Rebound Attacks on SKINNY hashing with Automatic Tools

Jian Guo[1], Shun Li[1], Guozhen Liu[1(✉)], and Phuong Pham[1]

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.
{guojian,shun.li,guozhen.liu}@ntu.edu.sg, pham0079@e.ntu.edu.sg

Abstract. In ToSC'20, a new approach combining Mix-Integer Linear Programming (MILP) tool and Constraint Programming (CP) tool to search for boomerang distinguishers is proposed and later used for rebound attack in ASIACRYPT'21 and CRYPTO'22. In this work, we extend these techniques to mount collision attacks on SKINNY-128-256 MMO hashing mode in classical and quantum settings. The first results of 17-round (and 15-round) free-start collision attack on this variant of SKINNY hashing mode are presented. Moreover, one more round of the inbound phase is covered leading to the best existing classical free-start collision attack of 19-round on the SKINNY-128-384 MMO hashing.

Keywords: Collision attacks, Rebound attacks, Quantum computation, Constraint programming, SKINNY

1 Introduction

In this work, we focus on the security analysis of SKINNY [1] family of lightweight block ciphers on Matyas-Meyer-Oseas (MMO) hashing mode [13]. Since introduced in CRYPTO'16, SKINNY attracts great attention from the community. It not only has competitive performance but also provides strong security guarantees in both single key as well as related key settings. A great amount of work ranging from standard cryptanalysis of the block cipher to constructing other cryptographic structures such as hash functions and the Authenticated Encryption with Associated Data (AEAD) schemes based on the block cipher has been published since it's proposed.

Two block sizes, *i.e.*, 64-bit and 128-bit are specified for the SKINNY family. For each block size n, the tweakey size t is defined as n, $2n$ and $3n$ for different variants which are denoted by SKINNY-n-t. For example, if $n = 128$, $t = 384$, we have the variant SKINNY-128-384. As there are too many works published on SKINNY, to explain our work in a neat and concise way only the related works are briefly introduced.

Related Work. In ToSC'20, Delaune *et al.* [6] proposed a new approach which combines the Mix-Integer Linear Programming (MILP) tool and the Constraint Programming (CP) tool to search for boomerang distinguishers on SKINNY. In this work, we extend their work to design advanced automatic models to search truncated differential trails of the SKINNY variants. In ASIACRYPT'21, Dong *et al.* [8] presented a MILP-based technique to mount quantum rebound attacks

on the SKINNY-128-384 MMO hashing. Later in CRYPTO'22, Dong *et al.* [7] combine triangulation and rebound attack to further increase the attacked rounds of SKINNY-128-384 MMO in both classical and quantum settings.

Our Contribution. The results of our work are summarized in Table 1. We mainly focus on rebound attacks on SKINNY-128-256 MMO hashing mode in classical and quantum settings. As far as we know, this is the first result on this SKINNY variant. In this work, the differential trails of SKINNY variants that are generated with the MILP-CP based automatic tools are widely employed to serve the cryptanalytic purpose. Moreover, we extend the 5-round trail of the inbound phase of the SKINNY-128-384 MMO to 6-round which gives the best attacking result.

Organization. This article is organized as follows. In Section 2, we give a brief description of SKINNY and introduce some basic notions as well as algorithms used in quantum computation. We revise the primary techniques that are broadly utilized in our work in section 3. Section 4 and Section 5 are the demonstration of several attacks on SKINNY MMO hashing. Section 6 concludes the paper.

Table 1: A summary of the results

SKINNY-128-256-MMO							
Target	Attack	Rounds	Time	C-Mem	qRAM	Setting	Ref.
Compression function	Free-start	15/48	$2^{55.8}$	-		Classical	Sect. 5.2
		17/48	$2^{49.5}$	-		Quantum	Sect. 5.1
	any	any	2^{64}	-		any	[2, 10, 18]
	any	any	$2^{42.7}$	-	$2^{42.7}$	Quantum	[3]
	any	any	$2^{51.2}$	$2^{25.6}$	-	Quantum	[4]
SKINNY-128-384-MMO							
Compression function	Free-start	19/56	$2^{51.2}$	-		Classical	[7]
		21/56	$2^{46.2}$	-		Quantum	[7]
		19/56	2^{35}	-		Classical	Sect. 4

2 Preliminaries

2.1 SKINNY MMO Hashing

SKINNY is a family of lightweight tweakable block ciphers that follow the classical substitution-permutaion network (SPN) and the TWEAKEY framework [11]. There are 6 variants in the SKINNY family each of which is denoted by SKINNY-n-t, where n (resp. t) denotes the block size (resp. tweakey size). Specifically, the block size $n \in \{64, 128\}$ and the tweakey size $t = z \cdot n$ with $z \in \{1, 2, 3\}$. The number of rounds of SKINNY-64-64/128/192 and SKINNY-128-128/256/384 are 32/36/40 and 40/48/56 respectively. The internal states of both the 64-bit and 128-bit versions are represented with 4×4 array of cells with each cell being a nibble in case

of $n = 64$ and a byte in case of $n = 128$. The tweakey which can contain both key and tweak material are essentially a group of z 4×4 arrays where $z \in \{1, 2, 3\}$. For all the SKINNY variants, the cells of state and tweakey are numbered row-wise. The round operations are described in the following and illustrated with Figure 1.

1. *SubCells* (SC) - The non-linear substitution layer that adopts 4-bit (resp. 8-bit) S-box for $n = 64$ (resp. $n = 128$) variants.
2. *AddConstants* (AC) - Xoring round constants to the first three cells of the first column of the internal state.
3. *AddRoundTweakey* (ART) - Adding tweakey (denoted by tk_i) to the internal state. Namely, the first two rows of tk_i are xored. The round tweakey is computed with
   - $z = 1$: $tk_i = (TK_1)_i$
   - $z = 2$: $tk_i = (TK_1)_i \oplus (TK_2)_i$
   - $z = 3$: $tk_i = (TK_1)_i \oplus (TK_2)_i \oplus (TK_3)_i$

   where $(TK_1)_i$, $(TK_2)_i$ and $(TK_3)_i$ of the i-th round are generated with the *tweakey scheduling algorithm*.
4. *ShiftRows* (SR) - Circular right shift on each row of the internal state. The number of shifts in each row j is j for $0 \leq j \leq 3$.
5. *MixColumns* (MC) - Multiplying each column of the internal state by a 4×4 binary matrix which is non-MDS, i.e.,

$$\mathtt{MC}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,1\,0 \\ 1\,0\,1\,0 \end{pmatrix} \times \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \text{ and } \mathtt{MC}^{-1}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0\,1\,0\,0 \\ 0\,1\,1\,1 \\ 0\,1\,0\,1 \\ 1\,0\,0\,1 \end{pmatrix} \times \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}. \tag{1}$$

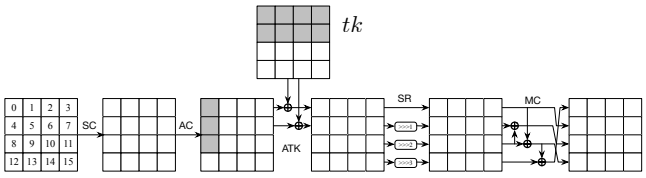

Figure 1: Round function of SKINNY

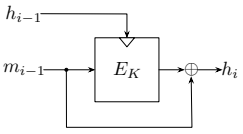

Figure 2: MMO mode

Tweakey Scheduling Algorithm (TSA) A linear tweakey scheduling algorithm is taken. The tweakey input is first loaded with a n, $2n$ or $3n$-bit tweakey input, *i.e.*, TK_1 with $z = 1$, (TK_1, TK_2) with $z = 2$, and (TK_1, TK_2, TK_3) with $z = 3$. The round tweakeys are generated as follows:

1. *Cell Permutation*: a permutation P defined as

$$P = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$$

   is applied to each of the TK_m arrays, namely, $TK_m[i] \leftarrow TK_m[P[i]]$ for all $0 \leq i \leq 15$ and $m \in 1, \cdots, z$.

2. *LFSR Update*: cells in the first two rows of TK_2 / (TK_2, TK_3) for $z = 2$ / 3 are individually updated using a 4-bit (if the cell is a nibble) or a 8-bit (if the cell is a byte) LFSR. Note that TK_1 is not updated in this phase.

SKINNY hashing in MMO mode A great category of cryptographic hash functions are based on one-way compression functions which are generally built from block ciphers. The Matyas-Meyer-Oseas (MMO) is one of the most extensively used method to transform any normal block cipher into a one-way compression function [13,15]. As illustrated in Figure 2, by applying (keyed) permutations with SKINNY round functions in MMO hashing mode, compression functions (denoted as f) are constructed. The SKINNY hashing H in MMO mode is therefore defined following the Merkle-Damgård construction [5,16], *i.e.*, $H(m) = h_n$ with

$$h_0 = IV$$
$$h_i = f(m_{i-1}, h_{i-1}) \oplus m_{i-1}, \text{ where } i \in \{1, \cdots, n\}.$$

Here m denotes the message which is spilt into n message blocks m_i, h_i are the intermediate variables or chaining values, and IV is the abbreviation for initial value or initial vector.

2.2 The Rebound attack

The rebound attack was introduced by Mendel et al. in [14] to mount collision attacks on hash functions that are constructed from block ciphers and permutations. As illustrated in Figure 3, there is an inbound phase and two outbound phases in the rebound attack where the targeted block cipher or permutation F is split into three subparts, namely, $F = F_{fw} \circ F_{in} \circ F_{bw}$.

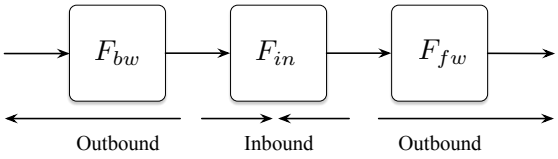

Figure 3: The rebound attack

In the inbound phase, the meet-in-the-middle technique is exploited to search truncated differential trails of low probability. For example, given the patterns of both input and output differences of the inbound trails, the whole truncated trails are determined with the meet-in-the-middle method. Afterwards, state pairs (named as starting points for the outbound phase) that conform to the inbound trails are generated. The number of starting points is called the degree of freedom in the inbound phase. In the outbound phase, the starting points are propagated backward and forward through F_{bw} and F_{fw} to obtain pairs that fulfill the outbound trails as well as other extra constraints in a brute-force fashion.

In essence, the rebound attack is a technique to efficiently generate message pairs that satisfy the inbound phase while only exhaustive search is involved in

the outbound phase. Assuming the probability of outbound trail is p, $1/p$ starting points must be prepared in the inbound phase to expect one pair following the outbound trail. Hence, the degree of freedom should be larger than $1/p$.

2.3 Collision Attacks and Its Variants

In regards to the cryptanalysis of a hash function H, a *collision attack* generates a message pair (m, m') such that $H(IV, m) = H(IV, m')$. Except for the standard collision, other well-accepted variants include *semi-free-start collision* and *free-start collision*. The goal of a *semi-free-start collision attack* is to find a pair (u, m) and (u, m') such that $H(u, m) = H(u, m')(u \neq IV)$ while the goal of a *free-start collision attack* is to find a pair (v, m) and (v', m') so that $H(v, m) = H(v', m')(v \neq v')$.

The semi-free-start collision and free-start collision attack on compression functions are defined in similar way if the hash function H is constructed by iterating the compression function with Merkle-Damgård construction. For example, both the semi-free-start and free-start collision attack on the MMO hashing mode shown in Figure 2 could take the advantage of the degrees of freedom from the chaining value h_{i-1} through the key schedule algorithm. In effect, better attacks such as [12, 17] were presented with this consideration. The significance of semi-free-start and free-start collision attacks should not be overlooked in security evaluation of Merkle-Damgård construction cause any kind of collision resistance including semi-free-start and free-start collisions is defined in its design principle.

2.4 Quantum Computing

Grover's Algorithm Grover's algorithm [9] is a quantum algorithm to solve the searching problem in a database which was later proved being optimal [19]. The database search problem is described in the following.

Problem 1. Let $F : \{0,1\}^n \to \{0,1\}$ be a boolean function. Supposing there is only one x such that $F(x) = 1$ and a quantum oracle access to F is given, find the x.

It approximately requires 2^n queries before finding the x in the classical setting. In comparison, the x is found with only $O(\sqrt{2^n} = 2^{n/2})$ queries with Grover's algorithm. Alternatively, the time complexity of the database search problem in the quantum setting is quadratic faster than that of the classical ones. In the general case of Problem 1 where $|\{x : F(x) = 1\}| = 2^t$, the Grover's algorithm returns x after making $O(\sqrt{2^n/2^t})$ quantum queries to F with high probability. As summarized in Table 1 the $2^{n/2}$ complexity is actually a tight bound of preimage attacks on hash functions in the quantum setting thanks to the optimality of the algorithm.

Except for the Grover's algorithm, there are other quantum collision finding aogirthm with better bounds. The BHT algorithm is introduced to generate collisions for a random function in $O(2^{n/3})$ time and $O(2^{n/3})$ quantum queries under

the assumption that quantum random access memory (qRAM) is available [3]. The quantum algorithm is subsequently extended to any random function [20]. If qRAM is not available the BHT algorithm become less efficient, *e.g.*, even slower than the birthday attack. To overcome the flaw, Chailloux et al. [4] proposed an efficient algorithm (called CNS) to efficiently generate a collision in time $\tilde{O}(2^{2n/5})$ with a quantum computer of $O(n)$ qubits. In that case, a large classical memory of size $\tilde{O}(2^{n/5})$ is required.

The bounds of quantum collision on hash functions based on SKINNY variants of 128-bit block size with the general quantum search algorithms are summarized in Table 1. That is, the quantum collision bound with Grover's algorithm is 2^{64} time complexity while the bound with BHT (or CNS) algorithm is $2^{42.7}$ (or $2^{51.2}$) time complexity but qRAM (or classical memory) is required.

3 Merging Multiple Inbound Phase

In this section, the *multiple inbound* technique that concatenates several 1-round inbound phases is proposed to extend the rounds covered in the inbound phase. Essentially, those 1-round inbound phases are connected by free bytes of the corresponding tweakeys. Therefore, it must be ensured that the value assignments to the related tweakeys of different rounds are not over-defined through the tweakey scheduling algorithm.

An example of a 3-round inbound phase (as depicted in Figure 4) that merges two 1-round inbound phases is described to explain the multiple inbound phases. Note that the `AC` operation is omitted in the round function as it doesn't change the difference. The `SC` operation is relabelled as `SB` for the rest of the paper. The `ART` operation (resp. the subtweakey tk) is relabelled as `AK` (resp. the subkey k) as the tweakey is treated the same as a normal round key in the cryptanalysis.

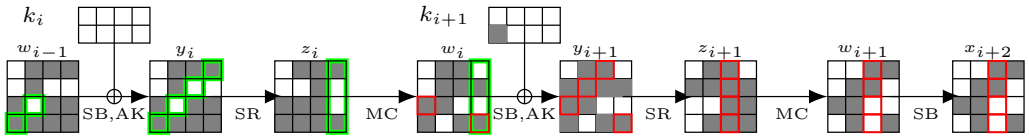

Figure 4: The 3-round multiple inbound phases [1]

In the multiple inbound phase, given the differential trail generated by the MILP-CP based automatic tools, the goal is to find state and key pairs that conform to the selected inbound phase. By taking advantage of the degrees of freedom from the subkeys k_i and k_{i+1} which can be efficiently calculated from tweakeys, the inbound phase is implemented with low memory. In specific,

– valid values of involved bytes in round states $w_{i-1}, x_i, w_i, x_{i+1}, w_{i+1}, x_{i+2}$ are first computed according to the (differential distribution table) DDT of the S-box where the input/output values satisfying input/output differences are

[1] The gray boxes represent the active cells. The green and red boxes indicate the values are concerned.

stored. Note that x_i, *i.e.*, the intermediate state after SB and before AK operations, is not reflected in Figure 4 considering that it shares the same difference pattern with w_{i-1}.

– valid values for pair of x_j, w_j can be further eliminated according to the inner operations of round function such as SB, SR, and MC. For example, green cells in Figure 4 are traced in the following way,
  - $x_i[9, 12]$ pass AK without change;
  - $y_i[3, 6, 9, 12]$ pass to $z_i[3, 7, 11, 15]$;
  - and $w_i[3, 7, 11, 15] = \mathtt{MC}(z_i[3, 7, 11, 15])$.

  Similar treatments apply to those red cells. As a consequence, $w_i[15]$ is related with both w_{i-1} and x_{i+2} which can be utilized as an effective filter for pairs.

When all valid values in $w_j[12, 13, 14, 15](j \in \{0, 1, \ldots, r-1\})$ are determined, we merge them to find a valid pair of state and subkeys. For instance, if we randomly pick a value for $w_{i-1}[12]$ and $w_i[15]$, the value of $w_i[3]$ can be easily obtained as $w_i[3] = \mathtt{SB}(w_{i-1}[12]) \oplus w_i[15]$ according to the MixColumn operation (1). By randomly picking another value for $x_{i+2}[7]$, $w_{i+1}[7]$ is computed from $w_{i+1}[7] = \mathtt{SB}^{-1}(x_{i+2}[7])$. Likewise, $z_{i+1}[3]$ is equal to $w_{i+1}[7]$ in accordance with the MixColumn operation (1), and $y_{i+1}[3] = z_{i+1}[3]$ due to the ShiftRow operation. Hence, subkey value $k_{i+1}[3] = \mathtt{SB}(w_i[3]) \oplus y_{i+1}[3]$.

In a nutshell, with this multiple inbound technique, the pairs of states as well as subkeys that follow the sophisticated inbound differential trail of longer rounds are effortlessly generated.

4 Improved Free-start Collision Attack on SKINNY-128-384 MMO in Classical Setting

In this section, we introduce an improved 19-round free-start collision attack on SKINNY-128-384 MMO hashing mode in classical setting. Aided by the technique developed in the last section, compared with the previously best result of the 5-round inbound phase given in [7], we obtain the first 6-round inbound phase. It's worth noticing that 6-round is the longest rounds covered by the inbound phase due to the constraint on the degree of freedom of the tweakeys. In total, an improved 19-round classical free-start collision attack with significantly reduced complexity is mounted given that one round of the exhaustive outbound phase is moved to the inbound phase.

In regards to the 19-round SKINNY-128-384 MMO hashing mode, the differential trail shown in Figure 8 in Appendix A which contains a 6-round inbound phase and a 13-round outbound phase is employed to derive the free-start collision attack in classical setting. We'd like to emphasize that the 19-round differential trial is generated with the automatic tools based on the model published in [6]. The 6-round multiple inbound phase covers from state w_7 to x_{13}. The outbound phase happens with probability 2^{-35}.

The effort of the 19-round rebound (or collision) attack is devoted to the 6-round multiple inbound phase as only exhaustive search involved in the outbound phase. Hence, as illustrated in Figure 5, only the inbound phase of the whole 19-round differential trails (which is shown in Figure 8) is elaborated in this section.

To launch the rebound attack, a multi-step *precomputation* method is performed to collect a number of pairs (*i.e.*, starting points) satisfying the 6-round inbound trail as shown in Figure 5. Thanks to the great degree of freedom of the tweakey, enough starting points are prepared by changing the exact value of the 384-bit tweakey.

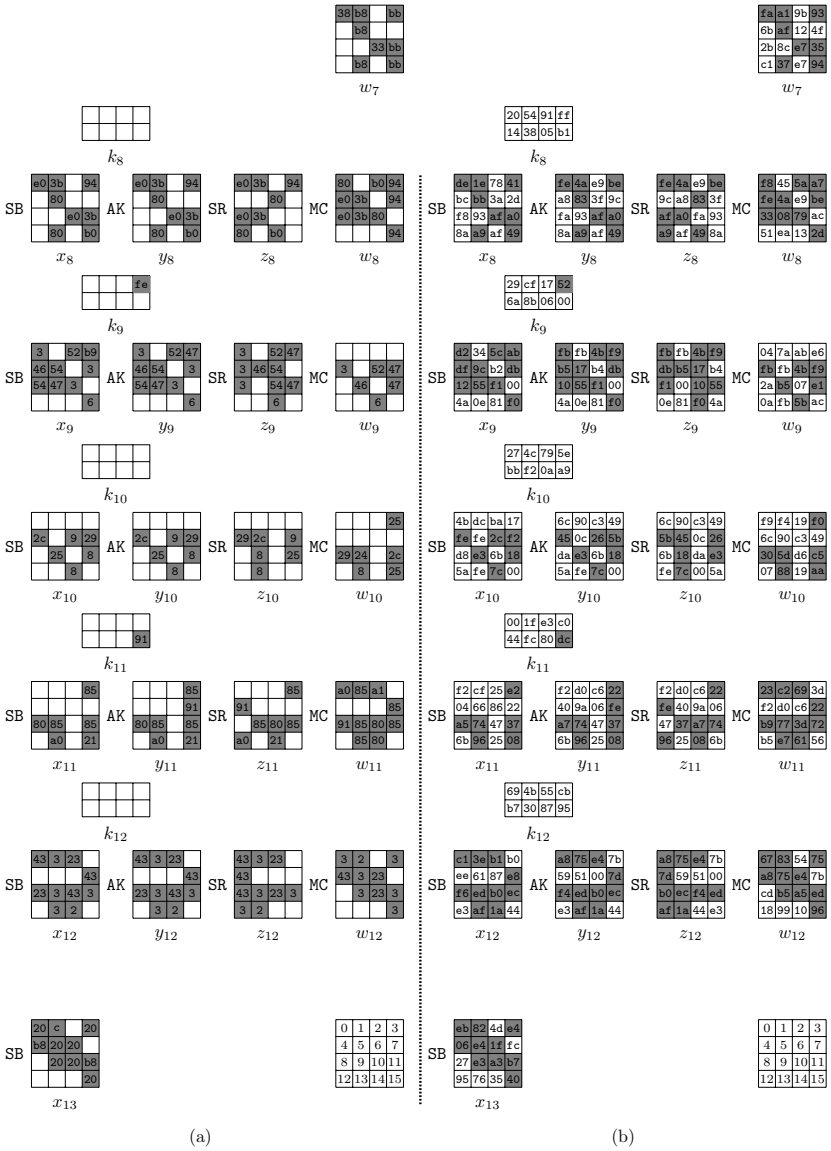

Figure 5: The 6-round multiple inbound phase of `SKINNY-128-384`: (a) The value of differences are given; (b) The value of state and subkey of one of the pair are given. And the values of k_i are the `XOR` of subkeys and constants of `AC` operator.

Precomputation in the multiple inbound phase The multi-step precomputation of the inbound phase that construct the conforming data pairs is explained with Figure 5.

1. Let's first consider the states from z_{10} to x_{11} in Figure 5(a). According to the definition of SKINNY round function, we have $z_{10}[9, 11, 13] = \mathtt{SR}(x_{10}[11, 9, 14])$ and all active bytes of w_{10} can be deduced by assessing DDT with fixed value of differences specified in Figure 5(a). In the second column of z_{10} and w_{10}, we have conditions "$w_{10}[5] \oplus w_{10}[13] = z_{10}[9]$" and "$w_{10}[1] \oplus w_{10}[13] = z_{10}[13]$" corresponding to Equation (1), both of which provide a filter of 2^{-8}. As the differences of the inbound trail are dedicatedly determined in advance, there are enough pairs to verify the filters derived from a given differences. For example, if $(w_{10}[5], w_{10}[13], z_{10}[9]) \in (\mathsf{DDT}[\mathtt{00_x}][\mathtt{00_x}] \times \mathsf{DDT}[\mathtt{8_x}][\mathtt{a0_x}] \times \mathsf{DDT}[\mathtt{47_x}][\mathtt{8_x}])$ are assigned for the condition "$w_{10}[5] \oplus w_{10}[13] = z_{10}[9]$", where $\mathsf{DDT}[\mathtt{00_x}][\mathtt{00_x}]$ represents a full set containing $\{\mathtt{00_x}, \mathtt{01_x}, \ldots\ldots, \mathtt{ff_x}\}$, and $\mathsf{DDT}[\mathtt{8_x}][\mathtt{a0_x}]$ is the subset of DDT with input-output differences $(\mathtt{8_x}, \mathtt{a0_x})$, the size of all combinations of pairs is therefore $|\mathsf{DDT}[\mathtt{00_x}][\mathtt{00_x}] \times \mathsf{DDT}[\mathtt{8_x}][\mathtt{a0_x}] \times \mathsf{DDT}[\mathtt{47_x}][\mathtt{8_x}]| = 256 \cdot 2^4 \cdot 2^3 > 2^8$.
2. When the value of $w_{10}[13]$ is chosen in the last step, $z_{11}[12]$ is determined with the related round operations as well. In addition, with all active bytes of w_{11} deduced through the DDT of round 12, state values of $z_{11}[8, 9, 10, 11]$ are computed with Equation (1) accordingly. The condition $w_{11}[0] \oplus w_{11}[12] = z_{11}[12]$ in the first column of z_{11} and w_{11} is deduced in the same way, which acts as another filter of 2^{-8}.
3. Perform similar steps from z_8 to w_{12}, we get a data and key pair as shown in Figure 5(b) conforming to the whole 6-round inbound trail.

The starting points collected in the multiple inbound phase are exhaustively checked in the outbound phase to search at least one pair that fulfill the outbound trail at the same time. In this work, a 19-round free-start collision attack on the SKINNY-128-384 MMO hashing mode with complexity 2^{35} is successfully obtained. Note that it's a practical free-start collision attack.

5 Free-start Collision Attack on SKINNY-128-256 MMO

In this section, we further introduce classical and quantum rebound attack on SKINNY-128-256 MMO hashing mode. In comparison with Section 4, less degree of freedom is provided from the tweakey of the SKINNY-128-256 MMO. Thus, less rounds is covered in the inbound phase, *i.e.*, a 3-round inbound phase is generated.

5.1 17-Round Quantum Free-start Collision Attack

In quantum setting, we derive the free-start collision attack on MMO hashing mode with 17-round SKINNY-128-256 using the differential characteristic shown in Figure 9 in Appendix A. The 3-round multiple inbound phase starts from state w_7 to x_{10}. The outbound phase happens with probability 2^{-99}.

The identical cryptanalytic strategy described in Section 4 is applied to this 17-round attack. A similar precomputation process illustrated in Figure 6 is performed in the 3-round multiple inbound phase to generate starting points that are exhaustive searched in the outbound phase.

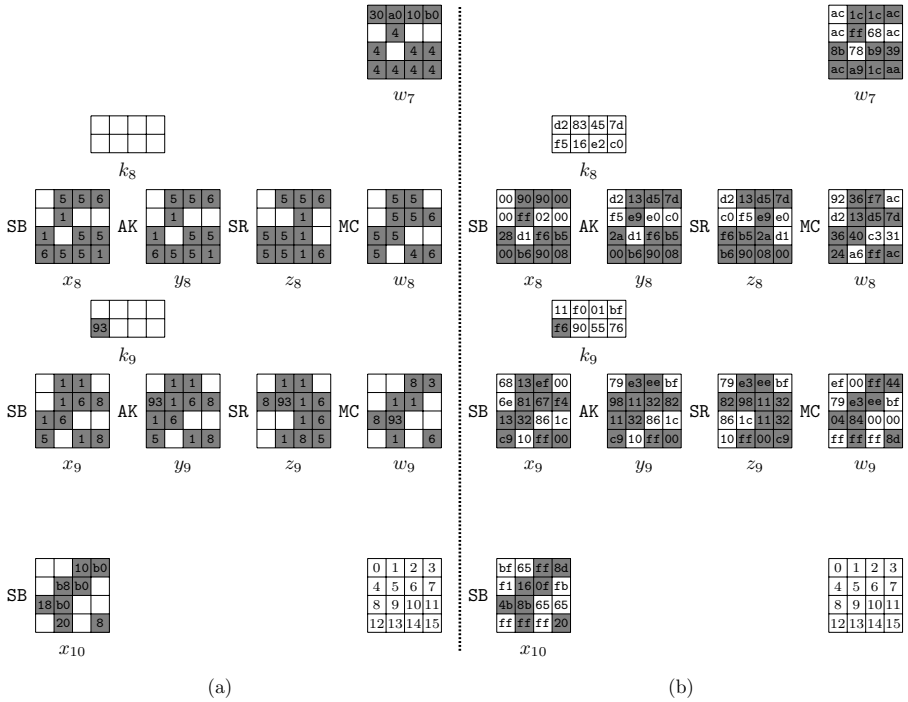

Figure 6: The 3-round multiple inbound phase of `SKINNY-128-256`: (a) The value of differences are given; (b) The value of state and subkey of one of the pair are given. And the values of k_i are the `XOR` of subkeys and constants of `AC` operator.

Overall, we obtain a 17-round free-start collision attack on SKINNY-128-256 MMO hashing in quantum setting of time complexity $2^{49.5}$ with the Grover's algorithm.

5.2 15-Round Classical Free-start Collision Attack

The differential trail of the first classical free-start collision attack on 15-round SKINNY-128-256 MMO hashing mode is given in Figure 10 in Appendix A. The multiple inbound phase includes 3 rounds starting from round 7 to round 9. The way to find starting points in the inbound phase is exactly the same as the 17-round attack in Section 5.1.

An example of the precomputed starting point shown in Figure 7 also satisfies the differential of the last two rows of w_5 to x_6. Since the outbound phase that excludes the S-boxes in the last two rows of x_6 happens with probability $2^{-55.8}$, the final time complexity of the 15-round free-start collision attack is $2^{55.8}$ in classical setting.

6 Conclusions

In this paper, we investigate the security of the SKINNY MMO hashings in quantum and classical settings with respect to collision attacks. Typically, the rebound method is used to achieve the collision attacks on SKINNY-128-256 and SKINNY-128-384 MMO hashings. We develop the MILP-CP based automatic tools to search

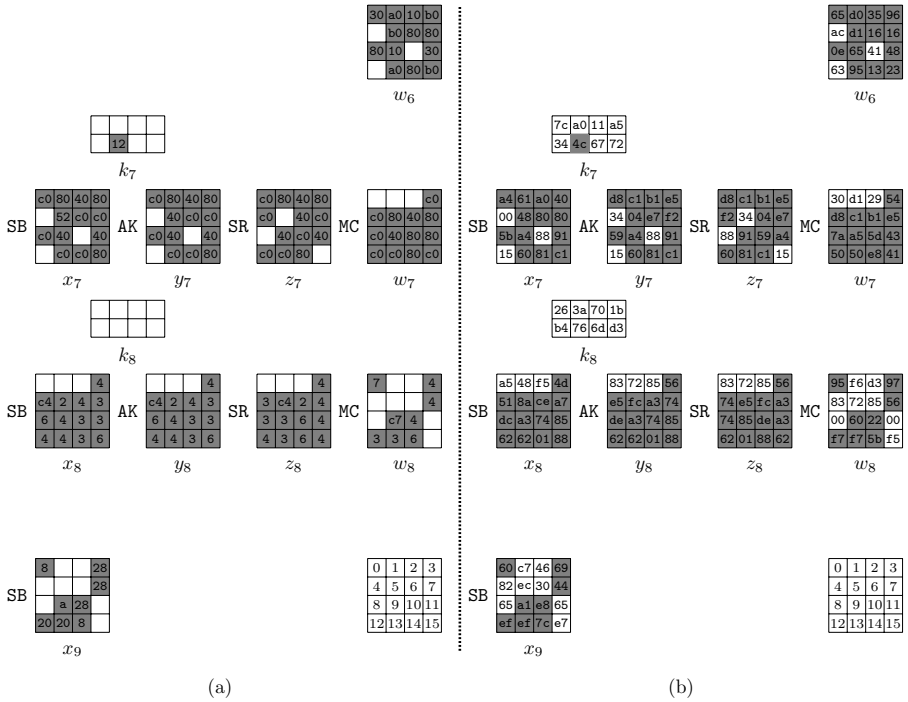

Figure 7: The 3-round multiple inbound phase of `SKINNY-128-256`: (a) The value of differences are given; (b) The value of state and subkey of one of the pair are given. And the values of k_i are the `XOR` of subkeys and constants of `AC` operator.

truncated differential trails of longer rounds for the SKINNY variants. The multiple inbound phase technique is also proposed to cover more rounds. Totally, we present a practical 19-round free-start collision attack on SKINNY-128-384 MMO in classical setting, a 17-round (resp. 15-round) free-start collision attack on SKINNY-128-256 MMO in quantum (resp. classical) setting. As far as we know, all those attacks are the currently best results of collision attacks on those SKINNY hashings. These results serve as an indication that, to achieve long-term security to the post-quantum era, current symmetric-key crypto-systems require careful security re-evaluation or even re-design before being adopted by post-quantum cryptography schemes.

References

1. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The skinny family of block ciphers and its low-latency variant mantis. In: Annual International Cryptology Conference. pp. 123–153. Springer (2016)
2. Bernstein, D.J.: Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete. SHARCS 2009 9: 105.
3. Brassard, G., Høyer, P., Tapp, A.: Quantum Cryptanalysis of Hash and Claw-Free Functions. In: Lucchesi, C.L., Moura, A.V. (eds.) LATIN 1998: Theoretical Informatics, 3rd Latin American Symposium. LNCS, vol. 1380, pp. 163–169. Springer, Heidelberg, Germany, Campinas, Brazil (Apr 20–24, 1998)
4. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography. In: Takagi, T., Peyrin, T.

(eds.) Advances in Cryptology – ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 211–240. Springer, Heidelberg, Germany, Hong Kong, China (Dec 3–7, 2017)
5. Damgård, I.B.: A design principle for hash functions. In: Conference on the Theory and Application of Cryptology. pp. 416–427. Springer (1989)
6. Delaune, S., Derbez, P., Vavrille, M.: Catching the fastest boomerangs application to SKINNY. IACR Trans. Symmetric Cryptol. 2020(4), 104–129 (2020), https://doi.org/10.46586/tosc.v2020.i4.104-129
7. Dong, X., Guo, J., Li, S., Pham, P.: Triangulating rebound attack on aes-like hashing. Cryptology ePrint Archive (2022)
8. Dong, X., Zhang, Z., Sun, S., Wei, C., Wang, X., Hu, L.: Automatic classical and quantum rebound attacks on aes-like hashing by exploiting related-key differentials. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 241–271. Springer (2021)
9. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. pp. 212–219 (1996)
10. Hosoyamada, A., Sasaki, Y.: Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 249–279. Springer, Heidelberg, Germany, Zagreb, Croatia (May 10–14, 2020)
11. Jean, J., Nikolić, I., Peyrin, T.: Tweaks and keys for block ciphers: the tweakey framework. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 274–288. Springer, Berlin, Heidelberg (2014)
12. Lamberger, M., Mendel, F., Rechberger, C., Rijmen, V., Schläffer, M.: Rebound distinguishers: Results on the full whirlpool compression function. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 126–143. Springer (2009)
13. Matyas, S.M.: Generating strong one-way functions with cryptographic algorithm. IBM Technical Disclosure Bulletin 27, 5658–5659 (1985)
14. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: The rebound attack: Cryptanalysis of reduced whirlpool and grøstl. In: International Workshop on Fast Software Encryption. pp. 260–276. Springer (2009)
15. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. Instructor 202101 (2021)
16. Merkle, R.C.: One way hash functions and des. In: Conference on the Theory and Application of Cryptology. pp. 428–446. Springer (1989)
17. Sasaki, Y., Wang, L., Wu, S., Wu, W.: Investigating fundamental security requirements on whirlpool: improved preimage and collision attacks. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 562–579. Springer (2012)
18. van Oorschot, P.C., Wiener, M.J.: Parallel Collision Search with Cryptanalytic Applications. Journal of Cryptology 12(1), 1–28 (Jan 1999)
19. Zalka, C.: Grovers quantum searching algorithm is optimal. Physical Review A 60(4), 2746 (1999)
20. Zhandry, M.: A note on the quantum collision and set equality problems. arXiv preprint arXiv:1312.1027 (2013)

A Figures on the Quantum and Classical Collision Attack on SKINNY MMO hashing

The 19-round SKINNY-128-384 using the differential characteristic shown in Figure 8 in quantum setting.

The quantum 17-round and classical 15-round free-start collision attack on SKINNY-128-256 MMO hashing mode which are shown in Figure 9 and Figure 10 respectively.

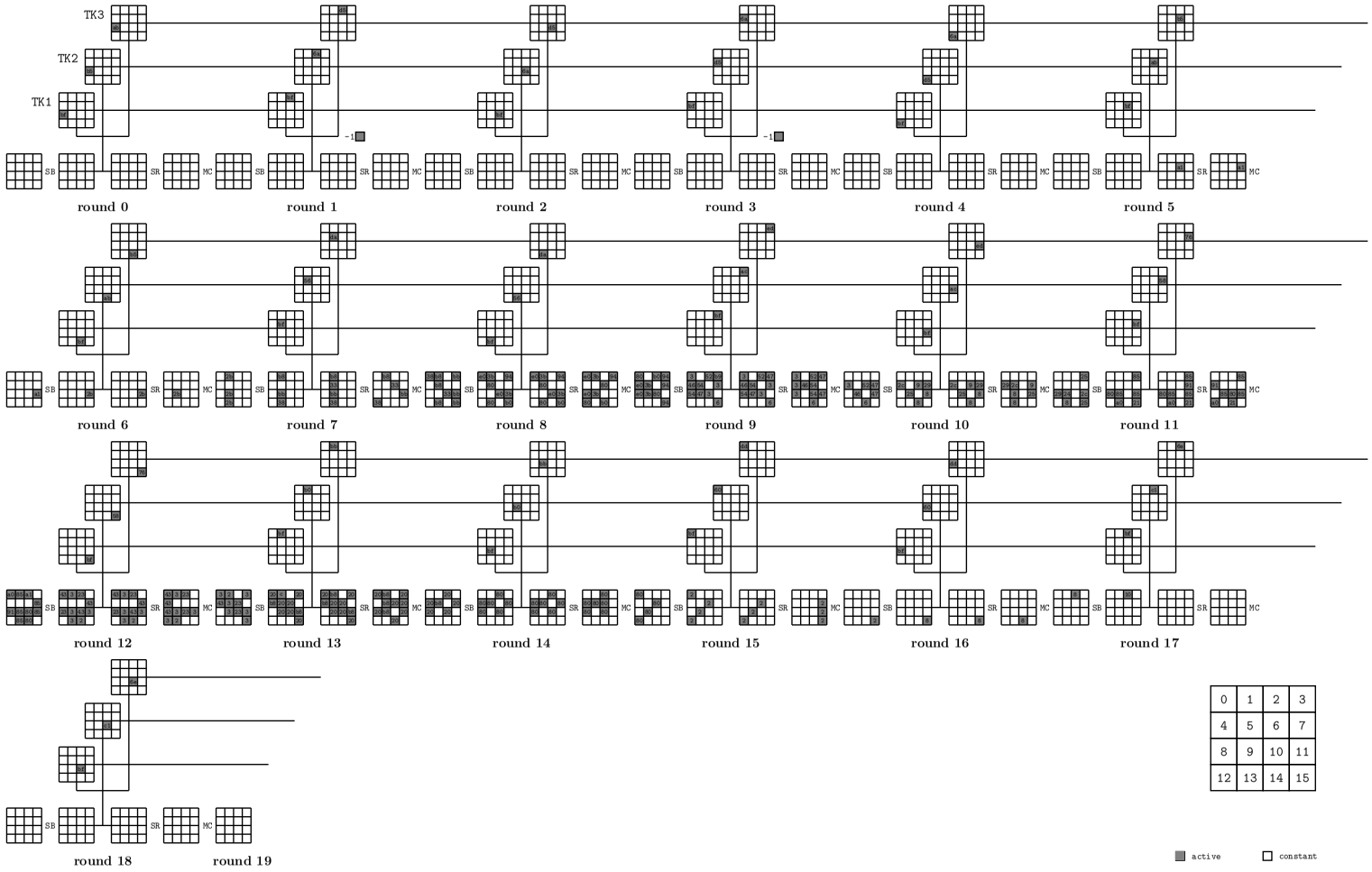

Figure 8: Free-start collision attack on 19-round `SKINNY-128-384`

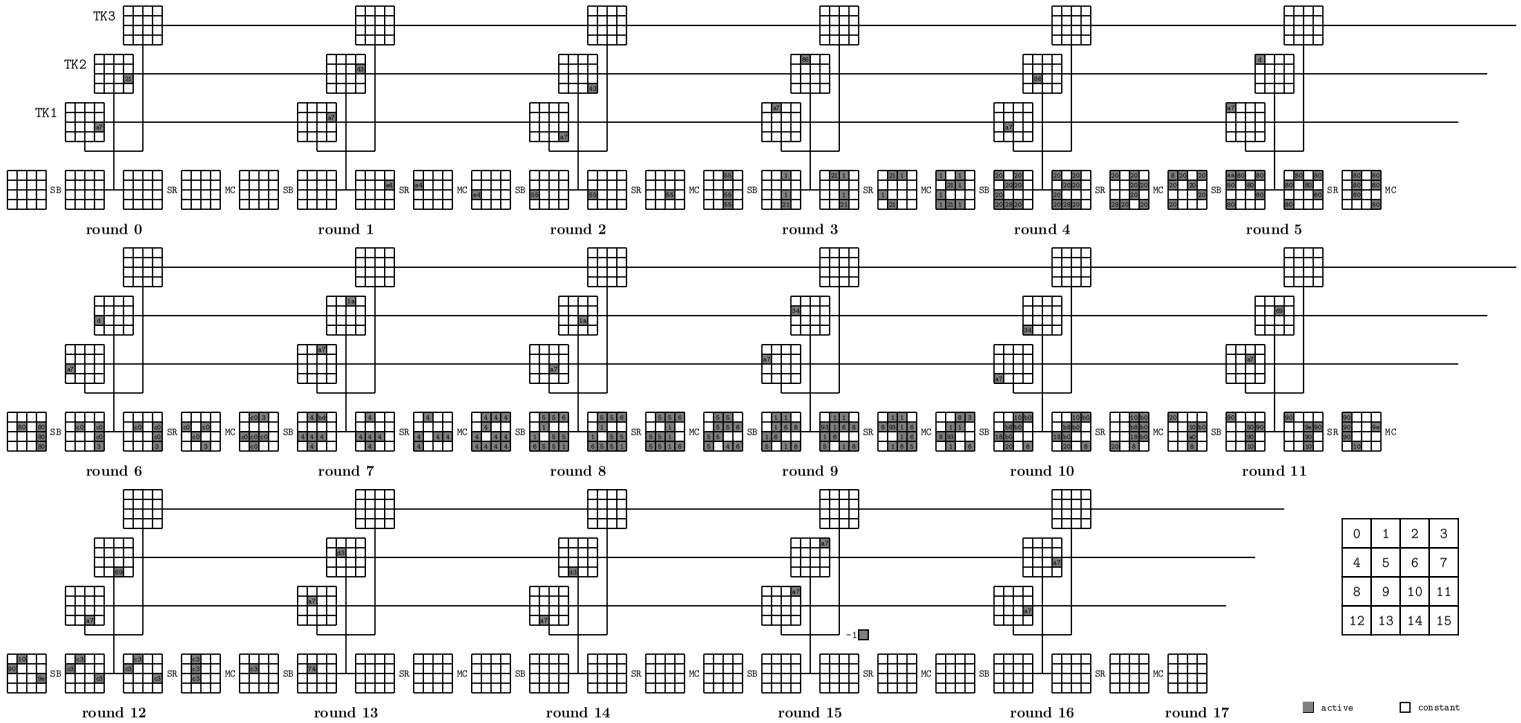

Figure 9: Free-start collision attack on 17-round SKINNY-128-256

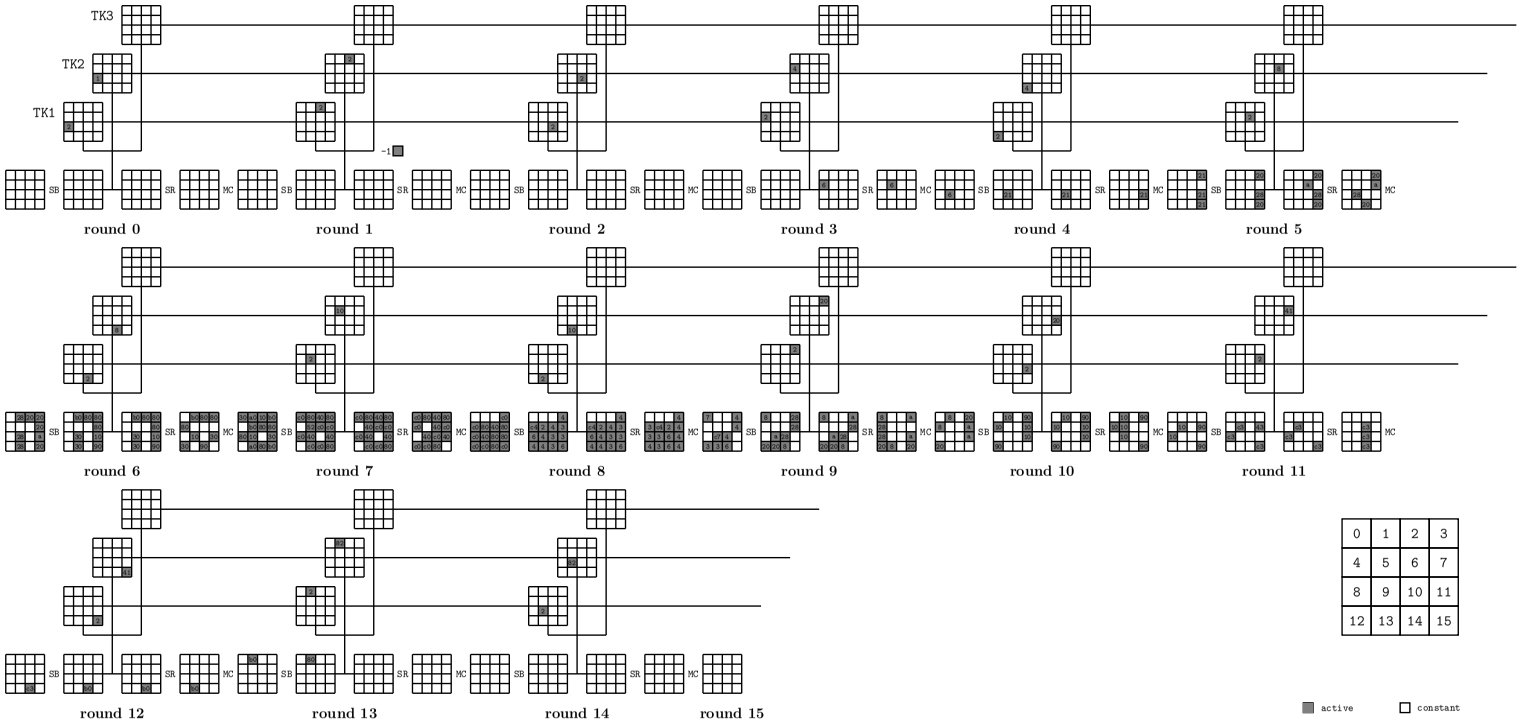

Figure 10: Free-start collision attack on 15-round SKINNY-128-256