Cryptanalysis of the Compression Function of SIMD

Hongbo Yu[1] and Xiaoyun Wang[2*]

No Institute Given

Abstract. SIMD is one of the second round candidates of the SHA-3 competition hosted by NIST. In this paper, we present some results on the compression function of SIMD 1.1 (the tweaked version) using the modular difference method. For SIMD-256, We give a free-start near collision attack on the compression function reduced to 20 steps with complexity 2^{-107}. And for SIMD-512, we give a free-start near collision attack on the 24-step compression function with complexity 2^{208}. Furthermore, we give a distinguisher attack on the full compression function of SIMD-512 with complexity 2^{398}. Our attacks are also applicable for the final compression function of SIMD.

Keywords: SIMD, SHA-3 Candidate, near collision, distinguishing attack

1 Introduction

Hash functions play a fundamental role in modern Cryptography. Due to the collision attacks on the series general hash functions [7, 8, 1], NIST hosted the SHA-3 hash function competition to select a new cryptographic hash function as the standard [5]. Until November 2008, NIST accepted 51 out of 64 submissions as the first round. In July 2009, NIST announced 14 second round candidates.

The hash function SIMD is one of the second round candidates, and it is designed by Leurent *et al*[4]. SIMD is a wide-pipe design based on the MD iterative structure. In Indocrypt 2009 [3], Mendel *et al* give a distinguisher attack on the SIMD-512 compression function with complexity $5.2^{425.8}$ using a differential distinguisher. Because Mendel *et al*'s attack, the designers found some bad properties of Feistel structure in SIMD, and they tweaked the SIMD by changing rotation constants and permutations for diffusion between parallel Feistels. The new version is named SIMD. In 2010 [4], Nikolic *et al* give the distinguishing attack for the compression function of 12-step SIMD-512 1.1 using the rotation distinguisher [2]. In this paper, we give series cryptanalysis results for the compression functions of the tweaked SIMD-256 and SIMD-512:

[*] Supported by 973 Project(No.2007CB807902), 863 Project(No.2006AA01Z420) and the National Natural Science Foundation of China(NSFC Grant No.60803125)

1. For SIMD-256 reduced to 20 steps, we give a free-start near collision attack with complexity 2^{107}. So far, this is the fist analysis result for the SIMD-256.
2. For SIMD-512 reduced to 24 steps, we give a free-start near collision attack with complexity 2^{208}. And for the full SIMD-512 compression function, we give a distinguishing attack with complexity 2^{398} using a difference distinguisher.

This paper is organized as follows. In section 2, we define some notations and give a brief description of SIMD. In section 3, we give the free-start near collision attack on 20-step SIMD-256. In section 4, we give a near collision attack on the 24-step SIMD-512 and a distinguishing attack for the full SIMD-512. Finally we conclude the paper in section 5.

2 Notations and Description of SIMD

The following notations can be used in this paper.

2.1 Notations

1. $+$ and $-$ denote addition and subtration modular 2^{32}.

2. $x_{i,j}$ is the j-th bit of x_i, where x_i is a 32-bit word and $x_{i,32}$ is the most significant bit.

3. $x_i[j]$ and $x_i[-j]$ (where x is a 32-bit word) are the resultant values of changing only the j-th bit of the word x_i from 0 to 1 and 1 to 0 respectively.

4. $x_i[j_1, j_2, ..., j_l]$ is the value resulting by changing the j_1-th, j_2-th, ...and j_l-th bits of x_i. Again the $+$ sign means that the bit is changed from 0 to 1, and the - sign means that the bit is changed from 1 to 0.

5. $<<<$ denote right-shift by n-bit.

6. h_i denote the chaining values in step i of SIMD-256 (or SIMD-512).

2.2 Description of SIMD

SIMD is an iterative hash function that follow the Merkle-Damgård design. The SIMD family hash function is based on two functions SIMD-256 and SIMD-512. The SIMD-n with $n \leq 256$ is defined as a truncation of SIMD-256, and SIMD-n with $256 \leq n \leq 512$ is defined as a truncation of SIMD-512. Each function SIMD-n takes as input a message of arbitrary size, and outputs a digest of n bits. The input message is padded and then divided into k 512-bit (resp. 1024-bit for SIMD-512) blocks for SIMD-256.

The compression function of SIMD-256 (resp. SIMD-512) takes a 512-bit (resp. 1024-bit) chaining value and a 512-bit (resp. 1024-bit) message and output another 512-bit (resp. 1024-bit) chaining value. Each 512-bit (resp. 1024-bit) block is first expanded into 4096 bits (resp. 8192 bits). The compression function of SIMD consist of 4 rounds, and each includes 8 steps. The feed-forward consists of 4 additional steps with the IV as the message input. Each step have 4 (resp. 8) parallel Feistel ladders , and they interact together because of the permutations $p(i)$'s. At each step, a new value is computed in each Feistel ladder, and this new value is sent to another Feistel ladder at the following step. In step i, the $j-th$ feistel ladder is given are as follows:

$$\begin{aligned}
a_i^j &= (d_{i-1}^j + w_i^j + \Phi(a_{i-1}^j, b_{i-1}^j, c_{i-1}^j)) <<< s_i + a_{i-1}^{p^{(i)}(j)} \\
b_i^j &= a_{i-1}^j <<< r_i \\
c_i^j &= b_{i-1}^j \\
d_i^j &= c_{i-1}^j
\end{aligned}$$

For SIMD-256, the permutation used at step i is $p^{(imod3)}$, and it is defined in the following:

j	0	1	2	3
$p^{(0)}(j)$	1	0	3	2
$p^{(1)}(j)$	2	3	0	1
$p^{(2)}(j)$	3	2	1	0

For SIMD-512, $p_i = p^{(imod7)}$, and the seven permutations are defined:

j	0	1	2	3	4	5	6	7
$p^{(0)}(j)$	1	0	3	2	5	4	7	6
$p^{(1)}(j)$	6	7	4	5	2	3	0	1
$p^{(2)}(j)$	2	3	0	1	6	7	4	5
$p^{(3)}(j)$	3	2	1	0	7	6	5	4
$p^{(4)}(j)$	5	4	7	6	1	0	3	2
$p^{(5)}(j)$	7	6	5	4	3	2	1	0
$p^{(6)}(j)$	4	5	6	7	0	1	2	3

In this paper, we omit to describe the message expansion algorithm because our attack is independent with the message expansion,.

The Boolean functions Φ used in the first 4 steps of each round is the chosen function IF and last 4 steps is the majority function MAJ. The rotation constants r_i and s_i can refer to the original paper [4], and they also are shown in our detail differential path.

3 The Free-start Near Collision Attack on the reduced SIMD-256

In this section, we use the modular differential method to find a differential path with high probability. The modular differential method was presented in

Eurocrypt 2005 by Wang *et al* [7], and it is a precise differential that uses integer modular subtraction in conjunction with exclusive-or as a measure of difference. There are four steps in attacking a hash function using the modular differential. The first step is to select an appropriate message or initial value difference, which determines the success probability of the attack. The key step of the modular differential attack is to select a feasible differential path according to the selected message difference or initial value difference. This difficult step requires intelligent analysis, sophisticated technique, lots of patience and good luck. The third phase is to derive the sufficient conditions that guarantee the feasibility of the differential path. In the process of searching for differential paths, the chaining variable conditions can be determined. A feasible differential path implies that all the chaining variable conditions deduced from the path do not contradict each other. The last step is the message/IV modification which forces the modified messages/IV to satisfy additional sufficient conditions.

3.1 Constructing the Specific Differential Path for 20-step SIMD-256

In this attack, the difference is only introduced in the IV because the expanded message has a minimal distance of 520 (resp. 1032) for SIMD-256 (resp. SIMD-512). Before the search of the differential path, we observe that the difference propagation of SIMD is slower in the backward direction than the forward direction. Our basic attack strategy is first to introduce one bit difference in the mediate chaining value and trace this difference forward and backward direction using the modular difference method to get a difference path with high probability. Because the IV is introduced in the four feed-forward steps as messages, we then adjust the differential path slightly so that the differences in IV can be used to cancel some difference of the the feed-forward steps.

For the SIMD-256, we introduce 1-bit initial difference in the last ladder of the 16-th step, and go 16 steps in the backward direction to obtain the initial difference, then we trace this difference in the forward direction for 4 steps to get a 20-step differential path which is shown in Table 1. From the Table 1, we observe that the difference $d_{20}[-18]$ of the forth ladder can be canceled by introducing a difference in d_0 of the first ladder. And then we expand the difference $b_0[-13]$ to $b_0[13, 14, ..., -18]$ to offset the impact in the computation of a_1 of the first ladder. This way, we go forward another four steps under the specific IV difference to get the difference in the chaining values of the feed-forward. It's easy to compute the probability of the differential path of Table 1 which holds with probability 2^{-203} for the selected IV difference. The sufficient conditions for the path of Table 1 is given in Table 2.

3.2 Message/IV Modification

In order to get a free-start near collision, we need to carry out the message or IV modification technique to fulfill the conditions in the IV and the chaining vales in the first round. In this section, we use the message/IV modification to fulfill the conditions in IV and a_1, a_2, a_3, and a_4. For convenient to describe, we denote the chaining values x_i in the j ladder x_i^j.

1. From the Table 2, there are 41 conditions in IV (a_0, b_0, c_0 and d_0 of the four ladders). These conditions can be satisfied by choosing the IV values freely.
2. There are 23 conditions in a_1^j,$j = 0, 1, 2, 3$, and these conditions can be satisfied by modifying the corresponding d_0^j. From the step update formula
$$a_1^j = (d_0^j + w_0^j + IF(a_0^j, b_0^j, c_0^j)) <<< 23 + a_0^{p(j)},$$
if the i-th bit in a_1^j doesn't satisfied, it's enough to set $d_0^j = d_0^j \oplus 2^{(i-24)mod32}$.
3. There are 12 conditions in a_2^j, $j = 0, 1, 2, 3$. From the trace
$$a_{2,i}^j \rightarrow d_{1,(i-17)mod32}^j \rightarrow c_{0,(i-17)mod32}^j,$$
the i-th bit of a_2^j can be modified by negating the $(i - 17)mod32$ bit of c_0^j. In the same way, we need to set the additional condition $a_{0,(i-17)mod32}^j = 1$ so that the change in c_0^j can not impact the output of a_1^j.
4. There are 10 conditions in a_3^j, $j = 0, 1, 2, 3$. From the trace
$$a_{3,i}^j \rightarrow d_{2,(i-27)mod32}^j \rightarrow c_{1,(i-27)mod32}^j \rightarrow b_{0,(i-27)mod32}^j,$$
the i-th bit of a_3^j can be modified by negating the $(i-27)mod32$ bit of b_0^j. We have to set the additional conditions $a_{0,(i-27)mod32}^j = 0$ and $a_{1,(i-27)mod32}^j = 1$ so that the change in b_0^j can not impact the output of a_1^j and a_2^j.
5. There are 10 conditions in a_4^j, $j = 0, 1, 2, 3$. From the trace
$$a_{4,i}^j \rightarrow d_{3,(i-3)mod32}^j \rightarrow c_{2,(i-3)mod32}^j \rightarrow b_{1,(i-3)mod32}^j \rightarrow a_{0,(i-3)mod32}^j,$$
the i-th bit of a_4^j can be modified by negating the bit $a_{0,(i-3)mod32}^j$. The additional conditions $b_{0,(i-3)mod32}^j = c_{0,(i-3)mod32}^j$ and $a_{1,(i-3)mod32}^j = 0$, and $a_{2,(i-3)mod32}^j = 1$ are needed so that the change in b_0^j can not impact the output of a_1^j and a_2^j and a_3^j. Furthermore, the change of $a_{0,(i-3)mod32}^j$ will cause the change in $a_1^{p(j)}$, we have to adjust the value of $d_0^{p(j)}$ to cancel this change.

In fact, we can also modify the conditions in a_5 and a_6, even a_7 and a_8, but it's more expensive and need to set many pre-conditions. It's worth to note that the conditions $a_{2,11}^1$, $a_{3,8}^0$, $a_{3,14}^3$ and $a_{3,18}^3$ can not be modified using the IV modification, because the additional conditions needed to modify these bits are contradict with the fix conditions in Table 2. We can modify these four conditions by the corresponding message. Due to the message expansion, we can not select the message completely arbitrary. So we use the IV modification as much as possible instead of message modification .

After the message/IV modification for the IV and $a_1 \sim a_4$, the differential path in Table 1 hold with probability 2^{-107}. This way, we can find a 25-bit free-start near collision for the 20-step SIMD-256 with complexity 2^{107} which is higher than the birthday attack.

4 Free-start Near Collision and Distinguishing Attack on SIMD-512

4.1 Free-start near collision attack for the compression function of 24-step SIMD-512

In this section, we will show that finding a free-start near collision for the 24-step SIMD-512 can be done with less effort than the birthday attack using our differential path. Similar to the Section 3, we introduce the 1-bit difference in chaining value of the 20-th step, and trace the difference in the forward and backward direction using the modular difference method. We get a near-collision differential path for 24-step SIMD-512 in Table 3. The probability for the differential path hold is about 2^{-352}. We utilize the message/IV modification technique to fulfill the 144 conditions in IV and $a_1 \sim a_4$. After the message/IV modification, the complexity to find a 47-bit free-start near collision for 24-step SIMD-512 is about 2^{208}.

4.2 A differential distinguisher for the compression function of full SIMD-512

Our strategy to find a differential path for the full SIMD-512 is different from that of the 24-step near collision differential path. We also start from 1-bit difference in the the 24-th step and trace this difference in backward direction. We expand the difference completely from the 8-th down to 3-th step, and shrink the difference from the 2-th step so that we can get the IV difference as little as possible. The differential distinguisher for the full SIMD-512 compression function is shown in Table 4, and its most expensive part focus on 3-9 steps.

The numbers of conditions on a_8, b_8, c_8, d_8, d_7, d_6, d_5, d_4 are as follows.

h_8	d_7	d_6	d_5	d_4
176	90	82	83	36

So we start from the chaining values h_8 and go in the backward and forward direction to compute the IV and output h_{36}. and the distinguishing algorithm for the full compression function of SIMD-512 are as follows.

1. Select a 1024-bit chaining values h_8 and a 1024-bit message M randomly, and let $h'_8 = h_8 \oplus \Delta h_8$ where Δh_8 is the difference in step 8. Modify h_8 to satisfy the 176 conditions. Compute the chaining values h_7 to h_4 and h'_7 to h'_4 in the backward directions.
2. Modify the conditions in d_7, d_6, d_5 and d_4 by the expanded message w_8, w_7, w_6 and w_5 respectively. Update the message M according to the 1024-bit expanded message w_5, w_6, w_7 and w_8 and compute the new expanded message.
3. Compute the chaining values $h_3 \sim h_0$ and $h'_3 \sim h'_0$ in the backward directions. If Δh_0 is equal to fixed difference ΔIV in Table 5, go to step 4; Otherwise, return step 1.

4. Compute $h_9 \sim h_{36}$ and $h'_9 \sim h'_{36}$ in the forward direction using h_8 and h'_8. If the differences Δh_{36} is equal to the fixed output difference in Table 5, stop; Otherwise, go back step 1.

By running the algorithm above, we can find a pair (M, IV) and (M, IV') which has the fixed input and output differences in Table 5 with complexity about 2^{398}. By using the more sophisticated message/IV modification techniques, the complexity can be improved furtherly. But for the random function with output length n-bit, to find a pair plain (P, P') which satisfy the fixed input and output difference has the probability 2^{-n}. So our differential distinguisher is applicable for both the compression function and the final compression function of SIMD.

5 Conclusions

In this paper, we find some differential paths using the modular difference method for reduced and full SIMD compression functions. Based on our differential path, we give the free-start near collision and distinguisher attack for the SIMD. Our attack does not contract with the security claims of the designer.

References

1. E.Biham, R.Chen, A.Joux, P.Carribault, C. Lemuet and W.Jalby, Collisions of SHA-0 and reduced SHA-1. Eurocrypt 2005, LNCS 3498, pp. 36-57, 2005.
2. D.khovratovich and I. Nikolic, Rotational Cryptanalysis of ARX, FSE 2010.
3. F.Mendel, T. Nad, A Distinguisher for the Compression Function of SIMD-512, Indocrypt 2009, LNCS 5922, pp.219-233, 2009.
4. G. Leurent, C.Bouillaguet, P.A.Fouque, SIMD Is a Message Digest. Submission to NIST(round 2), 2009.
5. National Institute of Standards and Technoloy: Annoucing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. Available online at: http://nist.gov.
6. I.Nikolić, J.Pieprzyk, etc., Rotational Cryptanalysis of (Modified) Versions of BMW and SIMD. Available at http://ehash.iaik.tugraz.at/wiki/SIMD.
7. X.Y. Wang, H.B. Yu, How to Break MD5 and Other Hash Functions, Eurocrypt'05, LNCS 3494, pp.19-35, 2005.
8. X.Y. Wang, Y.L. Yin, H.B. Yu, Finding collisions on the Full SHA-1, Crypto 2005, LNCS 3621, pp.17-36, 2005.

Table 1. The differential path for 20-step SIMD-256.

step	r	s	The first ladder	The second ladder	The third ladder	The forth ladder	pr
0			a_{0} $b_{0}[13, 14, \ldots, -18]$ c_{0} $d_{0}[18]$	a_{0} $b_{0}[7, 13]$ $c_{0}[-21, 26]$ d_{0}	$a_{0}[7, -3]$ $b_{0}[-1]$ $c_{0}[-32]$ d_{0}	a_{0} $b_{0}[-19, 20, 23, 24, -25]$ c_{0} $d_{0}[15]$	2^{-20}
1	3	23	a_{1} b_{1} $c_{1}[13, 14 \ldots, -18]$ d_{1}	a_{1} b_{1} $c_{1}[7, 13]$ $d_{1}[-21, 26]$	a_{1} $b_{1}[-6, 10]$ $c_{1}[-1]$ $d_{1}[-32]$	$a_{1}[15]$ b_{1} $c_{1}[-19, 20, 23, 24, -25]$ d_{1}	2^{-20}
2	23	17	a_{2} b_{2} c_{2} $d_{2}[13, 14, \ldots - 18]$	$a_{2}[-11, -12, -13, -14, 15]$ b_{2} c_{2} $d_{2}[7, 13]$	$a_{2}[-17]$ b_{2} $c_{2}[-6, 10]$ $d_{2}[-1]$	a_{2} $b_{2}[6]$ c_{2} $d_{2}[-19, 20, 23, 24, -25]$	2^{-13}
3	17	27	$a_{3}[-8]$ b_{3} c_{3} d_{3}	a_{3} $b_{3}[-28, -29, -30, -31, 32]$ c_{3} d_{3}	a_{3} $b_{3}[-2]$ c_{3} $d_{3}[-6, 10]$	$a_{3}[14, -18]$ b_{3} $c_{3}[6]$ d_{3}	2^{-12}
4	27	3	a_{4} $b_{4}[-3]$ c_{4} d_{4}	a_{4} b_{4} $c_{4}[-28, -29, -30, -31, 32]$ d_{4}	a_{4} b_{4} $c_{4}[-2]$ d_{4}	a_{4} $b_{4}[9, -13]$ c_{4} $d_{4}[6]$	2^{-10}
5	3	23	a_{5} b_{5} $c_{5}[-3]$ d_{5}	a_{5} b_{5} c_{5} $d_{5}[-28, -29, -30, -31, 32]$	a_{5} b_{5} c_{5} $d_{5}[-2]$	$a_{5}[29]$ b_{5} $c_{5}[9, -13]$ d_{5}	2^{-10}
6	23	17	a_{6} b_{6} c_{6} $d_{6}[-3]$	$a_{6}[-13, -14, 15]$ b_{6} c_{6} d_{6}	$a_{6}[-19]$ b_{6} c_{6} d_{6}	a_{6} $b_{6}[20]$ c_{6} $d_{6}[9, -13]$	2^{-8}
7	17	27	a_{7} b_{7} c_{7} d_{7}	a_{7} $b_{7}[-30, -31, 32]$ c_{7} d_{7}	a_{7} $b_{7}[-4]$ c_{7} d_{7}	$a_{7}[-8]$ b_{7} $c_{7}[20]$ d_{7}	2^{-6}
8	27	3	a_{8} b_{8} c_{8} d_{8}	a_{8} b_{8} $c_{8}[-30, -31, 32]$ d_{8}	a_{8} b_{8} $c_{8}[-4]$ d_{8}	a_{8} $b_{8}[-3]$ c_{8} $d_{8}[20]$	2^{-6}
9	28	19	a_{9} b_{9} c_{9} d_{9}	a_{9} b_{9} c_{9} $d_{9}[-30, -31, 32]$	a_{9} b_{9} c_{9} $d_{9}[-4]$	$a_{9}[7]$ b_{9} $c_{9}[-3]$ d_{9}	2^{-6}
10	19	22	a_{10} b_{10} c_{10} d_{10}	$a_{10}[20]$ b_{10} c_{10} d_{10}	a_{10} b_{10} c_{10} d_{10}	a_{10} $b_{10}[26]$ c_{10} $d_{10}[-3]$	2^{-3}
11	22	7	a_{11} b_{11} c_{11} d_{11}	a_{11} $b_{11}[10]$ c_{11} d_{11}	a_{11} b_{11} c_{11} d_{11}	a_{11} b_{11} $c_{11}[26]$ d_{11}	2^{-2}
12	7	28	a_{12} b_{12} c_{12} d_{12}	a_{12} b_{12} $c_{12}[10]$ d_{12}	a_{12} b_{12} c_{12} d_{12}	a_{12} b_{12} c_{12} $d_{12}[26]$	2^{-2}
13	28	19	a_{13} b_{13} c_{13} d_{13}	a_{13} b_{13} c_{13} $d_{13}[10]$	a_{13} b_{13} c_{13} d_{13}	$a_{13}[13]$ b_{13} c_{13} d_{13}	2^{-2}
14	19	22	a_{14} b_{14} c_{14} d_{14}	a_{14} b_{14} c_{14} d_{14}	a_{14} b_{14} c_{14} d_{14}	a_{14} $b_{14}[32]$ c_{14} d_{14}	2^{-1}
15	22	7	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} $c_{15}[32]$ d_{15}	2^{-1}
16	7	28	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} $d_{16}[32]$	2^{-1}
17	29	9	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	$a_{17}[-9]$ b_{17} c_{17} d_{17}	2^{-1}
18	9	15	$a_{18}[-18]$ b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} $b_{18}[-18]$ c_{18} d_{18}	2^{-2}
19	15	5	a_{19} $b_{19}[-1]$ c_{19} d_{19}	$a_{19}[1, -2]$ b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} $c_{19}[-18]$ d_{19}	2^{-4}
20	5	29	a_{20} b_{20} $c_{20}[-1]$ d_{20}	a_{20} $b_{20}[6, -7]$ c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	$a_{20}[-6]$ b_{20} c_{20} $d_{20}[-18]$	2^{-5}
21	4	13	$a_{21}[-10]$ b_{21} c_{21} $d_{21}[-1]$	$a_{21}[-26]$ b_{21} $c_{21}[6, -7]$ d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} $b_{21}[-10]$ c_{21} d_{21}	2^{-6}
22	13	10	$a_{22}[-7, -11]$ $b_{22}[-23]$ c_{22} d_{22}	a_{22} $b_{22}[-7]$ c_{22} $d_{22}[6, -7]$	$a_{22}[4, 31, -32]$ b_{22} c_{22} d_{22}	a_{22} b_{22} $c_{22}[-10]$ d_{22}	2^{-10}
23	10	25	$a_{23}[-9, 14, -28]$ $b_{23}[-17, -21]$ $c_{23}[-23]$ d_{23}	$a_{23}[-26, -31]$ b_{23} $c_{23}[-7]$ d_{23}	$a_{23}[-17, -21]$ $b_{23}[9, -10, 14]$ c_{23} d_{23}	$a_{23}[1, 27]$ b_{23} c_{23} $d_{23}[-10]$	2^{-16}
24	25	4	a_{24} $b_{24}[-2, 7, 21]$ $c_{24}[-17, -21]$ $d_{24}[-23]$	$a_{24}[-10, -14, 23, -27]$ $b_{24}[-19, -24]$ c_{24} $d_{24}[-7]$	$a_{24}[-19, -24]$ $b_{24}[-10, -14]$ $c_{24}[9, -10, 14]$ d_{24}	$a_{24}[-2, 7, -14, 19, -21]$ b_{24} c_{24} d_{24}	2^{-25}

Table 2. The sufficient conditions for the differential path of 20-step SIMD-256.

step	L_0	L_1	L_2	L_3
a_0	$a_{0,13} = 0$, $a_{0,14} = 0$, $a_{0,15} = 0$, $a_{0,16} = 0$, $a_{0,17} = 0$, $a_{0,18} = 1$	$a_{0,7} = 0$, $a_{0,10} = 0$, $a_{0,13} = 0$, $a_{0,21} = 1$, $a_{0,26} = 1$	$a_{0,1} = 0$, $a_{0,3} = 1$, $a_{0,7} = 0$, $a_{0,32} = 1$	$a_{0,19} = 1$, $a_{0,20} = 0$, $a_{0,23} = 0$, $a_{0,24} = 1$, $a_{0,25} = 0$
b_0	$b_{0,13} = 0$, $b_{0,14} = 0$, $b_{0,15} = 0$, $b_{0,16} = 0$, $b_{0,17} = 0$, $b_{0,18} = 1$	$b_{0,7} = 0$, $b_{0,13} = 0$	$b_{0,1} = 1$	$b_{0,15} = a_{0,12}$, $b_{0,19} = 1$, $b_{0,20} = 0$, $b_{0,23} = 0$, $b_{0,24} = 0$, $b_{0,25} = 1$
c_0		$c_{0,21} = 1$, $c_{0,26} = 0$	$c_{0,3} = b_{0,3}$, $c_{0,7} = b_{0,7}$	
d_0	$d_{0,18} = 0$			$d_{0,15} = 0$
a_1	$a_{1,13} = 1$, $a_{1,14} = 1$, $a_{1,15} = 1$, $a_{1,16} = 1$, $a_{1,17} = 1$, $a_{1,18} = 1$	$a_{1,7} = 1$, $a_{1,13} = 1$, $a_{1,20} = a_{0,8}$, $a_{1,21} = a_{0,9}$, $a_{1,22} = 1$, $a_{1,23} = a_{0,11}$, $a_{1,24} = a_{0,12}$	$a_{1,6} = 0$, $a_{1,10} = 0$, $a_{1,1} = 1$, $a_{1,26} = a_{0,14}$	$a_{1,15} = 0$, $a_{1,19} = 1$, $a_{1,20} = 1$, $a_{1,23} = 1$, $a_{1,24} = 1$, $a_{1,25} = 1$
a_2	$a_{2,23} = a_{1,17}$	$a_{2,11} = 1$, $a_{2,12} = 1$, $a_{2,13} = 1$, $a_{2,14} = 1$, $a_{2,15} = 0$	$a_{2,6} = 1$, $a_{2,10} = 1$, $a_{2,17} = 1$	$a_{2,1} = a_{1,27}$, $a_{2,6} = 0$, $a_{2,29} = a_{1,23}$
a_3	$a_{3,8} = 1$	$a_{3,28} = 0$, $a_{3,29} = 0$, $a_{3,30} = 0$, $a_{3,31} = 0$, $a_{3,32} = 1$	$a_{3,2} = 0$	$a_{3,6} = 1$, $a_{3,14} = 0$, $a_{3,18} = 1$
a_4	$a_{4,3} = a_{2,18}$	$a_{4,28} = a_{3,1}$, $a_{4,29} = a_{3,2}$, $a_{4,30} = a_{3,3}$, $a_{4,31} = b_{3,4}$, $a_{4,32} = a_{3,5}$	$a_{4,2} = a_{3,7}$	$a_{4,9} = a_{3,14}$, $a_{4,13} = a_{3,18}$, $a_{4,26} = a_{3,2}$
a_5	$a_{5,3} = a_{4,32}$	$a_{5,22} = a_{4,10}$, $a_{5,23} = a_{4,11}$, $a_{5,24} = a_{4,12}$	$a_{5,28} = a_{4,16}$	$a_{5,29} = 0$, $a_{5,9} = a_{4,6}$, $a_{5,13} = a_{4,10}$
a_6		$a_{6,13} = 1$, $a_{6,14} = 1$, $a_{6,15} = 0$	$a_{6,19} = 1$	$a_{6,20} = a_{4,17}$, $a_{6,23} = a_{5,17}$
a_7		$a_{7,30} = a_{5,7}$, $a_{7,31} = a_{5,8}$, $a_{7,32} = a_{5,9} \oplus 1$	$a_{7,4} = a_{5,13}$	$a_{7,8} = 1$, $a_{7,20} = a_{6,3}$
a_8		$a_{8,30} = 1$, $a_{8,31} = 1$, $a_{8,32} = 1$	$a_{8,4} = 1$	$a_{8,3} = 0$, $a_{8,11} = a_{7,12}$
a_9		$a_{9,1} = a_{8,24}$		$a_{9,3} = 1$, $a_{9,7} = 0$
a_{10}		$a_{10,20} = 0$		$a_{10,26} = 0$
a_{11}		$a_{11,10} = 0$		$a_{11,26} = 1$
a_{12}		$a_{12,10} = a_{11,3}$		$a_{12,17} = a_{11,6}$
a_{13}				$a_{13,13} = 0$
a_{14}				$a_{14,32} = a_{12,4}$
a_{15}				$a_{15,32} = a_{14,10}$
a_{16}				$a_{16,12} = a_{15,2}$
a_{17}	$a_{17,9} = a_{16,21}$			$a_{17,9} = 1$
a_{18}	$a_{18,18} = 1$	$a_{18,18} = a_{17,24}$, $a_{18,19} = a_{17,25}$		$a_{18,18} = 0$
a_{19}	$a_{19,1} = 0$	$a_{19,1} = 0$, $a_{19,2} = 1$,		$a_{19,1} = a_{18,23}$, $a_{19,18} = 1$
a_{20}	$a_{20,1} = 1$, $a_{20,3} = 0$, $a_{20,6} = a_{19,5}$	$a_{20,6} = 0$, $a_{20,7} = 0$, $a_{20,22} = a_{19,21}$		$a_{20,6} = 1$
a_{21}	$a_{21,10} = 1$, $a_{21,26} = 1$, $a_{21,30} = a_{20,7}$,	$a_{21,6} = 0$, $a_{21,7} = 0$, $a_{21,26} = 1$,	$a_{21,23} = a_{20,32}$, $a_{21,18} = a_{20,27}$, $a_{21,19} = a_{20,28} \oplus 1$	$a_{21,10} = 0$
a_{22}	$a_{22,7} = 1$, $a_{22,11} = 1$, $a_{22,23} = 0$, $a_{22,31} = a_{21,28}$, $a_{22,4} = a_{21,1}$, $a_{22,18} = a_{21,15}$	$a_{22,7} = 0$, $a_{22,16} = a_{21,13}$, $a_{22,21} = a_{21,18}$	$a_{22,4} = 0$, $a_{22,7} = a_{21,4}$, $a_{22,11} = a_{21,8}$, $a_{22,31} = 0$, $a_{22,32} = 1$	$a_{22,10} = 1$
a_{23}	$a_{23,9} = 1$, $a_{23,14} = 0$, $a_{23,28} = 1$, $a_{23,17} = 0$, $a_{23,21} = 0$, $a_{23,23} = 1$	$a_{23,7} = 1$, $a_{23,26} = 1$, $a_{23,31} = 1$	$a_{23,9} = 0$, $a_{23,10} = 0$, $a_{23,14} = 0$ $a_{23,17} = 1$, $a_{23,21} = 1$	
a_{24}		$a_{24,10} = 1$, $a_{24,14} = 1$, $a_{24,23} = 0$, $a_{24,27} = 1$	$a_{24,19} = 1$, $a_{24,24} = 1$	$a_{24,2} = 1$, $a_{24,7} = 0$, $a_{24,14} = 1$, $a_{24,19} = 0$, $a_{24,21} = 1$

Table 3. The near-collision differential path for 24-step SIMD-512.

step	r	s	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	pr
0			$a_0[6]$ $b_0[-8]$ $c_0[28]$ d_0	a_0 $b_0[-1, \ldots, -7, 8, 15]$ c_0 $d_0[-18]$	$a_0[-17]$ b_0 c_0 $d_0[-4]$	$a_0[24]$ $b_0[-15]$ $c_0[7, 8, \ldots, -13]$ $d_0[-12, 29]$	$a_0[2, -11]$ b_0 $c_0[21]$ d_0	a_0 $b_0[-16]$ $c_0[-14]$ $d_0[-10, 23]$	$a_0[32]$ $b_0[-28]$ c_0 $d_0[-31]$	a_0 $b_0[-18, 27]$ c_0 $d_0[6, 12]$	2^{-38}
1	3	23	a_1 $b_1[9]$ $c_1[-8]$ $d_1[28]$	a_1 b_1 $c_1[-1, \ldots - 7, 8, 15]$ d_1	a_1 $b_1[-20]$ c_1 d_1	a_1 $b_1[27]$ $c_1[-15]$ $d_1[7, 8, \ldots, -13]$	a_1 $b_1[5, -14]$ c_1 $d_1[21]$	$a_1[-1]$ b_1 $c_1[-16]$ $d_1[-14]$	$a_1[-22]$ $b_1[3]$ $c_1[-28]$ d_1	$a_1[-29, 30]$ b_1 $c_1[-18, 27]$ d_1	2^{-35}
2	23	17	a_2 b_2 $c_2[9]$ $d_2[-8]$	$a_2[25]$ b_2 c_2 $d_2[-1, \ldots, -7, 8, 15]$	a_2 b_2 $c_2[-20]$ d_2	$a_2[-25]$ b_2 $c_2[27]$ $d_2[-15]$	$a_2[6]$ b_2 $c_2[5, -14]$ d_2	$a_2[-31]$ $b_2[24]$ c_2 $d_2[-16]$	a_2 $b_2[-13]$ $c_2[3]$ $d_2[-28]$	a_2 $b_2[-20, 21]$ c_2 $d_2[-18, 27]$	2^{-29}
3	17	27	$a_3[-3]$ b_3 c_3 $d_3[9]$	$a_3[28]$ $b_3[10]$ c_3 d_3	a_3 b_3 c_3 $d_3[-20]$	a_3 $b_3[-10]$ c_3 $d_3[27]$	a_3 $b_3[23]$ c_3 $d_3[5, -14]$	$a_3[-11]$ $b_3[-16]$ $c_3[-24]$ d_3	a_3 b_3 $c_3[-13]$ $d_3[3]$	$a_3[-13, 22]$ b_3 $c_3[-20, 21]$ d_3	2^{-19}
4	27	3	$a_4[-12, -13, -14, 15]$ $b_4[-30]$ c_4 d_4	a_4 $b_4[23]$ $c_4[10]$ d_4	a_4 b_4 c_4 d_4	a_4 b_4 $c_4[-10]$ d_4	a_4 b_4 $c_4[23]$ d_4	a_4 $b_4[-6]$ $c_4[-16]$ $d_4[-24]$	a_4 b_4 c_4 $d_4[-13]$	a_4 $b_4[-8, 17]$ c_4 $d_4[-20, 21]$	2^{-17}
5	3	23	a_5 $b_5[-15, -16, -17, 18]$ $c_5[-30]$ d_5	a_5 b_5 $c_5[23]$ $d_5[10]$	a_5 b_5 c_5 d_5	a_5 b_5 c_5 $d_5[-10]$	a_5 b_5 c_5 $d_5[23]$	a_5 b_5 $c_5[-6]$ $d_5[-16]$	$a_5[4, -5]$ b_5 c_5 d_5	$a_5[11]$ b_5 $c_5[-8, 17]$ d_5	2^{-16}
6	23	17	a_6 b_6 $c_6[-15, -16, -17, 18]$ $d_6[-30]$	a_6 b_6 c_6 $d_6[23]$	$a_6[-27]$ b_6 c_6 d_6	$a_6[8]$ b_6 c_6 d_6	$a_6[-1]$ b_6 c_6 d_6	a_6 b_6 c_6 $d_6[-6]$	a_6 $b_6[27, -28]$ c_6 d_6	a_6 $b_6[2]$ c_6 $d_6[-8, 17]$	2^{-15}
7	17	27	a_7 b_7 c_7 $d_7[-15, -16, -17, 18]$	a_7 b_7 c_7 d_7	a_7 b_7 c_7 d_7	a_7 $b_7[-12]$ c_7 d_7	a_7 $b_7[25]$ c_7 d_7	$a_7[-1]$ $b_7[-18]$ c_7 d_7	a_7 b_7 $c_7[27, -28]$ d_7	$a_7[-3]$ b_7 $c_7[2]$ d_7	2^{-12}
8	27	3	$a_8[-18, -19, -20, 21]$ b_8 c_8 d_8	a_8 b_8 c_8 d_8	a_8 b_8 c_8 d_8	a_8 b_8 $c_8[-12]$ d_8	a_8 b_8 $c_8[25]$ d_8	a_8 $b_8[-28]$ $c_8[-18]$ d_8	a_8 b_8 c_8 $d_8[27, -28]$	a_8 $b_8[-30]$ c_8 $d_8[2]$	2^{-12}
9	28	19	a_9 $b_9[-14, -15, -16, 17]$ c_9 d_9	a_9 b_9 c_9 d_9	a_9 b_9 c_9 d_9	a_9 b_9 c_9 $d_9[-12]$	a_9 b_9 c_9 $d_9[25]$	a_9 b_9 $c_9[-28]$ $d_9[-18]$	a_9 b_9 c_9 d_9	$a_9[21]$ b_9 $c_9[-30]$ d_9	2^{-10}
10	19	22	a_{10} b_{10} $c_{10}[-14, -15, -16, 17]$ d_{10}	a_{10} b_{10} c_{10} d_{10}	a_{10} b_{10} c_{10} d_{10}	$a_{10}[-2]$ b_{10} c_{10} d_{10}	$a_{10}[15]$ b_{10} c_{10} d_{10}	a_{10} b_{10} c_{10} $d_{10}[-28]$	a_{10} b_{10} c_{10} d_{10}	a_{10} $b_{10}[8]$ c_{10} $d_{10}[-30]$	2^{-9}
11	22	7	a_{11} b_{11} c_{11} $d_{11}[-14, -15, -16, 17]$	a_{11} b_{11} c_{11} d_{11}	a_{11} b_{11} c_{11} d_{11}	a_{11} $b_{11}[-24]$ c_{11} d_{11}	a_{11} $b_{11}[5]$ c_{11} d_{11}	$a_{11}[-3]$ b_{11} c_{11} d_{11}	a_{11} b_{11} c_{11} d_{11}	a_{11} b_{11} $c_{11}[8]$ d_{11}	2^{-8}
12	7	28	a_{12} b_{12} c_{12} d_{12}	a_{12} b_{12} c_{12} d_{12}	a_{12} b_{12} c_{12} d_{12}	a_{12} b_{12} $c_{12}[-24]$ d_{12}	a_{12} b_{12} $c_{12}[5]$ d_{12}	a_{12} $b_{12}[-10]$ c_{12} $d_{12}[8]$	a_{12} b_{12} c_{12} d_{12}	a_{12} b_{12} c_{12} d_{12}	2^{-4}
13	28	19	a_{13} b_{13} c_{13} d_{13}	a_{13} b_{13} c_{13} d_{13}	a_{13} b_{13} c_{13} d_{13}	a_{13} b_{13} c_{13} $d_{13}[-24]$	a_{13} b_{13} c_{13} $d_{13}[5]$	a_{13} b_{13} $c_{13}[-10]$ d_{13}	a_{13} b_{13} c_{13} d_{13}	$a_{13}[27]$ b_{13} c_{13} d_{13}	2^{-4}
14	19	22	a_{14} b_{14} c_{14} d_{14}	a_{14} b_{14} c_{14} d_{14}	a_{14} b_{14} c_{14} d_{14}	a_{14} b_{14} c_{14} d_{14}	$a_{14}[27]$ b_{14} c_{14} d_{14}	a_{14} b_{14} c_{14} $d_{14}[-10]$	a_{14} $b_{14}[14]$ c_{14} d_{14}	a_{14} b_{14} c_{14} d_{14}	2^{-3}
15	22	7	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} $b_{15}[17]$ c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} c_{15} d_{15}	a_{15} b_{15} $c_{15}[14]$ d_{15}	2^{-2}
16	7	28	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} $c_{16}[17]$ d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} $d_{16}[14]$	2^{-2}
17	29	9	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} $d_{17}[17]$	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	$a_{17}[23]$ b_{17} c_{17} d_{17}	2^{-2}
18	9	15	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} $b_{18}[32]$ c_{18} d_{18}	2^{-1}
19	15	5	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} $c_{19}[32]$ d_{19}	2^{-1}
20	5	29	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} $d_{20}[32]$	2^{-1}

step	r	s	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	pr
21	29	9	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	$a_{21}[9]$ b_{21} c_{21} d_{21}	2^{-1}
22	9	15	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	$a_{22}[18]$ b_{22} c_{22} d_{22}	a_{22} $b_{22}[18]$ c_{22} d_{22}	2^{-2}
23	15	5	$a_{23}[-1, 2]$ b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} $b_{23}[1]$ c_{23} d_{23}	a_{23} b_{23} $c_{23}[18]$ d_{23}	2^{-4}
24	5	29	a_{24} $b_{24}[-6, 7]$ c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	$a_{24}[6]$ b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} $c_{24}[1]$ d_{24}	a_{24} b_{24} c_{24} $d_{24}[18]$	2^{-5}
25	4	13	a_{25} b_{25} $c_{25}[-6, 7]$ d_{25}	$a_{25}[10, 21, -22]$ b_{25} c_{25} d_{25}	$a_{25}[9]$ $b_{25}[10]$ c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	$a_{25}[-14, 15, 28]$ b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} $d_{25}[1]$	a_{25} b_{25} c_{25} d_{25}	2^{-11}
26	13	10	$a_{26}[9]$ b_{26} c_{26} $d_{26}[-6, 7]$	a_{26} $b_{26}[2, -3, 23]$ c_{26} d_{26}	a_{26} $b_{26}[22]$ $c_{26}[10]$ d_{26}	$a_{26}[-14]$ b_{26} c_{26} d_{26}	$a_{26}[23]$ b_{26} c_{26} d_{26}	a_{26} $b_{26}[9, -27, 28]$ c_{26} d_{26}	$a_{26}[-11, -17]$ b_{26} c_{26} d_{26}	$a_{26}[7]$ b_{26} c_{26} d_{26}	2^{-16}
27	10	25	$a_{27}[-4, 17, 27, 31]$ $b_{27}[19]$ c_{27} d_{27}	$a_{27}[-21]$ b_{27} $c_{27}[2, -3, 23]$ d_{27}	$a_{27}[14]$ b_{27} $c_{27}[22]$ $d_{27}[10]$	$a_{27}[1]$ $b_{27}[-24]$ c_{27} d_{27}	$a_{27}[-24]$ $b_{27}[1]$ c_{27} d_{27}	$a_{27}[-9]$ b_{27} $c_{27}[9, -27, 28]$ d_{27}	$a_{27}[-7]$ $b_{27}[-21, -27]$ c_{27} d_{27}	$a_{27}[-3, 16, 19]$ $b_{27}[17]$ c_{27} d_{27}	2^{-27}
28	25	4	$a_{28}[4, -17]$ $b_{28}[10, 20 -24, -29]$ $c_{28}[19]$ d_{28}	$a_{28}[-2, 32]$ $b_{28}[-14]$ c_{28} $d_{28}[2, -3, 23]$	$a_{28}[14, -32]$ $b_{28}[7]$ c_{28} $d_{28}[22]$	$a_{28}[-3, 9, 12, -28]$ $b_{28}[26]$ $c_{28}[-24]$ $d_{28}[12]$	$a_{28}[10, 20, -24, -29]$ $b_{28}[17]$ $c_{28}[1]$ d_{28}	$a_{28}[-14, -22]$ $b_{28}[-2]$ $c_{28}[9, -27, 28]$ d_{28}	$a_{28}[7]$ $b_{28}[-32]$ $c_{28}[-21, -27]$ d_{28}	$a_{28}[10, 16, 26]$ $b_{28}[9, 12, -28]$ $c_{28}[17]$ d_{28}	2^{-46}

Table 4. The differential path for full SIMD-512.

step	r	s	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	pr
0			a_0	$a_0[23, -24]$	$a_0[-3, 26, -27]$	$a_0[6]$	$a_0[11, 20, -21, 29]$	a_0	$a_0[-4, -23, 32]$	a_0	2^{-45}
			b_0	$b_0[-1, -15, 19]$	b_0	b_0	b_0	$b_0[-7, -8, 9]$	$b_0[10]$	$b_0[4, 7, -11, -13, 24, -27]$	
			$c_0[-3]$	c_0	$c_0[-17, -18, 19]$	$c_0[8, 26]$	$c_0[-3]$	$c_0[-4, -17, 32]$	c_0	c_0	
			d_0	d_0	d_0	$d_0[-4, 15]$	d_0	$d_0[-23]$	d_0	$d_0[3, -12, 16, 30]$	
1	3	23	a_1	a_1	$a_1[5, -18, -19, -20, -21, 22]$	$a_1[-27, 31]$	$a_1[11]$	a_1	a_1	$a_1[21]$	2^{-47}
			b_1	$b_1[26, -27]$	$b_1[-6, 29, -30]$	$b_1[9]$	$b_1[14, 23, -24, 32]$	b_1	$b_1[3, -7, -26]$	b_1	
			c_1	$c_1[-1, -15, 19]$	c_1	c_1	c_1	$c_1[-7, -8, 9]$	$c_1[10]$	$c_1[4, 7, -11, -13, 24, -27]$	
			$d_1[-3, -5]$	d_1	$d_1[-17, -18, 19]$	$d_1[8, 26]$	$d_1[-3]$	$d_1[-4, -17, 32]$	d_1	d_1	
2	23	17	$a_2[20, 21, -22]$	a_2	a_2	$a_2[11, 25]$	$a_2[20, 21, 22, 23, -24]$	$a_2[-2, -17, 21]$	a_2	a_2	2^{-49}
			b_2	b_2	$b_2[-9, -10, .., 13, 22]$	$b_2[-18, 22]$	$b_2[-2]$	b_2	b_2	$b_2[12]$	
			c_2	$c_2[26, -27]$	$c_2[-6, 29, -30]$	$c_2[9]$	$c_2[14, 23, -24, 32]$	c_2	$c_2[3, -7, -26]$	c_2	
			d_2	$d_2[-1, -15, 19]$	d_2	d_2	d_2	$d_2[-7, -8, 9]$	$d_2[10]$	$d_2[4, 7, -11, -13, 24, -27]$	
3	17	27	$a_3[17, 18, \ldots, -27]$	$a_3[-14, -15, \ldots, 19]$	a_3	a_3	$a_3[17]$	$a_3[2]$	a_3	$a_3[8, -9, 22, 23, \ldots, -29, -31, -32, 1]$	2^{-67}
			$b_3[5, 6, -7]$	b_3	b_3	$b_3[10, 28]$	$b_3[5, 6, 7 8, -9]$	$b_3[-2, 6, -19]$	b_3	b_3	
			c_3	c_3	$c_3[-9, -10, .., 13, 22]$	$c_3[-18, 22]$	$c_3[-2]$	c_3	c_3	$c_3[12]$	
			d_3	$d_3[26, -27]$	$d_3[29, -30]$	$d_3[9]$	$d_3[14, 23, -24, 32]$	d_3	$d_3[3, -7, -26]$	d_3	
4	27	3	a_4	$a_4[-22, 29]$	$a_4[-16, -17, \ldots, 22, -32]$	a_4	a_4	a_4	$a_4[-6, -7, -8, 9, -10]$	a_4	2^{-61}
			$b_4[12, 13, \ldots, -22]$	$b_4[-9, -10, \ldots, 14]$	b_4	b_4	$b_4[12]$	$b_4[29]$	b_4	$b_4[3, -4, 17, 18, \ldots, -24, -26, -27, 28]$	
			$c_4[5, 6, -7]$	c_4	c_4	$c_4[10, 28]$	$c_4[5, 6, 7 8, -9]$	$c_4[-2, 6, -19]$	c_4	c_4	
			d_4	d_4	$d_4[-9, -10] .., 13, 22]$	$d_4[-18, 22]$	$d_4[2]$	d_4	d_4	$d_4[12]$	
5	3	23	a_5	a_5	$a_5[13, -32]$	a_5	a_5	a_5	a_5	$a_5[-14, 15, -17]$	2^{-58}
			b_5	$b_5[-25, 32]$	$b_5[-3, 19]$	b_5	b_5	b_5	$b_5[-9, -10, -11, 12, -13]$	b_5	
			$c_5[12, 13, \ldots, -22]$	$c_5[-9, -10, \ldots, 14]$	c_5	c_5	$c_5[12]$	$c_5[29]$	c_5	$c_5[3, -4, 17, 18, \ldots, -24, -26, -27, 28]$	
			$d_5[5, 6, -7]$	d_5	d_5	$d_5[10, 28]$	$d_5[5, 6, 7 8, -9]$	$d_5[-2, 6, -19]$	d_5	d_5	
6	23	17	$a_6[3, -4, -22]$	a_6	a_6	$a_6[-13, -14, \ldots, 20, -27, -28, \ldots, 32]$	$a_6[22, 23, \ldots, -31]$	$a_6[-19]$	$a_6[-29, -30, -31, -32, -1, .., 6]$	a_6	2^{-84}
			b_6	b_6	$b_6[4, -23]$	b_6	b_6	b_6	b_6	$b_6[-5, 6, -7]$	
			c_6	$c_6[-25, 32]$	$c_6[-3, 19]$	c_6	c_6	c_6	$c_6[-9, -10, -11, 12, -13]$	c_6	
			$d_6[12, 13, \ldots, -22]$	$d_6[-9, -10, \ldots, 14]$	d_6	d_6	$d_6[12]$	$d_6[29]$	d_6	$d_6[3, -4, 17, 18, \ldots, -24, -26, -27, 28]$	
7	17	27	$a_7[-8]$	a_7	a_7	$a_7[-27]$	a_7	$a_7[-24, -25, \ldots, 29]$	a_7	$a_7[-21, -22, \ldots, 25]$	2^{-65}
			$b_7[-7, 20, -21]$	b_7	b_7	$b_7[-12, -13, \ldots 17, -30, -31, \ldots, 5]$	$b_7[7, 8, \ldots, -16]$	$b_7[-4]$	$b_7[14, 15, \ldots, -23]$	b_7	
			c_7	c_7	$c_7[4, -23]$	c_7	c_7	c_7	c_7	$c_7[-5, 6, -7]$	
			d_7	$d_7[-25, 32]$	$d_7[-3, 19]$	d_7	d_7	d_7	$d_7[9, -13]$	d_7	
8	27	3	$a_8[12]$	$a_8[-28]$	$a_8[-6]$	a_8	a_8	$a_8[28]$	$a_8[12]$	a_8	2^{-61}
			$b_8[-3]$	b_8	b_8	$b_8[-22]$	b_8	$b_8[-19, -20, \ldots, 24]$	b_8	$b_8[-16, 17, \ldots, 20]$	
			$c_8[-7, 20, -21]$	c_8	c_8	$c_8[-12, -13, \ldots 17, -30, -31, \ldots, 5]$	$c_8[7, 8, \ldots, -16]$	$c_8[-4]$	$c_8[14, 15, \ldots, -23]$	c_8	
			d_8	d_8	$d_8[4, -23]$	d_8	d_8	d_8	d_8	$d_8[-5, 6, -7]$	
9	28	19	a_9	$a_9[-15]$	$a_9[-10, 23]$	a_9	a_9	a_9	$a_9[10]$	$a_9[7, -26]$	2^{-65}
			$b_9[8]$	$b_9[-24]$	$b_9[-2]$	b_9	b_9	$b_9[24]$	$b_9[8]$	b_9	
			$c_9[-3]$	c_9	c_9	$c_9[-22]$	c_9	$c_9[-19, -20, \ldots, 24]$	c_9	$c_9[-16, -17, \ldots, 20]$	
			$d_9[-7, 20, -21]$	d_9	d_9	$d_9[-12, -13, \ldots 17, -30, -31, \ldots, 5]$	$d_9[7, 8, \ldots, -16]$	$d_9[-4]$	$d_9[14, 15, \ldots, -23]$	d_9	
10	19	22	a_{10}	a_{10}	a_{10}	$a_{10}[20]$	a_{10}	a_{10}	$a_{10}[-4]$	a_{10}	2^{-21}
			b_{10}	$b_{10}[-2]$	$b_{10}[10, -29]$	b_{10}	b_{10}	b_{10}	$b_{10}[29]$	$b_{10}[-13, 26]$	
			$c_{10}[8]$	$c_{10}[-24]$	$c_{10}[-2]$	c_{10}	c_{10}	$c_{10}[24]$	$c_{10}[8]$	c_{10}	
			$d_{10}[3, 4, -5]$	d_{10}	d_{10}	$d_{10}[-22]$	d_{10}	$d_{10}[19]$	d_{10}	$d_{10}[16]$	
11	22	7	a_{11}	a_{11}	a_{11}	$a_{11}[-29]$	a_{11}	a_{11}	a_{11}	$a_{11}[23]$	2^{-15}
			b_{11}	b_{11}	b_{11}	$b_{11}[10]$	b_{11}	b_{11}	$b_{11}[-26]$	b_{11}	
			c_{11}	$c_{11}[-2]$	$c_{11}[10, -29]$	c_{11}	c_{11}	c_{11}	$c_{11}[29]$	$c_{11}[-13, 26]$	
			$d_{11}[8]$	$d_{11}[-24]$	$d_{11}[-2]$	d_{11}	d_{11}	$d_{11}[24]$	$d_{11}[8]$	d_{11}	
12	7	28	$a_{12}[4]$	$a_{12}[-20]$	a_{12}	a_{12}	a_{12}	$a_{12}[-20, -21, 22]$	a_{12}	a_{12}	2^{-15}
			b_{12}	b_{12}	b_{12}	$b_{12}[-4]$	b_{12}	b_{12}	b_{12}	$b_{12}[30]$	
			c_{12}	c_{12}	c_{12}	$c_{12}[10]$	c_{12}	c_{12}	$c_{12}[-26]$	c_{12}	
			d_{12}	$d_{12}[-2]$	$d_{12}[10, -29]$	d_{12}	d_{12}	d_{12}	$d_{12}[29]$	$d_{12}[-13, 26]$	

step	r	s	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	pr
13	28	19	a_{13} $b_{13}[32]$ c_{13} d_{13}	$a_{13}[-21]$ $b_{13}[-16]$ c_{13} d_{13}	$a_{13}[-29, -30, 31]$ b_{13} c_{13} d_{13}	a_{13} b_{13} $c_{13}[-4]$ $d_{13}[10]$	a_{13} b_{13} c_{13} d_{13}	a_{13} $b_{13}[-16, -17, 18]$ c_{13} d_{13}	a_{13} b_{13} c_{13} $d_{13}[-26]$	$a_{13}[13]$ b_{13} $c_{13}[30]$ d_{13}	2^{-14}
14	19	22	a_{14} b_{14} $c_{14}[32]$ d_{14}	a_{14} $b_{14}[-8]$ $c_{14}[-16]$ d_{14}	$a_{14}[21]$ $b_{14}[-16, -17, 18]$ c_{14} d_{14}	a_{14} b_{14} c_{14} $d_{14}[-4]$	a_{14} b_{14} c_{14} d_{14}	a_{14} b_{14} $c_{14}[-16, -17, 18]$ d_{14}	a_{14} b_{14} c_{14} d_{14}	a_{14} $b_{14}[32]$ c_{14} $d_{14}[30]$	2^{-13}
15	22	7	a_{15} b_{15} c_{15} $d_{15}[32]$	a_{15} b_{15} $c_{15}[-8]$ $d_{15}[-16]$	a_{15} $b_{15}[11]$ $c_{15}[-16, -17, 18]$ d_{15}	$a_{15}[6]$ b_{15} c_{15} d_{15}	a_{15} $b_{15}[-32]$ c_{15} d_{15}	a_{15} b_{15} c_{15} $d_{15}[-16, -17, 18]$	a_{15} $b_{15}[-20]$ c_{15} d_{15}	$a_{15}[5]$ b_{15} $c_{15}[32]$ d_{15}	2^{-12}
16	7	28	$a_{16}[-28]$ b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} $d_{16}[-8]$	a_{16} b_{16} $c_{16}[11]$ $d_{16}[16]$	a_{16} b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	$a_{16}[12]$ b_{16} c_{16} d_{16}	a_{16} b_{16} c_{16} d_{16}	a_{16} $b_{16}[12]$ c_{16} $d_{16}[32]$	2^{-9}
17	29	9	a_{17} $b_{17}[-25]$ c_{17} d_{17}	$a_{17}[-17]$ b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} $d_{17}[11]$	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	a_{17} $b_{17}[9]$ c_{17} d_{17}	a_{17} b_{17} c_{17} d_{17}	a_{17} b_{17} $c_{17}[12]$ d_{17}	2^{-5}
18	9	15	a_{18} b_{18} $c_{18}[-25]$ d_{18}	a_{18} $b_{18}[-26]$ c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} $c_{18}[9]$ d_{18}	a_{18} b_{18} c_{18} d_{18}	a_{18} b_{18} c_{18} $d_{18}[12]$	2^{-4}
19	15	5	a_{19} b_{19} c_{19} $d_{19}[-25]$	a_{19} b_{19} $c_{19}[-26]$ d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} d_{19}	a_{19} b_{19} c_{19} $d_{19}[9]$	a_{19} b_{19} c_{19} d_{19}	$a_{19}[17]$ b_{19} c_{19} d_{19}	2^{-4}
20	5	29	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} $d_{20}[-26]$	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	a_{20} b_{20} c_{20} d_{20}	$a_{20}[6]$ b_{20} c_{20} d_{20}	a_{20} b_{20} d_{20}	a_{20} $b_{20}[22]$ c_{20} d_{20}	2^{-3}
21	29	9	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} $b_{21}[3]$ c_{21} d_{21}	a_{21} b_{21} c_{21} d_{21}	a_{21} b_{21} $c_{21}[22]$ d_{21}	2^{-2}
22	9	15	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} $c_{22}[3]$ d_{22}	a_{22} b_{22} c_{22} d_{22}	a_{22} b_{22} c_{22} $d_{22}[22]$	2^{-2}
23	15	5	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} d_{23}	a_{23} b_{23} c_{23} $d_{23}[3]$	a_{23} b_{23} c_{23} d_{23}	$a_{23}[27]$ b_{23} c_{23} d_{23}	2^{-2}
24	5	29	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} b_{24} c_{24} d_{24}	a_{24} $b_{24}[32]$ c_{24} d_{24}	2^{-1}
25	4	13	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} c_{25} d_{25}	a_{25} b_{25} $c_{25}[32]$ d_{25}	2^{-1}
26	13	10	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} d_{26}	a_{26} b_{26} c_{26} $d_{26}[32]$	2^{-1}
27	10	25	$a_{27}[25]$ b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	a_{27} b_{27} c_{27} d_{27}	2^{-1}
28	25	4	a_{28} b_{28} c_{28} d_{28}	a_{28} b_{28} c_{28} d_{28}	a_{28} b_{28} c_{28} d_{28}	$a_{28}[18]$ b_{28} c_{28} d_{28}	a_{28} b_{28} c_{28} d_{28}	a_{28} b_{28} c_{28} d_{28}	a_{28} b_{28} c_{28} d_{28}	a_{28} $b_{28}[18]$ c_{28} d_{28}	2^{-2}
29	4	13	a_{29} b_{29} c_{29} d_{29}	a_{29} b_{29} c_{29} d_{29}	$a_{29}[22]$ b_{29} c_{29} d_{29}	a_{29} $b_{29}[22]$ c_{29} d_{29}	a_{29} b_{29} c_{29} d_{29}	a_{29} b_{29} c_{29} d_{29}	a_{29} b_{29} c_{29} d_{29}	a_{29} b_{29} $c_{29}[18]$ d_{29}	2^{-3}
30	13	10	a_{30} b_{30} c_{30} d_{30}	a_{30} b_{30} c_{30} d_{30}	a_{30} $b_{30}[3]$ c_{30} d_{30}	a_{30} b_{30} $c_{30}[22]$ d_{30}	$a_{30}[3]$ b_{30} c_{30} d_{30}	a_{30} b_{30} c_{30} d_{30}	a_{30} b_{30} c_{30} d_{30}	a_{30} b_{30} c_{30} $d_{30}[18]$	2^{-4}
31	10	25	a_{31} b_{31} c_{31} d_{31}	a_{31} b_{31} c_{31} d_{31}	a_{31} b_{31} $c_{31}[3]$ d_{31}	a_{31} b_{31} c_{31} $d_{31}[22]$	a_{31} $b_{31}[13]$ c_{31} d_{31}	a_{31} b_{31} c_{31} d_{31}	$a_{31}[13]$ b_{31} c_{31} d_{31}	$a_{31}[-11, 12]$ b_{31} c_{31} d_{31}	2^{-6}
32	25	4	a_{32} b_{32} c_{32} d_{32}	a_{32} b_{32} c_{32} d_{32}	a_{32} b_{32} c_{32} $d_{32}[3]$	$a_{32}[26]$ b_{32} c_{32} d_{32}	$a_{32}[4]$ b_{32} $c_{32}[13]$ d_{32}	$a_{32}[6]$ b_{32} c_{32} d_{32}	a_{32} $b_{32}[6]$ c_{32} d_{32}	a_{32} $b_{32}[4]$ c_{32} d_{32}	2^{-8}
33	4	13	$a_{33}[10]$ b_{33} c_{33} d_{33}	$a_{33}[8]$ b_{33} c_{33} d_{33}	a_{33} b_{33} c_{33} d_{33}	a_{33} $b_{33}[30]$ c_{33} d_{33}	$a_{33}[-4]$ $b_{33}[8]$ c_{33} $d_{33}[13]$	$a_{33}[-14, -28, 32]$ $b_{33}[10]$ c_{33} d_{33}	$a_{33}[30]$ b_{33} $c_{33}[6]$ d_{33}	a_{33} b_{33} $c_{33}[4]$ d_{33}	2^{-13}
34	13	10	$a_{34}[-4, 13]$ $b_{34}[23]$ c_{34} d_{34}	$a_{34}[11]$ $b_{34}[21]$ c_{34} d_{34}	$a_{34}[-9, 13]$ b_{34} c_{34} d_{34}	$a_{34}[-17, 24]$ b_{34} $c_{34}[30]$ d_{34}	$a_{34}[16, 23]$ $b_{34}[-17]$ $c_{34}[8]$ d_{34}	a_{34} $b_{34}[-9, 13, -27]$ $c_{34}[10]$ d_{34}	$a_{34}[4, 18, -31, 32]$ $b_{34}[11]$ c_{34} $d_{34}[6]$	$a_{34}[23, 25]$ b_{34} c_{34} $d_{34}[4]$	2^{-27}
35	10	25	$a_{35}[1, 4, -13, 22, 26]$ $b_{35}[-14, 23]$ $c_{35}[23]$ d_{35}	a_{35} $b_{35}[21]$ $c_{35}[21]$ d_{35}	$a_{35}[9, 14]$ $b_{35}[-19, 23]$ c_{35} d_{35}	$a_{35}[1, 3]$ $b_{35}[2, -27]$ c_{35} d_{35}	$a_{35}[-14, 23]$ $b_{35}[1, 26]$ $c_{35}[-17]$ $d_{35}[8]$	$a_{35}[21, 32]$ b_{35} $c_{35}[-9, 13, -27]$ $d_{35}[10]$	$a_{35}[-10, -19, 23, 31]$ $b_{35}[-9, 10, 14, 28]$ $c_{35}[11]$ d_{35}	$a_{35}[2, -27, 29]$ $b_{35}[1, 3]$ c_{35} d_{35}	2^{-45}
36	25	4	$a_{36}[4]$ $b_{36}[-6, 15, 19, 26, 29]$ $c_{36}[-14, 23]$ $d_{36}[23]$	$a_{36}[-6, 15, 19, 25, 26, 29]$ b_{36} $c_{36}[21]$ $d_{36}[21]$	$a_{36}[26, 28]$ $b_{36}[2]$ $c_{36}[-19, 23]$ d_{36}	$a_{36}[2, -23]$ $b_{36}[26, 28]$ $c_{36}[2, -27]$ d_{36}	$a_{36}[12, 14, 25]$ $b_{36}[-7, 16]$ $c_{36}[1, 26]$ $d_{36}[17]$	$a_{36}[7, 11, 14, 15, 28]$ $b_{36}[14, 25]$ $c_{36}[$ $d_{36}[-9, 13, -27]$	$a_{36}[-20, 22]$ $b_{36}[-3, -12, 16, 24]$ $c_{36}[-9, 10, 14, 28]$ $d_{36}[11]$	$a_{36}[-2, 7, -12, 20, 24]$ $b_{36}[-20, 22, 27]$ $c_{36}[1, 3]$ d_{36}	2^{-63}