extra round connector.

3.3 Extension of TDA to Three Rounds by Guo *et al.* [GLL+20]

Guo *et al.* [GLL+20] also extended the above connectors upto three rounds i.e $R^3(\bar{M}||0^c) + R^3(\bar{M'}||0^c) = \Delta S_I$.further and hence achieve collision attacks for up to 6 rounds.

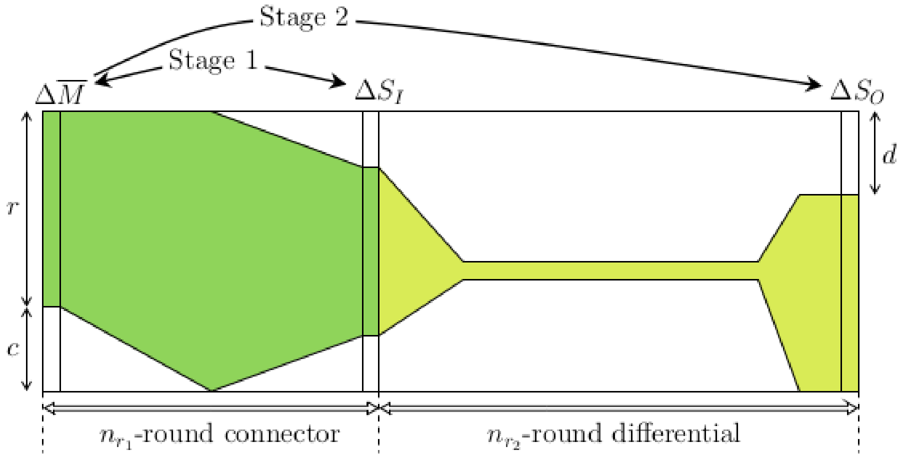

Figure 1.10: An overview of collision attack with connector [GLL+20]

They were combining 3 rounds differential trails and 3 rounds connectors and achieve collision attacks for up to 6 rounds. Here $n_{r_1} = 3$ and $n_{r_2} = 3$. The differential trail is then fulfilled probabilistically with many such message pairs, and collision was found when the first d bits of Δ_{S_0} are zero. First,they constructed an $n_{r_1} = 3$ -round connector and get a subspace of messages bypassing the first 3 rounds and then by brute force, find a colliding pair following the $n_{r_2} = 3$ rounds differential trail from the above subspaces.

Choosing β_2 in the 2 rounds connector:
First we have to choose β_2 before running the 3-round connector. The two requirements are:

- Given α_2 =$L^{-1}(\beta_2)$, a 2-round connector for the first two rounds.
- $\beta_2\rightarrow$ α_3 is of high probability where α_3 is the input differnce for the differential trail.

$$\alpha_0 \xrightarrow{L_0} \beta_0 \xrightarrow{\chi_0} \alpha_1 \xrightarrow{L_1} \beta_1 \xrightarrow{\chi_1} \alpha_2 \xrightarrow{L_2} \beta_2 \xrightarrow{\chi_2} \alpha_3 = \Delta S_I \text{ (given)}.$$

For constructing 3-round connectors, the second 2 rounds connector, β_2 is fixed. In this way, the second 2 rounds connector can be constructed successfully for the high probability $\beta_2\rightarrow$ α_3. Then similar to the 2 rounds connector, the 3 rounds connector were built.

3.4 Target Internal Difference Algorithm (TIDA) by Dinur *et al.* [DDS13]

Similar to the TDA, the TIDA is a technique that links an internal differential characteristic to the initial state of the KECCAK permutation, using one permutation round. This is also a heuristic randomized algorithm. TIDA is based on an analogous variant of the TDA for internal differential cryptanalysis. The outputs of TIDA are single-block messages whose internal state belongs to the target internal difference after one permutation round.

Let, a target internal difference $[i, t_1]$ is given after the first KECCAK S-box layer. The main idea is to find messages M such that $\chi \circ L(\bar{(}M)) \in [i, t_1]$, where $i \in \{1, 2, 4, 8, 16, 32\}$ and the rate r so that the algorithm should have sufficiently many degrees of freedom. We can check that we have a positive number of degrees of freedom only for $i = 32$ and for the Keccak versions with $n \in \{224, 256, 384\}$. For that the internal difference of the initial state is denoted by $[32, t_0]$. The internal difference after the linear layer (L) is denoted by $[32, t_{0.5}]$. For $i = 32$, the state is split into two parts. The target internal difference specifies the difference between the parts. Similar to the TDA, the TIDA has two phases: Difference Phase and Value Phase. The procedure of TIDA is similar to TDA. The set of values that satisfy the input difference and output difference are forms an affine subspace. If there is a large number of non-active S-boxes then it is difficult to solve the difference phase of the TIDA. But if we find a solution, then the dimension of the affine message subspace outputted by TIDA is expected to be large. The outputs of TIDA is an affine subspace of messages.

3.5 Simplified TIDA by Kuila *et al.* [KSPC14]

The main intuition of this paper "Practical Distinguishers against 6-Round KECCAK-f Exploiting Self-Symmetry" [KSPC14],is to exploit the self-symmetry of the internal state of KECCAK to distinguish up to 5-rounds with a probability of 1 using a single query. Finally, the extension to 6-rounds with a complexity of 2^{11} gives us the most efficient 6-round distinguisher. Let S be the arbitary state genrated by TIDA. The input and outputs of this algorithm are:

$$\text{Inputs} \rightarrow \begin{cases} \Delta_T(Target\ internal\ difference) \\ S_T(Specific\ Target\ State) \end{cases}$$

$$\text{Outputs} \rightarrow S : \begin{cases} \Delta_T = (Keccak(s)) \\ S_T \subset ((Keccak(S)) \cap S_T), \forall S \end{cases}$$

The constraint of difference phase of TIDA, "some specified positions of initial internal difference(Δ_I) are bound to 0" is ignored in this work. In this case we have full $(25 \times i)$ ($i \in \{1, 2, 4, 8, 16, 32\}$) degrees of freedom for any self-symmetric state S^i. The Self-Symmetric State is a technique that generates states that become self-symmetric after one round of Keccak. Let u be the number of specific target slices. Kuila *et al.* stated that to make sTIDA successful, if the quantity $(8 \times 25 - 25 \times u) > 0$ and the whole attack to be succeed if we have $(8 \times 25 - 25 \times u) > 11$. For the lower values of u the sTIDA will successfully produce two-symmetric states. For example if we take $u = 4$ then the attack will be succeed.

4 Understanding the Target Difference Algrithm

The main idea of TDA [DDS12] is for a given output difference Δ_T, we have to find a message pair (M^1, M^2) such that after one round Keccak it provides the given output difference i.e. $R(\bar{M}^1) + R(\bar{M}^2) = \Delta_T$, where $\bar{M}^1 = M^1||10000001||0^c$ and $\bar{M}^2 = M^2||10000001||0^c$. Now given output difference Δ_T, let Δ_I be the input difference i.e. $\bar{M}^1 + \bar{M}^2 = \Delta_I$. The Keccak consists of five step mappings θ, ρ, π, χ, ι. Here the mappings θ, ρ, π are linear and χ is non linear of degree 2. We consider L as a matrix, where $L = \rho \circ \pi \circ \theta$. The following observations are important.

- The last $c + 8$ bits of $\bar{M}^1$ are equal to $10000001||0^c$
- The last c bits of $(\bar{M}^1, \bar{M}^2)$ are same. So, The last c bits of Δ_I are zero because Δ_I is the difference (XOR) of two messages.

First this algorithm is splited into two phases: Difference Phase (Algorithm 1 and 2) and Value Phase (Algorithm 3 and 4). In Difference Phase, we are trying to construct a system of equations E_Δ and in the Value Phase we find the value of messages and input difference Δ_I. Figures 1.11 and 1.12 provides an overview of TDA.

Let, we take v variables and t number of active S-boxes in Algorithm 1. Also we added total $c + 5(v/5 - t) + 3t = v + c - 2t$ linear equations in E_Δ. Then the dimension of the solution set is $v - (v + c - 2t) = 2t - c$. If $2t - c > 0$ then our algorithm may succeed.

We can see that in the basic procedure of the difference phase sometimes we may get "No Solution" or "Fail" because this algorithm is heuristic. To obtain better results, the main idea behind the change the order of the S-boxes such

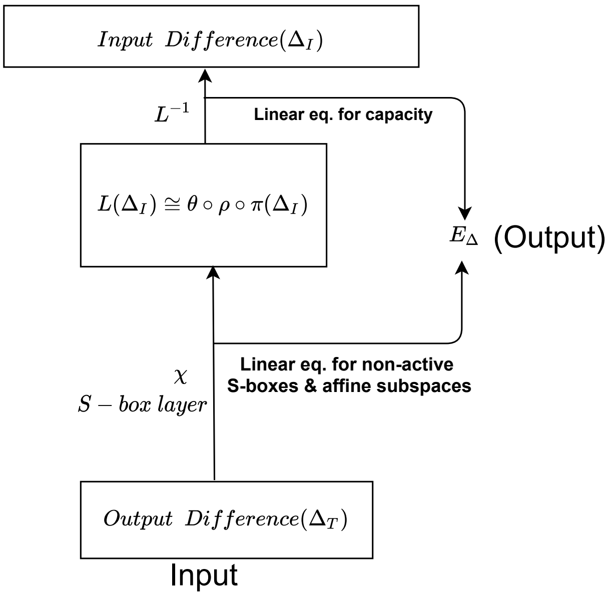
$Input\ Difference(\Delta_I)$
L^{-1}
Linear eq. for capacity
$L(\Delta_I) \cong \theta \circ \rho \circ \pi(\Delta_I)$
E_Δ (Output)
χ
$S-box\ layer$
Linear eq. for non-active
S-boxes & affine subspaces
$Output\ Difference(\Delta_T)$
Input

Figure 1.11: Difference phase of the TDA

that the S-boxes (which produces the inconsistent equations) are pushed to the front of the Input Difference Subset Data Structure (IDSD, Appendix C) order. For that, we have to use another algorithm the main procedure of difference phase.

Algorithm 1: Basic Procedure of Difference Phase of Target difference algorithm on Keccak

```
   input  : $\Delta_T$: Target Difference
   output: $E_\Delta$: System of Equations
1  $E_\Delta = \{\}$
2  $L(\Delta_I) = \{x_1, x_2, \dots x_{1600}\}$
3  $exp = L^{-1}(X)$, $E_\Delta = exp(c||p) == 0$ here c and p is capacity and
     padding bits respectively.
4  For each $320 - t$ non-active S-boxes,
     $E_\Delta = \{x_{i+1} == 0 \dots x_{i+5} == 0.\}$, for $i$-th non-active S-box.
5  if $E_\Delta$ is not consistent then
6      output Fail
7  end
8  else
9      for $t$ active S-boxes do
10         from $\Delta_T$ obtain $\delta^{out}$
11         Find all $\delta^{in}$ such that $DDT(\delta^{in}, \delta^{out}) > 0$.
12         Find all the 2D afiine subspaces from the $\delta^{in}$'s.
13         Add 3 affine equations to $E_\Delta$ from the 2D affine subset
             according to the IDSL (Appendix C)
14     end
15     if $E_\Delta$ is consistent then
16         continue to the next S-box
17     end
18     else if then
19         continue to the next subset in the IDSL, by incrementing the
             pointer and going to step 14
20     end
21     else
22         No Solution
23     end
24 end
```

Algorithm 2: The Main Procedure of Difference Phase

```
1  int counter, $T_1$;
2  while counter != $T_1$ do
3      Intialize counter = 0 and randomize the IDSD Sbox order.
4      Excute the bascic procedure;
5      if the basic procedure succeeds then
6          output $E_\Delta$;
7      end
8      else if the basic procedure fails then
9          abort;
10     end
11     else
12         counter++;
13         go to next step
14     end
15     Reset the pointer of the failed Sbox IDSL (Appendix C) to its value
         before the last basic procedure. Change the IDSD order by
         bringing the failed Sbox to the front and go to step 4.
16 end
```

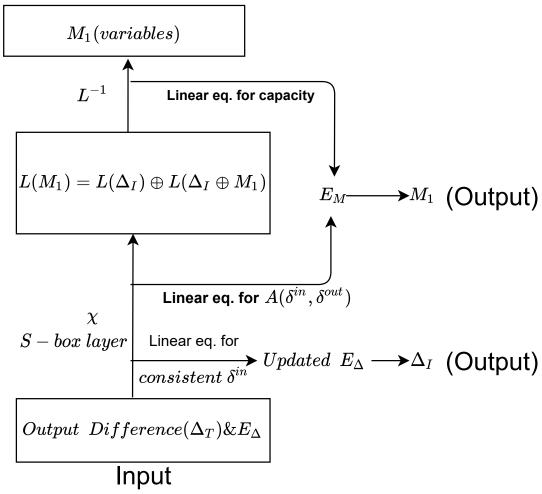
$M_1(variables)$
L^{-1}
Linear eq. for capacity
$L(M_1) = L(\Delta_I) \oplus L(\Delta_I \oplus M_1)$
$E_M \longrightarrow M_1$ (Output)
Linear eq. for $A(\delta^{in}, \delta^{out})$
χ
$S-box\ layer$
Linear eq. for
consistent δ^{in}
$Updated\ E_\Delta \longrightarrow \Delta_I$ (Output)
$Output\ Difference(\Delta_T) \& E_\Delta$
Input

Figure 1.12: Value phase of the TDA

Algorithm 3: Basic Procedure Value Phase of Target difference algorithm

```
   input  : $\Delta_T$: Target Input Difference, $E_\Delta$
   output: $M_1, \Delta_I$ such that
           $\texttt{Keccak}(M_1) \oplus \texttt{Keccak}(M_1 \oplus \Delta_I) = \Delta_T$ after one round.
1  $E_M = \{\}$
2  $exp = L^{-1}(X)$ where $X$ is set of $v$ variable
     $E_M = exp(c||p) == c||p$ here c and p is capacity and padding bits
     respectively.
3  for $t$ active sbox do
4      from $\Delta_T$ obtain $\delta^{out}$
5      find such $\delta_i^{in}$ which are consistent with $E_\Delta$ and sort them such
         that $DDT(\delta_i^{in}, \delta^{out}) \geq DDT(\delta_{i+1}^{in}, \delta^{out})$
6      for $\delta_i$ obtain the linear equations that define the affine subset
         $A(\delta_i^{in}; \delta^{out})$
7      Add equations to $E_M$
8      if $E_M$ is consistent then
9          Add equations for $\delta_i$ in $E_\Delta$ and go to step 4
10     end
11     else
12         check for $\delta_{i+1}$
13     end
14 end
```

Similar to the difference phase, the value phase has main procedure.

Algorithm 4: The Main Procedure of Value Phase

```
1  Intialize int counter = 0; int $T_2$; and obtain $E_\Delta$.
2  Excute the bascic procedure;
3  if the basic procedure of value phase succeeds then
4      output $E_\Delta$ and $E_M$;
5  end
6  else
7      counter++;
8      go to next step
9  end
10 if counter == $T_2$,"No Solution";.
11 Change the IDSD order by bringing the failed Sbox to the front and go
     to step excute the basic procedure 2 .
```

5 Discussion on 2D Affine Subspaces of Keccak S-box

An affine subset of a vector space V to be a subset of form

$$A = \{a + u \mid a \in V, u \in U\}$$

where U is a subspace of V.
Consider an input difference subset with every element of 5-bits. Now the cardinality of a 2-dimensional affine subspace should be 4. So, we get $(5-2) = 3$ equations from a 2-dimensional affine subspace.

For example, if we take an output difference 1 then the corresponding input difference set is $\{1,\ 3,\ 5,\ 7,\ 11,\ 15,\ 21,\ 23,\ 31\}$. If we consider the subset $\{1,\ 3,\ 5,\ 7\}$ then this subset forms a 2-dimensional affine subspace.
Example 1: Affine subsapce with three constants.

		x_1	x_2	x_3	x_4	x_5
1	$=$	0	0	0	0	1
3	$=$	0	0	0	1	1
5	$=$	0	0	1	0	1
7	$=$	0	0	1	1	1

Here we can see that $x_1 = 0;\ x_2 = 0;\ x_5 = 1$ and $x_3,\ x_4$ are variables. So, the subset $\{1,\ 3, 5,\ 7\}$ is an 2-dimensional affine subset. The affine equations for this affine subset are:

$$x_1 = 0$$
$$x_2 = 0$$
$$x_5 = 1$$

Example 2: Affine subspace with two constants and one linear equation.

		x_1	x_2	x_3	x_4	x_5
1	$=$	0	0	0	0	1
3	$=$	0	0	0	1	1
21	$=$	1	0	1	0	1
23	$=$	1	0	1	1	1

The affine equations for $\{1,\ 3, 21,\ 23\}$ are:

$$x_2 = 0$$
$$x_5 = 1$$
$$x_1 \oplus x_3 = 0$$

Example 3: Affine subspace with one constant and two linear equations

$$\begin{array}{ccccccc} & & x_1 & x_2 & x_3 & x_4 & x_5 \\ 1 & = & 0 & 0 & 0 & 0 & 1 \\ 11 & = & 0 & 1 & 0 & 1 & 1 \\ 21 & = & 1 & 0 & 1 & 0 & 1 \\ 31 & = & 1 & 1 & 1 & 1 & 1 \end{array}$$

The affine equations for $\{1,\ 3, 21,\ 23\}$ are:

$$\begin{aligned} x_5 &= 1 \\ x_1 \oplus x_3 &= 0 \\ x_2 \oplus x_4 &= 0 \end{aligned}$$

Example 4: Affine subspace with three linear equations.

$$\begin{array}{ccccccc} & & x_1 & x_2 & x_3 & x_4 & x_5 \\ 1 & = & 0 & 0 & 0 & 0 & 1 \\ 10 & = & 0 & 1 & 0 & 1 & 0 \\ 21 & = & 1 & 0 & 1 & 0 & 1 \\ 30 & = & 1 & 1 & 1 & 1 & 0 \end{array}$$

The affine equations for $\{1, 10, 21, 30\}$ are:

$$\begin{aligned} x_2 \oplus x_5 &= 1 \\ x_1 \oplus x_3 &= 0 \\ x_2 \oplus x_4 &= 0 \end{aligned}$$

Example 5: But, if we consider $\{1,\ 3,\ 11,\ 15\}$ then this subset does not form a 2-dimensional affine subspace.

$$\begin{array}{ccccccc} & & x_1 & x_2 & x_3 & x_4 & x_5 \\ 1 & = & 0 & 0 & 0 & 0 & 1 \\ 3 & = & 0 & 0 & 0 & 1 & 1 \\ 11 & = & 0 & 1 & 1 & 0 & 1 \\ 15 & = & 0 & 1 & 1 & 1 & 1 \end{array}$$

We can see that for this set $x_1 = 0$, $x_5 = 1$ but we can not get any linear equations from the variables. We find all the affine equations corresponding to all possible δ^{out}. The afiine equations corresponding to δ^{out} have been enumerated in Appendix D.

Property 1 [DDS12]. *For a non-zero 5-bit output difference δ^{out} to a* Keccak *S-box, the set of possible input differences, $\{\delta^{in} | DDT(\delta^{in}, \delta^{out}) > 0\}$, contains at least 5 (and up to 17) 2-dimensional affine subspaces.*

The above statement answers how many affine subspaces we can get from an input difference set corresponding to an output difference (δ^{out}). We have verified this statement practically. The number of 2-dimensional affine subspaces corresponding to all output differences is given in the Table 1.1.

Also, we need an order for choosing the affine subspaces. For that, we have to create another list named Input Difference Subset list (Refer Appendix C) for storing the affine subspaces with some order. The IDSLs are stored in the main Input Difference Subset Data structure (IDSD). The IDSD contains t entries (one entry per active S-box), sorted according to an IDSD order.

δ^{out}	# 2d AS	δ^{out}	# 2d AS
1	9	17	9
2	9	18	5
3	9	19	5
4	9	20	5
5	5	21	17
6	9	22	17
7	5	23	11
8	9	24	8
9	5	25	5
10	5	26	17
11	17	27	12
12	9	28	5
13	17	29	12
14	5	30	12
15	11	31	10
16	9		

Table 1.1: Number of 2D Affine Subspace (AS) of Keccak corresponding to All Output Difference

6 A Case Study of TDA on Keccak-50

In this Section, the difference phase and value phase will be discussed through an example i.e. we will take one output difference of length b, and then we will try to find the corresponding input difference amd message pairs . In KECCAK-$p[b, n_r]$, the width b must be 25, 50, 100, 200, 400, 800, or 1600 bits. But here we will take an output difference of length 50 bits. We consider the capacity $c = 10$. If the difference phase succeeds then we will store the system of equations E_Δ for the value phase. The difference phase and value phase will be discussed in the Section 6.1 and 6.2 respectively.

6.1 Difference Phase on Keccak-50

Input of this algorithm For $b = 50$, there are 2 slices. The output difference $\Delta_T =$

$$\begin{array}{ccccc} \multicolumn{5}{c}{\text{1st slice}} \\ [0 & 1 & 0 & 0 & 0] \\ [0 & 0 & 1 & 1 & 0] \\ [1 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{array} \qquad \begin{array}{ccccc} \multicolumn{5}{c}{\text{2nd slice}} \\ [0 & 1 & 0 & 0 & 1] \\ [1 & 0 & 1 & 0 & 1] \\ [1 & 0 & 0 & 1 & 0] \\ [0 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{array}$$

- Initialize an empty linear equation system E_Δ, with 50 variables for the unknown bits of $L(\Delta_I)$. Let $L(\Delta_I)$ is a set of 50 variables. Total there are 10 S-boxes and the number of slices is 2. The input of the S-boxes i.e. $L(\Delta_I)$ is:

$$\begin{array}{ccccc} \multicolumn{5}{c}{\text{1st slice}} \\ [x_{111} & x_{121} & x_{131} & x_{141} & x_{151}] \\ [x_{211} & x_{221} & x_{231} & x_{241} & x_{251}] \\ [x_{311} & x_{321} & x_{331} & x_{341} & x_{351}] \\ [x_{411} & x_{421} & x_{431} & x_{441} & x_{451}] \\ [x_{511} & x_{521} & x_{531} & x_{541} & x_{551}] \end{array} \qquad \begin{array}{ccccc} \multicolumn{5}{c}{\text{2nd slice}} \\ [x_{112} & x_{122} & x_{132} & x_{142} & x_{152}] \\ [x_{212} & x_{222} & x_{232} & x_{242} & x_{252}] \\ [x_{312} & x_{322} & x_{332} & x_{342} & x_{352}] \\ [x_{412} & x_{422} & x_{432} & x_{442} & x_{452}] \\ [x_{512} & x_{522} & x_{532} & x_{542} & x_{552}] \end{array}$$

- We considered the 50×50 matrix L, where $L = \rho \circ \pi \circ \theta$. At first, we are finding L^{-1}. Now we are multiplying L^{-1} with $L(\Delta_I)$ and getting Δ_I as a set of 50 expressions. Now from the observation we get last

$c = 10$ bits of Δ_I are zero. So we get 10 equations after equating the last 10 expressions of Δ_I with zero. We are storing all these equations in E_Δ.

- Now, we have Keccak S-boxes with input $L(\Delta_I)$ and output Δ_I. From the Δ_I we can see that there are total 3 (1st slice) $+\ 3$ (2nd slice)$=\ 6$ S-boxes are active and the remaining 4 S-boxes are non-active. For the non-active S-boxes, the input differences and output differences are zero. Since there are 4 non-active S-boxes. So we get 20 bits are zeroes in $L(\Delta_I)$ and store all these 20 equations in E_Δ. After adding these equations in E_Δ, we are checking that the system of equations E_Δ is consistent or not. Here the system of equations E_Δ becomes consistent. After putting 20 values in E_Δ, we get the following input difference $L(\Delta_I)$.

  $L(\Delta_I)$:

  $$\begin{array}{cc} \text{1st slice} & \text{2nd slice} \\ \begin{bmatrix} x_{111} & x_{121} & x_{131} & x_{141} & x_{151} \\ x_{211} & x_{221} & x_{231} & x_{241} & x_{251} \\ x_{311} & x_{321} & x_{331} & x_{341} & x_{351} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} x_{112} & x_{122} & x_{132} & x_{142} & x_{152} \\ x_{212} & x_{222} & x_{232} & x_{242} & x_{252} \\ x_{312} & x_{322} & x_{332} & x_{342} & x_{352} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

- Here, we have six active Keccak S-boxes. For an active S-boxes consider the output difference (δ^{out}) and corresponding input difference (δ^{in}), where DDT(δ^{in}, δ^{out}) > 0. Now from the DDT table we can find the possible input difference set. For example, if the output difference (δ^{out}) is 1 then the corresponding input difference set is $\{1,\ 3,\ 5,\ 7,\ 11,\ 15,\ 21,\ 23,\ 31\}$. After getting the input difference set, our next work is to find the possible 2-dimensional affine subspaces (Refer Section 5) from the input difference set. After obtaining the 2-dimensional affine subset we then narrow $5 - 2 = 3$ affine equations that defines this 5-bit input of current S-box to E_Δ. If E_Δ is consistent after adding these 3-affine equations in E_Δ, add the equations and continue to the next active S-box. Now if the E_Δ becomes inconsistent after adding these equations continue to the next affine subsets and so on. After the above procedure, the system of equations E_Δ becomes:

$x_{111} \oplus x_{112} \oplus x_{121} \oplus x_{122} \oplus x_{131} \oplus x_{142} \oplus x_{211} \oplus x_{231} \oplus x_{232} \oplus x_{241} \oplus$
$x_{242} \oplus x_{251} \oplus x_{311} \oplus x_{312} \oplus x_{322} \oplus x_{332} \oplus x_{352} = 0$
$x_{121} \oplus x_{122} \oplus x_{131} \oplus x_{132} \oplus x_{141} \oplus x_{151} \oplus x_{212} \oplus x_{221} \oplus x_{241} \oplus x_{242} \oplus$

$x_{251} \oplus x_{252} \oplus x_{311} \oplus x_{312} \oplus x_{321} \oplus x_{322} \oplus x_{331} \oplus x_{341} = 0$

$x_{111} \oplus x_{131} \oplus x_{132} \oplus x_{141} \oplus x_{142} \oplus x_{152} \oplus x_{211} \oplus x_{212} \oplus x_{222} \oplus x_{232} \oplus$
$x_{251} \oplus x_{321} \oplus x_{322} \oplus x_{331} \oplus x_{332} \oplus x_{342} \oplus x_{351} = 0$

$x_{112} \oplus x_{121} \oplus x_{141} \oplus x_{142} \oplus x_{151} \oplus x_{152} \oplus x_{211} \oplus x_{212} \oplus x_{221} \oplus x_{222} \oplus$
$x_{231} \oplus x_{242} \oplus x_{312} \oplus x_{331} \oplus x_{332} \oplus x_{341} \oplus x_{342} \oplus x_{352} = 0$

$x_{111} \oplus x_{112} \oplus x_{122} \oplus x_{132} \oplus x_{152} \oplus x_{221} \oplus x_{222} \oplus x_{231} \oplus x_{232} \oplus x_{241} \oplus$
$x_{252} \oplus x_{311} \oplus x_{321} \oplus x_{341} \oplus x_{342} \oplus x_{351} \oplus x_{352} = 0$

$x_{111} \oplus x_{112} \oplus x_{121} \oplus x_{122} \oplus x_{132} \oplus x_{141} \oplus x_{212} \oplus x_{231} \oplus x_{232} \oplus x_{241} \oplus$
$x_{242} \oplus x_{252} \oplus x_{311} \oplus x_{312} \oplus x_{321} \oplus x_{331} \oplus x_{351} = 0$

$x_{121} \oplus x_{122} \oplus x_{131} \oplus x_{132} \oplus x_{142} \oplus x_{152} \oplus x_{211} \oplus x_{222} \oplus x_{241} \oplus x_{242} \oplus$
$x_{251} \oplus x_{252} \oplus x_{311} \oplus x_{312} \oplus x_{321} \oplus x_{322} \oplus x_{332} \oplus x_{342} = 0$
$x_{112} \oplus x_{131} \oplus x_{132} \oplus x_{141} \oplus x_{142} \oplus x_{151} \oplus x_{211} \oplus x_{212} \oplus x_{221} \oplus x_{231} \oplus$
$x_{252} \oplus x_{321} \oplus x_{322} \oplus x_{331} \oplus x_{332} \oplus x_{341} \oplus x_{352} = 0$

$x_{111} \oplus x_{122} \oplus x_{141} \oplus x_{142} \oplus x_{151} \oplus x_{152} \oplus x_{211} \oplus x_{212} \oplus x_{221} \oplus x_{222} \oplus$
$x_{232} \oplus x_{241} \oplus x_{311} \oplus x_{331} \oplus x_{332} \oplus x_{341} \oplus x_{342} \oplus x_{351} = 0$

$x_{111} \oplus x_{112} \oplus x_{121} \oplus x_{131} \oplus x_{151} \oplus x_{221} \oplus x_{222} \oplus x_{231} \oplus x_{232} \oplus x_{242} \oplus$
$x_{251} \oplus x_{312} \oplus x_{322} \oplus x_{341} \oplus x_{342} \oplus x_{351} \oplus x_{352} = 0$
$x_{121} \oplus x_{131} = 1$
$x_{121} \oplus x_{141} = 1$
$x_{121} \oplus x_{151} = 1$
$x_{251} = 1$
$x_{211} \oplus x_{221} = 0$
$x_{211} \oplus x_{231} = 0$
$x_{321} = 0$
$x_{311} \oplus x_{331} = 1$
$x_{311} \oplus x_{351} = 1$
$x_{112} \oplus x_{122} = 0$
$x_{112} \oplus x_{142} = 1$
$x_{112} \oplus x_{152} = 0$
$x_{252} = 0$
$x_{242} = 1$
$x_{212} \oplus x_{232} = 1$
$x_{312} \oplus x_{332} = 1$
$x_{322} \oplus x_{342} = 0$

$x_{312} \oplus x_{322} \oplus x_{352} = 1$

The system of equations E_Δ has 28 equations and 30 variables. So, the solution of this system of equations is not unique. Then one of the solution i.e. $L(\Delta_I)$ is :

$$\begin{array}{ccccccccccc}
\multicolumn{5}{c}{\text{1st slice}} & & \multicolumn{5}{c}{\text{2nd slice}} \\
[0 & 1 & 0 & 0 & 1] & & [0 & 1 & 0 & 0 & 0] \\
[0 & 1 & 0 & 1 & 0] & & [1 & 1 & 1 & 1 & 1] \\
[1 & 0 & 0 & 0 & 0] & & [0 & 1 & 1 & 1 & 0] \\
[0 & 0 & 0 & 0 & 0] & & [0 & 0 & 0 & 0 & 0] \\
[0 & 0 & 0 & 0 & 0] & & [0 & 0 & 0 & 0 & 0]
\end{array}$$

Now, the output of the the differene phase is the system of equations E_Δ (Refer Algorithm 1). So we store the E_Δ for value phase.

.

6.2 Value Phase on Keccak-50

The inputs for the value phase are the system of equations E_Δ and Δ_T. We will discuss the algorithm for this phase with an example in detail and update our system of equations. Then we will get updated Δ_I and messages pairs.

- Similar to the difference phase, we initialize empty linear equations system E_M with 50 variables for the unknown bits of $L(\bar{M}^1)$.
  $L(\bar{M}^1)$:

$$\begin{array}{ccccccccccc}
\multicolumn{5}{c}{\text{1st slice}} & & \multicolumn{5}{c}{\text{2nd slice}} \\
[m_{111} & m_{121} & m_{131} & m_{141} & m_{151}] & & [m_{112} & m_{122} & m_{132} & m_{142} & m_{152}] \\
[m_{211} & m_{221} & m_{231} & m_{241} & m_{251}] & & [m_{212} & m_{222} & m_{232} & m_{242} & m_{252}] \\
[m_{311} & m_{321} & m_{331} & m_{341} & m_{351}] & & [m_{312} & m_{322} & m_{332} & m_{342} & m_{352}] \\
[m_{411} & m_{421} & m_{431} & m_{441} & m_{451}] & & [m_{412} & m_{422} & m_{432} & m_{442} & m_{452}] \\
[m_{511} & m_{521} & m_{531} & m_{541} & m_{551}] & & [m_{512} & m_{522} & m_{532} & m_{542} & m_{552}]
\end{array}$$

- We know that L is 50×50 matrix , where $L = \rho \circ \pi \circ \theta$. At first, we are finding L^{-1}. Now we are multiplying L^{-1} with $L(\bar{M}^1)$ and getting $\bar{M}^1$ as a set of 50 expressions. Now from the observation we get last

$c = 10$ (capacity part) bits of $\bar{M}^1$ are zero. So we get 10 equations after equating the last 10 expressions of $\bar{M}^1$ with zero. We storing all these equations in E_M.

- From the Δ_T, we are collecting the 6 active S-boxes. The active S-boxes are in decimal format $\{8, 6, 16, 9, 21, 18\}$. We iterate the 6 active S-boxes according to the IDSD order.

- Let us consider the first S-box is $\delta^{out} = 8$ (in binary) and finding the input differences (δ^{in}) such that $DDT(\delta^{in}, \delta^{out}) > 0$. The input difference set corresponding to 8 is $\{8, 9, 13, 24, 26, 25, 27, 29, 31\}$. Then we obtain all the S-box input differences that are consistent with E_Δ, denoting the set $\{\delta_i^{in}\}$ and sorting the δ^{in}'s in descending order according to DDT value (Table B). The consistent input differences are $\{8, 9, 24, 25\}$.

Property 2 [**DDS12**]. *Given a 5-bit input difference and 5-bit output difference δ^{out} to a* Keccak *S-box such that DDT(δ^{in}, δ^{out})> 0, denote the valuation set $V = \{x : S(x) + S(x + \delta^{in}) = \delta^{out}\}$ forms an affine subset and denoting the subset $A(\delta^{in}, \delta^{out})$.*

- We iterate the above consistent input differences one by one. Take $\delta_1^{in} = 8$. Then We are adding the linear equations $A(\delta_1^{in}, \delta^{out}) = A(8, 8)$ to E_M. The valuation set for input difference 8 and output difference 8 is $\{16, 17, 18, 19, 24, 25, 26, 27\}$.

		x_1	x_2	x_3	x_4	x_5
16	$=$	1	0	0	0	0
17	$=$	1	0	0	0	1
18	$=$	1	0	0	1	0
19	$=$	1	0	0	1	1
24	$=$	1	1	0	0	0
25	$=$	1	1	0	0	1
26	$=$	1	1	0	1	0
27	$=$	1	1	0	1	1

The equations are $x_1 = 1$ and $x_3 = 0$. If these equations are consistent with E_M then add these equations to E_M. In addition, add the additional equations $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0, x_5 = 0$ for the input difference 8, to E_Δ.
Otherwise, continue to the next input difference 9 and proceed the above

way. If no more input differences remain, output "No Solution".

- After iterating all the active S-boxes and their corresponding input differences which are consistent with E_Δ, the two systems of equations E_M and E_Δ is updated. From the E_Δ we get Δ_I and message pairs.
  E_M :

  $$\begin{gathered} m_{111}\oplus m_{112}\oplus m_{121}\oplus m_{122}\oplus m_{131}\oplus m_{142}\oplus m_{211}\oplus m_{231}\oplus m_{232}\oplus m_{241}\oplus \\ m_{242}\oplus m_{251}\oplus m_{311}\oplus m_{312}\oplus m_{322}\oplus m_{332}\oplus m_{352}\oplus m_{421}\oplus m_{422}\oplus m_{431}\oplus \\ m_{432}\oplus m_{441}\oplus m_{451}\oplus m_{512}\oplus m_{522}\oplus m_{541}\oplus m_{542}\oplus m_{551}\oplus m_{552} = 0, \end{gathered}$$

  $$\begin{gathered} m_{121}\oplus m_{122}\oplus m_{131}\oplus m_{132}\oplus m_{141}\oplus m_{151}\oplus m_{212}\oplus m_{221}\oplus m_{241}\oplus m_{242}\oplus \\ m_{251}\oplus m_{252}\oplus m_{311}\oplus m_{312}\oplus m_{321}\oplus m_{322}\oplus m_{331}\oplus m_{341}\oplus m_{412}\oplus m_{431}\oplus \\ m_{432}\oplus m_{441}\oplus m_{442}\oplus m_{452}\oplus m_{511}\oplus m_{512}\oplus m_{521}\oplus m_{532}\oplus m_{552} = 0, \end{gathered}$$

  $$\begin{gathered} m_{111}\oplus m_{131}\oplus m_{132}\oplus m_{141}\oplus m_{142}\oplus m_{152}\oplus m_{211}\oplus m_{212}\oplus m_{222}\oplus m_{232}\oplus \\ m_{251}\oplus m_{321}\oplus m_{322}\oplus m_{331}\oplus m_{332}\oplus m_{342}\oplus m_{351}\oplus m_{411}\oplus m_{421}\oplus m_{441}\oplus \\ m_{442}\oplus m_{451}\oplus m_{452}\oplus m_{511}\oplus m_{512}\oplus m_{521}\oplus m_{522}\oplus m_{531}\oplus m_{542} = 0, \end{gathered}$$

  $$\begin{gathered} m_{112}\oplus m_{121}\oplus m_{141}\oplus m_{142}\oplus m_{151}\oplus m_{152}\oplus m_{211}\oplus m_{212}\oplus m_{221}\oplus m_{222}\oplus \\ m_{231}\oplus m_{242}\oplus m_{312}\oplus m_{331}\oplus m_{332}\oplus m_{341}\oplus m_{342}\oplus m_{352}\oplus m_{411}\oplus m_{412}\oplus \\ m_{422}\oplus m_{431}\oplus m_{452}\oplus m_{521}\oplus m_{522}\oplus m_{531}\oplus m_{532}\oplus m_{541}\oplus m_{551} = 0, \end{gathered}$$

  $$\begin{gathered} m_{111}\oplus m_{112}\oplus m_{122}\oplus m_{132}\oplus m_{152}\oplus m_{221}\oplus m_{222}\oplus m_{231}\oplus m_{232}\oplus m_{241}\oplus \\ m_{252}\oplus m_{311}\oplus m_{321}\oplus m_{341}\oplus m_{342}\oplus m_{351}\oplus m_{352}\oplus m_{411}\oplus m_{412}\oplus m_{421}\oplus \\ m_{422}\oplus m_{432}\oplus m_{442}\oplus m_{511}\oplus m_{531}\oplus m_{532}\oplus m_{541}\oplus m_{542}\oplus m_{552} = 0, \end{gathered}$$

  $$\begin{gathered} m_{111}\oplus m_{112}\oplus m_{121}\oplus m_{122}\oplus m_{132}\oplus m_{141}\oplus m_{212}\oplus m_{231}\oplus m_{232}\oplus m_{241}\oplus \\ m_{242}\oplus m_{252}\oplus m_{311}\oplus m_{312}\oplus m_{321}\oplus m_{331}\oplus m_{351}\oplus m_{421}\oplus m_{422}\oplus m_{431}\oplus \\ m_{432}\oplus m_{442}\oplus m_{452}\oplus m_{511}\oplus m_{521}\oplus m_{541}\oplus m_{542}\oplus m_{551}\oplus m_{552} = 0, \end{gathered}$$

  $$\begin{gathered} m_{121}\oplus m_{122}\oplus m_{131}\oplus m_{132}\oplus m_{142}\oplus m_{152}\oplus m_{211}\oplus m_{222}\oplus m_{241}\oplus m_{242}\oplus \\ m_{251}\oplus m_{252}\oplus m_{311}\oplus m_{312}\oplus m_{321}\oplus m_{322}\oplus m_{332}\oplus m_{342}\oplus m_{411}\oplus m_{431}\oplus \\ m_{432}\oplus m_{441}\oplus m_{442}\oplus m_{451}\oplus m_{511}\oplus m_{512}\oplus m_{522}\oplus m_{531}\oplus m_{551} = 0, \end{gathered}$$

  $$\begin{gathered} m_{112}\oplus m_{131}\oplus m_{132}\oplus m_{141}\oplus m_{142}\oplus m_{151}\oplus m_{211}\oplus m_{212}\oplus m_{221}\oplus m_{231}\oplus \\ m_{252}\oplus m_{321}\oplus m_{322}\oplus m_{331}\oplus m_{332}\oplus m_{341}\oplus m_{352}\oplus m_{412}\oplus m_{422}\oplus m_{441}\oplus \\ m_{442}\oplus m_{451}\oplus m_{452}\oplus m_{511}\oplus m_{512}\oplus m_{521}\oplus m_{522}\oplus m_{532}\oplus m_{541} = 0, \end{gathered}$$

  $$\begin{gathered} m_{111}\oplus m_{122}\oplus m_{141}\oplus m_{142}\oplus m_{151}\oplus m_{152}\oplus m_{211}\oplus m_{212}\oplus m_{221}\oplus m_{222}\oplus \\ m_{232}\oplus m_{241}\oplus m_{311}\oplus m_{331}\oplus m_{332}\oplus m_{341}\oplus m_{342}\oplus m_{351}\oplus m_{411}\oplus m_{412}\oplus \end{gathered}$$

$m_{421} \oplus m_{432} \oplus m_{451} \oplus m_{521} \oplus m_{522} \oplus m_{531} \oplus m_{532} \oplus m_{542} \oplus m_{552} = 0,$

$m_{111} \oplus m_{112} \oplus m_{121} \oplus m_{131} \oplus m_{151} \oplus m_{221} \oplus m_{222} \oplus m_{231} \oplus m_{232} \oplus m_{242} \oplus$
$m_{251} \oplus m_{312} \oplus m_{322} \oplus m_{341} \oplus m_{342} \oplus m_{351} \oplus m_{352} \oplus m_{411} \oplus m_{412} \oplus m_{421} \oplus$
$m_{422} \oplus m_{431} \oplus m_{441} \oplus m_{512} \oplus m_{531} \oplus m_{532} \oplus m_{541} \oplus m_{542} \oplus m_{551} = 0,$
$m_{111} = 0,$
$m_{131} = 0,$
$m_{141} = 1,$
$m_{231} = 1,$
$m_{251} = 1,$
$m_{321} = 0,$
$m_{351} = 0,$
$m_{331} = 1,$
$m_{112} = 0,$
$m_{132} = 0,$
$m_{212} \oplus m_{222} = 0,$
$m_{212} \oplus m_{232} = 0,$
$m_{212} \oplus m_{242} = 1,$
$m_{212} \oplus m_{252} = 1,$
$m_{312} = 1,$
$m_{352} = 1,$
$m_{322} \oplus m_{332} = 1,$
$m_{322} \oplus m_{342} = 0.$

After solving the system of equations we get one of the messages.
$\bar{M}^1$:

1st slice

$$\begin{matrix} [0 & 1 & 1 & 0 & 0] \\ [1 & 1 & 0 & 0 & 0] \\ [1 & 0 & 0 & 1 & 0] \\ [0 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{matrix}$$

2nd slice

$$\begin{matrix} [1 & 0 & 1 & 1 & 0] \\ [1 & 0 & 1 & 1 & 1] \\ [0 & 0 & 1 & 1 & 0] \\ [1 & 0 & 1 & 1 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{matrix}$$

The additional equations which are adding with the previous E_{Δ}:

$x_{111} = 0,\ x_{131} = 0, x_{141} = 0, x_{121} = 1, x_{151} = 1,$
$x_{211} = 0,\ x_{221} = 0, x_{231} = 0, x_{251} = 0, x_{241} = 1,$
$x_{321} = 0, x_{331} = 0, x_{351} = 0, x_{311} = 1, x_{341} = 1,$
$x_{112} = 0, x_{132} = 0, x_{142} = 0, x_{152} = 0, x_{122} = 1,$
$x_{212} = 1, x_{222} = 1, x_{232} = 1, x_{242} = 1, x_{252} = 1,$
$x_{312} = 0, x_{352} = 0, x_{322} = 1, x_{332} = 1, x_{342} = 1.$

Now we can find the input difference from updated E_Δ.
Δ_I :

$$\begin{array}{ccccccccccc} \multicolumn{5}{c}{\text{1st slice}} & \quad & \multicolumn{5}{c}{\text{2nd slice}} \\ [0 & 0 & 1 & 0 & 1] & & [0 & 1 & 0 & 1 & 0] \\ [0 & 1 & 1 & 0 & 1] & & [0 & 1 & 1 & 0 & 1] \\ [1 & 0 & 1 & 1 & 1] & & [0 & 0 & 0 & 0 & 0] \\ [0 & 1 & 1 & 0 & 0] & & [0 & 1 & 0 & 0 & 1] \\ [0 & 0 & 0 & 0 & 0] & & [0 & 0 & 0 & 0 & 0] \end{array}$$

Then $\bar{M^2}$:

$$\begin{array}{ccccccccccc} \multicolumn{5}{c}{\text{1st slice}} & \quad & \multicolumn{5}{c}{\text{2nd slice}} \\ [0 & 1 & 0 & 0 & 1] & & [1 & 1 & 1 & 0 & 0] \\ [1 & 0 & 1 & 0 & 1] & & [1 & 1 & 0 & 1 & 0] \\ [0 & 0 & 1 & 0 & 1] & & [0 & 0 & 1 & 1 & 0] \\ [0 & 1 & 1 & 0 & 0] & & [1 & 1 & 1 & 1 & 1] \\ [0 & 0 & 0 & 0 & 0] & & [0 & 0 & 0 & 0 & 0] \end{array}$$

So finally we get one message pair for given Δ_T. But the system of equations E_Δ and E_M both have more than one solution. So we may get more than one message pair and Δ_I corresponding an Δ_T.

6.3 Verification of Correctness

To verify, we run one round KECCAK on both the messages M^1 (Refer 6.2) and M^2 (Refer 6.2).

$Keccak^1(\bar{M^1}) =$

$$\begin{array}{ccccccccccc} \multicolumn{5}{c}{\text{1st slice}} & \quad & \multicolumn{5}{c}{\text{2nd slice}} \\ [0 & 0 & 0 & 1 & 1] & & [0 & 0 & 0 & 0 & 0] \\ [1 & 0 & 0 & 0 & 1] & & [1 & 1 & 1 & 1 & 0] \\ [1 & 0 & 1 & 0 & 0] & & [0 & 0 & 0 & 0 & 1] \\ [0 & 1 & 0 & 0 & 1] & & [0 & 0 & 0 & 0 & 0] \\ [1 & 1 & 0 & 1 & 0] & & [0 & 0 & 0 & 0 & 0] \end{array}$$

$Keccak^1(\bar{M^2}) =$

$$\begin{array}{cc} \text{1st slice} & \text{2nd slice} \\ \begin{array}{ccccc} [0 & 1 & 0 & 1 & 1] \\ [1 & 0 & 1 & 1 & 1] \\ [0 & 0 & 1 & 0 & 0] \\ [0 & 1 & 0 & 0 & 1] \\ [1 & 1 & 0 & 1 & 0] \end{array} & \begin{array}{ccccc} [0 & 1 & 0 & 0 & 1] \\ [0 & 1 & 0 & 1 & 1] \\ [1 & 0 & 0 & 1 & 1] \\ [0 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{array} \end{array}$$

$$Keccak^1(\bar{M}^1) \oplus Keccak^1(\bar{M}^2) =$$

$$\begin{array}{cc} \text{1st slice} & \text{2nd slice} \\ \begin{array}{ccccc} [0 & 1 & 0 & 0 & 0] \\ [0 & 0 & 1 & 1 & 0] \\ [1 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{array} & \begin{array}{ccccc} [0 & 1 & 0 & 0 & 1] \\ [1 & 0 & 1 & 0 & 1] \\ [1 & 0 & 0 & 1 & 0] \\ [0 & 0 & 0 & 0 & 0] \\ [0 & 0 & 0 & 0 & 0] \end{array} \end{array}$$

which is equal to given Δ_T (Refer Section 6.1).

7 Searching the 2D Affine Subspaces of Ascon S-box

Dinur *et al.* stated that for Keccak, there are minimum 5 and maximum 17, 2-dimensional affine subspace for fixed δ^{out}. We have verified this property in the Section 5 using a searching algorithm implemented in Matlab. The degree of Keccak S-box is 2. Since the degree of the Ascon S-box is also 2, so we can study the number of minimum and maximum 2-dimensional affine subspaces for a fixed output difference of Ascon S-box. We use a similar implementation in Matlab to find the 2D affine subspaces (AS) and affine equations (AE). Then we get a new property for Ascon.

Property 3. *For a non-zero 5-bit output difference δ^{out} to a* Ascon *S-box, the set of possible input differences, $\{\delta^{in} | DDT(\delta^{in}, \delta^{out}) > 0\}$, contains at least 4 (and up to 17) 2-dimensional affine subspaces.*

The maximum number of 2D affine subspaces of both Keccak and Ascon S-box is 17. It is interesting to see that the minimum number of 2D affine subspaces for Ascon S-box is 4 but for Keccak S-box it was 5. The number of affine subspaces corresponding to all output differences are available in the Table 1.2. We have enumerated all the 2D affine subspaces and affine equations of the Ascon S-box. Most of them affine subspaces are enumerates in the Appendix D.

Example 1:
The output difference 18 has 17 (maximum) 2D affine subspaces. The input difference set corresponding to 17 is $\{$14, 23, 28, 31, 9, 10, 11, 13, 18, 22, 26, 27$\}$. Consider the subset $\{$14, 23, 11, 18$\}$.

$$\begin{array}{ccccccc} & & x_1 & x_2 & x_3 & x_4 & x_5 \\ 14 & = & 0 & 1 & 1 & 1 & 0 \\ 23 & = & 1 & 0 & 1 & 1 & 1 \\ 11 & = & 0 & 1 & 0 & 1 & 1 \\ 18 & = & 1 & 0 & 0 & 1 & 0 \end{array}$$

The the affine equations are:

$$\begin{aligned} x_4 &= 1 \\ x_1 \oplus x_2 &= 1 \\ x_1 \oplus x_3 \oplus x_5 &= 1 \end{aligned}$$

So, the subset $\{$14, 23, 11, 18$\}$ is a 2D affine subspace.

Example 2:
The output difference 30 has 4 (minimum) 2D affine subspaces. The input difference set corresponding to 17 is $\{$4, 1, 8, 25, 9, 11, 18, 22, 24, 30$\}$. Consider the subset $\{$4, 8, 18, 30$\}$.

$$\begin{array}{ccccccc} & & x_1 & x_2 & x_3 & x_4 & x_5 \\ 4 & = & 0 & 0 & 1 & 0 & 0 \\ 8 & = & 0 & 1 & 0 & 0 & 0 \\ 18 & = & 1 & 0 & 0 & 1 & 0 \\ 30 & = & 1 & 1 & 1 & 1 & 0 \end{array}$$

The the affine equations are:

$$\begin{aligned} x_5 &= 0 \\ x_1 \oplus x_4 &= 0 \\ x_1 \oplus x_2 \oplus x_3 &= 1 \end{aligned}$$

This is an example of 2D affine subspce corresponding to output difference 30.

δ^{out}	# 2d AS	δ^{out}	# 2d AS
1	5	17	9
2	9	18	17
3	11	19	9
4	8	20	11
5	9	21	5
6	8	22	5
7	11	23	5
8	9	24	9
9	8	25	5
10	5	26	5
11	5	27	16
12	5	28	17
13	8	29	11
14	9	30	4
15	16	31	15
16	8		

Table 1.2: Number of 2D Affine Subspace (AS) of Ascon corresponding to All Output Difference

8 Experimental Setup

We have implemented the TDA in Matlab platform. We ran our code on 64-bit intel-i3 CPU with 4 GB RAM machine. Our code is working on all the Keccak versions except the lanesize 64. For lanesize 64, the machine stops responding. Our code is able to finds the message pairs within 2 minutes for lanesize 2, 4, 8. But for the lanesize 16 and 32, it takes near about 20 minutes and 5 hours respectively. Also we find all the 2D affine subspaces of Keccak and Ascon S-box using a searching algorithm in Matlab.

9 Conclusion and Future Work

In this work, we have understood and implemented the diference phase and value phase of TDA on Keccak. We implemented the searching algorithm to enumerate the 2D affine subspace of the Keccak S-box and verified the property reported by Dinur *et al.* in the work where they introduced TDA. We applied the algorithm on the Ascon S-box and discovered a new property of the Ascon

S-box with respect to the number of 2D affine subspaces. All implementations are done in the Matlab platform. Since the sequence of linear layer and non-layer is reverse, so that TDA has to be adapted before applied to Ascon which will be an interesting work for the future. Another interesting aspect would be improved the TDA itself. Finally, TDA is an interesting cryptanalyst tool and understanding it, will help to apply it to other ciphers as well..

Bibliography

[BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and GV Assche. The keccak reference, version 3.0. *NIST SHA3 Submission Document (January 2011)*, 2011. 9

[BDPVA07] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sponge functions. In *ECRYPT hash workshop*, volume 2007. Citeseer, 2007. 1

[BDPVA09] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak specifications. *Submission to NIST (round 2)*, pages 320–337, 2009. 1, 2

[DDS12] Itai Dinur, Orr Dunkelman, and Adi Shamir. New attacks on keccak-224 and keccak-256. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 442–461. Springer, 2012. 1, 7, 8, 9, 12, 19, 24

[DDS13] Itai Dinur, Orr Dunkelman, and Adi Shamir. Collision attacks on up to 5 rounds of sha-3 using generalized internal differentials. In *International Workshop on Fast Software Encryption*, pages 219–240. Springer, 2013. 11

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1. 2. *Submission to the CAESAR Competition*, 2016. 5, 6, 7

[DGPW12] Alexandre Duc, Jian Guo, Thomas Peyrin, and Lei Wei. Unaligned rebound attack: application to keccak. In *International Workshop on Fast Software Encryption*, pages 402–421. Springer, 2012. 8

[Dwo15] Morris Dworkin. Sha-3 standard: Permutation-based hash and extendable-output functions, 2015-08-04 2015. 2, 3, 4, 5

[GJMG11] B Guido, D Joan, P Michaël, and VA Gilles. The Keccak SHA-3 Submission. 2011. 1

[GLL^{+}20] Jian Guo, Guohong Liao, Guozhen Liu, Meicheng Liu, Kexin Qiao, and Ling Song. Practical collision attacks against round-reduced sha-3. *Journal of Cryptology*, 33(1):228–270, 2020. 8, 9, 10

[KSPC14] Sukhendu Kuila, Dhiman Saha, Madhumangal Pal, and Dipanwita Roy Chowdhury. Practical distinguishers against 6-round keccak-f exploiting self-symmetry. In David Pointcheval and Damien Vergnaud, editors, *Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, volume 8469 of *Lecture Notes in Computer Science*, pages 88–108. Springer, 2014. 11

[QSLG17] Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo. New collision attacks on round-reduced keccak. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 216–243. Springer, 2017. 8, 9

[SMY^{+}12] George Sugihara, Robert May, Hao Ye, Chih-hao Hsieh, Ethan Deyle, Michael Fogarty, and Stephan Munch. Detecting causality in complex ecosystems. *science*, 338(6106):496–500, 2012. 1

Appendices

A Differential Distribution Table (DDT) of Keccak S-box

The χ mapping of Keccak takes a 5-bit input and gives 5-bit output. So the size of DDT is 32×32. Output difference left to right and input difference up to down :

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	8	0	8	0	8	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	8	0	0	0	8	0	0	0	8	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0
5	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4
6	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0
7	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
8	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	4	0	0	4	4	0	0	4	0	0	0	0	0	0	0	0	4	0	0	4	4	0	0	4
10	0	0	4	4	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4
11	0	4	4	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0
12	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0
13	0	0	0	0	4	0	0	4	4	0	0	4	0	0	0	0	0	0	0	0	4	0	0	4	4	0	0	4	0	0	0	0
14	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
15	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	8	8	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4	4	4	4	4	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	0	0	4	4	4	4	0	0	0	0	4	4
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
20	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4
21	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4	0
22	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0
23	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0
24	0	0	0	0	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4	0	0	0	0
25	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2
26	0	0	0	0	0	0	0	0	4	4	0	0	0	0	4	4	4	4	0	0	0	0	4	4	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0
28	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
29	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0
30	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
31	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2

B DDT of Ascon S-box

The S-box of `Ascon` takes a 5-bit input and gives 5-bit output. So the size of DDT is 32×32. Output difference left to right and input difference up to down :

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4
3	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0
4	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	4	4	0	4	0	4	0	4	0	0	4	0	4
6	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
7	0	0	4	4	0	0	4	4	0	0	4	4	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4
9	0	2	0	2	2	0	2	0	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2	0	2	0	2	2	0	2	0
10	0	2	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0	0	2
11	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
12	0	8	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0
13	0	2	0	2	0	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	0	2	0	2	0	2	0	2
14	0	4	4	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4	0	4	0	0	4	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0	0
16	0	0	0	0	0	0	0	0	0	8	0	8	0	0	0	0	0	0	0	0	0	0	0	0	8	0	8	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	8	0	8	0	8	0	0	0	0	0	0	0	0
18	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0
19	0	0	8	0	8	0	0	0	0	0	8	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	4	4	4	4	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	4	0	4	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
23	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0
24	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
25	0	0	0	4	0	0	4	0	4	0	0	0	0	4	0	0	4	0	0	0	0	4	0	0	0	0	0	4	0	0	4	0
26	0	2	2	0	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2	2	0	0	2
27	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
28	0	4	0	4	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0	0	0
29	0	0	0	4	0	4	0	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	0	0	0	4	0	4	0	0
30	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2
31	0	0	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0	0	0

C Input Difference Subset List

- Let Δ_T contains t active Sboxes and the corresponding output differences of Sboxes are $\delta_1^{out}, \delta_2^{out}, \ldots, \delta_t^{out}$.
- Consider δ_1^{out} and let the input difference set is $\{\delta_{11}^{in},\, \delta_{12}^{in},\, \delta_{13}^{in} \ldots \}$ where DDT($\delta_{1i}^{in},\, \delta_1^{out}$) > 0.
- Let the IDSL of the output difference δ_1^{out} is $IDSL_1$.
- At first we want to compare two input difference subsets $\{\delta_{11}^{in}, \delta_{12}^{in}, \delta_{13}^{in}, \delta_{14}^{in}\}$ and $\{\delta_{15}^{in}, \delta_{16}^{in}, \delta_{17}^{in}, \delta_{18}^{in}\}$ such that

$$DDT(\delta_{11}^{in}, \delta_1^{out}) \geq DDT(\delta_{12}^{in}, \delta_1^{out}) \geq DDT(\delta_{13}^{in}, \delta_1^{out}) \geq DDT(\delta_{14}^{in}, \delta_1^{out}) > 0$$

and

$$DDT(\delta_{15}^{in}, \delta_1^{out}) \geq DDT(\delta_{16}^{in}, \delta_1^{out}) \geq DDT(\delta_{17}^{in}, \delta_1^{out}) \geq DDT(\delta_{18}^{in}, \delta_1^{out}) > 0$$

.

- We first compare the sizes of the largest subset for which the size is bigger. If the sizes are equal , we compare DDT(δ_{12}^{in}, δ_1^{out}) and DDT(δ_{16}^{in}, δ_1^{out}), and so on. For example , let the output difference is 1 the from the DDT we get input difference set $\{1, 3, 5, 7, 11, 15, 21, 23, 31\}$ with

$$\begin{aligned} DDT(1,1) = 8, DDT(3,1) = 4, \quad & DDT(5,1) = 4, \\ DDT(7,1) = 2, DDT(11,1) = 4, \quad & DDT(15,1) = 2, \\ DDT(21,1) = 4, DDT(23,1) = 2, \quad & DDT(31,31) = 2. \end{aligned}$$

- IDSL = {{1, 3, 5, 11},{1, 3, 5, 21}, {1, 3, 5, 7}, {1, 3, 5, 15}, . . . }. In the above way we get IDSLs with respect to the output difference.

- Let $IDSL_1$, $IDSL_2$,. . . ,$IDSL_t$ are the IDSLs of the active Sboxes δ_1^{out}, δ_2^{out},. . . , δ_t^{out} respectively.

- All the IDSLs and output differences are stored in one data structure named IDSD. The number of element in IDSD is equal to t. IDSD is used for maintaining the order of Sboxes .

D List of 2D Affine Subspaces and Affine Equations of Keccak and Ascon.

Here we will give the possible 2 -dimensional affine subspaces and affine equations corresponding to output differences of Keccak and Ascon. From Table .3 to Table .11 are the tables for 2 -dimensional affine subspaces and affine equations of output differences for Keccak and the remaning tables are for Ascon .

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
1	{1, 3, 5, 7}	$x_1 = 0$, $x_2 = 0$, $x_5 = 1$
	{1, 3, 21, 23}	$x_2 = 0$, $x_5 = 1$, $x_1 \oplus x_3 = 0$
	{1, 5, 11, 15}	$x_1 = 0$, $x_5 = 1$, $x_2 \oplus x_4 = 0$
	{1, 11, 21, 31}	$x_5 = 1$, $x_1 \oplus x_3 = 0$, $x_2 \oplus x_4 = 0$
	{3, 11, 7, 15}	$x_1 = 0$, $x_4 = 1$, $x_5 = 1$
	{3, 11, 23, 31}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_3 = 0$
	{5, 21, 7, 23}	$x_2 = 0$, $x_3 = 1$, $x_5 = 1$
	{5, 21, 15, 31}	$x_3 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 0$
	{7, 15, 23, 31}	$x_3 = 1$, $x_4 = 1$, $x_5 = 1$
2	{2, 6, 10, 14}	$x_1 = 0$, $x_5 = 0$, $x_4 = 1$
	{2, 6, 11, 15}	$x_1 = 0$, $x_4 = 1$, $x_2 \oplus x_5 = 0$
	{2, 10, 22, 30}	$x_5 = 0$, $x_4 = 1$, $x_1 \oplus x_3 = 0$
	{2, 11, 22, 31}	$x_4 = 1$, $x_1 \oplus x_3 = 0$, $x_2 \oplus x_5 = 0$
	{6, 22, 14, 30}	$x_5 = 0$, $x_3 = 1$, $x_4 = 1$
	{6, 22, 15, 31}	$x_4 = 1$, $x_3 = 1$, $x_2 \oplus x_5 = 0$
	{10, 11, 14, 15}	$x_1 = 0$, $x_2 = 1$, $x_4 = 1$
	{10, 11, 30, 31}	$x_2 = 1$, $x_4 = 1$, $x_1 \oplus x_3 = 0$
	{14, 15, 30, 31}	$x_3 = 1$, $x_4 = 1$, $x_2 = 1$
3	{1, 3, 5, 7}	$x_1 = 0$, $x_2 = 0$, $x_5 = 1$
	{1, 3, 21, 23}	$x_2 = 0$, $x_5 = 1$, $x_1 \oplus x_3 = 0$
	{1, 5, 10, 14}	$x_1 = 0$, $x_2 \oplus x_4 = 0$, , $x_2 \oplus x_5 = 1$
	{1, 10, 21, 30}	$x_2 \oplus x_5 = 1$, $x_1 \oplus x_3 = 0$, $x_2 \oplus x_4 = 0$
	{3, 10, 7, 14}	$x_1 = 0$, $x_4 = 1$, $x_2 \oplus x_5 = 1$
	{3, 10, 23, 30}	$x_4 = 1$, $x_2 \oplus x_5 = 1$, $x_1 \oplus x_3 = 0$
	{5, 21, 7, 23}	$x_2 = 0$, $x_3 = 1$, $x_5 = 1$
	{5, 21, 14, 30}	$x_3 = 1$, $x_2 \oplus x_5 = 1$, $x_2 \oplus x_4 = 0$
	{7, 14, 23, 30}	$x_3 = 1$, $x_4 = 1$, $x_2 \oplus x_5 = 1$
4	{4, 12, 20, 28}	$x_4 = 0$, $x_5 = 0$, $x_3 = 1$
	{4, 12, 22, 30}	$x_5 = 0$, $x_3 = 1$, $x_1 \oplus x_4 = 0$
	{4, 13, 20, 29}	$x_4 = 0$, $x_3 = 1$, , $x_2 \oplus x_5 = 0$
	{4, 13, 22, 31}	$x_2 \oplus x_5 = 0$, $x_3 = 0$, $x_1 \oplus x_4 = 0$
	{12, 13, 28, 29}	$x_4 = 0$, $x_3 = 1$, $x_2 = 1$
	{12, 13, 30, 31}	$x_3 = 1$, $x_2 = 1$, $x_1 \oplus x_4 = 0$
	{20, 22, 28, 30}	$x_5 = 0$, $x_3 = 1$, $x_1 = 1$
	{20, 22, 29, 31}	$x_3 = 1$, $x_2 \oplus x_5 = 0$, $x_1 = 1$
	{28, 29, 30, 31}	$x_3 = 1$, $x_1 = 1$, $x_2 = 1$

Table .3: List of all 2D Affine Equations of Keccak for δ^{out}= 1, 2, 3, 4.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
5	$\{1, 3, 28, 30\}$	$x_1 \oplus x_2 = 0$, $x_1 \oplus x_3 = 0$, $x_1 \oplus x_5 = 1$
	$\{1, 11, 23, 29\}$	$x_5 = 1$, $x_1 \oplus x_3 = 0$, $x_1 \oplus x_2 \oplus x_4 = 0$
	$\{3, 11, 7, 15\}$	$x_1 = 0$, $x_4 = 1$, $x_5 = 1$
	$\{12, 7, 23, 28\}$	$x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_5 = 1$
	$\{12, 15, 29, 30\}$	$x_2 = 1$, $x_3 = 1$, $x_1 \oplus x_4 \oplus x_5 = 0$
6	$\{2, 6, 10, 14\}$	$x_1 = 0$, $x_5 = 0$, $x_4 = 1$
	$\{2, 6, 11, 15\}$	$x_1 = 0$, $x_4 = 1$, $x_2 \oplus x_5 = 0$
	$\{2, 10, 20, 28\}$	$x_5 = 0$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 = 0$
	$\{2, 11, 20, 29\}$	$x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 = 0$, $x_2 \oplus x_5 = 0$
	$\{6, 20, 14, 28\}$	$x_5 = 0$, $x_3 = 1$, $x_1 \oplus x_4 = 1$
	$\{6, 20, 15, 29\}$	$x_1 \oplus x_4 = 1$, $x_3 = 1$, $x_2 \oplus x_5 = 0$
	$\{10, 11, 14, 15\}$	$x_1 = 0$, $x_2 = 1$, $x_4 = 1$
	$\{10, 11, 28, 29\}$	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 = 0$
	$\{14, 15, 28, 29\}$	$x_3 = 1$, $x_1 \oplus x_4 = 1$, $x_2 = 1$
7	$\{1, 3, 29, 31\}$	$x_1 \oplus x_2 = 0$, $x_1 \oplus x_3 = 0$, $x_5 = 1$
	$\{1, 10, 23, 28\}$	$x_2 \oplus x_5 = 1$, $x_1 \oplus x_3 = 0$, $x_1 \oplus x_2 \oplus x_4 = 0$
	$\{3, 10, 7, 14\}$	$x_1 = 0$, $x_4 = 1$, $x_2 \oplus x_5 = 1$
	$\{13, 7, 23, 29\}$	$x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_5 = 1$
	$\{13, 14, 28, 31\}$	$x_2 = 1$, $x_3 = 1$, $x_1 \oplus x_4 \oplus x_5 = 1$
8	$\{8, 9, 24, 25\}$	$x_3 = 0$, $x_4 = 0$, $x_2 = 1$
	$\{8, 9, 26, 27\}$	$x_3 = 0$, $x_2 = 1$, $x_1 \oplus x_4 = 0$
	$\{8, 13, 24, 29\}$	$x_4 = 0$, $x_2 = 1$, $x_3 \oplus x_5 = 0$
	$\{8, 13, 26, 31\}$	$x_2 = 1$, $x_1 \oplus x_4 = 0$, $x_2 \oplus x_5 = 0$
	$\{9, 13, 25, 29\}$	$x_4 = 0$, $x_2 = 1$, $x_5 = 1$
	$\{9, 13, 27, 31\}$	$x_1 \oplus x_2 = 1$, $x_5 = 1$, $x_1 \oplus x_4 = 0$
	$\{24, 26, 25, 27\}$	$x_3 = 0$, $x_2 = 1$, $x_1 = 1$
	$\{24, 26, 29, 31\}$	$x_2 = 1$, $x_1 = 1$, $x_3 \oplus x_5 = 0$
	$\{25, 27, 29, 31\}$	$x_1 = 1$, $x_2 = 1$, $x_5 = 1$

Table .4: List of all 2D Affine Equations of Keccak for δ^{out}= 5, 6, 7, 8.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
9	{8, 24, 7, 23}	$x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_5 = 1$
	{8, 26, 15, 29}	$x_2 = 1$, $x_3 \oplus x_5 = 0$, $x_1 \oplus x_3 \oplus x_4 = 0$
	{3, 7, 25, 29}	$x_1 \oplus x_2 = 0$, $x_5 = 1$, $x_1 \oplus x_4 = 1$
	{3, 15, 23, 27}	$x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$, $x_5 = 1$
	{24, 26, 25, 27}	$x_3 = 0$, $x_2 = 1$, $x_1 = 1$
10	{2, 6, 25, 29}	$x_1 \oplus x_2 = 0$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_5 = 0$
	{2, 22, 15, 27}	$x_4 = 1$, $x_2 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{6, 22, 14, 30}	$x_1 \oplus x_3 = 0$, $x_5 = 0$, $x_1 \oplus x_4 = 1$
	{24, 14, 15, 25}	$x_2 = 1$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_4 = 1$
	{24, 27, 29, 30}	$x_1 = 1$, $x_2 = 1$, $x_3 \oplus x_4 \oplus x_5 = 0$
11	{3, 9, 13, 17}	$x_1 = 0$, $x_5 = 1$, $x_2 \oplus x_4 = 1$
	{3, 9, 23, 29}	$x_5 = 1$, $x_1 \oplus x_3 = 0$, $x_2 \oplus x_4 = 1$
	{3, 13, 23, 25}	$x_5 = 1$, $x_2 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{3, 7, 25, 29}	$x_5 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_4 = 1$
	{3, 7, 27, 31}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 = 0$
	{9, 13, 25, 29}	$x_4 = 0$, $x_2 = 1$, $x_5 = 1$
	{9,13, 27, 31}	$x_2 = 1$, $x_5 = 1$, $x_1 \oplus x_4 = 0$
	{9, 24, 14, 31}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{9, 7, 23, 25}	$x_5 = 1$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 = 1$
	{9, 14, 25, 30}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_3 \oplus x_5 = 1$
	{13, 24, 14, 27}	$x_2 = 1$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_4 \oplus x_5 = 1$
	{13, 7, 23, 29}	$x_3 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 1$
	{13, 14, 29, 30}	$x_2 = 1$, $x_3 = 1$, $x_4 \oplus x_5 = 1$
	{24, 25, 30, 31}	$x_1 = 1$, $x_2 = 1$, $x_3 \oplus x_4 = 0$
	{24, 27, 29, 30}	$x_1 = 1$, $x_2 = 1$, $x_3 \oplus x_4 \oplus x_5 = 0$
	{7, 14, 23, 30}	$x_3 = 1$, $x_4 = 1$, $x_2 \oplus x_5 = 1$
	{25, 27, 29, 31}	$x_1 = 1$, $x_2 = 1$, $x_5 = 1$
12	{4, 9, 20, 25}	$x_4 = 0$, $x_2 \oplus x_5 = 0$, $x_2 \oplus x_3 = 1$
	{4, 9, 22, 27}	$x)1 \oplus x_4 = 0$, $x_2 \oplus x_5 = 0$, $x_2 \oplus x_3 = 1$
	{4, 12, 22, 30}	$x_4 = 0$, $x_3 = 1$, , $x_5 = 0$
	{4, 12, 25, 28}	$x_5 = 0$, $x_3 = 1$, $x_1 \oplus x_4 = 0$
	{9, 12, 25, 28}	$x_4 = 0$, $x_3 \oplus x_5 = 1$, $x_2 = 1$
	{9, 12, 27, 30}	$x_3 \oplus x_5 = 1$, $x_2 = 1$, $x_1 \oplus x_4 = 0$
	{20, 22, 25, 27}	$x_2 \oplus x_5 = 0$, $x_2 \oplus x_3 = 1$, $x_1 = 1$
	{20, 22, 28, 30}	$x_3 = 1$, $x_5 = 0$, $x_1 = 1$
	{25, 27, 28, 30}	$x_2 = 1$, $x_1 = 1$, $x_3 \oplus x_5 = 1$

Table .5: List of all 2D Affine Equations of KECCAK for δ^{out}= 9, 10, 11, 12

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
13	{3, 5, 25, 31}	$x_5 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_3 \oplus x_4 = 1$
	{3, 21, 15, 25}	$x_4 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{3, 7, 27, 31}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 = 0$
	{3, 15, 23, 27}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{5, 12, 21, 28}	$x_4 = 0$, $x_3 = 1$, $x_2 \oplus x_5 = 1$
	{5, 12, 23, 30}	$x_3 = 1$, $x_1 \oplus x_4 = 0$, $x_2 \oplus x_5 = 1$
	{5, 21, 7, 23}	$x_2 = 0$, $x_3 = 1$, $x_5 = 1$
	{5, 21, 15, 31}	$x_3 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 0$
	{5, 7, 25, 27}	$x_5 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_3 = 1$
	{5, 7, 28, 30}	$x_3 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_5 = 1$
	{12, 21, 7, 30}	$x_3 = 1$, $x_2 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_4 = 1$
	{12, 7, 23, 28}	$x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_5 = 1$
	{12, 15, 28, 31}	$x_2 = 1$, $x_3 = 1$, $x_5 \oplus x_4 = 0$
	{21, 23, 25, 27}	$x_1 = 1$, $x_5 = 1$, $x_2 \oplus x_3 = 1$
	{21, 23, 28, 30}	$x_1 = 1$, $x_2 \oplus x_5 = 1$, $x_3 = 1$
	{7, 15, 23, 31}	$x_5 = 1$, $x_3 = 1$, $x_4 = 1$
	{25, 27, 28, 30}	$x_1 = 1$, $x_2 = 1$, $x_3 \oplus x_5 = 1$
14	{2, 6, 27, 31}	$x_4 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_5 = 0$
	{2, 20, 15, 25}	$x_1 \oplus x_4 = 1$, $x_2 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{6, 20, 14, 28}	$x_5 = 0$, $x_3 = 1$, $x_1 \oplus x_4 = 1$
	{26, 14, 15, 27}	$x_2 = 1$, $x_1 \oplus x_3 = 1$, $x_4 = 1$
	{26, 25, 28, 31}	$x_1 = 1$, $x_2 = 1$, $x_3 \oplus x_4 \oplus x_5 = 1$
15	{3, 26, 14, 23}	$x_4 = 1$, $x_2 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{5, 9, 21, 25}	$x_4 = 0$, $x_5 = 1$, $x_2 \oplus x_3 = 1$
	{5, 9, 23, 27}	$x_5 = 1$, $x_1 \oplus x_4 = 0$, $x_2 \oplus x_3 = 1$
	{5, 21, 23, 7}	$x_2 = 0$, $x_3 = 1$, $x_5 = 1$
	{5, 7, 25, 27}	$x_5 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_3 = 1$
	{5, 14, 23, 28}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_3 \oplus x_5 = 1$
	{9, 21, 7, 27}	$x_5 = 1$, $x_2 \oplus x_3 = 1$, $x_1 \oplus x_2 \oplus x_4 = 1$
	{9, 7, 23, 25}	$x_5 = 1$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 = 1$
	{9, 14, 27, 28}	$x_2 = 1$, $x_3 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 1$
	{21, 7, 14, 28}	$x_1 \oplus x_4 = 1$, $x_3 = 1$, $x_2 \oplus x_5 = 1$
	{21, 23, 25, 27}	$x_1 = 1$, $x_5 = 1$, $x_2 \oplus x_3 = 1$

Table .6: List of all 2D Affine Equations of Keccak for δ^{out}= 13, 14, 15.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
16	{16, 17, 18, 19}	$x_2 = 0$, $x_3 = 0$, $x_1 = 1$
	{16, 17, 26, 27}	$x_3 = 0$, $x_1 = 1$, $x_2 \oplus x_4 = 0$
	{16, 18, 21, 23}	$x_2 = 0$, $x_1 = 1$, $x_3 \oplus x_5 = 0$
	{16, 21, 26, 31}	$x_1 = 1$, $x_2 \oplus x_4 = 0$, $x_3 \oplus x_5 = 0$
	{17, 21, 19, 23}	$x_2 = 0$, $x_1 = 1$, $x_5 = 1$
	{17, 21, 27, 31}	$x_1 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 0$
	{18, 26, 19, 27}	$x_3 = 0$, $x_1 = 1$, $x_4 = 1$
	{18, 26, 23, 31}	$x_1 = 1$, $x_4 = 1$, $x_3 \oplus x_5 = 0$
	{19, 23, 27, 31}	$x_1 = 1$, $x_4 = 1$, $x_5 = 1$
17	{16, 5, 18, 7}	$x_2 = 0$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_5 = 1$
	{16, 5, 26, 15}	$x_1 \oplus x_3 = 0$, $x_1 \oplus x_5 = 1$, $x_2 \oplus x_4 = 0$
	{16, 17, 18, 19}	$x_2 = 0$, $x_3 = 0$, $x_1 = 1$
	{16, 17, 26, 27}	$x_3 = 0$, $x_1 = 1$, $x_2 \oplus x_4 = 0$
	{17, 5, 19, 7}	$x_2 = 0$, $x_1 \oplus x_3 = 1$, $x_5 = 1$
	{17, 5, 27, 15}	$x_1 \oplus x_3 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 0$
	{18, 26, 7, 15}	$x_1 \oplus x_5 = 1$, $x_1 \oplus x_3 = 1$, $x_4 = 1$
	{18, 26, 19, 27}	$x_3 = 0$, $x_1 = 1$, $x_4 = 1$
	{19, 15, 27, 7}	$x_1 \oplus x_3 = 1$, $x_4 = 1$, $x_5 = 1$
18	{16, 17, 14, 15}	$x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_4 = 1$
	{16, 21, 27, 30}	$x_2 \oplus x_3 \oplus x_5 = 0$, $x_1 = 1$, $x_2 \oplus x_4 = 0$
	{6, 14, 27, 19}	$x_4 = 1$, $x_1 \oplus x_5 = 0$, $x_1 \oplus x_3 = 1$
	{6, 15, 23, 30}	$x_4 = 1$, $x_3 = 1$, $x_1 \oplus x_2 \oplus x_5 = 9$
	{21, 19, 17, 23}	$x_2 = 0$, $x_1 = 1$, $x_5 = 1$
19	{16, 5, 14, 7}	$x_2 \oplus x_4 = 0$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{16, 17, 30, 31}	$x_2 \oplus x_3 = 0$, $x_1 = 1$, $x_2 \oplus x_4 = 0$
	{5, 17, 7, 19}	$x_2 = 0$, $x_5 = 1$, $x_1 \oplus x_3 = 1$
	{22, 7, 14, 31}	$x_4 = 1$, $x_3 = 1$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{22, 19, 27, 30}	$x_4 = 1$, $x_1 = 1$, $x_3 \oplus x_5 = 1$
20	{4, 12, 19, 27}	$x_1 \oplus x_4 = 0$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_5 = 0$
	{4, 13, 30, 23}	$x_1 \oplus x_4 = 0$, $x_3 = 1$, $x_1 \oplus x_2 \oplus x_5 = 0$
	{12, 13, 28, 29}	$x_4 = 0$, $x_2 = 1$, $x_3 = 1$
	{17, 19, 28, 30}	$x_1 = 1$, $x_2 \oplus x_3 = 0$, $x_2 \oplus x_5 = 1$
	{17, 23, 27, 29}	$x_5 = 1$, $x_1 = 1$, $x_2 \oplus x_3 \oplus x_4 = 0$

Table .7: List of all 2D Affine Equations of KECCAK for δ^{out}= 16, 17, 18, 19, 20

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
21	$\{12, 20, 7, 31\}$	$x_3 = 1$, $x_4 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_4 = 1$
	$\{12, 22, 7, 29\}$	$x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_5 = 1$
	$\{12, 15, 28, 31\}$	$x_2 = 1$, $x_3 = 1$, $x_4 \oplus x_5 = 0$
	$\{12, 15, 29, 30\}$	$x_2 = 1$, $x_3 = 1$, $x_1 \oplus x_4 \oplus x_5 = 0$
	$\{17, 20, 22, 19\}$	$x_2 = 0$, $x_1 = 1$, $x_3 \oplus x_5 = 1$
	$\{17, 20, 27, 30\}$	$x_1 = 1$, $x_2 \oplus x_4 = 0$, $x_3 \oplus x_5 = 1$
	$\{17, 22, 27, 28\}$	$x_1 = 1$, $x_3 \oplus x_5 = 1$, $x_2 \oplus x_3 \oplus x_4 = 0$
	$\{17, 19, 28, 30\}$	$x_1 = 1$, $x_2 \oplus x_5 = 1$, $x_2 \oplus x_3 = 0$
	$\{17, 19, 29, 31\}$	$x_5 = 1$, $x_1 = 1$, $x_2 \oplus x_3 = 0$
	$\{20, 22, 28, 30\}$	$x_3 = 1$, $x_5 = 0$, $x_1 = 1$
	$\{20, 22, 29, 31\}$	$x_3 = 1$, $x_2 \oplus x_5 = 0$, $x_1 = 1$
	$\{20, 7, 15, 28\}$	$x_3 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_5 = 1$
	$\{20, 19, 28, 27\}$	$x_1 = 1$, $x_3 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$
	$\{22, 7, 15, 30\}$	$x_3 = 1$, $x_4 = 1$, $x_1 \oplus x_5 = 1$
	$\{22, 19, 27, 30\}$	$x_1 = 1$, $x_3 \oplus x_5 = 1$, $x_4 = 1$
	$\{7, 15, 19, 27\}$	$x_5 = 1$, $x_1 \oplus x_3 = 1$, $x_4 = 1$
	$\{28, 29, 30, 31\}$	$x_1 = 1$, $x_2 = 1$, $x_3 = 1$
22	$\{6, 18, 26, 14\}$	$x_4 = 1$, $x_5 = 0$, $x_1 \oplus x_3 = 1$
	$\{6, 18, 15, 27\}$	$x_4 = 1$, $x_1 \oplus x_3 = 1$, $x_2 \oplus x_5 = 0$
	$\{6, 26, 15, 19\}$	$x_4 = 1$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_2 \oplus x_5 = 0$
	$\{6, 14, 19, 27\}$	$x_4 = 1$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_5 = 0$
	$\{6, 14, 23, 31\}$	$x_3 = 1$, $x_4 = 1$, $x_1 \oplus x_5 = 0$
	$\{17, 18, 28, 31\}$	$x_1 = 1$, $x_2 \oplus x_3 = 0$, $x_2 \oplus x_4 \oplus x_5 = 1$
	$\{17, 26, 23, 28\}$	$x_2 \oplus x_5 = 1$, $x_1 = 1$, $x_2 \oplus x_3 \oplus x_4 = 0$
	$\{17, 19, 29, 31\}$	$x_1 = 1$, $x_2 \oplus x_3 = 0$, $x_5 = 1$
	$\{17, 23, 27, 29\}$	$x_2 \oplus x_3 \oplus x_4 = 0$, $x_1 = 1$, $x_5 = 1$
	$\{18, 26, 19, 27\}$	$x_1 = 1$, $x_4 = 1$, $x_3 = 0$
	$\{18, 26, 23, 31\}$	$x_4 = 1$, $x_3 \oplus x_5 = 0$, $x_1 = 1$
	$\{18, 14, 15, 19\}$	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 = 1$
	$\{18, 19, 28, 29\}$	$x_1 = 1$, $x_2 \oplus x_3 = 0$, $x_2 \oplus x_4 = 1$
	$\{26, 14, 15, 27\}$	$x_2 = 1$, $x_4 = 1$, $x_1 \oplus x_3 = 1$
	$\{26, 27, 28, 29\}$	$x_1 = 1$, $x_2 = 1$, $x_3 \oplus x_4 = 1$
	$\{14, 15, 28, 29\}$	$x_2 = 1$, $x_3 = 1$, $x_1 \oplus x_4 = 1$
	$\{19, 23, 27, 31\}$	$x_1 = 1$, $x_5 = 1$, $x_4 = 1$

Table .8: List of all 2D Affine Equations of Keccak for δ^{out}= 21, 22.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
23	{13, 17, 27, 7}	$x_1 \oplus x_3 = 1$, $x_5 = 1$, $x_1 \oplus x_2 \oplus x_4 = 1$
	{18, 20, 26, 28}	$x_5 = 0$, $x_1 = 1$, $x_3 \oplus x_4 = 1$
	{18, 20, 27, 29}	$x_1 = 1$, $x_3 \oplus x_4 = 1$, $x_2 \oplus x_5 = 0$
	{18, 26, 19, 27}	$x_3 = 0$, $x_4 = 1$, $x_1 = 1$
	{18, 7, 14, 27}	$x_1 \oplus x_3 = 1$, $x_4 = 1$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{18, 28, 29, 19}	$x_1 = 1$, $x_2 \oplus x_3 = 0$, $x_2 \oplus x_4 = 1$
	{20, 26, 19, 29}	$x_1 = 1$, $x_3 \oplus x_4 = 1$, $x_2 \oplus x_3 \oplus x_5 = 1$
	{20, 7, 14, 29}	$x_3 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{20, 19, 27, 28}	$x_1 = 1$, $x_3 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$
	{26, 7, 14, 19}	$x_4 = 1$, $x_1 \oplus x_3 = 1$, $x_2 \oplus x_5 = 1$
	{26, 27, 28, 29}	$x_2 = 1$, $x_1 = 1$, $x_3 \oplus x_4 = 1$
24	{8, 9, 18, 19}	$x_1 \oplus x_2 = 1$, $x_3 = 0$, $x_1 \oplus x_2 = 1$
	{8, 9, 24, 25}	$x_2 = 1$, $x_3 = 0$, $x_4 = 0$
	{8, 13, 24, 29}	$x_4 = 0$, $x_2 = 1$, $x_3 \oplus x_5 = 0$
	{19, 23, 9, 13}	$x_5 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_4 = 0$
	{9, 13, 29, 25}	$x_2 = 1$, $x_4 = 0$, $x_5 = 1$
	{18, 24, 19, 25}	$x_1 = 1$, $x_3 = 0$, $x_2 \oplus x_4 = 1$
	{18, 24, 23, 29}	$x_1 = 1$, $x_2 \oplus x_4 = 1$, $x_3 \oplus x_5 = 0$
	{19, 23, 25, 29}	$x_1 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 1$
25	{8, 18, 7, 29}	$x_3 \oplus x_5 = 0$, $x_2 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{8, 24, 15, 31}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_3 \oplus x_5 = 0$
	{11, 7, 19, 31}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{11, 15, 25, 29}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_5 = 1$
	{18, 24, 19, 25}	$x_1 = 1$, $x_3 = 0$, $x_2 \oplus x_4 = 1$

Table .9: List of all 2D Affine Equations of Keccak for δ^{out}= 23, 24, 25.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
26	{6, 10, 19, 31}	$x_4 = 1$, $x_1 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{6, 11, 19, 30}	$x_4 = 1$, $x_3 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{6, 14, 23, 31}	$x_3 = 1$, $x_4 = 1$, $x_1 \oplus x_5 = 0$
	{6, 15, 23, 30}	$x_3 = 1$, $x_4 = 1$, $x_1 \oplus x_2 \oplus x_5 = 0$
	{10, 11, 24, 25}	$x_3 = 0$, $x_2 = 1$, $x_1 \oplus x_4 = 1$
	{10, 11, 14, 15}	$x_1 = 0$, $x_2 = 1$, $x_4 = 1$
	{10, 11, 30, 31}	$x_4 = 1$, $x_2 = 1$, $x_1 \oplus x_3 = 0$
	{10, 24, 15, 29}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_3 \oplus x_5 = 0$
	{10, 14, 19, 23}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_5 = 0$
	{10, 14, 25, 29}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_5 = 0$
	{11, 24, 14, 29}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{11, 15, 19, 23}	$x_5 = 1$, $x_1 \oplus x_2 = 1$, $x_4 = 1$
	{11, 15, 25, 29}	$x_2 = 1$, $x_5 = 1$, $x_1 \oplus x_4 = 1$
	{24, 14, 15, 25}	$x_2 = 1$, $x_1 \oplus x_3 = 1$, $x_1 \oplus x_4 = 1$
	{24, 25, 30, 31}	$x_1 = 1$, $x_3 \oplus x_4 = 0$, $x_2 = 1$
	{14, 15, 30, 31}	$x_2 = 1$, $x_3 = 1$, $x_4 = 1$
	{19, 23, 25, 29}	$x_1 = 1$, $x_5 = 1$, $x_2 \oplus x_4 = 1$
27	{9, 10, 13, 14}	$x_1 = 0$, $x_2 = 1$, $x_4 \oplus x_5 = 1$
	{9, 10, 29, 30}	$x_2 = 1$, $x_1 \oplus x_3 = 0$, $x_4 \oplus x_5 = 1$
	{9, 13, 25, 29}	$x_4 = 0$, $x_2 = 1$, $x_5 = 1$
	{9, 22, 24, 7}	$x_1 \oplus x_5 = 1$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 = 1$
	{9, 7, 19, 29}	$x_5 = 1$, $x_2 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{9, 14, 25, 30}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_3 \oplus x_5 = 1$
	{10, 13, 25, 30}	$x_2 = 1$, $x_4 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 1$
	{10, 7, 19, 30}	$x_4 = 1$, $x_2 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{10, 14, 25, 29}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_5 = 0$
	{13, 7, 25, 29}	$x_2 \oplus x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_3 = 1$
	{13, 14, 29, 30}	$x_2 = 1$, $x_3 = 1$, $x_4 \oplus x_5 = 1$
	{22, 14, 19, 29}	$x_1 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_3 \oplus x_5 = 1$
28	{4, 9, 19, 30}	$x_3 \oplus x_5 = 1$, $x_1 \oplus x_4 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{4, 12, 23, 31}	$x_3 = 1$, $x_1 \oplus x_4 = 0$, $x_1 \oplus x_5 = 0$
	{9, 12, 25, 28}	$x_4 = 0$, $x_2 = 1$, $x_3 \oplus x_5 = 1$
	{21, 19, 25, 31}	$x_1 = 1$, $x_2 \oplus x_3 \oplus x_4 = 1$, $x_5 = 1$
	{21, 23, 28, 30}	$x_1 = 1$, $x_3 = 1$, $x_2 \oplus x_5 = 1$

Table .10: List of all 2D Affine Equations of Keccak for δ^{out}= 26, 27, 28.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
29	{5, 20, 22, 7}	$x_1 \oplus x_4 = 1$, $x_1 \oplus x_5 = 0$, $x_2 \oplus x_3 = 1$
	{5, 20, 15, 30}	$x_3 = 0$, $x_4 = 1$, $x_1 \oplus x_2 = 1$
	{5, 22, 15, 28}	$x_3 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_5 = 0$
	{5, 7, 28, 30}	$x_3 = 0$, $x_4 = 1$, $x_1 \oplus x_2 = 1$
	{5, 15, 19, 25}	$x_1 = 0$, $x_2 = 1$, $x_4 = 1$
	{11, 12, 20, 19}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_3 \oplus x_5 = 0$
	{11, 12, 25, 30}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_5 = 0$
	{20, 22, 28, 30}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 0$
	{20, 7, 15, 28}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 0$
	{20, 19, 25, 30}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{22, 7, 15, 30}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$
	{22, 19, 25, 28}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 = 1$
30	{6, 10, 21, 25}	$x_1 \oplus x_4 = 1$, $x_1 \oplus x_5 = 0$, $x_2 \oplus x_3 = 1$
	{6, 21, 15, 28}	$x_3 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_5 = 0$
	{10, 11, 18, 19}	$x_3 = 0$, $x_4 = 1$, $x_1 \oplus x_2 = 1$
	{10, 11, 14, 15}	$x_1 = 0$, $x_2 = 1$, $x_4 = 1$
	{10, 18, 15, 23}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_3 \oplus x_5 = 0$
	{10, 14, 19, 23}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_5 = 0$
	{10, 15, 25, 28}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 0$
	{11, 18, 14, 23}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{11, 14, 25, 28}	$x_2 = 1$, $x_1 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$
	{11, 15, 19, 23}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 = 1$
	{18, 14, 15, 19}	$x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 = 1$
	{18, 23, 25, 28}	$x_1 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_3 \oplus x_5 = 0$
31	{5, 9, 19, 31}	$x_5 = 1$, $x_1 \oplus x_4 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{5, 10, 19, 28}	$x_2 \oplus x_5 = 1$, $x_3 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{5, 18, 24, 25}	$x_1 \oplus x_3 = 1$, $x_4 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_4 = 0$
	{5, 20, 14, 31}	$x_3 = 1$, $x_2 \oplus x_4 = 0$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{9, 10, 28, 31}	$x_2 = 1$, $x_1 \oplus x_3 = 0$, $x_1 \oplus x_4 \oplus x_5 = 1$
	{9, 18, 7, 28}	$x_1 \oplus x_5 = 1$, $x_2 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{9, 20, 14, 19}	$x_1 \oplus x_2 = 1$, $x_3 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 0$
	{10, 18, 7, 31}	$x_4 = 1$, $x_3 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{10, 20, 7, 25}	$x_1 \oplus x_4 = 1$, $x_2 \oplus x_3 = 1$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{18, 20, 25, 31}	$x_1 = 1$, $x_2 \oplus x_5 = 0$, $x_2 \oplus x_3 \oplus x_4 = 1$

Table .11: List of all 2D Affine Equations of Keccak for δ^{out}= 29,30, 31.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
1	{12, 3, 6, 9}	$x_1 = 0$, $x_2 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$
	{12, 28, 10, 26}	$x_5 = 0$, $x_2 = 1$, $x_3 \oplus x_4 = 1$
	{3, 28, 13, 18}	$x_1 \oplus x_5 = 1$, $x_2 \oplus x_3 = 0$, $x_2 \oplus x_4 = 1$
	{14, 6, 18, 26}	$x_5 = 0$, $x_4 = 1$, $x_1 \oplus x_3 = 1$
	{14, 9, 10, 13}	$x_1 = 0$, $x_2 = 1$, $x_4 \oplus x_5 = 1$
2	{19, 7, 14, 26}	$x_4 = 1$, $x_1 \oplus x_3 = 1$, $x_2 \oplus x_5 = 1$
	{19, 7, 31, 11}	$x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{19, 14, 23, 10}	$x_4 = 1$, $x_1 \oplus x_5 = 0$, $x_1 \oplus x_2 = 1$
	{19, 23, 31, 27}	$x_4 = 1$, $x_1 = 1$, $x_5 = 1$
	{7, 23, 10, 26}	$x_4 = 1$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_5 = 1$
	{7, 23, 11, 27}	$x_4 = 1$, $x_5 = 1$, $x_2 \oplus x_3 = 1$
	{14, 31, 10, 27}	$x_2 = 1$, $x_4 = 1$, $x_1 \oplus x_5 = 0$
	{14, 31, 11, 26}	$x_2 = 1$, $x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{10, 11, 26, 27}	$x_3 = 0$, $x_4 = 1$, $x_2 = 1$
3	{7, 28, 29, 6}	$x_3 = 1$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_2 = 0$
	{7, 9, 28, 18}	$x_2 \oplus x_4 = 1$, $x_1 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{25, 29, 31, 27}	$x_5 = 1$, $x_1 = 1$, $x_2 = 1$
	{25, 29, 9, 13}	$x_4 = 0$, $x_2 = 1$, $x_5 = 1$
	{25, 31, 11, 13}	$x_2 = 1$, $x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 1$
	{25, 6, 13, 18}	$x_1 \oplus x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_5 = 0$
	{25, 9, 11, 27}	$x_5 = 1$, $x_2 \oplus x_3 = 1$, $x_1 \oplus$ $x_2 \oplus x_4 = 1$
	{29, 31, 9, 11}	$x_1 \oplus x_3 = 0$, $x_2 = 1$, $x_5 = 1$
	{29, 11, 27, 13}	$x_2 = 1$, $x_5 = 1$, $x_3 \oplus x_4 = 1$
	{31, 6, 11, 18}	$x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$, $x_2 \oplus x_5 = 0$
	{31, 9, 13, 27}	$x_2 = 1$, $x_5 = 1$, $x_1 \oplus$ $x_4 = 0$

Table .12: List of all 2D Affine Equations of Ascon for δ^{out}= 1, 2, 3.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
4	{19, 9, 14, 20}	$x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 \oplus x_4 = 0$, $x_3 \oplus x_5 = 1$
	{19, 14, 23, 10}	$x_4 = 1$, $x_1 \oplus x_5 = 0$, $x_1 \oplus x_2 = 1$
	{19, 20, 31, 24}	$x_4 \oplus x_5 = 0$, $x_1 = 1$, $x_2 \oplus x_3 \oplus x_4 = 1$
	{19, 23, 31, 27}	$x_4 = 1$, $x_1 = 1$, $x_5 = 1$
	{14, 31, 9, 24}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{14, 31, 10, 27}	$x_2 = 1$, $x_4 = 1$, $x_1 \oplus x_5 = 0$
	{20, 23, 24, 27}	$x_1 = 1$, $x_2 \oplus x_3 = 1$, $x_4 \oplus x_5 = 0$
	{9, 10, 24, 27}	$x_2 = 1$, $x_3 = 0$, $x_1 \oplus x_4 \oplus x_5 = 1$
5	{3, 20, 13, 26}	$x_1 \oplus x_2 \oplus x_3 = 0$, $x_3 \oplus x_4 = 1$, $x_1 \oplus x_5 = 1$
	{3, 27, 21, 13}	$x_3 \oplus x_4 = 1$, $x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{3, 31, 6, 26}	$x_4 = 1$, $x_1 \oplus x_2 = 0$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{20, 21, 26, 27}	$x_2 \oplus x_4 = 0$, $x_1 = 1$, $x_2 \oplus x_3 = 1$
	{20, 29, 18, 27}	$x_1 = 1$, $x_2 \oplus x_5 = 0$, $x_3 \oplus x_4 = 1$
	{20, 31, 6, 13}	$x_3 = 1$, $x_2 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_4 = 1$
	{21, 29, 18, 26}	$x_1 = 1$, $x_3 \oplus x_4 = 1$, $x_3 \oplus x_5 = 0$
	{21, 31, 18, 24}	$x_1 = 1$, $x_3 \oplus x_5 = 0$, $x_2 \oplus x_3 \oplus x_4 = 1$
	{29, 31, 26, 24}	$x_3 \oplus x_5 = 0$, $x_1 = 1$, $x_2 = 1$
6	{4, 7, 8, 11}	$x_1 = 0$, $x_2 \oplus x_3 = 1$, $x_4 \oplus x_5 = 1$
	{4, 8, 20, 24}	$x_3 \oplus x_4 = 0$, $x_5 = 0$, $x_2 \oplus x_3 = 1$
	{4, 20, 9, 25}	$x_4 = 0$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_5 = 0$
	{20, 9, 26, 7}	$x_1 \oplus x_2 \oplus x_4 = 1$, $x_1 \oplus x5 = 1$, $x_2 \oplus x_3 = 1$
	{20, 24, 11, 7}	$x_1 \oplus x_4 = 1$, $x_1 \oplus x5 = 1$, $x_2 \oplus x_3 = 1$
	{25, 9, 8, 24}	$x_2 = 1$, $x_4 = 0$, $x_3 = 0$
	{25, 11, 8, 26}	$x_2 = 1$, $x_3 = 0$, $x_1 \oplus x_4 \oplus x_5 = 0$
	{9, 11, 26, 24}	$x_1 \oplus x_5 = 1$, $x_3 = 0$, $x_2 = 1$

Table .13: List of all 2D Affine Equations of Ascon for δ^{out}= 4, 5, 6 .

δ^{out}	2D affine subspaces	Corresponding linear equations
9	{16, 1, 3, 18}	$x_1 \oplus x_5 = 1$, $x_2 = 0$, $x_3 = 0$
	{16, 1, 15, 30}	$x_2 \oplus x_4 = 0$, $x_2 \oplus x_3 = 0$, $x_1 \oplus x_5 = 1$
	{16, 3, 21, 26}	$x_2 = 0$, $x_1 \oplus x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 1$
	{1, 21, 6, 18}	$x_2 = 0$, $x_4 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 0$
	{1, 21, 10, 30}	$x_2 \oplus x_5 = 1$, $x_2 \oplus x_4 = 0$, $x_1 \oplus x_3 = 0$
	{3, 15, 6, 10}	$x_1 = 0$, $x_2 \oplus x_3 \oplus x_5 = 1$, $x_4 = 1$
	{3, 15, 18, 30}	$x_4 = 1$, $x_2 \oplus x_3 = 0$, $x_1 \oplus x_5 = 1$
	{6, 10,18, 30}	$x_4 = 1$, $x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$
10	{19, 7, 10, 30}	$x_4 = 1$, $x_2 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
	{19, 23, 9, 13}	$x_5 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_4 = 0$
	{7, 23, 11, 27}	$x_5 = 1$, $x_2 \oplus x_3 = 1$, $x_4 = 1$
	{28, 9, 11, 30}	$x_1 \oplus x_5 = 1$, $x_2 = 1$, $x_1 \oplus x_3 = 0$
	{28, 10, 27, 13}	$x_3 \oplus x_4 = 1$, $x_2 = 1$, $x_1 \oplus x_3 \oplus x_5 = 0$
11	{16, 1, 11, 26}	$x_3 = 0$, $x_1 \oplus x_5 = 1$, $x_2 \oplus x_4 = 0$
	{16, 21, 27, 30}	$x_1 = 1$, $x_2 \oplus x_3 \oplus x_5 = 0$, $x_2 \oplus x_4 = 0$
	{1, 21, 6, 18}	$x_2 = 0$, $x_4 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 0$
	{7, 6, 26, 27}	$x_1 \oplus x_3 = 1$, $x_4 = 1$, $x_1 \oplus x_2 = 0$
	{7, 11, 18, 30}	$x_1 \oplus x_5 = 1$, $x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$
12	{19, 20, 10, 13}	$x_3 \oplus x_4 = 1$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 \oplus x_5 = 0$
	{19, 23, 26, 30}	$x_1 = 1$, $x_4 = 1$, $x_2 \oplus x_5 = 1$
	{15, 10, 27, 30}	$x_2 = 1$, $x_4 = 1$, $x_1 \oplus x_3 \oplus x_5 = 0$
	{15, 13, 24, 26}	$x_1 \oplus x_3 = 1$, $x_2 = 1$, $x_1 \oplus x_5 = 1$
	{20, 23, 24, 27}	$x_4 \oplus x_5 = 0$, $x_1 = 1$, $x_2 \oplus x_3 = 1$
13	{1, 25, 3, 27}	$x_1 \oplus x_2 = 0$, $x_5 = 1$, $x_3 = 0$
	{1, 6, 25, 30}	$x_1 \oplus x_2 = 0$, $x_3 \oplus x_4 = 0$, $x_3 \oplus x_5 = 1$
	{15, 3, 18, 30}	$x_2 \oplus x_3 = 0$, $x_4 = 1$, $x_1 \oplus x_5 = 1$
	{3, 27, 6, 30}	$x_4 = 1$, $x_3 \oplus x_5 = 1$, $x_1 \oplus x_2 = 0$
	{3, 9, 18, 24}	$x_1 \oplus x_5 = 1$, $x_3 = 0$, $x_2 \oplus x_4 = 1$
	{27, 15, 6, 18}	$x_1 \oplus x_3 = 1$, $x_2 \oplus x_5 = 0$, $x_4 = 1$
	{9, 15, 24, 30}	$x_2 = 1$, $x_3 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$
	{24, 20,18, 30}	$x_1 = 1$, $x_5 = 0$, $x_2 \oplus x_3 \oplus x_4 = 1$

Table .14: List of all 2D Affine Equations of Ascon for δ^{out}= 9, 10, 11, 12.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
21	{17, 2, 26, 9}	$x_3 = 0$, $x_1 \oplus x_2 \oplus x_4 = 1$, $x_4 \oplus x_5 = 1$
	{17, 31, 22, 24}	$x_1 = 1$, $x_2 \oplus x_3 \oplus x_5 = 1$, $x_3 \oplus x_4 = 0$
	{2, 31, 6, 27}	$x_1 \oplus x_5 = 0$, $x_1 \oplus x_2 = 0$, $x_4 = 1$
	{25, 6, 9, 22}	$x_2 \oplus x_5 = 0$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_3 = 1$
	{24, 25, 26, 27}	$x_1 = 1$, $x_2 = 1$, $x_3 = 0$
22	{4, 22, 26, 8}	$x_5 = 0$, $x_1 \oplus x_4 = 1$, $x_2 \oplus x_3 = 1$
	{4, 29, 11, 18}	$x_3 \oplus x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$, $x_2 \oplus x_5 = 0$
	{5, 11, 22, 24}	$x_1 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_4 = 0$, $x_2 \oplus x_3 = 1$
	{5, 13, 18, 26}	$x_1 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$, $x_1 \oplus x_3 = 1$
	{8, 29, 23, 24}	$x_3 \oplus x_5 = 0$, $x_2 = 1$, $x_4 = 0$
23	{17, 2, 24, 11}	$x_3 = 0$, $x_1 \oplus x_2 \oplus x_5 = 0$, $x_1 \oplus x_4 = 1$
	{17, 9, 22, 14}	$x_1 \oplus x_2 = 1$, $x_3 \oplus x_5 = 1$, $x_3 \oplus x_4 = 0$
	{2, 14, 6, 10}	$x_5 = 0$, $x_1 = 0$, $x_4 = 1$
	{24, 6, 8, 22}	$x_5 = 0$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_3 = 1$
	{8, 9, 10, 11}	$x_1 = 0$, $x_2 = 1$, $x_3 = 0$
24	{16, 1, 3, 18}	$x_2 = 0$, $x_3 = 0$, $x_1 \oplus x_5 = 1$
	{16, 1, 15, 30}	$x_2 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$, $x_2 \oplus x_3 = 0$
	{16, 3, 5, 22}	$x_2 = 0$, $x_1 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 1$
	{16, 5, 15, 26}	$x_2 \oplus x_4 = 0$, $x_1 \oplus x_3 = 1$, $x_3 \oplus x_5 = 1$
	{1, 5, 18, 22}	$x_2 = 0$, $x_1 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$
	{1, 5, 26, 30}	$x_1 \oplus x_2 = 0$, $x_1 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$
	{3, 15, 18, 30}	$x_2 \oplus x_3 = 0$, $x_4 = 1$, $x_1 \oplus x_5 = 1$
	{3, 15, 22, 26}	$x_1 \oplus x_5 = 1$, $x_4 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{18, 22, 26, 30}	$x_5 = 0$, $x_4 = 1$, $x_1 = 1$
25	{12, 15, 10, 9}	$x_1 = 0$, $x_3 \oplus x_4 \oplus x_5 = 1$, $x_2 = 1$
	{12, 6, 22, 28}	$x_5 = 0$, $x_3 = 1$, $x_2 \oplus x_4 = 1$
	{2, 9, 6, 13}	$x_2 \oplus x_5 = 0$, $x_2 \oplus x_4 = 1$, $x_1 = 0$
	{2, 10, 30, 22}	$x_5 = 0$, $x_4 = 1$, $x_1 \oplus x_3 = 0$
	{15, 28, 13, 30}	$x_1 \oplus x_5 = 1$, $x_2 = 1$, $x_3 = 1$
26	{16, 1, 10, 27}	$x_3 = 0$, $x_2 \oplus x_4 = 0$, $x_1 \oplus x_2 \oplus x_5 = 1$
	{16, 5, 11, 30}	$x_1 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 = 0$
	{5, 1, 22, 18}	$x_1 \oplus x_5 = 1$, $x_1 \oplus x_4 = 0$, $x_2 = 0$
	{23, 10, 11, 22}	$x_4 =$, $x_1 \oplus x_2 = 1$, $x_1 \oplus x_3 = 0$
	{18, 27, 23, 30}	$x_2 \oplus x_3 \oplus x_5 = 0$, $x_1 = 1$, $x_4 = 1$

Table .15: List of all 2D Affine Equations of Ascon for δ^{out}= 21, 22, 23, 24, 25, 26.

δ^{out}	**2D affine subspaces**	**Corresponding linear equations**
29	{2, 15, 21, 27}	$x_1 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{2, 15, 22, 27}	$x_2 \oplus x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 0$
	{5, 21, 13, 29}	$x_4 = 0$, $x_3 = 1$, $x_5 = 1$
	{5, 21, 6, 22}	$x_2 = 0$, $x_3 = 1$, $x_4 \oplus x_5 = 1$
	{5, 29, 6, 30}	$x_1 \oplus x_2 = 0$, $x_3 = 1$, $x_4 \oplus x_5 = 1$
	{5, 13, 22, 30}	$x_1 \oplus x_4 = 0$, $x_3 = 1$, $x_1 \oplus x_5 = 1$
	{30, 22, 21, 29}	$x_1 = 1$, $x_3 = 1$, $x_4 \oplus x_5 = 1$
	{21, 6, 13, 30}	$x_3 = 1$, $x_4 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_4 = 1$
	{21, 22, 24, 27}	$x_1 = 1$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 \oplus x_5 = 1$
	{29, 6, 13, 22}	$x_1 = 1$, $x_3 \oplus x_4 = 1$, $x_3 \oplus x_5 = 1$
	{29, 27, 24, 30}	$x_3 = 1$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_5 = 0$
30	{4, 8, 18, 30}	$x_5 = 0$, $x_1 \oplus x_2 \oplus x_3 = 1$, $x_1 \oplus x_4 = 0$
	{1, 9, 22, 30}	$x_1 \oplus x_3 = 0$, $x_1 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$
	{1, 11, 18, 24}	$x_1 \oplus x_5 = 1$, $x_3 = 0$, $x_1 \oplus x_2 \oplus x_4 = 0$
	{8, 25, 9, 24}	$x_3 = 0$, $x_4 = 0$, $x_2 = 1$
31	{2, 10, 5, 13}	$x_1 = 0$, $x_3 \oplus x_5 = 0$, $x_3 \oplus x_4 = 1$
	{2, 6, 26, 30}	$x_4 = 1$, $x_5 = 0$, $x_1 \oplus x_2 = 0$
	{2, 10, 22, 30}	$x_5 = 0$, $x_4 = 1$, $x_1 \oplus x_3 = 0$
	{5, 8, 21, 24}	$x_2 \oplus x_3 = 1$, $x_4 = 0$, $x_2 \oplus x_5 = 1$
	{5, 8, 6, 11}	$x_1 = 0$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_4 \oplus x_5 = 1$
	{5, 21, 6, 22}	$x_1 = 0$, $x_2 = 1$, $x_4 = 1$
	{5, 21, 10, 26}	$x_2 \oplus x_4 = 0$, $x_2 \oplus x_3 = 1$, $x_2 \oplus x_5 = 1$
	{5, 11, 22, 24}	$x_2 \oplus x_3 = 1$, $x_1 \oplus x_2 \oplus x_4 = 0$, $x_1 \oplus x_5 = 1$
	{5, 13, 22, 30}	$x_3 = 1$, $x_1 \oplus x_5 = 1$, $x_1 \oplus x_4 = 0$
	{8, 6, 22, 24}	$x_5 = 0$, $x_2 \oplus x_4 = 1$, $x_2 \oplus x_3 = 1$
	{8, 10, 24, 26}	$x_2 = 1$, $x_5 = 0$, $x_3 = 1$
	{21, 6, 11, 24}	$x_1 \oplus x_4 = 1$, $x_2 \oplus x_3 = 0$, $x_1 \oplus x_2 \oplus x_5 = 0$
	{21, 6, 13, 30}	$x_3 = 1$, $x_4 \oplus x_5 = 1$, $x_1 \oplus x_2 \oplus x_4 = 1$
	{6, 10, 22, 26}	$x_4 = 1$, $x_5 = 0$, $x_2 \oplus x_3 = 1$
	{11, 13, 24, 30}	$x_1 \oplus x_5 = 1$, $x_1 \oplus x_3 \oplus x_4 = 1$, $x_2 = 1$

Table .16: List of all 2D Affine Equations of Ascon for δ^{out}= 29, 30, 31.