Partial-Collision Attack on the Round-Reduced Compression Function of Skein-256

Hongbo Yu[1](✉), Jiazhe Chen[3], and Xiaoyun Wang[2,3]

[1] Department of Computer Science and Technology, Tsinghua University,
Beijing 100084, China

[2] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
{yuhongbo,xiaoyunwang}@mail.tsinghua.edu.cn

[3] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, School of Mathematics,
Shandong University, Jinan 250100, China
jiazhechen@mail.sdu.edu.cn

Abstract. The hash function Skein is one of 5 finalists of the NIST SHA-3 competition. It is based on the block cipher Threefish which only uses three primitive operations: modular addition, rotation and bitwise XOR (ARX). This paper proposes a free-start partial-collision attack on round-reduced Skein-256 by combing the rebound attack with the modular differential techniques. The main idea of our attack is to connect two short differential paths into a long one with another differential characteristic that is complicated. Following our path, we give a free-start partial-collision attack on Skein-256 reduced to 32 rounds with Hamming distance 50 and complexity about 2^{85} hash computations. In particular, we provide practical near-collision examples for Skein-256 reduced to 24 rounds and 28 rounds in the fixed tweaks and choosing tweaks setting separately.

As far as we know, this is the first construction of a non-linear differential path for Skein which can lead to significantly improvement over previous analysis.

Keywords: Hash function · Near-collision · SHA-3 · Skein

1 Introduction

Cryptographic hash functions are very important in modern cryptology which provide integrity, authentication, etc. In 2005, as the most widely used hash functions MD5 and SHA-1 were broken by Wang *et al.* [15,16], the status of the hash functions becomes alarming. To deal with the undesirable situation, NIST

Supported by 973 program (No. 2013CB834205), the National Natural Science Foundation of China (No. 61133013 and 61373142), the Tsinghua University Initiative Scientific Research Program (No. 20111080970), and Tsinghua National Laboratory for Information Science and Technology.

S. Moriai (Ed.): FSE 2013, LNCS 8424, pp. 263–283, 2014.
DOI: 10.1007/978-3-662-43933-3_14, © Springer-Verlag Berlin Heidelberg 2014

started a hash competition for a new hash standard (SHA-3) in 2007. A total of 64 hash function proposals were submitted, and 51 of them advanced to the first round. After more than one-year's evaluation, 14 submissions have entered into the second round. By 2010, the competition came into the final round, and 5 out of the second round candidates were selected as finalists. Now NIST chooses Keccak [2] as the SHA-3 winner.

Skein [3] is one of the five finalists, which is a ARX-type hash function (based on modular addition, rotation and exclusive-OR). The core of Skein is a tweakable block cipher called Threefish, which is proposed with 256-, 512-, 1024-bit block sizes and 72, 72, 80 rounds respectively. During the competition, Skein has been attracting the attention of the cryptanalysts, and there are several cryptanalytic results on the security of the compression function of Skein. At Asiacrypt 2009 [1], Aumasson *et al.* proposed a free-start near-collision attack for 17-round Skein-512 compression function with the old constants. At CANS 2010 [14], Su *et al.* presented free-start near-collisions of Skein-256/-512 reduced to 20 rounds and Skein-1024 reduced to 24 rounds. At Asiacrypt 2010 [9], Khovratovich *et al.* combined the rotational attack with the rebound attack, and gave distinguishers for 53-round Skein-256 and 57-round Skein-512 respectively. When the algorithm was getting into the second round, the authors had changed the rotation constants to resist the rotational attack [8,9]. For the new version of Skein, Leurent and Roy [12] gave a boomerang distinguisher for 32-round compression function of Skein-256 and Yu *et al.* [17] provided a boomerang distinguisher for 36-round Skein-512. At FSE 2012 [10], Khovratovich *et al.* gave a pseudo-preimage attack on 22-round Skein-512 hash function and 37-round Skein-512 compression function by the biclique method, and their complexities of the attack are only marginally lower than exhaustive search.

Rebound attack for the ARX-type hash function. The rebound attack was presented by Mendel *et al.* at FSE 2009 [5] during the SHA-3 evaluation, it is used to analyze the hash functions based on the AES-like structure. Series of hash functions such as Whirlpool, Grøstl and JH [5–7,11] are vulnerable to the rebound attack. Its basic strategy is to match two short truncated differentials in the middle using freedom degrees of the chaining values and messages. As the matching part is the S-box layer, which has a good distribution for the input and output differences, i.e., the average probability for each input/output difference pair to pass the S-box is 1/2, one can search the differentials that can be connected with high probability.

However, when applying the rebound attack to the ARX-type hash functions, we have to find two specific differentials that can be matched. Furthermore, there aren't S-boxes in the connecting layer, and the distribution of the differences by applying the modular addition, rotation and XOR operations is harder to decided than that of S-boxes. As a result, it is far more difficult to apply the rebound attack to the ARX-type hash functions by connecting two differential paths into a long one.

Our contribution. This paper focuses on the cryptanalysis of Skein-256 compression function. We attempt to apply the rebound-type idea to the differential

Table 1. The main results of this paper.

Type	Rounds	Hamming distance	Complexity
Fixed-tweak free-start near-collision	24 (4–28)	2	2^{26}
Free-tweak free-start near-collision	28 (0–28)	34	2^{44}
Free-tweak free-start near-collision	28 (4–32)	28	2^{41}
Free-tweak free-start partial-collision	32 (0–32)	50	2^{85}

attack on the ARX-type algorithms. We first find two short differential paths by the modular differential techniques, then connect them to get a 32-round differential path. Finally, by applying the message modification techniques, we give a partial-collision attack on 32-round Skein-256 compression function. In order to verify the validity of our differential path, we provide examples of near-collision which follow our differential path for Skein-256 reduced to 24 and 28 rounds. The main results of this paper are shown in Table 1.

The rest of the paper is organized as follows. In Sect. 2, we give some notations and a brief description of Skein-256 compression function. The main idea of our attack is described in Sect. 3. In Sect. 4, we demonstrate the techniques of our attack in detail. Finally, a conclusion is given in Sect. 5.

2 Preliminaries

In this section, we first give some notations used through the paper, and then describe the compression function of Skein-256 briefly.

2.1 Notations

1. $\oplus$: exclusive-OR (XOR)
2. $+$ and $-$: addition and subtraction modular 2^{64}
3. Δa: the XOR difference of a and a'
4. $\Delta^{+} a$: the modular subtraction difference of a and a' (modular 2^{64})
5. $\lll$: rotation to the left
6. $a_{i,j}$: the j-th bit of a_i, where a_i is a 64-bit word and $a_{i,64}$ is the most significant bit
7. $a_{i,j-k}$: the abbreviation of $a_{i,j}$, $a_{i,j+1}$,...,$a_{i,k}$

2.2 Near-Collision and Partial-Collision

The Handbook of Applied Cryptography [4] defines near-collision resistance by

Near-collision resistance. Let h be a hash function, it is hard to find any two inputs M, M' such that $h(M)$ and $h(M')$ differ in a small number of bits.

More specifically, h is a hash function that takes an n-bit initial value IV and an m-bit message block M as inputs, and outputs another n-bit chaining value.

A k-bit ($k < n$) near-collision on h is obtained whenever two messages M_1 and M_2 satisfy:

$$HW(h(M_1, IV) \oplus h(M_2, IV)) = n - k,$$

where HW denotes the Hamming distance. Usually, we comprehend the “small number” as $n - k \leq n/3$.

- For a generic attack, it is expected to have a k-bit near-collision with complexity about $\sqrt{2^n/C_n^k}$. For $n = 256$ and $k = 206$, the complexity is only approximate to 2^{39} hash computations; for $n = 256$ and $k = 28$, the complexity is about $2^{66.5}$.
- However, if we fix the k-bit colliding positions, the complexity for finding a near-collision with Hamming distance $n - k$ is about $2^{k/2}$ by the birthday paradox. Previous works [13] have used the terms **partial-collision** for this notion. For $n = 256$ and $k = 206$, the complexity to find a 206-bit partial-collision is about 2^{103}.
- When we fix the k-bit colliding positions and keep the differences in the other positions being non-zero (actually, in this case the output difference is a given difference with k-bit zeroes), the complexity for finding a k-bit near-collision is about $2^{n/2}$ by the birthday paradox. For $n = 256$, the complexity is 2^{128} no matter what the value of k is.
- Furthermore, when input difference is also fixed, the generic complexity would be 2^n. In this paper, our attack belong to this case.

2.3 Brief Description of the Compression Function of Skein-256

The compression function of Skein is defined as $H = E(IV, T, M) \oplus M$, where $E(IV, T, M)$ is the block cipher Threefish, M is the message, IV is the initial value and T is the tweak value. Here E takes the message as plaintext and the IV as master key. The word size which Skein operates on is 64 bits. For Skein-256, both M and IV are 256 bits, and the length of T is 128 bits. Let us denote $h_i = (a_i, b_i, c_i, d_i)$ as the output value of the i-th round, where a_i, b_i, c_i and d_i are 64-bit words. Let $h_0 = M$ be the plaintext, the encryption procedure of Threefish-256 is carried out for $i = 1$ to 72 as follows.

If $(i-1) \mod 4 = 0$, first compute $A_{i-1} = a_{i-1} + K_{(i-1)/4,a}$, $B_{i-1} = b_{i-1} + K_{(i-1)/4,b}$, $C_{i-1} = c_{i-1} + K_{(i-1)/4,c}$ and $D_{i-1} = d_{i-1} + K_{(i-1)/4,d}$, where $K_{(i-1)/4}$ are round subkeys which get involved every four rounds. Then carry out:

$$a_i = A_{i-1} + B_{i-1}, d_i = a_i \oplus (B_{i-1} \lll R_{i,1}),$$
$$c_i = C_{i-1} + D_{i-1}, b_i = c_i \oplus (D_{i-1} \lll R_{i,2}),$$

where $R_{i,1}$ and $R_{i,2}$ are rotation constants which can be found in [3]. For the sake of convenience, we denote $\overline{h_{i-1}} = (A_{i-1}, B_{i-1}, C_{i-1}, D_{i-1})$.

If $(i-1) \mod 4 \neq 0$, compute:

$$a_i = a_{i-1} + b_{i-1}, d_i = a_i \oplus (b_{i-1} \lll R_{i,1}),$$
$$c_i = c_{i-1} + d_{i-1}, b_i = c_i \oplus (d_{i-1} \lll R_{i,2}).$$

After the last round, the ciphertext is computed as $\overline{h_{72}}$.

The key schedule starts with the master key $K = (k_0, k_1, k_2, k_3)$ and the tweak value $T = (t_0, t_1)$. First we compute:

$$k_4 := 0x1bd11bdaa9fc1a22 \oplus \bigoplus_{i=0}^{3} k_i \quad \text{and} \quad t_2 := t_0 \oplus t_1.$$

Then the subkeys are derived for $s = 0$ to 18:

$$\begin{aligned} K_{s,a} &:= k_{(s+0) \bmod 5} \\ K_{s,b} &:= k_{(s+1) \bmod 5} + t_{s \bmod 3} \\ K_{s,c} &:= k_{(s+2) \bmod 5} + t_{(s+1) \bmod 3} \\ K_{s,d} &:= k_{(s+3) \bmod 5} + s \end{aligned}$$

3 Outline of Our Attack

Skein is one of the SHA-3 finalists which uses the operations modular addition, rotation and XOR. Because of the strong diffusion after several rounds, only short differential paths can be found for Skein. An easy way to get short differential path is to find a short local collision in the middle, and then extend the local collision forward and backward, see the left part of Fig. 1. After finding a differential path of this type, we try to modify the message of the first several rounds to enhance the efficiency. For Skein, by choosing proper differences in the messages, IVs and tweak values, we can get a local collision for 8 rounds. Then we can get differential paths with more rounds by extending the 8-round local collision forward and backward. But longer differential path is not easy to search as a single bit difference will propagate to a heavy weight difference after 4 rounds. A natural idea is raised to connect two short differential paths into a long one, and then cancel a vast number of conditions by using message modification techniques in the connecting layer, see the right part of Fig. 1. The most expensive part of this strategy is the connection of the two differential paths, which is described in Sect. 4. To solve this problem, we use the properties of both XOR difference and modular subtraction difference, and choose an optimal position for the connection. Then by the bit-carry technique (which is the key technique for the connection), we find a 8-round non-linear differential to connect two short differential paths with 16 and 8 rounds respectively. Consequently, a differential path with 32 rounds is constructed, which can be used to mount near-collision attack on 32-round Skein-256 by further applying message modification techniques to reduce the conditions. The details of our attack can be found in Sect. 4.

Actually, our method can be applied to the ARX-type hash functions that do not have complex message extensions, and the message words or IVs get involved every round (or every several rounds).

4 Partial Collisions for 32-Round Compression Function of Skein-256

As mentioned above, the basic idea of our near-collision attack is to connect two short differential paths into a long one. To achieve this purpose, there are several steps to be carried out. Firstly, proper difference in (K, T) should be chosen, which is the starting point of our attack. Secondly, we connect two short differential paths by the non-linear expansion in the middle rounds, and derive the sufficient conditions to guarantee the differential path to hold. Thirdly, the vast number of conditions in the intermediate rounds should be corrected by modifying the chaining variables, the key K and the tweak value T. Finally, after the message/IV modification, we search the remaining conditions by divide and conquer technique.

4.1 Finding Two Short Differential Paths

The differences of the master key $K = (k_0, k_1, k_2, k_3)$ and tweak value $T = (t_0, t_1)$ selected for our differential path are $\Delta k_3 = 2^{63}$ and $\Delta t_0 = 2^{63}$. According to the key schedule, the differences for the subkey $K_i = (K_{i,a}, K_{i,b}, K_{i,c}, K_{i,d})$ $(0 \leq i \leq 8)$ are shown in Table 2.

The first short differential path we used consists of 16 rounds. Because $\Delta K_1 = (0, 0, 0, 2^{63})$ and $\Delta K_2 = (0, 0, 0, 0)$, the intermediate values are selected to meet $\Delta h_4 = (0, 0, 0, 2^{63})$, resulting in an 8-round path with zero differential from rounds 5 to 12. By extending the difference Δh_4 in the backward direction for 4 rounds and the difference $\Delta \overline{h_{12}} = \Delta K_3$ in the forward direction for 4 rounds by the linear expansion, a 16-round differential path with high probability can be obtained.

The second differential path is shorter than the first one, as the number of zero-difference rounds in it is only 4. We choose Δh_{24} as $(0, 2^{63}, 2^{63}, 2^{63})$ to compensate the difference $\Delta K_6 = (0, 2^{63}, 2^{63}, 2^{63})$, which results in zero difference in rounds 25 to 28. As a consequence, a 8-round differential path with high probability can be obtained by linearly expanding the difference $\Delta \overline{h_{28}} = \Delta K_7$ in the forward direction for 4 rounds.

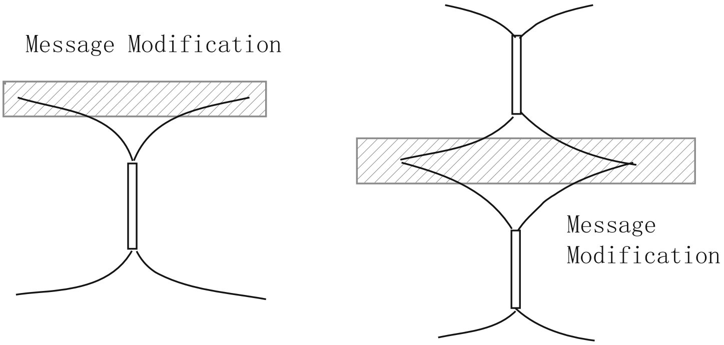

Fig. 1. Two attack models

Table 2. The subkey differences of 32-round Skein-256, given a difference $\delta = 2^{63}$ in k_3 and t_0.

i	Rd	$K_{i,a}$	$K_{i,b}$	$K_{i,c}$	$K_{i,d}$
0	0	k_0	$k_1 + t_0$	$k_2 + t_1$	k_3
		0	δ	0	δ
1	4	k_1	$k_2 + t_1$	$k_3 + t_2$	$k_4 + 1$
		0	0	0	δ
2	8	k_2	$k_3 + t_2$	$k_4 + t_0$	$k_0 + 2$
		0	0	0	0
3	12	k_3	$k_4 + t_0$	$k_0 + t_1$	$k_1 + 3$
		δ	0	0	0
4	16	k_4	$k_0 + t_1$	$k_1 + t_2$	$k_2 + 4$
		δ	0	δ	0
5	20	k_0	$k_1 + t_2$	$k_2 + t_0$	$k_3 + 5$
		0	δ	δ	δ
6	24	k_1	$k_2 + t_0$	$k_3 + t_1$	$k_4 + 6$
		0	δ	δ	δ
7	28	k_2	$k_3 + t_1$	$k_4 + t_2$	$k_0 + 7$
		0	δ	0	0
8	32	k_3	$k_4 + t_2$	$k_0 + t_0$	$k_1 + 8$
		δ	0	δ	0

4.2 Connecting the Two Short Differential Paths

The most difficult work in this paper is to connect the two short differential paths from rounds 16 to 24 by the non-linear difference expansion. We choose the 20-th round as the connecting point; the reason is that the 20-th round is the place where the subkeys is involved (in the form of integer modular addition), if we connect the two differential paths in this round, the only requirement is that the integer modular substraction differences $\Delta^+ h_{20}$ computed by the forward direction and the $\Delta^+ \overline{h_{20}}$ computed by the backward direction should satisfy the equation $\Delta^+ \overline{h_{20}} = \Delta^+ h_{20} + \Delta^+ K_5$. Otherwise, if we connect the two differential paths in the other rounds in which the subkeys do not intervene, both the integer modular substraction differences and the XOR differences computed by two directions must be equal. This will face more difficulties for connecting.

For example, let $\Delta a_i = 0x37$ be the XOR difference of round i computed in the forward direction, and $\Delta A_i = 0x11$ be the difference computed in the backward direction; the i-th round is the round where we want to match Δa_i and ΔA_i. If $i = 20$, it is easy to know that the difference $\Delta^+ a_i$ equals to $\Delta^+ A_i$ as long as $A_{i,1} = a_{i,1} \oplus 1$, $a_{i,1} = a_{i,2} = a_{i+3} \oplus 1$, $A_{i,5} = a_{i,5} \oplus 1$ and $a_{i,5} = a_{i,6} \oplus 1$.

Hence Δa_i and ΔA_i can be connected with probability 2^{-5}. Otherwise, if $i = 19$, it is obvious that Δa_i and ΔA_i can not be connected because $\Delta a_i \neq \Delta A_i$.

The major technique to connect two differential paths is the bit-carry technique; hundreds of bit equations need to be handled during the process of connection. Now we describe how to connect the two differential paths briefly.

For $16 < i \leq 20$, firstly we compute the modular difference $\Delta^+ a_{i+1} = \Delta^+ a_i + \Delta^+ b_i$ and $\Delta^+ c_{i+1} = \Delta^+ c_i + \Delta^+ d_i$, then we convert the modular differences into XOR differences so that Δa_i and Δc_i have the lowest Hamming weights respectively. Finally, the XOR differences Δb_{i+1} and Δd_{i+1} are computed as $\Delta b_{i+1} = \Delta c_{i+1} \oplus (\Delta d_i \lll R_{i,2})$ and $\Delta d_{i+1} = \Delta a_{i+1} \oplus (\Delta b_i \lll R_{i,1})$. In the same way, we can compute Δh_{24} to $\Delta \overline{h_{20}}$ by the backward direction so that the Hamming weights of Δa_i and Δc_i $(20 \leq i \leq 24)$ are as low as possible (see Table 2).

What we have to do next is to match Δh_{20} and $\Delta \overline{h_{20}}$ so that their integer modular substraction difference is equal to $\Delta^+ K_5$. Generally, we first select $\Delta^+ a_{20}$ and $\Delta^+ c_{20}$ as the targets, and adjust the differences $\Delta^+ A_{20}$ and $\Delta^+ C_{20}$ to match $\Delta^+ a_{20}$ and $\Delta^+ c_{20}$ respectively by making a decision for the differences of $\Delta \overline{h_{20}}$ to Δh_{24}. Then we regard ΔB_{20} and ΔD_{20} as the targets again, and adjust the differences Δb_{20} and Δd_{20} to be consistent with ΔB_{20} and ΔD_{20} by modifying the differences Δh_{16} to Δh_{20}.

In the following, we demonstrate how to match the modular substraction differences of a_{20} and A_{20} as an example. Here $\Delta^+ a_{20}$ is the target, hence we would like to adjust the difference $\Delta^+ A_{20}$ by modifying the differences Δa_{21}, Δd_{21}, Δb_{22}, Δa_{23} and Δd_{23} so that $\Delta^+ a_{20} = \Delta^+ A_{20}$. From Table 3, we can express the modular differences of Δa_{20} and ΔA_{20} as

$$\Delta^+ a_{20} = \pm \mathbf{2^0} \pm 2^3 \pm 2^8 \pm \mathbf{2^{12}} \pm 2^{14} + ...$$

$$\Delta^+ A_{20} = \pm \mathbf{2^0} \pm 2^2 \pm 2^4 \pm 2^6 \pm \mathbf{2^{12}} \pm 2^{24} + ...$$

In order to match the 13 least significant bits of $\Delta^+ a_{20}$ and $\Delta^+ A_{20}$, we should eliminate the differences $\pm 2^2 \pm 2^4 \pm 2^6$ and produce the differences $\pm 2^3 \pm 2^8$ for $\Delta^+ A_{20}$. What has to be done is extending the bit differences in bold in Table 3. We first extend the differences $\Delta B_{20,1}$, $\Delta B_{20,3}$, $\Delta B_{20,5}$ and $\Delta B_{20,7}$ to be $\Delta B_{20,1-2}$, $\Delta B_{20,3-4}$, $\Delta B_{20,5-6}$ and $\Delta B_{20,7-9}$, respectively. And then, to obtain these extensions, differences $\Delta d_{21,26}$, $\Delta b_{22,38}$ and $\Delta a_{23,32}$ are modified for $\Delta B_{20,1}$; $\Delta a_{21,28}$ is modified for $\Delta B_{20,3}$; $d_{21,30}$ and $c_{22,42}$ are modified for $\Delta B_{20,5}$. In Table 3, we show the bit differences after extension in the brackets. Because $A_{20} = a_{21} - B_{20}$, we can produce the desired differences $\pm 2^3 \pm 2^8$ for A_{20} by further setting some conditions on B_{20} as follows:

$$\begin{aligned}
&B_{20,1} = B_{20,2} = B_{20,3} \oplus 1, \\
&B_{20,4} = a_{20,4}, \\
&B_{20,4} = B_{20,5} = B_{20,6} = B_{20,7} = B_{20,8} \oplus 1, \\
&B_{20,9} = a_{20,9} \oplus 1.
\end{aligned}$$

Table 3. Two differential paths for rounds 16 ∼ 20 and rounds 24 ∼ $\overline{20}$.

Round	shifts	Δa_i	Δb_i	Δc_i	Δd_i
16	32, 32	12, 22, 64	6, 12, 26, 38, 44, 58	6, 12, 58, 64	12, 22, 54
17	14, 16	6, 22, 26, 38, 44, 58, 64	22, 28, 38, 54, 58, 64	6, 22, 54, 58, 64	6, 8, 20, 22, 38, 40, 44, 52, 64
18	52, 57	6, 26, 28, 44, 54	1, 8, 13, 15, 20, 31, 33, 37, 38, 40, 44, 45, 52, 54, 57, 58, 63	8, 20, 38, 40, 44, 52, 54, 58	6, 10, 16, 28, 42, 44, 46, 52, 54
19	23, 40	1, 6, 8, 13, 15, 20, 26, 28, 31, 33, 37, 40, 52, 57, 63	4, 6, 8, 10, 16, 18, 22, 30, 38, 40, 42, 45, 46, 50, 56, 58	6, 8, 10, 16, 20, 28, 38, 40, 42, 45, 58	1, 3, 4, 6, 8, 11, 15, 16, 17, 20, 22, 24, 26, 28, 33, 36, 37, 38, 40, 43, 52, 54, 56, 57, 60, 61, 63
20	5, 37	1, 4, 9, 13, 15, 18, 20, 22, 26, 28, 30, 33, 37, 42, 45, 50, 52, 56, 63	3, 6, 8, 9, 11, 13, 15, 16, 22, 24, 25, 26, 27, 29, 30, 34, 38, 40, 43, 48, 53, 56, 57, 59, 60, 61	1, 3, 8, 10, 15, 22, 24, 26, 33, 36, 41, 45, 52, 54, 56, 60, 63	1, 4, 11, 18, 20, 21, 22, 23, 26, 27, 28, 30, 31, 33, 35, 37, 42, 43, 47, 51, 52, 55, 56, 61
$+\Delta K_5$		0	2^{63}	2^{63}	2^{63}
$\overline{20}$	5, 37	1, 3, 5, 7, 13, 25, 27, 31, 35, 37, 50, 56, 60	**1**(1-2), **3**(3-4), **5**(5-6), **7**(7-9), 13, 25, 27, 31, 35, 37	9, 17, 19, 23, 26, 29, 41, 52, 57, 59, 61, 64	9, 17, 19, 23, 27, 29, 31, 41, 57, 59, 61
21	25, 33	**28**(28-29), **32** (32-34), 38, 50, 56, 60	28, 50, 56, 60	10, 26, 30, 42, 52, 62, 64	**26**(26-27), **30**(30-31), 52, 62
22	46, 12	32, 38	**38**(38-39)	10, **42**(42-43), 64	10, 42
23	58, 22	**32**(32-33)	32	64	0
24	32, 32	0	64	64	64

The entries of this Table indicate the positions of the difference bits of h_i.

Similarly, we can also match the other differences of a_{20} and A_{20}. That is, once an inconsistency occurs, we have to jump back to an earlier stage and make a different decision about the difference; this might result in changes of stages that are even earlier. Note that in this course, the following two requirements have to be considered.

1. For Skein-256, the subkeys (the IVs) intervene in the chaining values every 4 rounds, hence the degrees of freedom of four rounds between two subkeys are 256. As a result, the conditions deduced from guaranteeing the 4-round differential path to hold must be less than 256.
2. The conditions deduced from the 32-round differential path should be less than 640, because the degrees of the freedom of the M, K and T are 640.

The 32-round near-collision differential path is shown in Table 4. In Table 4, we use two kinds of difference: the XOR difference and the integer modular substraction difference. In the round $\bar{i}$ (the round after adding the subkey, $i = 0, 4, 8, ..., 28$), we express the difference in the positions a and c with the integer modular substraction difference, i.e., $\Delta^+ A_i = \Delta^+ a_i + \Delta^+ K_{i,a}$ and $\Delta^+ C_i = \Delta^+ c_i + \Delta^+ K_{i,c}$, because we only use the integer modular addition properties of A_i and C_i when computing the chaining value h_{i+1}). In the other positions of the differential path, we use the XOR difference (see Table 4).

Corresponding to the differential path in Table 4, we can compute the sufficient conditions in $h_{20} \sim h_0$ and $\overline{h_{20}} \sim \overline{h_{32}}$, which are shown in Tables 7 and 8 respectively.

4.3 Message/IV Modification

In order to fulfill the Message/IV modification, we replace the conditions $b_{i,j}$, $d_{i,j}$ ($\overline{16} \leq i \leq 19, 1 \leq j \leq 32$) from the round 19 down to round $\overline{16}$ in Table 7 with

Table 4. Differential path used for the partial-collision of 32-round compression function of Skein-256, with a probability of 2^{-89} after the message/IV modification.

Round	Δa_i	Δb_i	Δc_i	Δd_i
0	0500900a50210840	8100100210210800	0040040082044204	8040000084004204
$\overline{0}$:$+K_0$	$\Delta^+ a_0$	0100100210210800	$\Delta^+ c_0$	0040000084004204
1	0400800840000040	0000800040000040	0000040002040000	0000040002000000
2	0400000800000000	0000000800000000	0000000000040000	0000000000040000
3	0400000000000000	0400000000000000	0000000000000000	0000000000000000
4	0000000000000000	0000000000000000	0000000000000000	8000000000000000
$\overline{4}$:$+K_1$	0000000000000000	0000000000000000	0000000000000000	0000000000000000
$5-12$	0000000000000000	0000000000000000	0000000000000000	0000000000000000
$\overline{12}$:$+K_3$	8000000000000000	0000000000000000	0000000000000000	0000000000000000
13	8000000000000000	0000000000000000	0000000000000000	8000000000000000
14	8000000000000000	8000000000000800	8000000000000000	8000000000000000
15	0000000000000800	0000000000200000	0000000000000000	0200000000000820
16	0000000000200800	0600082002000820	0600000000000820	0020000000200800
$\overline{16}$:$+K_4$	$\Delta^+ a_{16} + 2^{63}$	0600182006000820	$\Delta^+ c_{16} + 2^{63}$	0020000000600800
17	8600182002200020	8260006008200000	8260000000200020	800819a0002801a0
18	08a0080006000020	4328099340d85f83	022819a000d80f80	08a82e0000008220
19	7898108fc7e9d4a1	0a4230a8a86980a0	0ac010a0004780a0	b1387ca0064840a5
20	d146001565005501	800001b6251fd503	4908150002104103	9900150068304100
$\overline{20}$:$+K_5$	$\Delta^+ a_{20}$	0000019fe700f703	$\Delta^+ c_{20} + 2^{63}$	39001f01ebf3ff00
21	dfc601eff8000000	f7fe000008000000	2019fe007a003e03	e0080001fe000003
22	00003fff80000000	000001e000000000	80001e0000003e00	0000020000000200
23	0000000780000000	0000000080000000	8000000000000000	0000000000000000
24	0000000000000000	8000000000000000	8000000000000000	8000000000000000
$\overline{24}$:$+K_6$	0000000000000000	8000000000000000	8000000000000000	8000000000000000
25-28	0000000000000000	0000000000000000	0000000000000000	0000000000000000
$\overline{28}$:$+K_7$	0000000000000000	8000000000000000	0000000000000000	0000000000000000
29	8000000000000000	0000000000000000	0000000000000000	8000000001000000
30	8000000000000000	8000001001000800	8000000001000000	8000000000000000
31	0000001001000800	0000000001200000	0000000001000000	0200001041040820
32	0000001000200800	4304083042040830	0200001040040820	0120001000200800
$\overline{32}$:$+K_8$	8000001000200800	c104081042040810	8200001040040820	0120001000200800
Output Difference	8500901a50010040	4004181250250010	82400410c2004a24	8160001084204a04

$a_{i+1,((j+R_{i+1,0}) \mod 64)} \oplus d_{i+1,((j+R_{i+1,0}) \mod 64)}$ and $b_{i+1,((j+R_{i+1,1}) \mod 64)} \oplus c_{i+1,((j+R_{i+1,1}) \mod 64)}$ respectively.

We divide the conditions in Tables 7 and 8 into three groups which are shown in Tables 9, 10, and 11 separately. The conditions in group-1 include all the conditions from round $\overline{16}$ to 20 which are determined by h_{20}=(a_{20}, b_{20}, c_{20} and d_{20}). The conditions in group-2 consist of the conditions in $\overline{h_{20}}$,h_{21},...,h_{24} and c_{16} that depend on h_{20} and K_5. All the other conditions are incorporated into group-3 which are decided by h_{20}, K_5, $K_{4,b}$ and $K_{4,d}$. The distribution of the conditions for 32-round Skein-256 is shown in Table 5.

There are 216 conditions in group-1, of which 174 conditions can be fulfilled by modifying the values of h_{20}. Most of conditions in group-2 can be corrected by modifying K_5 and only 18 conditions are left after message modification. The 15 conditions in a_{16}, b_{16}, d_{16} and a_{15} of group-3 can be modified by $K_{4,b}$ and $K_{4,d}$, and there are 89 conditions remaining after the message modification.

4.4 The Partial-Collision Attack on the Compression Function of 32-Round Skein-256

In our attack, we take the 256-bit value h_{20} and the 384-bit K_5, $K_{4,b}$ and $K_{4,d}$ as the random variables. As the chaining values h_{19}, h_{18}, h_{17} and $\overline{h_{16}}$ only depend on h_{20}, the search of the right h_{20} is independent of K_5 and K_4. Once h_{20} are fixed, the values of $\overline{h_{20}}$, h_{21}, h_{22}, h_{23}, h_{24} and c_{16} are only determined by K_5. Therefore, our near-collision search algorithm can be divided into three phases: the first phase is to find h_{20} that satisfies the conditions in group-1; the second phase is to find K_5 to ensure the conditions in group-2; the last phase is to find $K_{4,b}$ and $K_{4,d}$ so that the differential path in Table 4 holds.

The partial-collision search algorithm:

1. Select a 256-bit chaining value $h_{20} = (a_{20}, b_{20}, c_{20}, d_{20})$ which satisfies the 95 conditions in h_{20} in Table 9.
   - Compute the chaining value $h_{19} = (a_{19}, b_{19}, c_{19}, d_{19})$ from h_{20} and modify the 62 conditions in a_{19} and c_{19} in Table 9 by h_{20} using the message/IV modification techniques.
   - Calculate the chaining values $h_{18} = (a_{18}, b_{18}, c_{18}, d_{18})$, $h_{17} = (a_{17}, b_{17}, c_{17}, d_{17})$ and $\overline{h_{16}} = (A_{16}, B_{16}, C_{16}, D_{16})$ by h_{19} in the backward direction. Modify 17 out of the 59 conditions, and check whether the other 42 conditions hold. If so, goto step 2; otherwise, goto step 1.

Table 5. The conditions distribution for our attack of 32-round Skein-256.

Groups	Conditions	Modified conditions	Used message/IV
1	216	174	a_{20}, b_{20}, c_{20}, d_{20}
2	168	150	$K_{5,a}$, $K_{5,b}$, $K_{5,c}$, $K_{5,d}$
3	104	15	$K_{4,b}$, $K_{4,d}$

2. Choose the 256-bit subkey $K_5 = (K_{5,a}, K_{5,b}, K_{5,c}, K_{5,d})$ randomly.
   - Compute

$$\begin{aligned}\overline{h_{20}} &= h_{20} + K_5 = (A_{20}, B_{20}, C_{20}, D_{20}),\\ c_{16} &= C_{16} - K_{5,b}.\end{aligned}$$

   Modify the 53 conditions in B_{20} and D_{20} by $K_{5,b}$ and $K_{5,d}$ respectively.
   - Compute h_{21}, h_{22}, h_{23} and h_{24} by $\overline{h_{20}}$ in the forward direction. Modify the 97 conditions in h_{21}, h_{22} and h_{23} by K_5. Then check whether the other 18 conditions are satisfied. If so, goto step 3; otherwise, goto step 2.
3. Select the 128-bit value $K_{4,b}$ and $K_{4,d}$ randomly.
   - According to the key schedule,

$$\begin{aligned}&K_{5,a} = k_0, K_{5,b} = k_1 + t_2, K_{5,c} = k_2 + t_0, K_{5,d} = k_3 + 5,\\ &K_{4,a} = k_4, K_{4,b} = k_0 + t_1, K_{4,c} = k_1 + t_2, K_{4,d} = k_2 + 4,\end{aligned}$$

   where $k_4 = 0x1bd11bdaa9fc1a22 \oplus \bigoplus_{i=0}^{3} k_i$ and $t_2 = t_0 \oplus t_1$. Derive the key $K = (k_0, k_1, k_2, k_3)$ and the tweak value $T = (t_0, t_1)$:

$$\begin{aligned}k_0 &= K_{5,a},\\ k_1 &= K_{5,b} - ((K_{4,b} - K_{5,a}) \oplus (K_{5,c} - K_{4,d} + 4)),\\ k_2 &= K_{4,d} - 4,\\ k_3 &= K_{5,d} - 5,\\ t_0 &= K_{5,c} - K_{4,d} + 4,\\ t_1 &= K_{4,b} - K_{5,a}.\end{aligned}$$

   Then further deduce:

$$\begin{aligned}K_{4,a} = &\ 0x1bd11bdaa9fc1a22 \oplus K_{5,a} \oplus (K_{5,d} - 5) \oplus (K_{4,d} - 4) \oplus\\ &(K_{5,b} - ((K_{4,b} - K_{5,a}) \oplus (K_{5,c} - K_{4,d} + 4))),\\ K_{4,c} = &\ K_{5,b}.\end{aligned}$$

   - Compute $b_{16} = B_{16} - K_{4,b}$, $d_{16} = D_{16} - K_{4,d}$ and $a_{16} = A_{16} - K_{4,a}$. Modify the 15 conditions in b_{16}, d_{16} and a_{16} by $K_{4,b}$ and $K_{4,d}$ respectively.
4. Compute K_0, K_1, K_2, K_3, K_6, K_7, K_8 by K and T, calculate $\overline{h_{24}}$ to $\overline{h_{32}}$ by h_{24}, K_6, K_7 and K_8 in the forward direction, and compute h_{15} to h_0 by h_{16}, K_0, K_1, K_2 and K_3 in the backward direction.
5. Let $h'_{20} = h_{20} \oplus \Delta h_{20}$, where Δh_{20} is the difference of round 20 in Table 4. Let $K' = (k_0, k_1, k_2, k_3 + 2^{63})$ and $T' = (t_0 + 2^{63}, t_1)$, compute $h'_{19} \sim h'_0$ and $\overline{h'_{20}} \sim \overline{h'_{32}}$ by h'_{20}, K' and T'. Then check whether $h_0 \oplus h'_0 = \Delta h_0$ and $\overline{h_{32}} \oplus \overline{h'_{32}} = \Delta \overline{h_{32}}$, where Δh_0 and $\Delta \overline{h_{32}}$ are the differences in round 0 and round $\overline{32}$ of Table 4. If so, output the message pair $(M = h_0, M' = h'_0)$, the master key $K = (k_0, k_1, k_2, k_3)$ and the tweak $T = (t_0, t_1)$; otherwise, goto step 3.

Degrees of freedom analysis: We consider the degrees of freedom from the following four inspects:

Table 6. Free-start near collisions examples for Skein-256.

Near-Collision 1: a near collision with Hamming distance 2 from rounds 4 to 28	
Message of Round 4	
$M^{(1)}$	e06dae5ef2a07f47 ab4a1eb0d3ca9657 2df69dff1cf902f7 94f1d26c1640e047
$M^{(2)}$	e06dae5ef2a07f47 ab4a1eb0d3ca9657 2df69dff1cf902f7 14f1d26c1640e047
Key	
$K^{(1)}$	276233eabba1aee6 66468bf4f9186874 4c1044cb8ebdb40 71b6c3354128213a
$K^{(2)}$	276233eabba1aee6 66468bf4f9186874 4c1044cb8ebdb40 f1b6c3354128213a
Tweak	
$T^{(1)}$	000000000000000 000000000000000
$T^{(2)}$	800000000000000 000000000000000
Output: $a_4 \oplus \overline{a_{28}}$	
Output1	7d750ef8ccb0bbd0 1cc1e98ec9f9a18a eab66d1642a6c3f1 fa19cc4783700f1c
Output2	7d750ef8ccb0bbd0 9cc1e98ec9f9a18a eab66d1642a6c3f1 7a19cc4783700f1c
Near-Collision 2: a near collision with Hamming distance 34 from rounds 0 to 28	
Message of Round 0	
$M^{(1)}$	75567a6722e984c1 6aa74b49b44a4b0e 8dc87c2235fe4944 910233d1a5628f29
$M^{(2)}$	7056ea6d72c88c81; eba75b4ba46b430e 8d887822b7fa0b40 114233d12162cd2d
Key	
$K^{(1)}$	174b482acb8192de d581ea180039c605 6a83af6bc11fb1ca 73aaa3494528212f
$K^{(2)}$	174b482acb8192de d581ea180039c605 6a83af6bc11fb1ca f3aaa3494528212f
Tweak	
$T^{(1)}$	204974d2f898e9cd 0085794e10264ba2
$T^{(2)}$	a04974d2f898e9cd 0085794e10264ba2
Output: $a_0 \oplus \overline{a_{28}}$	
Output1	9ba9ee20f9e4dbfb d99ef6dbe703fd1b 567033e47cd85ebe bfa917f64a5f8926
Output2	9ea97e2aa9c5d3bb d89ee6d9f722f51b 563037e4fedc1cba 3fe917f6ce5fcb22
Near-Collision 3: a near collision with Hamming distance 28 from rounds 4 to 32	
Message of Round 4	
$M^{(1)}$	7c4d70e0bb911686 126e7d70b549e195 687401fcfdda8a32 74d4ba53d43c8f4b
$M^{(2)}$	7c4d70e0bb911686 126e7d70b549e195 687401fcfdda8a32 f4d4ba53d43c8f4b
Key	
$K^{(1)}$	174b482acb8192de f80431a5cb0dcdc8 43f0a9b602dfc4e2 73aaa3494528212f
$K^{(2)}$	174b482acb8192de f80431a5cb0dcdc8 43f0a9b602dfc4e2 f3aaa3494528212f
Tweak	
$T^{(1)}$	46dc7a88b6d8d6b5 b895bc87ab324c19
$T^{(2)}$	c6dc7a88b6d8d6b5 b895bc87ab324c19
Output: $a_4 \oplus \overline{a_{32}}$	
Output1	e5e0fd7e130df9ae cd8f77d82cf70926 abd50d673bc9fab1 feca27355d91f45d
Output2	65e0fd6e132df1ae 0c8b7fc86ef30136 29d50d777bcdf291 7fea27255db1fc5d

- The total degrees of the freedom come from the message M, the master key K and the tweak value T. For skein-256, we have $256 + 256 + 128 = 640$ degrees of freedom to mount our attack. The number of conditions in our differentials is 488 (see Tables 7 and 8). Hence the degrees of freedom are sufficient to perform our attack.
- The local degrees of the freedom from rounds 20 down to $\overline{16}$ (group-1) are 256 which come from the chaining variables $h_{20} = (a_{20}, b_{20}, c_{20}, d_{20})$. The number of the conditions in these 5 rounds is 216. It is enough to find a pair h_{20} and h'_{20} so that the differential path of this part holds.
- The conditions in $\overline{h_{20}}$, h_{21}, ... , h_{24} and c_{16} (group-2) are determined by K_5 with 256-bit freedom degrees. While the number of conditions of this part is only 168, so it's enough to search a right K_5.
- The degrees of the freedom from rounds $\overline{24}$ to 32 and rounds 16 down to 0 are 128. The number of conditions of this part is 104. Consequently, it's enough to search a partial-collision after the message modifications.

The complexity computation: The complexity of our attack includes three parts:

- The first part is to find a right 256-bit chaining value h_{20} so that it satisfies the 216 conditions of h_{20}, h_{19}, h_{18}, h_{17} and $\overline{h_{16}}$ in Table 7. After the message modifications, there are 42 conditions remaining. Hence the complexity of this part is about 2^{42} 32-round Skein-256 compression function operations.
- The second part is to find a right 256-bit value K_5 that satisfies the 168 conditions in Table 10. After message modifications, the complexity for this part is about 2^{18}.
- The third part is to find a 128-bit value $K_{4,b}$ and $K_{4,d}$ that satisfies the 104 conditions in Table 11. After message modification, the complexity for this part is about 2^{89}.

As a result, the total complexity of our attack is about $2^{42} + 2^{18} + 2^{89} \approx 2^{89}$ 32-round Skein-256 compression function operations. The complexity can be reduced further when considering the impact of additional paths.

4.5 Near-Collisions Examples for Skein-256

In order to verify our differential path in Table 4, we give an example of 24-round (4–28) near-collision without choosing the tweak. The complexity is about 2^{26}, and the Hamming distance is only 2. We also give two near-collision examples for 28-round Skein-256 in the free tweak setting. The first example is a near collision from rounds 0 to 28 with Hamming distance 34, and the second is from rounds 4 to 32 with Hamming distance 28. Even though the complexities of the attacks for the two near collisions were estimated to be about 2^{46} and 2^{43} respectively according to our differential path, we expect they will be lower in practice due to the impact of additional paths. They are confirmed by our implementations, and the practical complexities are about 2^{44} and 2^{41} for the two near collisions respectively. This also deduces the complexity of the partial-collision attack on 32-round Skein-256 by a factor of $2^{2+2} = 2^4$ resulting in an attack complexity 2^{85}. The near collisions are shown in Table 6.

4.6 Discussions about the Application to Skein-512

Our techniques can be also applied to Skein-512 and Skein-1024. Since Skein-512 is the primary proposal of Skein by the authors, we will mainly discuss how to apply our techniques to Skein-512: By selecting the differences for the master key $K = (k_0, k_1, ..., k_7)$ and the tweak value $T = (t_0, t_1)$ as $\Delta k_7 = 2^{63}$ and $\Delta t_0 = 2^{63}$, we construct the first short differential path from rounds 37 to 52 with a 8-round zero-differential (from rounds 41 to 48) and the second short differential path from rounds 57 to 68 with a 4-round zero-differential in the middle. Similar to the attack on Skein-256, connecting the two differential paths (between round 53 and round 60) is also the most difficult part of the attack. Moreover, we consider the connection to be even harder than that of Skein-256 since now 512 bits have to be connected. By leveraging the strategy of Skein-256 on Skein-512 with more carefulness, we estimate that the complexity of the attack on Skein-512 reduced to 32 rounds with Hamming distance 55 is about 2^{88} 32-round Skein-512 computations.

5 Conclusions

In this paper, we apply the rebound-type idea to the differential attack of the ARX-type hash algorithms and connect two specific short differentials into a long one. Utilizing our technique, we give three near-collision examples for 24 and 28 rounds Skein-256 compression function. The complexity of partial-collision attack on 32-round Skein-256 compression function is about 2^{85}. Our method has potential application to other ARX-type hash functions.

Appendix

Table 7. The sufficient conditions for Round 20 down to 0 of the differential path in Table 4.

20	a_{20}	$a_{20,27} = a_{20,25} \oplus 1$, $a_{20,31} = a_{20,30}$, $a_{20,33} = a_{20,31}$, $a_{20,35} = a_{20,30}$, $a_{20,37} = a_{20,30} \oplus 1$, $a_{20,51} = a_{20,50}$, $a_{20,57} = a_{20,55}$	7
	b_{20}	$b_{20,1} = a_{20,1}$, $b_{20,2} = a_{20,1} \oplus 1$, $b_{20,9} = a_{20,9} \oplus 1$, $b_{20,11} = a_{20,11} \oplus 1$, $b_{20,13} = a_{20,13} \oplus 1$, $b_{20,15} = a_{20,15}$, $b_{20,16} = a_{20,15}$, $b_{20,17} = a_{20,15}$, $b_{20,18} = a_{20,15}$, $b_{20,19} = a_{20,15}$, $b_{20,20} = a_{20,15}$, $b_{20,21} = a_{20,15} \oplus 1$, $b_{20,25} = a_{20,25} \oplus 1$, $b_{20,27} = a_{20,27}$, $b_{20,30} = a_{20,30}$, $b_{20,34} = a_{20,30} \oplus 1$, $b_{20,35} = a_{20,35} \oplus 1$, $b_{20,37} = a_{20,37} \oplus 1$, $b_{20,38} = a_{20,37} \oplus 1$	19
	c_{20}	$c_{20,2} = c_{20,1}$, $c_{20,21} = c_{20,15} \oplus 1$, $c_{20,45} = c_{20,43}$, $c_{20,63} = c_{20,60}$	4
	d_{20}	$d_{20,9} = c_{20,9}$, $d_{20,15} = c_{20,15} \oplus 1$, $d_{20,21} = c_{20,21}$, $d_{20,22} = c_{20,21} \oplus 1$, $d_{20,41} = c_{20,41}$, $d_{20,43} = c_{20,43} \oplus 1$, $d_{20,45} = c_{20,45} \oplus 1$, $d_{20,57} = c_{20,57} \oplus 1$, $d_{20,60} = c_{20,60}$, $d_{20,61} = c_{20,61}$	10
19	a_{19}	$a_{19,1} = a_{20,1}$, $a_{19,6} = b_{19,6} \oplus 1$, $a_{19,8} = a_{20,9}$, $a_{19,11} = a_{20,11}$, $a_{19,13} = a_{20,13}$, $a_{19,15} = a_{20,15}$, $a_{19,16} = a_{20,15}$, $a_{19,17} = a_{20,15} \oplus 1$, $a_{19,20} = b_{19,20} \oplus 1$, $a_{19,22} = b_{19,22} \oplus 1$, $a_{19,23} = a_{20,25} \oplus 1$, $a_{19,24} = a_{20,25}$, $a_{19,25} = a_{20,25} \oplus 1$, $a_{19,26} = a_{20,25}$, $a_{19,27} = a_{20,25}$, $a_{19,31} = a_{20,30}$, $a_{19,32} = a_{19,31} \oplus 1$, $a_{19,33} = a_{20,30} \oplus 1$, $a_{19,34} = a_{20,30}$, $a_{19,35} = a_{20,30}$, $a_{19,36} = a_{20,30}$, $a_{19,40} = b_{19,40}$, $a_{19,45} = b_{19,45} \oplus 1$, $a_{19,52} = b_{19,50}$, $a_{19,53} = a_{19,52} \oplus 1$, $a_{19,56} = a_{20,55} \oplus 1$, $a_{19,60} = a_{20,61} \oplus 1$, $a_{19,61} = a_{20,61} \oplus 1$, $a_{19,62} = a_{20,61}$, $a_{19,63} = a_{20,63} \oplus 1$	30
	b_{19}	$b_{19,8} = a_{19,9}$, $b_{19,16} = a_{20,15} \oplus 1$, $b_{19,17} = a_{20,15}$, $b_{19,22} = b_{19,20} \oplus 1$, $b_{19,23} = a_{20,25} \oplus 1$, $b_{19,28} = a_{20,25} \oplus 1$, $b_{19,30} = a_{20,30}$, $b_{19,32} = a_{20,30}$, $b_{19,36} = a_{20,30}$, $b_{19,38} = a_{20,30} \oplus 1$, $b_{19,40} = a_{20,41}$, $b_{19,46} = b_{19,45} \oplus 1$, $b_{19,50} = a_{20,50} \oplus 1$, $b_{19,55} = a_{20,55} \oplus 1$, $b_{19,58} = a_{20,55}$, $b_{19,60} = a_{20,61}$	16
	c_{19}	$c_{19,6} = d_{19,6} \oplus 1$, $c_{19,8} = a_{19,9}$, $c_{19,16} = a_{20,15} \oplus 1$, $c_{19,17} = c_{19,16}$, $c_{19,18} = c_{19,17}$, $c_{19,19} = c_{19,18}$, $c_{19,23} = d_{20,23} \oplus 1$, $c_{19,38} = d_{19,38} \oplus 1$, $c_{19,40} = d_{19,40}$, $c_{19,45} = d_{19,45} \oplus 1$, $c_{19,55} = c_{20,52} \oplus 1$, $c_{19,56} = c_{20,52}$, $c_{19,58} = c_{20,57}$, $c_{19,60} = c_{20,60} \oplus 1$	14
	d_{19}	$d_{19,1} = c_{20,1} \oplus 1$, $d_{19,3} = c_{20,1}$, $d_{19,8} = c_{20,9}$, $d_{19,15} = c_{20,15} \oplus 1$, $d_{19,20} = c_{20,15} \oplus 1$, $d_{19,26} = c_{20,26} \oplus 1$, $d_{19,27} = c_{20,26}$, $d_{19,40} = c_{20,41}$, $d_{19,43} = c_{20,43} \oplus 1$, $d_{19,44} = d_{19,43}$, $d_{19,46} = d_{19,43}$, $d_{19,47} = d_{19,46} \oplus 1$, $d_{19,52} = c_{20,52} \oplus 1$, $d_{19,53} = d_{19,52}$, $d_{19,54} = d_{19,53}$, $d_{19,57} = c_{20,57} \oplus 1$, $d_{19,61} = c_{20,61} \oplus 1$, $d_{19,62} = c_{20,61} \oplus 1$	18
18	a_{18}	$a_{18,6} = a_{19,6}$, $a_{18,26} = a_{19,26}$, $a_{18,27} = a_{19,27}$, $a_{18,44} = b_{18,44}$, $a_{18,54} = b_{18,54} \oplus 1$, $a_{18,56} = a_{19,56} \oplus 1$, $a_{18,60} = a_{19,60} \oplus 1$	7
	b_{18}	$b_{18,1} = a_{19,1} \oplus 1$, $b_{18,2} = a_{19,1}$, $b_{18,8} = a_{19,8} \oplus 1$, $b_{18,9} = a_{19,8} \oplus 1$, $b_{18,10} = a_{19,8}$, $b_{18,11} = a_{19,11} \oplus 1$, $b_{18,12} = a_{19,11}$, $b_{18,13} = a_{19,13}$, $b_{18,15} = a_{19,15} \oplus 1$, $b_{18,20} = a_{19,20} \oplus 1$, $b_{18,21} = a_{19,20} \oplus 1$, $b_{18,23} = a_{19,23}$, $b_{18,24} = a_{19,23}$, $b_{18,31} = a_{19,31} \oplus 1$, $b_{18,33} = a_{19,33}$, $b_{18,34} = b_{18,33}$, $b_{18,37} = b_{18,33} \oplus 1$, $b_{18,40} = a_{19,40} \oplus 1$, $b_{18,41} = b_{18,40} \oplus 1$, $b_{18,44} = a_{19,45}$, $b_{18,52} = a_{19,52} \oplus 1$, $b_{18,54} = a_{19,56}$, $b_{18,57} = a_{19,56} \oplus 1$, $b_{18,58} = a_{19,56}$, $b_{18,63} = a_{19,63}$	25
	c_{18}	$c_{18,8} = c_{19,8} \oplus 1$, $c_{18,9} = c_{18,8} \oplus 1$, $c_{18,10} = d_{18,10}$, $c_{18,11} = d_{18,10}$, $c_{18,12} = d_{18,10} \oplus 1$, $c_{18,20} = d_{18,16}$, $c_{18,21} = c_{18,20} \oplus 1$, $c_{18,23} = c_{19,23} \oplus 1$, $c_{18,24} = c_{19,23}$, $c_{18,38} = c_{19,38}$, $c_{18,40} = c_{19,40} \oplus 1$, $c_{18,41} = c_{18,40} \oplus 1$, $c_{18,44} = d_{18,44} \oplus 1$, $c_{18,45} = c_{19,45} \oplus 1$, $c_{18,52} = d_{18,52} \oplus 1$, $c_{18,54} = d_{18,54}$, $c_{18,58} = c_{19,58}$	17
	d_{18}	$d_{18,6} = c_{19,6}$, $d_{18,10} = c_{19,8}$, $d_{18,16} = c_{19,16} \oplus 1$, $d_{18,42} = c_{19,40} \oplus 1$, $d_{18,43} = d_{18,42} \oplus 1$, $d_{18,46} = c_{19,45}$, $d_{19,54} = c_{19,55}$, $d_{18,56} = c_{19,56}$, $d_{18,60} = c_{19,60}$	9
17	a_{17}	$a_{17,6} = a_{18,6}$, $a_{17,22} = b_{17,22} \oplus 1$, $a_{17,26} = a_{18,26} \oplus 1$, $a_{17,38} = b_{17,38}$, $a_{17,44} = a_{18,44} \oplus 1$, $a_{17,45} = a_{18,44}$, $a_{17,58} = a_{18,60}$, $a_{18,59} = a_{18,60}$	8
	b_{17}	$b_{17,28} = a_{18,26}$, $b_{17,39} = b_{17,38} \oplus 1$, $b_{17,54} = a_{18,54}$, $b_{17,55} = a_{18,55}$, $b_{17,58} = a_{18,60}$	5
	c_{17}	$c_{17,6} = d_{17,6} \oplus 1$, $c_{17,22} = d_{17,22}$, $c_{17,54} = c_{18,54} \oplus 1$, $c_{17,55} = c_{18,55}$, $c_{17,58} = c_{18,58} \oplus 1$	5
	d_{17}	$d_{17,8} = c_{18,8}$, $d_{17,9} = d_{17,8}$, $d_{17,20} = c_{18,20} \oplus 1$, $d_{17,22} = c_{18,23} \oplus 1$, $d_{17,38} = c_{18,38} \oplus 1$, $d_{17,40} = c_{18,40}$, $d_{17,41} = c_{18,41}$, $d_{17,44} = c_{18,44}$, $d_{17,45} = c_{18,45}$, $d_{17,52} = c_{18,52}$	10
$\overline{16}$	B_{16}	$B_{16,6} = a_{17,6}$, $B_{16,26} = a_{17,26} \oplus 1$, $B_{16,27} = B_{16,26} \oplus 1$, $B_{16,38} = a_{17,38}$, $B_{16,44} = a_{17,44}$, $B_{16,45} = a_{17,45}$, $B_{16,58} = a_{17,58}$, $B_{16,59} = a_{17,59} \oplus 1$	8
	D_{16}	$D_{16,22} = c_{17,22} \oplus 1$, $D_{16,23} = D_{16,22} \oplus 1$, $D_{16,54} = c_{17,54} \oplus 1$	3
16	a_{16}	$a_{16,12} = B_{16,12} \oplus 1$, $a_{16,22} = a_{17,22}$	2
	b_{16}	$b_{16,6} = B_{16,6} \oplus 1$, $b_{16,12} = B_{16,12}$, $b_{16,26} = B_{16,26} \oplus 1$, $b_{16,38} = B_{16,38}$, $b_{16,44} = B_{16,44} \oplus 1$, $b_{16,58} = B_{16,58}$, $b_{16,59} = B_{16,59}$	7
	c_{16}	$c_{16,6} = c_{17,6}$, $c_{16,12} = D_{16,12} \oplus 1$, $c_{16,58} = c_{17,58} \oplus 1$, $c_{16,59} = c_{17,59}$	4
	d_{16}	$d_{16,12} = D_{16,12}$, $d_{16,22} = D_{16,22} \oplus 1$, $d_{16,54} = D_{16,54}$	3
15	a_{15}	$a_{15,12} = a_{16,12}$	1
	b_{15}	$b_{15,22} = a_{16,22}$	1
	d_{15}	$d_{15,6} = c_{16,6}$, $d_{15,12} = c_{16,12}$, $d_{15,58} = c_{16,58} \oplus 1$	3
14	b_{14}	$b_{14,12} = a_{15,12}$	1
3	a_3	$a_{3,59} = b_{3,59} \oplus 1$	1
2	a_2	$a_{2,59} = a_{3,59}$, $a_{2,36} = b_{2,36} \oplus 1$	2
	c_2	$c_{2,19} = d_{2,19} \oplus 1$	1
1	a_1	$a_{1,7} = b_{1,7} \oplus 1$, $a_{1,31} = b_{1,31} \oplus 1$, $a_{1,36} = a_{2,36}$, $a_{1,48} = b_{1,48} \oplus 1$, $a_{1,59} = a_{2,59}$	5
	c_1	$c_{1,19} = c_{2,19}$, $c_{1,26} = d_{1,26} \oplus 1$, $c_{1,43} = d_{1,43} \oplus 1$	3
0	a_0	$a_{0,7} = a_{1,7}$, $a_{0,12} = B_{0,12} \oplus 1$, $a_{0,17} = B_{0,17} \oplus 1$, $a_{0,22} = B_{0,22} \oplus 1$, $a_{0,29} = B_{0,29} \oplus 1$, $a_{0,31} = a_{1,31}$, $a_{0,34} = B_{0,34} \oplus 1$, $a_{0,36} = a_{1,36}$, $a_{0,45} = B_{0,45} \oplus 1$, $a_{0,48} = a_{1,48}$, $a_{0,57} = B_{0,57} \oplus 1$, $a_{0,59} = a_{1,59}$	12
	b_0	$b_{0,12} = B_{0,12}$, $b_{0,17} = B_{0,17}$, $b_{0,22} = B_{0,22}$, $b_{0,45} = B_{0,45}$, $b_{0,29} = B_{0,29}$, $b_{0,34} = B_{0,34}$, $b_{0,57} = B_{0,57}$	7
	c_0	$c_{0,3} = D_{0,3} \oplus 1$, $c_{0,10} = D_{0,10} \oplus 1$, $c_{0,15} = D_{0,15} \oplus 1$, $c_{0,19} = c_{1,19}$, $c_{0,26} = c_{1,26} \oplus 1$, $D_{0,27} = c_{1,26} \oplus 1$, $c_{0,32} = D_{0,32} \oplus 1$, $c_{0,43} = c_{1,43}$, $c_{0,55} = c_{1,55}$	9
	d_0	$d_{0,3} = D_{0,3}$, $d_{0,10} = D_{0,10}$, $d_{0,15} = D_{0,15}$, $d_{0,27} = D_{0,27}$, $d_{0,32} = D_{0,32}$, $d_{0,55} = D_{0,55}$	6

Table 8. The sufficient conditions for Round $\overline{20} \sim 32$ of the differential path in Table 4.

$\overline{20}$	B_{20}	$B_{20,1} = b_{20,1}$, $B_{20,2} = b_{20,2}$, $B_{20,9} = b_{20,9} \oplus 1$, $B_{20,10} = b_{20,9}$, $B_{20,11} = b_{20,11}$, $B_{20,13} = b_{20,13} \oplus 1$, $B_{20,14} = b_{20,13}$, $B_{20,15} = b_{20,15}$, $B_{20,16} = b_{20,15} \oplus 1$, $B_{20,25} = b_{20,25} \oplus 1$, $B_{20,26} = b_{20,25}$, $B_{20,27} = b_{20,27}$, $B_{20,30} = b_{20,30} \oplus 1$, $B_{20,31} = b_{20,30} \oplus 1$, $B_{20,32} = b_{20,30} \oplus 1$, $B_{20,33} = b_{20,30}$, $B_{20,34} = b_{20,34}$, $B_{20,35} = b_{20,35} \oplus 1$, $B_{20,36} = b_{20,35}$, $B_{20,37} = b_{20,37} \oplus 1$, $B_{20,39} = b_{20,37}$, $B_{20,40} = b_{20,40}$, $B_{20,41} = b_{20,41}$	23
	D_{20}	$D_{20,9} = d_{20,9} \oplus 1$, $D_{20,10} = d_{20,9} \oplus 1$, $D_{20,11} = d_{20,9} \oplus 1$, $D_{20,12} = d_{20,9} \oplus 1$, $D_{20,13} = d_{20,9} \oplus 1$, $D_{20,14} = d_{20,9}$, $D_{20,15} = d_{20,15} \oplus 1$, $D_{20,16} = d_{20,15} \oplus 1$, $D_{20,17} = d_{20,15} \oplus 1$, $D_{20,18} = d_{20,15}$, $D_{20,21} = d_{20,21}$, $D_{20,22} = d_{20,22} \oplus 1$, $D_{20,23} = d_{20,22} \oplus 1$, $D_{20,24} = d_{20,22} \oplus 1$, $D_{20,25} = d_{20,22} \oplus 1$, $D_{20,26} = d_{20,22}$, $D_{20,28} = d_{20,28}$, $D_{20,30} = d_{20,30}$, $D_{20,31} = d_{20,31} \oplus 1$, $D_{20,32} = d_{20,31} \oplus 1$, $D_{20,33} = d_{20,31}$, $D_{20,41} = d_{20,41} \oplus 1$, $D_{20,42} = d_{20,41}$, $D_{20,43} = d_{20,43} \oplus 1$, $D_{20,44} = d_{20,43}$, $D_{20,45} = d_{20,45}$, $D_{20,57} = d_{20,57}$, $D_{20,60} = d_{20,60}$, $D_{20,61} = d_{20,61} \oplus 1$, $D_{20,62} = d_{20,61}$	30
21	a_{21}	$a_{21,28} = b_{20,27} \oplus 1$, $a_{21,29} = a_{21,28}$, $a_{21,30} = a_{21,28}$, $a_{21,31} = a_{21,28} \oplus 1$, $a_{21,32} = a_{20,30}$, $a_{21,33} = a_{21,32}$, $a_{21,34} = a_{21,32}$, $a_{21,35} = a_{21,32}$, $a_{21,36} = a_{21,32} \oplus 1$, $a_{21,38} = b_{20,38} \oplus 1$, $a_{21,39} = b_{20,38}$, $a_{21,40} = b_{20,40}$, $a_{21,41} = b_{20,41}$, $a_{21,50} = a_{20,50}$, $a_{21,51} = a_{20,51}$, $a_{21,55} = a_{20,55} \oplus 1$, $a_{21,56} = a_{20,55}$, $a_{21,57} = a_{20,57} \oplus 1$, $a_{21,58} = a_{20,57} \oplus 1$, $a_{21,59} = a_{20,57} \oplus 1$, $a_{21,60} = a_{20,57}$, $a_{21,61} = a_{20,61}$, $a_{21,63} = a_{20,63}$	23
	b_{21}	$b_{21,28} = a_{21,28}$, $b_{21,50} = a_{21,50} \oplus 1$, $b_{21,51} = a_{21,51}$, $b_{21,52} = a_{21,51}$, $b_{21,53} = a_{21,51}$, $b_{21,54} = a_{21,51} \oplus 1$, $b_{21,55} = a_{21,55} \oplus 1$, $b_{21,56} = a_{21,55}$, $b_{21,57} = a_{21,57} \oplus 1$, $b_{21,58} = a_{21,58} \oplus 1$, $b_{21,59} = a_{21,59}$, $b_{21,61} = a_{21,61}$, $b_{21,62} = a_{21,62} \oplus 1$, $b_{21,63} = a_{21,63} \oplus 1$	14
	c_{21}	$c_{21,1} = c_{20,1}$, $c_{21,2} = c_{20,2}$, $c_{21,10} = c_{20,9} \oplus 1$, $c_{21,11} = c_{20,9} \oplus 1$, $c_{21,12} = c_{20,9} \oplus 1$, $c_{21,13} = c_{20,9} \oplus 1$, $c_{21,14} = c_{20,9}$, $c_{21,26} = c_{20,26}$, $c_{21,28} = D_{20,28} \oplus 1$, $c_{21,29} = D_{20,28}$, $c_{21,30} = d_{20,30}$, $c_{21,31} = d_{20,31} \oplus 1$, $c_{21,42} = c_{20,41} \oplus 1$, $c_{21,43} = c_{21,42}$, $c_{21,44} = c_{21,42}$, $c_{21,45} = c_{21,42}$, $c_{21,46} = c_{21,42}$, $c_{21,47} = c_{21,42}$, $c_{21,48} = c_{21,42}$, $c_{21,49} = c_{21,42} \oplus 1$, $c_{21,52} = c_{20,52} \oplus 1$, $c_{21,53} = c_{20,52}$, $c_{21,62} = c_{20,60} \oplus 1$	23
	d_{21}	$d_{21,1} = c_{21,1} \oplus 1$, $d_{21,2} = c_{21,2} \oplus 1$, $d_{21,26} = c_{21,26}$, $d_{21,27} = c_{21,26} \oplus 1$, $d_{21,28} = c_{21,28} \oplus 1$, $d_{21,29} = c_{21,29} \oplus 1$, $d_{21,30} = c_{21,30} \oplus 1$, $d_{21,31} = c_{21,31}$, $d_{21,32} = c_{21,31} \oplus 1$, $d_{21,33} = c_{21,31}$, $d_{21,52} = c_{21,52}$, $d_{21,62} = c_{21,62}$, $d_{21,63} = c_{21,62} \oplus 1$	13
22	a_{22}	$a_{22,32} = a_{21,32}$, $a_{22,33} = a_{22,32}$, $a_{22,34} = a_{22,32}$, $a_{22,35} = a_{22,32}$, $a_{22,36} = a_{22,32}$, $a_{22,37} = a_{22,32} \oplus 1$, $a_{22,38} = a_{21,38}$, $a_{22,39} = a_{21,39}$, $a_{22,40} = a_{21,40}$, $a_{22,41} = a_{21,41} \oplus 1$, $a_{22,42} = a_{22,41}$, $a_{22,43} = a_{22,41}$, $a_{22,44} = a_{22,41}$, $a_{22,45} = a_{22,41}$, $a_{22,46} = a_{22,41} \oplus 1$	15
	b_{22}	$b_{22,38} = a_{22,38} \oplus 1$, $b_{22,39} = a_{22,39} \oplus 1$, $b_{22,40} = a_{22,40} \oplus 1$, $b_{22,41} = a_{22,41}$	4
	c_{22}	$c_{22,10} = c_{21,10}$, $c_{22,11} = c_{21,11}$, $c_{22,12} = c_{21,12}$, $c_{22,13} = c_{21,13}$, $c_{22,14} = c_{21,14}$, $c_{22,42} = c_{21,42}$, $c_{22,43} = c_{21,43}$, $c_{22,44} = c_{21,44}$, $c_{22,45} = c_{21,45} \oplus 1$	9
	d_{22}	$d_{22,10} = c_{22,10}$, $d_{22,42} = c_{22,42}$	2
23	a_{23}	$a_{23,32} = a_{22,32}$, $a_{23,33} = a_{22,33}$, $a_{23,34} = a_{22,34}$, $a_{23,35} = a_{22,35} \oplus 1$	4
	b_{23}	$b_{23,32} = a_{23,32}$	1
30	c_{30}	$c_{30,25} = d_{29,25}$	1
31	a_{31}	$a_{31,12} = b_{30,12}$, $a_{31,25} = b_{30,25}$, $a_{31,37} = b_{30,37}$	3
	b_{31}	$b_{31,25} = a_{31,25} \oplus 1$	1
	c_{31}	$c_{31,25} = c_{30,25}$	1
	d_{31}	$d_{31,25} = c_{31,25} \oplus 1$	1
32	a_{32}	$a_{32,12} = a_{31,12}$, $a_{32,22} = b_{31,22}$, $a_{32,37} = a_{31,37}$	3
	b_{32}	$b_{32,6} = b_{32,5} \oplus 1$, $b_{32,38} = b_{32,37} \oplus 1$, $b_{32,58} = b_{32,57} \oplus 1$	3
	c_{32}	$c_{32,6} = d_{31,6}$, $c_{32,12} = d_{31,12}$, $c_{32,19} = d_{31,19}$, $c_{32,31} = d_{31,31}$, $c_{32,37} = d_{31,37}$, $c_{32,58} = d_{31,58}$	6
$\overline{32}$	A_{32}	$A_{32,12} = a_{32,12}$, $A_{32,22} = a_{32,22}$, $A_{32,37} = a_{32,37}$	3
	B_{32}	$B_{32,5} = b_{32,5} \oplus 1$, $B_{32,12} = b_{32,12}$, $B_{32,19} = b_{32,19}$, $B_{32,26} = b_{32,26}$, $B_{32,31} = b_{32,31}$, $B_{32,37} = b_{32,37} \oplus 1$, $B_{32,44} = b_{32,44}$, $B_{32,51} = b_{32,51}$, $B_{32,57} = b_{32,57} \oplus 1$, $B_{32,63} = b_{32,63} \oplus 1$	10
	C_{32}	$C_{32,6} = c_{32,6}$, $C_{32,12} = c_{32,12}$, $C_{32,19} = c_{32,19}$, $C_{32,31} = c_{32,31}$, $C_{32,37} = c_{32,37}$, $C_{32,58} = c_{32,58}$	6
	D_{32}	$D_{32,12} = d_{32,12}$, $D_{32,22} = d_{32,22}$, $D_{32,37} = d_{32,37}$, $D_{32,54} = d_{32,54}$, $D_{32,57} = d_{32,57}$	5

Table 9. The conditions in group-1.

20	a_{20}	$a_{20,22} = a_{20,21}$, $a_{20,27} = a_{20,25} \oplus 1$, $a_{20,31} = a_{20,30}$, $a_{20,33} = a_{20,30}$, $a_{20,35} = a_{20,30}$, $a_{20,37} = a_{20,30} \oplus 1$, $a_{20,45} = a_{20,30} \oplus a_{20,43} \oplus a_{20,41} \oplus 1$, $a_{20,51} = a_{20,50}$, $a_{20,55} = a_{20,30} \oplus a_{20,43} \oplus 1$, $a_{20,57} = a_{20,55}$	10
	b_{20}	$b_{20,1} = a_{20,1}$, $b_{20,2} = a_{20,1} \oplus 1$, $b_{20,9} = a_{20,9} \oplus 1$, $b_{20,11} = a_{20,11} \oplus 1$, $b_{20,13} = a_{20,13} \oplus 1$, $b_{20,15} = a_{20,15}$, $b_{20,16} = a_{20,15}$, $b_{20,17} = a_{20,15}$, $b_{20,18} = a_{20,15}$, $b_{20,19} = a_{20,15}$, $b_{20,20} = a_{20,15}$, $b_{20,21} = a_{20,15} \oplus 1$, $b_{20,25} = a_{20,25} \oplus 1$, $b_{20,27} = a_{20,27}$, $b_{20,30} = a_{20,30}$, $b_{20,34} = a_{20,30} \oplus 1$, $b_{20,35} = a_{20,35} \oplus 1$, $b_{20,37} = a_{20,37} \oplus 1$, $b_{20,45} = b_{20,9} \oplus a_{20,43} \oplus a_{20,13}$, $b_{20,52} = a_{20,61} \oplus a_{20,60} \oplus a_{20,55}$ $b_{20,63} = b_{20,52} \oplus a_{20,21} \oplus a_{20,15} \oplus a_{20,60} \oplus a_{20,55} \oplus b_{20,26}$	21
	c_{20}	$c_{20,2} = c_{20,1}$, $c_{20,4} = a_{20,30} \oplus b_{20,4} \oplus a_{20,9} \oplus 1$, $c_{20,5} = a_{20,30} \oplus b_{20,5} \oplus a_{20,9}$, $c_{20,6} = a_{20,30} \oplus b_{20,6} \oplus a_{20,9} \oplus 1$, $c_{20,7} = a_{20,30} \oplus b_{20,7} \oplus a_{20,11} \oplus 1$, $c_{20,8} = a_{20,11} \oplus a_{20,30} \oplus b_{20,8}$, $c_{20,9} = a_{20,30} \oplus a_{20,43} \oplus b_{20,45}$, $c_{20,13} = a_{20,41} \oplus b_{20,13} \oplus a_{20,30}$, $c_{20,15} = a_{20,21} \oplus a_{20,15}$, $c_{20,16} = a_{20,30} \oplus a_{20,43} \oplus b_{20,16} \oplus 1$, $c_{20,17} = c_{20,16} \oplus b_{20,16} \oplus b_{20,17}$, $c_{20,18} = a_{20,61} \oplus a_{20,60} \oplus a_{20,55} \oplus b_{20,11} \oplus c_{20,11} \oplus b_{20,18}$, $c_{20,19} = c_{20,16} \oplus b_{20,16} \oplus b_{20,19}$, $c_{20,20} = b_{20,20} \oplus c_{20,16} \oplus b_{20,16} \oplus 1$, $c_{20,21} = c_{20,15} \oplus 1$, $c_{20,25} = b_{20,52} \oplus c_{20,15} \oplus b_{20,25}$, $c_{20,26} = a_{20,60} \oplus a_{20,55} \oplus b_{20,63}$, $c_{20,27} = b_{20,27} \oplus b_{20,25} \oplus c_{20,25}$, $c_{20,28} = b_{20,28} \oplus b_{20,25} \oplus c_{20,25}$, $c_{20,29} = a_{20,30} \oplus a_{20,55} \oplus b_{20,29}$, $c_{20,30} = b_{20,57} \oplus c_{20,15} \oplus b_{20,30}$, $c_{20,33} = a_{20,61} \oplus b_{20,33} \oplus a_{20,30} \oplus 1$, $c_{20,34} = a_{20,60} \oplus a_{20,55} \oplus b_{20,34}$, $c_{20,35} = b_{20,35} \oplus a_{20,60} \oplus a_{20,55}$, $c_{20,36} = a_{20,30} \oplus a_{20,43} \oplus a_{20,63} \oplus b_{20,36} \oplus a_{20,45}$, $c_{20,38} = b_{20,38} \oplus c_{20,1} \oplus 1$, $c_{20,40} = b_{20,40} \oplus c_{20,1}$, $c_{20,41} = c_{20,13} \oplus b_{20,13}$, $c_{20,43} = a_{20,30} \oplus a_{20,43}$, $c_{20,45} = c_{20,43}$, $c_{20,48} = a_{20,11} \oplus b_{20,48} \oplus a_{20,50}$, $c_{20,50} = a_{20,13} \oplus b_{20,50} \oplus a_{20,55}$, $c_{20,52} = b_{20,52} \oplus c_{20,15} \oplus 1$, $c_{20,53} = a_{20,15} \oplus b_{20,53} \oplus a_{20,55}$, $c_{20,54} = a_{20,15} \oplus b_{20,54} \oplus a_{20,55}$, $c_{20,57} = b_{20,57} \oplus c_{20,15} \oplus 1$, $c_{20,60} = a_{20,60} \oplus a_{20,55} \oplus 1$, $c_{20,61} = a_{20,25} \oplus b_{20,61} \oplus a_{20,1} \oplus 1$, $c_{20,62} = a_{20,25} \oplus b_{20,62} \oplus a_{20,1} \oplus 1$, $c_{20,63} = c_{20,60}$, $c_{20,64} = c_{20,26} \oplus b_{20,64}$	41
	d_{20}	$d_{20,1} = a_{20,1} \oplus a_{20,61}$, $d_{20,9} = c_{20,9}$, $d_{20,13} = a_{20,9} \oplus a_{20,13}$, $d_{20,15} = c_{20,15} \oplus 1$, $d_{20,21} = c_{20,21}$, $d_{20,22} = c_{20,21} \oplus 1$, $d_{20,23} = a_{20,23} \oplus c_{20,15} \oplus b_{20,13} \oplus c_{20,13}$, $d_{20,24} = a_{20,24} \oplus c_{20,15} \oplus c_{20,41} \oplus 1$, $d_{20,25} = a_{20,25} \oplus c_{20,59} \oplus b_{20,59} \oplus a_{20,63} \oplus 1$, $d_{20,27} = a_{20,27} \oplus a_{20,25} \oplus d_{20,25} \oplus 1$, $d_{20,28} = a_{20,25} \oplus a_{20,28} \oplus 1$, $d_{20,33} = a_{20,25} \oplus a_{20,33} \oplus 1$, $d_{20,35} = a_{20,30} \oplus a_{20,35}$, $d_{20,37} = a_{20,30} \oplus a_{20,37}$, $d_{20,41} = c_{20,41}$, $d_{20,43} = c_{20,43} \oplus 1$, $d_{20,45} = c^{1}_{20,45}$, $d_{20,51} = a_{20,50} \oplus a_{20,51} \oplus d_{20,50} \oplus 1$, $d_{20,55} = a_{20,50} \oplus a_{20,55} \oplus 1$, $d_{20,57} = c_{20,57} \oplus 1$, $d_{20,60} = c_{20,60}$, $d_{20,61} = c_{20,60}$, $d_{20,63} = a_{20,63} \oplus a_{20,55}$	23
19	a_{19}	$a_{19,1} = a_{20,1}$, $a_{19,3} = b_{20,40} \oplus c_{20,40} \oplus a_{20,50} \oplus d_{20,50}$, $a_{19,4} = a_{20,61} \oplus a_{20,11} \oplus b_{20,48} \oplus c_{20,48} \oplus b_{20,41} \oplus c_{20,41} \oplus b_{20,18} \oplus c_{20,18} \oplus a_{20,50} \oplus d_{20,50}$, $a_{19,6} = b_{19,6} \oplus 1$, $a_{19,8} = b_{19,8}$, $a_{19,11} = a_{20,11}$, $a_{19,13} = a_{20,13}$, $a_{19,15} = a_{20,15}$, $a_{19,16} = a_{20,15}$, $a_{19,17} = a_{20,15} \oplus 1$, $a_{19,20} = b_{19,20} \oplus 1$, $a_{19,22} = b_{19,22} \oplus 1$, $a_{19,23} = b_{19,23} = a_{20,25} \oplus 1$, $a_{19,24} = a_{20,25}$, $a_{19,25} = a_{20,25} \oplus 1$, $a_{19,26} = a_{20,25}$, $a_{19,27} = a_{20,25}$, $a_{19,28} = a_{19,4} \oplus d_{19,4} \oplus d_{19,45} \oplus d_{19,28} \oplus 1$ $a_{19,31} = a_{20,30}$, $a_{19,32} = a_{20,30} \oplus 1$, $a_{19,33} = a_{20,30} \oplus 1$, $a_{19,34} = a_{20,30}$, $a_{19,35} = a_{20,30}$, $a_{19,36} = a_{20,30}$, $a_{19,38} = b_{20,11} \oplus c_{20,11} \oplus a_{20,15} \oplus 1$, $a_{19,40} = b_{19,40} \oplus 1$, $a_{19,43} = b_{20,16} \oplus c_{20,16} \oplus a_{19,20} \oplus 1$, $a_{19,44} = b_{20,17} \oplus c_{20,17} \oplus a_{19,20} \oplus 1$, $a_{19,45} = b_{19,45}$, $a_{19,46} = b_{20,19} \oplus c_{20,19} \oplus a_{20,25} \oplus 1$, $a_{19,47} = b_{20,20} \oplus c_{20,20} \oplus a_{20,25} \oplus 1$, $a_{19,52} = a_{20,50} \oplus 1$, $a_{19,53} = a_{19,52} \oplus 1$, $a_{19,54} = b_{20,27} \oplus c_{20,27} \oplus a_{19,31} \oplus 1$, $a_{19,56} = a_{20,55} \oplus 1$, $a_{19,57} = b_{20,30} \oplus c_{20,30} \oplus a_{19,33}$, $a_{19,60} = a_{20,61} \oplus 1$, $a_{19,61} = a_{20,61} \oplus 1$ $a_{19,62} = a_{20,61}$, $a_{19,63} = a_{20,63} \oplus 1$, $a_{19,64} = b_{20,37} \oplus c_{20,37} \oplus a_{19,40}$	41
	c_{19}	$c_{19,3} = b_{19,3} \oplus b_{19,2} \oplus c_{19,2} \oplus 1$, $c_{19,6} = d_{19,6} \oplus 1$, $c_{19,8} = c_{20,9}$, $c_{19,18} = c_{20,15} \oplus 1$, $c_{19,19} = c_{20,15} \oplus 1$, $c_{19,22} = a_{20,27} \oplus d_{20,27} \oplus b_{20,18} \oplus c_{20,18} \oplus 1$, $c_{19,23} = d_{20,23} \oplus 1$, $c_{19,28} = a_{19,4} \oplus b_{20,41} \oplus c_{20,41} \oplus b_{20,18} \oplus c_{20,18} \oplus a_{20,33} \oplus d_{20,33} \oplus 1$, $c_{19,30} = a_{20,35} \oplus d_{20,35} \oplus c_{20,52} \oplus 1$, $c_{19,32} = a_{20,37} \oplus d_{20,37} \oplus c_{20,52}$, $c_{19,36} = a_{20,41} \oplus d_{20,41} \oplus c_{20,60} \oplus 1$, $c_{19,38} = d_{19,38} \oplus 1$, $c_{19,40} = c_{20,41}$, $c_{19,45} = d_{19,45} \oplus 1$, $c_{19,46} = a_{20,51} \oplus d_{20,51} \oplus c_{19,6}$, $c_{19,50} = c_{19,8} \oplus a_{20,55} \oplus d_{20,55}$, $c_{19,55} = c_{20,52} \oplus 1$, $c_{19,56} = c_{20,52}$, $c_{19,58} = c_{20,57}$, $c_{19,59} = c_{20,57}$, $c_{19,60} = c_{20,60} \oplus 1$	21
18	a_{18}	$a_{18,6} = a_{19,6}$, $a_{18,26} = a_{19,26}$, $a_{18,27} = a_{19,27}$, $a_{18,44} = b_{18,44}$, $a_{18,54} = b_{18,54} \oplus 1$, $a_{18,56} = a_{19,56} \oplus 1$, $a_{18,60} = a_{19,60} \oplus 1$, $a_{18,16} = a_{20,61} \oplus d_{20,61} \oplus c_{20,52} \oplus a_{20,25}$, $a_{18,42} = a_{20,23} \oplus d_{20,23} \oplus c_{20,15} \oplus a_{20,55} \oplus 1$, $a_{18,43} = a_{20,24} \oplus d_{20,24} \oplus c_{20,15} \oplus a_{20,55} \oplus 1$, $a_{18,46} = b_{20,18} \oplus c_{20,18} \oplus a_{20,61} \oplus 1$, $a_{18,58} = d_{18,58} \oplus d_{17,6} \oplus c_{18,54}$	12
	c_{18}	$c_{18,1} = a_{20,25} \oplus b_{20,61} \oplus c_{20,61} \oplus c_{20,9} \oplus 1$, $c_{18,2} = a_{19,25} \oplus b_{20,62} \oplus c_{20,62} \oplus c_{20,9} \oplus 1$, $c_{18,8} = c_{19,8} \oplus 1$, $c_{18,9} = c_{18,8} \oplus 1$, $c_{18,10} = d_{18,10}$, $c_{18,11} = d_{18,10}$, $c_{18,12} = d_{18,10} \oplus 1$, $c_{18,13} = a_{20,30} \oplus b_{20,9} \oplus c_{20,9} \oplus c_{20,15} \oplus 1$, $c_{18,15} = a_{20,15} \oplus b_{20,60} \oplus c_{20,60}$, $c_{18,20} = d_{18,16}$, $c_{18,21} = c_{18,20} \oplus 1$, $c_{18,23} = c_{19,23} \oplus 1$, $c_{18,24} = c_{19,23}$, $c_{18,31} = b_{20,11} \oplus c_{20,11} \oplus a_{20,30}$, $c_{18,33} = a_{20,55} \oplus b_{20,29} \oplus c_{20,29} \oplus c_{20,41}$, $c_{18,34} = a_{19,57} \oplus b_{20,30} \oplus c_{20,30} \oplus c_{20,41} \oplus 1$, $c_{18,37} = a_{20,61} \oplus b_{20,33} \oplus c_{20,33} \oplus a_{20,25} \oplus d_{20,25} \oplus c_{19,20}$, $c_{18,38} = c_{19,38}$, $c_{18,40} = c_{19,40} \oplus 1$, $c_{18,41} = c_{18,40} \oplus 1$, $c_{18,44} = d_{18,44} \oplus 1$, $c_{18,45} = c_{19,45} \oplus 1$, $c_{18,51} = a_{18,60} \oplus b_{18,51} \oplus a_{18,44} \oplus 1$, $c_{18,52} = d_{18,52} \oplus 1$, $c_{18,54} = d_{18,54}$, $c_{18,58} = c_{19,58}$	26
17	a_{17}	$a_{17,6} = a_{18,6}$, $a_{17,8} = d_{17,8} \oplus a_{18,60}$, $a_{17,9} = d_{17,9} \oplus a_{18,60}$ $a_{17,20} = a_{17,6} \oplus d_{17,20}$, $a_{17,22} = b_{17,22} \oplus 1$, $a_{17,26} = a_{18,26} \oplus 1$, $a_{17,38} = b_{17,38}$, $a_{17,40} = d_{17,40} \oplus a_{17,26} \oplus 1$, $a_{17,41} = d_{17,41} \oplus a_{17,26}$, $a_{17,44} = a_{18,44} \oplus 1$, $a_{17,45} = a_{18,44}$, $a_{17,52} = d_{17,52} \oplus a_{18,37}$, $a_{17,58} = a_{18,60}$, $a_{17,59} = a_{18,60}$	14
	c_{17}	$c_{17,6} = d_{17,6} \oplus 1$, $c_{17,22} = d_{17,22}$, $c_{17,38} = b_{17,38} \oplus c_{17,22} \oplus 1$ $c_{17,39} = b_{17,39} \oplus c_{17,22}$ $c_{17,54} = c_{18,54} \oplus 1$, $c_{17,55} = c_{18,55}$, $c_{17,58} = c_{18,58} \oplus 1$	7

Table 10. The conditions in group-2.

$\overline{20}$	B_{20}	$B_{20,1} = b_{20,1}$, $B_{20,2} = b_{20,2}$, $B_{20,9} = b_{20,9} \oplus 1$, $B_{20,10} = b_{20,9}$, $B_{20,11} = b_{20,11}$, $B_{20,13} = b_{20,13} \oplus 1$, $B_{20,14} = b_{20,13}$, $B_{20,15} = b_{20,15}$, $B_{20,16} = b_{20,15} \oplus 1$, $B_{20,25} = b_{20,25} \oplus 1$, $B_{20,26} = b_{20,25}$, $B_{20,27} = b_{20,27}$, $B_{20,30} = b_{20,30} \oplus 1$, $B_{20,31} = b_{20,30} \oplus 1$, $B_{20,32} = b_{20,30} \oplus 1$, $B_{20,33} = b_{20,30}$, $B_{20,34} = b_{20,34}$, $B_{20,35} = b_{20,35} \oplus 1$, $B_{20,36} = b_{20,35}$, $B_{20,37} = b_{20,37} \oplus 1$, $B_{20,39} = b_{20,37}$, $B_{20,40} = b_{20,40}$, $B_{20,41} = b_{20,41}$	23
	D_{20}	$D_{20,9} = d_{20,9} \oplus 1$, $D_{20,10} = d_{20,9} \oplus 1$, $D_{20,11} = d_{20,9} \oplus 1$, $D_{20,12} = d_{20,9} \oplus 1$, $D_{20,13} = d_{20,9} \oplus 1$, $D_{20,14} = d_{20,9}$, $D_{20,15} = d_{20,15} \oplus 1$, $D_{20,16} = d_{20,15} \oplus 1$, $D_{20,17} = d_{20,15} \oplus 1$, $D_{20,18} = d_{20,15}$, $D_{20,21} = d_{20,21}$, $D_{20,22} = d_{20,22} \oplus 1$, $D_{20,23} = d_{20,22} \oplus 1$, $D_{20,24} = d_{20,22} \oplus 1$, $D_{20,25} = d_{20,22} \oplus 1$, $D_{20,26} = d_{20,22}$, $D_{20,28} = d_{20,28}$, $D_{20,30} = d_{20,30}$, $D_{20,31} = d_{20,31} \oplus 1$, $D_{20,32} = d_{20,31} \oplus 1$, $D_{20,33} = d_{20,31}$, $D_{20,41} = d_{20,41} \oplus 1$, $D_{20,42} = d_{20,41}$, $D_{20,43} = d_{20,43} \oplus 1$, $D_{20,44} = d_{20,43}$, $D_{20,45} = d_{20,45}$, $D_{20,57} = d_{20,57}$, $D_{20,60} = d_{20,60}$, $D_{20,61} = d_{20,61} \oplus 1$, $D_{20,62} = d_{20,61}$	30
21	a_{21}	$a_{21,28} = b_{20,27} \oplus 1$, $a_{21,29} = a_{21,28}$, $a_{21,30} = a_{21,28}$, $a_{21,31} = a_{21,28} \oplus 1$, $a_{21,32} = a_{20,30}$, $a_{21,33} = a_{21,32}$, $a_{21,34} = a_{21,32}$, $a_{21,35} = a_{21,32}$, $a_{21,36} = a_{21,32} \oplus 1$, $a_{21,38} = b_{20,38} \oplus 1$, $a_{21,39} = b_{20,38}$, $a_{21,40} = b_{20,40}$, $a_{21,41} = b_{20,41}$, $a_{21,50} = a_{20,50}$, $a_{21,51} = a_{20,51}$, $a_{21,55} = a_{20,55} \oplus 1$, $a_{21,56} = a_{20,55}$, $a_{21,57} = a_{20,57} \oplus 1$, $a_{21,58} = a_{20,57} \oplus 1$, $a_{21,59} = a_{20,57} \oplus 1$, $a_{21,60} = a_{20,57}$, $a_{21,61} = a_{20,61}$, $a_{21,63} = a_{20,63}$	23
	b_{21}	$b_{21,28} = a_{21,28}$, $b_{21,50} = a_{21,50} \oplus 1$, $b_{21,51} = a_{21,51}$, $b_{21,52} = a_{21,51}$, $b_{21,53} = a_{21,51}$, $b_{21,54} = a_{21,51} \oplus 1$, $b_{21,55} = a_{21,55} \oplus 1$, $b_{21,56} = a_{21,55}$, $b_{21,57} = a_{21,57} \oplus 1$, $b_{21,58} = a_{21,58} \oplus 1$, $b_{21,59} = a_{21,59}$, $b_{21,61} = a_{21,61}$, $b_{21,62} = a_{21,62} \oplus 1$, $b_{21,63} = a_{21,63} \oplus 1$	14
	c_{21}	$c_{21,1} = c_{20,1}$, $c_{21,2} = c_{20,2}$, $c_{21,10} = c_{20,9} \oplus 1$, $c_{21,11} = c_{20,9} \oplus 1$, $c_{21,12} = c_{20,9} \oplus 1$, $c_{21,13} = c_{20,9} \oplus 1$, $c_{21,14} = c_{20,9}$, $c_{21,26} = c_{20,26}$, $c_{21,28} = D_{20,28} \oplus 1$, $c_{21,29} = D_{20,28}$, $c_{21,30} = d_{20,30}$, $c_{21,31} = d_{20,31} \oplus 1$, $c_{21,42} = c_{20,41} \oplus 1$, $c_{21,43} = c_{21,42}$, $c_{21,44} = c_{21,42}$, $c_{21,45} = c_{21,42}$, $c_{21,46} = c_{21,42}$, $c_{21,47} = c_{21,42}$, $c_{21,48} = c_{21,42}$, $c_{21,49} = c_{21,42} \oplus 1$, $c_{21,52} = c_{20,52} \oplus 1$, $c_{21,53} = c_{20,52}$, $c_{21,62} = c_{20,60} \oplus 1$	23
	d_{21}	$d_{21,1} = c_{21,1} \oplus 1$, $d_{21,2} = c_{21,2} \oplus 1$, $d_{21,26} = c_{21,26}$, $d_{21,27} = c_{21,26} \oplus 1$, $d_{21,28} = c_{21,28} \oplus 1$, $d_{21,29} = c_{21,29} \oplus 1$, $d_{21,30} = c_{21,30} \oplus 1$, $d_{21,31} = c_{21,31}$, $d_{21,32} = c_{21,31} \oplus 1$, $d_{21,33} = c_{21,31}$, $d_{21,52} = c_{21,52}$, $d_{21,62} = c_{21,62}$, $d_{21,63} = c_{21,62} \oplus 1$	13
22	a_{22}	$a_{22,32} = a_{21,32}$, $a_{22,33} = a_{22,32}$, $a_{22,34} = a_{22,32}$, $a_{22,35} = a_{22,32}$, $a_{22,36} = a_{22,32}$, $a_{22,37} = a_{22,32} \oplus 1$, $a_{22,38} = a_{21,38}$, $a_{22,39} = a_{21,39}$, $a_{22,40} = a_{21,40}$, $a_{22,41} = a_{21,41} \oplus 1$, $a_{22,42} = a_{22,41}$, $a_{22,43} = a_{22,41}$, $a_{22,44} = a_{22,41}$, $a_{22,45} = a_{22,41}$, $a_{22,46} = a_{22,41} \oplus 1$	15
	b_{22}	$b_{22,38} = a_{22,38} \oplus 1$, $b_{22,39} = a_{22,39} \oplus 1$, $b_{22,40} = a_{22,40} \oplus 1$, $b_{22,41} = a_{22,41}$	4
	c_{22}	$c_{22,10} = c_{21,10}$, $c_{22,11} = c_{21,11}$, $c_{22,12} = c_{21,12}$, $c_{22,13} = c_{21,13}$, $c_{22,14} = c_{21,14}$, $c_{22,42} = c_{21,42}$, $c_{22,43} = c_{21,43}$, $c_{22,44} = c_{21,44}$, $c_{22,45} = c_{21,45} \oplus 1$,	9
	d_{22}	$d_{22,10} = c_{22,10}$, $d_{22,42} = c_{22,42}$,	2
23	a_{23}	$a_{23,32} = a_{22,32}$, $a_{23,33} = a_{22,33}$, $a_{23,34} = a_{22,34}$, $a_{23,35} = a_{22,35} \oplus 1$	4
	b_{23}	$b_{23,32} = a_{23,32}$	1
16	c_{16}	$c_{16,6} = c_{17,6}$, $c_{16,12} = D_{16,12} \oplus 1$, $c_{16,58} = c_{17,58}$, $c_{16,59} = c_{17,58} \oplus 1$ $c_{16,38} = B_{16,38} \oplus c_{17,6}$, $c_{16,44} = B_{16,44} \oplus D_{16,12}$, $c_{16,26} = B_{16,26} \oplus c_{17,58} \oplus 1$	7

Table 11. The conditions in group-3.

16	a_{16}	$a_{16,12} = B_{16,12} \oplus 1$, $a_{16,22} = a_{17,22}$, $a_{16,54} = D_{16,54} \oplus a_{17,22}$	3
	b_{16}	$b_{16,6} = B_{16,6} \oplus 1$, $b_{16,12} = B_{16,12}$, $b_{16,26} = B_{16,26} \oplus 1$, $b_{16,38} = B_{16,38}$, $b_{16,44} = B_{16,44}$, $b_{16,58} = B_{16,58}$, $b_{16,59} = B_{16,59}$	7
	d_{16}	$d_{16,12} = D_{16,12}$, $d_{16,22} = D_{16,22} \oplus 1$, $d_{16,54} = D_{16,54}$	3
15	a_{15}	$a_{15,6} = c_{16,6} \oplus a_{16,12}$, $a_{15,12} = a_{16,12}$	2
3	a_3	$a_{3,59} = b_{3,59} \oplus 1$	1
2	a_2	$a_{2,59} = a_{3,59}$, $a_{2,36} = b_{2,36} \oplus 1$	2
	c_2	$c_{2,19} = d_{2,19} \oplus 1$	1
1	a_1	$a_{1,7} = b_{1,7} \oplus 1$, $a_{1,31} = b_{1,31} \oplus 1$, $a_{1,36} = a_{2,36}$, $a_{1,48} = b_{1,48} \oplus 1$, $a_{1,59} = a_{2,59}$	5
	c_1	$c_{1,19} = c_{2,19}$, $c_{1,26} = d_{1,26} \oplus 1$, $c_{1,43} = d_{1,43} \oplus 1$	3
0	a_0	$a_{0,7} = a_{1,7}$, $a_{0,12} = B_{0,12} \oplus 1$, $a_{0,17} = B_{0,17} \oplus 1$, $a_{0,22} = B_{0,22} \oplus 1$, $a_{0,29} = B_{0,29} \oplus 1$, $a_{0,31} = a_{1,31}$, $a_{0,34} = B_{0,34} \oplus 1$, $a_{0,36} = a_{1,36}$, $a_{0,45} = B_{0,45} \oplus 1$, $a_{0,48} = a_{1,48}$, $a_{0,57} = B_{0,57} \oplus 1$, $a_{0,59} = a_{1,59}$	12
	b_0	$b_{0,12} = B_{0,12}$, $b_{0,17} = B_{0,17}$, $b_{0,22} = B_{0,22}$, $b_{0,45} = B_{0,45}$, $b_{0,29} = B_{0,29}$, $b_{0,34} = B_{0,34}$, $b_{0,57} = B_{0,57}$	7
	c_0	$c_{0,3} = D_{0,3} \oplus 1$, $c_{0,10} = D_{0,10} \oplus 1$, $c_{0,15} = D_{0,15} \oplus 1$, $c_{0,19} = c_{1,19}$, $c_{0,26} = c_{1,26} \oplus 1$, $D_{0,27} = c_{1,26} \oplus 1$, $c_{0,32} = D_{0,32} \oplus 1$, $c_{0,43} = c_{1,43}$, $c_{0,55} = c_{1,55}$	9
	d_0	$d_{0,3} = D_{0,3}$, $d_{0,10} = D_{0,10}$, $d_{0,15} = D_{0,15}$, $d_{0,27} = D_{0,27}$, $d_{0,32} = D_{0,32}$, $d_{0,55} = D_{0,55}$	6
30	c_{30}	$c_{30,25} = d_{29,25}$	1
31	a_{31}	$a_{31,12} = b_{30,12}$, $a_{31,25} = b_{30,25}$, $a_{31,37} = b_{30,37}$	3
	b_{31}	$b_{31,25} = a_{31,25} \oplus 1$	1
	c_{31}	$c_{31,25} = c_{30,25}$	1
	d_{31}	$d_{31,25} = c_{31,25} \oplus 1$	1
32	a_{32}	$a_{32,12} = a_{31,12}$, $a_{32,22} = b_{31,22}$, $a_{32,37} = a_{31,37}$	3
	b_{32}	$b_{32,6} = b_{32,5} \oplus 1$, $b_{32,38} = b_{32,37} \oplus 1$, $b_{32,58} = b_{32,57} \oplus 1$	3
	c_{32}	$c_{32,6} = d_{31,6}$, $c_{32,12} = d_{31,12}$, $c_{32,19} = d_{31,19}$, $c_{32,31} = d_{31,31}$, $c_{32,37} = d_{31,37}$, $c_{32,58} = d_{31,58}$	6
$\overline{32}$	A_{32}	$A_{32,12} = a_{32,12}$, $A_{32,22} = a_{32,22}$, $A_{32,37} = a_{32,37}$	3
	B_{32}	$B_{32,5} = b_{32,5} \oplus 1$, $B_{32,12} = b_{32,12}$, $B_{32,19} = b_{32,19}$, $B_{32,26} = b_{32,26}$, $B_{32,31} = b_{32,31}$, $B_{32,37} = b_{32,37} \oplus 1$, $B_{32,44} = b_{32,44}$, $B_{32,51} = b_{32,51}$, $B_{32,57} = b_{32,57} \oplus 1$, $B_{32,63} = b_{32,63} \oplus 1$	10
	C_{32}	$C_{32,6} = c_{32,6}$, $C_{32,12} = c_{32,12}$, $C_{32,19} = c_{32,19}$, $C_{32,31} = c_{32,31}$, $C_{32,37} = c_{32,37}$, $C_{32,58} = c_{32,58}$	6
	D_{32}	$D_{32,12} = d_{32,12}$, $D_{32,22} = d_{32,22}$, $D_{32,37} = d_{32,37}$, $D_{32,54} = d_{32,54}$, $D_{32,57} = d_{32,57}$	5

References

1. Aumasson, J.-P., Çalık, Ç., Meier, W., Özen, O., Phan, R.C.-W., Varıcı, K.: Improved cryptanalysis of skein. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 542–559. Springer, Heidelberg (2009)
2. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: The KECCAK Reference. Submission to NIST (Round 3) (2011). http://keccak.noekeon.org/Keccak-reference-3.0.pdf
3. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein Hash Function Family. http://www.schneier.com/skein1.3.pdf
4. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
5. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: The rebound attack: cryptanalysis of reduced whirlpool and `Grøstl`. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 260–276. Springer, Heidelberg (2009)
6. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: Rebound attacks on the reduced `Grøstl` hash function. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 350–365. Springer, Heidelberg (2010)
7. Naya-Plasencia, M., Toz, D., Varici, K.: Rebound attack on JH42. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 252–269. Springer, Heidelberg (2011)
8. Khovratovich, D., Nikolić, I.: Rotational cryptanalysis of ARX. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 333–346. Springer, Heidelberg (2010)
9. Khovratovich, D., Nikolić, I., Rechberger, C.: Rotational rebound attacks on reduced skein. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 1–19. Springer, Heidelberg (2010)
10. Khovratovich, D., Rechberger, C., Savelieva, A.: Bicliques for preimages: attacks on Skein-512 and the SHA-2 family. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 244–263. Springer, Heidelberg (2012)
11. Lamberger, M., Mendel, F., Rechberger, C., Rijmen, V., Schläffer, M.: Rebound distinguishers: results on the full whirlpool compression function. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 126–143. Springer, Heidelberg (2009)
12. Leurent, G., Roy, A.: Boomerang attacks on hash function using auxiliary differentials. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 215–230. Springer, Heidelberg (2012)
13. Leurent, G., Thomsen, S.S.: Practical near-collisions on the compression function of BMW. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 238–251. Springer, Heidelberg (2011)
14. Su, B., Wu, W., Wu, S., Dong, L.: Near-collisions on the reduced-round compression functions of skein and BLAKE. In: Heng, S.-H., Wright, R.N., Goi, B.-M. (eds.) CANS 2010. LNCS, vol. 6467, pp. 124–139. Springer, Heidelberg (2010)
15. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)
16. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36. Springer, Heidelberg (2005)
17. Yu, H., Chen, J., Wang, X.: The boomerang attacks on the round-reduced Skein-512. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 287–303. Springer, Heidelberg (2013)