Experimental MitM Preimage Attacks on KECCAK and ASCON-XOF

December 12, 2024

1 Experimental MitM Preimage Attacks on 3-round ASCON-XOF

Based on the 3-round MitM characteristic on ASCON-XOF as shown in Figure 1, we deploy a conditional pseudo-preimage attack on 32-bit partial target to verify the correctness of our method. The 48 bit conditions on the inner part are given in Table 1. In Figure 1, the starting state $A^{(0)}$ contains 14 ■ and 24 ■, *i.e.*, $\lambda_{\mathcal{B}} = 14$ and $\lambda_{\mathcal{R}} = 24$. And there are 10 bit cancellations ($\sigma = 10$) imposed on ■, involving six linear cancellations ($s = 6$). In the practical attack, we omit the round constants and the linear layer p_L in the last round for simplicity. That is, we regard $S^{(2)}_{\{*,0\}}$ as the hash value, and there exist 14 bit matching points. We give one matching equation for example, which is

$$A^{(3)}_{\{2,1\}} \cdot (A^{(3)}_{\{2,4\}} + A^{(3)}_{\{2,2\}} + A^{(3)}_{\{2,0\}}) + A^{(3)}_{\{2,3\}} + A^{(3)}_{\{2,2\}} + A^{(3)}_{\{2,1\}} + A^{(3)}_{\{2,0\}} = S^{(3)}_{\{2,0\}}. \quad (1)$$

The attack procedure is listed in Algorithm 1. In our experiment, together with the 14 bit matching points, another 18 bits of $S^{(2)}_{\{x,0\}}$ ($x \in \{0, 1, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 18, 19, 20, 21, 22, 23\}$) are selected to form a 32-bit target. Without loss of generality, let the specified 32-bit partial target be all-zero. For the inner part, we simply fixed the value to satisfy the predefined bit conditions, *i.e.*, $A^{(0)}_{\{*,2\}} = A^{(0)}_{\{*,4\}} = 0x0$, $A^{(0)}_{\{*,1\}} = 0xc8142340c8142340$ and $A^{(0)}_{\{*,3\}} = 0x8713427087134270$. The ■ bits in $A^{(0)}_{\{*,0\}}$ are also fixed to zeros. We get the $s = 6$ linear cancellations as Equation 2, where

$$\begin{cases} A^{(0)}_{\{25,0\}} \oplus A^{(0)}_{\{27,0\}} \oplus A^{(0)}_{\{38,0\}} \oplus A^{(0)}_{\{47,0\}} \oplus A^{(0)}_{\{50,0\}} = c_0, \\ A^{(0)}_{\{15,0\}} \oplus A^{(0)}_{\{60,0\}} = c_1, \\ A^{(0)}_{\{0,0\}} \oplus A^{(0)}_{\{61,0\}} = c_2, \\ A^{(0)}_{\{6,0\}} \oplus A^{(0)}_{\{15,0\}} \oplus A^{(0)}_{\{18,0\}} \oplus A^{(0)}_{\{57,0\}} \oplus A^{(0)}_{\{59,0\}} = c_3, \\ A^{(0)}_{\{28,0\}} \oplus A^{(0)}_{\{47,0\}} = c_4, \\ A^{(0)}_{\{29,0\}} \oplus A^{(0)}_{\{32,0\}} = c_5. \end{cases} \quad (2)$$

$A^{(0)}_{\{7,1\}} = 0,\ A^{(0)}_{\{17,1\}} = 0,\ A^{(0)}_{\{26,1\}} = 0,\ A^{(0)}_{\{39,1\}} = 0,\ A^{(0)}_{\{49,1\}} = 0,\ A^{(0)}_{\{58,1\}} = 0;$
$A^{(0)}_{\{0,1\}} = 1,\ A^{(0)}_{\{1,1\}} = 1,\ A^{(0)}_{\{4,1\}} = 1,\ A^{(0)}_{\{11,1\}} = 1,\ A^{(0)}_{\{13,1\}} = 1, A^{(0)}_{\{18,1\}} = 1,\ A^{(0)}_{\{22,1\}} = 1,$
$A^{(0)}_{\{23,1\}} = 1,\ A^{(0)}_{\{25,1\}} = 1,\ A^{(0)}_{\{32,1\}} = 1,\ A^{(0)}_{\{33,1\}} = 1,\ A^{(0)}_{\{36,1\}} = 1,\ A^{(0)}_{\{43,1\}} = 1,\ A^{(0)}_{\{45,1\}} = 1,$
$A^{(0)}_{\{50,1\}} = 1,\ A^{(0)}_{\{54,1\}} = 1,\ A^{(0)}_{\{55,1\}} = 1,\ A^{(0)}_{\{57,1\}} = 1;$
$A^{(0)}_{\{0,3\}} \oplus A^{(0)}_{\{0,4\}} = 1,\ A^{(0)}_{\{5,3\}} \oplus A^{(0)}_{\{5,4\}} = 1,\ A^{(0)}_{\{6,3\}} \oplus A^{(0)}_{\{6,4\}} = 1,\ A^{(0)}_{\{7,3\}} \oplus A^{(0)}_{\{7,4\}} = 1,$
$A^{(0)}_{\{11,3\}} \oplus A^{(0)}_{\{11,4\}} = 1,\ A^{(0)}_{\{14,3\}} \oplus A^{(0)}_{\{14,4\}} = 1,\ A^{(0)}_{\{15,3\}} \oplus A^{(0)}_{\{15,4\}} = 1,\ A^{(0)}_{\{17,3\}} \oplus A^{(0)}_{\{17,4\}} = 1,$
$A^{(0)}_{\{22,3\}} \oplus A^{(0)}_{\{22,4\}} = 1,\ A^{(0)}_{\{25,3\}} \oplus A^{(0)}_{\{25,4\}} = 1,\ A^{(0)}_{\{26,3\}} \oplus A^{(0)}_{\{26,4\}} = 1,\ A^{(0)}_{\{27,3\}} \oplus A^{(0)}_{\{27,4\}} = 1;$
$A^{(0)}_{\{32,3\}} \oplus A^{(0)}_{\{32,4\}} = 1,\ A^{(0)}_{\{37,3\}} \oplus A^{(0)}_{\{37,4\}} = 1,\ A^{(0)}_{\{38,3\}} \oplus A^{(0)}_{\{38,4\}} = 1,\ A^{(0)}_{\{39,3\}} \oplus A^{(0)}_{\{39,4\}} = 1,$
$A^{(0)}_{\{43,3\}} \oplus A^{(0)}_{\{43,4\}} = 1,\ A^{(0)}_{\{46,3\}} \oplus A^{(0)}_{\{46,4\}} = 1,\ A^{(0)}_{\{47,3\}} \oplus A^{(0)}_{\{47,4\}} = 1,\ A^{(0)}_{\{49,3\}} \oplus A^{(0)}_{\{49,4\}} = 1,$
$A^{(0)}_{\{54,3\}} \oplus A^{(0)}_{\{54,4\}} = 1,\ A^{(0)}_{\{57,3\}} \oplus A^{(0)}_{\{57,4\}} = 1,\ A^{(0)}_{\{58,3\}} \oplus A^{(0)}_{\{58,4\}} = 1,\ A^{(0)}_{\{59,3\}} \oplus A^{(0)}_{\{59,4\}} = 1;$

Table 1: 48-bit Conditions in 3-round Experiment on `Ascon-XOF`

After the diagonalization, we get Equation 3 as

$$\begin{cases} A^{(0)}_{\{25,0\}} = A^{(0)}_{\{27,0\}} \oplus A^{(0)}_{\{38,0\}} \oplus A^{(0)}_{\{47,0\}} \oplus A^{(0)}_{\{50,0\}} \oplus c_0, \\ A^{(0)}_{\{60,0\}} = A^{(0)}_{\{15,0\}} \oplus c_1, \\ A^{(0)}_{\{0,0\}} = A^{(0)}_{\{61,0\}} \oplus c_2, \\ A^{(0)}_{\{6,0\}} = A^{(0)}_{\{15,0\}} \oplus A^{(0)}_{\{18,0\}} \oplus A^{(0)}_{\{57,0\}} \oplus A^{(0)}_{\{59,0\}} \oplus c_3, \\ A^{(0)}_{\{28,0\}} = A^{(0)}_{\{47,0\}} \oplus c_4, \\ A^{(0)}_{\{29,0\}} = A^{(0)}_{\{32,0\}} \oplus c_5. \end{cases} \tag{3}$$

Since each MitM episode produce 2^{14} preimages satisfying the 14 bit matching points, we need to repeat 2^4 MitM episodes to satisfying other fixed 18 bit zeros. The theoretical time is about 2^{18}, while the exhaustive search time is 2^{32}. The memory complexity is 2^{18}. On a platform of Interl I9 CPU with 32 GB memory, the program to find a partial target preimage can be done in seconds. We choose different $\bar{Y}_{\mathcal{R}}$ to get some examples, listed in Table 2.

2 Experimental MitM Preimage Attacks on Small-Scale Keccak

We choose Keccak$[r = 40, c = 160]$ to conduct a small-scale experiment as a proof, which is a challenge version in the Keccak Crunchy contest. It has a 200-bit state and outputs a 80-bit digest. We build an MILP model for Keccak$[r = 40, c = 160]$, following the strategies in our paper. The model is constructed form $A^{(0)}$ since the CP-kernel property can not be used in the first round. The matching process is also a little different. Suppose the first 80 bits of $A^{(r+1)}$ are the hash value, *i.e.*, $A^{(r+1)}_{\{x,0,z\}}$ and $A^{(r+1)}_{\{x,0,z\}}$, where $0 \le x \le 4, 0 \le z \le 7$. Applying the χ^{-1}, we can deduce $\pi^{(r)}_{\{x,0,z\}}$ and $\pi^{(r)}_{\{x,1,z\}}$. Then applying the

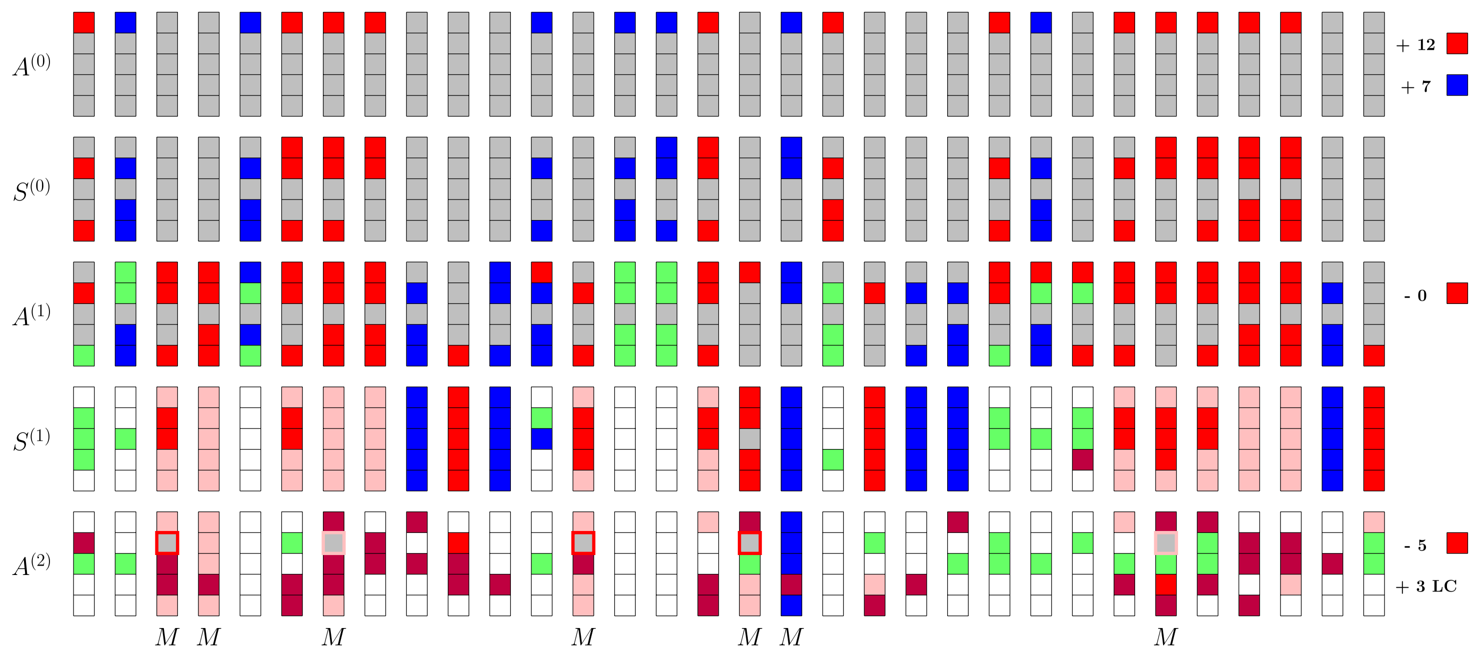

Figure 1: The 3-round MitM attack on Ascon-Xof

Algorithm 1: Experiments Preimage Attack on 3-round Ascon-Xof with 32-bit Partial Target

Fix the 14 bit matching points and another 18 bits as zeros, *i.e.*, $S^{(2)}_{\{x,0\}} = 0$, $(x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 26, 34, 35, 38, 44, 48, 49, 58\})$
Set the 256 bits of inner part of $A^{(0)}$ as fixed values, which satisfy the 48 conditions in Table 1
Set the ■ bits in $A^{(0)}_{\{*,0\}}$ as zeros
for *1 value of* $\bar{Y}_{\mathcal{R}} \in \mathbb{F}_2^6$ **do**
    Set the 6 linear cancellation constraints on 24 ■ as $\bar{Y}_{\mathcal{R}}$, and fix the ■ in $A^{(0)}$ as zero, *i.e.,* Equation 2. Then diagonalizethe equations system to Equation 3.
    for 2^{18} *values of the* ■ *bits* $A^{(0)}_{\{x,0\}}$, *(*$x \in \{5, 7, 15, 18, 22$ $26, 27, 32, 37, 38, 39, 47, 50, 54, 57, 58, 59, 61\}$*)* **do**
        Deduce $A^{(0)}_{\{x,0\}}$ $(x \in \{0, 6, 25, 28, 29, 60\})$, and compute forward to determine 4-bit ■/■ bits (denoted as $\tilde{Y}_{\mathcal{R}} \in \mathbb{F}_2^4$), and the 14-bit matching point. Build the table U and store the 24-bit ■ bits $v_{\mathcal{R}}$ of $A^{(0)}$ as well as the 14-bit matching point in $U[\tilde{Y}_{\mathcal{R}}]$.
    end
    for $\tilde{Y}_{\mathcal{R}} \in \mathbb{F}_2^4$ **do**
        Retrieve the 2^{14} elements of $U[\tilde{Y}_{\mathcal{R}}]$ and restore $v_{\mathcal{R}}$ in L_1 under the index of 14-bit matching point
        for 2^{14} *values of* ■ *bits* $v_{\mathcal{B}}$ **do**
            Compute to the 14-bit matching point and check against L_1 to retrieve combination $(X_{\mathcal{R}}, X_{\mathcal{B}}, X_{\mathcal{G}})$
            if $(X_{\mathcal{R}}, X_{\mathcal{B}}, X_{\mathcal{G}})$ *leads to the 18 bit zeros in* $S^{(2)}_{\{x,0\}}$ *(* $x \in \{0, 1, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 18, 19, 20, 21, 22, 23\}$*)* **then**
                Output the preimage
            end
        end
    end
end

Round	First row of preimage $\left(A^{(0)}_{\{*,0\}}\right)$	First 64-bit Target
$r=3$	431722384f120332	000000140c203989
	4107605046010126	000000d809a1205b
	481541108e06036e	00000048c9802f98
	411021000d11611a	000000c609d2285e
	430723684a13201e	00000138df537dd
	031200584a06237a	0000008b05461cdb
	4917633c8e112156	000000448c27138f
	411203288513606e	0000008a0da10a18
	08132108ca03407e	000000038c561852
	0b0563504d062302	000000805173d0e

Table 2: 32-bit Partial Target Preimage Examples of 3-round Ascon-Xof

inverse of ρ and π to $\pi^{(r)}_{\{x,0,z\}}$ and $\pi^{(r)}_{\{x,1,z\}}$, we can deduce the following equations due to the CP-kernel property:

$$\begin{cases} A^{(r)}_{\{0,0,z\}} + A^{(r)}_{\{0,2,z\}} = \pi^{(r)}_{\{0,0,z+\gamma[0,0]\}} + \pi^{(r)}_{\{2,1,z+\gamma[0,2]\}}, \\ A^{(r)}_{\{1,1,z\}} + A^{(r)}_{\{1,3,z\}} = \pi^{(r)}_{\{1,0,z+\gamma[1,1]\}} + \pi^{(r)}_{\{3,1,z+\gamma[1,3]\}}, \\ A^{(r)}_{\{2,2,z\}} + A^{(r)}_{\{2,4,z\}} = \pi^{(r)}_{\{2,0,z+\gamma[2,2]\}} + \pi^{(r)}_{\{4,1,z+\gamma[2,4]\}}, \\ A^{(r)}_{\{3,3,z\}} + A^{(r)}_{\{3,0,z\}} = \pi^{(r)}_{\{3,0,z+\gamma[3,3]\}} + \pi^{(r)}_{\{0,1,z+\gamma[3,0]\}}, \\ A^{(r)}_{\{4,4,z\}} + A^{(r)}_{\{4,1,z\}} = \pi^{(r)}_{\{4,0,z+\gamma[4,4]\}} + \pi^{(r)}_{\{1,1,z+\gamma[4,1]\}}, \end{cases} \tag{4}$$

where $0 \leq z \leq 7$.

We find a 3-round MitM preimage characteristic in Fig. 2, where $\lambda_{\mathcal{R}} = 23$, $\lambda_{\mathcal{B}} = 3$ and $\lambda_m = 3$. The 3 matching equations are given in Equation 5, where

$$\begin{cases} A^{(0)}_{\{0,0,7\}} \oplus A^{(0)}_{\{0,2,7\}} = \pi^{(2)}_{\{0,0,7\}} \oplus \pi^{(2)}_{\{2,1,2\}}, \\ A^{(0)}_{\{1,1,3\}} \oplus A^{(0)}_{\{1,3,3\}} = \pi^{(2)}_{\{1,0,7\}} \oplus \pi^{(2)}_{\{3,1,0\}}, \\ A^{(0)}_{\{2,2,1\}} \oplus A^{(0)}_{\{2,4,1\}} = \pi^{(2)}_{\{2,0,4\}} \oplus \pi^{(2)}_{\{4,1,6\}}. \end{cases} \tag{5}$$

There are $\sigma = 20$ cancellations of ■ bits, involving $s = 8$ linear cancellations, which are listed in Equation 6.

$$\begin{cases} A^{(0)}_{\{0,0,0\}} \oplus A^{(0)}_{\{2,0,7\}} = c_0, \\ A^{(0)}_{\{1,0,0\}} \oplus A^{(0)}_{\{3,0,7\}} = c_1, \\ A^{(0)}_{\{3,0,0\}} \oplus A^{(0)}_{\{0,0,7\}} = c_2, \\ A^{(0)}_{\{0,0,2\}} \oplus A^{(0)}_{\{2,0,1\}} = c_3, \\ A^{(0)}_{\{2,0,2\}} \oplus A^{(0)}_{\{4,0,1\}} = c_4, \\ A^{(0)}_{\{2,0,1\}} \oplus A^{(0)}_{\{1,0,1\}} \oplus A^{(0)}_{\{3,0,0\}} = c_5, \\ A^{(0)}_{\{3,0,6\}} \oplus A^{(0)}_{\{2,0,6\}} \oplus A^{(0)}_{\{4,0,5\}} = c_6, \\ A^{(0)}_{\{1,0,7\}} \oplus A^{(0)}_{\{0,0,7\}} \oplus A^{(0)}_{\{2,0,6\}} = c_7. \end{cases} \tag{6}$$

After the diagonalization, we get Equation 7 as

$$\begin{cases} A^{(0)}_{\{2,0,7\}} = A^{(0)}_{\{0,0,0\}} \oplus c_0, \\ A^{(0)}_{\{3,0,7\}} = A^{(0)}_{\{1,0,0\}} \oplus c_1, \\ A^{(0)}_{\{0,0,7\}} = A^{(0)}_{\{3,0,0\}} \oplus c_2, \\ A^{(0)}_{\{2,0,1\}} = A^{(0)}_{\{0,0,2\}} \oplus c_3, \\ A^{(0)}_{\{4,0,1\}} = A^{(0)}_{\{2,0,2\}} \oplus c_4, \\ A^{(0)}_{\{1,0,1\}} = A^{(0)}_{\{3,0,0\}} \oplus A^{(0)}_{\{0,0,2\}} \oplus c_3 \oplus c_5, \\ A^{(0)}_{\{4,0,5\}} = A^{(0)}_{\{3,0,6\}} \oplus A^{(0)}_{\{2,0,6\}} \oplus c_6, \\ A^{(0)}_{\{1,0,7\}} = A^{(0)}_{\{2,0,6\}} \oplus A^{(0)}_{\{3,0,0\}} \oplus c_2 \oplus c_7. \end{cases} \tag{7}$$

The attack procedure is listed in Algorithm 2. In our experiment, we omit the round constants addition. We also omit the χ layer in the last round, regarding $\pi^{(2)}$ as the hash value. To find the preimage with a 24-bit partial target, we fix the six bits $\pi^{(2)}$ in Equation 5, and another 18 bits $\pi^{(2)}$ to zeros, which are listed in Table 3. In the initial state, all gray bits are set to be zero. By traversing 15 active ■ bits, the other 8 ■ bits can be deduced according to Equation 7. The memory cost is 2^{15}, which is in comparable of the naive table-based method with 2^{23} memory complexity. Since each MitM episode produce 2^3 preimages satisfying the 3 bit matching points, we need to repeat 2^{18} MitM episodes to satisfying all fixed 24 bit zeros. The theoretical time is about 2^{21}. On a platform of Interl I9 CPU with 32 GB memory, the program to find the partial target preimage can be done in seconds. We choose different $\bar{Y}_{\mathcal{R}}$ and the results are listed in Table 4.

$\pi^{(2)}_{\{0,0,4\}}$,	$\pi^{(2)}_{\{0,0,5\}}$,	$\pi^{(2)}_{\{0,0,6\}}$,	$\pi^{(2)}_{\{0,0,7\}}$,	$\pi^{(2)}_{\{1,0,4\}}$,	$\pi^{(2)}_{\{1,0,5\}}$,	$\pi^{(2)}_{\{1,0,6\}}$,	$\pi^{(2)}_{\{1,0,7\}}$,
$\pi^{(2)}_{\{2,1,0\}}$,	$\pi^{(2)}_{\{2,1,1\}}$,	$\pi^{(2)}_{\{2,1,2\}}$,	$\pi^{(2)}_{\{2,1,3\}}$,	$\pi^{(2)}_{\{2,0,4\}}$,	$\pi^{(2)}_{\{2,0,5\}}$,	$\pi^{(2)}_{\{2,0,6\}}$,	$\pi^{(2)}_{\{2,0,7\}}$,
$\pi^{(2)}_{\{3,1,0\}}$,	$\pi^{(2)}_{\{3,1,1\}}$,	$\pi^{(2)}_{\{3,1,2\}}$,	$\pi^{(2)}_{\{3,1,3\}}$,	$\pi^{(2)}_{\{4,1,4\}}$,	$\pi^{(2)}_{\{4,1,5\}}$,	$\pi^{(2)}_{\{4,1,6\}}$,	$\pi^{(2)}_{\{4,1,7\}}$

Table 3: The 24 Bits Selected for Partial Target Preimge in Keccak

3 The Constraints for the χ Operation of Keccak

The χ operation maps $(a_0, a_1, a_2, a_3, a_4)$ to $(b_0, b_1, b_2, b_3, b_4)$, where $b_i = a_i \oplus (a_{i+1} \oplus 1) \cdot a_{i+2}$. We list the linear inequalities restricting the valid coloring patterns of $(a_i, a_{i+1}, a_{i+2}, b_i)$ in Equation 8, which are generated using the convex hull computation. Denote the bit representation of $(a_i, a_{i+1}, a_{i+2}, b_i)$ as $(\omega^1_0, \omega^1_1, \omega^1_2, \omega^2_0, \omega^2_1, \omega^2_2, \omega^3_0, \omega^3_1, \omega^3_2, \omega^O_0, \omega^O_1, \omega^O_2)$, and all the 28 linear inequalities

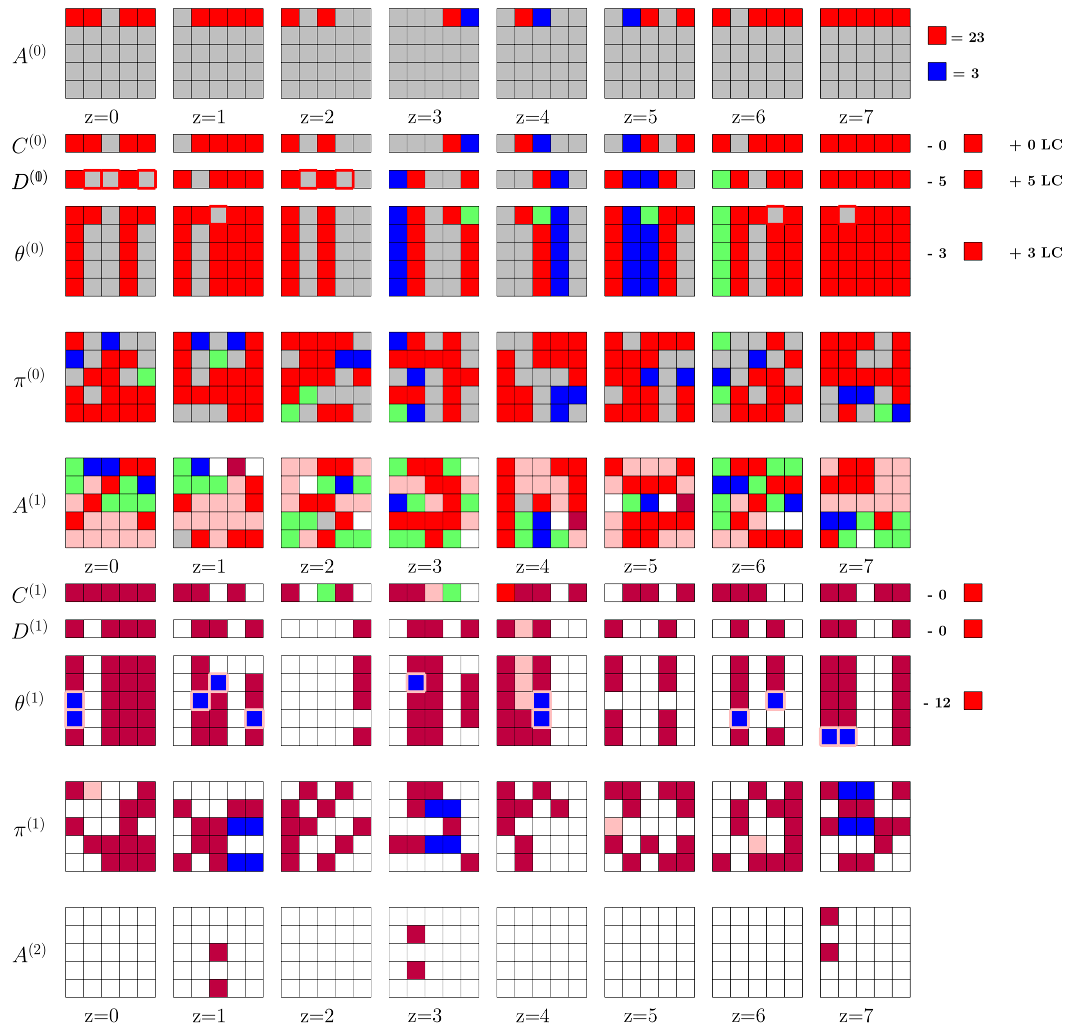

Figure 2: The 3-round MitM preimage attack on KECCAK$[r = 40, c = 160]$

Algorithm 2: Preimage Attack on 3-round KECCAK$[r = 40, c = 160]$

Set the 24 bits $\pi^{(2)}$ in Table 3 to zeros, and derive the 3 matching equations as Equation 5

Set $\blacksquare$ bits of $\mathrm{A}^{(0)}$ to zeros

for 2^6 *values of* $\bar{Y}_{\mathcal{R}} \in \mathbb{F}_2^{16}$ **do**

    Set the 8 linear cancellation constraints on 23 $\blacksquare$ as $\bar{Y}_{\mathcal{R}}$, and fix the $\blacksquare$ in $A^{(0)}$ as zero, *i.e.,* Equation 6. Then diagonalizethe equations system to Equation 7.

    for 2^{15} *values of the* $\blacksquare$ *bits* **do**

        Deduce the other 8 $\blacksquare$ bits as Equation 7, and compute forward to determine 12-bit value $\tilde{Y}_{\mathcal{R}} \in \mathbb{F}_2^{12}$ marked by $\blacksquare$/$\blacksquare$ bits, and the 3-bit matching point. Build the table U and store the 23-bit $\blacksquare$ bits of $A^{(0)}$ as well as the 3-bit matching point in $U[\tilde{Y}_{\mathcal{R}}]$.

    end

    for $\tilde{Y}_{\mathcal{R}} \in \mathbb{F}_2^{12}$ **do**

        for 2^3 *values in* $U[\tilde{Y}_{\mathcal{R}}]$ **do**

            Restore the values of $\blacksquare$ of $A^{(0)}$ and the corresponding matching point in a list L_1 (indexed by matching point)

        end

        for 2^3 *values of* $\blacksquare$ **do**

            Compute the matching point and check against L_1 to retrieve combination $(X_{\mathcal{R}}, X_{\mathcal{B}}, X_{\mathcal{G}})$

            if $(X_{\mathcal{R}}, X_{\mathcal{B}}, X_{\mathcal{G}})$ *leads to the 24 bits zeros* $\pi^{(2)}$ *in Table 3* **then**

                Output the preimage

            end

        end

    end

end

Round	First plane of $\left(A^{(0)}_{\{*,0,*\}}\right)$	80 bits Hash value $\left(\pi^{(2)}_{\{*,0,*\}},\ \pi^{(2)}_{\{*,1,*\}}\right)$
$r = 3$	83, c1, 65, 81, 10	60, f0, f0, e3, 82 4a, 1a, 02, 06, 40
	83, 01, 62, 43, c1	c0, 90, 10, 34, ee 34, c8, 04, 00, 20
	23, 01, 0a, 93, 17	20, 50, b0, f9, 0c 73, cc, 0e, 04, 00
	81, 09, 4c, 83, 94	b0, c0, b0, 21, b0 dc, e3, 04, 00, 30

Table 4: 24-bit Partial Target Preimage Examples of 3-round Keccak[$r = 40, c = 160$]

are

$$
\begin{cases}
\omega_1^1+\omega_2^1-\omega_0^2+\omega_1^2-\omega_0^3+\omega_1^3-\omega_1^O-3\omega_2^O\geq -2,\\
-\omega_2^2-\omega_2^3-2\omega_1^O+\omega_2^O\geq -2,\\
\omega_1^1+\omega_2^1+\omega_1^2+\omega_2^2+\omega_1^3+\omega_2^3-\omega_1^O-3\omega_2^O\geq 0,\\
\omega_1^1+\omega_2^1-2\omega_0^2-\omega_2^2-2\omega_0^3-\omega_2^3+2\omega_0^O-\omega_1^O-5\omega_2^O\geq -6,\\
-2\omega_1^1-\omega_1^2+\omega_2^2-\omega_1^3+\omega_2^3+2\omega_1^O-\omega_2^O\geq -3,\\
5\omega_0^1-\omega_1^1-\omega_2^1+4\omega_0^2-2\omega_2^2+2\omega_0^3-\omega_1^3-\omega_2^3-5\omega_0^O+\omega_1^O+2\omega_2^O\geq -4,\\
-\omega_2^1+\omega_0^2-\omega_1^2+\omega_2^2-\omega_2^3-\omega_1^O+2\omega_2^O\geq -2,\\
-\omega_2^1-\omega_2^2+\omega_0^3-\omega_1^3+\omega_2^3-\omega_1^O+2\omega_2^O\geq -2,\\
-\omega_2^1-\omega_1^2+\omega_2^2-\omega_1^3+\omega_2^3+\omega_2^O\geq -2,\\
-\omega_2^1+\omega_0^2-\omega_2^2+\omega_0^3-\omega_2^3-\omega_0^O-\omega_1^O+2\omega_2^O\geq -2,\\
-\omega_1^1-\omega_2^2+\omega_0^3-\omega_1^3+\omega_2^3+\omega_2^O\geq -2,\\
-\omega_1^1+\omega_0^2-\omega_1^2+\omega_2^2-\omega_2^3+\omega_2^O\geq -2,\\
-\omega_1^1+\omega_0^2-\omega_2^2+\omega_0^3-\omega_2^3-\omega_1^O+\omega_2^O\geq -2,\\
-\omega_0^2-\omega_2^3-\omega_2^O\geq -2,\\
-\omega_2^2-\omega_0^3-\omega_2^O\geq -2,\\
\omega_1^1-\omega_1^O\geq 0,\\
\omega_1^2-\omega_1^O\geq 0,\\
\omega_1^3-\omega_1^O\geq 0,\\
\omega_1^1+\omega_2^1-\omega_2^O\geq 0,\\
\omega_1^2+\omega_2^2-\omega_2^O\geq 0,\\
\omega_1^3+\omega_2^3-\omega_2^O\geq 0,\\
-\omega_0^O+\omega_1^O+\omega_2^O\geq 0,\\
-\omega_0^1+\omega_0^O-\omega_2^O\geq -1,\\
-\omega_0^1+\omega_0^O-\omega_1^O\geq -1,\\
-\omega_0^2+\omega_0^O-\omega_2^O\geq -1,\\
-\omega_0^2+\omega_0^O-\omega_1^O\geq -1,\\
-\omega_0^3+\omega_0^O-\omega_2^O\geq -1,\\
-\omega_0^3+\omega_0^O-\omega_1^O\geq -1.
\end{cases}
\tag{8}
$$