Cube-like Attack on Round-Reduced Initialization of Ketje Sr

Xiaoyang Dong, Zheng Li, Xiaoyun Wang and Ling Qin

Shandong University, Tsinghua University

FSE 2017
Tokyo, Japan

Outline--divided into 3 parts

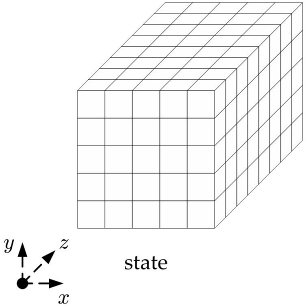
- Ketje
- Related Works
  - Cube-like attack
  - auxiliary variable
  - Linear stucture
- Our Attacks

Ketje

- designed by the Keccak Team
- one of the 16 survivors of 3rd CAESAR competition
- Specification of Ketje
  - Keccak-p permutations
  - MonkeyWrap
  - Four instances: Ketje Sr, Jr, Minor, Major

Keccak-p permutations

- designed by the Keccak Team
- tunable number of rounds
- 7 state sizes: *b*
  - b ∈ {25, 50, 100, 200, 400, 800, 1600}
- round function $R = \iota \circ \chi \circ \pi \circ \rho \circ \theta$



(a)

0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

(b)

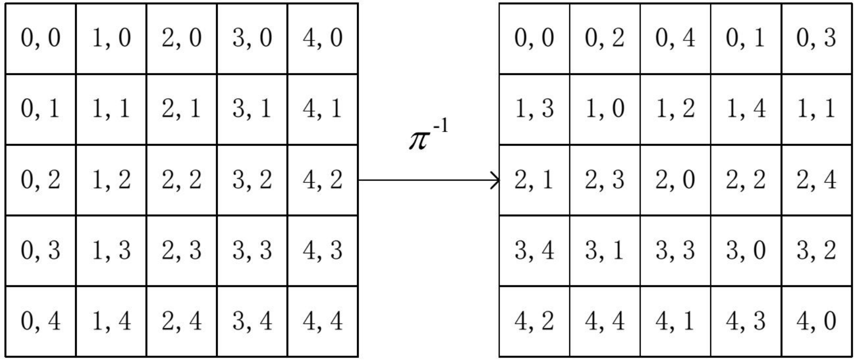
$$\theta : A[x,y] = A[x,y] \oplus \textstyle\sum_{j=0}^{4} (A[x-1,j] \oplus (A[x+1,j] \lll 1)).$$
$$\rho : A[x,y] = A[x,y] \lll r[x,y].$$
$$\pi : A[y, 2x+3y] = A[x,y].$$
$$\chi : A[x,y] = A[x,y] \oplus ((\neg A[x+1,y]) \wedge A[x+2,y].$$
$$\iota : A[0,0] = A[0,0] \oplus RC.$$

Keccak-p* permutations

- a twisted permutation proposed in Ketje v2

$$\textsc{Keccak}\text{-}p^*[b] = \pi \circ \textsc{Keccak}\text{-}p[b] \circ \pi^{-1}$$

$$\pi^{-1} : A[x+3y, x] = A[x, y].$$



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

$\xrightarrow{\pi^{-1}}$

0, 0	0, 2	0, 4	0, 1	0, 3
1, 3	1, 0	1, 2	1, 4	1, 1
2, 1	2, 3	2, 0	2, 2	2, 4
3, 4	3, 1	3, 3	3, 0	3, 2
4, 2	4, 4	4, 1	4, 3	4, 0

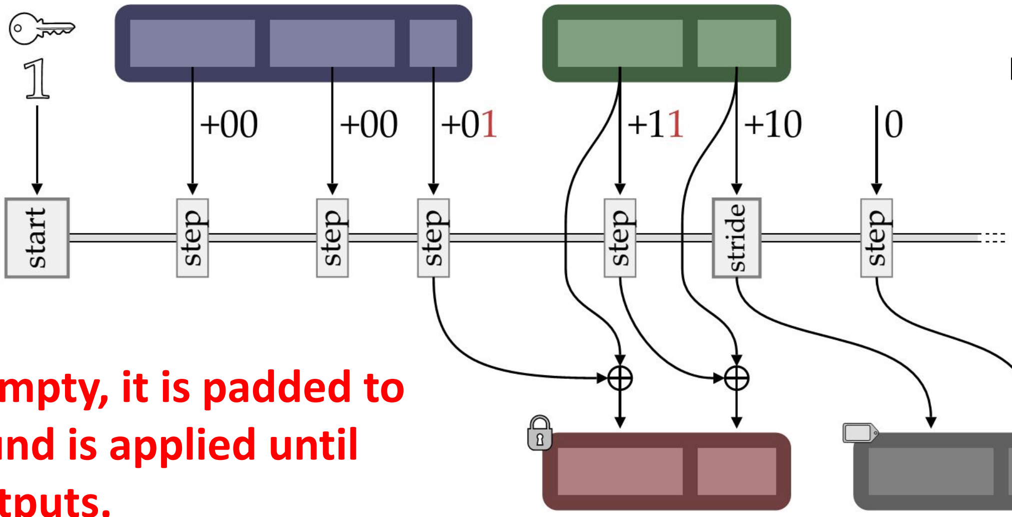
MonkeyWrap

- an authenticated encryption mode proposed by the Keccak team

1. Initialization
2. Proc. Associate
3. Proc. Plaintext
4. Finalization

Associate date

Plaintext



$n_{start} = 12,$
$n_{step} = 1,$
$n_{stride} = 6$

Note that:
When the AD is empty, it is padded to a block, so 13-round is applied until the ciphertext outputs.

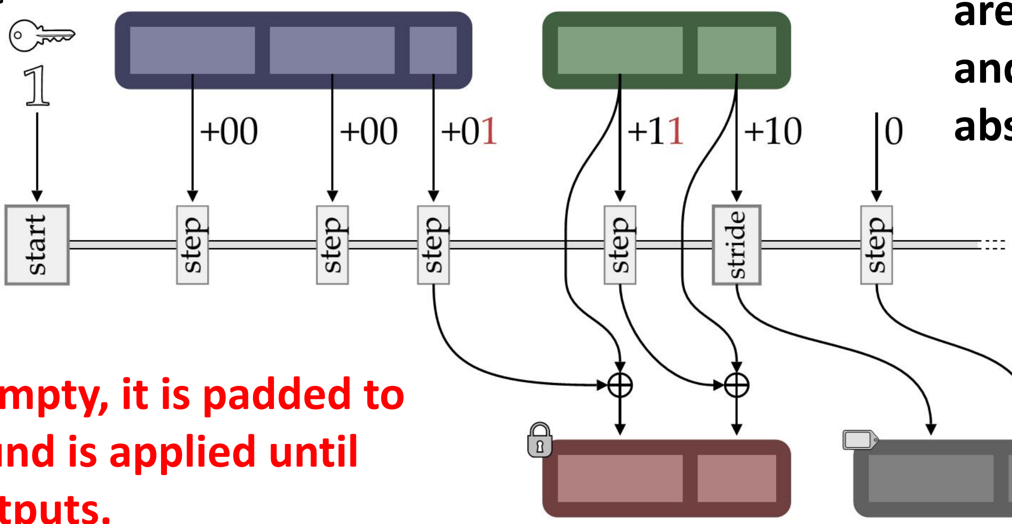
Ciphertext

Finalization: Tag

MonkeyWrap

- an authenticated encryption mode proposed by the Keccak team

1. Initialization
2. Proc. Associate
3. Proc. Plaintext
4. Finalization



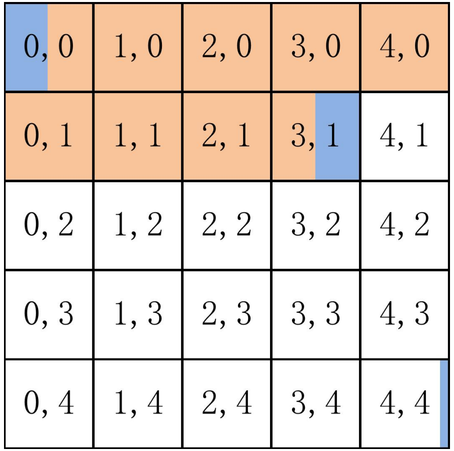
Ciphertext

Finalization: Tag

The AD and Plaintext are divided in to rho-bit and padded, absorbed successively.

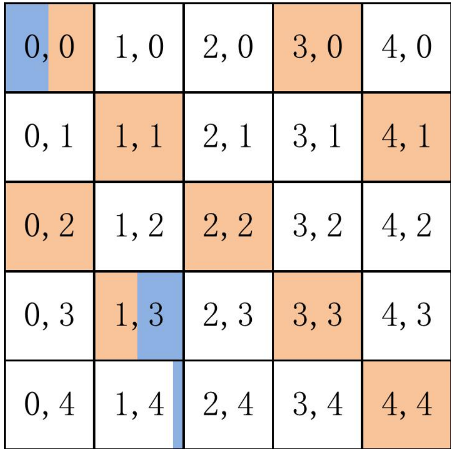
Note that:
When the AD is empty, it is padded to a block, so 13-round is applied until the ciphertext outputs.

Initialization state: Key and Nonce in Ketje Sr v1 and v2



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

Figure. Ketje Sr v1



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

Figure. Ketje Sr v2

- 128-bit key and 254-bit nonce; Pink lanes are key and blue lanes are padding

Summary for ketje

- Using MonkeyWrap
- n_{start} = 12, n_{step} = 1, n_{stride} = 6
- Four instances,

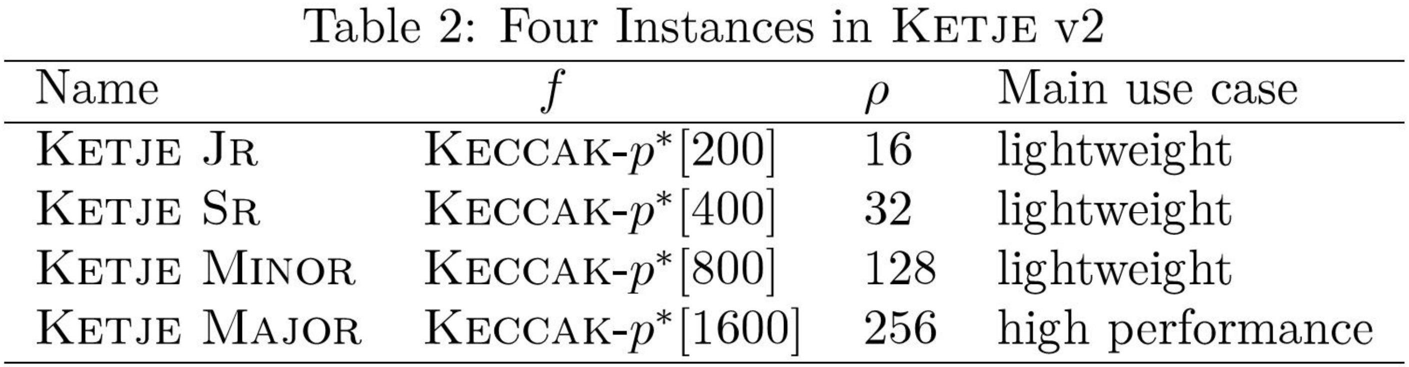


Table 2: Four Instances in Ketje v2

Name	f	ρ	Main use case
Ketje Jr	Keccak-$p^*[200]$	16	lightweight
Ketje Sr	Keccak-$p^*[400]$	32	lightweight
Ketje Minor	Keccak-$p^*[800]$	128	lightweight
Ketje Major	Keccak-$p^*[1600]$	256	high performance

ketje

- Using MonkeyWrap
- $n_{start} = 12$, $n_{step} = 1$, $n_{stride} = 6$
- Four instances,

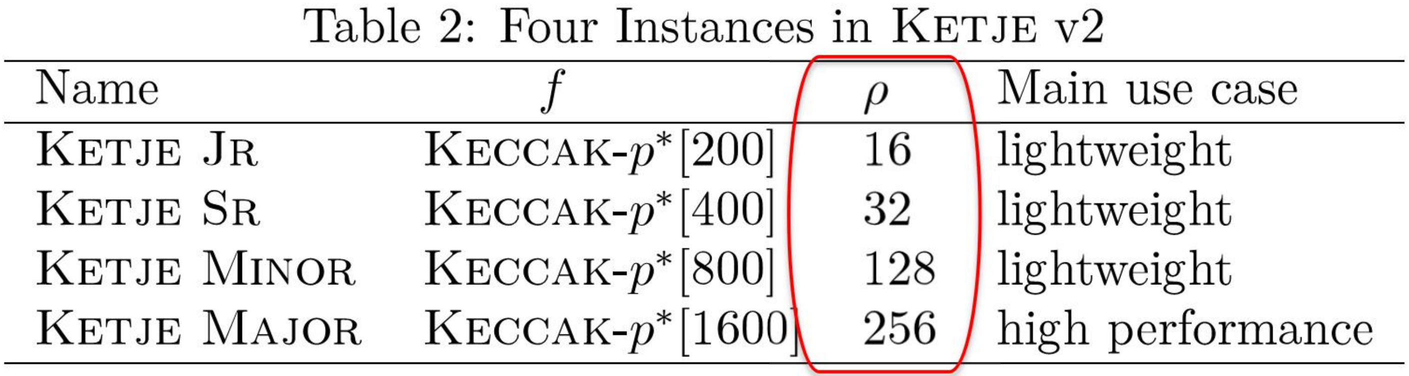


Table 2: Four Instances in Ketje v2

Name	f	ρ	Main use case
Ketje Jr	Keccak-p^*[200]	16	lightweight
Ketje Sr	Keccak-p^*[400]	32	lightweight
Ketje Minor	Keccak-p^*[800]	128	lightweight
Ketje Major	Keccak-p^*[1600]	256	high performance

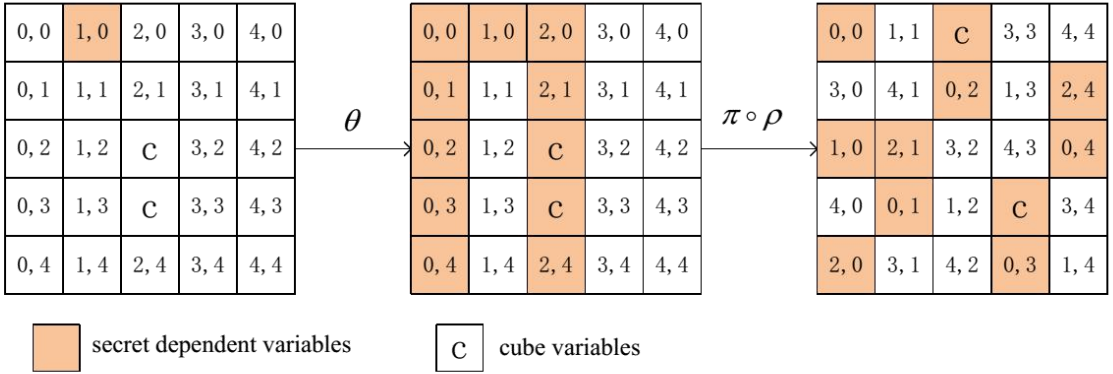
- ρ denotes the block size absorbed in each n_{step}

Related Works

- Cube Attack
  - ✓ proposed by Dinur and Shamir
  - ✓ they write the ANF of output bit: $P = tP_t + Q$, t is maxterm and P_t is superpoly
  - ✓ exploit the linear superpolys
- Dynamic Cube Attack (Dinur and Shamir)
- Cube-like Attack, divide-and-conquer (Dinur *et al.*)
- Conditional Cube Attack (Huang *et al*.)
- Linear Structure

Cube-like Attack (Dinur *et al.*)

- In the 1st round, cube bits are not multiplied together
- In the 1st round, only a part of key bits multiply with cube bits
  - Let k_i be the key bits which do not multiply with cube bits $\{v_1,...,v_{32}\}$
  - degree of round function is 2
  - after 6r, $k_i v_1 v_2 ... v_{32}$ will not appear



0, 0	▨ 1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	c	3, 2	4, 2
0, 3	1, 3	c	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

▨ 0, 0	▨ 1, 0	▨ 2, 0	3, 0	4, 0
▨ 0, 1	1, 1	▨ 2, 1	3, 1	4, 1
▨ 0, 2	1, 2	▨ c	3, 2	4, 2
▨ 0, 3	1, 3	▨ c	3, 3	4, 3
▨ 0, 4	1, 4	▨ 2, 4	3, 4	4, 4

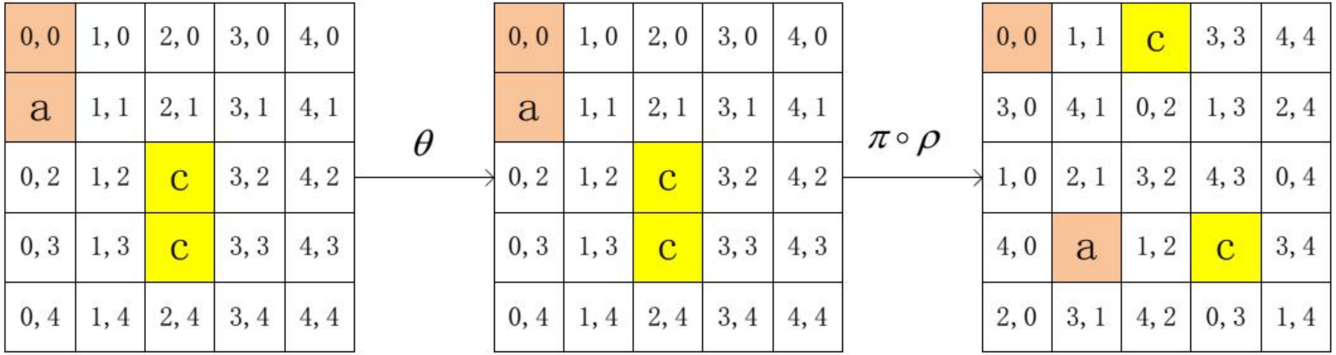
▨ 0, 0	1, 1	▨ c	3, 3	4, 4
3, 0	4, 1	▨ 0, 2	1, 3	▨ 2, 4
▨ 1, 0	▨ 2, 1	3, 2	4, 3	▨ 0, 4
4, 0	▨ 0, 1	1, 2	▨ c	3, 4
▨ 2, 0	3, 1	4, 2	▨ 0, 3	1, 4

▨ secret dependent variables

c cube variables

Auxiliary variables (Dinur *et al.*)

- Auxiliary variables are introduced as follows
- Suppose nonce in A[0,1] is equal to key bits in A[0,0]
- After θ ρ π, the diffusion of the key in A[0,0] is reduced to pink lanes. Thus, key in A[0,0] will not multiply with cube bits.



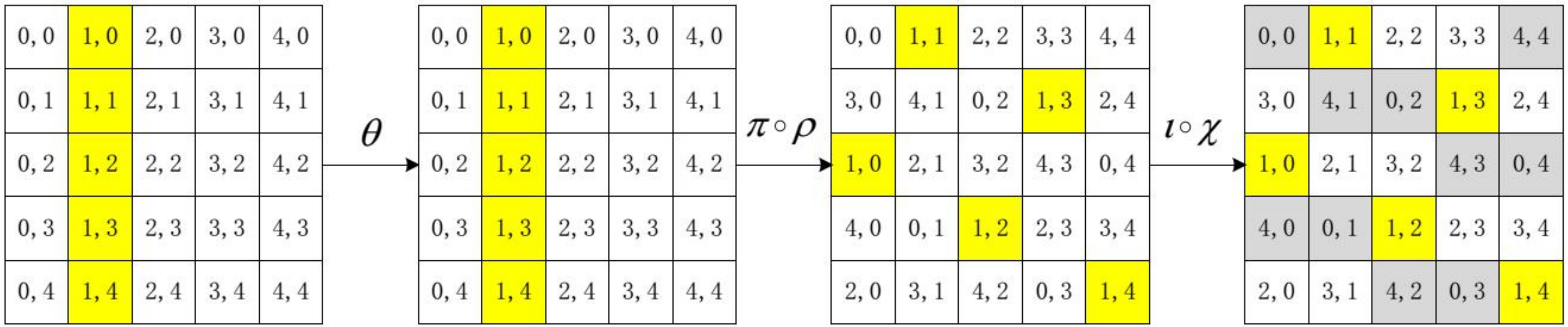
0, 0	1, 0	2, 0	3, 0	4, 0
a	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	c	3, 2	4, 2
0, 3	1, 3	c	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	4, 0
a	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	c	3, 2	4, 2
0, 3	1, 3	c	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	c	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	a	1, 2	c	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

Linear Structure

- Proposed by Guo, Liu and Song at ASIACRYPT 2016
- Find ways to get a set of variables that will not multiply together after the first/second round



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

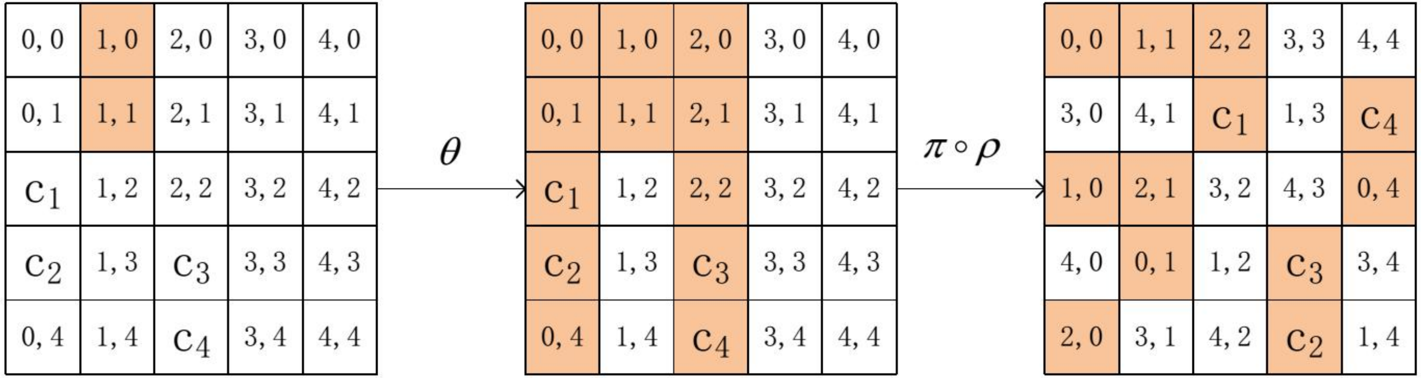
Figure. 1-round Linear Structure

Our Attacks

- Explore the linear structure in small state
- Find 32/64-dimension cubes that do not multiply together in the first round
- The cube do not multiply with as many key bits as possible

Explore the linear structure in small state

- Property 1: In Ketje Sr v1, 32 cube variables do not multiply with 32-bit keys in A[1, 0] and A[1, 1] in the first round, bits of ci are the cube variables and c1+c2 = const1, c3+c4 = const2, const1 and const2 are constants.



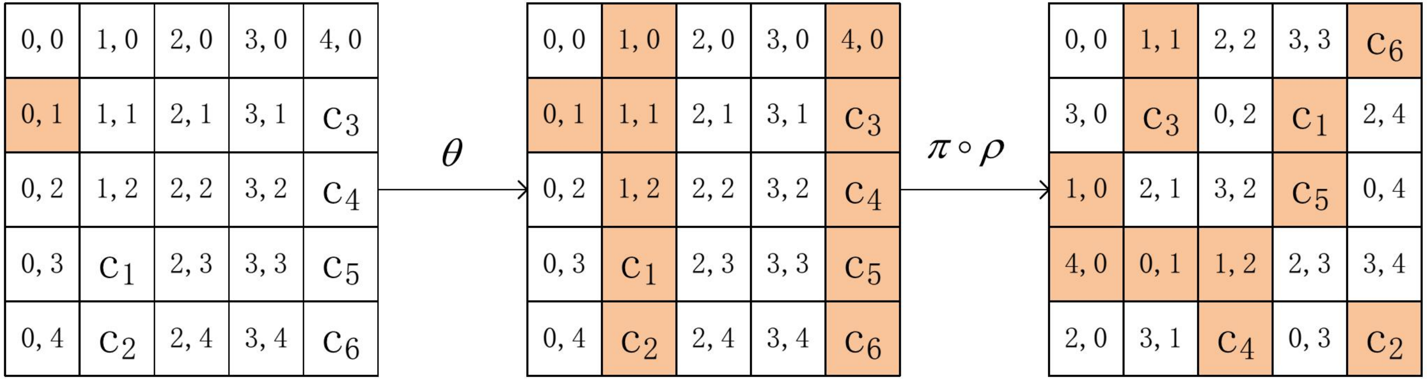
0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
c_1	1, 2	2, 2	3, 2	4, 2
c_2	1, 3	c_3	3, 3	4, 3
0, 4	1, 4	c_4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
c_1	1, 2	2, 2	3, 2	4, 2
c_2	1, 3	c_3	3, 3	4, 3
0, 4	1, 4	c_4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	c_1	1, 3	c_4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	0, 1	1, 2	c_3	3, 4
2, 0	3, 1	4, 2	c_2	1, 4

Explore the linear structure in small state

- Property 2: In Ketje Sr v1, without considering the last 2-bit padding in the nonce3,there are 64 cube variables that do not multiply with 16-bit keys in A[0, 1] in the first round, bits of ciare the cube variables and c1+c2 = const1,c3+c4+c5+c6 =const2, const1and const2 are constants.



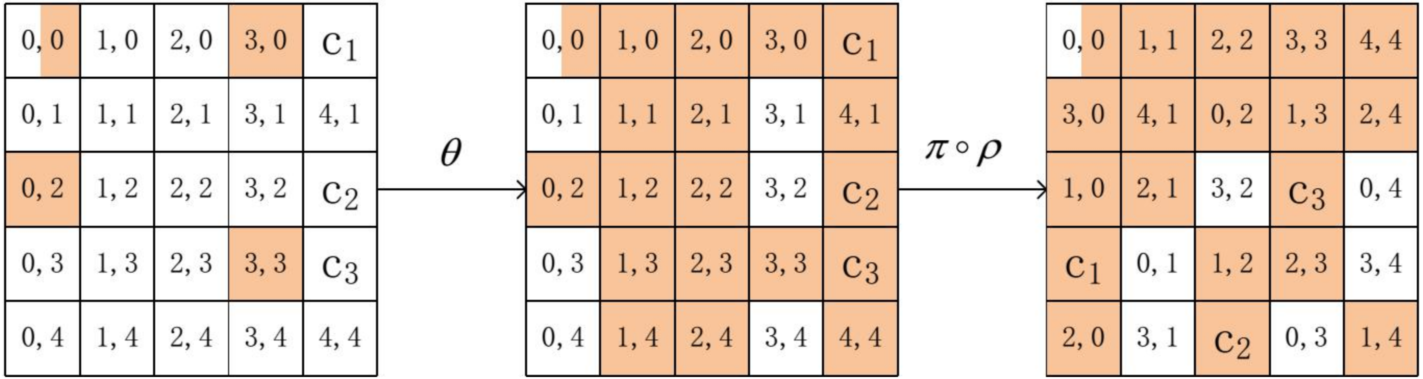
0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	c_3
0, 2	1, 2	2, 2	3, 2	c_4
0, 3	c_1	2, 3	3, 3	c_5
0, 4	c_2	2, 4	3, 4	c_6

0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	c_3
0, 2	1, 2	2, 2	3, 2	c_4
0, 3	c_1	2, 3	3, 3	c_5
0, 4	c_2	2, 4	3, 4	c_6

0, 0	1, 1	2, 2	3, 3	c_6
3, 0	c_3	0, 2	c_1	2, 4
1, 0	2, 1	3, 2	c_5	0, 4
4, 0	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	c_4	0, 3	c_2

Explore the linear structure in small state

- Property 3: In Ketje Sr v2, 32 cube variables do not multiply with 56-bit keys in A[0, 2],A[3, 0], A[3, 3] and half of A[0, 0] in the first round, bits of ci are the cube variables and c1+c2+c3 = const1, const1 is constant.



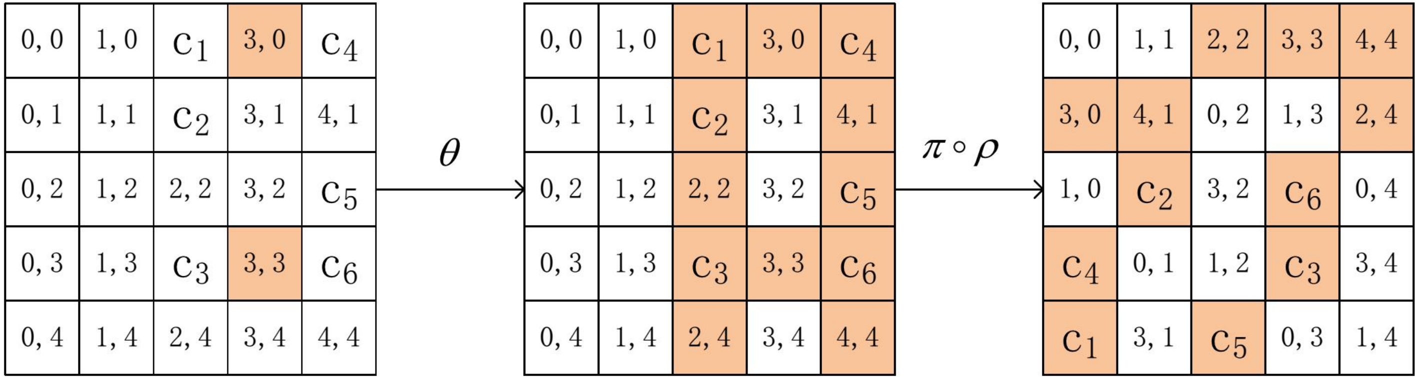
0, 0	1, 0	2, 0	3, 0	c_1
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	c_2
0, 3	1, 3	2, 3	3, 3	c_3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	c_1
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	c_2
0, 3	1, 3	2, 3	3, 3	c_3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	c_3	0, 4
c_1	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	c_2	0, 3	1, 4

Explore the linear structure in small state

- Property 4: In Ketje Sr v2, 64 cube variables do not multiply with 32-bit keys in A[3, 0] and A[3, 3] in the first round, bits of ci are the cube variables and c1+c2+c3 = const1 and c4+c5+c6 = const2, const1and const2 are constants.



0, 0	1, 0	c_1	3, 0	c_4
0, 1	1, 1	c_2	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	c_5
0, 3	1, 3	c_3	3, 3	c_6
0, 4	1, 4	2, 4	3, 4	4, 4

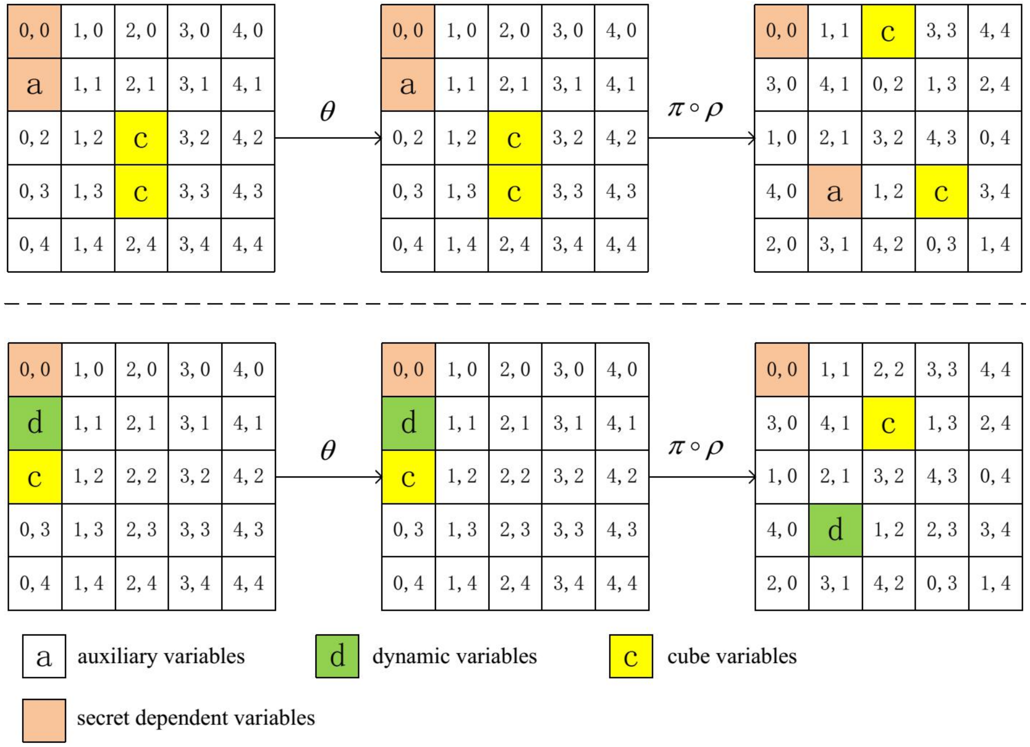
0, 0	1, 0	c_1	3, 0	c_4
0, 1	1, 1	c_2	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	c_5
0, 3	1, 3	c_3	3, 3	c_6
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	c_2	3, 2	c_6	0, 4
c_4	0, 1	1, 2	c_3	3, 4
c_1	3, 1	c_5	0, 3	1, 4

Dynamic cube variables

- Explore the linear structure in small state
- Dynamic cube variables
  - provide the same cube size with few variable lanes

Lower probability to multiply together



0, 0	1, 0	2, 0	3, 0	4, 0
a	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	c	3, 2	4, 2
0, 3	1, 3	c	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	4, 0
a	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	c	3, 2	4, 2
0, 3	1, 3	c	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	c	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	a	1, 2	c	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

0, 0	1, 0	2, 0	3, 0	4, 0
d	1, 1	2, 1	3, 1	4, 1
c	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	4, 0
d	1, 1	2, 1	3, 1	4, 1
c	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	c	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	d	1, 2	2, 3	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

a auxiliary variables

d dynamic variables

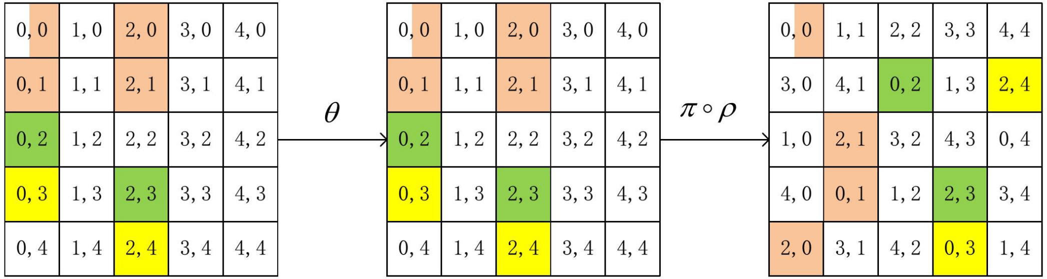
c cube variables

▨ secret dependent variables

6-round Attack on Ketje Sr v1

- A[1,0],A[1,1] will not multiply with cube variable according to Pro 1
- the pink lanes are the key that will not multiply with cube variables under conditions

$$\begin{cases} d_i = v_i \oplus k_{i+8}, i = 0, 1, ..., 7 \\ d_i = v_i \oplus k_{i-8} \oplus k_{i+8}, i = 8, 9, ..., 15 \\ d_i = v_i \oplus k_{i+8} \oplus k_{i+24}, i = 16, 17, ..., 31 \end{cases}$$



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

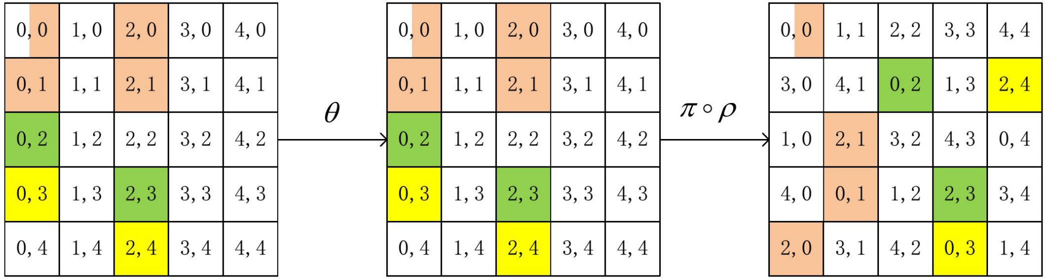
0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

6-round Attack on Ketje Sr v1

- So only 40bits key in A[3,0],A[3,1] and A[4,0] will multiply with cube variables under conditions, hence affect the cube sums after 6-round.

$$\begin{cases} d_i = v_i \oplus k_{i+8}, i = 0, 1, ..., 7 \\ d_i = v_i \oplus k_{i-8} \oplus k_{i+8}, i = 8, 9, ..., 15 \\ d_i = v_i \oplus k_{i+8} \oplus k_{i+24}, i = 16, 17, ..., 31 \end{cases}$$



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

6-round Attack on Ketje Sr v1

Preprocessing Phase:

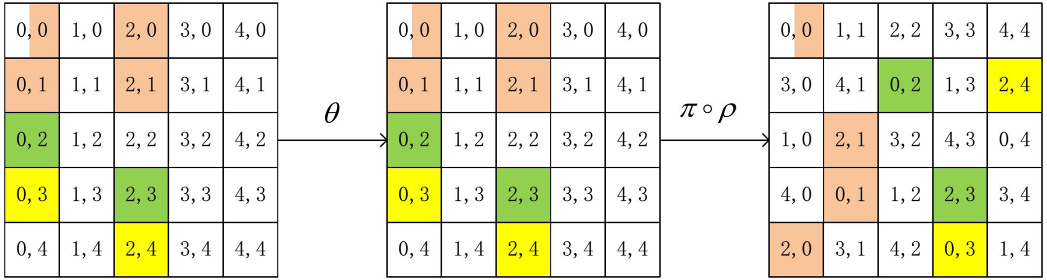
1. Set the $A[0,0,\{0,1,...,7\}] = \{0,1,0,0,1,0,0,0\}$, $A[3,1,\{8,9,...,15\}] = \{1,0,0,0,0,0,0,0\}$ and $A[4,4,\{14,15\}] = \{1,1\}$ to meet the padding rule. Set all other state bits to 0 (except $A[3,0]$, $A[4,0]$, $A[3,1,\{0,1,...,7\}]$, $A[4,1,0]$, 32-bit cube variables and dynamic variables).

2. For the 2^{40} possible values of $(A[3,0], A[4,0], A[3,1,\{0,1,...,7\}])$:

    (a) $A[4,1,0] = 0$, calculate the cube sums after 6 rounds for all the 32 output bits,

    (b) $A[4,1,0] = 1$, calculate the cube sums after 6 rounds for all the 32 output bits,

    (c) Store the two 32-bit cube sums in a sorted list L, next to the value of the corresponding $(A[3,0], A[4,0], A[3,1,\{0,1,...,7\}])$.



0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

$\xrightarrow{\theta}$

0, 0	1, 0	2, 0	3, 0	4, 0
0, 1	1, 1	2, 1	3, 1	4, 1
0, 2	1, 2	2, 2	3, 2	4, 2
0, 3	1, 3	2, 3	3, 3	4, 3
0, 4	1, 4	2, 4	3, 4	4, 4

$\xrightarrow{\pi \circ \rho}$

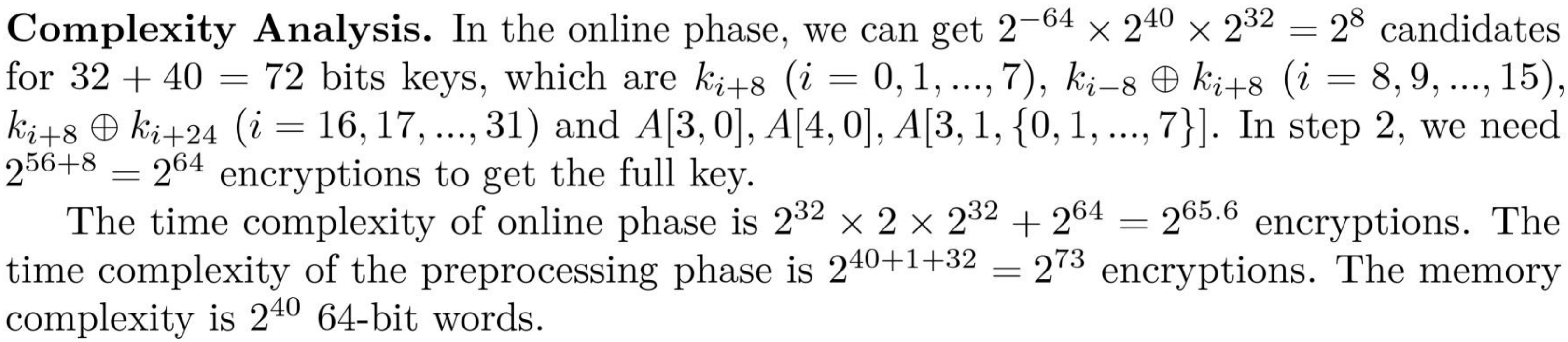
0, 0	1, 1	2, 2	3, 3	4, 4
3, 0	4, 1	0, 2	1, 3	2, 4
1, 0	2, 1	3, 2	4, 3	0, 4
4, 0	0, 1	1, 2	2, 3	3, 4
2, 0	3, 1	4, 2	0, 3	1, 4

6-round Attack on Ketje Sr v1

Online Phase:

1. For each guess of 2^{32} values: k_{i+8} $(i = 0, 1, ..., 7)$, $k_{i-8} \oplus k_{i+8}$ $(i = 8, 9, ..., 15)$ and $k_{i+8} \oplus k_{i+24}$ $(i = 16, 17, ..., 31)$, which are used to compute dynamic variables according to Equation 1:
   (a) $A[4, 1, 0] = 0$, request the outputs of the 2^{32} messages that make up the chosen cube (using the same constant as in the preprocessing phase). Note that according to Equation 1, dynamic variables are computed by the values of cube variables and the guessed keys. Calculate the 32-bit cube sums.
   (b) $A[4, 1, 0] = 1$, request the outputs of the 2^{32} messages that make up the chosen cube (using the same constant as in the preprocessing phase). Calculate the 32-bit cube sums.
   (c) Search cube sums in L.
   (d) For each match in L, retrieve $(A[3, 0], A[4, 0], A[3, 1, \{0, 1, ..., 7\}]\ )$ and store all the candidates combining with 32-bit value of k_{i+8} $(i = 0, 1, ..., 7)$, $k_{i-8} \oplus k_{i+8}$ $(i = 8, 9, ..., 15)$ and $k_{i+8} \oplus k_{i+24}$ $(i = 16, 17, ..., 31)$.
2. For each candidates, guess the remaining unknown $128 - 40 - 32 = 56$ key bits, and use one $(nonce, P, C, T)$ pair to check to get the full 128-bit key.

6-round Attack on Ketje Sr v1



Complexity Analysis. In the online phase, we can get $2^{-64} \times 2^{40} \times 2^{32} = 2^8$ candidates for $32 + 40 = 72$ bits keys, which are k_{i+8} $(i = 0, 1, ..., 7)$, $k_{i-8} \oplus k_{i+8}$ $(i = 8, 9, ..., 15)$, $k_{i+8} \oplus k_{i+24}$ $(i = 16, 17, ..., 31)$ and $A[3, 0]$, $A[4, 0]$, $A[3, 1, \{0, 1, ..., 7\}]$. In step 2, we need $2^{56+8} = 2^{64}$ encryptions to get the full key.

The time complexity of online phase is $2^{32} \times 2 \times 2^{32} + 2^{64} = 2^{65.6}$ encryptions. The time complexity of the preprocessing phase is $2^{40+1+32} = 2^{73}$ encryptions. The memory complexity is 2^{40} 64-bit words.

Other attacks

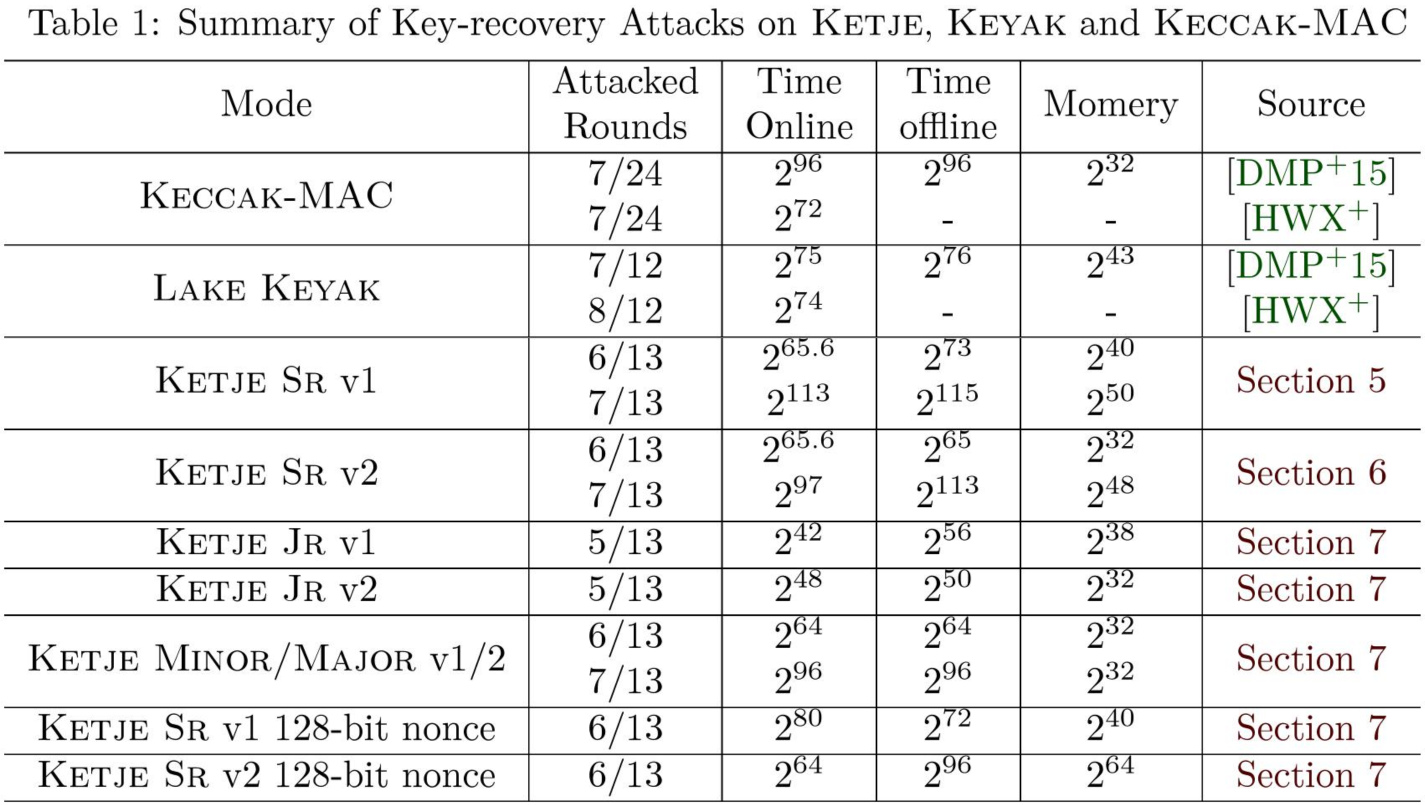


Table 1: Summary of Key-recovery Attacks on Ketje, Keyak and Keccak-MAC

Mode	Attacked Rounds	Time Online	Time offline	Momery	Source
Keccak-MAC	7/24	2^{96}	2^{96}	2^{32}	[DMP+15]
	7/24	2^{72}	-	-	[HWX+]
Lake Keyak	7/12	2^{75}	2^{76}	2^{43}	[DMP+15]
	8/12	2^{74}	-	-	[HWX+]
Ketje Sr v1	6/13	$2^{65.6}$	2^{73}	2^{40}	Section 5
	7/13	2^{113}	2^{115}	2^{50}	
Ketje Sr v2	6/13	$2^{65.6}$	2^{65}	2^{32}	Section 6
	7/13	2^{97}	2^{113}	2^{48}	
Ketje Jr v1	5/13	2^{42}	2^{56}	2^{38}	Section 7
Ketje Jr v2	5/13	2^{48}	2^{50}	2^{32}	Section 7
Ketje Minor/Major v1/2	6/13	2^{64}	2^{64}	2^{32}	Section 7
	7/13	2^{96}	2^{96}	2^{32}	
Ketje Sr v1 128-bit nonce	6/13	2^{80}	2^{72}	2^{40}	Section 7
Ketje Sr v2 128-bit nonce	6/13	2^{64}	2^{96}	2^{64}	Section 7

Thank you

Q?