Near-Collision Attack on the Step-Reduced Compression Function of Skein-256 *

Hongbo Yu[1], Jiazhe Chen[3], Keting jia[2], 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,ktjia,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 the 5 finalists of NIST SHA-3 competition. It is designed based on the threefish block cipher and it only uses three primitive operations: modular addition, rotation and bitwise XOR (ARX). In this paper, we combine two short differential paths to a long differential path using the modular differential technique. And we present the semi-free start near-collision attack up to the 32-step Skein-256 with the Hamming difference 51. The complexity of our attack is about 2^{105}.

Key words: Hash function, Near-collision, SHA-3, Skein

1 Introduction

Cryptographic hash functions, which provide integrity, authentication and etc., are very important in modern cryptology. In 2005, as the most widely used hash functions MD5 and SHA-1 were broken by Wang et al. [6][7], the status of the hash functions becomes alarming. Besides, people are worrying about the security of SHA-2 due to the same structure and design principle as MD5 and SHA-1. To deal with the undesirable situation, NIST started a hash competition for a new hash standard(SHA-3) in 2007. To our knowledge, 56 out of 64 submissions to the SHA-3 competition are publicly known and available. There are 51 submissions in the first round and 14 submissions have entered the second round. At this time, the competition comes into the third round that is also the final round, and 5 out of the 14 candidates are selected. Skein [2], which is a ARX-type hash function (which is based on modular addition, rotation and exclusive-OR), is one of the final round candidates. The core of the compression function of Skein is a tweakable block cipher called Threefish, which is defined with a 256-, 512-, 1024-bit block size and 72, 72, 80 rounds respectively. When the algorithm was getting into the second round, the authors had changed the rotation constants.

During the competition, Skein has been attracting the attentions of the cryptanalysts, and there are several cryptanalytic results on the security of the compression function of Skein. Aumasson et al. proposed near-collision of 17-step Skein-512 compression function for the old constants in [1], then Su et al. present near-collisions of Skein-256/-512 compression functions reduced to 20 steps and Skein-1024 reduced to 24 steps [5]. Khovratovich et al. combined the rotational attack and the rebound attack, and gave distinguishers of 53-step Skein-256 and 57-step Skein-512 respectively [4].

Our contribution. In this paper, we focus on the compression function of Skein-256. We first find two differentials by the modular differential technique, then connect them to get a differential with 32 steps. Finally, by applying the message modification technique, we find a near-collision of 32-step Skein-256 with Hamming difference 51, and the complexity of our attack is about

* Supported by the National Natural Science Foundation of China (No.60803125), "973" Project of China (No.2007CB807902) and the Tsinghua University Initiative Scientific Research Program (No.2009THZ01002).

2^{105}. To the best of our knowledge, our attack is the first attempt to apply the rebound-type idea to the differential attack of the ARX type algorithms.

The rest of the paper is organized as follows. In Section 2, we give some notations and a brief description of the compression function of Skein-256. The main idea of our attack is described in Section 3. In Section 4, we demonstrate the near-collision attack on the 32-step Skein-256. Finally, a conclusion of the paper is given in Section 5.

2 Preliminary

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' (modulo 2^{64})
5. $\lll$: rotation to the left

2.2 Brief Description of the Compression Function of Skein-256

The compression function of Skein can be defined as $H = E(IV, T, M) \oplus M$, where $E(K, T, P)$ 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 step, 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 are involved every four steps. 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 a rotation constants which can be found in [2]. 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 $\overline{h_{72}} = (a_{72}+K_{18,a}, b_{72}+K_{18,b}, c_{72}+K_{18,c}, d_{72}+K_{18,d})$.

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:

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

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

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

3 The Rebound Attack on the ARX-type Hash functions

The rebound attack was presented by Mendel et al. in FSE 2009 [3] during the SHA-3 competitions, it is very efficient to attack the hash functions based on the AES-like structure. Series hash functions such as Whirlpoor, Echo and Grøstl are vulnerable to the rebound attack. Its key idea is getting a long differential by connecting two short differentials, and one does not find two specific differential paths that can be connect, but two differentials that are sets of differential paths which have differences in some specific positions. As the connecting 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 always find differentials that can be connected.

However, when applying the rebound attack to the ARX-type hash functions, we have to find two specific paths that can be connected. Furthermore, we do not have S-boxes in the connecting part, and the distribution of the differences by applying the modular addition, XOR and rotation are much worse than that of S-boxes. As a result, the situation that two differential paths can not be connected occurs with high probability, and it is far more difficult to apply the rebound attack by connecting two differential paths into a long one to the ARX-type hash functions.

Skein and BLAKE are two ARX-type hash functions of the SHA-3 final round candidates. Because of the strong diffusion after several steps, only short differential paths are found for these two algorithms. A trivial way to get short differential path is to find a short local collision in the middle 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 steps 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 steps. Then we can get differential paths with more steps by extending the 8-step local collision forward and backward. But the differential is always not long enough as a single bit difference will evolve to a heavy weight difference after 4 steps. A natural idea will be raised to connect two short differential paths into a long one, and one can cancel a vast number of conditions by using message modification technique in the connecting part, see the right part of Fig. 1. But it is pretty difficult to connect the differential path, which is described in Section 4. To deal with the problem, we use properties of both XOR difference and modular subtraction difference, and choose a optimal position for the connection. Then by the bit carry technique, which is the key technique for the connection, we find non-linear differential of 8 steps to connect two short differential paths with 16 and 8 steps respectively. Consequently, a differential path with 32 steps is constructed, which can be used to mount near-collision attack on 32-step Skein-256 by further using the message modification technique. The detail of our attack can be found in Section 4.

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

4 Near Collisions for 32-step 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 that have to be carried

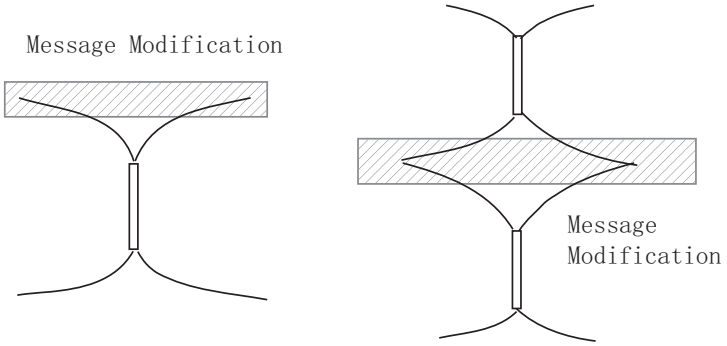

Fig. 1. Two Attack Models

out. Firstly, proper difference in (K, T) should be chosen, which is the starting point of our attack. Secondly, we connect two short differential path by the non-linear difference expansion in the middle steps and derive the sufficient conditions to guarantee that the differential path holds, which is the most challenging part in our attack. Thirdly, the vast number of conditions in the intermediate steps should be corrected by modifying the chaining variables, the key K and the tweak T. Finally, after the message/IV modifications, we search the remaining conditions by divide and conquer technique.

4.1 Construct a 32-step differential path for Skein-256

The difference for 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 is $\Delta k_3 = 2^{63}$ and $\Delta t_0 = 2^{63}$. According to the key expansion schedule, the difference for the subkey $K_i = (K_{i,a}, K_{i,b}, K_{i,c}, K_{i,d})$ $(0 \le i \le 8)$ is shown in Table 1.

Table 1. The subkey differences of 32-step Skein-256, given a difference $\delta = 2^{63}$ in k_3 and t_0.

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

The first short differential path we used consists of 16 steps. Because $\Delta K_1 = (0, 0, 0, 2^{63})$ and $\Delta K_2 = (0, 0, 0, 0)$, we select the intermediate values to meet $\Delta h_4 = (0, 0, 0, 2^{63})$. In this way, we get a 8-step path with zero difference from step 5 to 12. By extending the difference Δh_4 in

the backward direction for 5 steps and the difference $\Delta\overline{h_{12}} = \Delta K_3$ in the forward direction for 4 steps by the linear difference expansion, a 16-step differential path with high probability can be obtained.

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

The most expensive part in our work is to connect the two differential paths from steps 16 to 23 by the non-linear difference expansion. We first select step 20 as the connection step. Because the 20-th step is the step where the subkey is involved, the only thing we need for the two differential paths to be connected is that the integer modular substraction difference $\Delta^+ h_{20}$ computed by the forward direction and the $\Delta^+\overline{h_{20}}$ computed by the backward direction satisfy the equation $\Delta^+\overline{h_{20}} = \Delta^+ h_{20} + \Delta^+ K_5$. Otherwise, for example, if we connect the two differential path in step 19, both the integer modular substraction difference and the XOR difference in h_{19} by both direction must be equal. The major technique to connect the two differential path is the bit carries. The connection processor is a hard task, which needs to handle hundreds of bit equations. In the joint of the differential path, the following two requirements have to be considered.

1. Since the subkeys (the IV) are involved every 4 steps for Skein-256, the probability of the local differential between two subkeys must be higher than 2^{-256}, especially for steps $16 \sim 20$ and $\overline{20} \sim 24$.
2. The probability for the 32-step differential path must be higher than 2^{-640}, because the degrees of the freedom of the M, K and T are 640.

The 32-step near-collision differential path is shown in Table 2. In Table 2, we use two kinds of difference: the XOR difference and the integer modular substraction difference. In the step $\overline{i}$ (the step 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., $\Delta^+ A_i = \Delta^+ a_i$ and $\Delta^+ C_i = \Delta^+ c_i$. And in the other positions of the differential, we use the XOR difference.

According to the differential path in Table 2, we can derive the sufficient conditions in $h_{20} \sim h_0$ and $\overline{h_{20}} \sim \overline{h_{32}}$, which is shown in Table 4 and Table 5 respectively.

4.2 Message/IV modification

In order to carry out the Message/IV modification, we replace the conditions $b_{i,j}$, $d_{i,j}$ ($\overline{16} \le i \le 19, 1 \le j \le 32$) with $a_{i+1,((j+R_{i+1,0}) \mod 64)} \oplus d_{i+1,((j+R_{i+1,0}) \mod 64)}$ and $b_{i+1,((j+R_{i+1,1}) \mod 64)} \oplus c_{i+1,((j+R_{i+1,1}) \mod 64)}$ respectively from the Step 19 down to Step $\overline{16}$ in Table 4. In the same way, $b_{i,j}$ and $d_{i,j}$ ($\overline{20} \le i \le 24, 1 \le j \le 32$) are replaced with $c_{i,j} \oplus d_{i-1,((j-R_{i,1}) \mod 64)}$ and $a_{i,j} \oplus b_{i-1,((j-R_{i,0}) \mod 64)}$ respectively for the steps $\overline{20}$ to 24 in Table 5. The new conditions are shown in Table 6 and Table 7.

Then the distribution of the conditions of 32-step Skein-256 can be shown in Table 3.

Our message/IV modification can be divided into three parts:

1. The 178 conditions of h_{20} and h_{19} in Table 6 can be fulfilled by the chaining variable $h_{20} = (a_{20}, b_{20}, c_{20}, d_{20})$.
   - All conditions in h_{20} is easy to satisfied by choosing proper values.
   - The conditions $a_{19,j}$ can be corrected by $a_{20,j}$, $a_{20,((j+5) \mod 64)}$ and $d_{20,((j+5) \mod 64)}$.
   - The conditions $c_{19,j}$ can be corrected by $c_{20,j}$, $c_{20,((j+37) \mod 64)}$ and $b_{20,((j+37) \mod 64)}$.

Table 2. Differential path used for the near collision of 32-step compression function of Skein-256, with a probability of 2^{-105} after the message/IV modifications.

Round	Δa_i	Δb_i	Δc_i	Δd_i
0	0500900a50210840	8100100210210800	0040040086044204	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	0200082002000820	0200000000000820	0020000000200800
$\overline{16}$:+K_4	$\Delta^+ a_{16} + 2^{63}$	06000820060008e0	$\Delta^+ c_{16} + 2^{63}$	0020000000600800
17	8200082002200020	82e0006008600000	82e0000000600020	800809a0001801a0
18	0060080006000020	3f2809f340183f83	7e2819e000180f80	0068260000008620
19	015870bfc66853a3	028610a0682980a0	020030a0000f80a0	$f8f87ca007f7c7a7$
20	05c2010d72005101	800001$ff1e1fd101$	7$ef8f$50001104501	5500150077304501
$\overline{20}$:+K_5	$\Delta^+ a_{20}$	0000001$ffbfff103$	$\Delta^+ c_{20} + 2^{63}$	$fd001f0077f3ff01$
21	1$fffffe3f$8000000	0ffe000008000000	$e019fe03f2003e00$	20080001fe000000
22	000001ff80000000	000001e000000000	80001e0000000200	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	8000000000000000	8000000000000000
31	0000001001000800	0000000001200000	0000000001000000	0200001041040820
32	0000001000200800	4304083042040830	0200001040040820	0120001000200800
$\overline{32}$:+K_8	8000001000200800	4104081042040810	8200001040040820	0120001000000800
Near-collision	8500901a50010040	c004181250250010	82400410c6004a24	8160001084204a04

2. The 157 conditions of $\overline{h_{20}}$, h_{21} and h_{22} in Table 7 can be fulfilled by 256 bits out of the 384-bit (K, T).
   - Conditions in B_{20} and D_{20} can be corrected by subkey words $K_{5,b}$ and $K_{5,d}$ respectively.
   - Conditions in a_{21} and c_{21} can be corrected by subkey words $K_{5,a}$ and $K_{5,c}$ respectively.
   - Conditions in a_{22} and c_{22} can be corrected by using more careful modification of the 256-bit K_5.
3. The 9 conditions of b_{16} and d_{16} in Table 4 can be modified by the remaining 128 bits of (K, T).

Table 3. The conditions distribution of the 32-step Skein-256.

Step	Conditions	Modified conditions	Used message/IV
$0 \sim 12$	46	0	
$\overline{12} \sim 16$	20	9	K, T
$\overline{16} \sim 20$	242	178	h_{20}
$\overline{20} \sim 24$	162	157	K, T
$\overline{24} \sim 32$	43	0	

4.3 The Near-collision Attack for 32-step Skein-256

In our attack, we view the 256-bit value h_{20} and the 384-bit (K, T) as the random variables. As the chaining values a_{19}, h_{18}, h_{17} and $\overline{h_{16}}$ are only depend on h_{20}, the search of the right h_{20} can be independent from that of K and T. Therefore, in our algorithm, the first part is to find h_{20} that satisfies the differential path in steps 20 to $\overline{16}$, and the second part is to find K and T so that the differential path in Table 2 holds.

The near-collision search algorithm:

1. Select a 256-bit chaining value $h_{20} = (a_{20}, b_{20}, c_{20}, d_{20})$ which satisfies the 112 conditions of h_{20} in Table 6.
2. Compute the chaining values $h_{19} = (a_{19}, b_{19}, c_{19}, d_{19})$ from h_{20} by using the step operations:

$$\begin{aligned} b_{19} &= (a_{20} \oplus d_{20}) >>> 5 \\ a_{19} &= a_{20} - b_{19} \\ d_{19} &= (b_{20} \oplus c_{20}) >>> 37 \\ c_{19} &= c_{20} - d_{19} \end{aligned}$$

   and modify the 66 conditions in a_{19} and c_{19} in Table 6 by h_{20} using the message/IV modification technique.
3. 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. If a_{18}, c_{18}, a_{17} and c_{17} satisfy the 64 conditions in Table 6, goto step 4; Otherwise, goto step 1.
4. Choose the 256-bit subkey $K_5 = (K_{5,a}, K_{5,b}, K_{5,c}, K_{5,d})$ randomly. Compute

$$\overline{h_{20}} = h_{20} + K_5 = (A_{20}, B_{20}, C_{20}, D_{20}).$$

   Modify the 68 conditions in B_{20} and D_{20} by $K_{5,b}$ and $K_{5,d}$ respectively, and compute h_{21} and h_{22} by $\overline{h_{20}}$ in the forward direction. Then modify the 89 conditions in a_{21}, c_{21}, a_{22} and c_{22} of Table 6 by K_5.

5. Select the 128-bit value $K_{4,b}$ and $K_{4,d}$ randomly, and compute $b_{16} = B_{16} - K_{4,b}$ and $d_{16} = D_{16} - K_{4,d}$. The 9 conditions in b_{16} and d_{16} can be modified by $K_{4,b}$ and $K_{4,d}$ respectively.
6. According to the subkey deriving schedule,

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

where $k_4 = 0x1bd11bdaa9fc1a22 \oplus \bigoplus_{i=0}^{3} k_i$ and $t_2 = t_0 \oplus t_1$, we can derive the key $K = (k_0, k_1, k_2, k_3)$ and the tweak $T = (t_0, t_1)$ once we know $K_{4,b}$, $K_{4,d}$ and K_5:

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

And we can further deduce that

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

Furthermore, $a_{16} = A_{16} - K_{4,a}$ and $c_{16} = C_{16} - K_{4,c}$ can be computed.
7. Compute K_0, K_1, K_2, K_3, K_6, K_7, K_8 by K and T, calculate h_{23} to $\overline{h_{32}}$ by h_{22}, 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.
8. Let $h'_{20} = h_{20} \oplus \Delta h_{20}$, where Δh_{20} is the difference of step 20 in Table 2. 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 difference in step 0 and step $\overline{32}$ of Table 2. If so, output the message pair $(M = h_0, M' = h'_0)$, the master key $K = (k_0, k_1, k_2, k_3)$, the tweak $T = (t_0, t_1)$ and the near-collision difference $\Delta h_0 \oplus \Delta\overline{h_{32}}$; Otherwise, goto step 4.

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

- The total degrees of the freedom come from the message M, the master key K and the tweak 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 513 (See Table 4 and Table 5). So the degrees of freedom is sufficient to perform our purpose.
- The local degrees of the freedom from steps 20 down to $\overline{16}$ is 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 steps is 242 (See Table 6). It's some tight to search the local differentials from steps 20 down to $\overline{16}$ after the message modification. But we can release the degrees of freedom by finding a large number of differentials with the almost the same probability from steps $\overline{16}$ to 20, and these differentials have the same input and output differences in step $\overline{16}$ and step 20.
- The degrees of the freedom from steps $\overline{20}$ to 32 and steps 16 down to 0 are $256 + 128 = 384$. The number of conditions of these two parts is 271. So it's enough to search the near-collision after the message modifications.

The complexity computation: The complexity for our attack can be divided into two parts:

- The first part is to find a right 256-bit chaining value h_{20} so that it satisfies the 242 conditions of h_{20}, h_{19}, h_{18}, h_{17} and $\overline{h_{16}}$ in Table 4. The complexity is about 2^{64} 32-step Skein-256 compression function operations after the message/IV modification.
- The second part is to find a right 384-bit value (K, T) that satisfies the other 271 conditions in Table 4 and Table 5. The complexity for the this part is about 2^{105} operations.

As a result, the total complexity for our attack is about $2^{64} + 2^{105} \approx 2^{105}$.

5 Conclusions

In this paper, we first apply the rebound-type idea to the differential attack of the ARX type hash algorithms and connect two specific short differentials to a long one. Utilizing our technique, we give the 32-step semi-free start near-collision attack for Skein-256 with complexity about 2^{105}. Our method is also applicable to other ARX type hash functions.

References

1. Aumasson, J.-P., Calik, C., Meier, W., Ozen, O., Phan, R.C.W., Varici, K.: Improved Cryptanalysis of Skein. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 542-559. Springer, Heidelberg (2009)
2. 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
3. Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen: The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl. In: O. Dunkelman (ed.) FSE 2009. LNCS, vol. 5665, pp. 260-276. Springer, Heidelberg (2009)
4. Dmitry Khovratovich, Ivica Nikolić, and Christian Rechberger: Rotational Rebound Attacks on Reduced Skein. In: M. Abe (Ed.): ASIACRYPT 2010, LNCS, vol. 6477, pp. 1-19. Springer, Heidelberg (2010)
5. Bozhan Su, Wenling Wu, Shuang Wu, and Le Dong: Near-Collisions on the Reduced-Round Compression Functions of Skein and BLAKE. In: S.-H. Heng, R.N. Wright, and B.-M. Goi (Eds.): CANS 2010, LNCS 6467, pp. 124-139. Springer, Heidelberg (2010)
6. Wang, X.Y., Yu, H.B.: How to Break MD5 and Other Hash Functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19-35. Springer, Heidelberg (2005)
7. Wang, X.Y., Yin, Y.L., Yu, H.B.: Finding Collisions in the Full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17-36. Springer, Heidelberg (2005)

Table 4. The sufficient conditions for Step 20 down to 0 of the differential path in Table 2.

20	a_{20}	$a_{20,15} = a_{20,13}$, $a_{20,29} = a_{20,26} \oplus 1$, $a_{20,30} = a_{20,29}$, $a_{20,31} = a_{20,30}$, $a_{20,35} = a_{20,33}$, $a_{20,36} = a_{20,35}$, $a_{20,56} = a_{20,55} \oplus 1$, $a_{20,59} = a_{20,57} \oplus 1$	8
	b_{20}	$b_{20,1} = a_{20,1} \oplus 1$, $b_{20,9} = a_{20,9} \oplus 1$, $b_{20,13} = a_{20,13} \oplus 1$, $b_{20,15} = a_{20,15}$, $b_{20,16} = b_{20,15}$, $b_{20,17} = b_{20,16}$, $b_{20,18} = b_{20,17}$, $b_{20,19} = b_{20,18}$, $b_{20,20} = b_{20,19}$, $b_{20,21} = b_{20,20} \oplus 1$, $b_{20,26} = a_{20,26}$, $b_{20,27} = a_{20,26} \oplus 1$, $b_{20,29} = a_{20,29}$, $b_{20,33} = a_{20,33}$, $b_{20,34} = b_{20,33} \oplus 1$, $b_{20,35} = a_{20,35} \oplus 1$, $b_{20,36} = a_{20,36}$, $b_{20,37} = b_{20,36} \oplus 1$, $b_{20,38} = b_{20,37}$, $b_{20,39} = b_{20,38}$, $b_{20,40} = b_{20,39}$, $b_{20,41} = b_{20,40} \oplus 1$	22
	c_{20}	$c_{20,45} = c_{20,41}$, $c_{20,46} = c_{20,45}$, $c_{20,47} = c_{20,46}$, $c_{20,48} = c_{20,47} \oplus 1$, $c_{20,53} = c_{20,52}$, $c_{20,54} = c_{20,53}$, $c_{20,55} = c_{20,54}$, $c_{20,56} = c_{20,55}$, $c_{20,58} = c_{20,52} \oplus 1$, $c_{20,59} = c_{20,58} \oplus 1$, $c_{20,60} = c_{20,59} \oplus 1$	11
	d_{20}	$d_{20,1} = c_{20,1} \oplus 1$, $d_{20,9} = c_{20,9}$, $d_{20,11} = c_{20,11} \oplus 1$, $d_{20,15} = c_{20,15} \oplus 1$, $d_{20,21} = c_{20,21}$, $d_{20,22} = d_{20,21} \oplus 1$, $d_{20,25} = c_{20,25} \oplus 1$, $d_{20,27} = d_{20,26} \oplus 1$, $d_{20,41} = c_{20,41}$, $d_{20,43} = c_{20,43} \oplus 1$, $d_{20,45} = c_{20,45}$, $d_{20,57} = c_{20,52}$, $d_{20,59} = c_{20,59}$, $d_{20,61} = c_{20,61} \oplus 1$, $d_{20,63} = c_{20,63}$	15
19	a_{19}	$a_{19,1} = a_{20,1} \oplus 1$, $a_{19,2} = a_{19,1} \oplus 1$, $a_{19,6} = b_{19,6} \oplus 1$, $a_{19,8} = b_{19,8} \oplus 1$, $a_{19,9} = a_{20,9} \oplus 1$, $a_{19,10} = a_{19,9} \oplus 1$, $a_{19,13} = a_{20,13}$, $a_{19,15} = a_{20,15} \oplus 1$ $a_{19,20} = b_{19,20} \oplus 1$, $a_{19,22} = b_{19,22}$, $a_{19,23} = a_{19,22} \oplus 1$, $a_{19,26} = b_{19,28}$, $a_{19,27} = a_{19,26}$, $a_{19,32} = a_{19,31} \oplus 1$, $a_{19,31} = b_{19,30}$, $a_{19,33} = a_{20,33} \oplus 1$, $a_{19,34} = a_{19,33} \oplus 1$, $a_{19,35} = a_{19,34}$, $a_{19,36} = a_{19,35} \oplus 1$, $a_{19,37} = a_{19,36} \oplus 1$, $a_{19,38} = b_{19,38} \oplus 1$, $a_{19,40} = b_{19,40}$, $a_{19,45} = b_{19,45}$, $a_{19,46} = a_{19,45}$, $a_{19,47} = a_{19,46} \oplus 1$, $a_{19,52} = b_{19,50}$, $a_{19,53} = a_{19,52} \oplus 1$, $a_{19,55} = a_{20,55}$, $a_{19,57} = a_{20,57} \oplus 1$	29
	b_{19}	$b_{19,16} = a_{20,15} \oplus 1$, $b_{19,17} = b_{19,16} \oplus 1$, $b_{19,22} = b_{19,20} \oplus 1$, $b_{19,28} = a_{20,26} \oplus 1$, $b_{19,30} = a_{20,30} \oplus 1$, $b_{19,31} = b_{19,30} \oplus 1$, $b_{19,40} = a_{20,41}$, $b_{19,50} = a_{20,50} \oplus 1$, $b_{19,51} = b_{19,50}$, $b_{19,56} = a_{20,56}$, $b_{19,58} = a_{20,57} \oplus 1$	11
	c_{19}	$c_{19,6} = d_{19,6} \oplus 1$, $c_{19,8} = d_{19,8} \oplus 1$, $c_{19,16} = d_{19,16} + 1$, $c_{19,17} = c_{19,16}$, $c_{19,18} = c_{19,17}$, $c_{19,19} = c_{19,18} \oplus 1$, $c_{19,20} = c_{19,19} \oplus 1$, $c_{19,38} = d_{19,38} \oplus 1$, $c_{19,40} = c_{20,45}$, $c_{19,45} = c_{20,45} \oplus 1$, $c_{19,46} = d_{19,46}$, $c_{19,58} = d_{19,52}$	12
	d_{19}	$d_{19,1} = c_{20,1} \oplus 1$, $d_{19,2} = d_{19,1}$, $d_{19,3} = d_{19,2} \oplus 1$, $d_{19,9} = c_{20,9} \oplus 1$, $d_{19,10} = d_{19,9} \oplus 1$, $d_{19,11} = c_{20,11}$, $d_{19,15} = c_{20,15}$, $d_{19,17} = d_{19,16}$, $d_{19,18} = d_{19,17}$, $d_{19,19} = d_{19,18}$, $d_{19,21} = c_{20,21} \oplus 1$, $d_{19,22} = d_{19,20}$, $d_{19,23} = d_{19,22}$, $d_{19,24} = d_{19,23} \oplus 1$, $d_{19,25} = c_{20,25} \oplus 1$, $d_{19,26} = d_{19,25}$, $d_{19,27} = d_{19,26} \oplus 1$, $d_{19,40} = c_{20,41}$, $d_{19,43} = c_{20,43} \oplus 1$, $d_{19,44} = d_{19,43}$, $d_{19,45} = d_{19,44} \oplus 1$, $d_{19,47} = d_{19,46} \oplus 1$, $d_{19,52} = c_{20,52}$, $d_{19,53} = d_{19,52}$, $d_{19,54} = d_{19,53}$, $d_{19,55} = d_{19,54}$, $d_{19,56} = d_{19,55}$, $d_{19,60} = c_{20,60}$, $d_{19,61} = c_{20,61}$, $d_{19,62} = d_{19,61} \oplus 1$, $d_{19,63} = c_{20,63} \oplus 1$	31
18	a_{18}	$a_{18,6} = a_{19,6}$, $a_{18,26} = a_{19,26}$, $a_{18,27} = a_{19,27}$, $a_{18,44} = a_{19,45} \oplus 1$, $a_{18,54} = b_{18,54} \oplus 1$, $a_{18,55} = a_{19,55}$	6
	b_{18}	$b_{18,1} = a_{19,1}$, $b_{18,2} = a_{19,2}$, $b_{18,8} = a_{19,8}$, $b_{18,9} = a_{19,9}$, $b_{18,10} = b_{18,9}$, $b_{18,11} = b_{18,10}$, $b_{18,12} = b_{18,11} \oplus 1$, $b_{18,13} = a_{19,13} \oplus 1$, $b_{18,14} = a_{19,15} \oplus 1$, $b_{18,20} = a_{19,20} \oplus 1$, $b_{18,21} = b_{18,20}$, $b_{18,31} = a_{19,31} \oplus 1$, $b_{18,33} = a_{19,33}$, $b_{18,34} = b_{18,33}$, $b_{18,37} = a_{19,37}$, $b_{18,38} = a_{19,38} \oplus 1$, $b_{18,39} = b_{18,38} \oplus 1$, $b_{18,40} = a_{19,40} \oplus 1$, $b_{18,41} = b_{18,40} \oplus 1$, $b_{18,44} = a_{19,45} \oplus 1$, $b_{18,52} = a_{19,52} \oplus 1$, $b_{18,54} = a_{19,55}$, $b_{18,57} = a_{19,57} \oplus 1$, $b_{18,58} = b_{18,57}$, $b_{18,59} = b_{18,58}$, $b_{18,60} = b_{18,59}$, $b_{18,61} = b_{18,60}$, $b_{18,62} = b_{18,51} \oplus 1$	28
	c_{18}	$c_{18,8} = d_{18,10}$, $c_{18,9} = c_{18,8} \oplus 1$, $c_{18,10} = c_{18,9}$, $c_{18,11} = c_{18,10}$, $c_{18,12} = c_{18,11} \oplus 1$, $c_{18,20} = c_{19,20} \oplus 1$, $c_{18,21} = c_{18,20} \oplus 1$, $c_{18,38} = c_{19,38} \oplus 1$, $c_{18,39} = c_{18,38} \oplus 1$, $c_{18,40} = d_{18,42}$, $c_{18,41} = c_{18,40}$, $c_{18,44} = c_{18,41} \oplus 1$, $c_{18,45} = c_{19,45}$, $c_{18,52} = d_{18,52} \oplus 1$, $c_{18,54} = d_{18,54}$, $c_{18,58} = c_{19,58} \oplus 1$, $c_{18,59} = c_{18,58}$, $c_{18,60} = c_{18,59}$, $c_{18,61} = c_{18,60}$, $c_{18,62} = c_{18,61}$, $c_{18,63} = c_{18,62} + 1$	21
	d_{18}	$d_{18,6} = c_{19,6}$, $d_{18,11} = d_{18,10} \oplus 1$, $d_{18,10} = c_{19,8} \oplus 1$, $d_{18,16} = c_{19,16} \oplus 1$, $d_{18,42} = c_{19,40} \oplus 1$, $d_{18,43} = d_{18,42}$, $d_{18,46} = c_{19,46}$, $d_{18,55} = d_{18,54} \oplus 1$	8
17	a_{17}	$a_{17,6} = a_{18,6}$, $a_{17,22} = b_{17,22}$, $a_{17,26} = a_{18,26} \oplus 1$, $a_{17,38} = b_{17,38}$, $a_{17,44} = a_{18,44}$, $a_{17,58} = b_{17,58} \oplus 1$	6
	b_{17}	$b_{17,23} = b_{17,22} \oplus 1$, $b_{17,28} = a_{18,26}$, $b_{17,39} = b_{17,38} \oplus 1$, $b_{17,54} = a_{18,54}$, $b_{17,55} = a_{18,55} \oplus 1$, $b_{17,56} = b_{17,55} \oplus 1$	6
	c_{17}	$c_{17,6} = d_{17,6} \oplus 1$, $c_{17,22} = d_{17,20}$, $c_{17,23} = c_{17,22} \oplus 1$, $c_{17,54} = c_{18,54} \oplus 1$, $c_{17,55} = c_{17,54}$, $c_{17,56} = c_{17,55} \oplus 1$, $c_{17,58} = c_{18,58}$	7
	d_{17}	$d_{17,8} = c_{18,8}$, $d_{17,9} = d_{17,8}$, $d_{17,20} = c_{18,20}$, $d_{17,21} = d_{17,20}$, $d_{17,38} = c_{18,38} \oplus 1$, $d_{17,40} = c_{18,40}$, $d_{17,41} = c_{18,41}$, $d_{17,44} = c_{18,44} \oplus 1$, $d_{17,52} = c_{18,52}$	9
$\overline{16}$	B_{16}	$B_{16,6} = a_{17,6} \oplus 1$, $B_{16,7} = B_{16,6}$, $B_{16,8} = B_{16,7} \oplus 1$, $B_{16,26} = a_{17,26} \oplus 1$, $B_{16,27} = B_{16,26} \oplus 1$, $B_{16,38} = a_{17,38}$, $B_{16,44} = a_{17,44}$, $B_{16,58} = a_{17,58} \oplus 1$, $B_{16,59} = B_{16,58} \oplus 1$	9
	D_{16}	$D_{16,23} = D_{16,22} \oplus 1$, $D_{16,22} = c_{17,22}$, $D_{16,54} = c_{17,54} \oplus 1$	3
16	a_{16}	$a_{16,12} = B_{16,12} \oplus 1$, $a_{16,22} = a_{17,22}$	2
	b_{16}	$b_{16,6} = B_{16,6} \oplus 1$, $b_{16,12} = B_{16,12}$, $b_{16,26} = B_{16,26} \oplus 1$, $b_{16,38} = B_{16,38}$, $b_{16,44} = B_{16,44}$, $b_{16,58} = B_{16,58} \oplus 1$	6
	c_{16}	$c_{16,6} = c_{17,6}$, $c_{16,12} = D_{16,12} \oplus 1$, $c_{16,58} = c_{17,58}$	3
	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}	$b_{15,22} = a_{16,12}$	1
	d_{15}	$d_{15,6} = c_{16,6}$, $d_{15,12} = c_{16,12}$, $d_{15,58} = c_{16,58}$	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	$a_{1,36} = a_{2,36}$, $a_{1,59} = a_{2,59}$, $a_{1,7} = b_{1,7} \oplus 1$, $a_{1,31} = b_{1,31} \oplus 1$, $a_{1,48} = b_{1,48} \oplus 1$	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	$c_{0,3} = D_{0,3} \oplus 1$, $c_{0,10} = D_{0,10} \oplus 1$, $c_{0,15} = D_{0,15} \oplus 1$, $c_{0,19} = c_{1,19}$, $c_{0,26} = c_{1,26}$, $c_{0,27} = D_{0,27} \oplus 1$, $c_{0,32} = D_{0,32} \oplus 1$, $c_{0,43} = c_{1,43}$, $c_{0,55} = c_{1,55}$	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 5. The sufficient conditions for Step $\overline{20} \sim 32$ of the differential path in Table 2.

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

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

Table 7. The sufficient conditions for Step $\overline{20} \sim 24$ of the differential path in Table 2.

$\overline{20}$	B_{20}	$B_{20,1} = b_{20,1} \oplus 1$, $B_{20,2} = B_{20,1} \oplus 1$, $B_{20,3} = d_{20,26} \oplus b_{20,28} \oplus 1$, $B_{20,4} = d_{20,29} \oplus b_{20,28}$, $B_{20,5} = d_{20,30} \oplus b_{20,28}$, $B_{20,6} = d_{20,31} \oplus b_{20,28}$, $B_{20,7} = a_{20,29} \oplus d_{20,31} \oplus 1$, $B_{20,8} = a_{20,29} \oplus d_{20,31}$, $B_{20,9} = b_{20,9}$, $B_{20,13} = b_{20,13} \oplus 1$, $B_{20,14} = B_{20,13} \oplus 1$, $B_{20,15} = b_{20,15}$, $B_{20,16} = B_{20,15}$, $B_{20,17} = B_{20,16}$, $B_{20,18} = B_{20,17}$, $B_{20,19} = B_{20,18}$, $B_{20,20} = B_{20,19}$, $B_{20,21} = B_{20,20}$, $B_{20,22} = B_{20,21}$, $B_{20,23} = B_{20,22}$, $B_{20,24} = B_{20,23}$, $B_{20,25} = B_{20,24} \oplus 1$, $B_{20,26} = b_{20,26} \oplus 1$, $B_{20,27} = c_{20,52} \oplus a_{20,50}$, $B_{20,28} = b_{20,28}$, $B_{20,29} = b_{20,29} \oplus 1$, $B_{20,30} = B_{20,29}$, $B_{20,31} = B_{20,30}$, $B_{20,32} = B_{20,31} \oplus 1$, $B_{20,33} = b_{20,33}$, $B_{20,34} = b_{20,34}$, $B_{20,35} = b_{20,35}$, $B_{20,36} = b_{20,36}$, $B_{20,37} = b_{20,37} \oplus 1$	34
	D_{20}	$D_{20,1} = d_{20,1}$, $D_{20,9} = d_{20,9} \oplus 1$, $D_{20,10} = D_{20,9} \oplus 1$, $D_{20,11} = d_{20,11} \oplus 1$, $D_{20,12} = D_{20,11}$, $D_{20,13} = D_{20,12}$, $D_{20,14} = D_{20,13} \oplus 1$, $D_{20,15} = d_{20,15} \oplus 1$, $D_{20,16} = D_{20,15}$, $D_{20,17} = D_{20,16}$, $D_{20,18} = D_{20,17} \oplus 1$, $D_{20,19} = c_{20,52} \oplus a_{20,50} \oplus 1$, $D_{20,20} = c_{20,52} \oplus a_{20,50}$, $D_{20,21} = d_{20,21}$, $D_{20,22} = D_{20,21}$, $D_{20,23} = D_{20,22}$, $D_{20,24} = D_{20,23} \oplus 1$, $D_{20,25} = d_{20,25}$, $D_{20,26} = d_{20,26}$, $D_{20,27} = d_{20,27}$, $D_{20,29} = d_{20,29}$, $D_{20,30} = d_{20,30}$, $D_{20,31} = d_{20,31}$, $D_{20,41} = d_{20,41} \oplus 1$, $D_{20,42} = D_{20,41} \oplus 1$, $D_{20,43} = d_{20,43} \oplus 1$, $D_{20,44} = D_{20,43} \oplus 1$, $D_{20,45} = d_{20,45}$, $D_{20,57} = d_{20,57}$, $D_{20,59} = d_{20,59} \oplus 1$, $D_{20,60} = D_{20,59} \oplus 1$, $D_{20,61} = d_{20,61} \oplus 1$, $D_{20,62} = D_{20,61} \oplus 1$, $D_{20,63} = d_{20,63}$	34
21	a_{21}	$a_{21,26} = d_{20,26} \oplus B_{20,1} \oplus 1$, $a_{21,27} = d_{20,26} \oplus B_{20,2} \oplus 1$, $a_{21,28} = b_{20,28} \oplus 1$, $a_{21,29} = a_{21,28}$, $a_{21,30} = a_{21,29}$, $a_{21,31} = a_{21,30} \oplus 1$, $a_{21,32} = a_{20,29} \oplus 1$, $a_{21,33} = a_{21,32}$, $a_{21,34} = a_{21,33} \oplus 1$, $a_{21,38} = b_{20,38}$, $a_{21,39} = a_{21,38}$, $a_{21,40} = a_{21,39} \oplus 1$, $a_{21,41} = a_{20,41} \oplus 1$, $a_{21,42} = a_{21,41}$, $a_{21,43} = a_{21,42}$, $a_{21,44} = a_{21,43}$, $a_{21,45} = a_{21,44}$, $a_{21,46} = a_{21,45}$, $a_{21,47} = a_{21,46}$, $a_{21,48} = a_{21,47}$, $a_{21,49} = a_{21,48} \oplus 1$, $a_{21,50} = a_{20,50} \oplus 1$, $a_{21,51} = a_{21,50}$, $a_{21,52} = a_{21,51}$, $a_{21,53} = a_{21,52}$, $a_{21,54} = a_{21,53} \oplus 1$, $a_{21,55} = a_{20,55}$, $a_{21,56} = a_{21,55} \oplus 1$, $a_{21,57} = a_{20,57} \oplus 1$, $a_{21,58} = a_{21,57} \oplus 1$, $a_{21,59} = a_{20,59} \oplus 1$, $a_{21,60} = a_{21,59}$, $a_{21,61} = a_{21,60} \oplus 1$, $a_{21,62} = c_{20,62} \oplus B_{20,37} \oplus 1$	34
	c_{21}	$c_{21,10} = c_{20,9} \oplus 1$, $c_{21,11} = c_{21,10}$, $c_{21,12} = c_{21,11}$, $c_{21,13} = c_{21,12}$, $c_{21,14} = c_{21,13} \oplus 1$, $c_{21,26} = d_{20,26} \oplus 1$, $c_{21,28} = c_{21,27}$, $c_{21,29} = d_{20,29}$, $c_{21,30} = d_{20,30}$, $c_{21,31} = d_{20,31} \oplus 1$, $c_{21,32} = c_{21,31}$, $c_{21,33} = c_{21,32}$, $c_{21,34} = c_{21,33} \oplus 1$, $c_{21,42} = c_{20,41} \oplus 1$, $c_{21,43} = c_{21,42}$, $c_{21,44} = c_{21,43}$, $c_{21,45} = c_{21,44}$, $c_{21,46} = c_{21,45}$, $c_{21,47} = c_{21,46}$, $c_{21,48} = c_{21,47}$, $c_{21,49} = c_{21,48} \oplus 1$, $c_{21,50} = d_{20,15} \oplus a_{21,50}$, $c_{21,51} = d_{20,15} \oplus a_{21,51} \oplus 1$, $c_{21,52} = c_{20,52}$, $c_{21,53} = c_{21,52} \oplus 1$, $c_{21,54} = d_{20,21} \oplus a_{21,54} \oplus 1$, $c_{21,55} = d_{20,21} \oplus a_{21,55} \oplus 1$, $c_{21,56} = d_{20,21} \oplus a_{21,56} \oplus 1$, $c_{21,57} = d_{20,21} \oplus a_{21,57}$, $c_{21,58} = d_{20,25} \oplus a_{21,58} \oplus 1$, $c_{21,59} = d_{20,26} \oplus a_{21,59} \oplus 1$, $c_{21,60} = d_{20,27} \oplus a_{21,60}$, $c_{21,62} = c_{20,62} \oplus 1$, $c_{21,63} = c_{21,62} \oplus 1$	34
22	a_{22}	$a_{22,10} = c_{21,28} \oplus d_{20,59} \oplus c_{21,10}$, $a_{22,32} = a_{21,32}$, $a_{22,33} = a_{21,32}$, $a_{22,34} = a_{21,32}$, $a_{22,35} = a_{21,32}$, $a_{22,36} = a_{21,32}$, $a_{22,37} = a_{21,32} \oplus 1$, $a_{22,38} = a_{21,38}$, $a_{22,39} = a_{21,38}$, $a_{22,40} = a_{21,38} \oplus 1$, $a_{22,41} = a_{21,41} \oplus 1$, $a_{22,42} = a_{21,60} \oplus b_{20,35} \oplus c_{21,42}$	12
	c_{22}	$c_{22,10} = c_{21,10} \oplus 1$, $c_{22,38} = a_{21,26} \oplus B_{20,1} \oplus a_{22,38}$, $c_{22,39} = a_{21,27} \oplus B_{20,2} \oplus a_{22,38}$, $c_{22,40} = a_{21,28} \oplus B_{20,3} \oplus a_{22,38} \oplus 1$, $c_{22,41} = a_{21,29} \oplus B_{20,4} \oplus a_{22,41} \oplus 1$, $c_{22,42} = c_{21,42}$, $c_{22,43} = c_{21,42}$, $c_{22,44} = c_{21,42}$, $c_{22,45} = c_{21,42} \oplus 1$	9
23	a_{23}	$a_{23,32} = a_{22,32}$, $a_{23,33} = a_{23,32}$, $a_{23,34} = a_{23,33}$, $a_{23,35} = a_{23,34} \oplus 1$	4
	c_{23}	$c_{23,22} = d_{22,10} \oplus a_{23,32}$	1