Weak-Diffusion Structure: Meet-in-the-Middle Attacks on Sponge-based Hashing Revisited

Lingyue Qin[1,2], Boxin Zhao[2], Jialiang Hua[3], Xiaoyang Dong[3], and Xiaoyun Wang[3,4]

[1] BNRist, Tsinghua University, Beijing, China
qinly@tsinghua.edu.cn
[2] Zhongguancun Laboratory, Beijing, China
zhaobx@mail.zgclab.edu.cn
[3] Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China
{huajl18,xiaoyangdong,xiaoyunwang}@tsinghua.edu.cn
[4] Key Laboratory of Cryptologic Technology and Information Security (Ministry of Education), School of Cyber Science and Technology, Shandong University, Qingdao, China

Abstract. Besides the U.S. NIST standard `SHA-3` (`Keccak`), another sponge-based primitive `Ascon` was selected as the NIST standard for lightweight applications, recently. Exploring the security against attacks on the sponge-based hash functions is very important. At EUROCRYPT 2023, Qin *et al.* introduced the MitM preimage attack framework and the automatic tools for `Keccak`, `Ascon`, and `Xoodyak`.

In this paper, we extend Qin *et al.*'s MitM attack framework into collision attack and also develop various techniques to improve the automatic tools for both preimage and collision attacks. We introduce a novel initial structure called *weak-diffusion structure* that enjoys many more degrees of freedom to build the blue/red neutral sets than Qin *et al.*'s. In addition, a more flexible condition scheme is introduced to reduce the diffusion of variables. To further accelerate the solving of automatic model, we propose a heuristic two-stage searching strategy, which first finds many blue neutral sets with naturally weak-diffusion properties, and then solves different automatic models with different blue neutral sets prefixed. Also symmetry property of `Keccak` is applied to speed up the search.

At last, we introduce the first collision attack on 4-round `Keccak-512`. Besides, the first MitM-based preimage attack on 4-round `Keccak-384` is found that outperforms all previous attacks, while Qin *et al.* only found attack on `Keccak-512`. Moreover, we find collision attacks on reduced `Xoodyak` and `Ascon` with 1-2 rounds improvements than before. The complexities of preimage attacks on reduced `Xoodyak` and `Ascon` are also improved.

Keywords: `Keccak` · MITM · Automatic Tool · `Ascon`· `Xoodyak`

1 Introduction

A cryptographic hash function H, that maps a message M of arbitrary length into a short fixed-length h-bit target T, should satisfy the security properties:

- **Preimage resistance:** for given target T, the time complexity to find M, *s.t.* $H(M) = T$, should be not lower than 2^h,
- **Collision resistance:** the time complexity to find a message pair (M_1, M_2), *s.t.* $H(M_1) = H(M_2)$, should be not lower than $2^{h/2}$,
- **2nd-preimage resistance:** for given M, the time complexity to find $M' \neq M$, *s.t.* $H(M') = M$, should be not lower than 2^h.

Traditionally, hash functions are often built by iterating a compression function with Merkle-Damgård [49,18] domain extender, *e.g.*, `MD5`, `SHA-1`, and `SHA-2`. Due to the breakthrough attacks by Wang et al. [64,63] on `MD5` and `SHA-1`, the U.S. National Institute of Standards and Technology (NIST) started new standardization of hash functions in October 2008, *i.e.*, the `SHA-3` competition. After intense competition, the `Keccak` sponge function family [11] designed by Bertoni *et al.* won the competition in October 2012 and was subsequently standardized by the NIST as Secure Hash Algorithm-3 [52] (`SHA-3`) in August 2015. Instead of using the classical Merkle-Damgård construction, `Keccak` adopts a new construction called *sponge function*. Since 2008, `Keccak` has received intensive security analysis against the traditional security notions such as collision resistance [23,24,25,55,62,33,35], (second-) preimage resistance [36,50,9,46,21], etc. Due to the high efficiency and security, the sponge function or its variants become widely used to build hash functions and other primitives, such as `Ascon` [27], `Xoodyak` [17], `PHOTON` [37], etc.

The Meet-in-the-Middle (MitM) attack proposed by Diffie and Hellman in 1977 [20] is a time-memory trade-off cryptanalysis of symmetric-key primitives. Since then, the MitM attacks have been improved by more refined techniques and exploiting additional freedoms and structures, such as the internal state guessing [29], splice-and-cut [3], initial structure [59], bicliques [12,41], 3-subset MitM [13], (indirect-)partial matching [3,59], sieve-in-the-middle [16], match-box [31], dissection [22], MitM in differential view [42,30], and differential MitM [15], etc. Till now, the MitM attacks and its variants have broken `MD4` [44,34], `MD5` [59], `KeeLoq` [39], `HAVAL` [4,60], `GOST` [40], `GEA-1/2` [8,1], etc.

Automating the MitM attacks with computer-aided tools may discover more advanced attack configurations, which was first tried in [14,19] at CRYPTO 2011 and 2016 for `AES` and `AES`-like ciphers. At IWSEC 2018, Sasaki [58] introduced the 3-subset MitM attacks on `GIFT` block cipher with Mixed Integer Linear Programming (MILP). At EUROCRYPT 2021, Bao *et al.* [5] fully automated MitM preimage attacks with MILP on `AES`-like hashing, which is built from `AES`-like structures. Later on, this model was further developed into models of key-recovery and collision attacks by Dong *et al.* [28] and Bao *et al.* [6]. At CRYPTO 2022, Schrottenloher and Stevens [61] simplified the language of the automatic model and applied it in both classic and quantum settings.

MitM attack on sponge-based hash functions. The MitM attack has been widely used to attack Merkle-Damgård hash functions [59,3,34], whose compression function is usually built from a block cipher and the PGV hashing modes [54]. However, it was rarely used to attack sponge-based hash functions. At CRYPTO 2022, Schrottenloher and Stevens [61] first built several MitM attacks on sponge-based hash functions, *i.e.*, `SPHINCS+-Haraka` [10] and `Sparkle` [7]. But, the problem to build MitM attacks on `Keccak` was left open. At EUROCRYPT 2023, Qin *et al.* [56] introduced the generic framework of MitM preimage attacks on sponge-based hashing and first built the MitM attacks on 4-round `Keccak-512` [11], 3-/4-round `Ascon-XOF` [27], and 3-round `Xoodyak-XOF` [17]. On the Merkle-Damgård hashing, the splice-and-cut technique [3] is popular to build the MitM attacks. In the attack, the adversary starts from the internal states of the compression function to construct two independent forward and backward computation paths, which are then matched to produce a complete path solution thanks to the feed-forward mechanisms of the hashing modes (usually PGV modes [54]) adopted by the compression function. However, for sponge-based hashing, there is no feed-forward mechanisms and it is hard to build the backward and forward computation paths that meet in the middle. Moreover, for `Keccak`, the inverse round function is much more complex and the backward computation path is deemed to be ineffective. Therefore, Qin *et al.* introduced the MitM framework that only exploits two independent forward computation paths. They built MILP models to search the MitM configurations and studied various techniques to speedup the search, *e.g.*, the linear structure techniques [36].

Exploiting the weak diffusion properties of the permutations has been intensively studied particularly for preimage attacks on `Keccak` [36,46,47]. In the document of `Keccak`, the designers [11] first introduced the CP-kernel property, *i.e.*, θ is the identity when columns have even parity. The CP-kernel can be regarded as the case with the lowest diffusion. Later, Guo *et al.* [36] introduced the linear structures for preimage attacks. By assigning the conditions and consuming the degrees of freedom, the first few χ operations are linearized, and the θ operations are in (partially) CP-kernel. Therefore, the diffusion of the variables are reduced that all the variables are not multiplied with each other, and the linear system on those variables is built and solved to derive preimage attacks. At EUROCRYPT 2023, Qin *et al.* [56] borrowed the linear structure technique to build the MitM attacks on `Keccak`. For the MitM attack, the variables are divided into two independent sets. Any variable from one set should not be multiplied with the variables from the other set. However, within each set, the variables can be multiplied with each other freely, which is the key different feature from Guo *et al.*'s linear-structure attack.

Contributions. For `Keccak`, to accelerate the MILP search model of the MitM attacks, Qin *et al.* used a one-round linear structure as the initial structure to skip the MILP programming of the first round and reduce the scale of the MILP model. This structure is so strong that not only the θ operation but also χ in the first round act as identity on the variables. This is achieved by introducing

only a small amount of variables in the initial state and a large amount of conditions to reduce χ to be an identity operation. Therefore, only a few degrees of freedom of the variables are exploited in Qin *et al.*'s model, which covers only a small fraction of the whole space of the solutions, and may lose better MitM attacks. In this paper, we try to relax the restrictions on the initial structure to enlarge the search space of the MILP model. In fact, for MitM attacks, it is not necessary to make the first χ an identity like Qin *et al.* [56], and it is not necessary to completely linearize it like Guo *et al.* [36], either. We just need to make sure that variables from different neutral sets do not multiply. Hence, we introduce a new initial structure by exploiting the weak diffusion properties, which is named as *weak-diffusion structure*. It exploits more degrees of freedom for the variables compared to Qin *et al.*'s model. For example, in Qin *et al.*'s MitM attack on 4-round `Keccak-512`, only 4 lanes can be assigned as variables in the initial structure. However, in our *weak-diffusion structure*, 8 lanes can be assigned as variables. As we do not need the first χ to be identity or linear, the condition adding scheme is more flexible. In Qin *et al.*'s model, the condition adding scheme is actually fixed, since they are fully assigned to make the first χ an identity. In our MILP model, the condition adding scheme is programmed, and participates in the optimization and trade-off of many parameters.

As indicated by Li, Isobe and Shibutani [45], by finding partial target preimages with the MitM approach, one can build collision attacks on hash functions. The key feature of the MitM collision attack is to fix t-bit partial target as constant and expect to derive an m-bit matching for the MitM. The best case is that for t-bit partial target fixed, one can derive $m = t$ matching bits. In fact, to be better than birthday attack, $\frac{t}{2} < m \leq t$ should hold. However, for Qin *et al.*'s matching scheme in the attack on `Keccak`, only $m = \frac{t}{2}$ matching bits can be derived by fixing t-bit partial target, that disable the MitM collision attack on `Keccak`. Therefore, we introduce a different matching scheme that achieves the optimal case, *i.e.*, $m = t$ matching bits are derived by fixing t-bit partial target.

Empirically, we find the sound MitM solutions have a similar feature that one of the two neutral sets (*e.g.*, blue neutral set) is of low diffusion. Therefore, to further accelerate the solving of automatic model, we propose a heuristic two-stage searching strategy, which first finds many blue neutral sets with naturally very low diffusion property, and then solves different automatic models with different blue neutral sets prefixed.

At last, we improve the MitM attacks on `Keccak`, `Xoodyak` and `Ascon`. For the first time, we introduce the collision attack on 4-round `Keccak-512`, while the best previous collision attack reaches 3-round by Dinur, Dunkelman and Shamir ten years ago [24]. We also build the first MitM preimage attack on 4-round `Keccak-384` that outperforms the best previous linear-structure-based preimage attack [47]. For `Xoodyak-Hash`, we propose the first cryptanalysis result against collision attack that reaches 3 rounds. For `Ascon-Hash`, our collision attacks improve the best previous ones by up to 2 rounds. Additionally, improved MitM

preimage attacks are achieved for 4-round `Keccak-512`, 3-round `Xoodyak-XOF`, and 3-round `Ascon-XOF`. The results are summarized in Table 1.

Table 1: A Summary of the Attacks. Lin. Stru.: Linear Structure. Diff.: Differential. On 4-round `Keccak-384`, [57] claimed a preimage attack with 2^{371}, however, it was later proved to be not faster than brute force by [47]. †: this attack ignores the padding bits.

Target	Attacks	Methods	Rounds	Time	Memory	Brute force	Ref.
`Keccak-512`	Preimage	Lin.Stru.	2	2^{384}	-	2^{512}	[36]
		Lin.Stru.	2	2^{321}	-		[57]
		Lin.Stru.	2	2^{270}	-		[47]
		Lin.Stru.	2	2^{252}	-		[38]
		Lin.Stru.	3	2^{482}	-		[36]
		Lin.Stru.	3	2^{475}	-		[57]
		Lin.Stru.	3	2^{452}	-		[47]
		Lin.Stru.	3	2^{426}	-		[38]
		Rotational	4	2^{506}	-		[50]
		Algebraic	4	$2^{505.3}$	-		[9]
		MitM	4	$2^{504.58}$	2^{108}		[56]
		MitM	4	$2^{501.16}$	2^{212}		Sect. 4.4
	Collision	Diff.	2	Practical	-	2^{256}	[51]
		Diff.	3	Practical	-		[24]
		MitM	4	$2^{252.32}$	2^{251}		Sect. 4.3
`Keccak-384`	Preimage	Lin.Stru.	2	2^{129}	-	2^{384}	[36]
		Lin.Stru.	2	2^{113}	-		[57]
		Lin.Stru.	2	2^{89}	-		[43]
		Lin.Stru.	2	2^{28}	-		[38]
		Lin.Stru.	3	2^{322}	-		[36]
		Lin.Stru.	3	2^{321}	-		[57]
		Lin.Stru.	3	2^{271}	-		[38]
		Rotational	4	2^{378}	-		[50]
		Algebraic	4	$2^{377.3}$	-		[9]
		Lin.Stru.	4	2^{375}	-		[47]
		MitM	4	$2^{371.90}$	2^{368}		Sect. 4.5
	Collision	Internal Diff.	3	Practical	-	2^{192}	[24]
		Internal Diff.	4	2^{147}	-		[24]
`Xoodyak-XOF`	Preimage	Neural	1	-	-	2^{128}	[48]
		MitM	3	$2^{125.06}$	2^{97}		[56]
		MitM	3	$2^{121.77}$	2^{118}		Sect. 5
`Xoodyak-Hash`	Collision	MitM	3	$2^{125.52}$	$2^{124.51}$	2^{128}	Sect. 5
`Ascon-XOF`	Preimage	Algebraic	2	2^{103}	-	2^{128}	[27]
		MitM	3	$2^{120.58}$	2^{39}		[56]
		MitM	3	$2^{114.53}$	2^{30}		Sect. 6
		MitM	4	$2^{124.67}$	2^{50}		[56]
		Algebraic†	6	$2^{127.3}$	-		[27]
`Ascon-Hash`	Collision	Diff.	2	2^{125}	-	2^{128}	[65]
		Diff.	2	2^{103}	-		[32]
		MitM	3	$2^{121.85}$	2^{121}		Sect. 6
		MitM	4	$2^{126.77}$	2^{126}		Sect. 6

2 Preliminaries

This section introduces the sponge construction, the specifications of `Keccak`, `Ascon` and `Xoodyak`, and Qin *et al.*'s MitM attack on sponge-based hashing.

2.1 The Sponge-based Hash Function

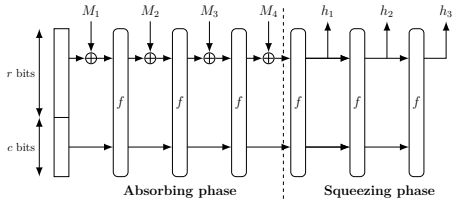

Fig. 1: The sponge construction

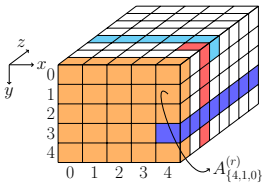

Fig. 2: The `Keccak` state

The sponge-based hash functions (e.g. `Keccak` [11], `Ascon` [27], `Xoodyak` [17]), are to name the hash functions applied the sponge construction [11]. The sponge construction works on a b-bit internal state, which is divided into two parts: the r-bit outer part (r is called the rate), and c-bit inner part (c is called the capacity). In Figure 1, one first initializes the b-bit state with the given value (all zero for `Keccak`). Then, pad and divide the given message into several r-bit blocks. In the absorbing phase, each r-bit message block is XORed into the state and an inner permutation f is applied. In the squeezing phase, produce the digest T of any desired length.

2.2 The `Keccak` Hash Function

Following the sponge construction, the `Keccak`-α versions [11] have $b = 1600$ and the capacity $c = 2\alpha$, where $\alpha \in \{224, 256, 384, 512\}$. The 1600-bit state can be viewed as a $5 \times 5 \times 64$ array of bits. Denote $A^{(r)}_{\{x,y,z\}}$ as the bit located at the x-th column, y-th row and z-th lane in the round r ($r \geq 0$), where $0 \leq x \leq 4,\ 0 \leq y \leq 4,\ 0 \leq z \leq 63$. For simplicity, all the coordinates are considered modulo 5 for x and y, and modulo 64 for z in the following paper. The inner permutation consists of 24 rounds, and each round has five operations $\iota \circ \chi \circ \pi \circ \rho \circ \theta$. The internal states of round r are denoted as $A^{(r)} \xrightarrow{\theta} \theta^{(r)} \xrightarrow{\rho} \rho^{(r)} \xrightarrow{\pi} \pi^{(r)} \xrightarrow{\chi} \chi^{(r)} \xrightarrow{\iota} A^{(r+1)}$.

We list the five operations in each round as follows:

$$\begin{aligned}
&\theta: \ \theta^{(r)}_{\{x,y,z\}} = A^{(r)}_{\{x,y,z\}} \oplus D^{(r)}_{\{x,z\}}, D^{(r)}_{\{x,z\}} = C^{(r)}_{\{x-1,z\}} \oplus C^{(r)}_{\{x+1,z-1\}}, C^{(r)}_{\{x,z\}} = \sum_{y'=0}^{4} A^{(r)}_{\{x,y',z\}},\\
&\rho: \ \rho^{(r)}_{\{x,y,z\}} = \theta^{(r)}_{\{x,y,z-\gamma[x,y]\}},\\
&\pi: \ \pi^{(r)}_{\{y,2x+3y,z\}} = \rho^{(r)}_{\{x,y,z\}},\\
&\chi: \ \chi^{(r)}_{\{x,y,z\}} = \pi^{(r)}_{\{x,y,z\}} \oplus (\pi^{(r)}_{\{x+1,y,z\}} \oplus 1) \cdot \pi^{(r)}_{\{x+2,y,z\}},\\
&\iota: \ A^{(r+1)} = \chi^{(r)} \oplus RC_r, RC_r \text{ is round-dependent constant,}
\end{aligned} \tag{1}$$

where the θ operation is divided into three steps. The rotation constants $\gamma[x, y]$ are given in Table 2 of Supplementary Material B.

This paper focuses on `Keccak-512` and `Keccak-384`, as well as `SHA3-512` and `SHA3-384`. The only difference between `Keccak`-α and `SHA3`-α is the padding rule. For `Keccak`-α, the message is padded with "10*1", which is a single bit 1 followed by the minimum number of 0s and followed by a single bit 1. For `SHA3`-α, the message is padded with "0110*1", to make the length a multiple of $(1600 - 2\alpha)$.

2.3 `Ascon` and `Xoodyak`

In our paper, we also give cryptanalysis on sponge-based hash functions of `Ascon` [27] and `Xoodyak` [17], whose specifications are given in Supplementary Material A. We focus on `Xoodyak-XOF`, `Xoodyak-Hash`, `Ascon-XOF`, and `Ascon-Hash`.

The `Xoodyak-XOF` and `Ascon-XOF` offer an arbitrary output length l and the preimage resistance is $\min(2^{128}, 2^l)$. We target on `Xoodyak-XOF` and `Ascon-XOF` with a 128-bit digest against the preimage attack.

For `Xoodyak-Hash` and `Ascon-Hash`, the output size is 256 bits, whose security claims are 2^{128} against both preimage and collision attacks. We only study them against the collision attacks.

2.4 The Meet-in-the-Middle Attack on Sponge-based Hashing

For Merkle–Damgård hash functions based compression functions with PGV hashing modes [54], the feedforward operations in the hashing modes (e.g., Davis-Meyer, Matyas-Meyer-Oseas and Miyaguchi-Preneel) make the *splice-and-cut* [3] technique possible for the Meet-in-the-Middle (MitM) attack. The input and output of a compression function can be regarded as concatenated through the feed-forward operation in these modes of operations. Then the compression function is in the form of a circle and any step can be selected as either the starting point or the matching point. From the starting point, the compression function is divided into two sub-functions so that a portion of bits of the input message only affect one sub-function and another portion of bits of the input message only affect the other sub-function as shown in Figure 3. Sub-functions are called forward chunk or backward chunk. The bits affecting only one chunk are called neutral bits. Thanks to the feed-forward operation, the first and last steps are consecutive, and thus the forward and backward chunks (partially)

meet to produce some deterministic relations between the two chunks, which are the so-called matching point. Improvements have been developed on both the starting point and the matching point, such as the (probabilistic) initial structure [59,60,34] and (indirect-) partial matching [3,59,60,2].

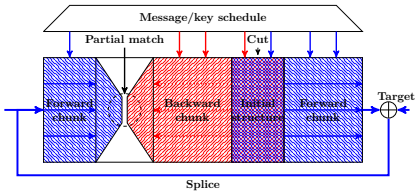

Fig. 3: The splice-and-cut MitM

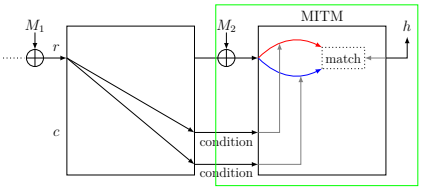

Fig. 4: Qin et al.'s MitM attack [56]

For sponge-based hash functions, without feed-forward mechanisms, the splice-and-cut MitM in Figure 3 can not be trivially applied. Qin *et al.* [56] introduced a new MitM framework for sponge-based hash functions as in Figure 4, where two independent forward chunks are applied. Starting from the r-bit outer part, the two neutral sets (red and blue neutral bits) compute independently forward to the matching points, which are the deterministic relations on the two sets by partially solving the inverse of the permutation from the h-bit target. In order to build longer MitM characteristics, Qin *et al.* applied conditions to reduce the diffusion of the red or blue neutral bits. For `Keccak`'s nonlinear operation $\chi : b_i = a_i \oplus (a_{i+1} \oplus 1) \cdot a_{i+2}$, suppose a_{i+1} is blue bit and a_i is red bit. Without conditions, b_i depends on both blue and red bits. Setting $a_{i+2} = 0$, b_i will only depend on the red bit a_i. Similar techniques with conditions are already used to build MitM attacks [59,3] on MD/SHA hashing with ARX structure. The conditions usually depend on bits from both inner part and outer part. The conditions determined by inner part can be modified by randomly choosing the first several message blocks as M_1 in Figure 4. The probability of M_1 satisfying ς conditions of the inner part is about $2^{-\varsigma}$. After finding one right M_1, assign arbitrary values to all bits except those neutral bits of M_2. Supposing the red and blue neutral sets of the outer part are of $2^{d_\mathcal{R}}$ and $2^{d_\mathcal{B}}$ values respectively, an MitM episode is performed as follows:

1. For each of $2^{d_\mathcal{R}}$ values, compute forward to the matching point.
2. For each of $2^{d_\mathcal{B}}$ values, compute forward to the matching point.
3. For the h-bit target, compute backward to derive an m-bit matching point.
4. Filter states.

The complexity of the MitM episode is $2^{\max(d_\mathcal{R}, d_\mathcal{B})} + 2^{d_\mathcal{R}+d_\mathcal{B}-m}$, which checks $2^{d_\mathcal{R}+d_\mathcal{B}}$ M_2. In order to find a h-bit target preimage, the episode should be repeated $2^{h-(d_\mathcal{R}+d_\mathcal{B})}$ times. After the ς conditions of inner part are satisfied, suppose M_2 provides 2^η MitM episodes. If $\eta + d_\mathcal{R} + d_\mathcal{B} < h$, we have to find

$2^{h-(\eta+d_{\mathcal{R}}+d_{\mathcal{B}})}$ M_1, satisfying the ς conditions. So the total time complexity is

$$2^{h-(\eta+d_{\mathcal{R}}+d_{\mathcal{B}})} \cdot 2^{\varsigma} + 2^{h-(d_{\mathcal{R}}+d_{\mathcal{B}})} \cdot (2^{\max(d_{\mathcal{R}},d_{\mathcal{B}})} + 2^{d_{\mathcal{R}}+d_{\mathcal{B}}-m}). \tag{2}$$

3 The MitM Collision Attack on Sponge-based Hashing

Definition 1 ((t-bit) partial target preimage attack [45]) *Given t-bit partial target of $T(= H(M))$, find M' such that t-bit of $T'(= H(M'))$ is the same as the t-bit of T at the same position, and the other part of T' is randomly obtained.*

Given the hash function H and the t-bit partial target, suppose the algorithm $\mathcal{A}$ can produce a preimage of the given t-bit partial target with a complexity of 2^s. Additionally, assume $\mathcal{A}$ outputs different preimages for different calls. The collision finding approach works as follows:

1. Given the hash function H that produces h-bit digest, randomly fix the t-bit partial target as constant. Call $\mathcal{A}$ to produce $2^{(h-t)/2}$ different (M, T) with the same fixed t-bit partial target.
2. From the $2^{(h-t)/2}$ (M, T), find a collision on the remaining $(h-t)$ bits of the full target.

The total complexity will be $2^{(h-t)/2} \times 2^s$. At FSE 2012, Li *et al.* [45] found the algorithm $\mathcal{A}$ can be efficiently built with MitM approach, thus converted the MitM preimage attacks into MitM (pseudo) collision attacks.

For the MitM collision attack, supposing for two neutral sets of $2^{d_{\mathcal{R}}}$ and $2^{d_{\mathcal{B}}}$ values, we get an m-bit match with fixed t-bit partial target, where $m \leq t$. In an MitM episode, $2^{d_{\mathcal{R}}} \times 2^{d_{\mathcal{B}}}$ messages are checked with MitM approach. After filtering with m-bit match, $2^{d_{\mathcal{R}}+d_{\mathcal{B}}-m}$ messages are left and further checked against the fixed t-bit partial target. At last, there are about $2^{d_{\mathcal{R}}+d_{\mathcal{B}}-t}$ messages satisfying the t-bit partial target for each MitM episode. The time complexity of one MitM episode is about $2^{\max(d_{\mathcal{R}},d_{\mathcal{B}})} + 2^{d_{\mathcal{R}}+d_{\mathcal{B}}-m}$. Totally, we need

$$2^{(h-t)/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t)} \tag{3}$$

MitM episodes to derive $2^{(h-t)/2}$ preimages of the t-bit partial target. Therefore, the time complexity to produce the collision is about

$$2^{(h-t)/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t)} \times (2^{\max(d_{\mathcal{R}},d_{\mathcal{B}})} + 2^{d_{\mathcal{R}}+d_{\mathcal{B}}-m}) = 2^{\frac{h}{2}-\min(d_{\mathcal{R}}-\frac{t}{2},d_{\mathcal{B}}-\frac{t}{2},m-\frac{t}{2})}. \tag{4}$$

The memory complexity is $2^{\min(d_{\mathcal{R}},d_{\mathcal{B}})} + 2^{\frac{h}{2}-\frac{t}{2}}$.

At CRYPTO 2021, Dong *et al.* [28] introduced the technique of *nonlinearly constrained neutral words* to compute the ■ and ■ neutral sets via a table-based precomputation phase. Suppose in the starting state, there are $\lambda_{\mathcal{R}}$ ■ bits and $\lambda_{\mathcal{B}}$ ■ bits, where $\lambda_{\mathcal{R}} \geq d_{\mathcal{R}}$, $\lambda_{\mathcal{B}} \geq d_{\mathcal{B}}$. After consuming $\lambda_{\mathcal{R}} - d_{\mathcal{R}}$ and $\lambda_{\mathcal{B}} - d_{\mathcal{B}}$ degrees of freedom (DoFs) for ■ and ■ with nonlinearly constrained, the independent neutral sets are prepared to perform the MitM episode. According to [28], both the time and memory complexities of one precomputation are $2^{\lambda_{\mathcal{R}}} + 2^{\lambda_{\mathcal{B}}}$.

After the precomputation, $2^{\lambda_{\mathcal{R}}-d_{\mathcal{R}}+\lambda_{\mathcal{B}}-d_{\mathcal{B}}}$ MitM episodes are produced. Therefore, according to (3), $2^{(h-t)/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t)-(\lambda_{\mathcal{R}}-d_{\mathcal{R}}+\lambda_{\mathcal{B}}-d_{\mathcal{B}})} = 2^{(h-t)/2+t-\lambda_{\mathcal{R}}-\lambda_{\mathcal{B}}}$ precomputations should be performed, whose time complexity is

$$2^{\frac{h}{2}-\min(\lambda_{\mathcal{R}}-\frac{t}{2},\lambda_{\mathcal{B}}-\frac{t}{2})}+2^{\lambda_{\mathcal{R}}}+2^{\lambda_{\mathcal{B}}}, \tag{5}$$

where the $2^{\lambda_{\mathcal{R}}}+2^{\lambda_{\mathcal{B}}}$ is to ensure that at least one precomputation is performed.

For the MitM collision attack on sponge-based hashing, we also need to consider the conditions. Taking the notations in Section 2.4 and Equ. (2), for MitM collision attacks we have to find $2^{(h-t)/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t)-\eta}$ M_1 that satisfy the conditions. This costs

$$2^{h/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t/2+\eta-\varsigma)}. \tag{6}$$

All in all, to perform the MitM collision attack with conditions and also take Dong *et al.*'s precomputation [28] into consideration, *i.e.*, adding (4), (5) and (6) together, the final time complexity is

$$2^{\frac{h}{2}-(d_{\mathcal{R}}+d_{\mathcal{B}}-\frac{t}{2}+\eta-\varsigma)}+2^{\frac{h}{2}-\min(d_{\mathcal{R}}-\frac{t}{2},d_{\mathcal{B}}-\frac{t}{2},m-\frac{t}{2},\lambda_{\mathcal{R}}-\frac{t}{2},\lambda_{\mathcal{B}}-\frac{t}{2})}+2^{\lambda_{\mathcal{R}}}+2^{\lambda_{\mathcal{B}}}. \tag{7}$$

The memory complexity is

$$2^{\lambda_{\mathcal{R}}}+2^{\lambda_{\mathcal{B}}}+2^{\min(d_{\mathcal{R}},d_{\mathcal{B}})}+2^{\frac{h}{2}-\frac{t}{2}}. \tag{8}$$

Therefore, to perform collision attack faster than birthday bound (*i.e.* $2^{h/2}$), the constraints $d_{\mathcal{R}} \leq \lambda_{\mathcal{R}} < h/2$, $d_{\mathcal{B}} \leq \lambda_{\mathcal{B}} < h/2$, $m > t/2$, $d_{\mathcal{R}} > t/2$, $d_{\mathcal{B}} > t/2$, $t > 0$, and $d_{\mathcal{R}} + d_{\mathcal{B}} - t/2 + \eta - \varsigma > 0$ should hold. In this paper, all our attacks satisfy $m = t$, therefore, (7) is reduced to

$$2^{\frac{h}{2}-(d_{\mathcal{R}}+d_{\mathcal{B}}-\frac{t}{2}+\eta-\varsigma)}+2^{\lambda_{\mathcal{R}}}+2^{\lambda_{\mathcal{B}}}+2^{\frac{h}{2}-\min(d_{\mathcal{R}}-\frac{t}{2},d_{\mathcal{B}}-\frac{t}{2},\frac{t}{2})}. \tag{9}$$

4 The MitM Collision and Preimage Attacks on Keccak

In this section, we first give an overview of the previous MitM framework on Keccak. Then we introduce our improved MILP models for the MitM collision and preimage attacks on Keccak. As applications, we give the first 4-round collision attack on Keccak-512, the improved 4-round preimage attacks on Keccak-512 and Keccak-384.

4.1 Qin *et al.*'s MILP-based MitM models on Keccak

In [56], Qin *et al.* introduced a new MitM framework for sponge-based hash functions. We briefly introduce their MILP-based automatic model. Different with other previous MILP models of the MitM attacks [5,28], they first gave a new coloring scheme of five colors (■, ■, ■, ■ and □), where the ■ is inspired by the indirect-partial matching technique [59,3]. In the model, each bit of the state takes one of the five colors with different meanings:

- `Gray` ■: global constant.
- `Red` ■: determined by ■ and ■ of starting state.
- `Blue` ■: determined by ■ and ■ of starting state.
- `Green` ■: determined by ■, ■ and ■, but the expression does not contain the product of ■ and ■.
- `White` □: determined by the product of ■ and ■.

The corresponding encoding scheme uses three 0-1 variables $(\omega_0, \omega_1, \omega_2)$ for each bit: $(1,1,1)$ represents ■, $(0,1,1)$ represents ■, $(1,1,0)$ represents ■, $(0,1,0)$ represents ■, and $(0,0,0)$ represents □. Then the attribute propagations of the five colors over the θ and χ operations of `Keccak` are modeled. The *linear structure* technique [36,26] is also applied to speed up the search and the model is constructed from the second round $A^{(1)}$.

As obtained in [36], given three known consecutive output bits of χ operation, two linear equations of the input bits can be constructed. E.g., assuming that $(\chi^{(r)}_{\{x,y,z\}}, \chi^{(r)}_{\{x+1,y,z\}}, \chi^{(r)}_{\{x+2,y,z\}})$ are known, there are two linear equations of $(\pi^{(r)}_{\{x,y,z\}}, \pi^{(r)}_{\{x+1,y,z\}}, \pi^{(r)}_{\{x+2,y,z\}}, \pi^{(r)}_{\{x+3,y,z\}})$:

$$\begin{aligned} \chi^{(r)}_{\{x,y,z\}} &= \pi^{(r)}_{\{x,y,z\}} \oplus (\chi^{(r)}_{\{x+1,y,z\}} \oplus 1) \cdot \pi^{(r)}_{\{x+2,y,z\}}, \\ \chi^{(r)}_{\{x+1,y,z\}} &= \pi^{(r)}_{\{x+1,y,z\}} \oplus (\chi^{(r)}_{\{x+2,y,z\}} \oplus 1) \cdot \pi^{(r)}_{\{x+3,y,z\}}. \end{aligned} \tag{10}$$

Then combining with the CP-kernel property [11], Qin *et al.* derived the leaked linear relations for matching.

Observation 1 (Matching Points of `Keccak-512` [56]) *Assume $A^{(r+1)}$ is the hash value and compute one round backward from $A^{(r+1)}$ to $A^{(r)}$ with Equ. (1). The following linear equations on $A^{(r)}$ can be derived for matching:*

$$\begin{aligned} A^{(r)}_{\{3,0,z-\gamma[3,0]\}} \oplus A^{(r)}_{\{3,3,z-\gamma[3,0]\}} \oplus (A^{(r+1)}_{\{1,1,z\}} \oplus 1) \cdot (A^{(r)}_{\{0,2,z-\gamma[0,2]\}} \oplus A^{(r)}_{\{0,0,z-\gamma[0,2]\}}) \\ = A^{(r+1)}_{\{0,1,z\}} \oplus \theta^{(r)}_{\{3,3,z-\gamma[3,0]\}} \oplus (A^{(r+1)}_{\{1,1,z\}} \oplus 1) \cdot \theta^{(r)}_{\{0,0,z-\gamma[0,2]\}}, \end{aligned} \tag{11}$$

$$\begin{aligned} A^{(r)}_{\{4,1,z-\gamma[4,1]\}} \oplus A^{(r)}_{\{4,4,z-\gamma[4,1]\}} \oplus (A^{(r+1)}_{\{2,1,z\}} \oplus 1) \cdot (A^{(r)}_{\{1,3,z-\gamma[1,3]\}} \oplus A^{(r)}_{\{1,1,z-\gamma[1,3]\}}) \\ = A^{(r+1)}_{\{1,1,z\}} \oplus \theta^{(r)}_{\{4,4,z-\gamma[4,1]\}} \oplus (A^{(r+1)}_{\{2,1,z\}} \oplus 1) \cdot \theta^{(r)}_{\{1,1,z-\gamma[1,3]\}}, \end{aligned} \tag{12}$$

where bits in $A^{(r+1)}$ and $\theta^{(r)}$ are known from the hash value. In Equ. (11), if $(A^{(r)}_{\{3,0,z-\gamma[3,0]\}}, A^{(r)}_{\{3,3,z-\gamma[3,0]\}}, A^{(r)}_{\{0,2,z-\gamma[0,2]\}}, A^{(r)}_{\{0,0,z-\gamma[0,2]\}})$ satisfy the following two conditions, there is 1-bit filter (the situation for Equ. (12) is similar):

(1) There is no □ in $(A^{(r)}_{\{3,0,z-\gamma[3,0]\}}, A^{(r)}_{\{3,3,z-\gamma[3,0]\}}, A^{(r)}_{\{0,2,z-\gamma[0,2]\}}, A^{(r)}_{\{0,0,z-\gamma[0,2]\}})$.

(2) $(A^{(r)}_{\{3,0,z-\gamma[3,0]\}}, A^{(r)}_{\{3,3,z-\gamma[3,0]\}})$ is of (■,■), (■,■), (■,■), (■,■), or (■,■), or opposite order .

4.2 New MILP model for MitM collision attack on `Keccak-512`

In our new bit-level MILP model, we reuse the coloring scheme and attribute propagation rules for θ and χ operations in [56].

Comments on Qin et al.*'s linear structure.* In Qin *et al.*'s model [56], a 1-round linear structure (LS) is applied as shown in Figure 5. Their linear structure is so strong that not only the θ operation acts as identity, but also the χ operation is identity. This is achieved by assigning variables in only four lanes of $A^{(0)}$ and also many conditions to make the χ operation as identity. Therefore, many degrees of freedom are consumed to maintain this linear structure. Moreover, different from *linear-structure* based preimage attacks [36], the variables with the same color can be multiplied in the MitM attacks and there is no need to keep strictly linear.

To improve the MitM attacks, we extend Qin *et al.*'s model with a series of techniques, which are briefly summarized below and then detailed in this section.

1. To enlarge the search space for better MitM attacks, we exploit initial structures with more freedom instead of Qin *et al.*'s "strong" linear structure.
2. Larger search space will increase the difficulty of solving the MILP model. To obtain feasible solutions in reasonable time, we add the conditions to control the diffusion of ■/■ bits and accelerate the search. In Qin *et al.*'s model, the conditions are also assigned but more strictly to make the first χ operation as identity. Therefore, their condition scheme is fixed after ■/■ bits are assigned in $A^{(0)}$, *i.e.*, each ■/■ bit before the first χ needs two bit conditions. However, in our condition scheme, the first χ is not an identity, and the conditions are assigned flexibly by the MILP model.
3. More conditions assigned will make the diffusion weaker, and then better MitM attacks may be discovered. However, according to Equ. (2), more conditions may bound the overall time complexity. Therefore, our MILP model with more flexible condition scheme will find the better tradeoff between the number of conditions and the diffusion of the two neutral sets.
4. The matching points used for MitM collision attack are different with the MitM preimage attack in `Keccak`. We bring in new objective function considering more parameters of the whole time complexity according to Equ. (9) including the size of ■/■ sets, the consumed degrees of freedom of ■/■ bits, the degree of matching, the number of conditions, etc.
5. To further accelerate the model, we introduce the two-stage approach to solve the model: Stage I, enumerate many neutral ■ sets with weak diffusion; Stage II, decompose the overall optimizing problem into many local optimizing problems by initiating different weak-diffusion ■ sets. This is a heuristic idea that we experimentally find many good solutions sharing the same property that the diffusion of ■ set is weak.

We detail the differences of the model in the following.

Exploiting weak-diffusion structures: Modelling Round 0. To expand the search space in anticipation of better MitM attacks, we do not use Qin *et al.*'s strong linear structure, but exploit initial structures with more degrees of freedom and still somewhat weak diffusion. Inspired by the structures with quadratic terms [47,57], we put the variables in the first four columns shown in Figure 6 marked by ■, and make θ operation in the first round as identity with CP-kernel

property. Denote the starting state as $A^{(0)}$. The variables $\{v_{0,z}, v_{1,z}, v_{2,z}, v_{3,z}\}$ $(0 \le z \le 63)$ are allocated as $A^{(0)}_{\{x,0,z\}} = v_{x,z},\ A^{(0)}_{\{x,1,z\}} = v_{x,z} \oplus c_{x,z},\ 0 \le x \le 3$, where $c_{x,z}$ are constants. After the χ operation, each variable will propagate to three state bits without control, and the quadratic terms may appear. To reduce the diffusion of the χ operation, proper constraints on ■ bits will be added, which are the so-called conditions.

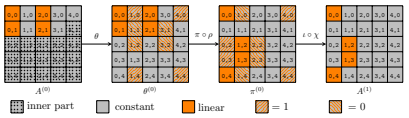

Fig. 5: The 1-round LS in [56]

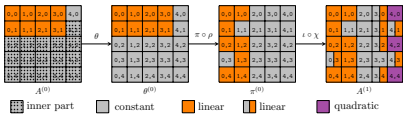

Fig. 6: The weak-diffusion structure

For the coloring scheme, each of the 1600 bits in the starting state $A^{(0)}$ takes one color of ■, ■ and ■. According to Figure 6, only the bits put with variables $\{v_{0,z}, v_{1,z}, v_{2,z}, v_{3,z}\}$ can be colored as ■ or ■. The bits determined by the same variable should be of the same color. Since $A^{(0)}_{\{x,0,z\}} \oplus A^{(0)}_{\{x,1,z\}} = c_{x,z}$ is constant, it consumes one degree of freedom (DoF) of ■ (■) if $A^{(0)}_{\{x,0,z\}}$ and $A^{(0)}_{\{x,1,z\}}$ are of ■ (■). Thereafter, the coloring pattern of the state keeps the same over the first θ operation. So the MILP model can be constructed from $\pi^{(0)}$. For the state bit $\pi^{(0)}_{\{x,y,z\}}$, we define three 0-1 variables $\pi^{(0)}_{\{x,y,z\}}[l]$ $(0 \le l \le 2)$ to represent its color, where $\pi^{(0)}_{\{x,y,z\}}[l]$ corresponds to ω_l of the encoding scheme in Sect. 4.1. The constraints for the bits $\pi^{(0)}$ marked by ■ are

$$\pi^{(0)}_{\{0,2x,z+\gamma[x,0]\}}[l] = \pi^{(0)}_{\{1,2x+3,z+\gamma[x,1]\}}[l],\ \pi^{(0)}_{\{0,2x,z\}}[1] = 1,\ \pi^{(0)}_{\{0,2x,z\}}[0] + \pi^{(0)}_{\{0,2x,z\}}[2] \ge 1. \tag{13}$$

where $0 \le x \le 3, 0 \le z \le 63$, "$\pi^{(0)}_{\{0,2x,z\}}[1] = 1$" means no □ bits exist and "$\pi^{(0)}_{\{0,2x,z\}}[0] + \pi^{(0)}_{\{0,2x,z\}}[2] \ge 1$" means no ■ bits exist. The other $1600 - 8 \times 64 = 1088$ bits are ■, where the corresponding $\pi^{(0)}_{\{x,y,z\}}[l] = 1$ $(0 \le l \le 2)$.

Therefore, the number of initial degrees of freedom for ■ and ■ are $\lambda_{\mathcal{B}} = \sum_{x=0}^{3}\sum_{z=0}^{63}(1 - \pi^{(0)}_{\{0,2x,z\}}[2])$ and $\lambda_{\mathcal{R}} = \sum_{x=0}^{3}\sum_{z=0}^{63}(1 - \pi^{(0)}_{\{0,2x,z\}}[0])$.

Modelling the χ operation with conditions in Round 0. Adding conditions to certain state bits can control the diffusion of the two neutral sets over the χ operation, but the number of conditions should be carefully considered, which may become the bottleneck of the time complexity as Equ. (2). In Qin *et al.*'s model, there is one variable at most in the five input bits of each χ operation and they fixed two conditions to make χ an identity as in Figure 5. However, some conditions are redundant in the programming. Taking Figure 7 and Figure 8 as examples with $\pi^{(0)}_{\{*,*,z\}} \xrightarrow{\iota\circ\chi} A^{(1)}_{\{*,*,z\}} \xrightarrow{\theta} \theta^{(1)}_{\{*,*,z\}}$. The Figure 7 is completely following the condition rules in Qin *et al.*'s model. But in Figure 8, without conditions $\pi^{(0)}_{\{2,2,z\}} = 0$ and $\pi^{(0)}_{\{2,3,z\}} = 0$, the $A^{(1)}_{\{0,3,z\}}$ and $A^{(1)}_{\{0,3,z\}}$ will be

■, which however does not affect the coloring pattern over the next θ operation. On one hand, since there are already ■ bits in $A^{(1)}_{\{0,0,z\}}$ and $A^{(1)}_{\{0,4,z\}}$, the color of $C^{(1)}_{\{0,z\}}$ (without consuming DoF of ■) will be ■, no matter $A^{(1)}_{\{0,2,z\}}$ and $A^{(1)}_{\{0,3,z\}}$ are ■ or ■. On the other hand, due to the ■ in $D^{(1)}_{\{0,z\}}$, all the five bits in $\theta^{(1)}_{\{0,*,z\}}$ must be ■ without consuming DoFs of ■. So the two conditions $\pi^{(0)}_{\{2,2,z\}} = 0$ and $\pi^{(0)}_{\{2,3,z\}} = 0$ are wasted. In our attack with weak-diffusion structure, there are two variables at most in the five inputs of each χ operation as Figure 6. Without conditions, the ■ bits will be linear on the variables in $A^{(0)}$. We can also add certain conditions to let the ■ bits to be constants. Therefore, unlike Qin *et al.*'s model, whether to add conditions will be flexibly programmed and determined by our model.

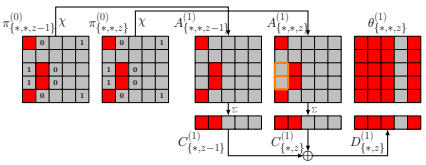

Fig. 7: Example (1)

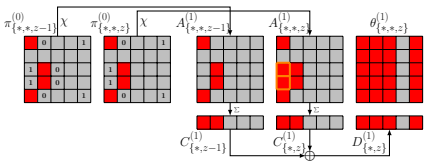

Fig. 8: Example (2)

In Figure 6, the bits in $\pi^{(0)}$ can only be ■ or ■ or ■ according to Equ. (13). We can add conditions on ■ bits to control the diffusion of χ, or let it propagate freely without conditions. As shown in Figure 6, among the five inputs of χ of each row, the bits $\pi^{(0)}_{\{2,y,z\}}$, $\pi^{(0)}_{\{3,y,z\}}$ and $\pi^{(0)}_{\{4,y,z\}}$ are always ■. There are totally three cases of the five inputs:

- `Case-0`: There are five ■ bits.
- `Case-1`: There is only one ■/■ bit, and the others are ■ bits.
- `Case-2`: There are two consecutive ■/■ bits, and the others are ■ bits.

For `Case-1` and `Case-2`, we give the rules of the diffusion over χ operation with conditions for `Keccak`, named as `CondSBOX-RULE`:

- `CondSBOX-RULE-1`: There is only one ■/■ bit in $\pi^{(0)}_{\{i,y,z\}}$ ($i = 0$ or 1). We add conditions to control the color of $(\chi^{(0)}_{\{i,y,z\}}, \chi^{(0)}_{\{i-1,y,z\}}, \chi^{(0)}_{\{i-2,y,z\}})$.
  1. $\chi^{(0)}_{\{i,y,z\}}$ will be the same color with $\pi^{(0)}_{\{i,y,z\}}$.
  2. If we set $\pi^{(0)}_{\{i+1,y,z\}} = 0$, $\chi^{(0)}_{\{i-1,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{i-1,y,z\}}$ will be the same color with $\pi^{(0)}_{\{i,y,z\}}$.
  3. If we set $\pi^{(0)}_{\{i-1,y,z\}} = 1$, $\chi^{(0)}_{\{i-2,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{i-2,y,z\}}$ will be the same color with $\pi^{(0)}_{\{i,y,z\}}$.

– `CondSBOX-RULE-2`: There are two consecutive ■/■ bits in $\pi^{(0)}_{\{0,y,z\}}$ and $\pi^{(0)}_{\{1,y,z\}}$. Since in the expression of $\chi^{(0)}_{\{4,y,z\}}$, there is a quadratic term $\pi^{(0)}_{\{0,y,z\}} \cdot \pi^{(0)}_{\{1,y,z\}}$. If $(\pi^{(0)}_{\{0,y,z\}}, \pi^{(0)}_{\{1,y,z\}})$ are (■, ■) or (■, ■), the color of $\chi^{(0)}_{\{4,y,z\}}$ will be □. To avoid the □ from appearing in the first round, we restrict the $(\pi^{(0)}_{\{0,y,z\}}, \pi^{(0)}_{\{1,y,z\}})$ to be of the same color, *i.e.*, (■, ■) or (■, ■). We add one condition to control the color of $(\chi^{(0)}_{\{0,y,z\}}, \chi^{(0)}_{\{1,y,z\}}, \chi^{(0)}_{\{3,y,z\}}, \chi^{(0)}_{\{4,y,z\}})$.
  1. $\chi^{(0)}_{\{0,y,z\}}$, $\chi^{(0)}_{\{1,y,z\}}$ and $\chi^{(0)}_{\{4,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.
  2. If we set $\pi^{(0)}_{\{4,y,z\}} = 1$, $\chi^{(0)}_{\{3,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{3,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.

For the state bit $\chi^{(0)}_{\{x,y,z\}}$, we also define three 0-1 variables $\chi^{(0)}_{\{x,y,z\}}[l]$ $(0 \le l \le 2)$ to represent its color. Then we allocate Binary variable $\texttt{Cond}_{\{x,y,z\}}$ for $\pi^{(0)}_{\{x,y,z\}}$, where $\texttt{Cond}_{\{x,y,z\}} = 1$ if and only if there is a condition on $\pi^{(0)}_{\{x,y,z\}}$. The rules `CondSBOX-RULE` can be described by the linear inequalities as follows:

– For $\chi^{(0)}_{\{1,y,z\}}$ and $\chi^{(0)}_{\{2,y,z\}}$, the colors are easy to determine: $\chi^{(0)}_{\{1,y,z\}}$ is always same with $\pi^{(0)}_{\{1,y,z\}}$, and $\chi^{(0)}_{\{2,y,z\}}$ is always ■. We get $\chi^{(0)}_{\{1,y,z\}}[l] = \pi^{(0)}_{\{1,y,z\}}[l]$ and $\chi^{(0)}_{\{2,y,z\}}[l] = 1$ $(0 \le l \le 2)$.
– For $\chi^{(0)}_{\{3,y,z\}}$, the color is affected by $\pi^{(0)}_{\{0,y,z\}}$, and can be controlled by the condition in $\pi^{(0)}_{\{4,y,z\}}$, where

$$\begin{cases} \chi^{(0)}_{\{3,y,z\}}[0] \ge \pi^{(0)}_{\{0,y,z\}}[0],\ \chi^{(0)}_{\{3,y,z\}}[2] \ge \pi^{(0)}_{\{0,y,z\}}[2],\ \chi^{(0)}_{\{3,y,z\}}[1] = \pi^{(0)}_{\{0,y,z\}}[1], \\ \texttt{Cond}_{\{4,y,z\}} = \chi^{(0)}_{\{3,y,z\}}[0] + \chi^{(0)}_{\{3,y,z\}}[2] - \pi^{(0)}_{\{0,y,z\}}[0] - \pi^{(0)}_{\{0,y,z\}}[2]. \end{cases}$$

– For $\chi^{(0)}_{\{0,y,z\}}$ and $\chi^{(4)}_{\{0,y,z\}}$, their colors are determined by $\pi^{(0)}_{\{0,y,z\}}$ and $\pi^{(0)}_{\{1,y,z\}}$. To avoid the □ in $\chi^{(4)}_{\{0,y,z\}}$, we first limit the color of $(\pi^{(0)}_{\{0,y,z\}}, \pi^{(0)}_{\{1,y,z\}})$ to be (■, ■) or (■, ■) or (■, ∗) or (∗,■), where ∗ represents ■/■/■, as

$$\pi^{(0)}_{\{0,y,z\}}[0] + \pi^{(0)}_{\{1,y,z\}}[2] \ge 1,\ \pi^{(0)}_{\{0,y,z\}}[2] + \pi^{(0)}_{\{1,y,z\}}[0] \ge 1.$$

– The color of $\chi^{(0)}_{\{4,y,z\}}$ is restricted by conditions on $\pi^{(0)}_{\{0,y,z\}}$ and $\pi^{(0)}_{\{1,y,z\}}$, and the color of $\chi^{(0)}_{\{0,y,z\}}$ is restricted by conditions on $\pi^{(0)}_{\{2,y,z\}}$, which are described by Equ. (17) and Equ. (18) in Supplementary Material B.

Denote μ to be number of total conditions. Thereafter, we can obtain $\mu = \sum_{x=0}^{4}\sum_{y=0}^{4}\sum_{z=0}^{63} \texttt{Cond}_{\{x,y,z\}}$, where $\texttt{Cond}_{\{3,y,z\}}$ is always 0. All valid coloring patterns of `CondSBOX-RULE-1` and `CondSBOX-RULE-2` with ■ in the inputs are shown in Figure 9 (same for ■).

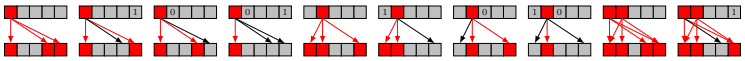

Fig. 9: `CondSBOX-RULE` for `Keccak`

Modelling Matching Points. In [56], the equations acting as matching points in Observation 1 can not be directly applied to our MitM collision attack[5]. Instead, we deduce some new relations of $A^{(r)}$ and the hash value, *i.e.*, the first 512 bits of $A^{(r+1)}$, to act as the matching points. With the known 320-bit $A^{(r+1)}_{\{*,0,*\}}$, we deduce $\pi^{(r)}_{\{*,0,*\}}$ by inverse χ. Then applying the inverse of the operations ρ, π and θ operation, we get

$$\pi^{(r)}_{\{x,0,z+\gamma[x,x]\}} = \theta^{(r)}_{\{x,x,z\}} = A^{(r)}_{\{x,x,z\}} \oplus A^{(r)}_{\{x-1,0,z\}} \oplus A^{(r)}_{\{x-1,1,z\}} \oplus A^{(r)}_{\{x-1,2,z\}} \oplus A^{(r)}_{\{x-1,3,z\}} \oplus A^{(r)}_{\{x-1,4,z\}} \oplus A^{(r)}_{\{x+1,0,z-1\}} \oplus A^{(r)}_{\{x+1,1,z-1\}} \oplus A^{(r)}_{\{x+1,2,z-1\}} \oplus A^{(r)}_{\{x+1,3,z-1\}} \oplus A^{(r)}_{\{x+1,4,z-1\}}. \tag{14}$$

Comparing to Qin *et al.*'s matching scheme in Observation 1, where only four bits in $A^{(r)}$ are needed to build one matching equation, we need 11 bits in $A^{(r)}$ to derive a matching equation. Since in $A^{(r)}$, many bits are □ and can not be used, therefore, it is another reason that we update Qin *et al.*'s model to enlarge the search space for sound solutions to build collision attacks.

Observation 2 (Conditions in Matching Point of MitM Collision Attack) *In Equ. (14), if the eleven bits in $A^{(r)}$ satisfy the following two conditions, then there is 1-bit filter after prefixing 1-bit partial target, i.e., $\theta^{(r)}_{\{x,x,z\}}$:*

(1) There is no □.
(2) There is ■, *or there are both* ■ *and* ■ *at the same time.*

We also use the Binary variable $\delta^{\mathcal{M}}_{\{x,z\}}$ $(0 \le x \le 4, 0 \le z \le 63)$ to represent whether there is a filtering in $\pi^{(r)}_{\{x,0,z+\gamma[x,x]\}}$ as Equ. (14). The constraints of $\delta^{\mathcal{M}}_{\{x,z\}}$ is similar to [56]. We allocate three 0-1 variables $\nu^{i}_{\{x,z\}}$ $(i \in \{0,1,2\}, 0 \le x \le 4, 0 \le z \le 63)$, where $\nu^{i}_{\{x,z\}} = 1$ $(i = 0,1,2)$ if and only if all ω_i's of the eleven bits of $A^{(r)}$ in Equ. (14) are 1. Then we can derive

$$\begin{cases} \nu^{1}_{\{x,z\}} - \delta^{\mathcal{M}}_{\{x,z\}} \ge 0, \ -\nu^{0}_{\{x,z\}} - \delta^{\mathcal{M}}_{\{x,z\}} + 1 \ge 0, \ -\nu^{2}_{\{x,z\}} - \delta^{\mathcal{M}}_{\{x,z\}} + 1 \ge 0, \\ \nu^{0}_{\{x,z\}} - \nu^{1}_{\{x,z\}} + \nu^{2}_{\{x,z\}} + \delta^{\mathcal{M}}_{\{x,z\}} \ge 0. \end{cases}$$

The number of partial target t equals the degree of matching m, i.e., $m = t = \sum_{x=0}^{5}\sum_{z=0}^{63}\delta^{\mathcal{M}}_{\{x,z\}}$. Considering $m \le t$, our matching scheme achieves the optimal case $(m = t)$ according to Equ. (4).

[5]When applying Qin *et al.*'s matching method to collision attacks, we need to fix 2-bit target to generate 1-bit matching, *i.e.*, $t = 2m$. For example, in Equ. (11), we need the values of $(A^{(r+1)}_{\{1,1,z\}} \oplus 1)$ and $(A^{(r+1)}_{\{0,1,z\}} \oplus \theta^{(r)}_{\{3,3,z-\gamma[3,0]\}} \oplus (A^{(r+1)}_{\{1,1,z\}} \oplus 1) \cdot \theta^{(r)}_{\{0,0,z-\gamma[0,2]\}})$ to build one equation as 1-bit filter. According to Equ. (7), when $t = 2m$, the time complexity will be not less than the brute force, i.e., $2^{h/2}$.

The Objective Function. According to Equ. (9), we consider all the parameters in the objective function. Assume $\xi_{\mathcal{R}}$ and $\xi_{\mathcal{B}}$ be the accumulated consumed DoFs of ■ and ■ bits. Therefore, we can get $d_{\mathcal{R}} = \lambda_{\mathcal{R}} - \xi_{\mathcal{R}}$, $d_{\mathcal{B}} = \lambda_{\mathcal{B}} - \xi_{\mathcal{B}}$. According to Equ. (9), suppose that for a given right M_1, that satisfies all the conditions, M_2 provide 2^{η} MitM episodes. Therefore, for a given right M_1, at most $2^{\eta+d_{\mathcal{B}}+d_{\mathcal{R}}-t}$ t-bit partial target preimages can be derived with a search space of $2^{\eta+d_{\mathcal{B}}+d_{\mathcal{R}}}$ M_2. Assume the μ conditions are all satisfied by modifying M_2. So those conditions can be represents as a linear system of $576-2\lambda_{\mathcal{B}}-2\lambda_{\mathcal{R}}$ ■ bits in M_2 and $\lambda_{\mathcal{B}}+\lambda_{\mathcal{R}}$ c variables in M_2. The possible solutions of M_2 is $576-\lambda_{\mathcal{B}}-\lambda_{\mathcal{R}}-\mu$. Since the consumed DoFs can also be precomputed to conduct the MitM episodes, we have $\eta = 576-\lambda_{\mathcal{B}}-\lambda_{\mathcal{R}}-\mu+\xi_{\mathcal{B}}+\xi_{\mathcal{R}} = 576-\mu-d_{\mathcal{B}}-d_{\mathcal{R}}$. Then, for a given M_1, M_2 can provide a search space of $2^{\eta+d_{\mathcal{B}}+d_{\mathcal{R}}} = 2^{576-\mu}$. To simplify the model, we restrict $\mu \leq 320$, so that only one right M_1 is needed to perform the collision attack (a space of about 2^{256} is needed, which is totally provided by M_2). However, in practice, a few conditions (denoted as ς) of the $\mu \leq 320$ conditions will be only determined by M_1. Then, the time to find one right M_1 is about 2^{ς}. However, in practice, ς is usually very small, e.g., $\varsigma = 65$ and $\mu = 302$ for our collision attack on `Keccak-512`, and $\varsigma = 8$ and $\mu = 200$ for our attack on `Keccak-384`. So the time 2^{ς} will be not the bottleneck of the overall attack. We introduce an auxiliary variable v_{obj} with the following constraints:

$$\begin{cases} \text{Maximize} \quad v_{obj}, \\ v_{obj} \leq d_{\mathcal{R}} - \dfrac{t}{2},\ v_{obj} \leq d_{\mathcal{B}} - \dfrac{t}{2},\ v_{obj} \leq \dfrac{t}{2},\ v_{obj} \leq \dfrac{h}{2} - \lambda_{\mathcal{R}}, v_{obj} \leq \dfrac{h}{2} - \lambda_{\mathcal{B}}. \end{cases}$$

The two-stage approach: speed up the searching of MILP model. With all above modelling strategies, we can build an MILP model for the MitM collision attack on r-round `Keccak`. However, since we set the initial state with larger space and relax the restrictions on the conditions of diffusion, the solving of the model is quite slow. To accelerate the searching to get fairly good solution in a reasonable time, we choose to restrict the diffusion of ■ set further.

In the first round, we restrict that the consumption DoFs of ■ set only happen in the θ operation due to CP-kernel property. Then impose full conditions related to ■ on $\pi^{(0)}$ to make χ operation an identity only for the ■ bits[6]. According to the results of [56] and our experiments, the number of ■ and ■ initial bits in $A^{(0)}$ are usually unbalanced, e.g., in Qin *et al.*'s 4-round preimage attack on `Keccak-512` [56], the number of ■ and ■ initial bits are 216 and 16, respectively. Therefore, the cost to impose full conditions only for ■ is not much and also the total search space of the MILP model does not decrease much.

After the first θ and χ, the ■ bits propagate freely over other subsequent operations. For a given $d_{\mathcal{B}}$, we find that different sets of ■ have different diffusion properties. For example, two ■ sets of $d_{\mathcal{B}} = 10$, where the first θ and χ are

[6] In Qin *et al.*'s model [56], they assign full conditions for both ■ and ■ bits, and make the χ operation an identity on both the ■ and ■ bits

identity, one ■ set only propagates to 20 bits in $D^{(1)}$ in Figure 10, but the other ■ set propagates to 40 bits in Figure 11. We formulate some rules to choose the weak diffusion of ■ bits:

- `RULE-1`: Given $d_{\mathcal{B}}$, we minimize the number of ■ bits in $D^{(1)}$, which is defined as $\sigma_{\mathcal{B}}$, since the ■ in $D^{(1)}_{\{x,z\}}$ will affect all five bits in $\theta^{(1)}_{\{x,*,z\}}$. In fact, we try ■ sets with minimal and some sub-minimal $\sigma_{\mathcal{B}}$'s in our model.
- `RULE-2`: With $\sigma_{\mathcal{B}}$ determined by `RULE-1`, we hope there are more space to choose ■ sets. In $\pi^{(0)}$ of Figure 6, the adjacent bits of ■ can not be ■ to avoid the □ in $\chi^{(0)}$. So we want to maximize the number of ■ in $\pi^{(0)}_{\{0,1,*\}}$ and $\pi^{(0)}_{\{1,3,*\}}$, where their adjacent bits are always ■ due to the initial structure, and therefore give more freedom to assign ■ bits.

We build an easy program to solve the small optimization problem following `RULE-1` and `RULE-2`. For `Keccak`-512, setting $d_{\mathcal{B}} = 10$, the minimum value of $\sigma_{\mathcal{B}}$ is 18. We give a weak diffusion of ■ set in Figure 10 (sub-optimal choice). There are 20 ■ bits in $A^{(0)}$, due to the CP-kernel property, $d_{\mathcal{B}} = 10$. Then from $\pi^{(0)}$ to $A^{(1)}$, for each ■, we add two conditions to prevent it from propagating to other bits. At last, there are $\sigma_{\mathcal{B}} = 20$ ■ bits in $D^{(1)}$, and 8 ■ bits in $\pi^{(0)}_{\{0,1,*\}}$ and $\pi^{(0)}_{\{1,3,*\}}$. We also give a strong diffusion of ■ set in Figure 11 with $d_{\mathcal{B}} = 10$. Applying the CP-kernel property and compulsory conditions, there are $\sigma_{\mathcal{B}} = 40$ ■ bits in $D^{(1)}$ and 6 ■ bits in $\pi^{(0)}_{\{0,1,*\}}$ and $\pi^{(0)}_{\{1,3,*\}}$.

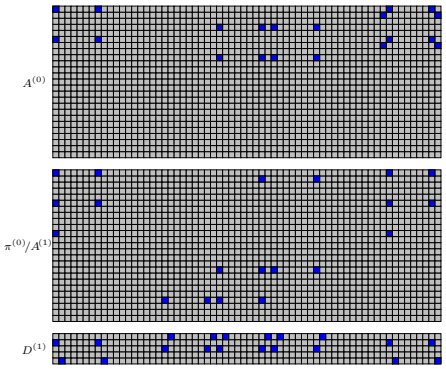

Fig. 10: A weak diffusion of ■ set

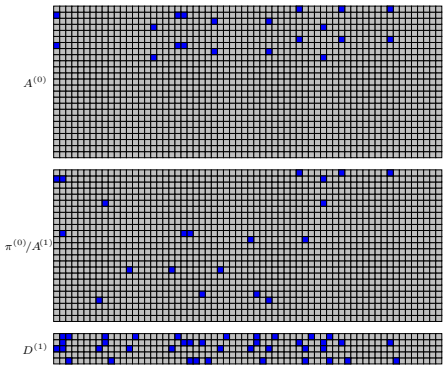

Fig. 11: A strong diffusion of ■ set

We introduce a two-stage approach to solve the MILP model:

1. Set the $d_{\mathcal{B}}$ for ■.
2. Search many sound configurations for ■ set with $d_{\mathcal{B}}$ following `RULE-1` and `RULE-2` with an easy program.
3. For different MILP models of MitM, fix the positions of ■ in $\pi^{(0)}$ with different configurations derived in Step 2, and run the MILP models independently with Gurobi until the MitM solutions are found.

4.3 The Collision Attack on 4-round Keccak-512

Applying our new MILP model and the two-stage search strategy, we mount a 4-round MitM collision attack on Keccak-512, as shown in Figure 12 (first part) and Figure 18 (second part in Supplementary Material B). The source code is in .... The consumed degrees of freedom of ■ bits are marked with ■/■, and the consumed degrees of freedom of ■ are marked with ■. We perform the collision attack with two message blocks (M_1, M_2) and place the MitM procedure in the 2nd block.

In the staring state $A^{(0)}$ of M_2, there are 20 ■ bits and 458 ■ bits. The ■ set follows the weak diffusion in Figure 10. Considering the initial structure in Figure 6, we introduce 239 Binary variables $v = \{v_0, v_1, \cdots, v_{238}\}$ and 239 Binary variables $c = \{c_0, c_1, \cdots, c_{238}\}$ to place at the $20 + 458 = 478$ ■ and ■ bits in $A^{(0)}$. For example, set $A^{(0)}_{\{0,0,0\}} = v_0$ and $A^{(0)}_{\{0,1,0\}} = v_0 \oplus c_0$ due to the CP-kernel property. That is, $\lambda_{\mathcal{R}} = 229$ and $\lambda_{\mathcal{B}} = 10$. After consuming 219 DoFs of ■ bits and 0 DoFs of ■ bits in the following operations, we have $d_{\mathcal{R}} = 10$ and $d_{\mathcal{B}} = 10$.

To reduce the diffusion of χ in round 0, we set 302 bit conditions in $\pi^{(0)}$, i.e. $\mu = 302$. With a given inner part, the 302 conditions on state $A^{(0)}$ can be regarded as a linear system of the $576 - 478 = 98$ ■ bits of outer part in M_2 and 239 Binary variables c. We compute the rank of the coefficient matrix of the linear system, which is 237. In other words, through some linear transformations, there are $302 - 237 = 65$ conditions out of the total 302 conditions only determined by the bits of inner part. So, we have to randomly test 2^{65} M_1 to compute an inner part satisfying the 65 conditions. Then for a right inner part, there are $2^{98+239-237} = 2^{100}$ solutions of M_2, which make all the 302 conditions hold. For each solution of M_2, the 98 ■ bits and 239 bits c in the outer part will be fixed. Following Observation 2, we get 10 matching equations as Equ. (19) in Supplementary Material B. One of the 10 matching equations is given as an example in Equ. (15):

$$\begin{aligned}\pi^{(3)}_{\{4,0,38\}} = A^{(3)}_{\{4,4,24\}} \oplus A^{(3)}_{\{3,0,24\}} \oplus A^{(r)}_{\{3,1,24\}} \oplus A^{(r)}_{\{3,2,24\}} \oplus A^{(r)}_{\{3,3,24\}} \oplus A^{(r)}_{\{3,4,24\}} \\ \oplus A^{(3)}_{\{0,0,23\}} \oplus A^{(3)}_{\{0,1,23\}} \oplus A^{(3)}_{\{0,2,23\}} \oplus A^{(3)}_{\{0,3,23\}} \oplus A^{(r)}_{\{0,4,23\}}.\end{aligned} \tag{15}$$

Our collision attack on 4-round Keccak-512 is given in Algorithm 1. In Line 1, by fixing $t = 10$ bits we derive $m = 10$ matching equations as Equ. (19). In each MitM episode between Line 13 to 20, we get $2^{10+10-10} = 2^{10}$ preimages that satisfy the $t = 10$ bits partial target. According to Equ. (3), we need $2^{(512-10)/2-10} = 2^{241}$ MitM episodes to build L. Assume 2^{ζ_1} possible values of M_1 are required and 2^{ζ_2} out of 2^{100} solutions of M_2 are required. Considering Line 8 and Line 11, there are 2^{ζ_2+219} MitM episodes, *i.e.*, $\zeta_2 = 22$. Therefore, we only need one right M_1 that satisfies the conditions in Line 4, *i.e.*, $\zeta_1 = 65$. The analysis of each step is given below:

– In Line 4, the time complexity is 2^{65} 4-round Keccak and $2^{65} \times 65$ simple operations to check if 65 conditions are satisfied.

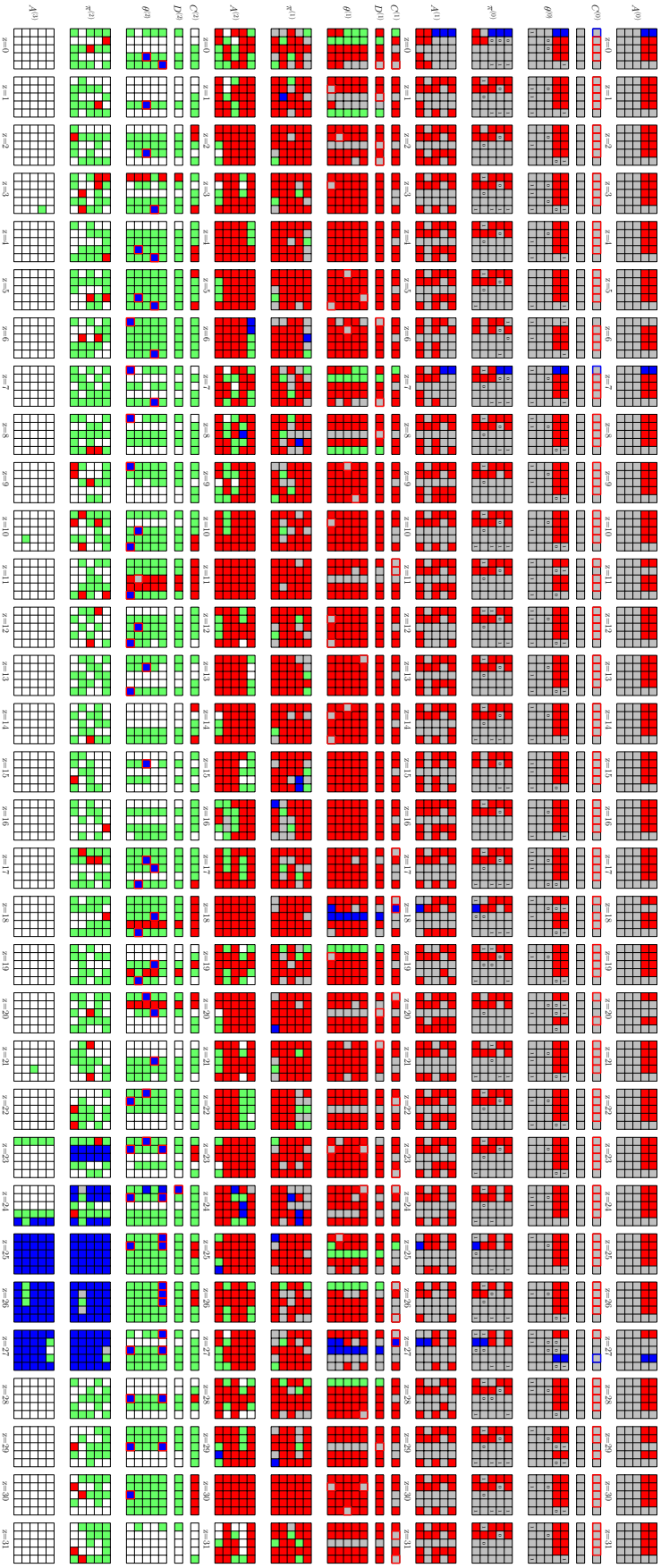

Fig. 12: The 4-round MitM collision attack on Keccak-512: Part 1

- In Line 7, the linear system is solved with time complexity of 302^3 bit operations to get 2^{100} solutions of M_2.
- In Line 10, the way to compute the matching point is borrowed from Qin *et al.* [56] to deal with ■ bits in the matching equations (15), which can be denoted as $f_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{B}} \oplus f_{\mathcal{G}} = 0$. $f_{\mathcal{R}}$ only contains monomials on ■/■ bits, $f_{\mathcal{B}}$ contains monomials on ■/■ bits, and $f_{\mathcal{G}}$ contains monomials on ■ bits and constants. We are going to compute the equation $f_{\mathcal{R}} = f_{\mathcal{B}} \oplus f_{\mathcal{G}}$ as filter. However, in $A^{(0)}$, there are $\lambda_{\mathcal{R}} = 229$ ■ variables, and $f_{\mathcal{B}}$ is actually changed with those 229 ■ variables. Given ■ and $c_{\mathcal{R}} \in \mathbb{F}_2^{219}$, for the 2^{10} values in $U[c_{\mathcal{R}}]$ and ■ neutral sets, $f_{\mathcal{R}}$ and $f_{\mathcal{B}}$ can be computed independently. We follow Qin *et al.*'s technique [56] to compute "$f_{\mathcal{R}} = f_{\mathcal{B}} \oplus f_{\mathcal{G}}$":
  1. Setting ■ in $A^{(0)}$ as 0, for each element of $U[c_{\mathcal{R}}]$, compute $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$.
  2. Randomly pick an element e of $U[c_{\mathcal{R}}]$ and set ■ in $A^{(0)}$ as 0, to compute $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$, where $Const(e)$ is determined by e.
  3. For ■ in $\mathbb{F}_2^{10}$, compute $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$ by setting the ■ $A^{(0)}$ bits as e. Therefore, get $f''_{\mathcal{M}} + f'''_{\mathcal{M}} = f_{\mathcal{B}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$ as filter.

  For detailed application, please refer to Line 10 to Line 17 of Algorithm 1. The time complexity of Line 10 is $2^{229+\zeta_2} \times \frac{3}{4} = 2^{250.58}$ 4-round `Keccak`, where the fraction $\frac{3}{4}$ means only 3-round `Keccak` is computed to get the matching point.
- In Line 12, the time complexity is $2^{22+219} \times \frac{3}{4} = 2^{240.58}$ 4-round `Keccak`.
- In Line 14, this step is just to retrieve $U[c_{\mathcal{R}}]$ to restore it in L_1 with matching point as index. Suppose one access to the table is equivalent to one Sbox application. The time complexity is $2^{22+219+10} \times \frac{1}{4\times 320} = 2^{240.67}$ 4-round `Keccak`, since there are 4×320 Sboxes for 4-round `Keccak`.
- In Line 17, the time complexity is $2^{22+219+10} \times \frac{3}{4} = 2^{250.58}$ 4-round `Keccak`.
- In Line 20, the time complexity is $2^{22+219+10} = 2^{251}$ 4-round `Keccak`.

The total time complexity is $2^{65} + 2^{65} \times 65 + 302^3 + 2^{250.58} + 2^{240.58} + 2^{240.67} + 2^{250.58} + 2^{251} = 2^{252.32}$ 4-round `Keccak`. The memory complexity is $2^{229} + 2^{251} \approx 2^{251}$ to store U and L.

4.4 New Preimage Attack on 4-round `Keccak-512`

We also build the MILP model for MitM preimage attack on `Keccak-512` following strategies in Section 4.2. The source code can be found in .... To further accelerate the searching, we use the symmetry to model the attack on small-size state instead of on large-size state. The symmetry of ciphers has already been studied in some previous works. In [53], Thomas Peyrin first studied the symmetry in the differential attacks, and invented the internal differential attacks. Bao et al. also exploited the symmetry of `AES`-like hashing to improve the MitM preimage attack [6]. For `Keccak`, Dinur *et al.* [24] used the symmetry of `Keccak` in z-axis to generate collisions with the formalized internal differential attacks. The rotational attack [50] on `Keccak` also utilised the symmetry of `Keccak` in z-axis. The states and most operations of `Keccak` have symmetric structures and parameters. Only the ι operation breaks it, which however does not affect the

Algorithm 1: Collision Attack on 4-round `Keccak-512`

Fix 10 bits of $\pi^{(3)}_{\{x,0,z\}}$ $(0 \le x \le 4, 0 \le z \le 63)$ in Equ. (19) to build the matching points
for 2^{ζ_1} *values of* M_1 **do**
  Compute the inner part of the 2nd block
  if *the 65 equations determined by the inner part are satisfied*
  `/* with probability of` 2^{-65} `*/`
  then
    Solve the system of 302 linear equations to get the 2^{100} solutions of M_2
    for *each of the* 2^{ζ_2} *solutions of* M_2 `/*` $\zeta_2 \le 100$ `*/`
    do
      Traversing the $2^{\lambda_{\mathcal{R}}} = 2^{229}$ values of ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine 219-bit ■/■ (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{219}$), and the 10-bit matching point in Equ. (19), *i.e.*, compute ten $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 229-bit ■ of $A^{(0)}$ as well as the 10-bit matching point in $U[c_{\mathcal{R}}]$.
      for $c_{\mathcal{R}} \in \mathbb{F}_2^{219}$ **do**
        Randomly pick a 229-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get ten $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
        for 2^{10} *values in* $U[c_{\mathcal{R}}]$ **do**
          Restore the values of ■ of $A^{(0)}$ and the corresponding matching point (*i.e.*, 10 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
        end
        for 2^{10} *values of* ■ **do**
          Set the 229-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 10 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by matching point.
        end
        for *values matched between* L_1 *and* L_2 **do**
          Compute the 512-bit target h from the matched ■ and ■ bits and store the (M_1, M_2, h) in L indexed by h
          if *the size of* L *is* $2^{(h-t)/2} = 2^{251}$ **then**
            Check L and return (M_1, M_2) and (M'_1, M'_2) with the same h
          end
        end
      end
    end
  end
end

color propagation in our MitM attack. For Keccak, the state of 64 slices can be viewed two 32 slices along the z-axis, where $A^{(0)}_{\{x,y,z\}} = A^{(0)}_{\{x,y,z+32\}}$. Applying the coloring rules over the operations of Keccak will not disturb the symmetry.

Finally, we obtain a new preimage attack on the 32 slices state version as Figure 19 in Supplementary Material C. The weak diffusion of ■ set over the 32 slices is also applied to accelerate the search. While setting $d_{\mathcal{B}} = 6$, the minimum value of $\sigma_{\mathcal{B}}$ is 12, which is used in our attack. While cloning the coloring pattern of the first 32 slices to the last 32 slices, we get an MitM preimage attack on the whole 64 slices state of Keccak-512. In total, the starting state $A^{(0)}$ contains 24 ■ bits and 424 ■ bits. We introduce 224 binary variables $v = \{v_0, v_1, \cdots, v_{223}\}$ and 224 binary variables $c = \{c_0, c_1, \cdots, c_{223}\}$. Those variables v_i's and c_i's are placed at the $24 + 424 = 448$ ■ and ■ bits in $A^{(0)}$. And then, we have $\lambda_{\mathcal{R}} = 212$ and $\lambda_{\mathcal{B}} = 12$. After consuming 200 DoFs of ■ bits and 0 DoFs of ■ bits in the following operations, we have $d_{\mathcal{R}} = 12$ and $d_{\mathcal{B}} = 12$. We derive $m = 12$ matching equations as Equ. (20) in Supplementary Material C.

The detailed 4-round preiamge attack on Keccak-512 is given in Algorithm 3 in Supplementary Material C. The time complexity is $2^{501.16}$ 4-round Keccak. The memory is 2^{212}.

4.5 The Preimage Attack on 4-round Keccak-384

Different from the weak-diffusion structure used in Figure 6 for Keccak-512, the weak-diffusion structure used for Keccak-384 is given in Figure 13, which covers 13 lanes, and the θ operation in the structure acts as identity with CP-kernel property. The variables $\{v_{0,z}, v_{1,z}, v_{2,z}, v_{3,z}, v_{4,z}, v_{5,z}, v_{6,z}, v_{7,z}\}$ $(0 \le z \le 63)$ are allocated in $A^{(0)}$ as

$$\begin{cases} A^{(0)}_{\{x,0,z\}} = v_{x,z},\ A^{(0)}_{\{x,1,z\}} = v_{x+5,z},\ A^{(0)}_{\{x,2,z\}} = v_{x,z} \oplus v_{x+5,z} \oplus c_{x,z},\ 0 \le x \le 2, \\ A^{(0)}_{\{x,0,z\}} = v_{x,z},\ A^{(0)}_{\{x,1,z\}} = v_{x,z} \oplus c_{x,z},\ 3 \le x \le 4, \end{cases}$$

where $c_{0,z}$, $c_{1,z}$, $c_{2,z}$, $c_{3,z}$, $c_{4,z}$ $(0 \le z \le 63)$ are constants. The constraints for the initial state $\pi^{(0)}$, the number of initial DoFs for ■ and ■ (*i.e.*, $\lambda_{\mathcal{B}}$ and $\lambda_{\mathcal{R}}$), and the conditions to control the diffusion over the χ operation, are slightly different from what we list for Keccak-512. We list the details in Supplementary Material D.1 for Keccak-384. The source code please refer to ....

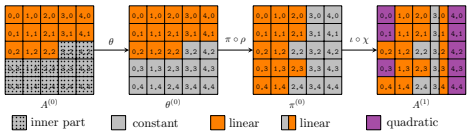

Fig. 13: The weak-diffusion structure of Keccak-384

Preimage Attack on 4-round `Keccak-384`. Searching with the MILP model, we find a 4-round MitM preimage attack on `Keccak-384` as shown in Figure 21 (first part) and Figure 22 (second part) in Supplementary Material D.2, where the DoFs of ■ and ■ in $A^{(0)}$ are 423 and 13, and there are totally 200 conditions on $\pi^{(0)}$.

Given an inner part, the 200 conditions on state $A^{(0)}$ will be a linear system of the $1600-384\times2-436 = 396$ variables of M_2, which will act as global parameters for the MitM episodes. We compute the rank of the coefficient matrix of the linear system, which is 192. In other words, through some linear transformations, there are $200 - 192 = 8$ equations only determined by the bits of inner part. We have to randomly test 2^8 M_1 to compute a right inner part satisfying the 8 equations. Then for a right inner part, there are $2^{396-192} = 2^{204}$ solutions of M_2, which make all the conditions hold. For each solution of M_2, the global variables in the outer part will be fixed. Then with the fixed inner part, we can conduct the MitM episodes to filter states.

Since only the first three columns contain ■ and ■ bits in $\pi^{(0)}$, $C^{(1)}_{\{x,z\}}$ with $x \in \{1,2,3\}$, $D^{(1)}_{\{2,z\}}$ with $0 \le z \le 63$, and $\theta^{(1)}_{\{2,y,z\}}$ with $0 \le y \le 4$ and $0 \le z \le 63$ will be linear on ■ and ■ in $A^{(0)}$. Totally, there are additionally 55 linear constraints of ■ bis in those $C^{(1)}_{\{x,z\}}$, $D^{(1)}_{\{2,z\}}$, and $\theta^{(1)}_{\{2,y,z\}}$ which consume 55 DoFs of ■ to let the bits be ■ or ■. Those constraints form a linear system of 55 equations on 423 ■ bits of $A^{(0)}$, and we list three examples of linear equations in Supplementary Material D.4. Besides the linear constraints for the ■ bits, there also are 354 nonlinear constraints of consume DoFs of ■ in Figure 21 and 22. Therefore, we get $d_{\mathcal{R}} = 423 - 55 - 354 = 14$ and $d_{\mathcal{B}} = 13$. The $m = 13$ matching equations are listed in Equ. (21) in Supplementary Material D.3.

We use two message blocks (M_1, M_2) to build the attack as Algorithm 2. For each MitM episode in Line 12 to 24, $2^{13}\times2^{14} = 2^{27}$ internal states are exhausted. In Line 10, for a given M_2, we can perform 2^{354} MitM episodes. To find a 384-bit target preimage, we need $2^{\zeta_1-8+\zeta_2+354+27} = 2^{384}$. We set $\zeta_1 = 8$ and $\zeta_2 = 3$, where we choose $2^{\zeta_1} = 2^8$ possible values of M_1 and $2^{\zeta_2} = 2^3$ solutions of M_2. The steps of Algorithm 2 are analyzed below:

- In Line 3, the time complexity is 2^8 4-round `Keccak` and $2^8 \times 200^3$ bit operations to solve the linear system (the time to solve a system of n linear equations is about $O(n^3)$).
- In Line 8, the time is $2^3 \times 55^3$ to solve linear system of 55 equations.
- In Line 9, the time is $2^{3+368} \times \frac{3}{4} = 2^{370.58}$ 4-round `Keccak` to build U.
- In Line 11, the time complexity is $2^{3+354} \times \frac{3}{4} = 2^{356.58}$ 4-round `Keccak`.
- In Line 13, this step is just to retrieve $U[c_{\mathcal{R}}]$ to restore it in L_1 with matching point as index. Suppose one access to the table is equivalent to one Sbox application. The time complexity is $2^{3+354+14} \times \frac{1}{4\times320} = 2^{360.67}$ 4-round `Keccak`, since there are 4×320 Sboxes for 4-round `Keccak`.
- In Line 16, the time complexity is $2^{3+354+13} \times \frac{3}{4} = 2^{369.58}$ 4-round `Keccak`.
- In Line 19, the time is $2^{3+354+14+13-13} \times \frac{3}{4} = 2^{370.58}$ 4-round `Keccak`.
- Line 23 is to check against the full target h, whose time complexity is $2^{3+354+14+13-13-307} = 2^{64}$ 4-round `Keccak`.

Algorithm 2: Preimage Attack on 4-round `Keccak-384`

Precompute inversely from the target to $\theta^{(3)}$
for 2^{ζ_1} *values of* M_1 **do**
  Compute the inner part of the 2nd block and solve the system of 200 linear equations
  if *the equations have solutions* `/* with probability of` 2^{-8} `*/`
  then
    for *each of the* 2^{ζ_2} *solutions of* M_2 `/*` $\zeta_2 \leq 204$ `*/`
    do
      Fix the 55 linear constraints on ■ as zero constants (e.g., fix $C^{(1)}_{\{1,11\}}$, $D^{(1)}_{\{2,5\}}$, $\theta^{(1)}_{\{2,3,2\}}$ in Supplementary Material D.4 as 0), and fix the ■ in $A^{(0)}$ as zero, then solve 55 linear equations to get $2^{423-55} = 2^{368}$ solutions for the ■ variables
      Traversing the 2^{368} values of ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine 354-bit ■/■ bits (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{354}$), and the 13-bit matching point, e.g., in Equ. (21), *i.e.*, compute thirteen $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 423-bit ■ bits of $A^{(0)}$ as well as the 13-bit matching point in $U[c_{\mathcal{R}}]$
      for $c_{\mathcal{R}} \in \mathbb{F}_2^{354}$ **do**
        Randomly pick a 423-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get 13 $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
        for 2^{14} *values in* $U[c_{\mathcal{R}}]$ **do**
          Restore the values of ■ of $A^{(0)}$ and the corresponding matching point (*i.e.*, 13 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
        end
        for 2^{13} *values of* ■ **do**
          Set the 423-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 13 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by matching point.
        end
        for *values matched between* L_1 *and* L_2 **do**
          Compute $\theta^{(3)}$ from the matched ■ and ■ bits
          if $\theta^{(3)}$ *satisfy the precomputed values*
          `/* Probability of` $2^{-(320-13)} = 2^{-307}$ `*/`
          then
            if *it leads to the given hash value* **then**
              Output the preimage
            end
          end
        end
      end
    end
  end
end

The total complexity is $2^{370.58}+2^{356.58}+2^{360.67}+2^{369.58}+2^{370.58}+2^{64} \approx 2^{371.9}$ 4-round Keccak. The memory to store U is 2^{368}.

Remark on padding rule. As the padding rule stated in Section 2.2, for Keccak the last message block has at least 2 padding bits, and for SHA3 there are 4 padding bits. In our MitM characteristics for Keccak-512 and Keccak-384 shown in Figures 12, 19 and 21, the bit positions of the 4 padding bits $A^{(0)}_{\{3,1,z\}}$ ($60 \le z \le 63$) are ■ bits, which can be fixed globally. The time and memory complexities will not change considering the 2 or 4 padding bits. Take the collision attack on Keccak-512 in Sect. 4.3 as an example. Since the rank of the linear system of the 302 conditions is unchanged considering the 2 or 4 padding bits to be constants, the value of ζ_1 keeps 65, where we test 2^{65} M_1 to get a right inner part. Then for the fixed right inner part, there are only 2^{98} or 2^{96} solutions of M_2 with 2 or 4 padding bits, respectively. Since we only need $2^{\zeta_2+219} = 2^{241}$ episodes, the number ζ_2 is 22, which is smaller than 98 or 96. So the time complexity is also $2^{252.32}$ for the collision attack on both Keccak-512 and SHA3-512.

5 Improved MitM Attacks on Xoodyak

We follow the MILP model for Xoodyak by Qin *et al.* [56], but exploit weak diffusion properties of the ■ set to speedup the search. For Xoodyak, the 128-bit message is located in the upper plane, i.e., $A^0_{\{*,2,*\}}$. There is only one ■ or ■ bit in each column at most, so the θ can not be identity. Assume that the DoFs of ■ bits don't consume in the computation. We hope the number of columns containing ■ bits in $\iota^{(0)}$ will be small, which is denoted by $\sigma_{\mathcal{B}}$. For example, let the initial DoFs of ■ be 8 and $d_{\mathcal{B}} = 8$. Figure 14(I) shows a weak diffusion with $\sigma_{\mathcal{B}} = 31$, while a strong diffusion has $\sigma_{\mathcal{B}} = 52$ in Figure 14(II). Since each column of $\iota^{(0)}$ is the input of an Sbox, the column involving ■ more likely produces □ once there also be ■. So applying the weak-diffusion ■ set likely leads to better results.

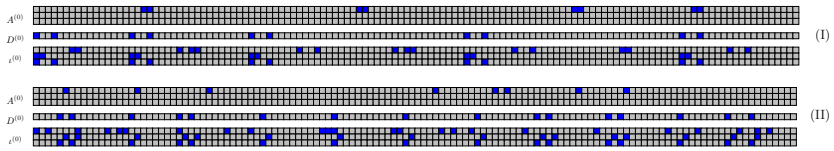

Fig. 14: A weak (I) and strong (II) diffusion of ■ set for Xoodyak

New MITM preimage attack on 3-round Xoodyak-XOF. Solving with the MILP model for Xoodyak with a weak diffusion as Figure 14(I), we get a new 3-round MITM preimage attack. The attack Figure 23 and other details are given in Supplementary Material E.1. The attack parameters are $\lambda_{\mathcal{R}} = 118$, $\lambda_{\mathcal{B}} = 8$, $d_{\mathcal{B}} = 8$, $d_{\mathcal{R}} = 118-111 = 7$, $\mu = 53$, $m = 7$. The time complexity of the 3-round preimage attack is $2^{121.77}$ 3-round Xoodyak-XOF, and the memory is 2^{118}.

Collision Attack on 3-round `Xoodyak-Hash`. The MitM characteristic on 3-round `Xoodyak-XOF` can also be used to build collision attack on `Xoodyak-Hash`, which is given in in Supplementary Material E.2. The time of the 3-round collision attack is $2^{125.52}$ 3-round `Xoodyak-Hash`, and the memory is $2^{124.51}$.

6 The MitM Collision and Preimage Attack on `Ascon-XOF`

The MILP model for `Ascon` follows Qin *et al.*'s model [56]. In order to speedup the model, we exploit the weak diffusion property of `Ascon`, and hope that for given $d_{\mathcal{B}}$, $A^{(1)}$ contains as few columns as possible that contain ■ bits. Let $\sigma_{\mathcal{B}}$ be the number of columns that contain ■ in $A^{(1)}$. For example, let the initial DoFs of ■ be 6, which are not consumed in the propagation, *i.e.*, $d_{\mathcal{B}} = 6$. Figure 15 shows a weak diffusion with $\sigma_{\mathcal{B}} = 16$, while a strong diffusion has $\sigma_{\mathcal{B}} = 49$ in Figure 16. In each Sbox of `Ascon`, if both ■ and ■ exist in the inputs, then there is a high probability that the Sbox outputs □. Therefore, a weak-diffusion ■ set naturally reduces the propagation of □.

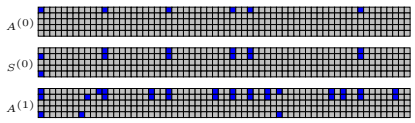

Fig. 15: A weak diffusion of ■ set

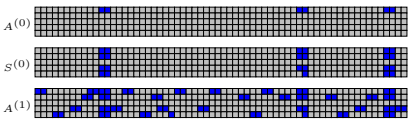

Fig. 16: A strong diffusion of ■ set

Improved Preimage Attack on 3-round `Ascon-XOF`. The improved 3-round preimage attack on `Ascon` is shown in Figure 24 and the details are given in Supplement Material F.1. For $d_{\mathcal{B}} = 14$, $\sigma_{\mathcal{B}} = 29$ for ■ set is a weak diffusion case. The attack parameters are $\lambda_{\mathcal{R}} = 30$, $\lambda_{\mathcal{B}} = d_{\mathcal{B}} = 14$, $d_{\mathcal{R}} = 30 - 16 = 14$, $\mu = 44$ and $m = t = 14$. The total time complexity is $2^{114.53}$ 3-round `Ascon`, and the memory is 2^{30}.

Collision Attack on 3-round `Ascon-Hash`. The MitM characteristic in Figure 24 on 3-round `Ascon-XOF` can also be used to build collision attack on `Ascon-Hash` (256-bit digest). We give the MitM collision attack on 3-round `Ascon-Hash` in Supplement Material F.2. The total time complexity is $2^{121.85}$ 3-round `Ascon` and the memory is 2^{121}.

Collision Attack on 4-round `Ascon-Hash`. The MitM characteristic on 4-round `Ascon-XOF` in [56] (see also in Figure 25 in Supplementary Material F.3) is used to build collision attack on `Ascon-Hash`, where $\lambda_{\mathcal{B}} = d_{\mathcal{B}} = 4$, $\lambda_{\mathcal{R}} = 54$, $d_{\mathcal{R}} = 54 - 50 = 4$, $m = t = 4$ and $\mu = 44$. We give the MitM collision attack on 4-round `Ascon-Hash` in Supplement Material F.3. The total time complexity is $2^{126.77}$ 4-round `Ascon` and the memory is 2^{126}.

7 Conclusion

In this paper, we extend the MitM attack framework on sponge-based hashing in [56] into the collision attack. Exploiting various techniques, we enrich the automatic tools for both MitM preimage and collision attacks. As applications, we apply those automatic tools to the U.S. NIST standard `SHA-3` (`Keccak`), `Ascon` (a new NIST standard for lightweight applications), and `Xoodyak`. For `Keccak`, we give the first collision attack on 4-round `Keccak-512`. We also give improved preimage attacks on 4-round `Keccak-512` and `Keccak-384`. For round-reduced `Xoodyak` and `Ascon`, we find collision attacks with 1-2 more rounds than before, and improve the complexities of the preimage attacks.

References

1. Dor Amzaleg and Itai Dinur. Refined cryptanalysis of the GPRS ciphers GEA-1 and GEA-2. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Proceedings, Part III*, volume 13277 of *LNCS*, pages 57–85. Springer, 2022.
2. Kazumaro Aoki, Jian Guo, Krystian Matusiewicz, Yu Sasaki, and Lei Wang. Preimages for step-reduced SHA-2. In Mitsuru Matsui, editor, *ASIACRYPT 2009, Proceedings*, volume 5912 of *LNCS*, pages 578–597. Springer, 2009.
3. Kazumaro Aoki and Yu Sasaki. Preimage attacks on one-block MD4, 63-step MD5 and more. In *SAC 2008*, volume 5381, pages 103–119. Springer, 2008.
4. Jean-Philippe Aumasson, Willi Meier, and Florian Mendel. Preimage attacks on 3-pass HAVAL and step-reduced MD5. In *SAC 2008*, volume 5381, pages 120–135.
5. Zhenzhen Bao, Xiaoyang Dong, Jian Guo, Zheng Li, Danping Shi, Siwei Sun, and Xiaoyun Wang. Automatic search of meet-in-the-middle preimage attacks on AES-like hashing. In *EUROCRYPT 2021, Part I*, volume 12696, pages 771–804.
6. Zhenzhen Bao, Jian Guo, Danping Shi, and Yi Tu. Superposition meet-in-the-middle attacks: Updates on fundamental security of AES-like hashing. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Proceedings, Part I*, volume 13507 of *LNCS*, pages 64–93. Springer, 2022.
7. Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Schwaemm and Esch: lightweight authenticated encryption and hashing using the Sparkle permutation family. *NIST Lightweight Cryptography*, 2019.
8. Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes. Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2. In *EUROCRYPT 2021, Proceedings, Part II*, volume 12697, pages 155–183. Springer, 2021.
9. Daniel J. Bernstein. Second preimages for 6 (7?(8??)) rounds of Keccak. *NIST mailing list*, 2010.
10. Daniel J Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, and Peter Schwabe. SPHINCS+: Submission to the NIST post-quantum project. 2017.
11. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak sponge function family main document. *Submission to NIST*, 3(30):320–337, 2009.

12. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In *ASIACRYPT 2011, Proceedings*, pages 344–371.
13. Andrey Bogdanov and Christian Rechberger. A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN. In *SAC 2010*, volume 6544, pages 229–240. Springer, 2010.
14. Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque. Automatic search of attacks on round-reduced AES and applications. In *CRYPTO 2011, Proceedings*, volume 6841, pages 169–187. Springer, 2011.
15. Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, and María Naya-Plasencia. Differential meet-in-the-middle cryptanalysis. *ePrint 2022/1640*.
16. Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière. Sieve-in-the-middle: Improved MITM attacks. In *CRYPTO 2013, Proceedings, Part I*, pages 222–240.
17. Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Xoodyak, a lightweight cryptographic scheme. *IACR Trans. Symmetric Cryptol.*, 2020(S1):60–87, 2020.
18. Ivan Damgård. A design principle for hash functions. In *CRYPTO '89*, pages 416–427.
19. Patrick Derbez and Pierre-Alain Fouque. Automatic search of meet-in-the-middle and impossible differential attacks. In *CRYPTO 2016, Proceedings, Part II*, volume 9815, pages 157–184. Springer, 2016.
20. Whitfield Diffie and Martin E. Hellman. Special feature exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, 10(6):74–84, 1977.
21. Itai Dinur. Cryptanalytic applications of the polynomial method for solving multivariate equation systems over GF(2). In *EUROCRYPT 2021, Proceedings, Part I*, volume 12696, pages 374–403. Springer, 2021.
22. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Efficient dissection of composite problems, with applications to cryptanalysis, knapsacks, and combinatorial search problems. In *CRYPTO 2012*, volume 7417, pages 719–740.
23. Itai Dinur, Orr Dunkelman, and Adi Shamir. New attacks on Keccak-224 and Keccak-256. In Anne Canteaut, editor, *FSE 2012*, volume 7549, pages 442–461.
24. Itai Dinur, Orr Dunkelman, and Adi Shamir. Collision attacks on up to 5 rounds of SHA-3 using generalized internal differentials. In *FSE 2013*, volume 8424, pages 219–240. Springer, 2013.
25. Itai Dinur, Orr Dunkelman, and Adi Shamir. Improved practical attacks on round-reduced Keccak. *J. Cryptol.*, 27(2):183–209, 2014.
26. Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michal Straus. Cube attacks and cube-attack-like cryptanalysis on the round-reduced Keccak sponge function. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Proceedings, Part I*, volume 9056, pages 733–761. Springer, 2015.
27. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.*, 34(3):33, 2021.
28. Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, and Lei Hu. Meet-in-the-middle attacks revisited: Key-recovery, collision, and preimage attacks. In *CRYPTO 2021, Proceedings, Part III*, volume 12827, pages 278–308. Springer.
29. Orr Dunkelman, Gautham Sekar, and Bart Preneel. Improved meet-in-the-middle attacks on reduced-round DES. In *INDOCRYPT 2007, Proceedings*, volume 4859, pages 86–100. Springer, 2007.
30. Thomas Espitau, Pierre-Alain Fouque, and Pierre Karpman. Higher-order differential meet-in-the-middle preimage attacks on SHA-1 and BLAKE. In *CRYPTO 2015, Proceedings, Part I*, volume 9215, pages 683–701. Springer, 2015.

31. Thomas Fuhr and Brice Minaud. Match box meet-in-the-middle attack against KATAN. In *FSE 2014*, pages 61–81, 2014.
32. David Gérault, Thomas Peyrin, and Quan Quan Tan. Exploring differential-based distinguishers and forgeries for ASCON. *IACR Trans. Symmetric Cryptol.*, 2021(3):102–136, 2021.
33. Jian Guo, Guohong Liao, Guozhen Liu, Meicheng Liu, Kexin Qiao, and Ling Song. Practical collision attacks against round-reduced SHA-3. *J. Cryptol.*, 33(1):228–270, 2020.
34. Jian Guo, San Ling, Christian Rechberger, and Huaxiong Wang. Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. In *ASIACRYPT 2010, Proceedings*, volume 6477, pages 56–75.
35. Jian Guo, Guozhen Liu, Ling Song, and Yi Tu. Exploring SAT for cryptanalysis: (quantum) collision attacks against 6-round SHA-3. *ePrint 2022/184*.
36. Jian Guo, Meicheng Liu, and Ling Song. Linear structures: Applications to cryptanalysis of round-reduced Keccak. In *ASIACRYPT 2016, Proceedings, Part I*, volume 10031, pages 249–274, 2016.
37. Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *CRYPTO 2011, Proceedings*, volume 6841 of *LNCS*, pages 222–239. Springer, 2011.
38. Le He, Xiaoen Lin, and Hongbo Yu. Improved preimage attacks on round-reduced Keccak-384/512 via restricted linear structures. Cryptol. ePrint Arch., 2022/788.
39. Sebastiaan Indesteege, Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel. A practical attack on KeeLoq. In *EUROCRYPT 2008, Proceedings*, volume 4965, pages 1–18. Springer, 2008.
40. Takanori Isobe. A single-key attack on the full GOST block cipher. *J. Cryptol.*, 26(1):172–189, 2013.
41. Dmitry Khovratovich, Gaëtan Leurent, and Christian Rechberger. Narrow-bicliques: Cryptanalysis of full IDEA. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012, Proceedings*, volume 7237, pages 392–410.
42. Simon Knellwolf and Dmitry Khovratovich. New preimage attacks against reduced SHA-1. In *CRYPTO 2012, Proceedings*, volume 7417, pages 367–383.
43. Rajendra Kumar, Nikhil Mittal, and Shashank Singh. Cryptanalysis of 2 round Keccak-384. In *INDOCRYPT 2018, Proceedings*, volume 11356, pages 120–133.
44. Gaëtan Leurent. MD4 is not one-way. In *FSE 2008*, volume 5086, pages 412–428.
45. Ji Li, Takanori Isobe, and Kyoji Shibutani. Converting meet-in-the-middle preimage attack into pseudo collision attack: Application to SHA-2. In Anne Canteaut, editor, *FSE 2012*, volume 7549, pages 264–286. Springer, 2012.
46. Ting Li and Yao Sun. Preimage attacks on round-reduced Keccak-224/256 via an allocating approach. In *EUROCRYPT 2019, Proceedings, Part III*, volume 11478, pages 556–584. Springer, 2019.
47. Fukang Liu, Takanori Isobe, Willi Meier, and Zhonghao Yang. Algebraic attacks on round-reduced Keccak. In *ACISP 2021, Proceedings*, volume 13083, pages 91–110.
48. Guozhen Liu, Jingwen Lu, Huina Li, Peng Tang, and Weidong Qiu. Preimage attacks against lightweight scheme Xoodyak based on deep learning. In *Future of Information and Communication Conference*, pages 637–648. Springer, 2021.
49. Ralph C. Merkle. A certified digital signature. In *CRYPTO 1989, Proceedings*, pages 218–238, 1989.
50. Pawel Morawiecki, Josef Pieprzyk, and Marian Srebrny. Rotational cryptanalysis of round-reduced Keccak. In *FSE 2013,*, volume 8424, pages 241–262.
51. María Naya-Plasencia, Andrea Röck, and Willi Meier. Practical analysis of reduced-round Keccak. In *INDOCRYPT 2011*, volume 7107, pages 236–254.

52. The U.S. National Institute of Standards and Technology. SHA-3 standard: Permutation-based hash and extendable-output functions. *Federal Information Processing Standard, FIPS 202, 5th August 2015.*
53. Thomas Peyrin. Improved differential attacks for ECHO and Grøstl. In *CRYPTO 2010, Proceedings*, volume 6223, pages 370–392. Springer, 2010.
54. Bart Preneel, René Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: A synthetic approach. In *CRYPTO '93*, volume 773, pages 368–378.
55. Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo. New collision attacks on round-reduced Keccak. In *EUROCRYPT 2017, Proceedings, Part III*, volume 10212, pages 216–243, 2017.
56. Lingyue Qin, Jialiang Hua, Xiaoyang Dong, Hailun Yan, and Xiaoyun Wang. Meet-in-the-middle preimage attacks on sponge-based hashing. *ePrint 2022/1714.*
57. Mahesh Sreekumar Rajasree. Cryptanalysis of round-reduced Keccak using non-linear structures. In *INDOCRYPT 2019*, volume 11898, pages 175–192.
58. Yu Sasaki. Integer linear programming for three-subset meet-in-the-middle attacks: Application to GIFT. In *IWSEC 2018*, volume 11049, pages 227–243.
59. Yu Sasaki and Kazumaro Aoki. Finding preimages in full MD5 faster than exhaustive search. In *EUROCRYPT 2009, Proceedings*, volume 5479, pages 134–152.
60. Yu Sasaki and Kazumaro Aoki. Preimage attacks on 3, 4, and 5-pass HAVAL. In *ASIACRYPT 2008, Proceedings*, volume 5350, pages 253–271. Springer, 2008.
61. André Schrottenloher and Marc Stevens. Simplified MITM modeling for permutations: New (quantum) attacks. In *CRYPTO 2022, Proceedings, Part III*, volume 13509, pages 717–747. Springer, 2022.
62. Ling Song, Guohong Liao, and Jian Guo. Non-full sbox linearization: Applications to collision attacks on round-reduced Keccak. In *CRYPTO 2017, Proceedings, Part II*, volume 10402, pages 428–451. Springer, 2017.
63. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In *CRYPTO 2005, Proceedings*, volume 3621, pages 17–36. Springer, 2005.
64. Xiaoyun Wang and Hongbo Yu. How to break MD5 and other hash functions. In *EUROCRYPT 2005, Proceedings*, volume 3494, pages 19–35. Springer, 2005.
65. Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. Collision attacks on round-reduced Gimli-Hash/Ascon-Xof/Ascon-Hash. *Cryptol. ePrint Arch., Paper 2019/111.*

Supplementary Material

A Specifications on Ascon and Xoodyak

A.1 The Ascon family

The Ascon family [27] includes the hash functions Ascon-Hash and Ascon-Hasha as well as the extendable output functions Ascon-XOF and Ascon-XOFa with sponge-based modes of operations. The inner permutation applies 12 round functions to a 320-bit state. Denote $A^{(r)}_{\{x,y\}}$ as the bit located in the x-th column ($0 \le x \le 63$) and the y-th row ($0 \le y \le 4$) in round $r \ge 0$. For simplicity, all the coordinates are considered modulo 64 for x and modulo 5 for y. The round function consists of three operations $p_L \circ p_S \circ p_C$. Denote the internal states of round r as $A^{(r)} \xrightarrow{p_S \circ p_C} S^{(r)} \xrightarrow{p_L} A^{(r+1)}$. The operations in each round are

$$
\begin{aligned}
p_C:&\ A^{(r)}_{\{x,2\}} = A^{(r)}_{\{x,2\}} \oplus RC_r, \text{ where } RC_r \text{ is round-dependent constant,}\\
p_S:&\ S^{(r)}_{\{x,*\}} = \mathrm{Sbox}(A^{(r)}_{\{x,*\}}), \text{ where Sbox is the nonlinear substitution operation,}\\
p_L:&\ A^{(r+1)}_{\{x,y\}} \leftarrow S^{(r)}_{\{x,y\}} \oplus S^{(r)}_{\{x-\gamma_1[y],y\}} \oplus S^{(r)}_{\{x-\gamma_2[y],y\}},
\end{aligned}
$$

where $\gamma_1 = [19, 61, 1, 10, 7]$ and $\gamma_2 = [28, 39, 6, 17, 41]$. Assume the Sbox maps $(a_0, a_1, a_2, a_3, a_4) \in \mathbb{F}_2^5$ to $(b_0, b_1, b_2, b_3, b_4) \in \mathbb{F}_2^5$, where a_0 is the most significant bit. We list the algebraic normal form (ANF) of the Sbox as follows:

$$
\begin{aligned}
b_0 &= a_4a_1 + a_3 + a_2a_1 + a_2 + a_1a_0 + a_1 + a_0,\\
b_1 &= a_4 + a_3a_2 + a_3a_1 + a_3 + a_2a_1 + a_2 + a_1 + a_0,\\
b_2 &= a_4a_3 + a_4 + a_2 + a_1 + 1,\\
b_3 &= a_4a_0 + a_4 + a_3a_0 + a_3 + a_2 + a_1 + a_0,\\
b_4 &= a_4a_1 + a_4 + a_3 + a_1a_0 + a_1.
\end{aligned} \tag{16}
$$

We focus on the analysis of Ascon-Hash and Ascon-XOF, where $b = 320$ and $r = 64$. For Ascon-Hash, the output size is 256 bits, and the security claim is 2^{128} against preimage and collision attacks. For Ascon-XOF, the output can be of arbitrary length l and the security claim against the preimage attack is $\min(2^{128}, 2^l)$. In this paper, we target on Ascon-Hash with 256-bit hash against the collision attack, and Ascon-XOF with 128-bit hash against preimage attack.

A.2 The Xoodyak and Xoodoo permutation

The Xoodyak [17] has a 384-bit state shown in Figure 17. The $A^{(r)}_{\{x,y,z\}}$ is denoted the bit located at the x-th column, y-th row , and z-th lane in the round r, where $0 \le x \le 3,\ 0 \le y \le 2,\ 0 \le z \le 31$. All the coordinates are of modulo 4 for x, modulo 3 for y, and modulo 32 for z. The inner Xoodoo permutation consists of

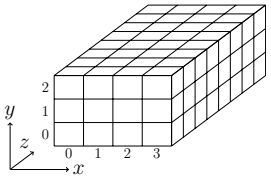

Fig. 17: Toy version of the Xoodoo state. The order in y is opposite to Keccak

12-round function. Denote the internal states of the round r as $A^{(r)} \xrightarrow{\theta} \theta^{(r)} \xrightarrow{\rho_{\text{west}}} \rho^{(r)} \xrightarrow{\iota} \iota^{(r)} \xrightarrow{\chi} \chi^{(r)} \xrightarrow{\rho_{\text{east}}} A^{(r+1)}$, where

$$\theta:\ \theta^{(r)}_{\{x,y,z\}} = A^{(r)}_{\{x,y,z\}} \oplus D^{(r)}_{\{x,z\}}, D^{(r)}_{\{x,z\}} = D^{(r)}_{\{x-1,z-5\}} \oplus D^{(r)}_{\{x-1,z-14\}}, C^{(r)}_{\{x,z\}} = \sum\nolimits_{y'=0}^{2} A^{(r)}_{\{x,y',z\}},$$
$$\rho_{\text{west}}:\ \rho^{(r)}_{\{x,0,z\}} = \theta^{(r)}_{\{x,0,z\}},\ \rho^{(r)}_{\{x,1,z\}} = \theta^{(r)}_{\{x-1,1,z\}},\ \rho^{(r)}_{\{x,2,z\}} = \theta^{(r)}_{\{x,2,z-11\}},$$
$$\iota:\ \iota^{(r)}_{\{0,0,z\}} = \rho^{(r)}_{\{0,0,z\}} \oplus RC_r,\ \text{where } RC_r \text{ is round-dependent constant},$$
$$\chi:\ \chi^{(r)}_{\{x,y,z\}} = \iota^{(r)}_{\{x,y,z\}} \oplus (\iota^{(r)}_{\{x,y+1,z\}} \oplus 1) \cdot \iota^{(r)}_{\{x,y+2,z\}},$$
$$\rho_{\text{east}}:\ A^{(r+1)}_{\{x,0,z\}} = \chi^{(r)}_{\{x,0,z\}},\ A^{(r+1)}_{\{x,1,z\}} = \chi^{(r)}_{\{x,1,z-1\}},\ A^{(r+1)}_{\{x,2,z\}} = \chi^{(r)}_{\{x-2,2,z-8\}}.$$

We focus on Xoodyak-XOF and Xoodyak-Hash, where $b = 384$ and $r = 128$. The Xoodyak-XOF offers an arbitrary output length l and the preimage resistance is $\min(2^{128}, 2^l)$. For Xoodyak-Hash, the output size is 256 bits, and the security claim is 2^{128} against preimage and collision attacks. We target on Xoodyak-XOF with output of 128-bit hash against the preimage attack, and Xoodyak-Hash with output of 256-bit hash against the collision attack.

B Parameters of the Collision Attack on 4-round Keccak-512

The offset $\gamma[x, y]$ in Keccak round function is given in Table 2.

	$x=0$	$x=1$	$x=2$	$x=3$	$x=4$
$y=0$	0	1	62	28	27
$y=1$	36	44	6	55	20
$y=2$	3	10	43	25	39
$y=3$	41	45	15	21	8
$y=4$	18	2	61	56	14

Table 2: The offset $\gamma[x, y]$ in the ρ operation for Keccak

The linear constraints for modelling the color of $\chi^{(0)}_{\{4,y,z\}}$ with conditions are given as following Equ. (17):

$$\begin{cases} \chi^{(0)}_{\{4,y,z\}}[0] \geq \pi^{(0)}_{\{0,y,z\}}[0] + \pi^{(0)}_{\{1,y,z\}}[0] - 1, \\ \chi^{(0)}_{\{4,y,z\}}[2] \geq \pi^{(0)}_{\{0,y,z\}}[2] + \pi^{(0)}_{\{1,y,z\}}[2] - 1, \\ \texttt{Cond}_{\{0,y,z\}} \geq \chi^{(0)}_{\{4,y,z\}}[0] + \chi^{(0)}_{\{4,y,z\}}[2] - \pi^{(0)}_{\{1,y,z\}}[0] - \pi^{(0)}_{\{1,y,z\}}[2], \\ \texttt{Cond}_{\{1,y,z\}} \geq \chi^{(0)}_{\{4,y,z\}}[0] + \chi^{(0)}_{\{4,y,z\}}[2] - \pi^{(0)}_{\{0,y,z\}}[0] - \pi^{(0)}_{\{0,y,z\}}[2], \\ \texttt{Cond}_{\{0,y,z\}} + \texttt{Cond}_{\{1,y,z\}} \leq \chi^{(0)}_{\{4,y,z\}}[0] + \chi^{(0)}_{\{4,y,z\}}[2] - 1, \\ \texttt{Cond}_{\{0,y,z\}} + \texttt{Cond}_{\{1,y,z\}} \leq \sum_{l=0,2} \chi^{(0)}_{\{4,y,z\}}[l] - \sum_{l=0,2} \pi^{(0)}_{\{0,y,z\}}[l] - \sum_{l=0,2} \pi^{(0)}_{\{1,y,z\}}[l] + 2. \end{cases} \tag{17}$$

The linear constraints for modelling the color of $\chi^{(0)}_{\{0,y,z\}}$ with conditions are given as Equ. (18):

$$\begin{cases} \chi^{(0)}_{\{0,y,z\}}[0] \leq \pi^{(0)}_{\{0,y,z\}}[0], \ \chi^{(0)}_{\{0,y,z\}}[2] \leq \pi^{(0)}_{\{0,y,z\}}[2], \\ \chi^{(0)}_{\{0,y,z\}}[2] \geq \pi^{(0)}_{\{0,y,z\}}[2] + \pi^{(0)}_{\{1,y,z\}}[2] - 1, \\ \texttt{Cond}_{\{2,y,z\}} \geq \chi^{(0)}_{\{0,y,z\}}[2] - \pi^{(0)}_{\{1,y,z\}}[2], \\ \texttt{Cond}_{\{2,y,z\}} \geq \chi^{(0)}_{\{0,y,z\}}[0] + \chi^{(0)}_{\{0,y,z\}}[2] - \pi^{(0)}_{\{1,y,z\}}[0] - \pi^{(0)}_{\{1,y,z\}}[2], \\ \texttt{Cond}_{\{2,y,z\}} \leq \chi^{(0)}_{\{0,y,z\}}[0] + \chi^{(0)}_{\{1,y,z\}}[2] - 1, \\ \texttt{Cond}_{\{2,y,z\}} \leq \sum_{l=0,2} \chi^{(0)}_{\{0,y,z\}}[l] - \sum_{l=0,2} \pi^{(0)}_{\{0,y,z\}}[l] - \sum_{l=0,2} \pi^{(0)}_{\{1,y,z\}}[l] + 2. \end{cases} \tag{18}$$

The ten matching equations in the collision attack on 4-round `Keccak-512` are given in Equ. (19):

$$\begin{aligned} \pi^{(3)}_{\{4,0,38\}} &= A^{(3)}_{\{4,4,24\}} \oplus A^{(3)}_{\{3,0,24\}} \oplus A^{(r)}_{\{3,1,24\}} \oplus A^{(r)}_{\{3,2,24\}} \oplus A^{(r)}_{\{3,3,24\}} \oplus A^{(r)}_{\{3,4,24\}} \\ &\quad \oplus A^{(3)}_{\{0,0,23\}} \oplus A^{(3)}_{\{0,1,23\}} \oplus A^{(3)}_{\{0,2,23\}} \oplus A^{(3)}_{\{0,3,23\}} \oplus A^{(r)}_{\{0,4,23\}}, \\ \pi^{(3)}_{\{2,0,4\}} &= A^{(3)}_{\{2,2,25\}} \oplus A^{(3)}_{\{1,0,25\}} \oplus A^{(r)}_{\{1,1,25\}} \oplus A^{(r)}_{\{1,2,25\}} \oplus A^{(r)}_{\{1,3,25\}} \oplus A^{(r)}_{\{1,4,25\}} \\ &\quad \oplus A^{(3)}_{\{3,0,24\}} \oplus A^{(3)}_{\{3,1,24\}} \oplus A^{(3)}_{\{3,2,24\}} \oplus A^{(3)}_{\{3,3,24\}} \oplus A^{(r)}_{\{3,4,24\}}, \\ \pi^{(3)}_{\{3,0,46\}} &= A^{(3)}_{\{3,3,25\}} \oplus A^{(3)}_{\{2,0,25\}} \oplus A^{(r)}_{\{2,1,25\}} \oplus A^{(r)}_{\{2,2,25\}} \oplus A^{(r)}_{\{2,3,25\}} \oplus A^{(r)}_{\{2,4,25\}} \\ &\quad \oplus A^{(3)}_{\{4,0,24\}} \oplus A^{(3)}_{\{4,1,24\}} \oplus A^{(3)}_{\{4,2,24\}} \oplus A^{(3)}_{\{4,3,24\}} \oplus A^{(r)}_{\{4,4,24\}}, \\ \pi^{(3)}_{\{1,0,6\}} &= A^{(3)}_{\{1,1,26\}} \oplus A^{(3)}_{\{0,0,26\}} \oplus A^{(r)}_{\{0,1,26\}} \oplus A^{(r)}_{\{0,2,26\}} \oplus A^{(r)}_{\{0,3,26\}} \oplus A^{(r)}_{\{0,4,26\}} \\ &\quad \oplus A^{(3)}_{\{2,0,25\}} \oplus A^{(3)}_{\{2,1,25\}} \oplus A^{(3)}_{\{2,2,25\}} \oplus A^{(3)}_{\{2,3,25\}} \oplus A^{(r)}_{\{2,4,25\}}, \\ \pi^{(3)}_{\{2,0,5\}} &= A^{(3)}_{\{2,2,26\}} \oplus A^{(3)}_{\{1,0,26\}} \oplus A^{(r)}_{\{1,1,26\}} \oplus A^{(r)}_{\{1,2,26\}} \oplus A^{(r)}_{\{1,3,26\}} \oplus A^{(r)}_{\{1,4,26\}} \\ &\quad \oplus A^{(3)}_{\{3,0,25\}} \oplus A^{(3)}_{\{3,1,25\}} \oplus A^{(3)}_{\{3,2,25\}} \oplus A^{(3)}_{\{3,3,25\}} \oplus A^{(r)}_{\{3,4,25\}}, \\ \pi^{(3)}_{\{3,0,47\}} &= A^{(3)}_{\{3,3,26\}} \oplus A^{(3)}_{\{2,0,26\}} \oplus A^{(r)}_{\{2,1,26\}} \oplus A^{(r)}_{\{2,2,26\}} \oplus A^{(r)}_{\{2,3,26\}} \oplus A^{(r)}_{\{2,4,26\}} \end{aligned}$$

$$
\begin{aligned}
&\oplus A^{(3)}_{\{4,0,25\}} \oplus A^{(3)}_{\{4,1,25\}} \oplus A^{(3)}_{\{4,2,25\}} \oplus A^{(3)}_{\{4,3,25\}} \oplus A^{(r)}_{\{4,4,25\}},\\
\pi^{(3)}_{\{0,0,27\}} = A^{(3)}_{\{0,0,27\}} &\oplus A^{(3)}_{\{4,0,27\}} \oplus A^{(r)}_{\{4,1,27\}} \oplus A^{(r)}_{\{4,2,27\}} \oplus A^{(r)}_{\{4,3,27\}} \oplus A^{(r)}_{\{4,4,27\}}\\
&\oplus A^{(3)}_{\{1,0,26\}} \oplus A^{(3)}_{\{1,1,26\}} \oplus A^{(3)}_{\{1,2,26\}} \oplus A^{(3)}_{\{1,3,26\}} \oplus A^{(r)}_{\{1,4,26\}},\\
\pi^{(3)}_{\{1,0,6\}} = A^{(3)}_{\{1,1,27\}} &\oplus A^{(3)}_{\{0,0,27\}} \oplus A^{(r)}_{\{0,1,27\}} \oplus A^{(r)}_{\{0,2,27\}} \oplus A^{(r)}_{\{0,3,27\}} \oplus A^{(r)}_{\{0,4,27\}}\\
&\oplus A^{(3)}_{\{2,0,26\}} \oplus A^{(3)}_{\{2,1,26\}} \oplus A^{(3)}_{\{2,2,26\}} \oplus A^{(3)}_{\{2,3,26\}} \oplus A^{(r)}_{\{2,4,26\}},\\
\pi^{(3)}_{\{2,0,6\}} = A^{(3)}_{\{2,2,27\}} &\oplus A^{(3)}_{\{1,0,27\}} \oplus A^{(r)}_{\{1,1,27\}} \oplus A^{(r)}_{\{1,2,27\}} \oplus A^{(r)}_{\{1,3,27\}} \oplus A^{(r)}_{\{1,4,27\}}\\
&\oplus A^{(3)}_{\{3,0,26\}} \oplus A^{(3)}_{\{3,1,26\}} \oplus A^{(3)}_{\{3,2,26\}} \oplus A^{(3)}_{\{3,3,26\}} \oplus A^{(r)}_{\{3,4,26\}},\\
\pi^{(3)}_{\{4,0,41\}} = A^{(3)}_{\{4,4,27\}} &\oplus A^{(3)}_{\{3,0,27\}} \oplus A^{(r)}_{\{3,1,27\}} \oplus A^{(r)}_{\{3,2,27\}} \oplus A^{(r)}_{\{3,3,27\}} \oplus A^{(r)}_{\{3,4,27\}}\\
&\oplus A^{(3)}_{\{0,0,26\}} \oplus A^{(3)}_{\{0,1,26\}} \oplus A^{(3)}_{\{0,2,26\}} \oplus A^{(3)}_{\{0,3,26\}} \oplus A^{(r)}_{\{0,4,26\}}.
\end{aligned}
\tag{19}
$$

The second part of the figure of the 4-round MitM collision attack on `Keccak-512` is given in Figure 18.

C Detailed Preimage Attack on 4-round `Keccak-512`

The new preimage attack on the 32 slices state version is given as Figure 19. The 12 matching equations in the preimage attack on 4-round `Keccak-512` are given in Equ. (20).

$$
\begin{cases}
A^{(3)}_{\{3,0,52\}} \oplus A^{(3)}_{\{3,3,52\}} \oplus (A^{(4)}_{\{1,1,16\}} \oplus 1) \cdot (A^{(3)}_{\{0,2,13\}} \oplus A^{(3)}_{\{0,0,13\}}) = A^{(4)}_{\{0,1,16\}} \oplus \theta^{(3)}_{\{3,3,52\}} \oplus (A^{(4)}_{\{1,1,16\}} \oplus 1) \cdot \theta^{(3)}_{\{0,0,13\}},\\
A^{(3)}_{\{3,0,20\}} \oplus A^{(3)}_{\{3,3,20\}} \oplus (A^{(4)}_{\{1,1,48\}} \oplus 1) \cdot (A^{(3)}_{\{0,2,45\}} \oplus A^{(3)}_{\{0,0,45\}}) = A^{(4)}_{\{0,1,48\}} \oplus \theta^{(3)}_{\{3,3,20\}} \oplus (A^{(4)}_{\{1,1,48\}} \oplus 1) \cdot \theta^{(3)}_{\{0,0,45\}},\\
A^{(3)}_{\{4,1,47\}} \oplus A^{(3)}_{\{4,4,47\}} \oplus (A^{(4)}_{\{2,1,3\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,22\}} \oplus A^{(3)}_{\{1,1,22\}}) = A^{(4)}_{\{1,1,3\}} \oplus \theta^{(3)}_{\{4,4,47\}} \oplus (A^{(4)}_{\{2,1,3\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,22\}},\\
A^{(3)}_{\{4,1,15\}} \oplus A^{(3)}_{\{4,4,15\}} \oplus (A^{(4)}_{\{2,1,35\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,54\}} \oplus A^{(3)}_{\{1,1,54\}}) = A^{(4)}_{\{1,1,35\}} \oplus \theta^{(3)}_{\{4,4,15\}} \oplus (A^{(4)}_{\{2,1,35\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,54\}},\\
A^{(3)}_{\{4,1,48\}} \oplus A^{(3)}_{\{4,4,48\}} \oplus (A^{(4)}_{\{2,1,4\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,23\}} \oplus A^{(3)}_{\{1,1,23\}}) = A^{(4)}_{\{1,1,4\}} \oplus \theta^{(3)}_{\{4,4,48\}} \oplus (A^{(4)}_{\{2,1,4\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,23\}},\\
A^{(3)}_{\{4,1,16\}} \oplus A^{(3)}_{\{4,4,16\}} \oplus (A^{(4)}_{\{2,1,36\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,55\}} \oplus A^{(3)}_{\{1,1,55\}}) = A^{(4)}_{\{1,1,36\}} \oplus \theta^{(3)}_{\{4,4,16\}} \oplus (A^{(4)}_{\{2,1,36\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,55\}},\\
A^{(3)}_{\{4,1,51\}} \oplus A^{(3)}_{\{4,4,51\}} \oplus (A^{(4)}_{\{2,1,7\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,26\}} \oplus A^{(3)}_{\{1,1,26\}}) = A^{(4)}_{\{1,1,7\}} \oplus \theta^{(3)}_{\{4,4,51\}} \oplus (A^{(4)}_{\{2,1,7\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,26\}},\\
A^{(3)}_{\{4,1,19\}} \oplus A^{(3)}_{\{4,4,19\}} \oplus (A^{(4)}_{\{2,1,39\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,59\}} \oplus A^{(3)}_{\{1,1,59\}}) = A^{(4)}_{\{1,1,39\}} \oplus \theta^{(3)}_{\{4,4,19\}} \oplus (A^{(4)}_{\{2,1,39\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,59\}},\\
A^{(3)}_{\{4,1,52\}} \oplus A^{(3)}_{\{4,4,52\}} \oplus (A^{(4)}_{\{2,1,8\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,27\}} \oplus A^{(3)}_{\{1,1,27\}}) = A^{(4)}_{\{1,1,8\}} \oplus \theta^{(3)}_{\{4,4,52\}} \oplus (A^{(4)}_{\{2,1,8\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,27\}},\\
A^{(3)}_{\{4,1,20\}} \oplus A^{(3)}_{\{4,4,20\}} \oplus (A^{(4)}_{\{2,1,40\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,60\}} \oplus A^{(3)}_{\{1,1,60\}}) = A^{(4)}_{\{1,1,40\}} \oplus \theta^{(3)}_{\{4,4,20\}} \oplus (A^{(4)}_{\{2,1,40\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,60\}},\\
A^{(3)}_{\{4,1,4\}} \oplus A^{(3)}_{\{4,4,4\}} \oplus (A^{(4)}_{\{2,1,24\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,43\}} \oplus A^{(3)}_{\{1,1,43\}}) = A^{(4)}_{\{1,1,24\}} \oplus \theta^{(3)}_{\{4,4,4\}} \oplus (A^{(4)}_{\{2,1,24\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,43\}},\\
A^{(3)}_{\{4,1,36\}} \oplus A^{(3)}_{\{4,4,36\}} \oplus (A^{(4)}_{\{2,1,56\}} \oplus 1) \cdot (A^{(3)}_{\{1,3,11\}} \oplus A^{(3)}_{\{1,1,11\}}) = A^{(4)}_{\{1,1,56\}} \oplus \theta^{(3)}_{\{4,4,36\}} \oplus (A^{(4)}_{\{2,1,56\}} \oplus 1) \cdot \theta^{(3)}_{\{1,1,11\}}.
\end{cases}
\tag{20}
$$

We derive inversely to get the other 116 Boolean equations with similar form with Equ. (20), which are used to further filter the partial matched states.

In our attack Algorithm 3 of the preimage attack on 4-round `Keccak-512`, we use two message blocks (M_1, M_2) to build the attack. There are totally 244

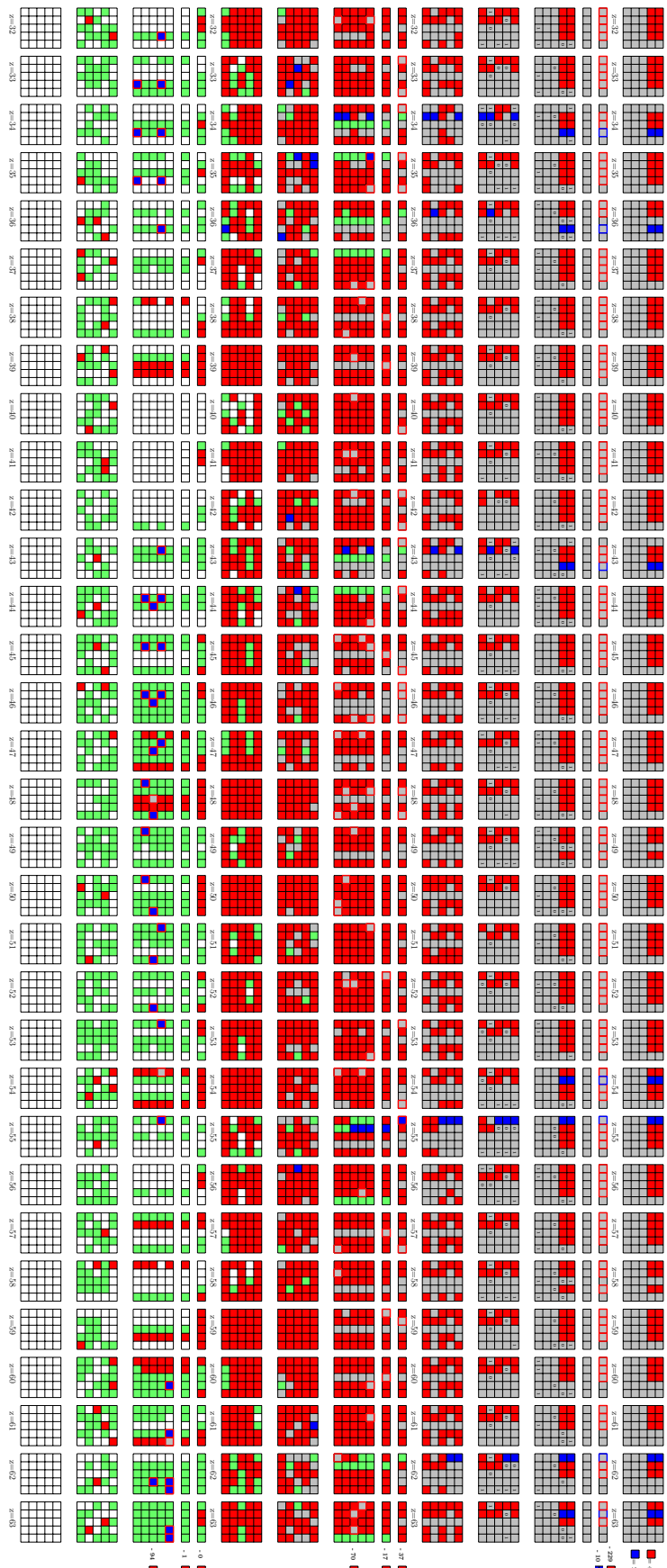

Fig. 18: The 4-round MitM collision attack on Keccak-512: Part 2

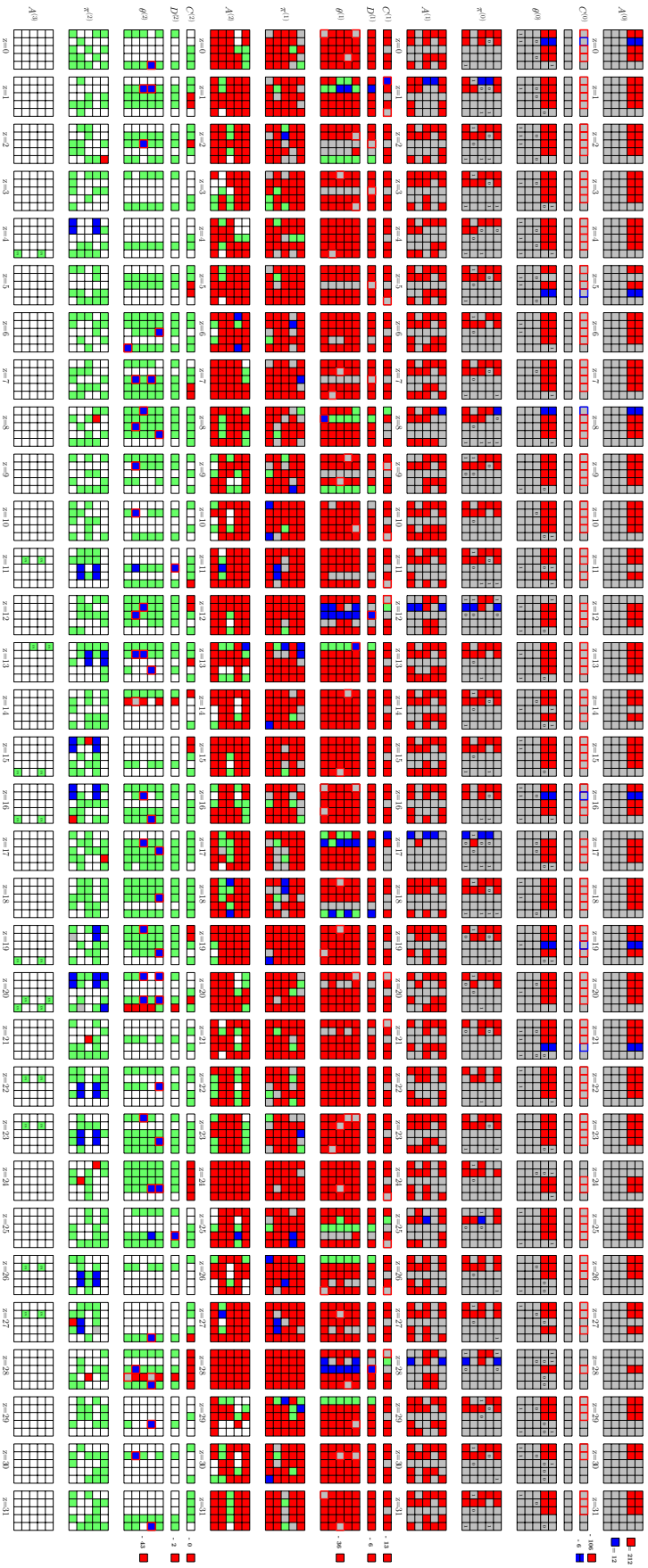

Fig. 19: The new 4-round MitM preimage attack on Keccak-512

Algorithm 3: Preimage Attack on 4-round `Keccak-512`

Precompute inversely from the target to $A^{(3)}$, and derive 128 Boolean equations of similar form with Equ. (20)
`/* Among them, 12 Boolean equations act as the matching points in the MitM phase. The other 116 Boolean equations are used to further filter the partial matched states. */`
for 2^{ζ} *values of* M_1 **do**
  Compute the inner part of the 2nd block and solve the system of 244 linear equations
  if *the equations have solutions* `/* with probability of` 2^{-38} `*/`
  then
    for *each of the* 2^{146} *solutions of* M_2 **do**
      `/* With` $\zeta = 180$`, there are` $2^{180-38+146} = 2^{288}$ `iterations */`
      Traversing the 2^{212} values of ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine 200-bit ■/■ bits (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{200}$), and the 12-bit matching point in Equ. (20), *i.e.*, compute 12 $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 212-bit ■ bits of $A^{(0)}$ as well as the 12-bit matching point in $U[c_{\mathcal{R}}]$.
      `/* This method to solve the nonlinear constrained neutral words is borrowed from Dong et al. [28]. */`
      for $c_{\mathcal{R}} \in \mathbb{F}_2^{200}$ **do**
        Randomly pick a 212-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get 12 $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
        for 2^{12} *values in* $U[c_{\mathcal{R}}]$ **do**
          Restore the values of ■ of $A^{(0)}$ and the corresponding matching point (*i.e.*, 12 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
        end
        for 2^{12} *values of* ■ **do**
          Set the 212-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 12 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by matching point.
        end
        for *values matched between* L_1 *and* L_2 **do**
          Compute $A^{(3)}$ from the matched ■ and ■ bits
          if $A^{(3)}$ *satisfy the 116 precomputed Boolean equations* `/* Probability of` 2^{-116} `*/`
          then
            if *it leads to the given hash value* **then**
              Output the preimage
            end
          end
        end
      end
    end
  end
end

conditions on $\pi^{(0)}$, i.e. $\mu = 244$. Given an inner part, the 244 conditions on state $A^{(0)}$ will be a linear system on 352 variables of M_2, including $576 - 448 = 128$ ■ bits and 224 Binary variables c. The rank of the coefficient matrix of the linear system is 206. There are $244 - 206 = 38$ conditions out of the total 244 only determined by the bits of inner part. Randomly test 2^{38} M_1 to expect one satisfying the 38 conditions of the inner part. Then for a right M_1, there are $2^{352-206} = 2^{146}$ solutions of M_2, which make all the 244 equations hold.

In Line 5, once we find solutions of M_2, we can perform 2^{200} MitM episodes in Line 13 to 24 for each of the 2^{244} solutions. For each MitM episode, $2^{12} \times 2^{12}$ internal states are exhausted. Suppose there needs 2^{ζ} possible values of M_1. To find a 512-bit target preimage, we need $2^{\zeta-38+146+200+12+12} = 2^{512}$, i.e., $\zeta = 180$. The steps of Algorithm 3 are analyzed below:

- In Line 4, the time complexity is 2^{180} 4-round `Keccak` and $2^{180} \times 244^3$ bit operations to solve the linear system (the time to solve a system of n linear equations is about $O(n^3)$).
- The 200 consumed DoFs of ■ bits of $A^{(0)}$ are used to make 200 internal bits (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{200}$) to be ■/■, so that the remaining ■ set of size 2^{12} can be computed independently to the ■ set. In Line 9, the time complexity is $2^{180-38+146+212} \times \frac{3}{4} = 2^{499.58}$ 4-round `Keccak`, since only 3 rounds from $A^{(0)}$ to $A^{(3)}$ are needed to derive the ■/■ bits and the matching points.
- In Line 12, the time complexity is $2^{180-38+146+200} \times \frac{3}{4} = 2^{487.58}$ 4-round `Keccak`.
- In Line 14, this step is just to retrieve $U[c_{\mathcal{R}}]$ to restore it in L_1 with 12-bit matching point as index. Suppose one access to the table is equivalent to one Sbox application. The time complexity is $2^{180-38+146+200+12} \times \frac{1}{4\times 320} = 2^{489.67}$ 4-round `Keccak`, since there are 4×320 Sboxes for 4-round `Keccak`.
- In Line 17, the time complexity is $2^{180-38+146+200+12} \times \frac{3}{4} = 2^{499.58}$ 4-round `Keccak`.
- In Line 20, the time is $2^{180-38+146+200+12+12-12} \times \frac{3}{4} = 2^{499.58}$ 4-round `Keccak`.
- In Line 21, $A^{(3)}$ is checked against the 116 Boolean equations precomputed in Line 1, which act as a filter of 2^{-116}. After the filter, the time of the final check against the target h is $2^{180-38+146+200+12-116} = 2^{384}$ 4-round `Keccak`.

The total complexity is $2^{180} + 2^{180} \times 244^3 + 2^{499.58} + 2^{487.58} + 2^{489.67} + 2^{499.58} + 2^{499.58} + 2^{384} \approx 2^{501.16}$ 4-round `Keccak`. The memory to store U is 2^{212}.

D Parameters of Attack on `Keccak-384`

We fist given the differencs of the MILP models for `Keccak-384`. Then we list the attack figures and matching equations for the preimage attack on 4-round `Keccak-384`. At last, we give three linear expressions of consuming DoFs.

D.1 MILP models for Keccak-384

Modelling the first round. Different from the weak-diffusion structure used in Figure 6 for Keccak-512, the weak-diffusion structure used for Keccak-384 is given in Figure 13, which covers 13 lanes, and the θ operation in the structure acts as an identity with CP-kernel property. The variables $\{v_{0,z}, v_{1,z}, v_{2,z}, v_{3,z}, v_{4,z}, v_{5,z}, v_{6,z}, v_{7,z}\}$ $(0 \le z \le 63)$ are allocated in $A^{(0)}$ as

$$\begin{cases} A^{(0)}_{\{x,0,z\}} = v_{x,z},\ A^{(0)}_{\{x,1,z\}} = v_{x+5,z},\ A^{(0)}_{\{x,2,z\}} = v_{x,z} \oplus v_{x+5,z} \oplus c_{x,z},\ 0 \le x \le 2, \\ A^{(0)}_{\{x,0,z\}} = v_{x,z},\ A^{(0)}_{\{x,1,z\}} = v_{x,z} \oplus c_{x,z},\ 3 \le x \le 4, \end{cases}$$

where $c_{0,z}, c_{1,z}, c_{2,z}, c_{3,z}, c_{4,z}$ $(0 \le z \le 63)$ are constants. To reduce the diffusion of the χ operation, proper constraints on ■ bits will be added.

Similar to Keccak-512, each of the 1600 bits in the starting state $A^{(0)}$ takes one color of ■, ■ and ■. The bits put with variables $v_{x,z}$ can be colored as ■ or ■. To make the coloring pattern of the state keeps the same over the first θ operation, it consumes one degree of freedom (DoF) of ■ (■) if $A^{(0)}_{\{x,0,z\}}$ is of ■ (■). So the MILP model can be constructed from $\pi^{(0)}$. For the state bit $\pi^{(0)}_{\{x,y,z\}}$, the constraints for the 13×64 bits $\pi^{(0)}$ put with variables $\{v_{0,z}, v_{1,z}, v_{2,z}, v_{3,z}, v_{4,z}, v_{5,z}, v_{6,z}, v_{7,z}\}$ are

$$\begin{cases} \pi^{(0)}_{\{0,2x,z+\gamma[x,0]\}}[l] = \pi^{(0)}_{\{1,2x+3,z+\gamma[x,1]\}}[l] = \pi^{(0)}_{\{2,2x+1,z+\gamma[x,2]\}}[l], \\ \pi^{(0)}_{\{0,2x,z\}}[1] = 1,\ \ \pi^{(0)}_{\{0,2x,z\}}[0] + \pi^{(0)}_{\{0,2x,z\}}[2] \ge 1, \end{cases}$$

where $0 \le x \le 2, 0 \le z \le 63$, and

$$\pi^{(0)}_{\{0,2x,z+\gamma[x,0]\}}[l] = \pi^{(0)}_{\{1,2x+3,z+\gamma[x,1]\}}[l],\ \pi^{(0)}_{\{0,2x,z\}}[1] = 1,\ \pi^{(0)}_{\{0,2x,z\}}[0] + \pi^{(0)}_{\{0,2x,z\}}[2] \ge 1,$$

where $3 \le x \le 4, 0 \le z \le 63$. The other capacity 768 bits are ■, where the corresponding $\pi^{(0)}_{\{x,y,z\}}[l] = 1$ $(0 \le l \le 2)$. Therefore, we can compute the number of initial degrees of freedom for ■ and ■ by

$$\begin{cases} \lambda_{\mathcal{B}} = 2 \cdot \sum_{x=0}^{2} \sum_{z=0}^{63} (1 - \pi^{(0)}_{\{0,2x,z\}}[2]) + \sum_{x=3}^{4} \sum_{z=0}^{63} (1 - \pi^{(0)}_{\{0,2x,z\}}[2]), \\ \lambda_{\mathcal{R}} = 2 \cdot \sum_{x=0}^{2} \sum_{z=0}^{63} (1 - \pi^{(0)}_{\{0,2x,z\}}[0]) + \sum_{x=3}^{4} \sum_{z=0}^{63} (1 - \pi^{(0)}_{\{0,2x,z\}}[0]). \end{cases}$$

Modelling the χ operation with conditions in Round 0. Comparing to the modelling strategy of Keccak-512, there are two additional cases for the five inputs of the χ operation:

- Case-3: There are two non-adjacent ■/■ bits, and the others are ■ bits.
- Case-4: There are three consecutive ■/■ bits, and the others are ■ bits.

For Case-3 and Case-4, we can also add conditions on ■ bits to control the diffusion of ■/■ bit.

– `CondSBOX-RULE-3`: There are two non-adjacent ■/■ bit in $\pi^{(0)}_{\{0,y,z\}}$ and $\pi^{(0)}_{\{2,y,z\}}$. To avoid the ■ from appearing in the first round, we restrict the $(\pi^{(0)}_{\{0,y,z\}}, \pi^{(0)}_{\{2,y,z\}})$ to be of the same color. The conditions to control the color are listed below:

  1. $\chi^{(0)}_{\{0,y,z\}}$ and $\chi^{(0)}_{\{2,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.
  2. If we set $\pi^{(0)}_{\{3,y,z\}} = 0$, $\chi^{(0)}_{\{1,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{1,y,z\}}$ will be the same color with $\pi^{(0)}_{\{2,y,z\}}$.
  3. If we set $\pi^{(0)}_{\{4,y,z\}} = 1$, $\chi^{(0)}_{\{3,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{3,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.
  4. If we set $\pi^{(0)}_{\{1,y,z\}} = 0$, $\chi^{(0)}_{\{4,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{4,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.

– `CondSBOX-RULE-4`: There are three consecutive ■/■ bits in $\pi^{(0)}_{\{0,y,z\}}$, $\pi^{(0)}_{\{1,y,z\}}$ and $\pi^{(0)}_{\{2,y,z\}}$. To avoid the □ from appearing in the first round, we restrict the $\pi^{(0)}_{\{0,y,z\}}$, $\pi^{(0)}_{\{1,y,z\}}$ and $\pi^{(0)}_{\{2,y,z\}}$ to be of the same color. We add conditions to control the color:

  1. $\chi^{(0)}_{\{0,y,z\}}$, $\chi^{(0)}_{\{1,y,z\}}$, $\chi^{(0)}_{\{2,y,z\}}$ and $\chi^{(0)}_{\{4,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.
  2. If we set $\pi^{(0)}_{\{4,y,z\}} = 1$, $\chi^{(0)}_{\{3,y,z\}}$ will be ■; otherwise, $\chi^{(0)}_{\{3,y,z\}}$ will be the same color with $\pi^{(0)}_{\{0,y,z\}}$.

The valid coloring patterns are listed in Figure 20. The matching scheme is same to Observation 2. The two-stage approach is also applied to speed up the search. The choices for the weak ■ sets are similar with `Keccak-512`, where the number of ■ bits in $D^{(1)}$ is counted.

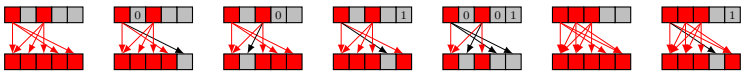

Fig. 20: Additional `CondSBOX-RULE` for `Keccak-384`

D.2 The attack figure of `Keccak-384`

The first and second parts of the attack figure are given in Figure 21 and 22.

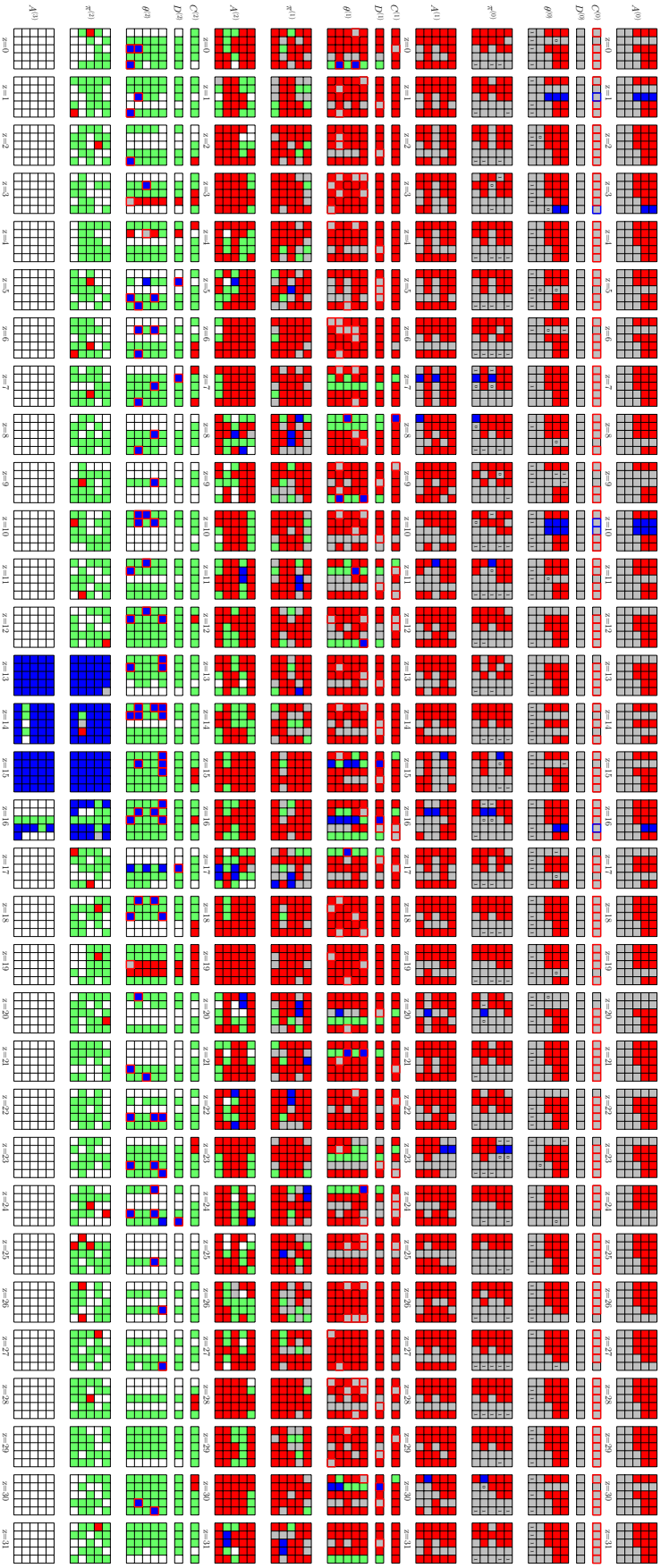

Fig. 21: The 4-round MitM preimage attack on Keccak-384: Part 1

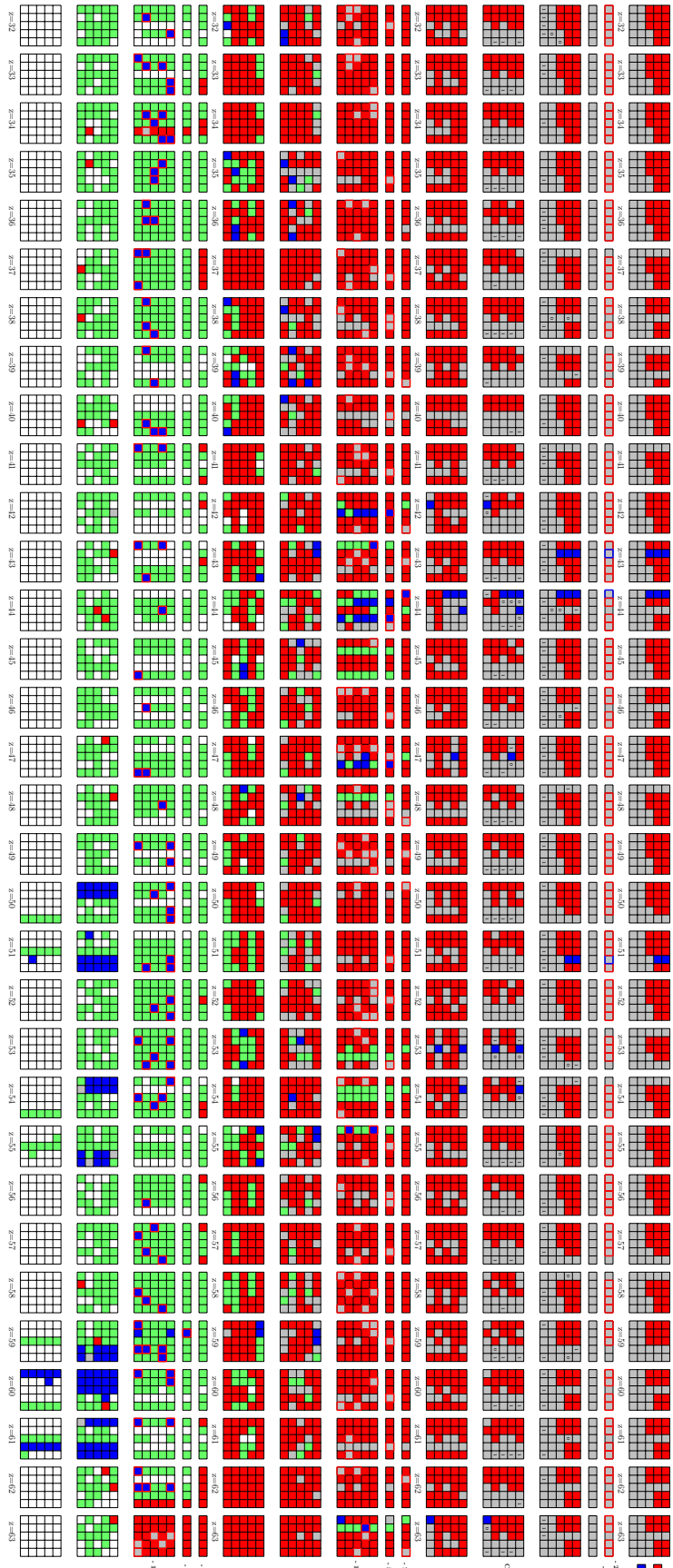

Fig. 22: The 4-round MitM preimage attack on Keccak-384: Part 2

D.3 Matching Equations of Keccak-384

The thirteen matching equations in the preimage attack on 4-round Keccak-384 are given as follows:

$$
\begin{cases}
\pi^{(3)}_{\{1,0,58\}} = A^{(3)}_{\{1,1,14\}} \oplus A^{(3)}_{\{0,0,14\}} \oplus A^{(3)}_{\{0,1,14\}} \oplus A^{(3)}_{\{0,2,14\}} \oplus A^{(3)}_{\{0,3,14\}} \oplus A^{(3)}_{\{0,4,14\}} \\
\qquad \oplus A^{(3)}_{\{2,0,13\}} \oplus A^{(3)}_{\{2,1,13\}} \oplus A^{(3)}_{\{2,2,13\}} \oplus A^{(3)}_{\{2,3,13\}} \oplus A^{(3)}_{\{2,4,13\}}, \\
\pi^{(3)}_{\{2,0,57\}} = A^{(3)}_{\{2,2,14\}} \oplus A^{(3)}_{\{1,0,14\}} \oplus A^{(3)}_{\{1,1,14\}} \oplus A^{(3)}_{\{1,2,14\}} \oplus A^{(3)}_{\{1,3,14\}} \oplus A^{(3)}_{\{1,4,14\}} \\
\qquad \oplus A^{(3)}_{\{3,0,13\}} \oplus A^{(3)}_{\{3,1,13\}} \oplus A^{(3)}_{\{3,2,13\}} \oplus A^{(3)}_{\{3,3,13\}} \oplus A^{(3)}_{\{3,4,13\}}, \\
\pi^{(3)}_{\{4,0,28\}} = A^{(3)}_{\{4,4,14\}} \oplus A^{(3)}_{\{3,0,14\}} \oplus A^{(3)}_{\{3,1,14\}} \oplus A^{(3)}_{\{3,2,14\}} \oplus A^{(3)}_{\{3,3,14\}} \oplus A^{(3)}_{\{3,4,14\}} \\
\qquad \oplus A^{(3)}_{\{0,0,13\}} \oplus A^{(3)}_{\{0,1,13\}} \oplus A^{(3)}_{\{0,2,13\}} \oplus A^{(3)}_{\{0,3,13\}} \oplus A^{(3)}_{\{0,4,13\}}, \\
\pi^{(3)}_{\{0,0,15\}} = A^{(3)}_{\{0,0,15\}} \oplus A^{(3)}_{\{4,0,15\}} \oplus A^{(3)}_{\{4,1,15\}} \oplus A^{(3)}_{\{4,2,15\}} \oplus A^{(3)}_{\{4,3,15\}} \oplus A^{(3)}_{\{4,4,15\}} \\
\qquad \oplus A^{(3)}_{\{1,0,14\}} \oplus A^{(3)}_{\{1,1,14\}} \oplus A^{(3)}_{\{1,2,14\}} \oplus A^{(3)}_{\{1,3,14\}} \oplus A^{(3)}_{\{1,4,14\}}, \\
\pi^{(3)}_{\{2,0,58\}} = A^{(3)}_{\{2,2,15\}} \oplus A^{(3)}_{\{1,0,15\}} \oplus A^{(3)}_{\{1,1,15\}} \oplus A^{(3)}_{\{1,2,15\}} \oplus A^{(3)}_{\{1,3,15\}} \oplus A^{(3)}_{\{1,4,15\}} \\
\qquad \oplus A^{(3)}_{\{3,0,14\}} \oplus A^{(3)}_{\{3,1,14\}} \oplus A^{(3)}_{\{3,2,14\}} \oplus A^{(3)}_{\{3,3,14\}} \oplus A^{(3)}_{\{3,4,14\}}, \\
\pi^{(3)}_{\{4,0,29\}} = A^{(3)}_{\{4,4,15\}} \oplus A^{(3)}_{\{3,0,15\}} \oplus A^{(3)}_{\{3,1,15\}} \oplus A^{(3)}_{\{3,2,15\}} \oplus A^{(3)}_{\{3,3,15\}} \oplus A^{(3)}_{\{3,4,15\}} \\
\qquad \oplus A^{(3)}_{\{0,0,14\}} \oplus A^{(3)}_{\{0,1,14\}} \oplus A^{(3)}_{\{0,2,14\}} \oplus A^{(3)}_{\{0,3,14\}} \oplus A^{(3)}_{\{0,4,14\}}, \\
\pi^{(3)}_{\{3,0,37\}} = A^{(3)}_{\{3,3,16\}} \oplus A^{(3)}_{\{2,0,16\}} \oplus A^{(3)}_{\{2,1,16\}} \oplus A^{(3)}_{\{2,2,16\}} \oplus A^{(3)}_{\{2,3,16\}} \oplus A^{(3)}_{\{2,4,16\}} \\
\qquad \oplus A^{(3)}_{\{4,0,15\}} \oplus A^{(3)}_{\{4,1,15\}} \oplus A^{(3)}_{\{4,2,15\}} \oplus A^{(3)}_{\{4,3,15\}} \oplus A^{(3)}_{\{4,4,15\}}, \\
\pi^{(3)}_{\{4,0,30\}} = A^{(3)}_{\{4,4,16\}} \oplus A^{(3)}_{\{3,0,16\}} \oplus A^{(3)}_{\{3,1,16\}} \oplus A^{(3)}_{\{3,2,16\}} \oplus A^{(3)}_{\{3,3,16\}} \oplus A^{(3)}_{\{3,4,16\}} \\
\qquad \oplus A^{(3)}_{\{4,0,15\}} \oplus A^{(3)}_{\{4,1,15\}} \oplus A^{(3)}_{\{4,2,15\}} \oplus A^{(3)}_{\{4,3,15\}} \oplus A^{(3)}_{\{4,4,15\}}, \\
\pi^{(3)}_{\{3,0,8\}} = A^{(3)}_{\{3,3,51\}} \oplus A^{(3)}_{\{2,0,51\}} \oplus A^{(3)}_{\{2,1,51\}} \oplus A^{(3)}_{\{2,2,51\}} \oplus A^{(3)}_{\{2,3,51\}} \oplus A^{(3)}_{\{2,4,51\}} \\
\qquad \oplus A^{(3)}_{\{4,0,50\}} \oplus A^{(3)}_{\{4,1,50\}} \oplus A^{(3)}_{\{4,2,50\}} \oplus A^{(3)}_{\{4,3,50\}} \oplus A^{(3)}_{\{4,4,50\}}, \\
\pi^{(3)}_{\{3,0,12\}} = A^{(3)}_{\{3,3,55\}} \oplus A^{(3)}_{\{2,0,55\}} \oplus A^{(3)}_{\{2,1,55\}} \oplus A^{(3)}_{\{2,2,55\}} \oplus A^{(3)}_{\{2,3,55\}} \oplus A^{(3)}_{\{2,4,55\}} \\
\qquad \oplus A^{(3)}_{\{4,0,54\}} \oplus A^{(3)}_{\{4,1,54\}} \oplus A^{(3)}_{\{4,2,54\}} \oplus A^{(3)}_{\{4,3,54\}} \oplus A^{(3)}_{\{4,4,54\}}, \\
\pi^{(3)}_{\{1,0,40\}} = A^{(3)}_{\{1,1,60\}} \oplus A^{(3)}_{\{0,0,60\}} \oplus A^{(3)}_{\{0,1,60\}} \oplus A^{(3)}_{\{0,2,60\}} \oplus A^{(3)}_{\{0,3,60\}} \oplus A^{(3)}_{\{0,4,60\}} \\
\qquad \oplus A^{(3)}_{\{2,0,59\}} \oplus A^{(3)}_{\{2,1,59\}} \oplus A^{(3)}_{\{2,2,59\}} \oplus A^{(3)}_{\{2,3,59\}} \oplus A^{(3)}_{\{2,4,59\}}, \\
\pi^{(3)}_{\{3,0,18\}} = A^{(3)}_{\{3,3,61\}} \oplus A^{(3)}_{\{2,0,61\}} \oplus A^{(3)}_{\{2,1,61\}} \oplus A^{(3)}_{\{2,2,61\}} \oplus A^{(3)}_{\{2,3,61\}} \oplus A^{(3)}_{\{2,4,61\}} \\
\qquad \oplus A^{(3)}_{\{4,0,60\}} \oplus A^{(3)}_{\{4,1,60\}} \oplus A^{(3)}_{\{4,2,60\}} \oplus A^{(3)}_{\{4,3,60\}} \oplus A^{(3)}_{\{4,4,60\}}, \\
\pi^{(3)}_{\{4,0,11\}} = A^{(3)}_{\{4,4,61\}} \oplus A^{(3)}_{\{3,0,61\}} \oplus A^{(3)}_{\{3,1,61\}} \oplus A^{(3)}_{\{3,2,61\}} \oplus A^{(3)}_{\{3,3,61\}} \oplus A^{(3)}_{\{3,4,61\}} \\
\qquad \oplus A^{(3)}_{\{0,0,60\}} \oplus A^{(3)}_{\{0,1,60\}} \oplus A^{(3)}_{\{0,2,60\}} \oplus A^{(3)}_{\{0,3,60\}} \oplus A^{(3)}_{\{0,4,60\}}.
\end{cases}
\tag{21}
$$

D.4 Linear Expressions of Consuming Positions of Keccak-384

There are total fifty five linear expressions, and three examples are given as follows:

$$
\begin{aligned}
\mathbf{C}^{(\mathbf{1})}_{\{\mathbf{1,11}\}} = {} & A^{(0)}_{\{0,0,8\}} \cdot A^{(0)}_{\{2,3,29\}} \oplus A^{(0)}_{\{0,0,8\}} \cdot A^{(0)}_{\{0,3,30\}} \oplus A^{(0)}_{\{0,0,8\}} \cdot A^{(0)}_{\{1,3,30\}} \oplus A^{(0)}_{\{0,0,8\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{0,0,8\}} \cdot \\
& A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{0,0,8\}} \cdot c_{\{2,29\}} \oplus A^{(0)}_{\{0,0,8\}} \cdot c_{\{0,30\}} \oplus A^{(0)}_{\{3,0,20\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{4,0,53\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{4,1,53\}} \oplus \\
& A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{4,2,53\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{4,3,53\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{3,3,54\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{4,4,53\}} \oplus
\end{aligned}
$$

$$A^{(0)}_{\{2,0,32\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{2,0,32\}} \cdot c_{\{2,54\}} \oplus A^{(0)}_{\{4,0,55\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot A^{(0)}_{\{2,3,29\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot A^{(0)}_{\{0,3,30\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot$$
$$A^{(0)}_{\{1,3,30\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot c_{\{2,29\}} \oplus A^{(0)}_{\{0,1,8\}} \cdot c_{\{0,30\}} \oplus A^{(0)}_{\{1,1,31\}} \oplus$$
$$A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{4,0,53\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{4,1,53\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{4,2,53\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{4,3,53\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{2,3,54\}} \oplus$$
$$A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{3,3,54\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{2,1,32\}} \cdot c_{\{2,54\}} \oplus A^{(0)}_{\{4,0,53\}} \cdot A^{(0)}_{\{3,2,31\}} \oplus$$
$$A^{(0)}_{\{4,0,53\}} \cdot A^{(0)}_{\{3,3,31\}} \oplus A^{(0)}_{\{4,0,53\}} \cdot A^{(0)}_{\{1,3,32\}} \oplus A^{(0)}_{\{4,0,53\}} \cdot A^{(0)}_{\{3,4,31\}} \oplus A^{(0)}_{\{4,0,53\}} \cdot A^{(0)}_{\{1,4,32\}} \oplus A^{(0)}_{\{4,0,53\}} \cdot c_{\{3,31\}} \oplus$$
$$A^{(0)}_{\{4,0,53\}} \cdot c_{\{1,32\}} \oplus A^{(0)}_{\{4,0,53\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{4,0,53\}} \oplus A^{(0)}_{\{0,0,54\}} \oplus A^{(0)}_{\{3,0,59\}} \cdot A^{(0)}_{\{1,2,1\}} \oplus A^{(0)}_{\{3,0,59\}} \cdot A^{(0)}_{\{2,3,0\}} \oplus$$
$$A^{(0)}_{\{3,0,59\}} \cdot A^{(0)}_{\{0,3,1\}} \oplus A^{(0)}_{\{3,0,59\}} \cdot A^{(0)}_{\{2,4,0\}} \oplus A^{(0)}_{\{3,0,59\}} \cdot A^{(0)}_{\{0,4,1\}} \oplus A^{(0)}_{\{3,0,59\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{3,0,59\}} \cdot c_{\{0,1\}} \oplus$$
$$A^{(0)}_{\{3,0,59\}} \oplus A^{(0)}_{\{0,1,39\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot A^{(0)}_{\{3,2,31\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot A^{(0)}_{\{3,3,31\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot A^{(0)}_{\{1,3,32\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot A^{(0)}_{\{3,4,31\}} \oplus$$
$$A^{(0)}_{\{4,1,53\}} \cdot A^{(0)}_{\{1,4,32\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot c_{\{3,31\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot c_{\{1,32\}} \oplus A^{(0)}_{\{4,1,53\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{4,1,53\}} \oplus A^{(0)}_{\{0,1,54\}} \oplus$$
$$A^{(0)}_{\{3,1,59\}} \cdot A^{(0)}_{\{1,2,1\}} \oplus A^{(0)}_{\{3,1,59\}} \cdot A^{(0)}_{\{2,3,0\}} \oplus A^{(0)}_{\{3,1,59\}} \cdot A^{(0)}_{\{0,3,1\}} \oplus A^{(0)}_{\{3,1,59\}} \cdot A^{(0)}_{\{2,4,0\}} \oplus A^{(0)}_{\{3,1,59\}} \cdot A^{(0)}_{\{0,4,1\}} \oplus$$
$$A^{(0)}_{\{3,1,59\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{3,1,59\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{3,1,59\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{3,2,59\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{3,3,59\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot$$
$$A^{(0)}_{\{1,3,60\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{2,3,60\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{1,4,60\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot c_{\{1,60\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot$$
$$A^{(0)}_{\{4,2,49\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{3,2,50\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{4,3,49\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{2,3,50\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{4,4,49\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot$$
$$A^{(0)}_{\{2,4,50\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot c_{\{4,49\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot c_{\{2,50\}} \oplus A^{(0)}_{\{3,2,3\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{2,3,29\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{0,3,30\}} \oplus$$
$$A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{1,3,30\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot c_{\{2,29\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot c_{\{0,30\}} \oplus$$
$$A^{(0)}_{\{4,2,19\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot A^{(0)}_{\{4,2,53\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot A^{(0)}_{\{4,3,53\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot A^{(0)}_{\{3,3,54\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot$$
$$A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{3,2,31\}} \cdot c_{\{2,54\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot A^{(0)}_{\{3,2,36\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot A^{(0)}_{\{4,2,36\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot$$
$$A^{(0)}_{\{0,3,35\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot A^{(0)}_{\{3,3,36\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot A^{(0)}_{\{0,4,35\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot A^{(0)}_{\{3,4,36\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot c_{\{0,35\}} \oplus A^{(0)}_{\{4,2,34\}} \cdot$$
$$c_{\{3,36\}} \oplus A^{(0)}_{\{4,2,34\}} \oplus A^{(0)}_{\{3,2,36\}} \cdot A^{(0)}_{\{1,3,33\}} \oplus A^{(0)}_{\{3,2,36\}} \cdot A^{(0)}_{\{0,3,34\}} \oplus A^{(0)}_{\{3,2,36\}} \cdot A^{(0)}_{\{4,3,34\}} \oplus A^{(0)}_{\{3,2,36\}} \cdot A^{(0)}_{\{1,4,33\}} \oplus$$
$$A^{(0)}_{\{3,2,36\}} \cdot A^{(0)}_{\{4,4,34\}} \oplus A^{(0)}_{\{3,2,36\}} \cdot c_{\{1,33\}} \oplus A^{(0)}_{\{3,2,36\}} \cdot c_{\{4,34\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{1,3,33\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{0,3,34\}} \oplus$$
$$A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{4,3,34\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{1,4,33\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{4,4,34\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot c_{\{1,33\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot c_{\{4,34\}} \oplus$$
$$A^{(0)}_{\{4,2,39\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot A^{(0)}_{\{0,3,2\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot A^{(0)}_{\{3,3,3\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot A^{(0)}_{\{4,3,3\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot A^{(0)}_{\{0,4,2\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot$$
$$A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{4,2,49\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{0,3,2\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{3,3,3\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot$$
$$A^{(0)}_{\{4,3,3\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{0,4,2\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot$$
$$A^{(0)}_{\{3,3,31\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot A^{(0)}_{\{1,3,32\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot A^{(0)}_{\{3,4,31\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot A^{(0)}_{\{1,4,32\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot c_{\{3,31\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot$$
$$c_{\{1,32\}} \oplus A^{(0)}_{\{4,2,53\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{4,2,53\}} \oplus A^{(0)}_{\{0,2,54\}} \oplus A^{(0)}_{\{3,2,55\}} \oplus A^{(0)}_{\{3,2,59\}} \cdot A^{(0)}_{\{2,3,0\}} \oplus A^{(0)}_{\{3,2,59\}} \cdot A^{(0)}_{\{0,3,1\}} \oplus$$
$$A^{(0)}_{\{3,2,59\}} \cdot A^{(0)}_{\{2,4,0\}} \oplus A^{(0)}_{\{3,2,59\}} \cdot A^{(0)}_{\{0,4,1\}} \oplus A^{(0)}_{\{3,2,59\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{3,2,59\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{3,2,59\}} \oplus A^{(0)}_{\{2,3,0\}} \cdot$$
$$A^{(0)}_{\{3,3,59\}} \oplus A^{(0)}_{\{2,3,0\}} \cdot A^{(0)}_{\{1,3,60\}} \oplus A^{(0)}_{\{2,3,0\}} \cdot A^{(0)}_{\{2,3,60\}} \oplus A^{(0)}_{\{2,3,0\}} \cdot A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{2,3,0\}} \cdot A^{(0)}_{\{1,4,60\}} \oplus A^{(0)}_{\{2,3,0\}} \cdot$$
$$c_{\{1,60\}} \oplus A^{(0)}_{\{0,3,1\}} \cdot A^{(0)}_{\{3,3,59\}} \oplus A^{(0)}_{\{0,3,1\}} \cdot A^{(0)}_{\{1,3,60\}} \oplus A^{(0)}_{\{0,3,1\}} \cdot A^{(0)}_{\{2,3,60\}} \oplus A^{(0)}_{\{0,3,1\}} \cdot A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{0,3,1\}} \cdot$$
$$A^{(0)}_{\{1,4,60\}} \oplus A^{(0)}_{\{0,3,1\}} \cdot c_{\{1,60\}} \oplus A^{(0)}_{\{0,3,2\}} \cdot A^{(0)}_{\{4,3,49\}} \oplus A^{(0)}_{\{0,3,2\}} \cdot A^{(0)}_{\{2,3,50\}} \oplus A^{(0)}_{\{0,3,2\}} \cdot A^{(0)}_{\{4,4,49\}} \oplus A^{(0)}_{\{0,3,2\}} \cdot$$
$$A^{(0)}_{\{2,4,50\}} \oplus A^{(0)}_{\{0,3,2\}} \cdot c_{\{4,49\}} \oplus A^{(0)}_{\{0,3,2\}} \cdot c_{\{2,50\}} \oplus A^{(0)}_{\{0,3,2\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{4,3,49\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{2,3,50\}} \oplus$$
$$A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{4,4,49\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{2,4,50\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot c_{\{4,49\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot c_{\{2,50\}} \oplus A^{(0)}_{\{3,3,3\}} \oplus A^{(0)}_{\{4,3,3\}} \cdot$$
$$A^{(0)}_{\{4,3,49\}} \oplus A^{(0)}_{\{4,3,3\}} \cdot A^{(0)}_{\{2,3,50\}} \oplus A^{(0)}_{\{4,3,3\}} \cdot A^{(0)}_{\{4,4,49\}} \oplus A^{(0)}_{\{4,3,3\}} \cdot A^{(0)}_{\{2,4,50\}} \oplus A^{(0)}_{\{4,3,3\}} \cdot c_{\{4,49\}} \oplus A^{(0)}_{\{4,3,3\}} \cdot$$
$$c_{\{2,50\}} \oplus A^{(0)}_{\{4,3,3\}} \oplus A^{(0)}_{\{1,3,7\}} \cdot A^{(0)}_{\{2,3,29\}} \oplus A^{(0)}_{\{1,3,7\}} \cdot A^{(0)}_{\{0,3,30\}} \oplus A^{(0)}_{\{1,3,7\}} \cdot A^{(0)}_{\{1,3,30\}} \oplus A^{(0)}_{\{1,3,7\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus$$
$$A^{(0)}_{\{1,3,7\}} \cdot A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{1,3,7\}} \cdot c_{\{2,29\}} \oplus A^{(0)}_{\{1,3,7\}} \cdot c_{\{0,30\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{2,3,29\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{0,3,30\}} \oplus$$
$$A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{1,3,30\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot c_{\{2,29\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot c_{\{0,30\}} \oplus$$
$$A^{(0)}_{\{4,3,19\}} \oplus A^{(0)}_{\{2,3,20\}} \oplus A^{(0)}_{\{2,3,29\}} \cdot A^{(0)}_{\{1,4,7\}} \oplus A^{(0)}_{\{2,3,29\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{2,3,29\}} \cdot c_{\{1,7\}} \oplus A^{(0)}_{\{2,3,29\}} \cdot c_{\{0,8\}} \oplus$$

$$A^{(0)}_{\{2,3,29\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{2,3,29\}} \oplus A^{(0)}_{\{0,3,30\}} \cdot A^{(0)}_{\{1,4,7\}} \oplus A^{(0)}_{\{0,3,30\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{0,3,30\}} \cdot c_{\{1,7\}} \oplus A^{(0)}_{\{0,3,30\}} \cdot$$
$$c_{\{0,8\}} \oplus A^{(0)}_{\{0,3,30\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{0,3,30\}} \oplus A^{(0)}_{\{1,3,30\}} \cdot A^{(0)}_{\{1,4,7\}} \oplus A^{(0)}_{\{1,3,30\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{1,3,30\}} \cdot c_{\{1,7\}} \oplus$$
$$A^{(0)}_{\{1,3,30\}} \cdot c_{\{0,8\}} \oplus A^{(0)}_{\{1,3,30\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{1,3,30\}} \oplus A^{(0)}_{\{2,3,30\}} \oplus A^{(0)}_{\{0,3,31\}} \oplus A^{(0)}_{\{3,3,31\}} \cdot A^{(0)}_{\{4,3,53\}} \oplus A^{(0)}_{\{3,3,31\}} \cdot$$
$$A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{3,3,31\}} \cdot A^{(0)}_{\{3,3,54\}} \oplus A^{(0)}_{\{3,3,31\}} \cdot A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{3,3,31\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{3,3,31\}} \cdot c_{\{2,54\}} \oplus A^{(0)}_{\{1,3,32\}} \cdot$$
$$A^{(0)}_{\{4,3,53\}} \oplus A^{(0)}_{\{1,3,32\}} \cdot A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{1,3,32\}} \cdot A^{(0)}_{\{3,3,54\}} \oplus A^{(0)}_{\{1,3,32\}} \cdot A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{1,3,32\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{1,3,32\}} \cdot$$
$$c_{\{2,54\}} \oplus A^{(0)}_{\{1,3,33\}} \cdot A^{(0)}_{\{0,3,35\}} \oplus A^{(0)}_{\{1,3,33\}} \cdot A^{(0)}_{\{3,3,36\}} \oplus A^{(0)}_{\{1,3,33\}} \cdot A^{(0)}_{\{0,4,35\}} \oplus A^{(0)}_{\{1,3,33\}} \cdot A^{(0)}_{\{3,4,36\}} \oplus A^{(0)}_{\{1,3,33\}} \cdot$$
$$c_{\{0,35\}} \oplus A^{(0)}_{\{1,3,33\}} \cdot c_{\{3,36\}} \oplus A^{(0)}_{\{1,3,33\}} \oplus A^{(0)}_{\{0,3,34\}} \cdot A^{(0)}_{\{0,3,35\}} \oplus A^{(0)}_{\{0,3,34\}} \cdot A^{(0)}_{\{3,3,36\}} \oplus A^{(0)}_{\{0,3,34\}} \cdot A^{(0)}_{\{0,4,35\}} \oplus$$
$$A^{(0)}_{\{0,3,34\}} \cdot A^{(0)}_{\{3,4,36\}} \oplus A^{(0)}_{\{0,3,34\}} \cdot c_{\{0,35\}} \oplus A^{(0)}_{\{0,3,34\}} \cdot c_{\{3,36\}} \oplus A^{(0)}_{\{0,3,34\}} \oplus A^{(0)}_{\{4,3,34\}} \cdot A^{(0)}_{\{0,3,35\}} \oplus A^{(0)}_{\{4,3,34\}} \cdot$$
$$A^{(0)}_{\{3,3,36\}} \oplus A^{(0)}_{\{4,3,34\}} \cdot A^{(0)}_{\{0,4,35\}} \oplus A^{(0)}_{\{4,3,34\}} \cdot A^{(0)}_{\{3,4,36\}} \oplus A^{(0)}_{\{4,3,34\}} \cdot c_{\{0,35\}} \oplus A^{(0)}_{\{4,3,34\}} \cdot c_{\{3,36\}} \oplus A^{(0)}_{\{4,3,34\}} \oplus$$
$$A^{(0)}_{\{0,3,35\}} \cdot A^{(0)}_{\{1,4,33\}} \oplus A^{(0)}_{\{0,3,35\}} \cdot A^{(0)}_{\{4,4,34\}} \oplus A^{(0)}_{\{0,3,35\}} \cdot c_{\{1,33\}} \oplus A^{(0)}_{\{0,3,35\}} \cdot c_{\{4,34\}} \oplus A^{(0)}_{\{3,3,36\}} \cdot A^{(0)}_{\{1,4,33\}} \oplus$$
$$A^{(0)}_{\{3,3,36\}} \cdot A^{(0)}_{\{4,4,34\}} \oplus A^{(0)}_{\{3,3,36\}} \cdot c_{\{1,33\}} \oplus A^{(0)}_{\{3,3,36\}} \cdot c_{\{4,34\}} \oplus A^{(0)}_{\{1,3,38\}} \oplus A^{(0)}_{\{4,3,39\}} \oplus A^{(0)}_{\{4,3,49\}} \cdot A^{(0)}_{\{0,4,2\}} \oplus$$
$$A^{(0)}_{\{4,3,49\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{4,3,49\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{4,3,49\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{2,3,50\}} \cdot A^{(0)}_{\{0,4,2\}} \oplus A^{(0)}_{\{2,3,50\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus$$
$$A^{(0)}_{\{2,3,50\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{2,3,50\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{4,3,53\}} \cdot A^{(0)}_{\{3,4,31\}} \oplus A^{(0)}_{\{4,3,53\}} \cdot A^{(0)}_{\{1,4,32\}} \oplus A^{(0)}_{\{4,3,53\}} \cdot c_{\{3,31\}} \oplus$$
$$A^{(0)}_{\{4,3,53\}} \cdot c_{\{1,32\}} \oplus A^{(0)}_{\{4,3,53\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{4,3,53\}} \oplus A^{(0)}_{\{0,3,54\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot A^{(0)}_{\{3,4,31\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot A^{(0)}_{\{1,4,32\}} \oplus$$
$$A^{(0)}_{\{2,3,54\}} \cdot c_{\{3,31\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot c_{\{1,32\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{3,3,54\}} \cdot A^{(0)}_{\{3,4,31\}} \oplus A^{(0)}_{\{3,3,54\}} \cdot$$
$$A^{(0)}_{\{1,4,32\}} \oplus A^{(0)}_{\{3,3,54\}} \cdot c_{\{3,31\}} \oplus A^{(0)}_{\{3,3,54\}} \cdot c_{\{1,32\}} \oplus A^{(0)}_{\{3,3,54\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{3,3,54\}} \oplus A^{(0)}_{\{3,3,55\}} \oplus A^{(0)}_{\{3,3,59\}} \cdot$$
$$A^{(0)}_{\{2,4,0\}} \oplus A^{(0)}_{\{3,3,59\}} \cdot A^{(0)}_{\{0,4,1\}} \oplus A^{(0)}_{\{3,3,59\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{3,3,59\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{3,3,59\}} \oplus A^{(0)}_{\{1,3,60\}} \cdot A^{(0)}_{\{2,4,0\}} \oplus$$
$$A^{(0)}_{\{1,3,60\}} \cdot A^{(0)}_{\{0,4,1\}} \oplus A^{(0)}_{\{1,3,60\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{1,3,60\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{1,3,60\}} \oplus A^{(0)}_{\{2,3,60\}} \cdot A^{(0)}_{\{2,4,0\}} \oplus A^{(0)}_{\{2,3,60\}} \cdot$$
$$A^{(0)}_{\{0,4,1\}} \oplus A^{(0)}_{\{2,3,60\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{2,3,60\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{2,3,60\}} \oplus A^{(0)}_{\{2,4,0\}} \cdot A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{2,4,0\}} \cdot A^{(0)}_{\{1,4,60\}} \oplus$$
$$A^{(0)}_{\{2,4,0\}} \cdot c_{\{1,60\}} \oplus A^{(0)}_{\{0,4,1\}} \cdot A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{0,4,1\}} \cdot A^{(0)}_{\{1,4,60\}} \oplus A^{(0)}_{\{0,4,1\}} \cdot c_{\{1,60\}} \oplus A^{(0)}_{\{0,4,2\}} \cdot A^{(0)}_{\{4,4,49\}} \oplus$$
$$A^{(0)}_{\{0,4,2\}} \cdot A^{(0)}_{\{2,4,50\}} \oplus A^{(0)}_{\{0,4,2\}} \cdot c_{\{4,49\}} \oplus A^{(0)}_{\{0,4,2\}} \cdot c_{\{2,50\}} \oplus A^{(0)}_{\{0,4,2\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot A^{(0)}_{\{4,4,49\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot$$
$$A^{(0)}_{\{2,4,50\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot c_{\{4,49\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot c_{\{2,50\}} \oplus A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{1,4,7\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{1,4,7\}} \cdot A^{(0)}_{\{0,4,30\}} \oplus$$
$$A^{(0)}_{\{1,4,7\}} \cdot c_{\{2,29\}} \oplus A^{(0)}_{\{1,4,7\}} \cdot c_{\{0,30\}} \oplus A^{(0)}_{\{4,4,8\}} \cdot A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{4,4,8\}} \cdot A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{4,4,8\}} \cdot c_{\{2,29\}} \oplus$$
$$A^{(0)}_{\{4,4,8\}} \cdot c_{\{0,30\}} \oplus A^{(0)}_{\{4,4,19\}} \oplus A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{2,4,29\}} \cdot c_{\{1,7\}} \oplus A^{(0)}_{\{2,4,29\}} \cdot c_{\{0,8\}} \oplus A^{(0)}_{\{2,4,29\}} \cdot c_{\{4,8\}} \oplus$$
$$A^{(0)}_{\{2,4,29\}} \oplus A^{(0)}_{\{0,4,30\}} \cdot c_{\{1,7\}} \oplus A^{(0)}_{\{0,4,30\}} \cdot c_{\{0,8\}} \oplus A^{(0)}_{\{0,4,30\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{0,4,30\}} \oplus A^{(0)}_{\{2,4,30\}} \oplus A^{(0)}_{\{0,4,31\}} \oplus$$
$$A^{(0)}_{\{3,4,31\}} \cdot A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{3,4,31\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{3,4,31\}} \cdot c_{\{2,54\}} \oplus A^{(0)}_{\{1,4,32\}} \cdot A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{1,4,32\}} \cdot A^{(0)}_{\{2,4,54\}} \oplus$$
$$A^{(0)}_{\{1,4,32\}} \cdot c_{\{2,54\}} \oplus A^{(0)}_{\{1,4,33\}} \cdot A^{(0)}_{\{0,4,35\}} \oplus A^{(0)}_{\{1,4,33\}} \cdot A^{(0)}_{\{3,4,36\}} \oplus A^{(0)}_{\{1,4,33\}} \cdot c_{\{0,35\}} \oplus A^{(0)}_{\{1,4,33\}} \cdot c_{\{3,36\}} \oplus$$
$$A^{(0)}_{\{1,4,33\}} \oplus A^{(0)}_{\{4,4,34\}} \cdot A^{(0)}_{\{0,4,35\}} \oplus A^{(0)}_{\{4,4,34\}} \cdot A^{(0)}_{\{3,4,36\}} \oplus A^{(0)}_{\{4,4,34\}} \cdot c_{\{0,35\}} \oplus A^{(0)}_{\{4,4,34\}} \cdot c_{\{3,36\}} \oplus A^{(0)}_{\{4,4,34\}} \oplus$$
$$A^{(0)}_{\{0,4,35\}} \cdot c_{\{1,33\}} \oplus A^{(0)}_{\{0,4,35\}} \cdot c_{\{4,34\}} \oplus A^{(0)}_{\{3,4,36\}} \cdot c_{\{1,33\}} \oplus A^{(0)}_{\{3,4,36\}} \cdot c_{\{4,34\}} \oplus A^{(0)}_{\{1,4,38\}} \oplus A^{(0)}_{\{4,4,39\}} \oplus$$
$$A^{(0)}_{\{4,4,49\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{4,4,49\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{2,4,50\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{2,4,50\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{4,4,53\}} \cdot c_{\{3,31\}} \oplus$$
$$A^{(0)}_{\{4,4,53\}} \cdot c_{\{1,32\}} \oplus A^{(0)}_{\{4,4,53\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{4,4,53\}} \oplus A^{(0)}_{\{0,4,54\}} \oplus A^{(0)}_{\{2,4,54\}} \cdot c_{\{3,31\}} \oplus A^{(0)}_{\{2,4,54\}} \cdot c_{\{1,32\}} \oplus$$
$$A^{(0)}_{\{2,4,54\}} \cdot c_{\{2,32\}} \oplus A^{(0)}_{\{2,4,54\}} \oplus A^{(0)}_{\{3,4,55\}} \oplus A^{(0)}_{\{3,4,59\}} \cdot c_{\{2,0\}} \oplus A^{(0)}_{\{3,4,59\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{1,4,60\}} \cdot$$
$$c_{\{2,0\}} \oplus A^{(0)}_{\{1,4,60\}} \cdot c_{\{0,1\}} \oplus A^{(0)}_{\{1,4,60\}} \oplus c_{\{2,0\}} \cdot c_{\{1,60\}} \oplus c_{\{0,1\}} \cdot c_{\{1,60\}} \oplus c_{\{0,2\}} \cdot c_{\{4,49\}} \oplus$$
$$c_{\{0,2\}} \cdot c_{\{2,50\}} \oplus c_{\{0,2\}} \oplus c_{\{3,3\}} \cdot c_{\{4,49\}} \oplus c_{\{3,3\}} \cdot c_{\{2,50\}} \oplus c_{\{3,3\}} \oplus c_{\{1,7\}} \cdot c_{\{2,29\}} \oplus$$
$$c_{\{1,7\}} \cdot c_{\{0,30\}} \oplus c_{\{0,8\}} \cdot c_{\{2,29\}} \oplus c_{\{0,8\}} \cdot c_{\{0,30\}} \oplus c_{\{4,8\}} \cdot c_{\{2,29\}} \oplus c_{\{4,8\}} \cdot c_{\{0,30\}} \oplus$$
$$c_{\{4,19\}} \oplus c_{\{2,20\}} \oplus c_{\{3,20\}} \oplus c_{\{2,29\}} \oplus c_{\{0,30\}} \oplus c_{\{2,30\}} \oplus c_{\{0,31\}} \oplus c_{\{3,31\}} \cdot c_{\{2,54\}} \oplus c_{\{1,32\}} \cdot$$
$$c_{\{2,54\}} \oplus c_{\{2,32\}} \cdot c_{\{2,54\}} \oplus c_{\{1,33\}} \cdot c_{\{0,35\}} \oplus c_{\{1,33\}} \cdot c_{\{3,36\}} \oplus c_{\{1,33\}} \oplus c_{\{4,34\}} \cdot c_{\{0,35\}} \oplus$$
$$c_{\{4,34\}} \cdot c_{\{3,36\}} \oplus c_{\{4,34\}} \oplus c_{\{1,38\}} \oplus c_{\{4,39\}} \oplus c_{\{2,54\}} \oplus c_{\{3,55\}} \oplus c_{\{4,55\}} \oplus c_{\{1,60\}}$$

$$\mathbf{D}^{(\mathbf{1})}_{\{\mathbf{2},\mathbf{5}\}} = A^{(0)}_{\{0,0,2\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{0,0,2\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{0,0,2\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{0,0,2\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{0,0,2\}} \cdot$$
$$A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{0,0,2\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{0,0,2\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot$$
$$A^{(0)}_{\{2,3,48\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot A^{(0)}_{\{3,3,48\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{2,0,26\}} \cdot$$
$$c_{\{2,48\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot A^{(0)}_{\{4,2,11\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot A^{(0)}_{\{4,3,11\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot A^{(0)}_{\{2,3,12\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot A^{(0)}_{\{4,4,11\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot$$
$$A^{(0)}_{\{2,4,12\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot A^{(0)}_{\{3,4,12\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot c_{\{4,11\}} \oplus A^{(0)}_{\{4,0,41\}} \cdot c_{\{2,12\}} \oplus A^{(0)}_{\{4,0,41\}} \oplus A^{(0)}_{\{4,0,49\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot$$
$$A^{(0)}_{\{3,2,53\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot A^{(0)}_{\{3,3,53\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot A^{(0)}_{\{1,3,54\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot A^{(0)}_{\{3,4,53\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot$$
$$A^{(0)}_{\{1,4,54\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot c_{\{3,53\}} \oplus A^{(0)}_{\{1,0,59\}} \cdot c_{\{1,54\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot$$
$$A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{0,1,2\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{1,1,25\}} \oplus$$
$$A^{(0)}_{\{2,1,26\}} \cdot A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{2,1,26\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{2,1,26\}} \cdot A^{(0)}_{\{2,3,48\}} \oplus A^{(0)}_{\{2,1,26\}} \cdot A^{(0)}_{\{3,3,48\}} \oplus A^{(0)}_{\{2,1,26\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus$$
$$A^{(0)}_{\{2,1,26\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{2,1,26\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{2,1,26\}} \cdot c_{\{2,48\}} \oplus A^{(0)}_{\{0,1,33\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot A^{(0)}_{\{3,2,53\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot$$
$$A^{(0)}_{\{3,3,53\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot A^{(0)}_{\{1,3,54\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot A^{(0)}_{\{3,4,53\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot A^{(0)}_{\{1,4,54\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot$$
$$c_{\{3,53\}} \oplus A^{(0)}_{\{1,1,59\}} \cdot c_{\{1,54\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot$$
$$A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{1,0,1\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{0,0,23\}} \oplus A^{(0)}_{\{2,0,44\}} \cdot A^{(0)}_{\{3,2,61\}} \oplus$$
$$A^{(0)}_{\{2,0,44\}} \cdot A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{2,0,44\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{2,0,44\}} \cdot A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{2,0,44\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{2,0,44\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus$$
$$A^{(0)}_{\{2,0,44\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{2,0,44\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{0,0,48\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot$$
$$A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{1,1,1\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{3,1,14\}} \oplus$$
$$A^{(0)}_{\{0,1,23\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot A^{(0)}_{\{3,2,61\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot$$
$$A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{2,1,44\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{0,1,48\}} \oplus A^{(0)}_{\{2,1,63\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot$$
$$A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot$$
$$c_{\{2,23\}} \oplus A^{(0)}_{\{1,2,1\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot$$
$$A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{4,2,2\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot A^{(0)}_{\{3,2,41\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot$$
$$A^{(0)}_{\{0,3,40\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot A^{(0)}_{\{3,3,41\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot A^{(0)}_{\{0,4,40\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot A^{(0)}_{\{3,4,41\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot c_{\{0,40\}} \oplus A^{(0)}_{\{4,2,11\}} \cdot$$
$$c_{\{3,41\}} \oplus A^{(0)}_{\{4,2,13\}} \oplus A^{(0)}_{\{0,2,23\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot A^{(0)}_{\{2,3,48\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot$$
$$A^{(0)}_{\{3,3,48\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{3,2,25\}} \cdot c_{\{2,48\}} \oplus A^{(0)}_{\{4,2,27\}} \oplus$$
$$A^{(0)}_{\{4,2,28\}} \cdot A^{(0)}_{\{3,2,30\}} \oplus A^{(0)}_{\{4,2,28\}} \cdot A^{(0)}_{\{4,2,30\}} \oplus A^{(0)}_{\{4,2,28\}} \cdot A^{(0)}_{\{0,3,29\}} \oplus A^{(0)}_{\{4,2,28\}} \cdot A^{(0)}_{\{3,3,30\}} \oplus A^{(0)}_{\{4,2,28\}} \cdot A^{(0)}_{\{0,4,29\}} \oplus$$
$$A^{(0)}_{\{4,2,28\}} \cdot A^{(0)}_{\{3,4,30\}} \oplus A^{(0)}_{\{4,2,28\}} \cdot c_{\{0,29\}} \oplus A^{(0)}_{\{4,2,28\}} \cdot c_{\{3,30\}} \oplus A^{(0)}_{\{4,2,28\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot A^{(0)}_{\{1,3,27\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot$$
$$A^{(0)}_{\{0,3,28\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot A^{(0)}_{\{4,3,28\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot A^{(0)}_{\{1,4,27\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot A^{(0)}_{\{4,4,28\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot c_{\{1,27\}} \oplus A^{(0)}_{\{3,2,30\}} \cdot$$
$$c_{\{4,28\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot A^{(0)}_{\{1,3,27\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot A^{(0)}_{\{0,3,28\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot A^{(0)}_{\{4,3,28\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot A^{(0)}_{\{1,4,27\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot$$
$$A^{(0)}_{\{4,4,28\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot c_{\{1,27\}} \oplus A^{(0)}_{\{4,2,30\}} \cdot c_{\{4,28\}} \oplus A^{(0)}_{\{4,2,33\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{4,3,11\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{2,3,12\}} \oplus$$
$$A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{4,4,11\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{2,4,12\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{3,4,12\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot c_{\{4,11\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot c_{\{2,12\}} \oplus$$
$$A^{(0)}_{\{3,2,41\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot A^{(0)}_{\{3,2,61\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot$$
$$A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{4,2,43\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot A^{(0)}_{\{3,2,61\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot$$
$$A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot$$
$$c_{\{0,60\}} \oplus A^{(0)}_{\{2,2,44\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot A^{(0)}_{\{3,2,61\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot$$
$$A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{3,2,44\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{4,2,46\}} \oplus$$
$$A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{3,3,25\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{1,3,26\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{3,4,25\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{1,4,26\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot c_{\{3,25\}} \oplus$$
$$A^{(0)}_{\{4,2,47\}} \cdot c_{\{1,26\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot c_{\{2,26\}} \oplus A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{0,2,48\}} \oplus A^{(0)}_{\{3,2,49\}} \oplus A^{(0)}_{\{3,2,52\}} \oplus A^{(0)}_{\{3,2,53\}} \cdot A^{(0)}_{\{2,3,58\}} \oplus$$

$$A^{(0)}_{\{3,2,53\}} \cdot A^{(0)}_{\{0,3,59\}} \oplus A^{(0)}_{\{3,2,53\}} \cdot A^{(0)}_{\{2,4,58\}} \oplus A^{(0)}_{\{3,2,53\}} \cdot A^{(0)}_{\{0,4,59\}} \oplus A^{(0)}_{\{3,2,53\}} \cdot c_{\{2,58\}} \oplus A^{(0)}_{\{3,2,53\}} \cdot c_{\{0,59\}} \oplus$$
$$A^{(0)}_{\{3,2,53\}} \cdot c_{\{1,59\}} \oplus A^{(0)}_{\{3,2,53\}} \oplus A^{(0)}_{\{3,2,60\}} \oplus A^{(0)}_{\{3,2,61\}} \cdot A^{(0)}_{\{4,3,43\}} \oplus A^{(0)}_{\{3,2,61\}} \cdot A^{(0)}_{\{2,3,44\}} \oplus A^{(0)}_{\{3,2,61\}} \cdot A^{(0)}_{\{4,4,43\}} \oplus$$
$$A^{(0)}_{\{3,2,61\}} \cdot A^{(0)}_{\{2,4,44\}} \oplus A^{(0)}_{\{3,2,61\}} \cdot c_{\{4,43\}} \oplus A^{(0)}_{\{3,2,61\}} \oplus A^{(0)}_{\{3,2,62\}} \oplus A^{(0)}_{\{1,3,1\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{1,3,1\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus$$
$$A^{(0)}_{\{1,3,1\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{1,3,1\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{1,3,1\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{1,3,1\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{1,3,1\}} \cdot c_{\{0,24\}} \oplus$$
$$A^{(0)}_{\{4,3,2\}} \cdot A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{4,3,2\}} \cdot A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{4,3,2\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{4,3,2\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{4,3,2\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus$$
$$A^{(0)}_{\{4,3,2\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{4,3,2\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{4,3,11\}} \cdot A^{(0)}_{\{0,3,40\}} \oplus A^{(0)}_{\{4,3,11\}} \cdot A^{(0)}_{\{3,3,41\}} \oplus A^{(0)}_{\{4,3,11\}} \cdot A^{(0)}_{\{0,4,40\}} \oplus$$
$$A^{(0)}_{\{4,3,11\}} \cdot A^{(0)}_{\{3,4,41\}} \oplus A^{(0)}_{\{4,3,11\}} \cdot c_{\{0,40\}} \oplus A^{(0)}_{\{4,3,11\}} \cdot c_{\{3,41\}} \oplus A^{(0)}_{\{2,3,12\}} \cdot A^{(0)}_{\{0,3,40\}} \oplus A^{(0)}_{\{2,3,12\}} \cdot A^{(0)}_{\{3,3,41\}} \oplus$$
$$A^{(0)}_{\{2,3,12\}} \cdot A^{(0)}_{\{0,4,40\}} \oplus A^{(0)}_{\{2,3,12\}} \cdot A^{(0)}_{\{3,4,41\}} \oplus A^{(0)}_{\{2,3,12\}} \cdot c_{\{0,40\}} \oplus A^{(0)}_{\{2,3,12\}} \cdot c_{\{3,41\}} \oplus A^{(0)}_{\{4,3,13\}} \oplus A^{(0)}_{\{2,3,14\}} \oplus$$
$$A^{(0)}_{\{2,3,22\}} \oplus A^{(0)}_{\{0,3,23\}} \oplus A^{(0)}_{\{1,3,23\}} \oplus A^{(0)}_{\{2,3,23\}} \cdot A^{(0)}_{\{1,4,1\}} \oplus A^{(0)}_{\{2,3,23\}} \cdot A^{(0)}_{\{4,4,2\}} \oplus A^{(0)}_{\{2,3,23\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{2,3,23\}} \cdot$$
$$c_{\{4,2\}} \oplus A^{(0)}_{\{2,3,23\}} \oplus A^{(0)}_{\{0,3,24\}} \cdot A^{(0)}_{\{1,4,1\}} \oplus A^{(0)}_{\{0,3,24\}} \cdot A^{(0)}_{\{4,4,2\}} \oplus A^{(0)}_{\{0,3,24\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{0,3,24\}} \cdot c_{\{4,2\}} \oplus$$
$$A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot A^{(0)}_{\{1,4,1\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot A^{(0)}_{\{4,4,2\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot c_{\{4,2\}} \oplus A^{(0)}_{\{1,3,24\}} \oplus$$
$$A^{(0)}_{\{2,3,24\}} \oplus A^{(0)}_{\{0,3,25\}} \oplus A^{(0)}_{\{3,3,25\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{3,3,25\}} \cdot A^{(0)}_{\{2,3,48\}} \oplus A^{(0)}_{\{3,3,25\}} \cdot A^{(0)}_{\{3,3,48\}} \oplus A^{(0)}_{\{3,3,25\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus$$
$$A^{(0)}_{\{3,3,25\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{3,3,25\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{3,3,25\}} \cdot c_{\{2,48\}} \oplus A^{(0)}_{\{1,3,26\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{1,3,26\}} \cdot A^{(0)}_{\{2,3,48\}} \oplus$$
$$A^{(0)}_{\{1,3,26\}} \cdot A^{(0)}_{\{3,3,48\}} \oplus A^{(0)}_{\{1,3,26\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{1,3,26\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{1,3,26\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{1,3,26\}} \cdot c_{\{2,48\}} \oplus$$
$$A^{(0)}_{\{1,3,26\}} \oplus A^{(0)}_{\{0,3,27\}} \oplus A^{(0)}_{\{1,3,27\}} \cdot A^{(0)}_{\{0,3,29\}} \oplus A^{(0)}_{\{1,3,27\}} \cdot A^{(0)}_{\{3,3,30\}} \oplus A^{(0)}_{\{1,3,27\}} \cdot A^{(0)}_{\{0,4,29\}} \oplus A^{(0)}_{\{1,3,27\}} \cdot A^{(0)}_{\{3,4,30\}} \oplus$$
$$A^{(0)}_{\{1,3,27\}} \cdot c_{\{0,29\}} \oplus A^{(0)}_{\{1,3,27\}} \cdot c_{\{3,30\}} \oplus A^{(0)}_{\{1,3,27\}} \oplus A^{(0)}_{\{4,3,27\}} \oplus A^{(0)}_{\{0,3,28\}} \cdot A^{(0)}_{\{0,3,29\}} \oplus A^{(0)}_{\{0,3,28\}} \cdot A^{(0)}_{\{3,3,30\}} \oplus$$
$$A^{(0)}_{\{0,3,28\}} \cdot A^{(0)}_{\{0,4,29\}} \oplus A^{(0)}_{\{0,3,28\}} \cdot A^{(0)}_{\{3,4,30\}} \oplus A^{(0)}_{\{0,3,28\}} \cdot c_{\{0,29\}} \oplus A^{(0)}_{\{0,3,28\}} \cdot c_{\{3,30\}} \oplus A^{(0)}_{\{0,3,28\}} \oplus A^{(0)}_{\{4,3,28\}} \cdot$$
$$A^{(0)}_{\{0,3,29\}} \oplus A^{(0)}_{\{4,3,28\}} \cdot A^{(0)}_{\{3,3,30\}} \oplus A^{(0)}_{\{4,3,28\}} \cdot A^{(0)}_{\{0,4,29\}} \oplus A^{(0)}_{\{4,3,28\}} \cdot A^{(0)}_{\{3,4,30\}} \oplus A^{(0)}_{\{4,3,28\}} \cdot c_{\{0,29\}} \oplus A^{(0)}_{\{4,3,28\}} \cdot$$
$$c_{\{3,30\}} \oplus A^{(0)}_{\{4,3,28\}} \oplus A^{(0)}_{\{0,3,29\}} \cdot A^{(0)}_{\{1,4,27\}} \oplus A^{(0)}_{\{0,3,29\}} \cdot A^{(0)}_{\{4,4,28\}} \oplus A^{(0)}_{\{0,3,29\}} \cdot c_{\{1,27\}} \oplus A^{(0)}_{\{0,3,29\}} \cdot c_{\{4,28\}} \oplus$$
$$A^{(0)}_{\{3,3,30\}} \cdot A^{(0)}_{\{1,4,27\}} \oplus A^{(0)}_{\{3,3,30\}} \cdot A^{(0)}_{\{4,4,28\}} \oplus A^{(0)}_{\{3,3,30\}} \cdot c_{\{1,27\}} \oplus A^{(0)}_{\{3,3,30\}} \cdot c_{\{4,28\}} \oplus A^{(0)}_{\{1,3,32\}} \oplus A^{(0)}_{\{4,3,33\}} \oplus$$
$$A^{(0)}_{\{0,3,40\}} \cdot A^{(0)}_{\{4,4,11\}} \oplus A^{(0)}_{\{0,3,40\}} \cdot A^{(0)}_{\{2,4,12\}} \oplus A^{(0)}_{\{0,3,40\}} \cdot A^{(0)}_{\{3,4,12\}} \oplus A^{(0)}_{\{0,3,40\}} \cdot c_{\{4,11\}} \oplus A^{(0)}_{\{0,3,40\}} \cdot c_{\{2,12\}} \oplus$$
$$A^{(0)}_{\{0,3,40\}} \oplus A^{(0)}_{\{3,3,41\}} \cdot A^{(0)}_{\{4,4,11\}} \oplus A^{(0)}_{\{3,3,41\}} \cdot A^{(0)}_{\{2,4,12\}} \oplus A^{(0)}_{\{3,3,41\}} \cdot A^{(0)}_{\{3,4,12\}} \oplus A^{(0)}_{\{3,3,41\}} \cdot c_{\{4,11\}} \oplus A^{(0)}_{\{3,3,41\}} \cdot$$
$$c_{\{2,12\}} \oplus A^{(0)}_{\{3,3,41\}} \oplus A^{(0)}_{\{4,3,43\}} \cdot A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{4,3,43\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{4,3,43\}} \cdot A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{4,3,43\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus$$
$$A^{(0)}_{\{4,3,43\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{4,3,43\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{4,3,43\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{2,3,44\}} \cdot A^{(0)}_{\{0,3,60\}} \oplus A^{(0)}_{\{2,3,44\}} \cdot A^{(0)}_{\{3,3,61\}} \oplus$$
$$A^{(0)}_{\{2,3,44\}} \cdot A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{2,3,44\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{2,3,44\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{2,3,44\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{2,3,44\}} \cdot c_{\{3,61\}} \oplus$$
$$A^{(0)}_{\{4,3,46\}} \oplus A^{(0)}_{\{2,3,47\}} \oplus A^{(0)}_{\{3,3,47\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot A^{(0)}_{\{3,4,25\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot A^{(0)}_{\{1,4,26\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot c_{\{3,25\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot$$
$$c_{\{1,26\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot c_{\{2,26\}} \oplus A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{0,3,48\}} \oplus A^{(0)}_{\{2,3,48\}} \cdot A^{(0)}_{\{3,4,25\}} \oplus A^{(0)}_{\{2,3,48\}} \cdot A^{(0)}_{\{1,4,26\}} \oplus A^{(0)}_{\{2,3,48\}} \cdot$$
$$c_{\{3,25\}} \oplus A^{(0)}_{\{2,3,48\}} \cdot c_{\{1,26\}} \oplus A^{(0)}_{\{2,3,48\}} \cdot c_{\{2,26\}} \oplus A^{(0)}_{\{2,3,48\}} \oplus A^{(0)}_{\{3,3,48\}} \cdot A^{(0)}_{\{3,4,25\}} \oplus A^{(0)}_{\{3,3,48\}} \cdot A^{(0)}_{\{1,4,26\}} \oplus$$
$$A^{(0)}_{\{3,3,48\}} \cdot c_{\{3,25\}} \oplus A^{(0)}_{\{3,3,48\}} \cdot c_{\{1,26\}} \oplus A^{(0)}_{\{3,3,48\}} \cdot c_{\{2,26\}} \oplus A^{(0)}_{\{3,3,48\}} \oplus A^{(0)}_{\{3,3,49\}} \oplus A^{(0)}_{\{3,3,52\}} \oplus A^{(0)}_{\{1,3,53\}} \oplus$$
$$A^{(0)}_{\{2,3,53\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot A^{(0)}_{\{2,3,58\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot A^{(0)}_{\{0,3,59\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot A^{(0)}_{\{2,4,58\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot A^{(0)}_{\{0,4,59\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot$$
$$c_{\{2,58\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot c_{\{0,59\}} \oplus A^{(0)}_{\{3,3,53\}} \cdot c_{\{1,59\}} \oplus A^{(0)}_{\{3,3,53\}} \oplus A^{(0)}_{\{1,3,54\}} \cdot A^{(0)}_{\{2,3,58\}} \oplus A^{(0)}_{\{1,3,54\}} \cdot A^{(0)}_{\{0,3,59\}} \oplus$$
$$A^{(0)}_{\{1,3,54\}} \cdot A^{(0)}_{\{2,4,58\}} \oplus A^{(0)}_{\{1,3,54\}} \cdot A^{(0)}_{\{0,4,59\}} \oplus A^{(0)}_{\{1,3,54\}} \cdot c_{\{2,58\}} \oplus A^{(0)}_{\{1,3,54\}} \cdot c_{\{0,59\}} \oplus A^{(0)}_{\{1,3,54\}} \cdot c_{\{1,59\}} \oplus$$
$$A^{(0)}_{\{1,3,54\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot A^{(0)}_{\{2,3,58\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot A^{(0)}_{\{0,3,59\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot A^{(0)}_{\{2,4,58\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot A^{(0)}_{\{0,4,59\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot$$
$$c_{\{2,58\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot c_{\{0,59\}} \oplus A^{(0)}_{\{2,3,54\}} \cdot c_{\{1,59\}} \oplus A^{(0)}_{\{2,3,54\}} \oplus A^{(0)}_{\{2,3,58\}} \cdot A^{(0)}_{\{3,4,53\}} \oplus A^{(0)}_{\{2,3,58\}} \cdot A^{(0)}_{\{1,4,54\}} \oplus$$
$$A^{(0)}_{\{2,3,58\}} \cdot c_{\{3,53\}} \oplus A^{(0)}_{\{2,3,58\}} \cdot c_{\{1,54\}} \oplus A^{(0)}_{\{0,3,59\}} \cdot A^{(0)}_{\{3,4,53\}} \oplus A^{(0)}_{\{0,3,59\}} \cdot A^{(0)}_{\{1,4,54\}} \oplus A^{(0)}_{\{0,3,59\}} \cdot c_{\{3,53\}} \oplus$$
$$A^{(0)}_{\{0,3,59\}} \cdot c_{\{1,54\}} \oplus A^{(0)}_{\{0,3,59\}} \oplus A^{(0)}_{\{0,3,60\}} \cdot A^{(0)}_{\{4,4,43\}} \oplus A^{(0)}_{\{0,3,60\}} \cdot A^{(0)}_{\{2,4,44\}} \oplus A^{(0)}_{\{0,3,60\}} \cdot c_{\{4,43\}} \oplus A^{(0)}_{\{0,3,60\}} \oplus$$
$$A^{(0)}_{\{3,3,60\}} \oplus A^{(0)}_{\{4,3,60\}} \oplus A^{(0)}_{\{3,3,61\}} \cdot A^{(0)}_{\{4,4,43\}} \oplus A^{(0)}_{\{3,3,61\}} \cdot A^{(0)}_{\{2,4,44\}} \oplus A^{(0)}_{\{3,3,61\}} \cdot c_{\{4,43\}} \oplus A^{(0)}_{\{3,3,61\}} \oplus A^{(0)}_{\{4,3,61\}} \cdot$$

$$A^{(0)}_{\{4,4,43\}} \oplus A^{(0)}_{\{4,3,61\}} \cdot A^{(0)}_{\{2,4,44\}} \oplus A^{(0)}_{\{4,3,61\}} \cdot c_{\{4,43\}} \oplus A^{(0)}_{\{4,3,61\}} \oplus A^{(0)}_{\{3,3,62\}} \oplus A^{(0)}_{\{1,3,63\}} \oplus A^{(0)}_{\{1,4,1\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus$$
$$A^{(0)}_{\{1,4,1\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{1,4,1\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{1,4,1\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{4,4,2\}} \cdot A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{4,4,2\}} \cdot A^{(0)}_{\{0,4,24\}} \oplus$$
$$A^{(0)}_{\{4,4,2\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{4,4,2\}} \cdot c_{\{0,24\}} \oplus A^{(0)}_{\{4,4,11\}} \cdot A^{(0)}_{\{0,4,40\}} \oplus A^{(0)}_{\{4,4,11\}} \cdot A^{(0)}_{\{3,4,41\}} \oplus A^{(0)}_{\{4,4,11\}} \cdot c_{\{0,40\}} \oplus$$
$$A^{(0)}_{\{4,4,11\}} \cdot c_{\{3,41\}} \oplus A^{(0)}_{\{2,4,12\}} \cdot A^{(0)}_{\{0,4,40\}} \oplus A^{(0)}_{\{2,4,12\}} \cdot A^{(0)}_{\{3,4,41\}} \oplus A^{(0)}_{\{2,4,12\}} \cdot c_{\{0,40\}} \oplus A^{(0)}_{\{2,4,12\}} \cdot c_{\{3,41\}} \oplus$$
$$A^{(0)}_{\{3,4,12\}} \cdot A^{(0)}_{\{0,4,40\}} \oplus A^{(0)}_{\{3,4,12\}} \cdot A^{(0)}_{\{3,4,41\}} \oplus A^{(0)}_{\{3,4,12\}} \cdot c_{\{0,40\}} \oplus A^{(0)}_{\{3,4,12\}} \cdot c_{\{3,41\}} \oplus A^{(0)}_{\{4,4,13\}} \oplus A^{(0)}_{\{2,4,14\}} \oplus$$
$$A^{(0)}_{\{2,4,22\}} \oplus A^{(0)}_{\{0,4,23\}} \oplus A^{(0)}_{\{2,4,23\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{2,4,23\}} \cdot c_{\{4,2\}} \oplus A^{(0)}_{\{2,4,23\}} \oplus A^{(0)}_{\{0,4,24\}} \cdot c_{\{0,2\}} \oplus A^{(0)}_{\{0,4,24\}} \cdot$$
$$c_{\{4,2\}} \oplus A^{(0)}_{\{0,4,24\}} \oplus A^{(0)}_{\{2,4,24\}} \oplus A^{(0)}_{\{0,4,25\}} \oplus A^{(0)}_{\{3,4,25\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{3,4,25\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{3,4,25\}} \cdot c_{\{4,47\}} \oplus$$
$$A^{(0)}_{\{3,4,25\}} \cdot c_{\{2,48\}} \oplus A^{(0)}_{\{1,4,26\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{1,4,26\}} \cdot A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{1,4,26\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{1,4,26\}} \cdot c_{\{2,48\}} \oplus$$
$$A^{(0)}_{\{1,4,26\}} \oplus A^{(0)}_{\{1,4,27\}} \cdot A^{(0)}_{\{0,4,29\}} \oplus A^{(0)}_{\{1,4,27\}} \cdot A^{(0)}_{\{3,4,30\}} \oplus A^{(0)}_{\{1,4,27\}} \cdot c_{\{0,29\}} \oplus A^{(0)}_{\{1,4,27\}} \cdot c_{\{3,30\}} \oplus A^{(0)}_{\{1,4,27\}} \oplus$$
$$A^{(0)}_{\{4,4,27\}} \oplus A^{(0)}_{\{4,4,28\}} \cdot A^{(0)}_{\{0,4,29\}} \oplus A^{(0)}_{\{4,4,28\}} \cdot A^{(0)}_{\{3,4,30\}} \oplus A^{(0)}_{\{4,4,28\}} \cdot c_{\{0,29\}} \oplus A^{(0)}_{\{4,4,28\}} \cdot c_{\{3,30\}} \oplus A^{(0)}_{\{4,4,28\}} \oplus$$
$$A^{(0)}_{\{0,4,29\}} \cdot c_{\{1,27\}} \oplus A^{(0)}_{\{0,4,29\}} \cdot c_{\{4,28\}} \oplus A^{(0)}_{\{3,4,30\}} \cdot c_{\{1,27\}} \oplus A^{(0)}_{\{3,4,30\}} \cdot c_{\{4,28\}} \oplus A^{(0)}_{\{1,4,32\}} \oplus A^{(0)}_{\{4,4,33\}} \oplus$$
$$A^{(0)}_{\{0,4,40\}} \cdot c_{\{4,11\}} \oplus A^{(0)}_{\{0,4,40\}} \cdot c_{\{2,12\}} \oplus A^{(0)}_{\{0,4,40\}} \oplus A^{(0)}_{\{3,4,41\}} \cdot c_{\{4,11\}} \oplus A^{(0)}_{\{3,4,41\}} \cdot c_{\{2,12\}} \oplus A^{(0)}_{\{3,4,41\}} \oplus$$
$$A^{(0)}_{\{4,4,43\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus A^{(0)}_{\{4,4,43\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{4,4,43\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{4,4,43\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{2,4,44\}} \cdot A^{(0)}_{\{0,4,60\}} \oplus$$
$$A^{(0)}_{\{2,4,44\}} \cdot A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{2,4,44\}} \cdot c_{\{0,60\}} \oplus A^{(0)}_{\{2,4,44\}} \cdot c_{\{3,61\}} \oplus A^{(0)}_{\{4,4,46\}} \oplus A^{(0)}_{\{2,4,47\}} \oplus A^{(0)}_{\{4,4,47\}} \cdot c_{\{3,25\}} \oplus$$
$$A^{(0)}_{\{4,4,47\}} \cdot c_{\{1,26\}} \oplus A^{(0)}_{\{4,4,47\}} \cdot c_{\{2,26\}} \oplus A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{0,4,48\}} \oplus A^{(0)}_{\{2,4,48\}} \cdot c_{\{3,25\}} \oplus A^{(0)}_{\{2,4,48\}} \cdot c_{\{1,26\}} \oplus$$
$$A^{(0)}_{\{2,4,48\}} \cdot c_{\{2,26\}} \oplus A^{(0)}_{\{2,4,48\}} \oplus A^{(0)}_{\{3,4,49\}} \oplus A^{(0)}_{\{3,4,52\}} \oplus A^{(0)}_{\{1,4,53\}} \oplus A^{(0)}_{\{3,4,53\}} \cdot A^{(0)}_{\{2,4,58\}} \oplus A^{(0)}_{\{3,4,53\}} \cdot A^{(0)}_{\{0,4,59\}} \oplus$$
$$A^{(0)}_{\{3,4,53\}} \cdot c_{\{2,58\}} \oplus A^{(0)}_{\{3,4,53\}} \cdot c_{\{0,59\}} \oplus A^{(0)}_{\{3,4,53\}} \cdot c_{\{1,59\}} \oplus A^{(0)}_{\{3,4,53\}} \oplus A^{(0)}_{\{1,4,54\}} \cdot A^{(0)}_{\{2,4,58\}} \oplus A^{(0)}_{\{1,4,54\}} \cdot$$
$$A^{(0)}_{\{0,4,59\}} \oplus A^{(0)}_{\{1,4,54\}} \cdot c_{\{2,58\}} \oplus A^{(0)}_{\{1,4,54\}} \cdot c_{\{0,59\}} \oplus A^{(0)}_{\{1,4,54\}} \cdot c_{\{1,59\}} \oplus A^{(0)}_{\{1,4,54\}} \oplus A^{(0)}_{\{2,4,58\}} \cdot c_{\{3,53\}} \oplus$$
$$A^{(0)}_{\{2,4,58\}} \cdot c_{\{1,54\}} \oplus A^{(0)}_{\{0,4,59\}} \cdot c_{\{3,53\}} \oplus A^{(0)}_{\{0,4,59\}} \cdot c_{\{1,54\}} \oplus A^{(0)}_{\{0,4,59\}} \oplus A^{(0)}_{\{0,4,60\}} \cdot c_{\{4,43\}} \oplus A^{(0)}_{\{0,4,60\}} \oplus$$
$$A^{(0)}_{\{3,4,60\}} \oplus A^{(0)}_{\{3,4,61\}} \cdot c_{\{4,43\}} \oplus A^{(0)}_{\{3,4,61\}} \oplus A^{(0)}_{\{3,4,62\}} \oplus A^{(0)}_{\{1,4,63\}} \oplus c_{\{0,2\}} \cdot c_{\{2,23\}} \oplus c_{\{0,2\}} \cdot c_{\{0,24\}} \oplus$$
$$c_{\{4,2\}} \cdot c_{\{2,23\}} \oplus c_{\{4,2\}} \cdot c_{\{0,24\}} \oplus c_{\{4,11\}} \cdot c_{\{0,40\}} \oplus c_{\{4,11\}} \cdot c_{\{3,41\}} \oplus c_{\{2,12\}} \cdot c_{\{0,40\}} \oplus$$
$$c_{\{2,12\}} \cdot c_{\{3,41\}} \oplus c_{\{4,13\}} \oplus c_{\{2,14\}} \oplus c_{\{2,22\}} \oplus c_{\{2,23\}} \oplus c_{\{0,24\}} \oplus c_{\{2,24\}} \oplus c_{\{0,25\}} \oplus c_{\{3,25\}} \cdot$$
$$c_{\{4,47\}} \oplus c_{\{3,25\}} \cdot c_{\{2,48\}} \oplus c_{\{1,26\}} \cdot c_{\{4,47\}} \oplus c_{\{1,26\}} \cdot c_{\{2,48\}} \oplus c_{\{1,26\}} \oplus c_{\{2,26\}} \cdot c_{\{4,47\}} \oplus$$
$$c_{\{2,26\}} \cdot c_{\{2,48\}} \oplus c_{\{1,27\}} \cdot c_{\{0,29\}} \oplus c_{\{1,27\}} \cdot c_{\{3,30\}} \oplus c_{\{1,27\}} \oplus c_{\{4,27\}} \oplus c_{\{4,28\}} \cdot c_{\{0,29\}} \oplus$$
$$c_{\{4,28\}} \cdot c_{\{3,30\}} \oplus c_{\{4,28\}} \oplus c_{\{1,32\}} \oplus c_{\{4,33\}} \oplus c_{\{0,40\}} \oplus c_{\{3,41\}} \oplus c_{\{4,43\}} \cdot c_{\{0,60\}} \oplus c_{\{4,43\}} \cdot$$
$$c_{\{3,61\}} \oplus c_{\{4,46\}} \oplus c_{\{2,47\}} \oplus c_{\{4,47\}} \oplus c_{\{2,48\}} \oplus c_{\{3,49\}} \oplus c_{\{4,49\}} \oplus c_{\{3,52\}} \oplus c_{\{1,53\}} \oplus c_{\{3,53\}} \cdot$$
$$c_{\{2,58\}} \oplus c_{\{3,53\}} \cdot c_{\{0,59\}} \oplus c_{\{3,53\}} \cdot c_{\{1,59\}} \oplus c_{\{3,53\}} \oplus c_{\{1,54\}} \cdot c_{\{2,58\}} \oplus c_{\{1,54\}} \cdot c_{\{0,59\}} \oplus$$
$$c_{\{1,54\}} \cdot c_{\{1,59\}} \oplus c_{\{1,54\}} \oplus c_{\{0,59\}} \oplus c_{\{0,60\}} \oplus c_{\{3,60\}} \oplus c_{\{3,61\}} \oplus c_{\{3,62\}} \oplus c_{\{1,63\}}$$
$$\theta^{(\mathbf{1})}_{\{\mathbf{2},\mathbf{3},\mathbf{2}\}} = A^{(0)}_{\{3,0,11\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot A^{(0)}_{\{4,2,44\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot A^{(0)}_{\{4,3,44\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot A^{(0)}_{\{2,3,45\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot A^{(0)}_{\{3,3,45\}} \oplus$$
$$A^{(0)}_{\{2,0,23\}} \cdot A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot c_{\{4,44\}} \oplus A^{(0)}_{\{2,0,23\}} \cdot c_{\{2,45\}} \oplus A^{(0)}_{\{3,0,37\}} \cdot A^{(0)}_{\{3,2,3\}} \oplus$$
$$A^{(0)}_{\{3,0,37\}} \cdot A^{(0)}_{\{3,3,3\}} \oplus A^{(0)}_{\{3,0,37\}} \cdot A^{(0)}_{\{1,3,4\}} \oplus A^{(0)}_{\{3,0,37\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{3,0,37\}} \cdot A^{(0)}_{\{1,4,4\}} \oplus A^{(0)}_{\{3,0,37\}} \cdot A^{(0)}_{\{2,4,4\}} \oplus$$
$$A^{(0)}_{\{3,0,37\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{3,0,37\}} \cdot c_{\{1,4\}} \oplus A^{(0)}_{\{3,0,37\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{2,0,9\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{2,1,9\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot$$
$$A^{(0)}_{\{4,2,8\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{2,2,9\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{4,3,8\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{2,3,9\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot$$
$$A^{(0)}_{\{2,4,9\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{4,0,38\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{4,0,38\}} \oplus A^{(0)}_{\{4,0,46\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot A^{(0)}_{\{3,2,50\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot$$
$$A^{(0)}_{\{3,3,50\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot A^{(0)}_{\{1,3,51\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot A^{(0)}_{\{2,3,51\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot A^{(0)}_{\{3,4,50\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot A^{(0)}_{\{1,4,51\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot$$
$$c_{\{3,50\}} \oplus A^{(0)}_{\{1,0,56\}} \cdot c_{\{1,51\}} \oplus A^{(0)}_{\{1,0,56\}} \oplus A^{(0)}_{\{0,0,63\}} \cdot A^{(0)}_{\{2,3,20\}} \oplus A^{(0)}_{\{0,0,63\}} \cdot A^{(0)}_{\{0,3,21\}} \oplus A^{(0)}_{\{0,0,63\}} \cdot A^{(0)}_{\{1,3,21\}} \oplus$$
$$A^{(0)}_{\{0,0,63\}} \cdot A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{0,0,63\}} \cdot A^{(0)}_{\{0,4,21\}} \oplus A^{(0)}_{\{0,0,63\}} \cdot c_{\{2,20\}} \oplus A^{(0)}_{\{0,0,63\}} \cdot c_{\{0,21\}} \oplus A^{(0)}_{\{1,1,22\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot$$
$$A^{(0)}_{\{4,2,44\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot A^{(0)}_{\{4,3,44\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot A^{(0)}_{\{2,3,45\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot A^{(0)}_{\{3,3,45\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot$$

$$A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot c_{\{4,44\}} \oplus A^{(0)}_{\{2,1,23\}} \cdot c_{\{2,45\}} \oplus A^{(0)}_{\{0,1,30\}} \oplus A^{(0)}_{\{1,1,56\}} \cdot A^{(0)}_{\{3,2,50\}} \oplus A^{(0)}_{\{1,1,56\}} \cdot A^{(0)}_{\{3,3,50\}} \oplus$$
$$A^{(0)}_{\{1,1,56\}} \cdot A^{(0)}_{\{1,3,51\}} \oplus A^{(0)}_{\{1,1,56\}} \cdot A^{(0)}_{\{2,3,51\}} \oplus A^{(0)}_{\{1,1,56\}} \cdot A^{(0)}_{\{3,4,50\}} \oplus A^{(0)}_{\{1,1,56\}} \cdot A^{(0)}_{\{1,4,51\}} \oplus A^{(0)}_{\{1,1,56\}} \cdot c_{\{3,50\}} \oplus$$
$$A^{(0)}_{\{1,1,56\}} \cdot c_{\{1,51\}} \oplus A^{(0)}_{\{1,1,56\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot A^{(0)}_{\{2,3,20\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot A^{(0)}_{\{0,3,21\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot A^{(0)}_{\{1,3,21\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot$$
$$A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot A^{(0)}_{\{0,4,21\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot c_{\{2,20\}} \oplus A^{(0)}_{\{0,1,63\}} \cdot c_{\{0,21\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot$$
$$A^{(0)}_{\{1,3,46\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot A^{(0)}_{\{0,4,47\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot$$
$$c_{\{1,46\}} \oplus A^{(0)}_{\{1,0,0\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{1,0,0\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{0,0,37\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{0,1,37\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{0,2,37\}} \oplus$$
$$A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{3,2,38\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{2,0,9\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus$$
$$A^{(0)}_{\{2,0,9\}} \cdot c_{\{3,38\}} \oplus A^{(0)}_{\{2,0,11\}} \oplus A^{(0)}_{\{0,0,20\}} \oplus A^{(0)}_{\{0,0,22\}} \oplus A^{(0)}_{\{4,0,24\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{2,1,9\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{4,2,8\}} \oplus$$
$$A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{2,2,9\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{4,3,8\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{2,3,9\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{2,4,9\}} \oplus$$
$$A^{(0)}_{\{0,0,37\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{0,0,37\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{0,0,37\}} \oplus A^{(0)}_{\{2,0,44\}} \oplus A^{(0)}_{\{3,0,59\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot$$
$$A^{(0)}_{\{1,3,46\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot A^{(0)}_{\{0,4,47\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot$$
$$c_{\{1,46\}} \oplus A^{(0)}_{\{2,0,63\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{2,0,63\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{0,1,37\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{0,2,37\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{3,2,38\}} \oplus$$
$$A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{2,1,9\}} \cdot c_{\{3,38\}} \oplus$$
$$A^{(0)}_{\{2,1,11\}} \oplus A^{(0)}_{\{0,1,20\}} \oplus A^{(0)}_{\{0,1,22\}} \oplus A^{(0)}_{\{4,1,24\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{4,2,8\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{2,2,9\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{4,3,8\}} \oplus$$
$$A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{2,3,9\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{2,4,9\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{0,1,37\}} \cdot c_{\{4,8\}} \oplus$$
$$A^{(0)}_{\{0,1,37\}} \oplus A^{(0)}_{\{2,1,44\}} \oplus A^{(0)}_{\{3,1,59\}} \oplus A^{(0)}_{\{2,1,60\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot A^{(0)}_{\{4,2,47\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot A^{(0)}_{\{1,3,46\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus$$
$$A^{(0)}_{\{2,1,63\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot A^{(0)}_{\{0,4,47\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot c_{\{1,46\}} \oplus A^{(0)}_{\{2,1,63\}} \cdot c_{\{4,47\}} \oplus$$
$$A^{(0)}_{\{2,1,63\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{4,2,36\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{4,3,36\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{2,3,37\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot$$
$$A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot c_{\{4,36\}} \oplus A^{(0)}_{\{3,2,3\}} \cdot c_{\{2,37\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{0,2,37\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{3,2,38\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot$$
$$A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{4,2,8\}} \cdot c_{\{3,38\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot$$
$$A^{(0)}_{\{0,2,37\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot A^{(0)}_{\{3,2,38\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot$$
$$A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{2,2,9\}} \cdot c_{\{3,38\}} \oplus A^{(0)}_{\{4,2,10\}} \oplus A^{(0)}_{\{2,2,11\}} \oplus A^{(0)}_{\{0,2,20\}} \oplus A^{(0)}_{\{0,2,22\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot A^{(0)}_{\{4,2,44\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot$$
$$A^{(0)}_{\{4,3,44\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot A^{(0)}_{\{2,3,45\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot A^{(0)}_{\{3,3,45\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot$$
$$c_{\{4,44\}} \oplus A^{(0)}_{\{3,2,22\}} \cdot c_{\{2,45\}} \oplus A^{(0)}_{\{4,2,24\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot A^{(0)}_{\{3,2,27\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot A^{(0)}_{\{4,2,27\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot A^{(0)}_{\{0,3,26\}} \oplus$$
$$A^{(0)}_{\{4,2,25\}} \cdot A^{(0)}_{\{3,3,27\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot A^{(0)}_{\{0,4,26\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot A^{(0)}_{\{3,4,27\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot c_{\{0,26\}} \oplus A^{(0)}_{\{4,2,25\}} \cdot c_{\{3,27\}} \oplus$$
$$A^{(0)}_{\{4,2,25\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot A^{(0)}_{\{0,3,25\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot A^{(0)}_{\{4,3,25\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot A^{(0)}_{\{1,4,24\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot$$
$$A^{(0)}_{\{4,4,25\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot c_{\{1,24\}} \oplus A^{(0)}_{\{3,2,27\}} \cdot c_{\{4,25\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot A^{(0)}_{\{0,3,25\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot$$
$$A^{(0)}_{\{4,3,25\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot A^{(0)}_{\{1,4,24\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot A^{(0)}_{\{4,4,25\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot c_{\{1,24\}} \oplus A^{(0)}_{\{4,2,27\}} \cdot c_{\{4,25\}} \oplus A^{(0)}_{\{4,2,30\}} \oplus$$
$$A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{3,3,3\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{1,3,4\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{1,4,4\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot A^{(0)}_{\{2,4,4\}} \oplus$$
$$A^{(0)}_{\{4,2,36\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{4,2,36\}} \cdot c_{\{1,4\}} \oplus A^{(0)}_{\{4,2,36\}} \oplus A^{(0)}_{\{0,2,37\}} \cdot A^{(0)}_{\{4,3,8\}} \oplus A^{(0)}_{\{0,2,37\}} \cdot A^{(0)}_{\{2,3,9\}} \oplus A^{(0)}_{\{0,2,37\}} \cdot$$
$$A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{0,2,37\}} \cdot A^{(0)}_{\{2,4,9\}} \oplus A^{(0)}_{\{0,2,37\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{0,2,37\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{0,2,37\}} \oplus A^{(0)}_{\{3,2,38\}} \cdot A^{(0)}_{\{4,3,8\}} \oplus$$
$$A^{(0)}_{\{3,2,38\}} \cdot A^{(0)}_{\{2,3,9\}} \oplus A^{(0)}_{\{3,2,38\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{3,2,38\}} \cdot A^{(0)}_{\{2,4,9\}} \oplus A^{(0)}_{\{3,2,38\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{3,2,38\}} \cdot c_{\{4,8\}} \oplus$$
$$A^{(0)}_{\{3,2,38\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot A^{(0)}_{\{3,2,58\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot A^{(0)}_{\{0,3,57\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot A^{(0)}_{\{3,3,58\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot A^{(0)}_{\{4,3,58\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot$$
$$A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot A^{(0)}_{\{3,4,58\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot c_{\{0,57\}} \oplus A^{(0)}_{\{4,2,40\}} \cdot c_{\{3,58\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{3,2,58\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot$$
$$A^{(0)}_{\{0,3,57\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{3,3,58\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{4,3,58\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot A^{(0)}_{\{3,4,58\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot$$
$$c_{\{0,57\}} \oplus A^{(0)}_{\{3,2,41\}} \cdot c_{\{3,58\}} \oplus A^{(0)}_{\{4,2,43\}} \oplus A^{(0)}_{\{2,2,44\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot A^{(0)}_{\{3,3,22\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot A^{(0)}_{\{1,3,23\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot$$
$$A^{(0)}_{\{3,4,22\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot A^{(0)}_{\{1,4,23\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot c_{\{3,22\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot c_{\{1,23\}} \oplus A^{(0)}_{\{4,2,44\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{4,2,44\}} \oplus$$

$$A^{(0)}_{\{3,2,46\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{2,2,63\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{0,3,0\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{2,3,63\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot A^{(0)}_{\{0,4,0\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot$$
$$A^{(0)}_{\{2,4,63\}} \oplus A^{(0)}_{\{4,2,47\}} \cdot c_{\{0,0\}} \oplus A^{(0)}_{\{3,2,49\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{2,3,55\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{0,3,56\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{2,4,55\}} \oplus$$
$$A^{(0)}_{\{3,2,50\}} \cdot A^{(0)}_{\{0,4,56\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot c_{\{2,55\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot c_{\{0,56\}} \oplus A^{(0)}_{\{3,2,50\}} \cdot c_{\{1,56\}} \oplus A^{(0)}_{\{3,2,57\}} \oplus A^{(0)}_{\{3,2,58\}} \cdot$$
$$A^{(0)}_{\{4,3,40\}} \oplus A^{(0)}_{\{3,2,58\}} \cdot A^{(0)}_{\{2,3,41\}} \oplus A^{(0)}_{\{3,2,58\}} \cdot A^{(0)}_{\{4,4,40\}} \oplus A^{(0)}_{\{3,2,58\}} \cdot A^{(0)}_{\{2,4,41\}} \oplus A^{(0)}_{\{3,2,58\}} \cdot c_{\{4,40\}} \oplus A^{(0)}_{\{3,2,58\}} \cdot$$
$$c_{\{2,41\}} \oplus A^{(0)}_{\{3,2,58\}} \oplus A^{(0)}_{\{3,2,59\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot A^{(0)}_{\{1,3,46\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot$$
$$A^{(0)}_{\{0,4,47\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot c_{\{1,46\}} \oplus A^{(0)}_{\{2,2,63\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{2,2,63\}} \oplus A^{(0)}_{\{4,2,63\}} \cdot A^{(0)}_{\{2,3,20\}} \oplus$$
$$A^{(0)}_{\{4,2,63\}} \cdot A^{(0)}_{\{0,3,21\}} \oplus A^{(0)}_{\{4,2,63\}} \cdot A^{(0)}_{\{1,3,21\}} \oplus A^{(0)}_{\{4,2,63\}} \cdot A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{4,2,63\}} \cdot A^{(0)}_{\{0,4,21\}} \oplus A^{(0)}_{\{4,2,63\}} \cdot c_{\{2,20\}} \oplus$$
$$A^{(0)}_{\{4,2,63\}} \cdot c_{\{0,21\}} \oplus A^{(0)}_{\{0,3,0\}} \cdot A^{(0)}_{\{1,3,46\}} \oplus A^{(0)}_{\{0,3,0\}} \cdot A^{(0)}_{\{4,3,47\}} \oplus A^{(0)}_{\{0,3,0\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{0,3,0\}} \cdot A^{(0)}_{\{0,4,47\}} \oplus$$
$$A^{(0)}_{\{0,3,0\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{0,3,0\}} \cdot c_{\{1,46\}} \oplus A^{(0)}_{\{0,3,0\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{0,3,0\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{4,3,36\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot$$
$$A^{(0)}_{\{2,3,37\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot c_{\{4,36\}} \oplus A^{(0)}_{\{3,3,3\}} \cdot c_{\{2,37\}} \oplus A^{(0)}_{\{1,3,4\}} \cdot$$
$$A^{(0)}_{\{4,3,36\}} \oplus A^{(0)}_{\{1,3,4\}} \cdot A^{(0)}_{\{2,3,37\}} \oplus A^{(0)}_{\{1,3,4\}} \cdot A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{1,3,4\}} \cdot A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{1,3,4\}} \cdot c_{\{4,36\}} \oplus A^{(0)}_{\{1,3,4\}} \cdot$$
$$c_{\{2,37\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{4,3,8\}} \cdot$$
$$c_{\{3,38\}} \oplus A^{(0)}_{\{2,3,9\}} \cdot A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{2,3,9\}} \cdot A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{2,3,9\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{2,3,9\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{2,3,9\}} \cdot$$
$$c_{\{3,38\}} \oplus A^{(0)}_{\{4,3,10\}} \oplus A^{(0)}_{\{2,3,11\}} \oplus A^{(0)}_{\{2,3,19\}} \oplus A^{(0)}_{\{0,3,20\}} \oplus A^{(0)}_{\{1,3,20\}} \oplus A^{(0)}_{\{2,3,20\}} \cdot A^{(0)}_{\{1,3,62\}} \oplus A^{(0)}_{\{2,3,20\}} \cdot A^{(0)}_{\{4,3,63\}} \oplus$$
$$A^{(0)}_{\{2,3,20\}} \cdot A^{(0)}_{\{1,4,62\}} \oplus A^{(0)}_{\{2,3,20\}} \cdot A^{(0)}_{\{4,4,63\}} \oplus A^{(0)}_{\{2,3,20\}} \cdot c_{\{1,62\}} \oplus A^{(0)}_{\{2,3,20\}} \cdot c_{\{0,63\}} \oplus A^{(0)}_{\{2,3,20\}} \cdot c_{\{4,63\}} \oplus$$
$$A^{(0)}_{\{2,3,20\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot A^{(0)}_{\{1,3,62\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot A^{(0)}_{\{4,3,63\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot A^{(0)}_{\{1,4,62\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot A^{(0)}_{\{4,4,63\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot$$
$$c_{\{1,62\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot c_{\{0,63\}} \oplus A^{(0)}_{\{0,3,21\}} \cdot c_{\{4,63\}} \oplus A^{(0)}_{\{0,3,21\}} \oplus A^{(0)}_{\{1,3,21\}} \cdot A^{(0)}_{\{1,3,62\}} \oplus A^{(0)}_{\{1,3,21\}} \cdot A^{(0)}_{\{4,3,63\}} \oplus$$
$$A^{(0)}_{\{1,3,21\}} \cdot A^{(0)}_{\{1,4,62\}} \oplus A^{(0)}_{\{1,3,21\}} \cdot A^{(0)}_{\{4,4,63\}} \oplus A^{(0)}_{\{1,3,21\}} \cdot c_{\{1,62\}} \oplus A^{(0)}_{\{1,3,21\}} \cdot c_{\{0,63\}} \oplus A^{(0)}_{\{1,3,21\}} \cdot c_{\{4,63\}} \oplus$$
$$A^{(0)}_{\{1,3,21\}} \oplus A^{(0)}_{\{2,3,21\}} \oplus A^{(0)}_{\{0,3,22\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot A^{(0)}_{\{4,3,44\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot A^{(0)}_{\{2,3,45\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot A^{(0)}_{\{3,3,45\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot$$
$$A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot c_{\{4,44\}} \oplus A^{(0)}_{\{3,3,22\}} \cdot c_{\{2,45\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot A^{(0)}_{\{4,3,44\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot$$
$$A^{(0)}_{\{2,3,45\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot A^{(0)}_{\{3,3,45\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot c_{\{4,44\}} \oplus A^{(0)}_{\{1,3,23\}} \cdot$$
$$c_{\{2,45\}} \oplus A^{(0)}_{\{1,3,23\}} \oplus A^{(0)}_{\{0,3,24\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot A^{(0)}_{\{0,3,26\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot A^{(0)}_{\{3,3,27\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot A^{(0)}_{\{0,4,26\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot$$
$$A^{(0)}_{\{3,4,27\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot c_{\{0,26\}} \oplus A^{(0)}_{\{1,3,24\}} \cdot c_{\{3,27\}} \oplus A^{(0)}_{\{1,3,24\}} \oplus A^{(0)}_{\{4,3,24\}} \oplus A^{(0)}_{\{0,3,25\}} \cdot A^{(0)}_{\{0,3,26\}} \oplus A^{(0)}_{\{0,3,25\}} \cdot$$
$$A^{(0)}_{\{3,3,27\}} \oplus A^{(0)}_{\{0,3,25\}} \cdot A^{(0)}_{\{0,4,26\}} \oplus A^{(0)}_{\{0,3,25\}} \cdot A^{(0)}_{\{3,4,27\}} \oplus A^{(0)}_{\{0,3,25\}} \cdot c_{\{0,26\}} \oplus A^{(0)}_{\{0,3,25\}} \cdot c_{\{3,27\}} \oplus A^{(0)}_{\{0,3,25\}} \oplus$$
$$A^{(0)}_{\{4,3,25\}} \cdot A^{(0)}_{\{0,3,26\}} \oplus A^{(0)}_{\{4,3,25\}} \cdot A^{(0)}_{\{3,3,27\}} \oplus A^{(0)}_{\{4,3,25\}} \cdot A^{(0)}_{\{0,4,26\}} \oplus A^{(0)}_{\{4,3,25\}} \cdot A^{(0)}_{\{3,4,27\}} \oplus A^{(0)}_{\{4,3,25\}} \cdot c_{\{0,26\}} \oplus$$
$$A^{(0)}_{\{4,3,25\}} \cdot c_{\{3,27\}} \oplus A^{(0)}_{\{4,3,25\}} \oplus A^{(0)}_{\{0,3,26\}} \cdot A^{(0)}_{\{1,4,24\}} \oplus A^{(0)}_{\{0,3,26\}} \cdot A^{(0)}_{\{4,4,25\}} \oplus A^{(0)}_{\{0,3,26\}} \cdot c_{\{1,24\}} \oplus A^{(0)}_{\{0,3,26\}} \cdot$$
$$c_{\{4,25\}} \oplus A^{(0)}_{\{3,3,27\}} \cdot A^{(0)}_{\{1,4,24\}} \oplus A^{(0)}_{\{3,3,27\}} \cdot A^{(0)}_{\{4,4,25\}} \oplus A^{(0)}_{\{3,3,27\}} \cdot c_{\{1,24\}} \oplus A^{(0)}_{\{3,3,27\}} \cdot c_{\{4,25\}} \oplus A^{(0)}_{\{1,3,29\}} \oplus$$
$$A^{(0)}_{\{4,3,30\}} \oplus A^{(0)}_{\{4,3,36\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{4,3,36\}} \cdot A^{(0)}_{\{1,4,4\}} \oplus A^{(0)}_{\{4,3,36\}} \cdot A^{(0)}_{\{2,4,4\}} \oplus A^{(0)}_{\{4,3,36\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{4,3,36\}} \cdot$$
$$c_{\{1,4\}} \oplus A^{(0)}_{\{4,3,36\}} \oplus A^{(0)}_{\{0,3,37\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{0,3,37\}} \cdot A^{(0)}_{\{2,4,9\}} \oplus A^{(0)}_{\{0,3,37\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{0,3,37\}} \cdot c_{\{4,8\}} \oplus$$
$$A^{(0)}_{\{0,3,37\}} \oplus A^{(0)}_{\{2,3,37\}} \cdot A^{(0)}_{\{3,4,3\}} \oplus A^{(0)}_{\{2,3,37\}} \cdot A^{(0)}_{\{1,4,4\}} \oplus A^{(0)}_{\{2,3,37\}} \cdot A^{(0)}_{\{2,4,4\}} \oplus A^{(0)}_{\{2,3,37\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{2,3,37\}} \cdot$$
$$c_{\{1,4\}} \oplus A^{(0)}_{\{2,3,37\}} \oplus A^{(0)}_{\{3,3,38\}} \cdot A^{(0)}_{\{4,4,8\}} \oplus A^{(0)}_{\{3,3,38\}} \cdot A^{(0)}_{\{2,4,9\}} \oplus A^{(0)}_{\{3,3,38\}} \cdot A^{(0)}_{\{3,4,9\}} \oplus A^{(0)}_{\{3,3,38\}} \cdot c_{\{4,8\}} \oplus$$
$$A^{(0)}_{\{3,3,38\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot A^{(0)}_{\{0,3,57\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot A^{(0)}_{\{3,3,58\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot A^{(0)}_{\{4,3,58\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot$$
$$A^{(0)}_{\{3,4,58\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot c_{\{0,57\}} \oplus A^{(0)}_{\{4,3,40\}} \cdot c_{\{3,58\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot A^{(0)}_{\{0,3,57\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot A^{(0)}_{\{3,3,58\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot$$
$$A^{(0)}_{\{4,3,58\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot A^{(0)}_{\{3,4,58\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot c_{\{0,57\}} \oplus A^{(0)}_{\{2,3,41\}} \cdot c_{\{3,58\}} \oplus A^{(0)}_{\{4,3,43\}} \oplus$$
$$A^{(0)}_{\{2,3,44\}} \oplus A^{(0)}_{\{3,3,44\}} \oplus A^{(0)}_{\{4,3,44\}} \cdot A^{(0)}_{\{3,4,22\}} \oplus A^{(0)}_{\{4,3,44\}} \cdot A^{(0)}_{\{1,4,23\}} \oplus A^{(0)}_{\{4,3,44\}} \cdot c_{\{3,22\}} \oplus A^{(0)}_{\{4,3,44\}} \cdot c_{\{1,23\}} \oplus$$
$$A^{(0)}_{\{4,3,44\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{4,3,44\}} \oplus A^{(0)}_{\{0,3,45\}} \oplus A^{(0)}_{\{2,3,45\}} \cdot A^{(0)}_{\{3,4,22\}} \oplus A^{(0)}_{\{2,3,45\}} \cdot A^{(0)}_{\{1,4,23\}} \oplus A^{(0)}_{\{2,3,45\}} \cdot c_{\{3,22\}} \oplus$$
$$A^{(0)}_{\{2,3,45\}} \cdot c_{\{1,23\}} \oplus A^{(0)}_{\{2,3,45\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{2,3,45\}} \oplus A^{(0)}_{\{3,3,45\}} \cdot A^{(0)}_{\{3,4,22\}} \oplus A^{(0)}_{\{3,3,45\}} \cdot A^{(0)}_{\{1,4,23\}} \oplus A^{(0)}_{\{3,3,45\}} \cdot$$

$$c_{\{3,22\}} \oplus A^{(0)}_{\{3,3,45\}} \cdot c_{\{1,23\}} \oplus A^{(0)}_{\{3,3,45\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{3,3,45\}} \oplus A^{(0)}_{\{1,3,46\}} \cdot A^{(0)}_{\{2,3,63\}} \oplus A^{(0)}_{\{1,3,46\}} \cdot A^{(0)}_{\{0,4,0\}} \oplus$$
$$A^{(0)}_{\{1,3,46\}} \cdot A^{(0)}_{\{2,4,63\}} \oplus A^{(0)}_{\{1,3,46\}} \cdot c_{\{0,0\}} \oplus A^{(0)}_{\{3,3,46\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot A^{(0)}_{\{2,3,63\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot A^{(0)}_{\{0,4,0\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot$$
$$A^{(0)}_{\{2,4,63\}} \oplus A^{(0)}_{\{4,3,47\}} \cdot c_{\{0,0\}} \oplus A^{(0)}_{\{3,3,49\}} \oplus A^{(0)}_{\{1,3,50\}} \oplus A^{(0)}_{\{2,3,50\}} \oplus A^{(0)}_{\{3,3,50\}} \cdot A^{(0)}_{\{2,3,55\}} \oplus A^{(0)}_{\{3,3,50\}} \cdot A^{(0)}_{\{0,3,56\}} \oplus$$
$$A^{(0)}_{\{3,3,50\}} \cdot A^{(0)}_{\{2,4,55\}} \oplus A^{(0)}_{\{3,3,50\}} \cdot A^{(0)}_{\{0,4,56\}} \oplus A^{(0)}_{\{3,3,50\}} \cdot c_{\{2,55\}} \oplus A^{(0)}_{\{3,3,50\}} \cdot c_{\{0,56\}} \oplus A^{(0)}_{\{3,3,50\}} \cdot c_{\{1,56\}} \oplus$$
$$A^{(0)}_{\{1,3,51\}} \cdot A^{(0)}_{\{2,3,55\}} \oplus A^{(0)}_{\{1,3,51\}} \cdot A^{(0)}_{\{0,3,56\}} \oplus A^{(0)}_{\{1,3,51\}} \cdot A^{(0)}_{\{2,4,55\}} \oplus A^{(0)}_{\{1,3,51\}} \cdot A^{(0)}_{\{0,4,56\}} \oplus A^{(0)}_{\{1,3,51\}} \cdot c_{\{2,55\}} \oplus$$
$$A^{(0)}_{\{1,3,51\}} \cdot c_{\{0,56\}} \oplus A^{(0)}_{\{1,3,51\}} \cdot c_{\{1,56\}} \oplus A^{(0)}_{\{2,3,51\}} \cdot A^{(0)}_{\{2,3,55\}} \oplus A^{(0)}_{\{2,3,51\}} \cdot A^{(0)}_{\{0,3,56\}} \oplus A^{(0)}_{\{2,3,51\}} \cdot A^{(0)}_{\{2,4,55\}} \oplus$$
$$A^{(0)}_{\{2,3,51\}} \cdot A^{(0)}_{\{0,4,56\}} \oplus A^{(0)}_{\{2,3,51\}} \cdot c_{\{2,55\}} \oplus A^{(0)}_{\{2,3,51\}} \cdot c_{\{0,56\}} \oplus A^{(0)}_{\{2,3,51\}} \cdot c_{\{1,56\}} \oplus A^{(0)}_{\{2,3,55\}} \cdot A^{(0)}_{\{3,4,50\}} \oplus$$
$$A^{(0)}_{\{2,3,55\}} \cdot A^{(0)}_{\{1,4,51\}} \oplus A^{(0)}_{\{2,3,55\}} \cdot c_{\{3,50\}} \oplus A^{(0)}_{\{2,3,55\}} \cdot c_{\{1,51\}} \oplus A^{(0)}_{\{2,3,55\}} \oplus A^{(0)}_{\{0,3,56\}} \cdot A^{(0)}_{\{3,4,50\}} \oplus A^{(0)}_{\{0,3,56\}} \cdot$$
$$A^{(0)}_{\{1,4,51\}} \oplus A^{(0)}_{\{0,3,56\}} \cdot c_{\{3,50\}} \oplus A^{(0)}_{\{0,3,56\}} \cdot c_{\{1,51\}} \oplus A^{(0)}_{\{0,3,57\}} \cdot A^{(0)}_{\{4,4,40\}} \oplus A^{(0)}_{\{0,3,57\}} \cdot A^{(0)}_{\{2,4,41\}} \oplus A^{(0)}_{\{0,3,57\}} \cdot$$
$$c_{\{4,40\}} \oplus A^{(0)}_{\{0,3,57\}} \cdot c_{\{2,41\}} \oplus A^{(0)}_{\{0,3,57\}} \oplus A^{(0)}_{\{3,3,57\}} \oplus A^{(0)}_{\{4,3,57\}} \oplus A^{(0)}_{\{3,3,58\}} \cdot A^{(0)}_{\{4,4,40\}} \oplus A^{(0)}_{\{3,3,58\}} \cdot A^{(0)}_{\{2,4,41\}} \oplus$$
$$A^{(0)}_{\{3,3,58\}} \cdot c_{\{4,40\}} \oplus A^{(0)}_{\{3,3,58\}} \cdot c_{\{2,41\}} \oplus A^{(0)}_{\{3,3,58\}} \oplus A^{(0)}_{\{4,3,58\}} \cdot A^{(0)}_{\{4,4,40\}} \oplus A^{(0)}_{\{4,3,58\}} \cdot A^{(0)}_{\{2,4,41\}} \oplus A^{(0)}_{\{4,3,58\}} \cdot$$
$$c_{\{4,40\}} \oplus A^{(0)}_{\{4,3,58\}} \cdot c_{\{2,41\}} \oplus A^{(0)}_{\{4,3,58\}} \oplus A^{(0)}_{\{3,3,59\}} \oplus A^{(0)}_{\{1,3,60\}} \oplus A^{(0)}_{\{1,3,62\}} \cdot A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{1,3,62\}} \cdot A^{(0)}_{\{0,4,21\}} \oplus$$
$$A^{(0)}_{\{1,3,62\}} \cdot c_{\{2,20\}} \oplus A^{(0)}_{\{1,3,62\}} \cdot c_{\{0,21\}} \oplus A^{(0)}_{\{2,3,63\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{2,3,63\}} \cdot A^{(0)}_{\{0,4,47\}} \oplus A^{(0)}_{\{2,3,63\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus$$
$$A^{(0)}_{\{2,3,63\}} \cdot c_{\{1,46\}} \oplus A^{(0)}_{\{2,3,63\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{2,3,63\}} \oplus A^{(0)}_{\{4,3,63\}} \cdot A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{4,3,63\}} \cdot A^{(0)}_{\{0,4,21\}} \oplus A^{(0)}_{\{4,3,63\}} \cdot$$
$$c_{\{2,20\}} \oplus A^{(0)}_{\{4,3,63\}} \cdot c_{\{0,21\}} \oplus A^{(0)}_{\{0,4,0\}} \cdot A^{(0)}_{\{1,4,46\}} \oplus A^{(0)}_{\{0,4,0\}} \cdot A^{(0)}_{\{0,4,47\}} \oplus A^{(0)}_{\{0,4,0\}} \cdot A^{(0)}_{\{4,4,47\}} \oplus A^{(0)}_{\{0,4,0\}} \cdot$$
$$c_{\{1,46\}} \oplus A^{(0)}_{\{0,4,0\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{0,4,0\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{3,4,3\}} \cdot c_{\{4,36\}} \oplus$$
$$A^{(0)}_{\{3,4,3\}} \cdot c_{\{2,37\}} \oplus A^{(0)}_{\{1,4,4\}} \cdot A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{1,4,4\}} \cdot A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{1,4,4\}} \cdot c_{\{4,36\}} \oplus A^{(0)}_{\{1,4,4\}} \cdot c_{\{2,37\}} \oplus$$
$$A^{(0)}_{\{2,4,4\}} \cdot A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{2,4,4\}} \cdot A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{2,4,4\}} \cdot c_{\{4,36\}} \oplus A^{(0)}_{\{2,4,4\}} \cdot c_{\{2,37\}} \oplus A^{(0)}_{\{4,4,8\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus$$
$$A^{(0)}_{\{4,4,8\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{4,4,8\}} \cdot c_{\{3,38\}} \oplus A^{(0)}_{\{2,4,9\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{2,4,9\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{2,4,9\}} \cdot c_{\{3,38\}} \oplus$$
$$A^{(0)}_{\{3,4,9\}} \cdot A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{3,4,9\}} \cdot A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{3,4,9\}} \cdot c_{\{3,38\}} \oplus A^{(0)}_{\{4,4,10\}} \oplus A^{(0)}_{\{2,4,11\}} \oplus A^{(0)}_{\{2,4,19\}} \oplus A^{(0)}_{\{0,4,20\}} \oplus$$
$$A^{(0)}_{\{2,4,20\}} \cdot A^{(0)}_{\{1,4,62\}} \oplus A^{(0)}_{\{2,4,20\}} \cdot A^{(0)}_{\{4,4,63\}} \oplus A^{(0)}_{\{2,4,20\}} \cdot c_{\{1,62\}} \oplus A^{(0)}_{\{2,4,20\}} \cdot c_{\{0,63\}} \oplus A^{(0)}_{\{2,4,20\}} \cdot c_{\{4,63\}} \oplus$$
$$A^{(0)}_{\{2,4,20\}} \oplus A^{(0)}_{\{0,4,21\}} \cdot A^{(0)}_{\{1,4,62\}} \oplus A^{(0)}_{\{0,4,21\}} \cdot A^{(0)}_{\{4,4,63\}} \oplus A^{(0)}_{\{0,4,21\}} \cdot c_{\{1,62\}} \oplus A^{(0)}_{\{0,4,21\}} \cdot c_{\{0,63\}} \oplus A^{(0)}_{\{0,4,21\}} \cdot$$
$$c_{\{4,63\}} \oplus A^{(0)}_{\{0,4,21\}} \oplus A^{(0)}_{\{2,4,21\}} \oplus A^{(0)}_{\{0,4,22\}} \oplus A^{(0)}_{\{3,4,22\}} \cdot A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{3,4,22\}} \cdot A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{3,4,22\}} \cdot c_{\{4,44\}} \oplus$$
$$A^{(0)}_{\{3,4,22\}} \cdot c_{\{2,45\}} \oplus A^{(0)}_{\{1,4,23\}} \cdot A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{1,4,23\}} \cdot A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{1,4,23\}} \cdot c_{\{4,44\}} \oplus A^{(0)}_{\{1,4,23\}} \cdot c_{\{2,45\}} \oplus$$
$$A^{(0)}_{\{1,4,23\}} \oplus A^{(0)}_{\{1,4,24\}} \cdot A^{(0)}_{\{0,4,26\}} \oplus A^{(0)}_{\{1,4,24\}} \cdot A^{(0)}_{\{3,4,27\}} \oplus A^{(0)}_{\{1,4,24\}} \cdot c_{\{0,26\}} \oplus A^{(0)}_{\{1,4,24\}} \cdot c_{\{3,27\}} \oplus A^{(0)}_{\{1,4,24\}} \oplus$$
$$A^{(0)}_{\{4,4,24\}} \oplus A^{(0)}_{\{4,4,25\}} \cdot A^{(0)}_{\{0,4,26\}} \oplus A^{(0)}_{\{4,4,25\}} \cdot A^{(0)}_{\{3,4,27\}} \oplus A^{(0)}_{\{4,4,25\}} \cdot c_{\{0,26\}} \oplus A^{(0)}_{\{4,4,25\}} \cdot c_{\{3,27\}} \oplus A^{(0)}_{\{4,4,25\}} \oplus$$
$$A^{(0)}_{\{0,4,26\}} \cdot c_{\{1,24\}} \oplus A^{(0)}_{\{0,4,26\}} \cdot c_{\{4,25\}} \oplus A^{(0)}_{\{3,4,27\}} \cdot c_{\{1,24\}} \oplus A^{(0)}_{\{3,4,27\}} \cdot c_{\{4,25\}} \oplus A^{(0)}_{\{1,4,29\}} \oplus A^{(0)}_{\{4,4,30\}} \oplus$$
$$A^{(0)}_{\{4,4,36\}} \cdot c_{\{3,3\}} \oplus A^{(0)}_{\{4,4,36\}} \cdot c_{\{1,4\}} \oplus A^{(0)}_{\{4,4,36\}} \oplus A^{(0)}_{\{0,4,37\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{0,4,37\}} \oplus A^{(0)}_{\{2,4,37\}} \cdot c_{\{3,3\}} \oplus$$
$$A^{(0)}_{\{2,4,37\}} \cdot c_{\{1,4\}} \oplus A^{(0)}_{\{2,4,37\}} \oplus A^{(0)}_{\{3,4,38\}} \cdot c_{\{4,8\}} \oplus A^{(0)}_{\{3,4,38\}} \oplus A^{(0)}_{\{4,4,40\}} \cdot A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{4,4,40\}} \cdot A^{(0)}_{\{3,4,58\}} \oplus$$
$$A^{(0)}_{\{4,4,40\}} \cdot c_{\{0,57\}} \oplus A^{(0)}_{\{4,4,40\}} \cdot c_{\{3,58\}} \oplus A^{(0)}_{\{2,4,41\}} \cdot A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{2,4,41\}} \cdot A^{(0)}_{\{3,4,58\}} \oplus A^{(0)}_{\{2,4,41\}} \cdot c_{\{0,57\}} \oplus$$
$$A^{(0)}_{\{2,4,41\}} \cdot c_{\{3,58\}} \oplus A^{(0)}_{\{4,4,43\}} \oplus A^{(0)}_{\{2,4,44\}} \oplus A^{(0)}_{\{4,4,44\}} \cdot c_{\{3,22\}} \oplus A^{(0)}_{\{4,4,44\}} \cdot c_{\{1,23\}} \oplus A^{(0)}_{\{4,4,44\}} \cdot c_{\{2,23\}} \oplus$$
$$A^{(0)}_{\{4,4,44\}} \oplus A^{(0)}_{\{0,4,45\}} \oplus A^{(0)}_{\{2,4,45\}} \cdot c_{\{3,22\}} \oplus A^{(0)}_{\{2,4,45\}} \cdot c_{\{1,23\}} \oplus A^{(0)}_{\{2,4,45\}} \cdot c_{\{2,23\}} \oplus A^{(0)}_{\{2,4,45\}} \oplus A^{(0)}_{\{1,4,46\}} \cdot$$
$$A^{(0)}_{\{2,4,63\}} \oplus A^{(0)}_{\{1,4,46\}} \cdot c_{\{0,0\}} \oplus A^{(0)}_{\{3,4,46\}} \oplus A^{(0)}_{\{0,4,47\}} \cdot A^{(0)}_{\{2,4,63\}} \oplus A^{(0)}_{\{0,4,47\}} \cdot c_{\{0,0\}} \oplus A^{(0)}_{\{4,4,47\}} \cdot A^{(0)}_{\{2,4,63\}} \oplus$$
$$A^{(0)}_{\{4,4,47\}} \cdot c_{\{0,0\}} \oplus A^{(0)}_{\{3,4,49\}} \oplus A^{(0)}_{\{1,4,50\}} \oplus A^{(0)}_{\{3,4,50\}} \cdot A^{(0)}_{\{2,4,55\}} \oplus A^{(0)}_{\{3,4,50\}} \cdot A^{(0)}_{\{0,4,56\}} \oplus A^{(0)}_{\{3,4,50\}} \cdot c_{\{2,55\}} \oplus$$
$$A^{(0)}_{\{3,4,50\}} \cdot c_{\{0,56\}} \oplus A^{(0)}_{\{3,4,50\}} \cdot c_{\{1,56\}} \oplus A^{(0)}_{\{1,4,51\}} \cdot A^{(0)}_{\{2,4,55\}} \oplus A^{(0)}_{\{1,4,51\}} \cdot A^{(0)}_{\{0,4,56\}} \oplus A^{(0)}_{\{1,4,51\}} \cdot c_{\{2,55\}} \oplus$$
$$A^{(0)}_{\{1,4,51\}} \cdot c_{\{0,56\}} \oplus A^{(0)}_{\{1,4,51\}} \cdot c_{\{1,56\}} \oplus A^{(0)}_{\{2,4,55\}} \cdot c_{\{3,50\}} \oplus A^{(0)}_{\{2,4,55\}} \cdot c_{\{1,51\}} \oplus A^{(0)}_{\{2,4,55\}} \oplus A^{(0)}_{\{0,4,56\}} \cdot$$
$$c_{\{3,50\}} \oplus A^{(0)}_{\{0,4,56\}} \cdot c_{\{1,51\}} \oplus A^{(0)}_{\{0,4,57\}} \cdot c_{\{4,40\}} \oplus A^{(0)}_{\{0,4,57\}} \cdot c_{\{2,41\}} \oplus A^{(0)}_{\{0,4,57\}} \oplus A^{(0)}_{\{3,4,57\}} \oplus A^{(0)}_{\{3,4,58\}} \cdot$$

$$
\begin{aligned}
&c_{\{4,40\}} \oplus A^{(0)}_{\{3,4,58\}} \cdot c_{\{2,41\}} \oplus A^{(0)}_{\{3,4,58\}} \oplus A^{(0)}_{\{3,4,59\}} \oplus A^{(0)}_{\{1,4,60\}} \oplus A^{(0)}_{\{1,4,62\}} \cdot c_{\{2,20\}} \oplus A^{(0)}_{\{1,4,62\}} \cdot c_{\{0,21\}} \oplus \\
&A^{(0)}_{\{2,4,63\}} \cdot c_{\{1,46\}} \oplus A^{(0)}_{\{2,4,63\}} \cdot c_{\{4,47\}} \oplus A^{(0)}_{\{2,4,63\}} \oplus A^{(0)}_{\{4,4,63\}} \cdot c_{\{2,20\}} \oplus A^{(0)}_{\{4,4,63\}} \cdot c_{\{0,21\}} \oplus c_{\{0,0\}} \cdot \\
&c_{\{1,46\}} \oplus c_{\{0,0\}} \cdot c_{\{4,47\}} \oplus c_{\{0,0\}} \oplus c_{\{3,3\}} \cdot c_{\{4,36\}} \oplus c_{\{3,3\}} \cdot c_{\{2,37\}} \oplus c_{\{1,4\}} \cdot c_{\{4,36\}} \oplus \\
&c_{\{1,4\}} \cdot c_{\{2,37\}} \oplus c_{\{4,8\}} \cdot c_{\{3,38\}} \oplus c_{\{4,10\}} \oplus c_{\{3,11\}} \oplus c_{\{2,19\}} \oplus c_{\{2,20\}} \cdot c_{\{1,62\}} \oplus c_{\{2,20\}} \cdot \\
&c_{\{0,63\}} \oplus c_{\{2,20\}} \cdot c_{\{4,63\}} \oplus c_{\{2,20\}} \oplus c_{\{0,21\}} \cdot c_{\{1,62\}} \oplus c_{\{0,21\}} \cdot c_{\{0,63\}} \oplus c_{\{0,21\}} \cdot c_{\{4,63\}} \oplus \\
&c_{\{0,21\}} \oplus c_{\{2,21\}} \oplus c_{\{3,22\}} \cdot c_{\{4,44\}} \oplus c_{\{3,22\}} \cdot c_{\{2,45\}} \oplus c_{\{1,23\}} \cdot c_{\{4,44\}} \oplus c_{\{1,23\}} \cdot c_{\{2,45\}} \oplus \\
&c_{\{1,23\}} \oplus c_{\{2,23\}} \cdot c_{\{4,44\}} \oplus c_{\{2,23\}} \cdot c_{\{2,45\}} \oplus c_{\{1,24\}} \cdot c_{\{0,26\}} \oplus c_{\{1,24\}} \cdot c_{\{3,27\}} \oplus c_{\{1,24\}} \oplus \\
&c_{\{4,25\}} \cdot c_{\{0,26\}} \oplus c_{\{4,25\}} \cdot c_{\{3,27\}} \oplus c_{\{4,25\}} \oplus c_{\{1,29\}} \oplus c_{\{4,30\}} \oplus c_{\{4,36\}} \oplus c_{\{2,37\}} \oplus c_{\{3,38\}} \oplus \\
&c_{\{4,40\}} \cdot c_{\{0,57\}} \oplus c_{\{4,40\}} \cdot c_{\{3,58\}} \oplus c_{\{2,41\}} \cdot c_{\{0,57\}} \oplus c_{\{2,41\}} \cdot c_{\{3,58\}} \oplus c_{\{4,43\}} \oplus c_{\{4,44\}} \oplus \\
&c_{\{0,45\}} \oplus c_{\{2,45\}} \oplus c_{\{3,46\}} \oplus c_{\{4,46\}} \oplus c_{\{3,49\}} \oplus c_{\{1,50\}} \oplus c_{\{3,50\}} \cdot c_{\{2,55\}} \oplus c_{\{3,50\}} \cdot c_{\{0,56\}} \oplus \\
&c_{\{3,50\}} \cdot c_{\{1,56\}} \oplus c_{\{1,51\}} \cdot c_{\{2,55\}} \oplus c_{\{1,51\}} \cdot c_{\{0,56\}} \oplus c_{\{1,51\}} \cdot c_{\{1,56\}} \oplus c_{\{2,55\}} \oplus c_{\{1,56\}} \oplus \\
&c_{\{0,57\}} \oplus c_{\{3,57\}} \oplus c_{\{3,58\}} \oplus c_{\{1,60\}} \oplus 1
\end{aligned}
$$

E The Details of Attacks on 3-round Xoodyak-XOF and Xoodyak-Hash

In this section, we give the details of the preimage attack on 3-round Xoodyak-XOF and the collision attack on 3-round Xoodyak-Hash.

E.1 New MITM preimage attack on 3-round Xoodyak-XOF

Solving with the MILP model for Xoodyak with a weak diffusion with $\sigma_{\mathcal{B}} = 10$, we get a new 3-round MITM preimage attack as shown in Figure 23. The attack is performed with two message blocks (M_1, M_2), where M_2 has two padding bits '10'. The MITM attack is placed in the 2nd block. The starting state $A^{(0)}$ contains 8 ■ bits and 118 ■ bits, i.e. $\lambda_{\mathcal{B}} = 118$, $\lambda_{\mathcal{R}} = 8$. There are totally 53 conditions on ■ bits of $\iota^{(0)}$, which are listed in Table 3. In the computation from $A^{(0)}$ to $\iota^{(2)}$, the consumed DoFs of ■ is 111 and the consumed DoFs of ■ is 0. Therefore, $d_{\mathcal{B}} = 8$, $d_{\mathcal{R}} = 118 - 111 = 7$. We get $m = 7$ matching equations as Equ. (22) with the deterministic relations of $\iota^{(2)}$.

$$
\begin{aligned}
&\chi^{(2)}_{\{1,2,8\}} = \iota^{(2)}_{\{1,2,8\}} \oplus (\iota^{(2)}_{\{1,0,8\}} \oplus 1) \cdot \iota^{(2)}_{\{1,1,8\}},\ \chi^{(2)}_{\{1,2,10\}} = \iota^{(2)}_{\{1,2,10\}} \oplus (\iota^{(2)}_{\{1,0,10\}} \oplus 1) \cdot \iota^{(2)}_{\{1,1,10\}},\\
&\chi^{(2)}_{\{2,2,10\}} = \iota^{(2)}_{\{2,2,10\}} \oplus (\iota^{(2)}_{\{2,0,10\}} \oplus 1) \cdot \iota^{(2)}_{\{2,1,10\}}, \chi^{(2)}_{\{1,2,17\}} = \iota^{(2)}_{\{1,2,17\}} \oplus (\iota^{(2)}_{\{1,0,17\}} \oplus 1) \cdot \iota^{(2)}_{\{1,1,17\}},\\
&\chi^{(2)}_{\{1,2,26\}} = \iota^{(2)}_{\{1,2,26\}} \oplus (\iota^{(2)}_{\{1,0,26\}} \oplus 1) \cdot \iota^{(2)}_{\{1,1,26\}}, \chi^{(2)}_{\{1,2,31\}} = \iota^{(2)}_{\{1,2,31\}} \oplus (\iota^{(2)}_{\{1,0,31\}} \oplus 1) \cdot \iota^{(2)}_{\{1,1,31\}},\\
&\chi^{(2)}_{\{2,2,31\}} = \iota^{(2)}_{\{2,2,31\}} \oplus (\iota^{(2)}_{\{2,0,31\}} \oplus 1) \cdot \iota^{(2)}_{\{2,1,31\}}.
\end{aligned}
\tag{22}
$$

The 53 conditions are actually linear equation system on the 256 bits of inner part. Therefore, it is expected to find a solution of the system with probability of 2^{-53} for a given 256-bit inner part. We give the attack procedure in Algorithm 4. In the MitM episode in Line 8 to 20, a space of $2^{7+8} = 2^{15}$ is searched. Assume 2^{ζ} is the number of needed M_1. In order to search a 128-bit preimage, we have

to search a space of $2^{\zeta-53+111+15} = 2^{128}$, i.e., $\zeta = 55$. Each step of Algorithm 4 is analyzed below:

- In Line 2, the time complexity is $2^{55} \times 53^3 = 2^{72.2}$ bit operations and 2^{55} 3-round `Xoodyak`.
- In Line 5, the time complexity is $2^{55-53+118} \times \frac{128+128+7}{128\times 3} = 2^{119.45}$ 3-round `Xoodyak`. The fraction $\frac{128+128+7}{128\times 3}$ is because that in the last round only 7 Sboxes with matching point are computed, while there are totally 128×3 Sboxes applications in the 3-round `Xoodyak`.
- In Line 7, the time is $2^{55-53+111} \times \frac{128+128+7}{128\times 3} = 2^{112.45}$ 3-round `Xoodyak`.
- In Line 9, the time is $2^{55-53+111+7} \times \frac{1}{384} = 2^{111.41}$ 3-round `Xoodyak`. This step is just to retrieve the values $U[c_{\mathcal{R}}]$ and restore it in L_1. Assuming one table access is about one Sbox application, we get the fraction $\frac{1}{384}$.
- In Line 12, the time is $2^{55-53+111+8} \times \frac{128+128+7}{128\times 3} = 2^{120.45}$ 3-round `Xoodyak`.
- In Line 15, the time complexity is $2^{55-53+111+15-7} \times \frac{2}{3} = 2^{120.41}$ 3-round `Xoodyak`.
- In Line 16, we only compute 5 Sboxes with $\rho^{(2)}$ to gain a filter of 2^{-5}, whose time complexity is $2^{55-53+111+15-7} \times \frac{5}{128\times 3} = 2^{114.73}$ 3-round `Xoodyak`.
- In Line 19, we check the remaining states with the remaining $128-7-5 = 116$ Sboxes, which is $2^{55-53+111+15-7-5} \times \frac{116}{384} = 2^{114.27}$ 3-round `Xoodyak`.

The total complexity of the 3-round attack is $2^{72.2} + 2^{55} + 2^{119.45} + 2^{112.45} + 2^{111.41} + 2^{120.45} + 2^{120.41} + 2^{114.73} + 2^{114.27} = 2^{121.77}$ 3-round `Xoodyak-XOF`, and the memory to store U is 2^{118}.

$\iota^{(0)}_{\{1,0,0\}} = 1; \iota^{(0)}_{\{3,1,0\}} = 0; \iota^{(0)}_{\{3,2,0\}} = 1; \iota^{(0)}_{\{2,0,1\}} = 0; \iota^{(0)}_{\{2,1,1\}} = 1; \iota^{(0)}_{\{3,0,1\}} = 0;$
$\iota^{(0)}_{\{3,1,1\}} = 1; \iota^{(0)}_{\{1,0,4\}} = 1; \iota^{(0)}_{\{1,2,4\}} = 0; \iota^{(0)}_{\{3,2,4\}} = 1; \iota^{(0)}_{\{3,1,4\}} = 0; \iota^{(0)}_{\{0,1,6\}} = 1; \iota^{(0)}_{\{2,0,6\}} = 0;$
$\iota^{(0)}_{\{2,1,6\}} = 1; \iota^{(0)}_{\{3,0,6\}} = 0; \iota^{(0)}_{\{3,1,6\}} = 1; \iota^{(0)}_{\{1,0,9\}} = 1; \iota^{(0)}_{\{1,2,9\}} = 0; \iota^{(0)}_{\{3,2,9\}} = 1; \iota^{(0)}_{\{3,1,9\}} = 0;$
$\iota^{(0)}_{\{0,0,11\}} = 0; \iota^{(0)}_{\{0,1,11\}} = 1; \iota^{(0)}_{\{3,0,11\}} = 0; \iota^{(0)}_{\{3,1,11\}} = 1; \iota^{(0)}_{\{0,0,15\}} = 0; \iota^{(0)}_{\{0,1,15\}} = 1;$
$\iota^{(0)}_{\{1,0,15\}} = 0; \iota^{(0)}_{\{1,1,15\}} = 1; \iota^{(0)}_{\{2,0,15\}} = 0; \iota^{(0)}_{\{2,1,15\}} = 1; \iota^{(0)}_{\{3,0,15\}} = 0; \iota^{(0)}_{\{3,1,15\}} = 1; \iota^{(0)}_{\{1,0,18\}} = 1;$
$\iota^{(0)}_{\{2,0,18\}} = 0; \iota^{(0)}_{\{3,1,18\}} = 0; \iota^{(0)}_{\{3,2,18\}} = 1; \iota^{(0)}_{\{0,0,20\}} = 0; \iota^{(0)}_{\{0,1,20\}} = 1; \iota^{(0)}_{\{3,0,20\}} = 0; \iota^{(0)}_{\{3,1,20\}} = 1;$
$\iota^{(0)}_{\{2,0,24\}} = 0; \iota^{(0)}_{\{2,1,24\}} = 1; \iota^{(0)}_{\{3,0,24\}} = 0; \iota^{(0)}_{\{3,1,24\}} = 1; \iota^{(0)}_{\{1,0,27\}} = 1; \iota^{(0)}_{\{1,2,27\}} = 0;$
$\iota^{(0)}_{\{2,0,27\}} = 0; \iota^{(0)}_{\{3,1,27\}} = 0; \iota^{(0)}_{\{3,2,27\}} = 1; \iota^{(0)}_{\{0,0,29\}} = 0; \iota^{(0)}_{\{0,1,29\}} = 1; \iota^{(0)}_{\{3,0,29\}} = 0; \iota^{(0)}_{\{3,1,29\}} = 1$

Table 3: Bit Conditions in 3-round Attack on `Xoodyak-XOF`

E.2 Collision Attack on 3-round `Xoodyak-Hash`

The MitM characteristic on 3-round `Xoodyak-XOF` can also be used to build collision attack on `Xoodyak-Hash`, which is given in Algorithm 5. In one MitM episode in Line 9 to 16, $2^{7+8-7} = 2^8$ partial target preimages are expected to find. According to Equ. (3), we need $2^{(h-t)/2-8} = 2^{116.5}$ MitM episodes to build the collision attack, *i.e.*, $2^{\zeta-53+111} = 2^{116.5}$, i.e., $\zeta = 58.5$. Each step of Algorithm 5 is analyzed below:

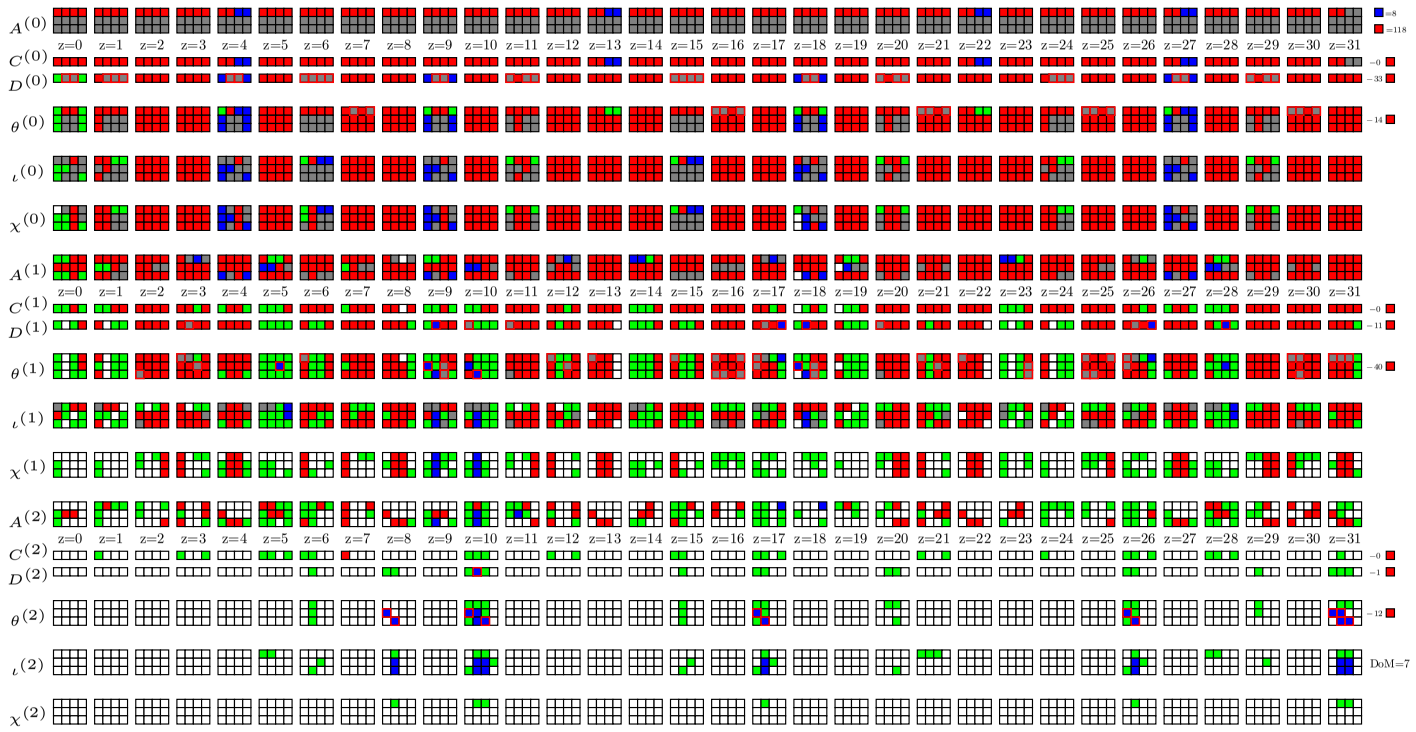

Fig. 23: The MitM preimage attack on 3-round `Xoodyak-XOF`

Algorithm 4: New Preimage Attack on 3-round `Xoodyak-XOF`

for 2^{ζ} *values of* M_1 **do**
  Compute the inner part of the 2nd block and solve the system of 53 linear equations
  if *the equations have solutions* `/* with probability of` 2^{-53} `*/`
  then
    Traversing the 2^{118} values of ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine 111-bit ■/■ bits (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{111}$), and the 7-bit matching point in Equ. (22), *i.e.*, compute 7 bits $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 118-bit ■ bits of $A^{(0)}$ as well as the 7-bit matching point in $U[c_{\mathcal{R}}]$.
    for $c_{\mathcal{R}} \in \mathbb{F}_2^{111}$ **do**
      Randomly pick a 118-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get 7 bits $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
      for 2^7 *values in* $U[c_{\mathcal{R}}]$ **do**
        Restore the values of ■ of $A^{(0)}$ and the corresponding matching point (*i.e.*, 7 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
      end
      for 2^8 *values of* ■ **do**
        Set the 118-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 7 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by matching point.
      end
      for *values matched between* L_1 *and* L_2 **do**
        Compute $\iota^{(2)}$ from the matched ■ and ■ cells
        if $\iota^{(2)}$ *satisfy the first 5 Sbox* `/* Probability of` 2^{-5}`. This step is to avoid computing all Sboxes of` $\iota^{(2)}$ `and only use partial Sboxes to filter first. */`
        then
          Check $\iota^{(2)}$ against the remaining 116 Sboxes
          if *it leads to the given hash value* **then**
            Output the preimage
          end
        end
      end
    end
  end
end

- In Line 3, the time complexity is $2^{58.5} \times 53^3 = 2^{75.68}$ bit operations and $2^{58.5}$ 3-round Xoodyak.
- In Line 6, the time complexity is $2^{58.5-53+118} \times \frac{128+128+7}{128\times 3} = 2^{122.95}$ 3-round Xoodyak. The fraction $\frac{128+128+7}{128\times 3}$ is because that in the last round only 7 Sboxes with matching point are computed, while there are totally 128×3 Sboxes applications in the 3-round Xoodyak.
- In Line 8, the time is $2^{58.5-53+111} \times \frac{128+128+7}{128\times 3} = 2^{115.95}$ 3-round Xoodyak.
- In Line 10, the time is $2^{58.5-53+111+7} \times \frac{1}{384} = 2^{114.91}$ 3-round Xoodyak. This step is just to retrieve the values $U[c_{\mathcal{R}}]$ and restore it in L_1. Assuming one table access is about one Sbox application, we get the fraction $\frac{1}{384}$.
- In Line 13, the time is $2^{58.5-53+111+8} \times \frac{128+128+7}{128\times 3} = 2^{123.95}$ 3-round Xoodyak.
- In Line 16, the time complexity is $2^{58.5-53+111+15-7} = 2^{124.5}$ 3-round Xoodyak.

The total complexity of the 3-round attack is $2^{75.68} + 2^{58.5} + 2^{122.95} + 2^{115.95} + 2^{114.91} + 2^{123.95} + 2^{124.5} = 2^{125.52}$ 3-round Xoodyak-Hash, and the memory to store U and L is $2^{118} + 2^{124.5} = 2^{124.51}$.

F The Detail of Attacks on 3-round Ascon-XOF and 3-/4-round Ascon-Hash

In this section, we give the details of the preimage attack on 3-round Ascon-XOF and the collision attacks on 3-/4-round Ascon-Hash.

F.1 The details of the preimage attack on 3-round Ascon-XOF

The improved 3-round preimage attack on Ascon is shown in Figure 24. The starting state $A^{(0)}$ contains 14 ■ bits and 30 ■ bits, where $\lambda_{\mathcal{R}} = 30$ and $\lambda_{\mathcal{B}} = 14$. The $\sigma_{\mathcal{B}} = 29$ for ■ set, which is a weak diffusion case. There are totally 44 conditions on ■ of $A^{(0)}$, *i.e.*, $\mu = 44$, which are listed in Table 4. In the computation from $A^{(0)}$ to $A^{(2)}$, the consumed DoFs of ■ are 16 and there is no DoF of ■ consumed. Therefore, $d_{\mathcal{B}} = 14$, $d_{\mathcal{R}} = 30 - 16 = 14$. The 14 matching

Algorithm 5: Collision Attack on 3-round `Xoodyak-Hash`

Fixed the $t = 7$ ■ bits of $\chi^{(2)}$ in Figure 23 as zero.
for 2^{ζ} *values of* M_1 **do**
  Compute the inner part of the 2nd block and solve the system of 53 linear equations
  if *the equations have solutions* `/* with probability of` 2^{-53} `*/`
  then
    Traversing the 2^{118} values of ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine 111-bit ■/■ bits (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{111}$), and the 7-bit matching point in Equ. (22), *i.e.*, compute 7 bits $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 118-bit ■ bits of $A^{(0)}$ as well as the 7-bit matching point in $U[c_{\mathcal{R}}]$.
    for $c_{\mathcal{R}} \in \mathbb{F}_2^{111}$ **do**
      Randomly pick a 118-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get 7 bits $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
      for 2^7 *values in* $U[c_{\mathcal{R}}]$ **do**
        Restore the values of ■ of $A^{(0)}$ and the corresponding matching point (*i.e.*, 7 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
      end
      for 2^8 *values of* ■ **do**
        Set the 118-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 7 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by matching point.
      end
      for *values matched between* L_1 *and* L_2 **do**
        Compute the 256-bit target h from the matched ■ and ■ cells and store the (M_1, M_2, h) in L indexed by h
        if *the size of* L *is* $2^{(h-t)/2} = 2^{124.5}$ **then**
          Check L and return (M_1, M_2) and (M'_1, M'_2) with the same h
        end
      end
    end
  end
end

bit equations ($m = 14$) are given in Equ. (23), where

$$\begin{cases}
A^{(2)}_{\{0,4\}} \cdot A^{(2)}_{\{0,1\}} + A^{(2)}_{\{0,3\}} + A^{(2)}_{\{0,2\}} \cdot A^{(2)}_{\{0,1\}} + A^{(2)}_{\{0,2\}} + A^{(3)}_{\{0,1\}} \cdot A^{(2)}_{\{0,0\}} + A^{(2)}_{\{0,1\}} + A^{(2)}_{\{0,0\}} = S^{(2)}_{\{0,0\}}, \\
A^{(2)}_{\{3,4\}} \cdot A^{(2)}_{\{3,1\}} + A^{(2)}_{\{3,3\}} + A^{(2)}_{\{3,2\}} \cdot A^{(2)}_{\{3,1\}} + A^{(2)}_{\{3,2\}} + A^{(3)}_{\{3,1\}} \cdot A^{(2)}_{\{3,0\}} + A^{(2)}_{\{3,1\}} + A^{(2)}_{\{3,0\}} = S^{(2)}_{\{3,0\}}, \\
A^{(2)}_{\{4,4\}} \cdot A^{(2)}_{\{4,1\}} + A^{(2)}_{\{4,3\}} + A^{(2)}_{\{4,2\}} \cdot A^{(2)}_{\{4,1\}} + A^{(2)}_{\{4,2\}} + A^{(3)}_{\{4,1\}} \cdot A^{(2)}_{\{4,0\}} + A^{(2)}_{\{4,1\}} + A^{(2)}_{\{4,0\}} = S^{(2)}_{\{4,0\}}, \\
A^{(2)}_{\{6,4\}} \cdot A^{(2)}_{\{6,1\}} + A^{(2)}_{\{6,3\}} + A^{(2)}_{\{6,2\}} \cdot A^{(2)}_{\{6,1\}} + A^{(2)}_{\{6,2\}} + A^{(3)}_{\{6,1\}} \cdot A^{(2)}_{\{6,0\}} + A^{(2)}_{\{6,1\}} + A^{(2)}_{\{6,0\}} = S^{(2)}_{\{6,0\}}, \\
A^{(2)}_{\{11,4\}} \cdot A^{(2)}_{\{11,1\}} + A^{(2)}_{\{11,3\}} + A^{(2)}_{\{11,2\}} \cdot A^{(2)}_{\{11,1\}} + A^{(2)}_{\{11,2\}} + A^{(3)}_{\{11,1\}} \cdot A^{(2)}_{\{11,0\}} + A^{(2)}_{\{11,1\}} + A^{(2)}_{\{11,0\}} = S^{(2)}_{\{11,0\}}, \\
A^{(2)}_{\{14,4\}} \cdot A^{(2)}_{\{14,1\}} + A^{(2)}_{\{14,3\}} + A^{(2)}_{\{14,2\}} \cdot A^{(2)}_{\{14,1\}} + A^{(2)}_{\{14,2\}} + A^{(3)}_{\{14,1\}} \cdot A^{(2)}_{\{14,0\}} + A^{(2)}_{\{14,1\}} + A^{(2)}_{\{14,0\}} = S^{(2)}_{\{14,0\}}, \\
A^{(2)}_{\{17,4\}} \cdot A^{(2)}_{\{17,1\}} + A^{(2)}_{\{17,3\}} + A^{(2)}_{\{17,2\}} \cdot A^{(2)}_{\{17,1\}} + A^{(2)}_{\{17,2\}} + A^{(3)}_{\{17,1\}} \cdot A^{(2)}_{\{17,0\}} + A^{(2)}_{\{17,1\}} + A^{(2)}_{\{17,0\}} = S^{(2)}_{\{17,0\}}, \\
A^{(2)}_{\{23,4\}} \cdot A^{(2)}_{\{23,1\}} + A^{(2)}_{\{23,3\}} + A^{(2)}_{\{23,2\}} \cdot A^{(2)}_{\{23,1\}} + A^{(2)}_{\{23,2\}} + A^{(3)}_{\{23,1\}} \cdot A^{(2)}_{\{23,0\}} + A^{(2)}_{\{23,1\}} + A^{(2)}_{\{23,0\}} = S^{(2)}_{\{23,0\}}, \\
A^{(2)}_{\{26,4\}} \cdot A^{(2)}_{\{26,1\}} + A^{(2)}_{\{26,3\}} + A^{(2)}_{\{26,2\}} \cdot A^{(2)}_{\{26,1\}} + A^{(2)}_{\{26,2\}} + A^{(3)}_{\{26,1\}} \cdot A^{(2)}_{\{26,0\}} + A^{(2)}_{\{26,1\}} + A^{(2)}_{\{26,0\}} = S^{(2)}_{\{26,0\}}, \\
A^{(2)}_{\{37,4\}} \cdot A^{(2)}_{\{37,1\}} + A^{(2)}_{\{37,3\}} + A^{(2)}_{\{37,2\}} \cdot A^{(2)}_{\{37,1\}} + A^{(2)}_{\{37,2\}} + A^{(3)}_{\{37,1\}} \cdot A^{(2)}_{\{37,0\}} + A^{(2)}_{\{37,1\}} + A^{(2)}_{\{37,0\}} = S^{(2)}_{\{37,0\}}, \\
A^{(2)}_{\{46,4\}} \cdot A^{(2)}_{\{46,1\}} + A^{(2)}_{\{46,3\}} + A^{(2)}_{\{46,2\}} \cdot A^{(2)}_{\{46,1\}} + A^{(2)}_{\{46,2\}} + A^{(3)}_{\{46,1\}} \cdot A^{(2)}_{\{46,0\}} + A^{(2)}_{\{46,1\}} + A^{(2)}_{\{46,0\}} = S^{(2)}_{\{46,0\}}, \\
A^{(2)}_{\{48,4\}} \cdot A^{(2)}_{\{48,1\}} + A^{(2)}_{\{48,3\}} + A^{(2)}_{\{48,2\}} \cdot A^{(2)}_{\{48,1\}} + A^{(2)}_{\{48,2\}} + A^{(3)}_{\{48,1\}} \cdot A^{(2)}_{\{48,0\}} + A^{(2)}_{\{48,1\}} + A^{(2)}_{\{48,0\}} = S^{(2)}_{\{48,0\}}, \\
A^{(2)}_{\{53,4\}} \cdot A^{(2)}_{\{53,1\}} + A^{(2)}_{\{53,3\}} + A^{(2)}_{\{53,2\}} \cdot A^{(2)}_{\{53,1\}} + A^{(2)}_{\{53,2\}} + A^{(3)}_{\{53,1\}} \cdot A^{(2)}_{\{53,0\}} + A^{(2)}_{\{53,1\}} + A^{(2)}_{\{53,0\}} = S^{(2)}_{\{53,0\}}, \\
A^{(2)}_{\{56,4\}} \cdot A^{(2)}_{\{56,1\}} + A^{(2)}_{\{56,3\}} + A^{(2)}_{\{56,2\}} \cdot A^{(2)}_{\{56,1\}} + A^{(2)}_{\{56,2\}} + A^{(3)}_{\{56,1\}} \cdot A^{(2)}_{\{56,0\}} + A^{(2)}_{\{56,1\}} + A^{(2)}_{\{56,0\}} = S^{(2)}_{\{56,0\}}.
\end{cases} \tag{23}$$

We use 3 message blocks (M_1, M_2, M_3) to conduct the preimage attack on `Ascon-XOF` with 128-bit hash. The 3-round MitM preimage attack is given in Algorithm 6. We firstly choose 2^ζ possible (M_1, M_2) to meet the 44 conditions of the inner part. In M_3, there are $64-30-14-2 = 18$ free ■ bits in Line 6 excluding the 30 ■ bits, 14 ■ bits and 2-bit padding. In Line 11 to Line 26, a subspace of 2^{14+14} is traversed. To find a 128-bit preimage, we need to exhaustively search a space of $2^{\zeta-44+18+16+14+14} = 2^{128}$, i.e., $\zeta = 110$. The time complexity of steps in Alg. 6 are analyzed below:

- In Line 3, the time complexity is $2^{110} \times 2 = 2^{111}$ 3-round `Ascon`.
- In Line 8, the time complexity of computing the ■ bits except those ■ bits in $A^{(1)}$ is $2^{\zeta-44+18} \times \frac{1}{3} = 2^{84} \times 2^{-1.58} = 2^{82.42}$ 3-round `Ascon`.
- In Line 9, for each of the 2^{30} possible values of ■ bits in $A^{(0)}$, we need compute $30 + 58 = 88$ out of the total $64 \times 3 = 192$ Sbox applications (3 rounds) to build U. Hence, the time of Line 9 is $2^{\zeta-44+18+30} \times \frac{88}{192} = 2^{114} \times 2^{-1.13} = 2^{112.87}$ 3-round `Ascon`.
- In Line 11, the time complexity is $2^{\zeta-44+18+16} \times \frac{88}{192} = 2^{98.87}$ 3-round `Ascon`.
- In Line 13, since U stores 30 ■ bits and 14-bit matching point, building L_1 is just to retrieve the values in $U[c_{\mathcal{R}}]$. Assume one table access is about one Sbox application, the time of Line 13 is $2^{\zeta-44+18+16+14} \times \frac{1}{192} = 2^{114} \times 2^{-7.58} = 2^{106.42}$ 3-round `Ascon`.
- In Line 16, given 14 ■ bits of $A^{(0)}$, the time of computing the 14-bit matching point is $14 + 27 = 41$ Sbox applications[7]. Therefore, the time of Line 16 is $2^{\zeta-44+18+16+14} \times \frac{41}{192} = 2^{111.77}$ 3-round `Ascon`.

[7]For example, the 27 Sbox applications are those Sboxes with at least one ■ or ■ bits in state $S^{(1)}$.

– In Line 19, we also compute the two Sboxes of $A^{(2)}$ (10 bits) as the early partial filter. Since in Line 8, the Sboxes determined by ■ bits in $A^{(1)}$ are already computed, we only need compute $30+14$ Sboxes to get the whole $A^{(1)}$. Then, each of the 10 bits is depending on 3 Sboxes of $S^{(1)}$, where 30 Sboxes are assumed to be computed from $A^{(1)}$ to $S^{(1)}$. We totally have to compute $30+14+30+2=76$ Sboxes to compute the first 2 Sboxes of $S^{(2)}$. The time of Line 19 is $2^{\zeta-44+18+16+14}\times\frac{76}{192}=2^{114}\times 2^{-1.34}=2^{112.66}$ 3-round `Ascon`.
– In Line 23, the time is $2^{\zeta-44+18+16+14-2}=2^{112}$ 3-round `Ascon`.

The total time complexity is $2^{111}+2^{82.42}+2^{112.87}+2^{98.87}+2^{106.42}+2^{111.77}+2^{112.66}+2^{112}\approx 2^{114.53}$ 3-round `Ascon`. The memory is 2^{30} to store U.

$A^{(0)}_{\{2,1\}}=0, A^{(0)}_{\{2,3\}}+A^{(0)}_{\{2,4\}}=1; A^{(0)}_{\{5,1\}}=0, A^{(0)}_{\{5,3\}}+A^{(0)}_{\{5,4\}}=1; A^{(0)}_{\{9,1\}}=0; A^{(0)}_{\{11,1\}}=1;$
$A^{(0)}_{\{13,1\}}=0, A^{(0)}_{\{13,3\}}+A^{(0)}_{\{13,4\}}=1; A^{(0)}_{\{14,1\}}=0; A^{(0)}_{\{16,1\}}=0, A^{(0)}_{\{16,3\}}+A^{(0)}_{\{16,4\}}=1;$
$A^{(0)}_{\{19,1\}}=0,\ A^{(0)}_{\{19,3\}}+A^{(0)}_{\{19,4\}}=1; A^{(0)}_{\{20,1\}}=0; A^{(0)}_{\{22,1\}}=0,\ A^{(0)}_{\{22,3\}}+A^{(0)}_{\{22,4\}}=1; A^{(0)}_{\{23,1\}}=0;$
$A^{(0)}_{\{24,1\}}=0; A^{(0)}_{\{26,1\}}=1, A^{(0)}_{\{26,3\}}+A^{(0)}_{\{26,4\}}=1; A^{(0)}_{\{31,1\}}=0; A^{(0)}_{\{33,1\}}=0,\ A^{(0)}_{\{33,3\}}+A^{(0)}_{\{33,4\}}=1;$
$A^{(0)}_{\{34,1\}}=0; A^{(0)}_{\{35,1\}}=0, A^{(0)}_{\{35,3\}}+A^{(0)}_{\{35,4\}}=1; A^{(0)}_{\{36,1\}}=0; A^{(0)}_{\{41,1\}}=0, A^{(0)}_{\{41,3\}}+A^{(0)}_{\{41,4\}}=1;$
$A^{(0)}_{\{42,1\}}=1; A^{(0)}_{\{43,1\}}=0, A^{(0)}_{\{43,3\}}+A^{(0)}_{\{43,4\}}=1; A^{(0)}_{\{44,1\}}=0; A^{(0)}_{\{46,1\}}=1;$
$A^{(0)}_{\{47,1\}}=1,\ A^{(0)}_{\{47,3\}}+A^{(0)}_{\{47,4\}}=1; A^{(0)}_{\{51,1\}}=1,\ A^{(0)}_{\{51,3\}}+A^{(0)}_{\{51,4\}}=1; A^{(0)}_{\{52,1\}}=1;$
$A^{(0)}_{\{53,1\}}=0; A^{(0)}_{\{55,1\}}=0; A^{(0)}_{\{56,1\}}=0; A^{(0)}_{\{58,1\}}=1,\ A^{(0)}_{\{58,3\}}+A^{(0)}_{\{58,4\}}=1;$

Table 4: Bit Conditions in 3-round Attack on `Ascon-XOF`

F.2 The details of the collision attack on 3-round `Ascon-Hash`

The MitM characteristic on 3-round `Ascon-XOF` in Figure 24 can also be used to build collision attacks on `Ascon-Hash` (256-bit digest), where $\lambda_{\mathcal{B}}=d_{\mathcal{B}}=14$, $\lambda_{\mathcal{R}}=30$, $d_{\mathcal{R}}=14$, $m=t=14$ and $\mu=44$. We give the MitM collision attack on 3-round `Ascon-Hash` in Algorithm 7. We also use three message blocks (M_1,M_2,M_3) to conduct the collision attack, and the MitM procedure is placed at the 3rd block. In one MitM episode in Line 11 to Line 22, $2^{d_{\mathcal{R}}+d_{\mathcal{B}}-t}=2^{14+14-14}=2^{14}$ partial target preimages are expected to find. According to Equ. (3), we need $2^{(h-t)/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t)}=2^{(256-14)/2-14}=2^{107}$ MitM episodes to build the collision attack, i.e., $2^{\zeta-44+18+16}=2^{107}$ and $\zeta=117$. The time complexity of steps in Alg. 7 are analyzed below:

– In Line 3, the time complexity is $2^{117}\times 2=2^{118}$ 3-round `Ascon`.
– In Line 8, the time complexity is $2^{\zeta-44+18}\times\frac{1}{3}=2^{91}\times 2^{-1.58}=2^{89.42}$ 3-round `Ascon`.
– In Line 9, the time complexity is $2^{\zeta-44+18+30}\times\frac{88}{192}=2^{121}\times 2^{-1.13}=2^{119.87}$ 3-round `Ascon`.

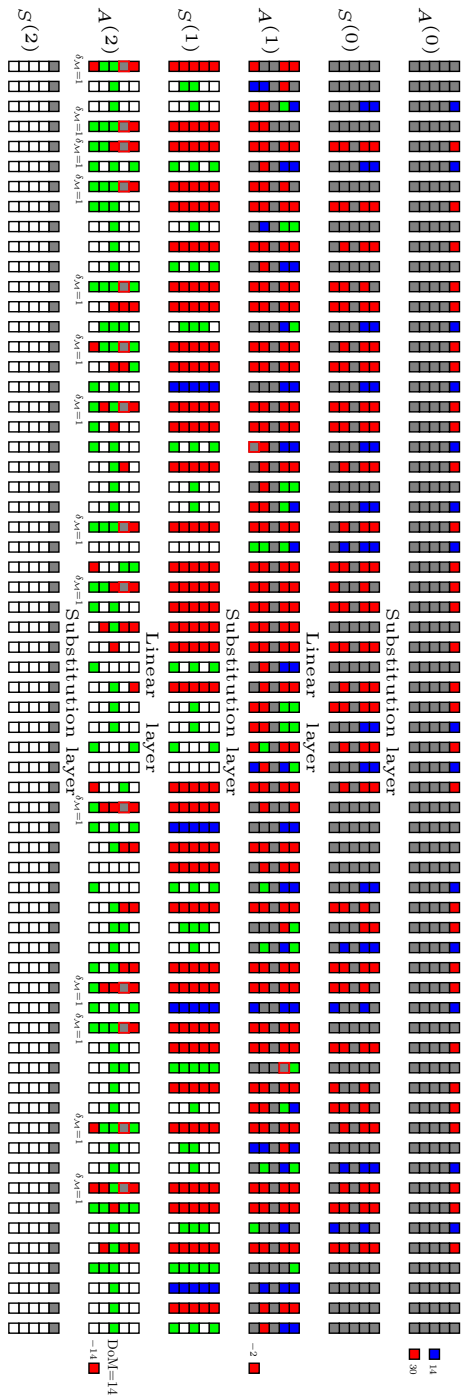

Fig. 24: Improved 3-round Preimage Attack on Ascon-XOF

Algorithm 6: Improved Preimage Attack on 3-round `Ascon-XOF`

Inversely precompute $S^{(2)}_{\{*,0\}}$ with the first 64-bit hashing value
for 2^{ζ} *values of* (M_1, M_2) **do**
  Compute the inner part of the 3rd block
  if *the conditions in Table 4 are satisfied* `/* probability of` 2^{-44} `*/`
  then
    for $2^{64-14-30-2} = 2^{18}$ *values of the* ■ *bits in* M_3
    do
      Compute the ■ bits in $A^{(0)}$ to $A^{(1)}$, except those ■ bits
      Traversing the $2^{\lambda_{\mathcal{R}}} = 2^{30}$ values for ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine the 16-bit ■/■ (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{16}$), and the 14-bit matching point in Equ. (23), *i.e.*, compute fourteen $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 30-bit ■ of $A^{(0)}$ as well as the 14-bit matching point in $U[c_{\mathcal{R}}]$.
      for $c_{\mathcal{R}} \in \mathbb{F}_2^{16}$ **do**
        Randomly pick a 30-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get fourteen $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
        for 2^{14} *values in* $U[c_{\mathcal{R}}]$ **do**
          Restore the values of ■ of $A^{(0)}$ and the corresponding 14-bit matching point (*i.e.*, 14 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 indexed by the matching point
        end
        for 2^{14} *values of* ■ **do**
          Set the 30-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 14 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by the 14-bit matching point
        end
        for *values matched between* L_1 *and* L_2 **do**
          Compute 2 Sboxes of $S^{(2)}$
          if *the 2 Sboxes satisfy the precomputed* $S^{(2)}_{\{*,0\}}$
          `/* probability of` 2^{-2}`. This step is to avoid computing all Sboxes of` $S^{(2)}$ `and only use partial Sboxes to filter first */`
          then
            if *it leads to the given hash value* **then**
              Output the preimage
            end
          end
        end
      end
    end
  end
end

- In Line 13, the time complexity is $2^{\zeta-44+18+16+14} \times \frac{1}{192} = 2^{121} \times 2^{-7.58} = 2^{113.42}$ 3-round Ascon.
- In Line 16, given 14 ■ bits of $A^{(0)}$, the time of computing the 14-bit matching point is $14 + 27 = 41$ Sbox applications. Therefore, the time of Line 16 is $2^{\zeta-44+18+16+14} \times \frac{(14+27)}{192} = 2^{121} \times 2^{-2.16} = 2^{118.77}$ 3-round Ascon.
- In Line 19, the time complexity is $2^{\zeta-44+18+16+14} = 2^{121}$ 3-round Ascon.

The total time complexity is $2^{118}+2^{89.42}+2^{119.87}+2^{113.42}+2^{118.77}+2^{121} \approx 2^{121.85}$ 3-round Ascon. The memory is $2^{30} + 2^{121} = 2^{121}$ to store U and L.

F.3 The details of the collision attack on 4-round Ascon-Hash

The MitM characteristic on 4-round Ascon-XOF in [56] (see also in Figure 25) can also be used to build collision attacks on Ascon-Hash, where $\lambda_{\mathcal{B}} = d_{\mathcal{B}} = 4$, $\lambda_{\mathcal{R}} = 54$, $d_{\mathcal{R}} = 54 - 50 = 4$, $m = t = 4$ and $\mu = 44$. We give the MitM collision attack on 4-round Ascon-Hash in Algorithm 8. We also use three message blocks (M_1, M_2, M_3) to conduct the collision attack, and the MitM procedure is placed at the 3rd block. In one MitM episode in Line 11 to Line 22, $2^{d_{\mathcal{R}}+d_{\mathcal{B}}-t} = 2^{4+4-4} = 2^4$ partial target preimages are expected to find. According to Equ. (3), we need $2^{(h-t)/2-(d_{\mathcal{R}}+d_{\mathcal{B}}-t)} = 2^{(256-4)/2-4} = 2^{122}$ MitM episodes to build the collision attack, i.e., $2^{\zeta-44+4+50} = 2^{122}$ and $\zeta = 112$. The time complexity of steps in Alg. 8 are analyzed below:

- In Line 3, the time complexity is $2^{112} \times 2 = 2^{113}$ 4-round Ascon.
- In Line 8, the time complexity is $2^{\zeta-44+4} \times \frac{1}{3} = 2^{72} \times 2^{-1.58} = 2^{70.42}$ 3-round Ascon.
- In Line 9, the time complexity is $2^{\zeta-44+4+54} \times \frac{(54+56+30)}{256} = 2^{126} \times 2^{-0.87} = 2^{125.13}$ 4-round Ascon.
- In Line 13, the time complexity is $2^{\zeta-44+4+50+4} \times \frac{1}{256} = 2^{118}$ 4-round Ascon.
- In Line 16, given 4 ■ bits of $A^{(0)}$, the time of computing the 4-bit matching point is $4 + 14 + 22 = 40$ Sbox applications. Therefore, the time of Line 16 is $2^{\zeta-44+4+50+4} \times \frac{40}{256} = 2^{126} \times 2^{-2.68} = 2^{123.32}$ 4-round Ascon.
- In Line 19, the time complexity is $2^{\zeta-44+4+50+4} = 2^{126}$ 4-round Ascon.

The total time complexity is $2^{113}+2^{70.42}+2^{125.13}+2^{118}+2^{123.32}+2^{126} \approx 2^{126.77}$ 4-round Ascon. The memory is $2^{54} + 2^{126} = 2^{126}$ to store U and L.

Algorithm 7: Collision Attack on 3-round `Ascon-XOF`

Fix the 14 bits of $S^{(2)}_{\{*,0\}}$ in Equ. (23) to build the matching points
for 2^{ζ} *values of* (M_1, M_2) **do**
  Compute the inner part of the 3rd block
  if *the conditions in Table 4 are satisfied* `/* probability of` 2^{-44} `*/`
  then
    for $2^{64-14-30-2} = 2^{18}$ *values of the* ■ *bits in* M_3
    do
      Compute the ■ bits in $A^{(0)}$ to $A^{(1)}$, except those ■ bits
      Traversing the $2^{\lambda_{\mathcal{R}}} = 2^{30}$ values for ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine the 16-bit ■/■ (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{16}$), and the 14-bit matching point in Equ. (23), *i.e.*, compute fourteen $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 30-bit ■ of $A^{(0)}$ as well as the 14-bit matching point in $U[c_{\mathcal{R}}]$
      for $c_{\mathcal{R}} \in \mathbb{F}_2^{16}$ **do**
        Randomly pick a 30-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get fourteen $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
        for 2^{14} *values in* $U[c_{\mathcal{R}}]$ **do**
          Restore the values of ■ of $A^{(0)}$ and the corresponding 14-bit matching point (*i.e.*, 14 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
        end
        for 2^{14} *values of* ■ **do**
          Set the 30-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 14 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by the 14-bit matching point.
        end
        for *values matched between* L_1 *and* L_2 **do**
          Compute the 256-bit target h from the matched ■ and ■ bits and store the (M_1, M_2, M_3, h) in L indexed by h
          if *the size of* L *is* $2^{(h-t)/2} = 2^{121}$ **then**
            Check L and return (M_1, M_2, M_3) and (M'_1, M'_2, M'_3) with the same h
          end
        end
      end
    end
  end
end

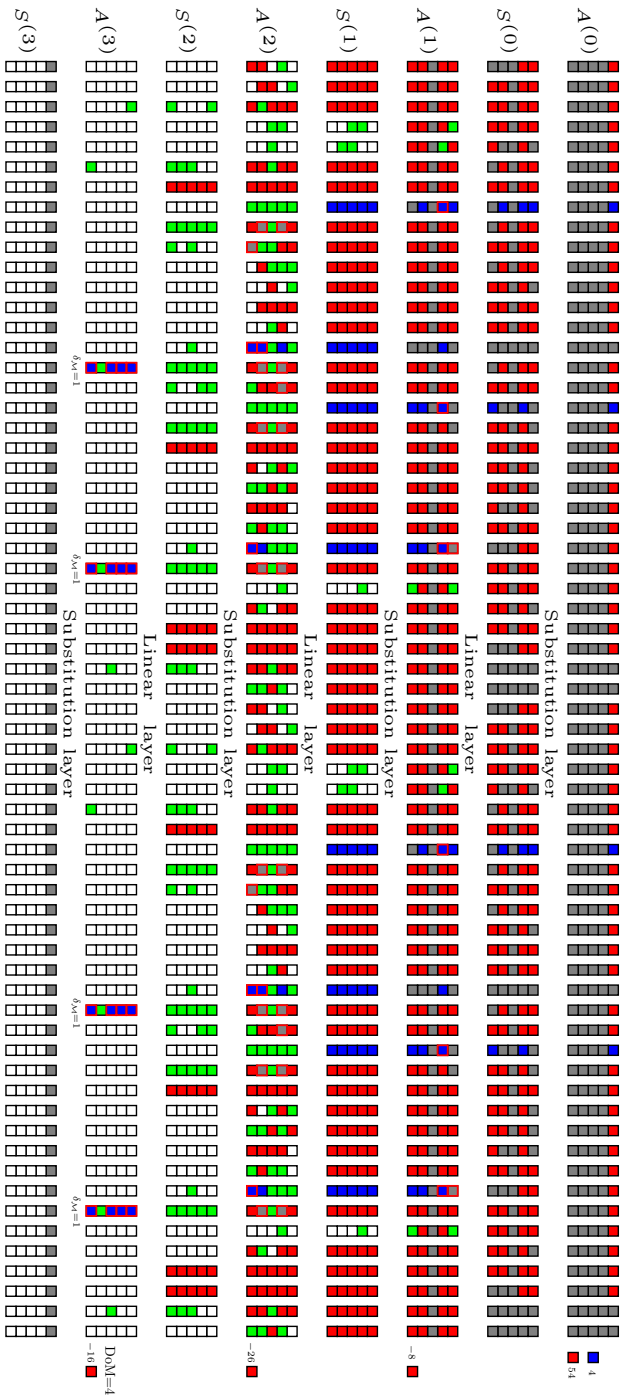

Fig. 25: The MitM characteristic on 4-round Ascon-XOF

Algorithm 8: Collision Attack on 4-round `Ascon-XOF`

Fix the 4 bits of $S^{(3)}_{\{*,0\}}$ to build the matching points
for 2^{ζ} *values of* (M_1, M_2) **do**
  Compute the inner part of the 3rd block
  if *the 44 conditions are satisfied* `/* probability of` 2^{-44} `*/`
  then
    for $2^{64-4-54-2} = 2^4$ *values of the free* ■ *bits in* M_3
    do
      Compute the ■ bits in $A^{(0)}$ to $A^{(1)}$, except those ■ bits
      Traversing the $2^{\lambda_{\mathcal{R}}} = 2^{54}$ values for ■ in $A^{(0)}$ while fixing ■ as 0, compute forward to determine the 50-bit ■/■ (denoted as $c_{\mathcal{R}} \in \mathbb{F}_2^{50}$), and the 4-bit matching point, *i.e.*, compute four $f'_{\mathcal{M}} = f_{\mathcal{R}} \oplus f_{\mathcal{G}}$. Build the table U and store the 54-bit ■ of $A^{(0)}$ as well as the 4-bit matching point in $U[c_{\mathcal{R}}]$.
      for $c_{\mathcal{R}} \in \mathbb{F}_2^{50}$ **do**
        Randomly pick a 54-bit ■ $e \in U[c_{\mathcal{R}}]$, and set ■ in $A^{(0)}$ as 0, compute to the matching point to get four $f'''_{\mathcal{M}} = f_{\mathcal{G}} + Const(e)$
        for 2^4 *values in* $U[c_{\mathcal{R}}]$ **do**
          Restore the values of ■ of $A^{(0)}$ and the corresponding 4-bit matching point (*i.e.*, 4 $f_{\mathcal{R}} \oplus f_{\mathcal{G}} = f'_{\mathcal{M}}$) in a list L_1 (indexed by matching point)
        end
        for 2^4 *values of* ■ **do**
          Set the 54-bit ■ in $A^{(0)}$ as e. Compute to the matching point to get 4 $f''_{\mathcal{M}} = f_{\mathcal{B}} + f_{\mathcal{G}} + Const(e)$. Together with $f'''_{\mathcal{M}}$, compute $f_{\mathcal{B}} = f''_{\mathcal{M}} + f'''_{\mathcal{M}}$ and store ■ in L_2 indexed by the 4-bit matching point.
        end
        for *values matched between* L_1 *and* L_2 **do**
          Compute the 256-bit target h from the matched ■ and ■ bits and store the (M_1, M_2, M_3, h) in L indexed by h
          if *the size of* L *is* $2^{(h-t)/2} = 2^{126}$ **then**
            Check L and return (M_1, M_2, M_3) and (M'_1, M'_2, M'_3) with the same h
          end
        end
      end
    end
  end
end