Characterization of Column Parity Kernel and Differential Cryptanalysis of Keccak

Yin Tan, Kalikinkar Mandal and Guang Gong

Department of Electrical and Computer Engineering, University of Waterloo, Canada
{y24tan,kmandal,ggong}@uwaterloo.ca

Abstract. Keccak was seleted as SHA-3 by NIST among 64 submissions in 2012. The submitted version of Keccak has an internal state size of $b = 1600$ bits, and the output size of $224, 256, 384, 512$ bits. Recently, the differential cryptanalysis on Keccak has been received a lot of attention for building a distinguisher and for producing (near-)collisions. In these investigations, a common technique used for finding a good differential path is to choose an input difference from the column parity kernel (CP-kernel). In this paper, we first present the transformation matrices of the linear components θ, ρ, π of the Keccak round function. Using the transformation matrix for θ, we show that the dimension of the CP-kernel is $20w + 1$, instead of the value $20w$ provided in the submission of Keccak, where $w = 2^\ell$, $b = 25w$. Then we determine the exact number of CP-kernel elements of Hamming weight t with $1 \leq t \leq b$ and provide an algorithm for finding all CP-kernel elements with Hamming weight t. This greatly improves the complexity of finding low Hamming weight CP-kernel elements, compared to a random search or slice-wise search. We also study the double kernel path, which was mentioned by the designers of Keccak and some of them were discovered by Naya-Plasencia *et al.*. We first provide a characterization of such differential paths, and then, based on this characterization and exploiting an interesting property of Keccak's Sbox, we propose a new algorithm for finding all double kernel paths of Keccak. Finally, we propose the concept of almost double kernel path by modifying a condition of the double kernel path. After providing the characterization of almost double kernel paths and an algorithm for searching them, we present the best 2- and 3-round differential paths known so far, which can lead to 4-round collisions and 5-round near-collisions for Keccak-224, 256, 384, 512 using the target difference algorithm.
Keywords: Keccak, SHA-3, Column parity kernel, Differential cryptanalysis, Linear algebra, Collision

1 Introduction

Cryptographic hash function is a function which compresses a long message to a shorter one, or equivalently, is a function from $\{0,1\}^*$ to $\mathbb{F}_2^n$. The design and cryptanalysis of hash functions is one of the most important topics in cryptography due to their wide applications on providing assurance of data integrity. For instance, they are used in digital signature algorithms and message authentication codes. For the applications of hash functions, one is referred to, for instance, the textbooks [17,19]. As a secure hash function, it should resist preimage, second-preimage and collision attacks. In recent years, a number of serious threats have been found on the standardized hash functions [20,21,22] and in response to these threats, NIST initialized the SHA-3 competition in November 2007. In October 2012, NIST announced Keccak as the winner of the competition [3]. The design of Keccak is based on the sponge construction [3], and the submitted version of Keccak has an internal state size of $b = 1600$ bits, and the output size of $\{224, 256, 384, 512\}$ bits.

A lot of cryptanalyses on Keccak-$f[b]$ have been performed including distinguishing attacks, second-preimage attacks and differential attacks [1,2,7,8,10,11,18]. Using a zero-sum distinguisher [14], one can build a distinguisher for a significant number of rounds of the internal permutation of Keccak [6,7,8,15]. Bernstein presented a (second-)preimage attack on 8-round Keccak with computational complexity $2^{511.5}$ for the version with output 512 bits [2]. Recently, several research papers on the differential cryptanalysis of Keccak-$f[b]$ have been published [10,11,18]. Naya-Plasencia *et al.* [18] discovered the differential characteristics up to 3-round for Keccak. In [18], the authors made use of the free bits of the input to obtain CPK elements with low Hamming weights and discovered some double kernel paths. Duc *et al.* [11] presented the differential characteristics up to 5-round for all variants of Keccak. Using the differential characteristic and applying further techniques, either a distinguisher of Keccak with more number of

rounds can be built [11,18], or (near-)collisions can be produced [10,18]. It is worth to mention that the authors in [10,18] used the column parity kernel (CPK) elements as input difference to obtain good differential characteristics. The key reason for choosing a CPK element as an input difference Δ is that the Hamming weight of the input difference will the same as the Hamming weight of $\pi\rho\theta(\Delta)$, after passing through the diffusion layer in the first round. As a result, the number of active Sboxes in the Sbox layer will still be fewer. In [3], the designers of Keccak mentioned the existence of double kernel paths (2-round kernel paths). Dinur *et al.* [10] proposed the target difference algorithm for extending two more rounds of Keccak and presented the 4-round collisions and 5-round near-collisions using 2-round and 3-round differential characteristics, respectively.

In this paper, we first provide the characterization of the CPK elements as it is important for the future cryptanalysis of Keccak. In our study, we consider the transformation matrix for each linear transformation θ, π, ρ of Keccak's round function, and hence the structure of the CPK can be regarded as the kernel space of the linear transformation $(\theta + id)$, where id is the identity mapping. We prove the dimension of the CPK is $20w + 1$ with $w = 2^\ell$, $b = 25w$, and hence the size of the CPK is 2^{20w+1}. This points out a mistake in the submission of Keccak [3] that claims the size of the CPK is 2^{20w} (see [3, Section 2.4.3]). In addition to compute the dimension of the CPK, for a give integer t with $1 \leq t \leq b$, we explicitly determine all CPK elements with Hamming weight t and enumerate the exact number of such elements. Moreover, based on this result, we propose a new algorithm for determining all CPK elements with a given Hamming weight.

We then study the double kernel paths. Although some of them were discovered in [18], it is not clear that which elements may generate double kernel paths. First, we present a necessary and sufficient condition for the existence of double kernel paths/trails. Relying on the characterization and exploiting an interesting property of the nonlinear function χ_5 in Keccak, we provide an algorithm for determining all double kernel paths and our experiment finds many new 2-round kernel paths. We should mention that a similar technique that our algorithm uses can also be found in [10,12,13]. Finally, we propose a variant of the double kernel path, called *almost double kernel path*. A similar characterization of almost double paths and an algorithm for searching them are presented. We apply the algorithm on Keccak and successfully discover the best differential paths for 2-round and 3-round. Applying the target difference algorithm, one can produce 4-round collisions and 5-round near-collisions using the newly obtained 2-round and 3-round paths with the best complexity. We provide a comparison of the complexity for producing 4-round collisions and 5-round near-collisions in Table 1. In the table, we write the number of rounds as the form $(2 + r)$ to denote our new differential path is r-round plus the extra two rounds by the rebound attack and the target difference algorithm.

Table 1. The complexity comparison for finding collisions and near-collisions

(2+2)-round		(2+3)-round		(2+2)-round		(2+3)-round		Ref
Keccak-224	Keccak-256	Keccak-224	Keccak-256	Keccak-384	Keccak-512	Keccak-384	Keccak-512	
2^{-23}	2^{-23}	2^{-41}	2^{-45}	2^{-23}	2^{-23}	2^{-51}	2^{-60}	This paper
2^{-24}	2^{-24}	2^{-57}	2^{-59}	–	–	–	–	[10]

The rest of the paper is organized as follows. In Section 2, we briefly review the design of Keccak, but from the scrambling mode point of view. We also give the transformation matrices of the linear transformations of the round function of Keccak, which will be used in the following sections. We study the structure of the CPK and determine its the dimension in Section 3. One can find the exact number of CPK elements with Hamming weight t and how to obtain all such elements therein. In Section 4, we first provide a characterization of a double kernel path, followed by its application to Keccak for finding new double kernel paths. Finally, we characterize almost double kernel path and present the best 2- and 3-round differential paths known so far.

2 Another look at the design of Keccak-$f[b]$

In this section, we briefly review the design of Keccak. Instead of repeating the description of Keccak as those in [3], we introduce Keccak from the scrambling mode of operation point of view. There are total seven instances of Keccak$[b]$ for width $b = 25 \cdot 2^\ell$ with $0 \leq \ell \leq 6$ and the number of iteration for Keccak$[b]$ is $N_r = 2\ell + 12$.

2.1 Notations

In this section, we fix some notations which will be used throughout the paper.

- $\mathbb{F}_2 = \{0, 1\}$ is the Galois field with 2 elements.
- $b = 25 \cdot w$, where $w = 2^\ell$ for $0 \leq \ell \leq 6$;
- For a linear transformation $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the notation $\mathrm{Ker}(L)$ denotes the kernel (null) space of L, i.e., the set of elements with $L(x) = 0$;
- For a linear function L from $\mathbb{F}_2^n$ to itself, its transformation matrix is denoted by M_L; $\dim(\mathrm{Ker}(M_L))$ denotes the dimension of $\mathrm{Ker}(M_L)$.
- Given any field $\mathbb{F}_{2^n}$, we identify it the same as the vector space $\mathbb{F}_2^n$;
- For a binary sequence $\mathbf{s}$, define its support set $\mathrm{Supp}(\mathbf{s}) = \{i : 0 \leq i \leq \mathrm{len}(\mathbf{s}) - 1 | \mathbf{s}[\mathrm{i}] = 1\}$;
- If do not state explicitly, we use Keccak to denote Keccak-$f[1600]$;
- $\mathrm{LSB}_r(B)$ and $\mathrm{MSB}_c(B)$ denote the first r right-most bits and the last c left-most bits of B, respectively, i.e., $B = \mathrm{MSB}_c(B)||\mathrm{LSB}_r(B)$, if the length of B equals $(c + r)$.
- $\mathbb{M}(\mathbb{F}_2, m, n)$ is the ring of $m \times n$ matrices with elements in $\mathbb{F}_2$;
- For a vector $\mathbf{c}$, $\mathrm{wt}(\mathbf{c})$ denotes its Hamming weight, i.e. the number of positions in $\mathbf{c}$ which are nonzero;
- Given s integers k_i with $\sum_{i=1}^{s} k_i = n$, the notation $\binom{n}{k_1,\ldots,k_s}$ denotes the multinomial coefficient defined by $\binom{n}{k_1,\ldots,k_s} = \frac{n!}{k_1!\cdots k_s!}$.

2.2 Overview of Keccak in scrambling mode

The design of Keccak is based on the sponge construction [3] and the operation of Keccak$[b]$ consists of two phases, the *absorbing* phase and the *squeezing* phase. Before inputting a message $M \in \{0, 1\}^*$ to Keccak, it is first padded by the multi-rate rule so that the length of $M' = \mathrm{pad(M)}$ is a multiple of r ([3, page 7]).

Writing M' as the form $M' = M_1||M_2||\cdots||M_d$ such that $M_i \in \mathbb{F}_2^r$, $1 \leq i \leq d$. The internal state of Keccak can be considered as a register of length $b = c + r$, where in the first right-most r bits, an input message M_i is absorbed. The function f is obtained by iterating of the round function R (defined below) N_r times. Letting B_i be the content of the internal state of the register at the i-th round. Before absorbing the message M_1, the register is initialized with all-zero, i.e., $B_0 = \mathbf{0}$. For the first message M_1, the content of the register is $B_1 = \mathrm{MSB}_c(B_0)||(M_1 \oplus \mathrm{LSB}_r(B_0))$. For each message M_i, the content B_i of the register is taken as input to the Keccak permutation f and the Keccak permutation outputs $B = f(\mathrm{MSB}_c(B_i)||(M_i \oplus \mathrm{LSB}_r(B_i)))$. The internal state for message M_{i+1} is updated as $B_{i+1} = \mathrm{MSB}_c(B)||(M_{i+1} \oplus \mathrm{LSB}_r(B))$.

When all messages M_i's are processed by the absorbing phase, Keccak switches to the squeezing phase. After the absorbing phase, the output of the Keccak permutation is $B_{d+1} = f(B_d)$, which is the content of the register. In the squeezing phase, the register is updated as $B_{i+1} = f(B_i), B_{d+1} = f(B_d), i \geq d + 1$. Assume that Keccak is required to output t bits and s is the smallest integer such that $0 \leq sr - t \leq r - 1$. For $1 \leq j \leq s$, Keccak outputs $\mathrm{LSB}_r(B_j)$, denoted by O_j. Finally, after having the value $O = O_1||O_2||\cdots||O_s$, Keccak outputs $\mathrm{MSB}_t(O)$. A block diagram of Keccak's absorbing and squeezing phase is illustrated in Figures 1 and 2. The mode of operation presented in Figure 1 is known as the *scrambling mode* [9].

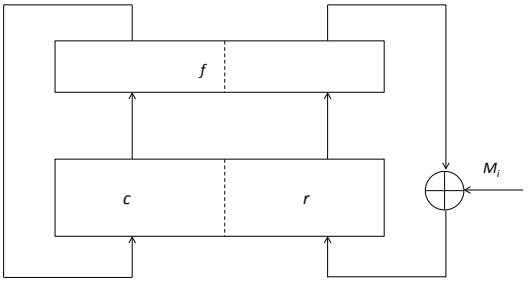


Fig. 1. Absorbing phase of Keccak

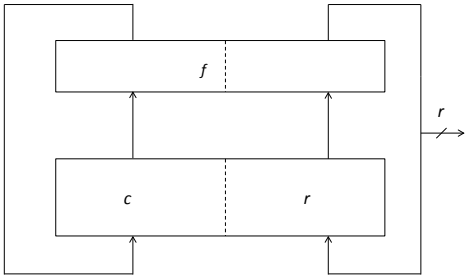


Fig. 2. Squeezing phase of Keccak

2.3 Round function of Keccak

The round function R of Keccak is composed of 5 functions, $R = \mathrm{RC} \circ \chi \circ \pi \circ \rho \circ \theta$, where RC is the round constant addition function, $\chi = (\chi_5, \cdots, \chi_5)$ is the S-box layer and χ_5 is a permutation from $\mathbb{F}_{2^5}$ to itself, and the functions π, ρ, θ are linear permutations. The following figure shows the flow of the round function.

$$S_i \xrightarrow{\theta} S_i^1 \xrightarrow{\pi} S_i^2 \xrightarrow{\rho} S_i^3 \xrightarrow{\chi} S_i^4 \xrightarrow{\mathrm{RC}} S_{i+1}.$$

Fig. 3. Round function of Keccak

For $d = w(5y + x) + z$, an integer d in the range $[0, b-1]$ uniquely corresponds to a 3-tuple $[x, y, z]$ and vice versa, where $x, y \in \mathbb{Z}_5$ and $z \in \mathbb{Z}_w$ with $w = 2^\ell$. Using this one-to-one correspondence, the designers of Keccak mapped an element in $\mathbb{F}_2^b$ as an element that is a three-dimensional array of elements in $\mathbb{F}_2$. Such representation of elements in $\mathbb{F}_2^b$ originates from the design of Keccak and it describes Keccak very elegantly. However, for the convenience of our study of Keccak, we prefer to express an element in $\mathbb{F}_2^b$ as a one-dimensional array, not a three-dimension array. It is very easy to achieve this by regarding a 3-tuple $[x, y, z] \in \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_w$ as an integer $d = w(5y + x) + z$. Note that the arithmetic operations of x and y are over $\mathbb{Z}_5$ and the operations of z are over $\mathbb{Z}_w$.

We describe the Keccak round function by the composition of the product of several matrices and the Sbox layer. One should note that, using this representation, we need to change the flow of the round function in Figure 3 a little by introducing a new function α, called *arrange bits function*. Because, when an internal state passes through χ, the bits of the internal state are needed to arrange in order to apply the 5-bit Sbox χ_5. More precisely, by the definition of χ in [3], given an internal state $(a_0, ..., a_{b-1})$, the i-th Sbox takes $(a_{5rw+s}, a_{(5r+1)w+s}, ..., a_{(5r+4)w+s})$ as input where $i = 5s + r$ and $0 \le s \le 63$, $0 \le r \le 4$. In other words, α is a function from $\mathbb{F}_2^b$ to $\mathbb{F}_2^b$ defined by

$$\alpha : (a_i : 0 \le i \le b-1) \mapsto \left(a_{(5r+j)w+s} : 0 \le j, r \le 4, 0 \le s \le 63\right). \tag{1}$$

It is easy easy to verify that α is a linear function. We denote by M_θ, M_ρ, M_π, and M_α the transformation matrices for the linear transformations θ, ρ, π and α, respectively. We note that each matrix is a square matrix of order b. Mathematically, the above four matrices are defined

as

$$(M_\theta)_{i,j} = \begin{cases} 1 & \text{if } i = j, 0 \le i, j \le b-1, \\ 1 & \text{if } i = w(5y+x)+z, j = w(5y'+x-1)+z, 0 \le y' \le 4, \\ 1 & \text{if } i = w(5y+x)+z, j = w(5y'+x+1)+z-1, 0 \le y' \le 4, \\ 0 & \text{otherwise,} \end{cases}$$

$$(M_\rho)_{i,j} = \begin{cases} 1 & \text{if } i = w(5y+x)+z, j = w(5y+x)+z-T(x,y), \\ 0 & \text{otherwise,} \end{cases}$$

$$(M_\pi)_{i,j} = \begin{cases} 1 & \text{if } i = w(5y+x)+z, j = w(5(2x+3y)+y)+z, \\ 0 & \text{otherwise,} \end{cases}$$

$$(M_\alpha)_{i,j} = \begin{cases} 1 & \text{if } i = 25s+r, j = wr+s, 0 \le r \le 24, 0 \le s \le 63 \\ 0 & \text{otherwise,} \end{cases}$$

where $T(x,y)$ is the translation constant defined in [3]. In [**?**,11], the authors used "$+T(x,y)$" while defining ρ transformation, but in the specification [3] the designer of Keccak used "$-T(x,y)$" while defining ρ transformation. In this paper, we follow the definition of ρ transformation as what is presented in the specification. Note that each row of M_θ contains 11 ones, and the matrices M_ρ, M_π, and M_α are permutation matrices. By the definition of π and ρ in Section 2, one can easily check that they are both permutation transformations, or equivalently, the transformation matrices corresponding to them are permutation matrices (there is exactly one 1 in each row and column). Using the above matrices, the round function R of Keccak can be written as $R = \mathrm{RC} \circ M_\alpha^{-1} \circ \chi \circ M_\alpha \cdot M_\pi \cdot M_\rho \cdot M_\theta$ and the flow of the round function is as follows: where $\cdot$ denotes the matrix multiplication and $\circ$ denotes the composition of χ and a

$$S_i \xrightarrow{M_\theta} S_i^1 \xrightarrow{M_\rho} S_i^2 \xrightarrow{M_\pi} S_i^3 \xrightarrow{M_\alpha} S_i^4 \xrightarrow{\chi} S_i^5 \xrightarrow{M_\alpha^{-1}} S_i^6 \xrightarrow{\mathrm{RC}} S_{i+1}$$

Fig. 4. Round function of Keccak using transformation matrix

linear function. Since in the rest of the paper we are considering the differential cryptanalysis of Keccak, we will omit the function RC in the following sections.

3 Column parity kernel

In the differential cryptanalysis of Keccak, it is natural to choose an input difference Δ such that, after passing through the diffusion layer $\alpha \circ \pi \circ \rho \circ \theta$, the Hamming weight of the image $(\alpha \circ \pi \circ \rho \circ \theta)(\Delta)$ will not increase too much, since it will invoke fewer active Sboxes and will not increase the complexity too much. To achieve this, we only need to find an input difference Δ such that $\mathrm{wt}(\theta(\Delta)) - \mathrm{wt}(\Delta)$ is as small as possible (recall that the transformation matrices of ρ, π, α are permutation matrices). Of course, in the optimal case one may expect is that $\mathrm{wt}(\theta(\Delta)) - \mathrm{wt}(\Delta) = 0$ and this can be achieved when $\theta(\Delta) = \Delta$. We give the following definition which appeared in [3].

Definition 1 ([3]). *An input difference Δ is called a column parity kernel (CPK in short) element if it is invariant to the function θ, i.e. $\theta(\Delta) = \Delta$.*

In the following, we first study the transformation matrix for θ and prove the dimension of the CPK is $20w+1$ rather than $20w$ as stated in [3, page 25], followed by determining all CPK elements. Then we enumerate the exact number of CPK elements for a given Hamming weight t and provide a new algorithm for finding all CPK elements with Hamming weight t.

3.1 Transformation matrix of θ

Since θ is a linear function from $\mathbb{F}_2^b$ to $\mathbb{F}_2^b$, we may represent the linear transformation θ by its transformation matrix M_θ with entries in $\mathbb{F}_2$. The following result determines the matrix M_θ.

Theorem 1. *Let $b = 25w$, where $w = 2^\ell$ and $0 \le \ell \le 6$. The matrix M_θ corresponding to the linear transformation θ is as following:*

$$M_\theta = \begin{pmatrix} X + I_{5w} & X & X & X & X \\ X & X + I_{5w} & X & X & X \\ X & X & X + I_{5w} & X & X \\ X & X & X & X + I_{5w} & X \\ X & X & X & X & X + I_{5w} \end{pmatrix}, \tag{2}$$

where X is the $5w \times 5w$ matrix defined in Table 2 below and I_{5w} is the $5w \times 5w$ identity matrix.

Proof. For an internal state $S = (S_0, ..., S_{b-1})$, recall that $\theta : \mathbb{F}_2^b \to \mathbb{F}_2^b$ is defined by

$$\theta\left(S_{w(5y+x)+z}\right) = S_{w(5y+x)+z} + \sum_{y'=0}^{4} S_{w(5y'+(x-1))+z} + \sum_{y'=0}^{4} S_{w(5y'+(x+1))+(z-1)}.$$

This implies that in the $(w(5y + x) + z)$-th row of M_θ, the entries in the following columns

$$\{w(5y + x) + z, w(5y' + (x - 1)) + z, w(5y' + (x + 1)) + (z - 1), 0 \le y' \le 4\} \tag{3}$$

are 1. It can be observed that all diagonal elements of M_θ are 1. Define the matrix $M' = M_\theta + I_b$ where I_b is the identity matrix of order b. We now show that each row and each column in M' are binary sequences of length b with period $5w$. We only prove the result for the rows and omit the proof for the columns as they are similar. For the i-th row of M', denote its support set by $\mathrm{Supp}_i = \{j \mid M'(i, j) = 1 \text{ and } 0 \le j \le b - 1\}$. In order to prove the $(w(5y + x) + z)$-th row of M' is a sequence of period $5w$, it is sufficient to show that $j \in \mathrm{Supp}_{w(5y+x)+z}$ if and only if $(j + 5w) \in \mathrm{Supp}_{w(5y+x)+z}$. Assume that $j = w(5y' + x') + z'$ for some $x', y' \in \mathbb{Z}_5$ and $z' \in \mathbb{Z}_w$. Since

$$(w(5y' + x') + z') + 5w = w(5(y' + 1) + x') + z' \tag{4}$$

and by (3), we see that $w(5y' + x') + z' \in \mathrm{Supp}_{w(5y+x)+z}$ if and only if $(w(5y' + x') + z') + 5w \in \mathrm{Supp}_{w(5y+x)+z}$. Note that $(y' + 1)$ in (4) is reduced by modulo 5. Therefore, the matrix M' can be written as

$$M' = \begin{pmatrix} X & X & X & X & X \\ X & X & X & X & X \\ X & X & X & X & X \\ X & X & X & X & X \\ X & X & X & X & X \end{pmatrix}, \tag{5}$$

where X is a $5w \times 5w$ matrix, which is determined as follows:

(i) For row 0, we have $0 = w(5 \cdot 0 + 0) + 0$ and hence $x = y = z = 0$. By (3) and applying the periodicity of the row (letting $y' = 0$), its support set is $\{4w, 2w - 1\}$;
(ii) For row 1, we have $1 = w(5 \cdot 0 + 0) + 1$ and then $x = y = 0, z = 1$. Similar as above, the support set is $\{w, 4w + 1\}$;
(iii) Continuing this process, the support sets of all rows of X are as following:

Table 2. Support sets of rows in X

Rows	Support set
0 to $w-1$	$\{2w-1,4w\},\{w,4w+1\},\{w+1,4w+2\},\ldots,\{2w-2,5w-1\}$
w to $2w-1$	$\{0,3w-1\},\{1,2w\},\{2,2w+1\},\ldots,\{w-1,3w-2\}$
$2w$ to $3w-1$	$\{w,4w-1\},\{w+1,3w\},\{w+2,3w+1\},\ldots,\{2w-1,4w-2\}$
$3w$ to $4w-1$	$\{2w,5w-1\},\{2w+1,4w\},\{2w+2,4w+1\},\ldots,\{3w-1,5w-2\}$
$4w$ to $5w-1$	$\{3w,w-1\},\{3w+1,0\},\{3w+2,1\},\ldots,\{4w-1,w-2\}$

We complete the proof. □

We present an interesting property of X by pointing out that X is the adjacent matrix of a cycle graph (a graph that consists of a single cycle).

Definition 2. *We define the θ'-graph $\mathcal{G}=(V,E)$ as follows:*

- *The set of vertices V is $\{\mathrm{Supp}(r_i): 0\le i\le 5w-1\}$, where $\mathrm{Supp}(r_i)$ is the support set of the i-th row of X;*
- *Two vertices R_1,R_2 are adjacent if and only if $R_1\cap R_2\neq\emptyset$.*

Proposition 1. *Let the notations be the same as Theorem 1. Then the girth of the θ'-graph $\mathcal{G}$ defined above is $5w$, or equivalently, the θ'-graph $\mathcal{G}$ is a $5w$-cycle graph.*

Proof. First we call vertices corresponding to the rows from 0 to $w-1$ type I vertices, from w to $2w-1$ type II vertices, from $2w$ to $3w-1$ type III vertices, from $3w$ to $4w-1$ type IV vertices, from $4w$ to $5w-1$ type V vertices. To prove the result, it is sufficient to find a $5w$-cycle in $\mathcal{G}$, which is rountine but easy. We provide the method to find such cycle and leave the details to the intereted readers. We start from the the first type I vertex $V_1=\{2w-1,4w\}$, one may find a type IV vertex $V_2=\{4w,2w+1\}$ which is incident to it. Clearly V_2 is incident to a type II vertex $V_3=\{2w+1,2\}$, V_3 is incident to a type V vertex $V_4=\{2,3w+3\}$, and V_4 is incident to a type III vertex $V_5=\{3w+3,w+4\}$. Finally, V_5 is incident to a type I vertex $V_6=\{w+4,4w+5\}$. Continuing this process (type I-type IV-type II-type V-type III-type I), one may find the required cycle. We finish the proof. □

We provide an example below to understand the interesting property in Proposition 1.

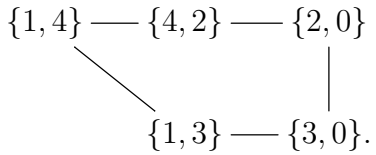
Example 1. When $b=25$, the transformation matrix M_θ of Keccak-f[25] is of the form (2), where X is given by

$$X=\begin{pmatrix}0\,1\,0\,0\,1\\1\,0\,1\,0\,0\\0\,1\,0\,1\,0\\0\,0\,1\,0\,1\\1\,0\,0\,1\,0\end{pmatrix}.$$

According to the definition of the graph $\mathcal{G}$, the vertices of $\mathcal{G}$ is the set

$$V=\{\{1,4\},\{0,2\},\{1,3\},\{2,4\},\{0,3\}\}.$$

It is easy to see that $\mathcal{G}$ is the following 5-cycle graph:



3.2 Dimension of column parity kernel

By Definition 1, an element Δ belongs to CPK if and only if $\theta(\Delta) = \Delta$, and then $(\theta+id)(\Delta) = 0$, where id is the identity mapping defined as $id(x) = x$. Denoting $\theta + id$ by θ'. Clearly θ' is still a linear transformation and we use the notation $M_{\theta'}$ to denote the transformation matrix of θ'. It is not difficult to show that $M_{\theta'} = M_\theta + I_b$ (it equals M' defined in (5)). Therefore, the dimension of the CPK is the dimension of the kernel space of $M_{\theta'}$, which is equal to $b - \mathrm{Rank}(M_{\theta'})$. The next result determines the rank of $M_{\theta'}$.

Theorem 2. *The rank of $M_{\theta'}$ is $5w-1$. Therefore, the dimension of the CP-kernel is $20w+1$.*

Proof. Clearly $M_{\theta'} = J \otimes X$, where J is the 5×5 all-one matrix and $\otimes$ is the Kronecker product of two matrices. Since $\mathrm{Rank}(M_{\theta'}) = \mathrm{Rank}(J \otimes X) = \mathrm{Rank}(X)\mathrm{Rank}(J) = \mathrm{Rank}(X)$ (note that $\mathrm{Rank}(J) = 1$), it is enough to determine the rank of X which is defined in Table 2. It can be seen from Table 2 that each index i with $0 \le i \le 5w-1$ appears in the support sets of the rows of X exactly twice. Therefore, by denoting the rows of X by r_i with $0 \le i \le 5w-1$ and by notice that all entries of X belong to $\mathbb{F}_2$, we have

$$r_0 + r_1 + \cdots + r_{5w-1} = (0, 0, \ldots, 0).$$

Since none of rows in X is a zero vector and by the above equation the sum of any $(5w-1)$ rows is nonzero. Therefore, we have that $\mathrm{Rank}(M_{\theta'}) = \mathrm{Rank}(X) = 5w-1$ and $\dim(\mathrm{Ker}(M_{\theta'})) = b - \mathrm{Rank}(M_{\theta'}) = 20w+1$. This completes the proof. □

Remark 1. If the entries of $M_{\theta'}$ are regarded as integers 0 and 1, then one may check that the rank of $M_{\theta'}$ is $5w$. Hence the dimension of the CPK is $20w$. However, since θ' is a linear transformation over $\mathbb{F}_2^b$, the entries of its transformation matrix should be in $\mathbb{F}_2$ (the rank is the so-called 2-rank).

3.3 Determining all CP-kernel elements

As explained at the beginning of Section 3, a CPK element of low Hamming weight can be used as the input difference of a differential path. For example, in [3,10,11,18], the authors used the CPK elements, for instance, with Hamming weights 2 and 6 as the input differences and they found good differential characteristics. However, to the best of our knowledge, there is no method that can determine all CPK elements with a given Hamming weight. In this section, we make use of Theorems 1 and 2 to determine all CPK elements with Hamming weight t for $1 \le t \le b$. We use the following lemma to prove the main theorem in this section. For convenience, for any two vectors $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_2^{b/5}$, we use the notation $\mathrm{Supp}(\mathbf{c}_1, \mathbf{c}_2)$ to denote the number of positions in $\mathbf{c}_1, \mathbf{c}_2$ such that they are both equal 1.

Lemma 1. *For any four vectors $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \boldsymbol{c}_4 \in \mathbb{F}_2^{b/5}$, we have*

(i) $\mathrm{wt}(\boldsymbol{c}_1 + \boldsymbol{c}_2) = \mathrm{wt}(\mathbf{c}_1) + \mathrm{wt}(\mathbf{c}_2) - 2\mathrm{Supp}(\mathbf{c}_1, \mathbf{c}_2)$;

(ii) $\mathrm{wt}\left(\sum_{i=1}^{4} \mathbf{c}_i\right) = \sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i) - 2\left(\mathrm{Supp}(\mathbf{c}_1, \mathbf{c}_2) + \mathrm{Supp}(\mathbf{c}_3, \mathbf{c}_4) + \mathrm{Supp}(\mathbf{c}_1 + \mathbf{c}_2, \mathbf{c}_3 + \mathbf{c}_4)\right)$.

Proof. The result (i) is well known [16], we omit the proof. For (ii), denoting $\mathbf{c} = (\mathbf{c}_1 + \mathbf{c}_2) + (\mathbf{c}_3 + \mathbf{c}_4)$. Applying (i), we have $\mathrm{wt}(\mathbf{c}) = \mathrm{wt}(\mathbf{c}_1 + \mathbf{c}_2) + \mathrm{wt}(\mathbf{c}_3 + \mathbf{c}_4) - 2\mathrm{Supp}(\mathbf{c}_1 + \mathbf{c}_2, \mathbf{c}_3 + \mathbf{c}_4)$. Further applying (i) on the right hand side of the above equation we get the required equation. The proof is completed. □

Theorem 3. *Let t be a positive integer with $1 \le t \le b$. For a column vector $\boldsymbol{c}$ of length b, writing it as the form $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_5)^T$, where $\boldsymbol{c}_i$ is a column vector of length $b/5$ for $1 \le i \le 5$. Assume the Hamming weight of $\boldsymbol{c}$ is t. Then $\boldsymbol{c}$ is a CPK element if and only if $\sum_{i=1}^{5} \boldsymbol{c}_i \in \{\boldsymbol{0}, \boldsymbol{1}\}$, where $\boldsymbol{0}, \boldsymbol{1}$ are the all-zero and all-one vectors of length $b/5$. Furthermore, the set of CPK elements with Hamming weight t is:*

(i) if $t < b/5$, then

$$CPK_t = \left\{ (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_4, \sum_{i=1}^{4} \boldsymbol{c}_i)^{\mathrm{T}} \mid \sum_{i=1}^{4} \mathrm{wt}(\boldsymbol{c}_i) + \mathrm{wt}\left(\sum_{i=1}^{4} \boldsymbol{c}_i\right) = t \right\}.$$

(ii) if $b/5 \leq t \leq b$, then

$$CPK_t = \left\{ (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_4, \sum_{i=1}^{4} \boldsymbol{c}_i)^{\mathrm{T}} \mid \sum_{i=1}^{4} \mathrm{wt}(\boldsymbol{c}_i) + \mathrm{wt}\left(\sum_{i=1}^{4} \boldsymbol{c}_i\right) = t \right\}$$
$$\bigcup \left\{ (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_4, \boldsymbol{1} + \sum_{i=1}^{4} \boldsymbol{c}_i)^{\mathrm{T}} \mid \sum_{i=1}^{4} \mathrm{wt}(\boldsymbol{c}_i) - \mathrm{wt}\left(\sum_{i=1}^{4} \boldsymbol{c}_i\right) = t - b/5 \right\}.$$

where $\boldsymbol{c}_i \in \mathbb{M}(\mathbb{F}_2, b/5, 1)$ for $1 \leq i \leq 4$. Finally, there is no CPK elements with odd Hamming weight, and when the weight t is even, the size of CPK_t is:

(iii) if $t < b/5$, then

$$\#CPK_t = \sum_{(x_0,\ldots,x_{15}) \in \Phi_1} \binom{b/5}{x_0, x_1, \ldots, x_{15}},$$

(iv) if $b/5 \leq t \leq b$, then

$$\#CPK_t = \sum_{(x_0,\ldots,x_{15}) \in \Phi_1 \cup \Phi_2} \binom{b/5}{x_0, x_1, \ldots, x_{15}},$$

where Φ_1 and Φ_2 are defined in (8) and (9) below.

Proof. First of all, by the proof of Theorem 2, the rank of X is $5w-1$, and hence $\dim(\mathrm{Ker}(X)) = 5w-(5w-1) = 1$. Since the weight of each row of X is 2, it is easy to see then $\mathrm{Ker}(X) = \{\mathbf{0}, \mathbf{1}\}$. By Theorem 1, an element $\mathbf{c}$ is a CPK element if and only if $M_{\theta'} \cdot \mathbf{c} = \mathbf{0}$. By the form of $M_{\theta'}$ in (5), expanding the equation $M_{\theta'} \cdot \mathbf{c} = \mathbf{0}$ we have

$$(X(\mathbf{c}_1 + \cdots + \mathbf{c}_5), \ldots, X(\mathbf{c}_1 + \cdots + \mathbf{c}_5)) = \mathbf{0},$$

which implies that $X(\mathbf{c}_1 + \cdots + \mathbf{c}_5) = \mathbf{0}$, hence $\mathbf{c}_1 + \cdots + \mathbf{c}_5 \in \mathrm{Ker}(X)$. This proves the first part of the theorem.

Next, on the one hand, from the above arguments, it can be verified that all elements in $\mathrm{CPK_t}$ are in CPK as the sum of the $\mathbf{c}_i$ is in $\mathrm{Ker}(X)$ and their weights are t (one may use the result that $\mathrm{wt}(\mathbf{1} + \mathbf{c}) = b/5 - \mathrm{wt}(\mathbf{c})$ for $\mathbf{c} \in \mathbb{F}_2^{b/5}$ in the case $t \geq b/5$). On the other hand, for any element $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5) \in (\mathbb{F}_2^{b/5})^5$ with Hamming weight t, it is in CPK if and only if $\sum_{i=1}^{5} \mathbf{c}_i \in \mathrm{Ker}(X) = \{\mathbf{0}, \mathbf{1}\}$. If $\mathbf{c}_5 = \sum_{i=1}^{4} \mathbf{c}_i$, we obtain $\mathrm{wt}(\mathbf{c}_5) = t - \sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i)$, since $\mathrm{wt}(\mathbf{c}) = \sum_{i=1}^{5} \mathrm{wt}(\mathbf{c}_i)$. Similarly, if $\mathbf{c}_5 = \mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i$, we have $\mathrm{wt}(\mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i) = t - \sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i)$, and by substituting $\mathrm{wt}(\mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i) = b/5 - \mathrm{wt}(\sum_{i=1}^{4} \mathbf{c}_i)$, we obtain $b/5 - \mathrm{wt}(\sum_{i=1}^{4} \mathbf{c}_i) + \sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i) = t$. Finally, the case $\mathbf{c}_5 = \mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i$ only happens when $t \geq b/5$, since $\sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i) \geq \mathrm{wt}(\sum_{i=1}^{4} (\mathbf{c}_i))$. We complete the proof of the second part of the theorem.

Now we determine the size of CPK_t. We first show that there is no CPK elements with odd weight. Otherwise, $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5)$ is a CPK element with odd weight t. From the second part of this theorem, we know that $\mathbf{c}_5$ equals either $\sum_{i=1}^{4} \mathbf{c}_i$ or $\mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i$. In the former case, by Lemma 1(ii), the parity of $\mathrm{wt}(\mathbf{c}_5)$ is the same as the parity of $\sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i)$, and then $t = \mathrm{wt}(\mathbf{c}_5) + \sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i)$ is even, which is a contradiction. Similarly, for the latter case, we have that $\mathrm{wt}(\mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i) = b/5 - \mathrm{wt}(\sum_{i=1}^{4} \mathbf{c}_i)$. Since $t = \mathrm{wt}(\mathbf{c}_5) + \sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i) = b/5 - \mathrm{wt}(\sum_{i=1}^{4} \mathbf{c}_i) +$

$\sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i)$, and $b/5$ is even, $\mathrm{wt}(\sum_{i=1}^{4} \mathbf{c}_i)$ has the same parity with $\sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i)$, we again get t is even, which is a contradiction. In the following we assume that t is even. We first consider the case $t < b/5$. Again, from the second part of this theorem, we know that a CPK element $\mathbf{c}$ is of the form $\mathbf{c}_5 = \sum_{i=1}^{4} \mathbf{c}_i$, and $\sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i) + \mathrm{wt}\left(\sum_{i=1}^{4} \mathbf{c}_i\right) = t$. By Lemma 1(ii), we get

$$\sum_{i=1}^{4} \mathrm{wt}(\mathbf{c}_i) - (\mathrm{Supp}(\mathbf{c}_1, \mathbf{c}_2) + \mathrm{Supp}(\mathbf{c}_3, \mathbf{c}_4) + \mathrm{Supp}(\mathbf{c}_1 + \mathbf{c}_2, \mathbf{c}_3 + \mathbf{c}_4)) = t/2. \tag{6}$$

Therefore, the number of elements in CPK_t is equivalent to counting the number of elements $\mathbf{c}_i$ for $1 \le i \le 4$ that satisfy (6). Actually, for any four vectors $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4$, in each bit there are altogether 16 cases, i.e. from $(0,0,0,0)$ to $(1,1,1,1)$, we use the following table to list for each case, the value contributed to the left hand side of (6). For a CPK element with

$\begin{pmatrix}\mathbf{c}_1[i]\\ \mathbf{c}_2[i]\\ \mathbf{c}_3[i]\\ \mathbf{c}_4[i]\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\1\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\\1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\\0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\\1\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$
LHS of (6)	$0-0$	$1-0$	$1-0$	$2-1$	$1-0$	$2-1$	$2-1$	$3-1$	$1-0$	$2-1$	$2-1$	$3-1$	$2-1$	$3-1$	$3-1$	$4-2$

weight t, for $0 \le i \le 15$, assume the state i (in 4-bit binary expression form) appears in $\{(\mathbf{c}_1[j], \mathbf{c}_2[j], \mathbf{c}_3[j], \mathbf{c}_4[j])^{\mathrm{T}} : 1 \le j \le b/5\}$ for x_i times. Then, by (6), we have

$$\begin{aligned} &x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + 2x_7 + x_8 + x_9 + x_{10} + 2x_{11} + x_{12} + 2x_{13} + 2x_{14} + 2x_{15} = t/2,\\ &x_0 + x_1 + \cdots + x_{15} = b/5. \end{aligned} \tag{7}$$

Let

$$\Phi_1 = \{\mathbf{x} = (x_0, \ldots, x_{15}) : x_i \in \mathbb{N} \mid \mathbf{x} \text{ satisfies (7)}\}. \tag{8}$$

Therefore, by the above discussions, we see that there are $\binom{b/5}{x_0,\ldots,x_{15}}$ choices of $\mathbf{c}$ which are in CPK and with weight t, where $\mathbf{x} = (x_0, \ldots, x_{15}) \in \Phi_1$.

For the case $t \ge b/5$, a CPK element $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_5)$ can be either of the form $\mathbf{c}_5 = \sum_{i=1}^{4} \mathbf{c}_i$, or of the form $\mathbf{c}_5 = \mathbf{1} + \sum_{i=1}^{4} \mathbf{c}_i$. The proof is similar and we leave it to interested readers. The set Φ_2 is defined to be the set of solutions $\mathbf{x} = (x_0, \ldots, x_{15}) \in \mathbb{N}^{16}$ which satisfies the following equations:

$$\begin{aligned} &x_3 + x_5 + x_6 + x_7 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + 2x_{15} = t/2 - b/10,\\ &x_0 + x_1 + \cdots + x_{15} = b/5. \end{aligned} \tag{9}$$

We complete the proof. □

We explicitly give all CPK elements with Hamming weight 2 below.

Corollary 1. *There are* 3200 *CPK elements with Hamming weight* 2 *and they are all of the form* $(\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \boldsymbol{c}_4, \boldsymbol{c}_5)$*, where three of* $\boldsymbol{c}_i$ *are* $\boldsymbol{0}$ *and the other two are equal and with Hamming weight* 1*.*

Proof. Replacing $t = 2$ in Theorem 3, it is easy to verify that there are 10 solutions of the equation (7), all of which are of the form $\{x_0 = 319, x_i = 1, x_j = 0 \text{ for } j \ne i \text{ and } 0\}$, where $i \in \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12\}$. By Theorem 3, there are $10 \cdot \binom{320}{1,\ 319} = 3200$ CPK elements with Hamming weight 2. Furthermore, by the second part of Theorem 3, all such CPK elements are of the form in the theorem. □

We use the following table to list the number of CPK elements with Hamming weight up to 10 by Theorem 3. One may refer to [24] for a list of them. Please note that there are no CPK elements with odd weights.

Table 3. Number of CPK elements with Hamming Weight no more than 10

Weight	2	4	6	8	10
Number	3200	5105600	5415344000	$\approx 2^{41.3}$	$\approx 2^{50.1}$

The proof of Theorem 3 provides a method to search for all input differences in CPK and with a given Hamming weight. More precisely, we describe the method in the following Algorithm 1.

Algorithm 1 Finding All CPK Elements with Hamming Weight t

procedure T-HW-CPK(t)
  $M = \begin{pmatrix} \mathbf{c}_1 \\ \dots \\ \mathbf{c}_4 \end{pmatrix} \leftarrow \begin{pmatrix} 0 \ \dots \ 0 \\ \dots\dots\dots \\ 0 \ \dots \ 0 \end{pmatrix}_{4\times 320}$
  $\mathrm{CPK}_t \leftarrow \{\}$
  if $t < b/5$ **then**
    Determining Φ_1, the set of solutions $\mathbf{x}$ of Equation (7)
    for each $\mathbf{x} = (\mathbf{x_0}, \dots, \mathbf{x_{15}}) \in \mathbf{\Phi_1}$ **do**
      for $0 \le i \le 15$ **do**
        Choosing x_i columns from M and let the value be i (binary expression of i);
      end for
      $\mathrm{CPK_t} \leftarrow \mathrm{CPK_t} \cup \{(\mathbf{c}_1, \dots, \mathbf{c}_4, \sum_{\mathrm{i}=1}^{4} \mathbf{c}_\mathrm{i})\}$
      $M \leftarrow \mathbf{0}_{4\times 320}$
    end for
  else
    Determining Φ_1, Φ_2, the set of solutions $\mathbf{x}$ of Equations (7) and (9)
    for each $\mathbf{x} = (\mathbf{x_0}, \dots, \mathbf{x_{15}}) \in \mathbf{\Phi_1}$ **do**
      for $0 \le i \le 15$ **do**
        Choosing x_i columns from M and let the value be i (binary expression of i);
      end for
      $\mathrm{CPK_t} \leftarrow \mathrm{CPK_t} \cup \{(\mathbf{c}_1, \dots, \mathbf{c}_4, \sum_{\mathrm{i}=1}^{4} \mathbf{c}_\mathrm{i})\}$
      $M \leftarrow \mathbf{0}_{4\times 320}$
    end for
    for each $\mathbf{x} = (\mathbf{x_0}, \dots, \mathbf{x_{15}}) \in \mathbf{\Phi_2}$ **do**
      for $0 \le i \le 15$ **do**
        Choosing x_i columns from M and let the value be i (binary expression of i);
      end for
      $\mathrm{CPK_t} \leftarrow \mathrm{CPK_t} \cup \{(\mathbf{c}_1, \dots, \mathbf{c}_4, \mathbf{1} + \sum_{\mathrm{i}=1}^{4} \mathbf{c}_\mathrm{i})\}$
      $M \leftarrow \mathbf{0}_{4\times 320}$
    end for
    Output CPK_t
  end if
end procedure

4 Discovering all double kernel paths of Keccak

In [18], the authors used CPK elements as input differences to discover double differential paths (defined below). These differential paths are interesting as the difference of the state values after the first round is still a CPK element. To the best of our knowledge, there is no characterization of the input differences that may generate a double kernel path, although some of them were found in [18]. In this section, we give a characterization of the existence of such paths. Using this characterization and an interesting property of χ_5, we propose a new algorithm to find

double kernel paths. We should mention that all double kernel paths can be obtained by this algorithm.

4.1 Characterization of double kernel paths

We start by formally defining the double kernel path. One can also find the definition of double kernel path in [18].

Definition 3. *Let M be an element in $\mathbb{F}_2^b$. Define the tuple $\mathcal{M} = (M_1, M_2, M_3) \in (\mathbb{F}_2^b)^3$. It is called a double kernel path of Keccak if, for each integer i with $1 \leq i \leq 2$, the following hold:*

(i) $\theta(M_i) = M_i$;
(ii) $M_{i+1} = (\pi\rho)(M_i)$;
(iii) $\Pr_{x \in \mathbb{F}_2^b} (\chi(x + \alpha(\pi\rho)^i(M_i)) + \chi(x) = \alpha(\pi\rho)^i(M_i)) > 0$.

The following result gives the complexity of the differential attack using a double kernel path. The proof is easy and we omit it.

Proposition 2. *Let $\mathcal{M}$ be a double kernel path of Keccak. Assume that*

$$\Pr_{x \in \mathbb{F}_2^b} \left(\chi(x + \alpha(\pi\rho)^i(M_i)) + \chi(x) = \alpha(\pi\rho)^i(M_i)\right) = p_i$$

for each integer i with $1 \leq i \leq 2$. Then

$$\Pr_{x \in \mathbb{F}_2^b} \left(R^2(x + M_1) + R^2(x) = M_3\right) = p_1 p_2,$$

where R is the round function of Keccak and R^2 is the composition of 2 round functions.

We use Figure 5 to depict a double kernel path. Let $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M))$ be a double kernel differential path. In the figure, the arrow $A \xrightarrow{g} B$ denotes that $g(x + A) + g(x) = B$, i.e., the output difference of two internal states with difference A is B, the arrow $A \Rightarrow B$ denotes the result B is obtained from the condition A.

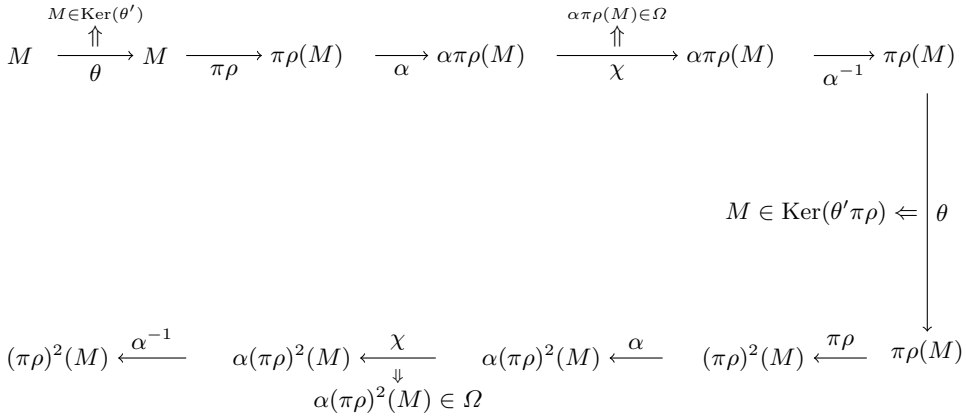


Fig. 5. Characterization a double kernel trail of Keccak

We now determine the elements $M \in \mathbb{F}_2^b$ such that $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M))$ is a double kernel path. We first define two sets for later discussions. For Sbox χ_5, define

$$Y = \{a : a \in \mathbb{F}_{2^5} | \#\{x : x \in \mathbb{F}_{2^5} | \chi_5(x + a) + \chi_5(x) = a\} > 0\}. \tag{10}$$

Furthermore, define the subset Ω of $\mathbb{F}_2^b$ by

$$\Omega = \{(\omega_1, \ldots, \omega_{320}) : \omega_i \in Y, 1 \leq i \leq 320\}. \tag{11}$$

Now we give the result.

Theorem 4. *Let M be an element in $\mathbb{F}_2^b$. It generates a double kernel path $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M))$ if and only if*

$$M \in \mathrm{Ker}(\theta') \cap \mathrm{Ker}(\theta'(\pi\rho)) \cap (\alpha\pi\rho)^{-1}(\Omega) \cap (\alpha(\pi\rho)^2)^{-1}(\Omega). \tag{12}$$

Proof. First assume that a double kernel path $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M))$ exists. Then from Figure 5 one can notice that M in the set in (12). Conversely, for each element M in (12), we need to show that $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M)$ is a double kernel path. This is easy by verifying the three conditions in Definition 3, we omit the details here. □

4.2 Condition for the existence of a double kernel path

In the next section, we propose a new algorithm based on Theorem 4 for finding double kernel paths, but we present the general idea behind the new algorithm in this section. By Theorem 4, a double kernel path $\mathcal{M}$ exists if and only if M satisfies (12). First, using the language of matrix multiplication, the condition $M \in \mathrm{Ker}(\theta') \cap \mathrm{Ker}(\theta'(\pi\rho))$ implies that $M_{\theta'(\pi\rho)^i} \cdot M = \mathbf{0}$, where $M_{\theta'(\pi\rho)^i}$ is the transformation matrix corresponding to the linear transformation $\theta'(\pi\rho)^i$ for $i = 0, 1$. Letting K_1 be the matrix defined by

$$K_1 = \left(M_{\theta'}, M_{\theta'(\pi\rho)}\right)^{\mathrm{T}}, \tag{13}$$

we have

$$K_1 \cdot M = \begin{pmatrix} M_{\theta'} \\ M_{\theta'(\pi\rho)} \end{pmatrix} \cdot M = \mathbf{0} \tag{14}$$

for all M satisfying (12).

Second, we need $M \in (\alpha\pi\rho)^{-1}(\Omega) \cap (\alpha(\pi\rho)^2)^{-1}(\Omega)$ for all solutions M of the equation (14). Finding such M is much more difficult as it can be regarded as a problem of decoding a nonlinear code by taking $\bigcap_{i=0}^{1}(\alpha(\pi\rho)^{i+1})^{-1}(\Omega)$ as a nonlinear code and M is a received codeword. We state this problem formally below.

Problem 1. Find an element M in $(\alpha\pi\rho)^{-1}(\Omega) \cap (\alpha(\pi\rho)^2)^{-1}(\Omega)$, where M is solution of the equation (14).

We solve this problem by splitting it into two relative easy subproblems. It is easy to see that an element $M \in \mathbb{F}_2^b$ satisfying (12) if and only if

$$M \in (\mathrm{Ker}(\theta') \cap \mathrm{Ker}(\theta'(\pi\rho))) \cap (\alpha(\pi\rho)^{i+1})^{-1}(\Omega) \quad \text{for } i \text{ with } 0 \le i \le 1. \tag{15}$$

Applying $\alpha(\pi\rho)^{i+1}$ on both sides of (15) we have

$$\alpha(\pi\rho)^{i+1}(M) \in \alpha(\pi\rho)^{i+1}\left(\mathrm{Ker}(\theta') \cap \mathrm{Ker}(\theta'(\pi\rho))\right) \cap \Omega. \tag{16}$$

Denoting $\alpha(\pi\rho)^{i+1}(M)$ by M_i for $0 \le i \le 1$. Again, using the language of matrix, the condition $M_i \in \alpha(\pi\rho)^{i+1}\left(\mathrm{Ker}(\theta') \cap \mathrm{Ker}(\theta'(\pi\rho))\right)$ is equivalent to

$$\left(K_1 M^{-1}_{\alpha(\pi\rho)^{i+1}}\right) \cdot M_i = \mathbf{0}, \tag{17}$$

where $M_{\alpha(\pi\rho)^{i+1}}$ is the matrix of $\alpha(\pi\rho)^{i+1}$ and K_1 is the matrix defined in (13). By (16), our target is find M_i's which are also in Ω. We state this problem below.

Problem 2. For $i = 0, 1$, find elements M_i in Ω, where M_i is a solution of the equation (17).

As one can see from the above arguments, Problem 1 and Problem 2 are closely related. Indeed, assume Problem 2 is solved, namely we found a set of M_i, say $\mathcal{M}_i$, such that (16) holds for $i = 0, 1$. Then, by recalling $M_i = \alpha(\pi\rho)^{i+1}(M)$, there is no difficulty to see that the element M satisfying (12) must satisfy

$$M \in \bigcap_{i=0}^{1} (\alpha(\pi\rho)^{i+1})^{-1}(\mathcal{M}_i)$$

where the linear function $\alpha(\pi\rho)^{i+1}$ applies on the set $\mathcal{M}_i$ means it applies on each element of the set. Therefore, we reduce solving Problem 1 into solving the Subproblems 2 for $i = 0, 1$. We summarize the above discussions into the following result.

Theorem 5. *Let the notation be the same as above. If there exists an element M which is a solution of equation (14) and it is also in the set $\bigcap_{i=0}^{1}(\alpha(\pi\rho)^{i+1})^{-1}(\mathcal{M}_i)$, then $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M))$ is a double kernel path of* Keccak.

Proof. The proof follows from the above discussions in this section. □

4.3 An algorithm for finding double kernel paths

We present an interesting observation of the function χ_5 in Keccak.

Fact 1 *Let Y be the set defined in (10). Then*

(i) there are 80 *affine subspaces of dimension* 2 *with elements in Y;*
(ii) there are 60 *affine subspaces of dimension* 2 *with elements in Y', where $Y' = Y \setminus \{0\}$.*

For the convenience of the reader, we list the 80 affine subspaces of dimension 2 with elements in Y in Appendix A. It is worthwhile to mention that Fact 1 is not true for any quadratic function (recall that χ_5 is quadratic). For example, one can verify that, for the function $F(x) = x^3 + x^9$ defined on $\mathbb{F}_{2^5}$, there are no affine subspaces of dimension greater than one with elements in the set $\{a : a \in \mathbb{F}_{2^5} | \#\{x : x \in \mathbb{F}_{2^5} | F(x + a) + F(x) = a\} > 0\}$.

In the following, we use the notation Y to denote the set defined in (10), and $\mathcal{Y}$ to denote the set of affine subspaces of dimension 2 with elements in Y. For later usage we define an ordering relation in Y to order the elements in Y and $\mathcal{Y}$.

Definition 4. *First, for each element $a \in Y$, define*

$$\delta(a) = \#\{x \in \mathbb{F}_{2^5} | \chi_5(x + a) + \chi_5(x) = a\}.$$

For two elements $a_1, a_2 \in Y$, we call $a_1 \preccurlyeq a_2$ if and only if $\delta(a_1) \leq \delta(a_2)$. Moreover, we may define the ordering relation in $\mathcal{Y}$ as follows. For two ordered affine subspaces $A = \{a_1, a_2, a_3, a_4\}$ and $B = \{b_1, b_2, b_3, b_4\} \in \mathcal{Y}$, we call $A \preccurlyeq B$ if and only if $\max_{i=1}^{4}\{\delta(a_i)\} \leq \max_{i=1}^{4}\{\delta(b_i)\}$.

The following result is useful to us.

Proposition 3. *Let A be an affine subspace of dimension m of $\mathbb{F}_2^n$, i.e. $A = a + S$, where $a \in \mathbb{F}_{2^n}$ and S is a subspace of $\mathbb{F}_2^n$ where the dimension of S is m. Then there exists an $(n - m) \times n$ matrix M_A and a constant $c_A \in \mathbb{F}_2^n$ such that $M_A \cdot a = c_A$ if and only if $a \in A$.*

In the following, for each affine subspace $A \in \mathcal{Y}$, we denote the matrix and the constant corresponding to A as those in Proposition 3 by M_A and c_A. Now we are ready to describe the algorithm to solve Problem 2 for $i = 0, 1$. Our target is to find an element M_i in Ω, where M_i is a solution of the equation $\left(K_1 M^{-1}_{\alpha(\pi\rho)^{i+1}}\right) \cdot M_i = \mathbf{0}$. Without loss of generality, we use the case $i = 0$ to explain the the roadmap of the algorithm.

Step 1. Initialize the matrix $E = K_1 M^{-1}_{\alpha(\pi\rho)}$ and the column vector $b = \mathbf{0}$ with length of $\#row(E)$;

Step 2. Iterate over the 320 Sboxes:
- For each Sbox, choosing affine subspace A from $\mathcal{Y}$ according to the ordering in $\mathcal{Y}$.
- Computing the matrix M_A and constant column vector c_A by Proposition 3. Letting $E' = (E, M_A)^{\mathrm{T}}$ and $b' = (b, c_A)^{\mathrm{T}}$.
- If the equation $E'x = b'$ is consistent, update $E = E'$ and $b = b'$; else choosing the next affine subspace.
- If all affine subspaces are exhausted, but no E' found such that $E'x = b'$ is consistent, then output FAIL.

Step 3. Output a special solution of the equation $Ex = b$, and the basis of the kernel space of E.

Several remarks on the above algorithm are in the sequel:

(i) Note that we do not specify which Sboxes are non-active in the above algorithm. Actually, the number of non-active Sboxes is determined by the rank of $K_1 M^{-1}_{\alpha(\pi\rho)}$. Because, for each non-active Sbox, we need to add 5 rows in the matrix E (as the matrix and the column vector in Proposition 3 corresponding to the subspace $\{0\}$ is the identity matrix and the zero vector, and for different Sboxes, these 5 rows are linear independent after adding into E). Therefore, one can specify at most $\lfloor (1600 - \mathrm{Rank}(K_1 M_{\alpha(\pi\rho)}))/5 \rfloor$ non-active Sboxes. Otherwise, there is only zero solution of the equation $Ex = b$.

(ii) If one prefers certain Sbox must be active, namely the value of this Sbox must be nonzero, we choose affine subspaces for this Sbox from the set $\mathcal{Y}' = \mathcal{Y} \setminus \{A : A \in \mathcal{Y} \mid 0 \in A\}$. Similar to the above comment, the number of active Sboxes is at most $\lfloor (1600 - \mathrm{Rank}(K_1 M_{\alpha(\pi\rho)}))/3 \rfloor$. The reason for the denominator is 3 is that for any affine subspace of dimension 2, the matrix in Proposition 3 corresponding to it has 3 rows and they are linearly independent for different Sbox after adding to E. In the following, we call an Sbox *must active* if it is specified to be active before the algorithm executes, otherwise it is called *not necessary active* Sbox. However, we should mention that for the not necessary active Sboxes, after running the above algorithm, the value in this Sbox may be nonzero. This is clear from the fact that, during the execution of the algorithm, its priority is to keep for the consistency of the equations.

(iii) Similar to the case of the target difference algorithm in [10], there is no guarantee that the above algorithm will always be succeeded, it totally relies on experiment.

(iv) When the algorithm succeeds for each $i = 0, 1$, the solution space of $E_i x = b_i$ is clearly an affine subspace, which is denoted by $\mathcal{M}_i$. Finally if the intersection $\bigcap_{i=0}^{1} \alpha(\pi\rho)^{i+1})^{-1}(\mathcal{M}_i)$ is nonempty then the elements in the intersection can generate double kernel paths.

Let us give an example of applying the above algorithm to find double kernel path $\mathcal{M} = (M, \pi\rho(M), (\pi\rho)^2(M))$ of Keccak below.

Example 2. We randomly fix 2 must active Sboxes, and use the above algorithm to search for two sets $\mathcal{M}_1$ and $\mathcal{M}_2$ defined above. The intersection $\bigcap_{i=0}^{1}(\alpha(\pi\rho)^{i+1})^{-1}(\mathcal{M}_i)$ is the following 1600-bit message:

0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000008000000000000000000000000000000000000000
0000000080000000000000000000000000000000000000004000000000000000
0000000000000080000000000000000000000080000000000000000400000000
0000000000000000000000000000000000,

where each digit is a hexadecimal number. Here $\mathcal{M}_1, \mathcal{M}_2$ are the solution spaces of the equation $E_1 x = b_1$ and $E_2 x = b_2$. We list the special solutions of the equations $E_i x = b_i$ and the basis of the solutions space of $E_i x = 0$ for $i = 1, 2$ in Appendix B. One can also check that the probability for the 2-round kernel differential path generated by M is 2^{-24}.

Finally we state the algorithms for searching the double kernel paths of Keccak.

Algorithm 2 Finding Intersection $\mathrm{Ker}(K_1 M^{-1}_{\alpha(\pi\rho)^{i+1}}) \cap \Omega$

procedure KD(i)
  $E \leftarrow K_1 M^{-1}_{\alpha(\pi\rho)^{i+1}}$ and $b \leftarrow \mathbf{0}$
  for each must active Sbox S **do**
    (a) Choosing an affine subspace A from $\mathcal{Y}'$ according to the ordering
    (b) Constructing matrix M_A and c_A as in Proposition 3
    (c) $E' \leftarrow \binom{E}{M_A}$ and $b' \leftarrow \binom{b}{c_A}$
    if E' is consistent with respect to b' **then**
      $E \leftarrow E'$ and $b \leftarrow b'$
    else if there are still unused affine subspaces in $\mathcal{Y}'$ **then**
      Continue to the next affine subspace in $\mathcal{Y}'$ and execute (a)
    else
      return FAIL.
    end if
  end for
  for each $(320 - t)$ not necessary active Sbox **do**
    (a) Choosing an affine subspace A from $\mathcal{Y}$ according to the ordering
    (b) Constructing matrix M_A and c_A as in Proposition 3
    (c) $E' \leftarrow \binom{E}{M_A}$ and $b' \leftarrow \binom{b}{c_A}$
    if E' is consistent with respect to b' **then**
      $E \leftarrow E'$ and $b \leftarrow b'$
    else if there are still unused affine subspaces in $\mathcal{Y}$ **then**
      Continue to the next affine subspace and execute (a)
    else
      return FAIL.
    end if
  end for
  return E and b
end procedure

5 Almost double kernel path

One can see from the definition of double kernel path that the restrictions on the input difference M and $\pi\rho(M)$ are very high. Under some circumstances it restricts us to find the best differential path. In this section, we propose a variant of double kernel path, called *almost double kernel path* in Definition 5. Interestingly, in searching of such differential paths, we discover many 2-round differential path with complexity better than all known examples. Furthermore, by using such differential paths, we also found the 3-round differential paths with the best complexity known so far.

Definition 5. *Let $\mathcal{M} = (M_1, M_2, M_3)$ be a 3-tuple with elements in $\mathbb{F}_2^b$. It is called an almost double kernel path of Keccak if the following hold:*

(i) $\theta(M_i) = M_i$ *for* $1 \le i \le 2$;
(ii) $M_2 = \pi\rho(M_1), M_3 \in \{a \in \mathbb{F}_2^b | \#\{x \in \mathbb{F}_2^b : \chi(x + \alpha(M_2)) + \chi(x) = a\} \neq 0\}$;
(iii) $\Pr_{\mathrm{x} \in \mathbb{F}_2^{\mathrm{b}}} (\chi(\mathrm{x} + \alpha\pi\rho(\mathrm{M}_1)) + \chi(\mathrm{x}) = \alpha\pi\rho(\mathrm{M}_1)) > 0$.

Algorithm 3 Finding Double Kernel Path

```
1: procedure KDP
2:     i ← 0
3:     for 0 ≤ i ≤ 1 do
4:         if KD(i) eq FAIL then
5:             return FAIL
6:         else
7:             E_i, b_i ← KD(i)
8:             M_i ← Solutions of the equation E_i x = b_i
9:             M'_i ← (α(πρ)^{i+1})^{-1}(M_i)
10:        end if
11:    end for
12:    M ← ⋂_{i=0}^{1} M'_i
13:    if #M > 0 then
14:        return SUCCESS, M
15:    else
16:        return FAIL, {}
17:    end if
18: end procedure
```

The only difference between a double kernel path and an almost double kernel path is that, in the 2-nd round, the output difference may not be equal to the input difference $\alpha(\pi\rho)^2(M)$. As explained above, the reason for defining an almost double kernel path is that, by loosing the restriction, in some cases we may find better differential paths. The following figure illustrates an almost double kernel differential path. The arrow $\dashrightarrow$ in the figure shows its difference with the double kernel differential path in Figure 5.

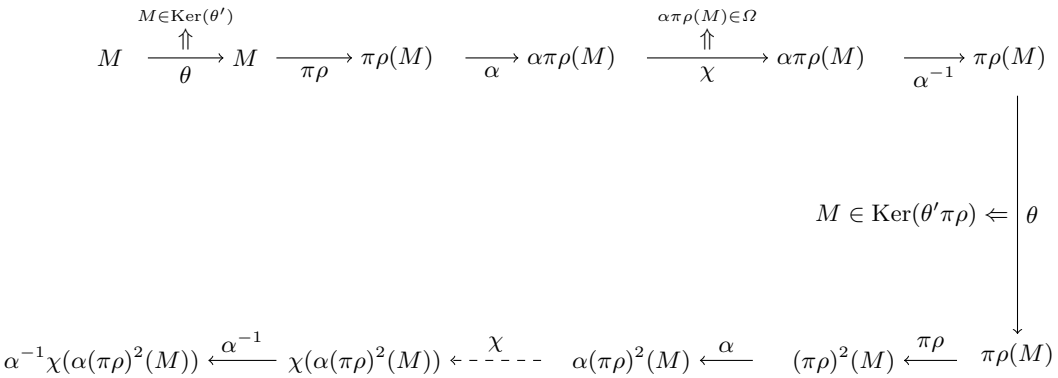


Fig. 6. An almost double kernel trail

It is easy to characterize the almost double kernel path as the one in Theorem 4. We state it below.

Theorem 6. *Let M be an element in $\mathbb{F}_2^b$. It generates an almost double kernel path $\mathcal{M} = (M, \pi\rho(M), M_3)$ if and only if*

$$M \in \mathrm{Ker}(\theta') \cap \mathrm{Ker}(\theta'\pi\rho)^i) \cap (\alpha(\pi\rho))^{-1}(\Omega).$$

The algorithm to solve Problem 2 can also be used to search for almost double kernel paths without difficulty. We state the algorithm for searching for almost double kernel paths below. In the algorithm, we give an input ACCEPTABLE as a lower bound of the complexity of the 2-round differential path one expects.

Algorithm 4 Finding Almost Double Kernel Differential Path

procedure KDP(ACCEPTABLE)
  if KD(0) eq FAIL **then**
    return FAIL
  else
    $E_0, b_0 \leftarrow$ KD(0)
    $\mathcal{M}_0 \leftarrow$ Solutions of the equation $E_0 x = b_0$
    $\mathcal{M}' \leftarrow (\alpha(\pi\rho))^{-1}(\mathcal{M}_0)$
    for $M \in \mathcal{M}'$ **do**
      $M_1 \leftarrow M$
      $M_2 \leftarrow \pi\rho(M_1)$
      for $M_3 \in \{a \in \mathbb{F}_2^b \mid \#\{x \in \mathbb{F}_2^b : \chi(x + \alpha(M_2)) + \chi(x) = a\} \neq 0\}$ **do**
        Compute the complexity c of the path (M_1, M_2, M_3)
        if $c \geq$ ACCEPTABLE **then**
          return (M_1, M_2, M_3)
        end if
      end for
    end for
  end if
  return FAIL
end procedure

6 Application of 2- and 3-round differential characteristics to find (near)-collisions of Keccak

Applying Algorithms 3 and 4, we found many double kernel paths and almost double kernel paths. Thanks to Theorem 3, we performed a search for all CPK elements with Hamming weights 2, 4, and 6 as input differences. For the double kernel paths, the best complexity is 2^{-24}, which is the same as the ones found in [10,11]. However, for the almost double kernel paths, our newly obtained differential paths have the best complexity 2^{-23}. Furthermore, using almost double kernel paths as the first 2-round, we succeed in obtaining 3-round differential paths with the best complexity 2^{-126}.

If one applies the rebound attack techniques as presented in [11] on the newly obtained 2-round differential characteristics, then one can get 3-round differential characteristics with complexity 2^{-35}, which is the same as the complexity value for 3-round differential paths presented in [3]. However, when the rebound attack techniques are applied on our 3-round differential characteristics, we can obtain 4-round differential characteristics with probability 2^{-138}, which is the best value known so far.

Furthermore, the new differential characteristics can also be used to find (near-)collisions of 4-round and 5-round Keccak with better complexity using the target difference algorithm proposed in [10]. In the target difference algorithm, a target difference is obtained by going backward one round from the input difference of a r-round differential characteristic and then, an input difference and a set of message pairs for the target difference are found to produce (near-)collisions. Thus, using the target difference algorithm one can produce $(r + 2)$-round (near)-collisions using a r-round differential characteristic. By applying the target difference algorithm on our 2-round and 3-round differential characteristics with the best complexity, one can produce 4-round collisions and 5-round near-collisions with a better complexity, respectively for all versions of Keccak. We note that the complexity for producing a (near-)collision also depends on the number of active Sboxes in the first n bits in the last round. As mentioned earlier, many 3-round differential paths were found, but we choose those differential characteristics that have the minimum number of active Sboxes in the first n bits in the last round for Keccak, which are presented in Appendix C. A comparison of the probability value of our differential characteristics and the characteristics of [10] for producing 4-round collisions and 5-round near-

collisions is presented in Table 1. We do not present the results of (near-)collisions for the differential paths since it is out of scope of this paper.

7 Concluding remarks and future work

In this paper, we investigated the properties of the component functions of Keccak's round function. Especially, we studied the linear transformations using their transformation matrices, which enables us to apply tools from linear algebra easily. By studying the transformation matrix of θ, we proved that the dimension of the CPK is $(20w + 1)$, but not the value $20w$ presented in the submission of Keccak. Moreover, we were able to explicitly express and enumerate the exact number of the CPK elements with a given Hamming weight t. Considering the CPK as a linear code with $M_{\theta'}$ as a parity check matrix, our work indeed determined the weight distribution of this code. Furthermore, we studied the double kernel path of Keccak for the differential cryptanalysis by providing a characterization of the existence of double kernel paths. This surely helps us to better understand the design of Keccak and is useful for the future research. Relying on the characterization, we proposed a new algorithm for obtaining all double kernel paths. The difference between our technique and the method in [18] is that using our algorithm one can obtain all double kernel paths. Finally, we proposed the concept of almost double kernel path and presented an algorithm for finding almost double kernel paths. Using our new algorithm, we experimentally found almost double kernel paths with better complexity than all known 2-round differential paths. More interestingly, using almost double kernel paths as the first 2-round, we discovered 3-round differential paths with the best complexity known so far. Our newly obtained differential paths can be used to produce 4-round collisions and 5-round near-collisions using the target difference algorithm.

As a future research problem, it would be interesting to investigate whether it is possible to further apply the proven properties of the CPK elements to find r-round differential paths $(r \geq 5)$ of Keccak with better complexity.

References

1. Aumasson, J.-P., Meier, W.: Zero-sum distinguishers for deduced Keccak-f and for the core functions of Luffa and Hamsi. Presented at the rump session of CHES 2009, 2009.
2. Bernstein, D.J.: Second preimages for 6 (7? (8??)) rounds of Keccak?. `http://ehash.iaik.tugraz.at/uploads/6/65/NIST-mailing-list_Bernstein-Daemen.txt` (2010)
3. Bertoni, G., Daemen, J., and Peeters, M., Assche, G.V.: The Keccak reference. `http://keccak.noekeon.org/Keccak-reference-3.0.pdf` (2011)
4. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: The Keccak SHA-3 submission. Submission to NIST (Round 3) (2011)
5. Bosma, W., Cannon, J. J., Fieker, C., Steel, A. (eds.): Handbook of magma functions. Edition 2.16 (2010)
6. Boura C., Canteaut, A.: On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$. IEEE Trans. on Information Theory, 59(1), 691-702 (2013)
7. Boura C., Canteaut, A., De Cannière, C.: Higher-order differential properties of Keccak and Luffa. In: Joux, A. (ed.) FSE 2011, LNCS, vol. 6733, pp. 252-269, Springer, Heidelberg (2011)
8. Boura, C., Canteaut, A.: Zero-sum distinguishers for iterated permutations and application to Keccak-f and Hamsi-256. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2011, LNCS, vol. 6544, pp. 1-17, Springer, Heidelberg (2011)
9. Chen, L., Gong, G.: Communication system security. Boca Raton, Florida, USA, Chapman & Hall/CRC (2012)
10. Dinur, I., Dunkelman, O., Shamir, A.: New attacks on Keccak-224 and Keccak-256. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 442-461, Springer, Heidelberg (2012)
11. Duc, A., Guo, J., and Peyrin, T., Wei, L.: Unaligned rebound attack: application to Keccak. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 402-421, Springer, Heidelberg (2012)
12. Khovratovich, D., Biryukov, A., Nikolic, I.: Speeding up collision search for byte-oriented hash functions. In: Fischlin, M. (ed.) CT-RSA 2009, LNCS, vol. 5473, pp. 164-181, Springer, Heidelberg (2009)
13. Khovratovich, D.: Cryptanalysis of hash functions with structures. In: Jacobson, M.J., Jr., Rijmen, V., and Safavi-Naini, R. (eds.) SAC 2009, LNCS, vol. 5867, pp. 108-125, Springer, Heidelberg (2009)
14. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1995, LNCS, vol. 1008, pp. 196-211, Springer, Heidelberg (1995)

15. Lai, X., Duan, M.: Improved zero-sum distinguisher for full round Keccak-f permutation. Cryptology ePrint Archive, Report 2011/023 (2011), http://eprint.iacr.org/2011/023
16. MacWilliams, F. J., Sloane, N. J. A.: The theory of error-correcting codes, II. Amsterdam-New York-Oxford (1977)
17. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. CRC Press (1997)
18. Naya-Plasencia, M., Röck, A., Meier, W.: Practical analysis of reduced-round Keccak. In: Bernstein, D.J., Chatterjee, S. (eds.) INDOCRYPT 2011. LNCS, vol. 7107, pp. 236-254, Springer, Heidelberg (2011)
19. Stinson, D.R.: Cryptography - theory and practice. CRC Press (1995)
20. Wang, X., Yu, H., Yin, Y.-L.: Efficient collision search attacks on SHA-0. In: Shoup, V. (ed.) CRYPTO 2005, LNCS, vol. 3621, pp. 1-16, Springer, Heidelberg (2005)
21. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005, LNCS, vol. 3621, pp. 17-36, Springer, Heidelberg (2005)
22. Yu, H., Wang, X.: Near-collision attack on the compression function of dynamic SHA2. Cryptology ePrint Archive, Report 2009/179 (2009), http://eprint.iacr.org/2009/179
23. NIST, the SHA-3 competition (2007-2012). http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
24. Tan, Y., : Computational results on Keccak. In www.ytan.me.

Appendix

A Affine subspaces of dimension 2 with elements in Y

In this section, we present all the affine subspaces of dimension 2 with elements in the set Y defined in Fact 1. There are total 80 elements in Y which are provided in Table 4. The subspaces in the following table are ordered by the ordering defined in Definition 4, and the elements in each affine subspaces are also ordered. In Table 4, the 5-tuple elements are represented in the hexadecimal form. For instance, the affine subspace $\{(0,0,0,0,0),(0,0,0,0,1),(0,0,1,0,0),(0,0,0,1,1)\}$ is represented by $[00,01,02,03]$.

Table 4. All affine subspaces in $\mathcal{Y}$

[00, 01, 02, 03]	[00, 01, 10, 11]	[00, 01, 06, 07]	[00, 01, 18, 19]
[00, 02, 04, 06]	[00, 02, 0C, 0E]	[00, 02, 11, 13]	[00, 04, 08, 0C]
[00, 04, 03, 07]	[00, 04, 18, 1C]	[00, 08, 10, 18]	[00, 08, 06, 0E]
[00, 08, 11, 19]	[00, 10, 03, 13]	[00, 10, 0C, 1C]	[00, 03, 1F, 1C]
[00, 06, 19, 1F]	[00, 0C, 13, 1F]	[00, 18, 1F, 07]	[00, 11, 1F, 0E]
[01, 02, 04, 07]	[01, 02, 10, 13]	[01, 02, 1F, 1C]	[01, 04, 03, 06]
[01, 04, 19, 1C]	[01, 08, 10, 19]	[01, 08, 18, 11]	[01, 08, 07, 0E]
[01, 10, 1F, 0E]	[01, 03, 0C, 0E]	[01, 03, 11, 13]	[01, 06, 18, 1F]
[01, 0C, 11, 1C]	[01, 13, 0E, 1C]	[01, 19, 1F, 07]	[02, 04, 08, 0E]
[02, 04, 19, 1F]	[02, 08, 06, 0C]	[02, 08, 13, 19]	[02, 10, 03, 11]
[02, 10, 0E, 1C]	[02, 03, 06, 07]	[02, 03, 18, 19]	[02, 06, 18, 1C]
[02, 0C, 11, 1F]	[02, 13, 1F, 0E]	[02, 19, 07, 1C]	[04, 08, 10, 1C]
[04, 08, 13, 1F]	[04, 10, 0C, 18]	[04, 10, 13, 07]	[04, 03, 18, 1F]
[04, 06, 0C, 0E]	[04, 06, 11, 13]	[04, 0C, 11, 19]	[04, 13, 19, 0E]
[04, 1F, 07, 1C]	[08, 10, 1F, 07]	[08, 03, 0C, 07]	[08, 03, 18, 13]
[08, 06, 11, 1F]	[08, 0C, 18, 1C]	[08, 13, 07, 1C]	[08, 19, 1F, 0E]
[10, 03, 0C, 1F]	[10, 06, 18, 0E]	[10, 06, 11, 07]	[10, 18, 11, 19]
[10, 13, 1F, 1C]	[10, 19, 07, 0E]	[03, 06, 19, 1C]	[03, 0C, 13, 1C]
[03, 18, 07, 1C]	[03, 11, 0E, 1C]	[06, 0C, 13, 19]	[06, 18, 19, 07]
[06, 11, 19, 0E]	[0C, 18, 13, 07]	[0C, 11, 13, 0E]	[18, 11, 07, 0E]

B $\mathcal{M}_1$ and $\mathcal{M}_2$ of Example 2

In this section, we provide the solution space $\mathcal{M}_i$ of $E_i x = b_i$ for $i = 0, 1$ in Example 2. One may check by a computer that $M \in (\alpha\pi\rho)^{-1}(\mathcal{M}_1) \cap (\alpha(\pi\rho)^2)^{-1}(\mathcal{M}_2)$, where M is the element in Example 2. We give these solution spaces by providing a special solution and the basis of

$\mathrm{Ker}(E_i), i = 1, 2$. We denote by S_{E_i} the special solution for the system of affine equations $E_i \cdot S_{E_i} = b_i$. For the first system of affine equations, the dimension of the solution space is 185, and for the second system of linear equations the dimension of the solution space is 3. The basis elements of the first and second solution space are provided in Table 5 and Table 6, respectively. Note that each basis element is a binary 1600-tuple. The computations were performed by MAGMA [5]. In Tables 5 and 6, we represent a 1600-tuple by giving the support set (in hexadecimal). We first give two special solutions of the equation $E_iX = b_i$ for $i = 1, 2$:

(i)

$S_{E_1} =$
$1880218C2310C6110C630886318C0318C0318C630886310043108221884110C630886$
$21846318C2310C6110C63088631844308C6218C6110C630886318C0318FFC18C6300$
$C43184631844318C200886110863088621844210C0100C63180631844118C2008C6100$
$46308023184021840010C2000861000430800218400000C600046200061100030880001844$
$000C220004010002008001004000802000401000020806100400080200040100020080010$
$0400000000000000000000000000000000000000000100001$

(ii)

$S_{E_2} =$
0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000008000000
0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000080001000000000000000000000040000000
0000000000400000000000000000000000000000000000000000000000000000000800000
00000000000000000000000000000000000.

Next two tables contain the basis elements of $\mathrm{Ker}(E_1)$ and $\mathrm{Ker}(E_2)$.

Table 5: Basis elements of $\mathrm{Ker}(E_1)$

Row No.	Support set of the row
1	3 17 379 37e 38d 392 3d7 3dc 3f1 3f6 40a 40f 469 46e 553 558 5bc 5c1 5d5 5da 5e0 5f4 639 63e
2	4 18 2c4 2c9 356 365 3f1 3f6 43b 440 4cd 4e1 5b7 5bc 62a 63e
3	8 17 220 225 373 378 405 40f 4e5 4ef 57c 590
4	9 18 1d4 1d9 2c4 2c9 356 365 374 379 3f1 3f6 43b 440 4cd 4e1 53a 53f 5bc 5c1 5c7 5d1 62a 63e
5	d 17 9a ae 35a 35f 38d 392 3d7 3dc 3ec 3f6 40a 40f 469 46e 4d1 4d6 553 558 563 577 5d5 5da 5e0 5f4 639 63e
6	e 18 24c 256 2c4 2c9 2d9 2e8 356 365 3f1 3f6 43b 440 4cd 4e1 5ad 5bc 62a 63e
7	12 17 342 34c 374 379 38c 38d 391 392 3a6 3ab 3be 3c3 3d7 3dc 3f0 3f1 3f5 3f6 40a 40f 41e 423 450 455 469 46e 482 487 508 50d 53a 53f 553 558 56c 571 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5ee 5f3 5f4 5f9 60d 611 620 639 63e
8	13 18 2c4 2c9 2d8 2e2 356 365 36f 379 3f1 3f6 43b 440 4cd 4e1 5bc 5c1 62a 63e
9	1c 30 342 34c 374 379 38c 38d 391 397 3be 3c3 3d7 3dc 3f1 3f6 41e 428 450 455 469 46e 508 50d 53a 53f 553 558 595 5a9 5bc 5c1 5c7 5db 5e0 5f4 611 620 639 63e
10	1d 31 2dd 2e2 36f 379 38d 392 3d7 3dc 3f1 3f6 454 459 469 46e 4e6 4fa 553 558 5bc 5c1 5d0 5da 5e0 5f4 639 63e
11	21 30 239 23e 38c 391 41e 428 4fe 508 595 5a9
12	22 31 1ed 1f2 2dd 2e2 36f 379 3d7 3dc 3f1 3f6 454 459 469 46e 4e6 4fa 5bc 5c1 5ea 5f4 639 63e
13	26 30 b3 c7 342 34c 373 374 378 379 38c 38d 391 392 3be 3c3 3d7 3dc 3f1 3f6 405 40a 41e 428 450 455 469 46e 4ea 4ef 508 50d 53a 53f 553 558 57c 590 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5f4 611 620 639 63e
14	27 31 265 26f 2dd 2e2 2f2 301 36f 379 38d 392 3d7 3dc 3f1 3f6 454 459 469 46e 4e6 4fa 553 558 5bc 5c1 5c6 5da 5e0 5f4 639 63e
15	2b 30 342 34c 35b 365 374 379 38c 391 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 409 40e 41e 428 437 43c 450 455 49b 4a0 508 50d 521 526 53a 53f 585 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 612 620 626 62a 63e
16	2c 31 2dd 2e2 2f1 2fb 36f 379 388 38d 3d7 3dc 3f1 3f6 454 459 469 46e 4e6 4fa 553 558 5bc 5c1 5e0 5f4 639 63e

17	35 49 342 34c 35b 365 374 379 38c 391 3a5 3aa 3ab 3b0 3be 3c3 3f1 3f6 41e 423 437 441 450 455 508 50d 521 526 53a 53f 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 611 620 62a 63e
18	36 4a 2ac 2b6 342 34c 35b 365 374 379 38c 391 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 41e 423 437 43c 450 455 46d 477 508 50d 521 526 53a 53f 57b 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5e9 5ee 607 60c 611 620 62a 63e
19	39 3a 3e 3f cc e0 252 257 27e 288 28e 29d 2ac 2b6 2ca 2cf 2f6 2fb 30b 31a 342 34c 374 379 388 38c 38d 391 3a5 3aa 3be 3bf 3c3 3c4 3d7 3d8 3dc 3dd 3f0 3f1 3f6 3ff 41e 423 437 43c 450 455 469 46e 472 477 4ff 502 503 508 50d 511 512 513 517 521 53a 53f 553 558 562 56c 57b 58a 594 595 5a3 5a9 5ae 5bc 5c1 5c2 5c7 5db 5df 5e0 5ee 5f4 5f9 607 60c 60d 620 625 639 63e
20	44 49 35b 365 374 379 3a5 3aa 3be 3c3 3d8 3dd 3f1 3f6 422 427 437 441 450 455 4b4 4b9 521 526 53a 53f 59e 5a3 5ae 5bc 5c1 5c2 5c7 5db 620 625 62a 62b 63e 63f
21	45 4a 2ac 2b6 30a 314 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3bf 3c3 3c4 3f1 3f6 41e 423 437 43c 450 455 46d 477 508 50d 521 526 53a 53f 57b 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 620 62a 63e
22	4e 62 35b 365 374 379 3a5 3aa 3be 3c3 3c4 3c9 3f1 3f6 437 43c 450 45a 521 526 53a 53f 5ae 5bc 5c1 5c2 5c7 5db 607 60c 62a 63e
23	4f 63 30f 314 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3c3 3f1 3f6 41e 423 437 43c 450 455 486 48b 508 50d 518 521 526 52c 53a 53f 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 602 607 611 620 62a 63e
24	53 62 26b 270 3be 3c3 450 45a 530 53a 5c7 5db
25	54 63 21f 224 30f 314 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3bf 3c3 3c4 3f1 3f6 41e 423 437 43c 450 455 486 48b 508 50d 518 521 526 52c 53a 53f 585 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 612 61c 620 62a 63e
26	58 62 e5 f9 35b 365 374 379 3be 3c3 3f1 3f6 450 45a 51c 526 53a 53f 5bc 5c1 5c7 5db 62a 63e
27	59 63 297 2a1 30f 314 324 333 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3c3 3f1 3f6 41e 423 437 43c 450 455 486 48b 508 50d 518 521 526 52c 53a 53f 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 5f8 607 611 620 62a 63e
28	5d 62 2c4 2c9 356 365 374 379 3be 3c3 3f1 3f6 450 45a 4d2 4e1 53a 53f 5bc 5c1 5c7 5db 62a 63e
29	5e 63 30f 314 323 32d 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3ba 3be 3c3 3c4 3f1 3f6 41e 423 437 43c 450 455 486 48b 508 50d 518 521 526 52c 53a 53f 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 620 62a 63e
30	67 7b 374 379 3be 3c3 3dd 3e2 3f1 3f6 450 455 46e 473 53a 53f 5bc 5c1 5c7 5db 620 625 639 63e
31	68 7c 328 32d 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3f1 3f6 437 43c 450 455 49f 4a4 521 526 531 53a 53f 545 5ae 5bc 5c1 5c2 5c7 5db 607 60c 61b 620 62a 63e
32	6c 7b 284 289 3d7 3dc 469 473 549 553 5e0 5f4
33	6d 7c 238 23d 328 32d 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3d8 3dd 3f1 3f6 437 43c 450 455 49f 4a4 521 526 531 53a 53f 545 59e 5a3 5ae 5bc 5c1 5c2 5c7 5db 607 60c 620 625 62a 62b 635 63e
34	71 7b fe 112 374 379 3f1 3f6 46e 473 535 53f 5bc 5c1 639 63e
35	72 7c 2b0 2ba 328 32d 33d 34c 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3f1 3f6 437 43c 450 455 49f 4a4 521 526 531 53a 53f 545 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 620 62a 63e
36	76 7b 2dd 2e2 36f 379 3f1 3f6 46e 473 4eb 4fa 5bc 5c1 639 63e
37	77 7c 328 32d 33c 346 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3d3 3dd 3f1 3f6 437 43c 450 455 49f 4a4 521 526 531 53a 53f 545 5ae 5bc 5c1 5c2 5c7 5db 607 60c 620 625 62a 63e
38	80 94 342 34c 374 379 38c 391 3a6 3ab 3be 3c3 3f0 3f1 3f5 3fb 41e 423 450 455 482 48c 508 50d 53a 53f 56c 571 595 5a9 5bc 5c1 5c7 5db 5ee 5f3 5f9 60d 611 620
39	81 95 341 346 374 379 3be 3c3 3d3 3dd 3f1 3f6 450 455 4b8 4bd 53a 53f 54a 55e 5bc 5c1 5c7 5db 620 625 634 63e
40	85 94 29d 2a2 3f0 3f5 482 48c 562 56c 5f9 60d
41	86 95 24c 251 2d9 2e8 341 346 374 379 3be 3c3 3d3 3dd 450 455 4b8 4bd 53a 53f 54a 55e 5ad 5c1 5c7 5db 620 625
42	8a 94 117 12b 342 34c 374 379 38c 391 3a6 3ab 3be 3c3 3d7 3dc 3f0 3f1 3f5 3f6 41e 423 450 455 469 46e 482 48c 508 50d 53a 53f 54e 553 56c 571 595 5a9 5bc 5c1 5c7 5db 5e0 5ee 5f3 5f4 5f9 60d 611 620 639 63e
43	8b 95 2c9 2d3 341 346 356 365 374 379 3be 3c3 3d3 3dd 3f1 3f6 450 455 4b8 4bd 53a 53f 54a 55e 5bc 5c1 5c7 5db 620 625 62a 63e
44	90 95 341 346 355 35f 374 379 3be 3c3 3d3 3dd 3ec 3f1 450 455 4b8 4bd 53a 53f 54a 55e 5bc 5c1 5c7 5db 620 625
45	99 ad 35b 365 38d 392 3a5 3aa 3bf 3c4 3d7 3dc 409 40a 40e 414 437 43c 469 46e 49b 4a5 521 526 553 558 585 58a 5ae 5c2 5d5 5da 5e0 5f4 607 60c 612 626 62a 639
46	9e ad 2b6 2bb 409 40e 49b 4a5 57b 585 612 626
47	9f ae 265 26a 2f2 301 35a 35f 38d 392 3d7 3dc 3ec 3f6 469 46e 4d1 4d6 553 558 563 577 5c6 5da 5e0 5f4 639 63e
48	a3 ad 130 144 342 34c 35b 365 374 379 38c 391 3a5 3a6 3aa 3ab 3be 3bf 3c3 3c4 3f1 3f6 409 40e 41e 423 437 43c 450 455 49b 4a5 508 50d 521 526 53a 53f 567 571 585 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 612 620 626 62a 63e
49	a4 ae 2e2 2ec 35a 35f 36f 379 3ec 3f1 4d1 4d6 563 577 5bc 5c1
50	a8 ad 30f 314 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3bf 3c3 3c4 3f1 3f6 409 40e 41e 423 437 43c 450 455 49b 4a5 508 50d 51d 521 526 52c 53a 53f 585 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 612 620 626 62a 63e
51	a9 ae 35a 35f 36e 378 38d 392 3d7 3dc 3ec 3f6 405 40a 469 46e 4d1 4d6 553 558 563 577 5d5 5da 5e0 5f4 639 63e
52	b2 c6 342 34c 38c 391 3d8 3dd 41e 422 427 42d 4b4 4be 508 50d 595 59e 5a3 5a9 611 625 62b 63f
53	b7 c6 2cf 2d4 422 427 4b4 4be 594 59e 62b 63f
54	b8 c7 27e 283 30b 31a 342 34c 373 374 378 379 38c 38d 391 392 3be 3c3 3d7 3dc 3f1 3f6 405 40a

	41e 423 450 455 469 46e 4ea 4ef 508 50d 53a 53f 553 558 57c 590 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5df 5e0 5ee 5f4 611 620 639 63e
55	bc c6 149 15d 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3d8 3dd 3f1 3f6 422 427 437 43c 450 455 4b4 4be 521 526 53a 53f 580 58a 59e 5a3 5ae 5bc 5c1 5c2 5c7 5db 607 60c 620 625 62a 62b 63e 63f
56	bd c7 2fb 305 373 378 388 392 405 40a 4ea 4ef 57c 590 5d5 5da
57	c1 c6 328 32d 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3d8 3dd 3f1 3f6 422 427 437 43c 450 455 4b4 4be 521 526 536 53a 53f 545 59e 5a3 5ae 5bc 5c1 5c2 5c7 5db 607 60c 620 625 62a 62b 63e 63f
58	c2 c7 342 34c 373 374 378 379 387 38c 38d 392 3be 3c3 3d7 3dc 3f1 3f6 405 40a 450 455 469 46e 4ea 4ef 508 50d 53a 53f 553 558 57c 590 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5f4 611 620 639 63e
59	cb df 2c4 2c9 356 35b 3a5 3aa 437 446 4d7 4e1 521 526 5ae 5c2
60	d0 df 2c4 2c9 2e8 2ed 356 365 3f1 3f6 4d7 4e1 5ad 5bc 62a 63e
61	d1 e0 27e 288 28e 297 29c 29d 2ac 2b6 2ca 2cf 2f6 2fb 30b 31a 324 333 374 379 388 38d 3a6 3ab 3be 3bf 3c3 3c4 3d7 3d8 3dc 3dd 3f1 3f6 450 455 469 46e 472 477 4ff 502 503 511 512 513 53a 53f 553 558 562 571 57b 58a 594 5a3 5bc 5c1 5c7 5db 5df 5e0 5f3 5f4 5f8 60c 620 625 639 63e
62	d5 df 162 176 2c4 2c9 356 365 374 379 3be 3c3 3d8 3dd 3f1 3f6 450 455 4d7 4e1 53a 53f 599 5a3 5bc 5c1 5c7 5db 620 625 62a 63e
63	d6 e0 27e 288 28e 29d 2ac 2b6 2ca 2cf 2f6 2fb 30b 314 31a 31e 342 34c 35b 365 388 38c 38d 391 3a1 3a5 3a6 3aa 3bf 3c4 3d7 3d8 3dc 3dd 41e 423 437 43c 469 46e 472 477 4ff 502 503 508 50d 511 512 513 521 526 553 558 562 571 57b 58a 594 595 5a3 5a9 5ae 5c2 5df 5e0 5ee 5f4 607 60c 611 625 62a 639
64	da df 2c4 2c9 341 346 356 365 374 379 3be 3c3 3d3 3dd 3f1 3f6 450 455 4d7 4e1 53a 53f 54f 55e 5bc 5c1 5c7 5db 620 625 62a 63e
65	db e0 27e 288 28e 29d 2ac 2b6 2ca 2cf 2f6 2fb 30b 31a 374 379 388 38d 3a0 3a6 3aa 3ab 3be 3bf 3c3 3c4 3d7 3d8 3dc 3dd 3f1 3f6 437 43c 450 455 469 46e 472 477 4ff 502 503 511 512 513 53a 53f 553 558 562 571 57b 58a 594 5a3 5bc 5c1 5c7 5db 5df 5e0 5f3 5f4 607 60c 620 625 639 63e
66	e4 f8 2dd 2e2 36f 374 3be 3c3 450 45f 4f0 4fa 53a 53f 5c7 5db
67	e9 f8 2dd 2e2 301 306 36f 379 38d 392 3d7 3dc 3f1 3f6 469 46e 4f0 4fa 553 558 5bc 5c1 5c6 5da 5e0 5f4 639 63e
68	ea f9 2b0 2b5 33d 34c 35b 365 374 379 3be 3c3 3f1 3f6 450 455 51c 526 53a 53f 5bc 5c1 5c7 5db 611 620 62a 63e
69	ee f8 17b 18f 2dd 2e2 36f 379 4f0 4fa 5b2 5c1
70	ef f9 32d 337 3a5 3aa 3ba 3c4 437 43c 51c 521 5ae 5c2 607 60c
71	f3 f8 2dd 2e2 35a 35f 36f 379 3ec 3f1 4f0 4fa 568 577 5bc 5c1
72	f4 f9 35b 365 374 379 3b9 3be 3f1 3f6 51c 526 53a 53f 5bc 5c1 5c7 5db 62a 63e
73	fd 111 2ac 2b6 35b 365 3a5 3aa 3bf 3c4 437 43c 46e 472 477 478 4ff 509 521 526 57b 58a 5ae 5c2 607 60c 62a 639
74	102 111 2ac 2b6 31a 31f 342 34c 35b 365 374 379 38c 391 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 41e 423 437 43c 450 455 472 477 4ff 508 509 50d 521 526 53a 53f 57b 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5df 5ee 607 60c 611 620 62a 63e
75	103 112 2c9 2ce 356 365 374 379 3f1 3f6 535 53f 5bc 5c1 62a 63e
76	107 111 194 1a8 2ac 2b6 35b 365 38d 392 3a5 3aa 3bf 3c4 3d7 3dc 437 43c 469 46e 472 477 4ff 509 521 526 553 558 57b 58a 5ae 5c2 5cb 5da 5e0 5f4 607 60c 62a 639
77	108 112 346 350 3be 3c3 3d3 3dd 450 455 535 53a 5c7 5db 620 625
78	10c 111 2ac 2b6 35b 365 373 378 38d 392 3a5 3aa 3bf 3c4 3d7 3dc 405 40a 437 43c 469 46e 472 477 4ff 509 521 526 553 558 57b 581 58a 590 5ae 5c2 5d5 5da 5e0 5f4 607 60c 62a 639
79	10d 112 374 379 3d2 3dc 3f1 3f6 469 46e 535 53f 5bc 5c1 639 63e
80	116 12a 30f 314 3a1 3a6 3f0 3f5 482 491 522 52c 56c 571 5f9 60d
81	11b 12a 30f 314 333 338 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3c3 3f1 3f6 41e 423 437 43c 450 455 508 50d 521 522 526 52c 53a 53f 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 5f8 607 611 620 62a 63e
82	11c 12b 2e2 2e7 36f 379 3d7 3dc 3f1 3f6 469 46e 54e 553 5bc 5c1 5e0 5f4 639 63e
83	120 12a 1ad 1c1 30f 314 3a1 3ab 522 52c 5e4 5f3
84	121 12b 35f 369 3d7 3dc 3ec 3f6 469 46e 54e 553 5e0 5f4 639 63e
85	125 12a 30f 314 38c 391 3a1 3ab 41e 423 522 52c 59a 5a9 5ee 5f3
86	126 12b 342 34c 374 379 38c 391 3a6 3ab 3be 3c3 3d7 3dc 3eb 3f0 3f1 3f6 41e 423 450 455 469 46e 508 50d 53a 53f 54e 553 56c 571 595 5a9 5bc 5c1 5c7 5db 5e0 5ee 5f3 5f4 5f9 60d 611 620 639 63e
87	12f 143 328 32d 3ba 3bf 409 40e 49b 4aa 53b 545 585 58a 612 626
88	134 143 328 32d 34c 351 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3f1 3f6 437 43c 450 455 521 526 53a 53b 53f 545 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 620 62a 63e
89	135 144 2fb 300 342 34c 374 379 388 38c 38d 391 3a6 3ab 3be 3c3 3d7 3dc 3f1 3f6 41e 423 450 455 469 46e 508 50d 53a 53f 553 558 567 571 595 5a9 5bc 5c1 5c7 5db 5e0 5ee 5f3 5f4 611 620 639 63e
90	139 143 1c6 1da 328 32d 3ba 3c4 53b 545 5fd 60c
91	13a 144 342 34c 374 378 379 382 38c 38d 391 392 3a6 3ab 3be 3c3 3d7 3dc 3f1 3f6 405 40a 41e 423 450 455 469 46e 508 50d 53a 53f 553 558 567 571 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5ee 5f3 5f4 611 620 639 63e
92	13e 143 328 32d 3a5 3aa 3ba 3c4 437 43c 53b 545 5b3 5c2 607 60c
93	13f 144 342 34c 35b 365 374 379 38c 391 3a5 3a6 3aa 3ab 3be 3bf 3c3 3c4 3f1 3f6 404 409 41e 423 437 43c 450 455 508 50d 521 526 53a 53f 567 571 585 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 612 620 626 62a 63e
94	148 15c 341 346 3d3 3d8 422 427 4b4 4c3 554 55e 59e 5a3 62b 63f
95	14d 15c 341 346 365 36a 374 379 3be 3c3 3d3 3dd 3f1 3f6 450 455 53a 53f 554 55e 5bc 5c1 5c7 5db 620 625 62a 63e
96	14e 15d 314 319 342 34c 35b 365 374 379 38c 391 3a1 3a5 3aa 3ab 3be 3bf 3c3 3c4 3f1 3f6 41e 423 437 43c 450 455 508 50d 521 526 53a 53f 580 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 607 60c 611 620 62a 63e

97	152 15c 1df 1f3 341 346 3d3 3dd 554 55e 616 625
98	153 15d 342 34c 35b 365 374 379 38c 39b 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 437 43c 450 455 508 50d 521 526 53a 53f 580 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 620 62a 63e
99	157 15c 341 346 3be 3c3 3d3 3dd 450 455 554 55e 5cc 5db 620 625
100	158 15d 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3d8 3dd 3f1 3f6 41d 422 437 43c 450 455 521 526 53a 53f 580 58a 59e 5a3 5ae 5bc 5c1 5c2 5c7 5db 607 60c 620 625 62a 62b 63e 63f
101	161 175 2c4 2c9 356 35a 35f 365 3ec 3f6 4dc 4e1 56d 577 62a 63e
102	166 175 35a 35f 379 383 3ec 3f1 56d 577 5bc 5c1
103	167 176 32d 332 35b 365 374 379 3a5 3aa 3ba 3be 3c3 3c4 3d8 3dd 3f1 3f6 437 43c 450 455 521 526 53a 53f 599 5a3 5ae 5bc 5c1 5c2 5c7 5db 607 60c 620 625 62a 63e
104	16b 175 1f8 20c 35a 35f 3ec 3f6 56d 577 62f 63e
105	16c 176 35b 365 374 379 3a5 3b4 3be 3c3 3d8 3dd 3f1 3f6 450 455 521 526 53a 53f 599 5a3 5ae 5bc 5c1 5c2 5c7 5db 620 625 62a 63e
106	170 175 35a 35f 3d7 3dc 3ec 3f6 469 46e 56d 577 5e5 5f4 639 63e
107	171 176 2c4 2c9 356 365 374 379 3be 3c3 3d8 3dd 3f1 3f6 436 440 450 455 4cd 4e1 53a 53f 599 5a3 5bc 5c1 5c7 5db 620 625 62a 63e
108	17a 18e 2dd 2e2 36f 373 378 379 38d 392 3d7 3dc 3f1 3f6 405 40a 469 46e 4f5 4fa 553 558 586 590 5bc 5c1 5d5 5da 5e0 5f4 639 63e
109	17f 18e 373 378 392 39c 405 40a 586 590 5d5 5da
110	180 18f 346 34b 374 379 3be 3c3 3d3 3dd 450 455 53a 53f 5b2 5c1 5c7 5db 620 625
111	184 18e 211 220 4e5 4ef 57c 586
112	185 18f 374 379 3be 3cd 53a 53f 5b2 5c1 5c7 5db
113	189 18e 342 34c 373 374 378 379 38c 38d 391 392 3a6 3ab 3be 3c3 3d7 3dc 3f1 3f6 405 40a 41e 423 450 455 469 46e 508 50d 53a 53f 553 558 56c 571 586 590 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5ee 5f3 5f4 5f9 5fe 611 620 639 63e
114	18a 18f 2dd 2e2 36f 379 44f 459 4e6 4fa 5b2 5c1
115	193 1a7 2ac 2b6 342 34c 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 437 43c 450 455 472 477 4ff 508 50d 50e 521 526 53a 53f 57b 58a 595 59f 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 620 62a 63e
116	198 1a7 38c 391 3ab 3b5 41e 423 59f 5a9 5ee 5f3
117	199 1a8 35f 364 38d 392 3d7 3dc 3ec 3f6 469 46e 553 558 5cb 5da 5e0 5f4 639 63e
118	19d 1a7 22a 239 4fe 508 595 59f
119	19e 1a8 38d 392 3d7 3e6 553 558 5cb 5da 5e0 5f4
120	1a2 1a7 342 34c 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 437 43c 450 455 508 50d 521 526 53a 53f 585 58a 595 59f 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 612 617 620 62a 63e
121	1a3 1a8 2ac 2b6 35b 365 38d 392 3a5 3aa 3bf 3c4 3d7 3dc 437 43c 468 469 46e 477 521 526 553 558 57b 58a 5ae 5c2 5cb 5da 5e0 5f4 607 60c 62a 639
122	1ac 1c0 30f 314 342 34c 35b 365 374 379 38c 391 3a1 3ab 3be 3c3 3f1 3f6 41e 423 450 455 508 50d 521 526 527 52c 53a 53f 595 5a9 5ae 5b8 5bc 5c1 5c7 5db 5ee 5f3 611 620 62a 63e
123	1b1 1c0 3a5 3aa 3c4 3ce 437 43c 5b8 5c2 607 60c
124	1b2 1c1 342 34c 374 378 379 37d 38c 38d 391 392 3be 3c3 3d7 3dc 3f1 3f6 405 40a 41e 423 450 455 469 46e 508 50d 53a 53f 553 558 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5e4 5ee 5f4 611 620 639 63e
125	1b6 1c0 243 252 517 521 5ae 5b8
126	1b7 1c1 3a6 3ab 3f0 3ff 56c 571 5e4 5f3 5f9 60d
127	1bb 1c0 35b 365 374 379 3be 3c3 3d8 3dd 3f1 3f6 450 455 521 526 53a 53f 59e 5a3 5ae 5b8 5bc 5c1 5c7 5db 620 625 62a 62b 630 63e
128	1bc 1c1 30f 314 3a1 3ab 481 48b 518 52c 5e4 5f3
129	1c5 1d9 328 32d 35b 365 374 379 3a5 3aa 3ba 3c4 3f1 3f6 437 43c 521 526 53a 53f 540 545 5ae 5bc 5c1 5c2 5c7 5d1 607 60c 62a 63e
130	1ca 1d9 3be 3c3 3dd 3e7 450 455 5d1 5db 620 625
131	1cb 1da 342 34c 35b 365 374 379 38c 396 3a5 3aa 3be 3c3 3f1 3f6 437 43c 450 455 508 50d 521 526 53a 53f 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5fd 607 611 620 62a 63e
132	1cf 1d9 25c 26b 530 53a 5c7 5d1
133	1d0 1da 3bf 3c4 409 418 585 58a 5fd 60c 612 626
134	1d5 1da 328 32d 3ba 3c4 49a 4a4 531 545 5fd 60c
135	1de 1f2 341 346 374 379 3be 3c3 3d3 3d7 3dc 3dd 3f1 3f6 450 455 469 46e 53a 53f 559 55e 5bc 5c1 5c7 5db 5ea 5f4 620 625 639 63e
136	1e3 1f2 3d7 3dc 3f6 400 469 46e 5ea 5f4 639 63e
137	1e4 1f3 35b 365 374 379 3a5 3af 3be 3c3 3f1 3f6 450 455 521 526 53a 53f 5ae 5bc 5c1 5c2 5c7 5db 616 620 62a 63e
138	1e8 1f2 275 284 549 553 5e0 5ea
139	1e9 1f3 3d8 3dd 422 431 59e 5a3 616 625 62b 63f
140	1ee 1f3 341 346 3d3 3dd 4b3 4bd 54a 55e 616 625
141	1f7 20b 342 34c 35a 35f 374 379 38c 391 3a6 3ab 3be 3c3 3ec 3f1 41e 423 450 455 508 50d 53a 53f 56c 571 572 577 595 5a9 5bc 5c1 5c7 5db 5ee 5f3 5f9 603 611 620
142	1fc 20b 342 34c 374 379 38c 38d 391 392 3a6 3ab 3be 3c3 3d7 3dc 3f1 3f6 40a 419 41e 423 450 455 469 46e 508 50d 53a 53f 553 558 56c 571 595 5a9 5bc 5c1 5c7 5d5 5da 5db 5e0 5ee 5f3 5f4 5f9 603 611 620 639 63e
143	1fd 20c 374 379 3be 3c8 3f1 3f6 53a 53f 5bc 5c1 5c7 5db 62f 63e
144	1ff 200 204 205 27e 288 2ac 2b6 2e2 2e7 30b 31a 35b 365 36f 379 3a5 3a6 3aa 3ab 3bf 3c4 3f1 3f6 437 43c 472 477 4ff 50e 521 526 567 571 57b 58a 5ae 5bc 5c1 5c2 5df 5f3 607 60c 62a 63e
145	210 224 35b 365 373 378 38d 392 3a5 3aa 3bf 3c4 3d7 3dc 405 40a 437 43c 469 46e 521 526 553 558 585 58a 58b 590 5ae 5c2 5d5 5da 5e0 5f4 607 60c 612 61c 62a 639
146	215 224 342 34c 35b 365 374 379 38c 391 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 41e 432 437 43c 450 455

	508 50d 521 526 53a 53f 585 58a 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 612 61c 620 62a 63e
147	216 220 373 378 38d 392 3d7 3e1 405 40a 4e5 4ef 553 558 57c 590 5d5 5da 5e0 5f4
148	21a 224 2a7 2b6 57b 585 612 61c
149	21b 220 2dd 2e2 36f 373 378 379 38d 392 3d7 3dc 3f1 3f6 405 40a 459 463 469 46e 4e5 4e6 4ef 4fa 553 558 57c 590 5bc 5c1 5d5 5da 5e0 5f4 639 63e
150	229 23d 342 34c 3d8 3dd 508 50d 595 59e 5a3 5a4 611 625 62b 635
151	22e 23d 35b 365 374 379 3a5 3aa 3be 3c3 3d8 3dd 3f1 3f6 437 44b 450 455 521 526 53a 53f 59e 5a3 5ae 5bc 5c1 5c2 5c7 5db 620 625 62a 62b 635 63e
152	22f 239 38c 391 3a6 3ab 3f0 3fa 41e 423 4fe 508 56c 571 595 5a9 5ee 5f3 5f9 60d
153	233 23d 2c0 2cf 594 59e 62b 635
154	234 239 2ac 2b6 342 34c 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 437 43c 450 455 477 47c 4fe 50d 521 526 53a 53f 57b 58a 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 620 62a 63e
155	242 24c 2d9 2e8 35b 365 3f1 3f6 521 526 5ad 5ae 5bc 5bd 62a 63e
156	247 24c 2d9 2e8 374 379 3be 3c3 450 464 53a 53f 5ad 5c1 5c7 5db
157	248 252 3a5 3aa 3bf 3c4 409 413 437 43c 517 521 585 58a 5ae 5c2 607 60c 612 626
158	24d 252 30f 314 342 34c 35b 365 374 379 38c 391 3a1 3ab 3be 3c3 3f1 3f6 41e 423 450 455 48b 495 508 50d 517 518 526 52c 53a 53f 595 5a9 5bc 5c1 5c7 5db 5ee 5f3 611 620 62a 63e
159	25b 265 2f2 301 374 379 38d 392 3d7 3dc 3f1 3f6 469 46e 53a 53f 553 558 5bc 5c1 5c6 5c7 5d6 5da 5e0 5f4 639 63e
160	260 265 2f2 301 38d 392 3d7 3dc 469 47d 553 558 5c6 5da 5e0 5f4
161	261 26b 3be 3c3 3d8 3dd 422 42c 450 455 530 53a 59e 5a3 5c7 5db 620 625 62b 63f
162	266 26b 328 32d 35b 365 374 379 3a5 3aa 3ba 3c4 3f1 3f6 437 43c 4a4 4ae 521 526 530 531 53f 545 5ae 5bc 5c1 5c2 607 60c 62a 63e
163	274 27e 30b 31a 342 34c 374 379 38c 391 3be 3c3 3d7 3dc 3f1 3f6 41e 423 450 455 469 46e 508 50d 53a 53f 595 5a9 5bc 5c1 5c7 5db 5df 5ee 5ef 5f4 611 620 639 63e
164	279 27e 30b 31a 3a6 3ab 3f0 3f5 482 496 56c 571 5df 5f3 5f9 60d
165	27a 284 2c4 2c9 356 365 3d7 3dc 440 445 469 46e 4cd 4e1 549 553 5e0 5f4 62a 639
166	27f 284 341 346 374 379 3be 3c3 3d3 3d7 3dc 3dd 3f1 3f6 450 455 469 46e 4bd 4c7 53a 53f 549 54a 553 55e 5bc 5c1 5c7 5db 5e0 5f4 620 625 639 63e
167	28d 297 324 333 342 34c 35b 365 374 379 38c 391 3a5 3a6 3aa 3ab 3be 3c3 3f1 3f6 41e 423 437 43c 450 455 508 50d 521 526 53a 53f 56c 571 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 5f8 5f9 607 608 611 620 62a 63e
168	292 297 324 333 3bf 3c4 409 40e 49b 4af 585 58a 5f8 60c 612 626
169	293 29d 2dd 2e2 342 34c 36f 374 38c 391 3a6 3ab 3be 3c3 41e 423 450 455 459 45e 4e6 4fa 508 50d 53a 53f 562 571 595 5a9 5c7 5db 5ee 5f3 611 620
170	298 29d 342 34c 35a 35f 374 379 38c 391 3a6 3ab 3be 3c3 3ec 3f1 41e 423 450 455 4d6 4e0 508 50d 53a 53f 562 563 571 577 595 5a9 5bc 5c1 5c7 5db 5ee 5f3 611 620
171	2a6 2b0 33d 34c 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 437 43c 450 455 521 526 53a 53f 585 58a 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 612 620 621 62a 63e
172	2ab 2b0 33d 34c 3d8 3dd 422 427 4b4 4c8 59e 5a3 611 625 62b 63f
173	2b1 2b6 35b 365 373 378 38d 392 3a5 3aa 3bf 3c4 3d7 3dc 405 40a 437 43c 469 46e 4ef 4f9 521 526 553 558 57b 57c 58a 590 5ae 5c2 5d5 5da 5e0 5f4 607 60c 62a 639
174	2bf 2c9 356 365 374 379 3be 3c3 3d8 3dd 3f1 3f6 450 455 53a 53f 59e 5a3 5bc 5c1 5c7 5db 620 625 62a 62b 63a 63e
175	2c5 2cf 30f 314 342 34c 38c 391 3a1 3ab 3d8 3dd 41e 423 48b 490 508 50d 518 52c 594 595 5a3 5a9 5ee 5f3 611 625
176	2de 2e8 328 32d 35b 365 3a5 3aa 3ba 3c4 3f1 3f6 437 43c 4a4 4a9 521 526 531 545 5ad 5ae 5bc 5c2 607 60c 62a 63e
177	2e3 2e8 35b 365 3f1 3f6 526 52b 5ad 5bc 62a 63e
178	2f7 301 341 346 374 379 38d 392 3be 3c3 3d3 3d7 3dc 3dd 3f1 3f6 450 455 469 46e 4bd 4c2 53a 53f 54a 553 558 55e 5bc 5c1 5c6 5c7 5da 5db 5e0 5f4 620 625 639 63e
179	2fc 301 374 379 38d 392 3d7 3dc 3f1 3f6 469 46e 53f 544 553 558 5bc 5c1 5c6 5da 5e0 5f4 639 63e
180	310 31a 342 34c 35a 35f 374 379 38c 391 3be 3c3 3ec 3f1 41e 423 450 455 4d6 4db 508 50d 53a 53f 563 577 595 5a9 5bc 5c1 5c7 5db 5df 5ee 611 620
181	315 31a 342 34c 374 379 38c 391 3be 3c3 3d7 3dc 3f1 3f6 41e 423 450 455 469 46e 508 50d 53a 53f 553 55d 595 5a9 5bc 5c1 5c7 5db 5df 5e0 5ee 5f4 611 620 639 63e
182	329 333 35b 365 373 378 38d 392 3a5 3aa 3d7 3dc 405 40a 437 43c 469 46e 4ef 4f4 521 526 553 558 57c 590 5ae 5c2 5d5 5da 5e0 5f4 5f8 607 62a 639
183	32e 333 342 34c 35b 365 374 379 38c 391 3a5 3a6 3aa 3ab 3be 3c3 3f1 3f6 41e 423 437 43c 450 455 508 50d 521 526 53a 53f 571 576 595 5a9 5ae 5bc 5c1 5c2 5c7 5db 5ee 5f3 5f8 607 611 620 62a 63e
184	347 34c 35b 365 374 379 3a5 3aa 3be 3bf 3c3 3c4 3f1 3f6 437 43c 450 455 521 526 53a 53f 58a 58f 5ae 5bc 5c1 5c2 5c7 5db 607 60c 611 620 62a 63e
185	360 365 374 379 3be 3c3 3d8 3dd 3f1 3f6 450 455 53a 53f 5a3 5a8 5bc 5c1 5c7 5db 620 625 62a 63e

Table 6. Basis elements of $\mathrm{Ker}(E_2)$

Row No.	Support set of the row
1	4 9 d e 13 1d 21 22 26 27 2c 30 31 35 3a 4e 58 5d 62 67 71 76 7b 7c 81 86 8b 8f 90 a8 b2 b7 c2 c7 cc d1 d5 d6 db df e0 e4 e9 f3 f8 f9 fd 10c 117 11c 120 121 126 12a 12b 130 134 13a 13f 148 149 14d 14e 153 158 161 166 16b 170 175 176 17a 17b 17f 180 184 185 18a 18e 18f 193 194 19d 19e 1ac 1b1 1bb 1c6 1cb 1cf 1d0 1d5 1df 1e3 1e9 1f3 1f7 1fc 206 210 21a 21b 21f 224 225 233 238 23d 243 248 24d 252 260 26a 270 274 275 279 27a 27f 283 284 288 289 28e 292 297 298 2a1 2a2 2ab 2b5 2ba 2bb 2bf 2c5 2c9 2ca 2ce 2cf 2d9 2de 2e3 2e8 2ec 2ed 2f2 2f6 2f7 2fc 300 301 305 30a 30b 30f 310 314 315 31a 31f 323 32d 332 337 338 33c 33d 342 346 347 34c 350 35f 364 36e 36f 374 379 37d 37e 388 38d 391 392 397 3a5 3af 3b4 3b5 3b9 3be 3c3 3c8 3d2 3dc 3e1 3e7 3f1 3fa 3fb 3ff 404 405 409 40a 40f 414 415 416 422 42c 42d 432 436 437 43b 43c 441 446 44a 44b 459 45e 464 468 46d 477 47c 481 482 486 487 48b 48c 491 49b 4a0 4a5 4aa 4ae 4b3 4b4 4b5 4b8 4be 4cc 4cd 4d1 4d6 4e1 4e5 4ef 4f4 4f9 4fa 4fe 4ff 508 509 526 530 531 535 536 53b 540 545 54a 54f 554 559 55e 562 567 571 576 577 57b 580 585 58a 590 59a 59b 59c 59e 59f 5a3 5a4 5a8 5a9 5ae 5b3 5b8 5bc 5bd 5c2 5c7 5cb 5cc 5d1 5d6 5e0 5e4 5e9 5ea 5ee 5f3 5f4 5f8 5f9 5fd 5fe 602 603 608 60c 60d 617 61b 620 621 625 62a 62f 639 63e
2	8 18 4f 54 59 5d 5e 68 6d 72 77 80 9e a3 b8 bc c2 df e0 e9 f9 130 135 13a 13e 144 149 14e 153 157 158 161 17f 184 194 199 19d 19e 1a3 1c0 1da 1e8 211 21b 21f 225 22a 22b 22c 22f 234 238 239 242 25b 260 275 27a 27e 27f 283 284 2a1 2ba 2bb 2c9 300 306 30b 310 315 319 31a 323 33c 341 356 35a 35f 360 364 382 387 39b 39c 3e6 3ec 3f1 3f6 3fa 3fb 41d 422 43b 440 445 463 468 47c 47d 4c7 4cd 4d2 4d7 4db 4dc 4f5 4fe 503 51c 521 549 55d 55e 567 577 5a8 5ae 5b3 5b8 5bc 5bd 5cc 5d6 5df 5fd 602 61b 63e 63f
3	17 18 31 6d 72 76 77 81 86 8b 8f 90 99 9e b7 b8 bc d5 f8 f9 112 135 149 14e 153 158 162 167 16c 170 171 17a 17f 193 194 198 19d 19e 1b6 1d9 1da 1f2 1f3 21b 22a 22b 22c 22f 234 238 239 243 248 24d 251 252 25b 274 279 27e 283 292 297 2ba 2bb 2d3 2d4 300 30b 310 315 319 31a 324 329 32e 332 333 33c 355 35f 373 378 39b 39c 3b4 3b5 3e6 3ec 3f6 3fa 403 405 40a 40f 413 414 415 416 41d 42d 436 43b 440 454 459 463 47c 495 496 4af 4cd 4db 4e6 4eb 4f0 4f4 4fe 504 50e 517 51c 535 53a 553 55d 576 590 5bc 5c7 5cc 5d1 5d5 5d6 5df 5e0 5e5 5ea 5ef 5f8 5fd 616 634 63e

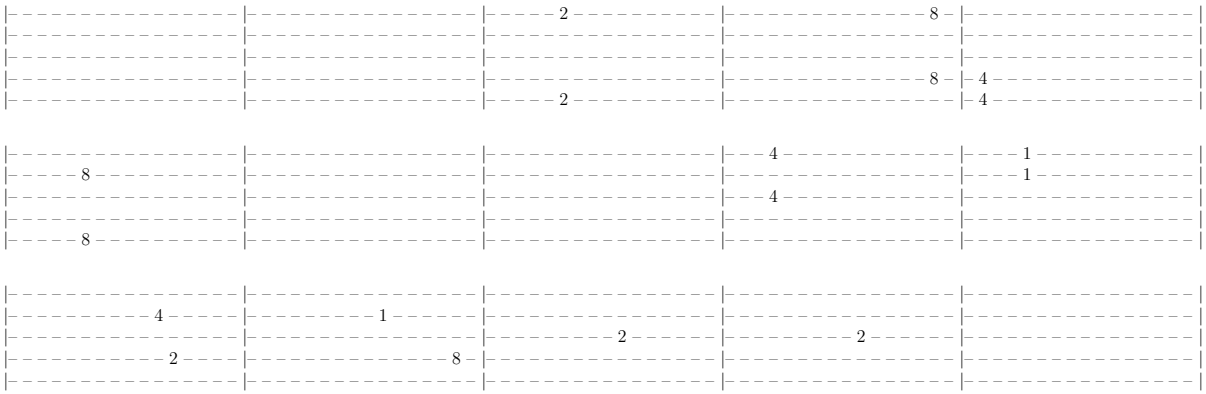
C New differential paths of Keccak-n with $n = 224, 256, 384, 512$ with the best complexity for producing (near-)collisions

In this section, we present five new differential characteristics for Keccak, which can lead to 4-round collisions and 5-round near-collisions using the target differential algorithm [10]. To the best of our knowledge, the presented differential characteristics are the best in terms of the complexity. All the 2-round differential characteristics are almost double paths. Following the representation of differential characteristic in [10], we present five new and better different differential characteristics for Keccak-224, Keccak-256, Keccak-384 and Keccak-512 and a comparison of the complexity is provided in Table 1.

C.1 4-round and 5-round differential path for Keccak-224 and Keccak-256

Characteristic 1: This characteristic can be used to produce a 4-round collision with probability 2^{-23} for Keccak-224 and Keccak-256 by using the target difference algorithm. The probability of the first transition is 2^{-12} since there are 6 active Sboxes. The probability for the second transition is 2^{-11} since there are total 5 active Sboxes. For Keccak-224 and Keccak-256, there are no active Sboxes at the third round, as a result, the probability for the third round is 1.

47A591EB – 74CB23D	C913D64799B – 7AC8	1D6C8F593DA991EB	88FAB23D5833D647	2B2C7AC8CB958F59
47A591EB – 74CB23D	C913D64799B – 7AC8	1D6C8F593DA991EB	88FAB23D5833D647	2B2C7AC8CB958F59
47A591EB – 74CB23D	C913D64799B – 7AC8	1D6C8F593DB991EB	88FAB23D5833D647	2B2C7AC8CB948F59
47A591EB – 74CB23D	C913D64799B – 7AC8	1D6C8F593DE991EB	88FAB23D4833D647	2B2C7AC8CB958F59
47A591EB – 74CB23D	D913D64799B – 7AC8	1D6C8F593DA991EB	88FEB23D5833D647	2B2C7AC8CB958F59

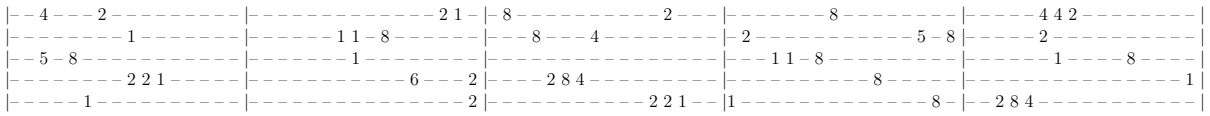


One may be curious that why the probability of the second transition is 2^{-11}. We claim that there are 5 active Sboxes in total in the second transition, while in the figure it shows that there are 6 active Sboxes. For the second input difference, after passing through the diffusion layer $\alpha \circ \pi \circ \rho \circ \theta$, the internal state is the following:

Note that the two consecutive numbers in bold means they are in the same active Sbox as each number is represented in 4-bit, but the Sbox takes 5-bit as input.

Characteristic 2: This differential characteristic can be used to produce a 5-round near-collision with probability $2^{-(12+11+12+6)} = 2^{-41}$ for Keccak-224 and with probability $2^{-(12+11+12+10)} = 2^{-45}$ for Keccak-256. The probability for the first 2-round is $2^{-(12+11)} = 2^{-23}$ and the probability of the third transition is 2^{-12}, since there are total 6 active Sboxes at this round. For Keccak-224, the number of active Sboxes at the fourth transition is 3 whereas for Keccak-256, the number of active Sboxes at the fourth transition in the left-most 256 bits is 5. Using this differential characteristic, one can produce a near-collision with a better success probability than that of the differential characteristics presented in [10].

83A6591EA3D2C8F5	CCD83D646489EB23	9ED4C8F58EB647AC	AC19EB23C47D591E	65CAC7AC95963D64
83A6591EA3D2C8F5	CCD83D646489EB23	9ED4C8F58EB647AC	AC19EB23C47D591E	65CAC7AC95963D64
83A6591EA3D2C8F5	CCD83D646489EB23	9EDCC8F58EB647AC	AC19EB23C47D591E	65CA47AC95963D64
83A6591EA3D2C8F5	CCD83D646489EB23	9EF4C8F58EB647AC	A419EB23C47D591E	65CAC7AC95963D64
83A6591EA3D2C8F5	CCD83D646C89EB23	9ED4C8F58EB647AC	AC19EB23C47F591E	65CAC7AC95963D64



Similar to the case in **Characteristic 1**, for the second input difference, after passing through the diffusion layer $\alpha \circ \pi \circ \rho \circ \theta$, the internal state is the following:

As a result, the probability of the second transition is 2^{-11}. Again, the two consecutive numbers in bold means they are in the same active Sbox as each number is represented in 4-bit, but the Sbox takes 5-bit as input.

C.2 4-round and 5-round differential path for Keccak-384 and Keccak-512

Characteristic 3: This characteristic can be used to produce a 2-round collision with probability $2^{-(12+11)} = 2^{-23}$ for Keccak-384 and a near-collision for Keccak-512. The numbers of active Sboxes for the first and second transition are 6 and 5, respectively. Note that this characteristic can also be used to find a collision for Keccak-224 and Keccak-256.

23D6 – E99647A8F4B	AC8F336 – F5919227	1EB27B5323D63AD9	647AB – 67AC8F11F5	F591972B1EB25658
23D6 – E99647A8F4B	AC8F336 – F5919227	1EB27B5323D63AD9	647AB – 67AC8F11F5	F591972B1EB25658
23D6 – E99647A8F4B	AC8F336 – F5919227	1EB27B7323D63AD9	647AB – 67AC8F11F5	F59197291EB25658
23D6 – E99647A8F4B	AC8F336 – F5919227	1EB27BD323D63AD9	647A9 – 67AC8F11F5	F591972B1EB25658
23D6 – E99647A8F4B	AC8F336 – F591B227	1EB27B5323D63AD9	647AB – 67AC8F11FD	F591972B1EB25658

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- 4 - - - - - - - - - - - - -	- - - - - - - - - 1 - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - 1 - - - - - - -	- - - - - - - - - - - - - 8 - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- 4 - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - 8 - -

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - 8	2 - - - - - - - - - - - - - - -
1 - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	2 - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - 8	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
1 - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - 8 - - - - - - - - -	- - - - - 2 - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - 4 - - - - - - - - - -	- - - - - 4 - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - 4 - - - - - - - - -	- - - - - - - - - 1 - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -

For the second input difference, after passing through the diffusion layer $\alpha \circ \pi \circ \rho \circ \theta$, the internal state is the following:

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - **5** - - - 8 - - - -	- - - - - - - 4 - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - 8 - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - 1 - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -

which shows the probability for this transition is 2^{-11}.

Characteristic 4: This differential characteristic can lead to a 3-round near-collision for Keccak-384 with probability $2^{-(12+11+12+16)} = 2^{-51}$. The probability for the first 2-round is $2^{-(12+11)} = 2^{-23}$ and the probability of the third transition is 2^{-12}, since there are total 6 active Sboxes at this round. Since in the fourth transition the number of active Sboxes in the left-most 384 is 8, the probability of the fourth transition is 2^{-16}.

EB – 74CB23D47A591	4799B – 7AC8C913D6	593DA991EB1D6C8F	3D5833D64788FAB2	C8CB958F592B2C7A
EB – 74CB23D47A591	4799B – 7AC8C913D6	593DA991EB1D6C8F	3D5833D64788FAB2	C8CB958F592B2C7A
EB – 74CB23D47A591	4799B – 7AC8C913D6	593DB991EB1D6C8F	3D5833D64788FAB2	C8CB948F592B2C7A
EB – 74CB23D47A591	4799B – 7AC8C913D6	593DE991EB1D6C8F	3D4833D64788FAB2	C8CB958F592B2C7A
EB – 74CB23D47A591	4799B – 7AC8D913D6	593DA991EB1D6C8F	3D5833D64788FEB2	C8CB958F592B2C7A

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - 2 -	- - - - - - - - 8 - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - 8 - - - - - - - -	- - - - - - - - - - - 4 - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - 2 -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - 4 - - - -

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - 4 - -	- - - - - - - - - - - - - - 1 -
- - - - - - - - - - - - - - 8 -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - 1 -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - 4 - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - 8 -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - 4 - - - - - - - - - - -	- - - 1 - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - 2 - - - - - - - - - - -	- - - 2 - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - 2 - - - - - - - - - -	- - - - - - - - 8 - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -

- - - - 8 - - - 4 - - - - - - -	2 - - - - - - - - - - - - - - 4	- - 1 - - - - - - - - - - - 4 -	- - - - - - - - 1 - - - - - - - -	- - - - - - - 8 8 4 - - - - - - -
- - - - - - - - - - 2 - - - - -	- - - - - - - - 2 2 1 - - - - -	- - - - 1 - - - - 8 - - - - - -	1 - - 4 - - - - - - - - - - - 10	- - - - - - - 4 - - - - - - - -
- - - - 10 1 - - - - - - - - - -	- - - - - - - - - - 2 - - - - - -	- - - - - - - - - - - - - - - -	- - - - - 2 2 1 - - - - - - - -	- - - - - - - - 2 - - - 1 - - -
- - - - - - - - - - 4 4 2 - - -	- 4 - - - - - - - - - - - 12 - -	- - - - - - 5 - 8 - - - - - - - -	- - - - - - - - - - - - 1 - - - - -	- 2 - - - - - - - - - - - - - - -
- - - - - - - 2 - - - - - - - - -	- 4 - - - - - - - - - - - - - - -	- - - - - - - - - - - - - 4 4 2	- - 2 - - - - - - - - - - - - 1	- - - - 5 - 8 - - - - - - - - -

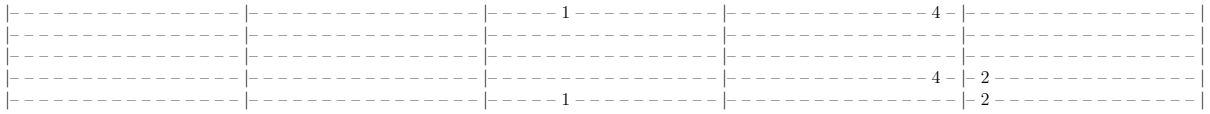
For the second input difference, after passing through the diffusion layer $\alpha \circ \pi \circ \rho \circ \theta$, the internal state is the following:

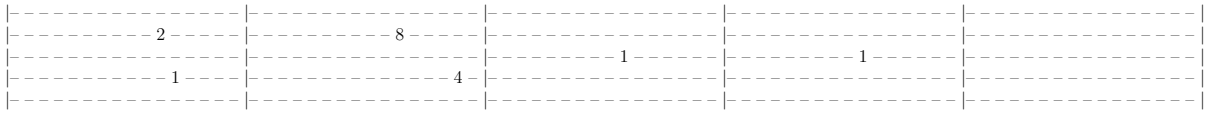
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - **2 8** - - - 4	- - - - - - - - - - - 2 - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - 4 - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - 8 - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - - - - -

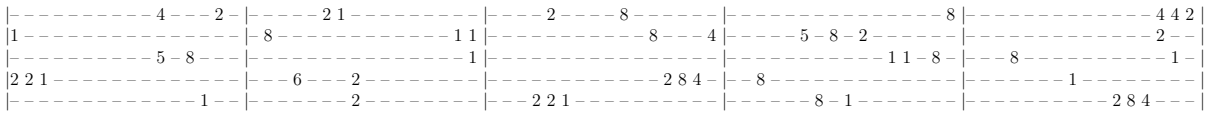
The two consecutive numbers in bold means they are in the same active Sbox and the probability for the second transition is 2^{-11}.

Characteristic 5: This differential characteristic can lead to a 3-round near-collision for Keccak-512 with probability $2^{-(12+11+12+25)} = 2^{-60}$. The probability values for the first 3-round are the same as the probability values of Keccak-384. In the last transition, the number of active Sboxes in the left-most 512 bits is equal to 12, as a result, the probability of this transition is 2^{-25}. Note that 11 active Sboxes have input differences of Hamming weight 1, which have probability 2^{-2} and one active Sbox whose input difference has Hamming weight 2, which has probability 2^{-3}.

A3D2C8F583A6591E	6489EB23CCD83D64	8EB647AC9ED4C8F5	C47D591EAC19EB23	95963D6465CAC7AC
A3D2C8F583A6591E	6489EB23CCD83D64	8EB647AC9ED4C8F5	C47D591EAC19EB23	95963D6465CAC7AC
A3D2C8F583A6591E	6489EB23CCD83D64	8EB647AC9EDCC8F5	C47D591EAC19EB23	95963D6465CA47AC
A3D2C8F583A6591E	6489EB23CCD83D64	8EB647AC9EF4C8F5	C47D591EA419EB23	95963D6465CAC7AC
A3D2C8F583A6591E	6C89EB23CCD83D64	8EB647AC9ED4C8F5	C47F591EAC19EB23	95963D6465CAC7AC







For the second input difference, after passing through the diffusion layer $\alpha \circ \pi \circ \rho \circ \theta$, the internal state is the following:

The two consecutive numbers in bold means they are in the same active Sbox.