Gröbner Basis based Cryptanalysis of SHA-1

Makoto Sugita[1], Mitsuru Kawazoe[2], and Hideki Imai[3]

[1] IT Security Center, Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku Tokyo, 113-6591, Japan
m-sugita@ipa.go.jp
[2] Faculty of Liberal Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho Naka-ku Sakai Osaka 599-8531 Japan
kawazoe@las.osakafu-u.ac.jp
[3] National Institute of Advanced Industrial Science and Technology (AIST),
Akihabara Dai Bldg., 1-18-13 Sotokanda,
Chiyoda-ku, Tokyo 101-0021, Japan
Department of Electrical, Electronic and Communication Engineering,
Faculty of Science and Engineering, Chuo University,
1-13-27 Kasuga Bunkyo-ku, Tokyo 112-8551 Japan
h-imai@aist.go.jp

Abstract. Recently, Wang proposed a new method to cryptanalyze SHA-1 and found collisions of the 58-round SHA-1. The complexity of Wang's method to cryptanalyze the 58-round SHA-1 is 2^{34} SHA-1 computation. Moreover, Wang et al. gave the complexity evaluation against the full SHA-1 which is claimed to be 2^{62}. The aim of this article is to sophisticate and improve Wang's attack by using Gröbner basis techniques and to reduce the complexity of the attack for SHA-1. In this article, we apply Gröbner basis techniques to a cryptanalysis of SHA-1. We introduce a new notion of "semi-neutral bit" and propose an improved message modification technique based on Gröbner basis technique. In the case of the 58-round SHA-1, the complexity of an attack based on our improved message modification is 2^8 message modification which is equivalent to 2^{31} SHA-1 experimentally in our latest implementation. We found many new collisions for the 58-round SHA-1. Moreover, in the case of the full SHA-1, the complexity of our algorithm when it is applied to the first iteration of a two-iteration attack for the full SHA-1 is 2^{51} message modification (symbolic computation), whereas Wang's method needs 2^{62}. Though the complexity of the attack for the full SHA-1 is reduced, symbolic computations are still very slow at this moment. However we conjecture that our algorithm can be improved by techniques of error correcting code and Gröbner basis.

Keywords: SHA-1, Gröbner basis, differential attack

1 Introduction

MD4 is a first dedicated hash function proposed by R. Rivest in 1990, and MD5 was proposed as an improved version of MD4 in 1991 also by R. Rivest. Following the same design paradigm, SHA-0 was published by NIST in 1993 and SHA-1 was issued by NIST in 1995 as a Federal Information Processing Standard. SHA-2 was also proposed by NIST as an improved version of SHA-1 where the length of hash results are 256, 384, 512.

In the first cryptanalysis of these algorithms, Dobbertin [4] has found semi-free start collision of MD5. Later on, Wang [15], [14] has proposed collision attack on SHA-0 whose complexity was estimated to be as 2^{45} SHA-0 computation. Chabaud-Joux [3] independently found a differential collision attack against SHA-0 using essentially the same pattern. Introducing a new approach based on the neutral bit, near-collisions and multi-collisions, for SHA-0 and a reduced SHA-1 have been reported in [2], [6], [1].

Employing the modular differential attack and a message modification technique, Wang [16] has found collisions for the following hash functions MD4, MD5, HAVAL-128, RIPEMD, and in [7], [12], it is proposed how to break MD4, RIPEMD, MD5 and other hash functions, with the attack complexity against MD4 and MD5 proportional to 2^8 and 2^{37}, respectively. In [13] and [11], efficient collision search attacks against SHA-0 and 58-round SHA-1 have been reported as well as a complexity evaluation against the full SHA-1 claimed to be 2^{69} SHA-1 computation and in the improved approach to be 2^{62}. (cf. [10], [9], [17])

In this article, we apply our method to analyze the 58-round SHA-1 and the full SHA-1. Our method is based on the Gaussian elimination and Gröbner basis techniques. Our key ideas are to view a set of sufficient conditions as a system of equations via non-linear boolean functions and to consider message modifications as error-correcting procedures for non-linear codes. Starting from a disturbance vector for SHA-1, we determine sufficient conditions for a message to have a collision message with respect to the given disturbance vector, tables of control bits and control relations which needed in the conventional message modification, and a list of semi-neutral bits and adjusters which are defined later and used in our improved message modification. From the above information, the complexity of our method to find a collision is estimated. In the case of 58-round SHA-1, the complexity of our method to find a collision is 2^8 message modifications(though our implementation is very slow, equivalent to 2^{31} SHA-1 computation experimentally) whereas Wang's method needs 2^{34} SHA-1 computation. Moreover we found many collisions for 58-round SHA-1 which are different from Wang's result. In the case of the full SHA-1, the complexity of the first iteration in a two-iteration attack for the full SHA-1 is estimated to be 2^{51} message modification, whereas Wang's method needs 2^{62}. Though the complexity is reduced to 2^{51} message modification, symbolic computations are very slow at this moment. However we conjecture that our algorithm can be improved by techniques of error correcting codes and Gröbner basis.

Finally, we give an outline of this article. In Section 2, we give the description of SHA-1 and summarize Wang's analysis. In Section 3, we give some notation and definitions. In Section 4, we show our method to cryptanalysis of SHA-1. In Section 5, we explain how to construct sufficient conditions and how to construct *advanced* sufficient conditions by using the Gaussian elimination. In Section 6, we introduce a new notion called *semi-neutral bit*, and propose an improved message modification. Moreover, we give an algebraic descriptions for our improved message modification and consider the relation with error-correcting process for error-correcting codes. In Section 7, we show our result of cryptanalysis for the 58-round SHA-1. In Section 8, we show our result of cryptanalysis for the full SHA-1. Same as Wang's attack, our cryptanalysis for the full SHA-1 is a *two-iteration attack*, that is, a cryptanalysis for the full SHA-1 to find a two-block collision. In Appendix, we give a short remark on how to construct a message differential with low Hamming weight.

2 Description of SHA-1 and Wang's analysis

2.1 SHA-1 algorithm

The hash function SHA-1 generates a 160-bit hash result from a message of length less than 2^{64} bits. It has the Merkle/Damgard structure like other hash functions, and has 160-bit chaining values and a 512-bit message block, and initial chaining values (IV) are fixed. From a 512-bit block of the padded message, SHA-1 divides it into 16×32-bit words $(m_0, m_1, \cdots, m_{15})$ and expands the message by

$$m_i = (m_{i-3} \oplus m_{i-8} \oplus m_{i-14} \oplus m_{i-16}) \lll 1$$

for $i = 16, \cdots, 79$, where $x \lll n$ denotes n-bit left rotation of x. Using expanded messages, for $i = 0, 1, \cdots, 79$,

$$a_{i+1} = (a_i \lll 5) + f_i(b_i, c_i, d_i) + e_i + m_i + k_{i+1},$$

$$b_{i+1} = a_i,\ c_{i+1} = b_i \lll 30,\ d_{i+1} = c_i,\ e_{i+1} = d_i$$

where the initial chaining value $IV = (a_0, b_0, c_0, d_0, e_0)$ is ($0x67452301$, $0xefcdab89$, $0x98badcfe$, $0x10325476$, $0xc3d2e1f0$) and functions f_i are defined as in Table 1. In the following, we express 32-bit words as hexadecimal numbers.

round	Boolean function f_i	constant k_i
$1-20$	IF: $(x \wedge y) \vee (\neg x \wedge z)$	$0x5a827999$
$21-40$	XOR: $x \oplus y \oplus z$	$0x6ed6eba1$
$41-60$	MAJ: $(x \wedge y) \wedge (x \vee z) \wedge (y \vee z)$	$0x8fabbcdc$
$61-80$	XOR: $x \oplus y \oplus z$	$0xca62c1d6$

Table 1. Definition of function f_i

2.2 Wang's attack

Wang's attack is summarized as follows.

- Find disturbance vector with low Hamming weight (difference for subtractions modulo 2^{32}).
- Construct differential paths by specifying conditions so that the differential path will occur with high probabilities.
- Generate a message randomly, modify it using message modification techniques, and find a collision.

By this method, Wang et al. has succeeded in finding collisions of MD4, MD5, RIPEMD, SHA-0 and 58-round SHA-1.

In the case of the full SHA-1, Wang's attack needs to use a two-iteration, i.e. each message in a collision including two message blocks (1024-bit). They proposed a disturbance vector for the full SHA-1 and estimated the complexity of their attack. Using a message modification technique they greatly improved the collision probability. In [11], they claimed that complexity to find a collision of the full SHA-1 is 2^{69} and in CRYPTO'05 Rump Session, they claimed that they have improved complexity into 2^{62}. In the Rump Session, they claimed that they found new collision path of SHA-1 and described strategies for a message modification. This strategy is: First they determine which message bits are possible candidates for modification. The message modification process must respect all chaining variable conditions and message conditions may require adding extra chaining variable conditions in round 1-16 and message conditions. The message modification follows certain topological order coming from correlations among chaining variable conditions.

3 Definition and Notation

We take a complete set of representatives of $\mathbb{Z}/2^{32}\mathbb{Z}$ as $\{0, 1, 2, \ldots, 2^{32}-1\}$. and identify the ring $\mathbb{Z}/2^{32}\mathbb{Z}$ as the set $\{0, 1, 2, \ldots, 2^{32}-1\}$. When we ignore carry effects in the arithmetic of $\mathbb{Z}/2^{32}\mathbb{Z}$, we consider the ring $\mathbb{Z}/2^{32}\mathbb{Z}$ as the vector space $\mathbb{F}_2^{32}$ by using a set theoretical bijective mapping $\mathbb{F}_2^{32} \ni (x_{31}, x_{30}, \ldots, x_0) \mapsto x_{31}2^{31} + x_{30}2^{30} + \cdots + x_1 2^1 + x_0 2^0 \in \mathbb{Z}/2^{32}\mathbb{Z}$.

Definition 1. *Let $m = (m_{31}, m_{30}, \ldots, m_0)$, $m' = (m'_{31}, m'_{30}, \ldots, m'_0)$ be vectors of $\mathbb{F}_2^{32}$. For a pair (m, m'), we define the following notation.*

$$\Delta^+ m_j = \begin{cases} 1 & \text{if } (m_j, m'_j) = (0,1) \\ 0 & \text{otherwise,} \end{cases} \qquad \Delta^- m_j = \begin{cases} 1 & \text{if } (m_j, m'_j) = (1,0) \\ 0 & \text{otherwise,} \end{cases}$$

We define $\Delta^\pm m_j$ by $\Delta^\pm m_j = \Delta^+ m_j \oplus \Delta^- m_j$. Moreover, we define
$\Delta^+ m = (\Delta^+ m_{31}, \Delta^+ m_{30}, \ldots, \Delta^+ m_0)$, $\Delta^- m = (\Delta^- m_{31}, \Delta^- m_{30}, \ldots, \Delta^- m_0)$
and $\Delta^\pm m = \Delta^+ m \oplus \Delta^- m$.

It is obvious that $\Delta^{\pm} m_j = m'_j + m_j \in \mathbb{F}_2$ and $\Delta^{\pm} m = m' + m \in \mathbb{F}_2^{32}$.

Using the above definition, a "disturbance vector" and a "differential" are defined as follows.

Definition 2. *Let m_i, a_i, b_i, c_i, d_i, e_i be as in the definition of SHA-1 and m'_i, a'_i, b'_i, c'_i, d'_i, e'_i another message and its variables. They can be considered as vectors of $\mathbb{F}_2^{32}$. Then, following Wang's notation, we call a vector in the form $(\Delta^{\pm} m_i, \Delta^{\pm} a_i, \Delta^{\pm} b_i, \Delta^{\pm} c_i, \Delta^{\pm} d_i, \Delta^{\pm} e_i)_{i=0,1,\ldots,79}$ a "disturbance vector", and $(\Delta^{+} m_i, \Delta^{-} m_i, \Delta^{+} a_i, \Delta^{-} a_i, \ldots, \Delta^{+} e_i, \Delta^{-} e_i)_{i=0,1,\ldots,79}$ a "differential". We also call an element of $\mathbb{Z}/2^{32}\mathbb{Z}$ identified with $(\Delta^{+} m_i, \Delta^{-} m_i, \Delta^{+} a_i, \Delta^{-} a_i, \ldots)$ a "differential".*

Since a disturbance vector ignores the sign '$\pm$', there are many different vectors $(\Delta^{+} m_{i,j}, \Delta^{-} m_{i,j}, \ldots)$ corresponding to the same disturbance vector. So, the choice of a representative $(\Delta^{+} m_{i,j}, \Delta^{-} m_{i,j}, \ldots)$, that is, the choice of a differential is important in an analysis of SHA-1.

It is convenient to use the following definition to consider the ambiguity of the choice of a differential.

Definition 3. *For a message space $M = \mathbb{Z}/2^{32}\mathbb{Z}$, we define a function $f : (M \times M) \to M$ by $(x_1, x_2) \mapsto (x_1 - x_2)$ where we consider $'-'$ as subtraction of $\mathbb{Z}/2^{32}\mathbb{Z}$. We define differential δM by $\delta M = (M \times M)/\sim$ where for $\delta m_1, \delta m_2 \in \delta M$, $\delta m_1 \sim \delta m_2$ is satisfied if and only if $f(\delta m_1) = f(\delta m_2)$.*

Proposition 1. $\delta M \cong M$

Proof. This is obvious from the definition of δM.

We define operator $+$ in δM as follows. For $\delta m_1 = (m_1^+, m_1^-) \in \delta M$, $\delta m_2 = (m_2^+, m_2^-) \in \delta M$,

$$\delta m_1 + \delta m_2 = (m_1^+ + m_2^+, m_1^- + m_2^-)$$

Same as the case of disturbance vectors, a choice of a representative (m, m') for a given class δm is very important. When δm is given as a part of a disturbance vector, we call a representative (m, m') for it a "message differential". The important problem is to find a good message differential. Heuristically, a good message differential has low Hamming weight. To find such good message differential, we use the following calculation.

- Calculate $\delta m_3 = (m_3^+, m_3^-) = \delta m_1 + \delta m_2 = (m_1^+ + m_2^+, m_1^- + m_2^-)$.
- Cancel the bit of (m_3^+, m_3^-): If $m_{3,j}^+ = m_{3,j}^- = 1$, change $m_{3,j}^+ = m_{3,j}^- = 0$.

We define operator $-$ in δM as follows. For $\delta m_1 = (m_1^+, m_1^-)$, $\delta m_2 = (m_2^+, m_2^-)$,

$$\delta m_1 - \delta m_2 = (m_1^+ + m_2^-, m_1^- + m_2^+)$$

In calculation, we also use the steps given below.

- Calculate $\delta m_3 = (m_3^-, m_3^-) = \delta m_1 - \delta m_2 = (m_1^+ + m_2^-, m_1^- + m_2^+)$
- Cancel the bit of (m_3^+, m_3^-): If $m_{3,j}^+ = m_{3,j}^- = 1$, change $m_{3,j}^+ = m_{3,j}^- = 0$.

In order to check whether $\delta m_1 = \delta m_2$ or not, we only have to calculate $\delta m_1 - \delta m_2$ and check $\delta m_1 - \delta m_2 = (0, 0)$.

4 Our method

Our method to cryptanalyze SHA-1 is described as follows.

1. Find disturbance vector with low Hamming weight from 21-round to final round. In this calculation we approximate MAJ function as XOR which holds with probability 3/4 per round.

2. From first round to 20-round, find a differential (difference for subtractions modulo 2^{32}) so that $\delta a_{-4}(=\delta e_0 \lll 2)$, $\delta a_{-3}(=\delta d_0 \lll 2)$, $\delta a_{-2}(\ \delta c_0 \lll 2)$, $\delta a_{-1}(=\delta b_0)$, δa_0 is a local collision. We ignore carry effects here.
3. Calculate *sufficient conditions* on $\{a_i\}_{i=0,1,\ldots,20}$ considering carry effects by our semi-automatic method.
4. Determine *advanced sufficient conditions* on m_i by the Gaussian elimination based method.
5. Determine *advanced sufficient conditions* on a_i which contain information for an improved message modification technique.
6. Generate a message randomly, and modify it using *conventional/improved* message modification techniques and find collisions.

In the above, Step 4, 5 and 6 are based on our new idea. In Step 4, we use the Gaussian elimination and in Step 5, we use an idea from Gröbner basis techniques. A method used in Step 6 is based on an idea analogous to error-correcting for non-linear codes. Since the method of Step 1 and 2 is based on the essentially same idea of Wang's attack, we omit the details of Step 1 and 2 and only describe steps after from Step 3.

5 Sufficient conditions for collisions

For a given disturbance vector and a constructed differential we can determine sufficient conditions for collisions on m_i and a_i such that if m_i'' (and a_i'') satisfies these conditions, we can obtain a pair of messages whose differential coincides with a disturbance vector and gives a SHA-1 collision. By the construction, sufficient conditions depend on a choice of a disturbance vector and its differential.

5.1 How to calculate sufficient conditions on a_i?

In this step, we may only consider expanded messages by ignoring relations arising from the message expansion.

For a given disturbance vector, we calculate sufficient conditions of chaining variables by adjusting b_i, c_i, d_i so that

$$\delta f_i(b_i, c_i, d_i) = \delta a_{i+1} - (\delta a_i \lll 5) - \delta e_i - \delta m_i.$$

In this calculation, we must adjust carry effects by hand, because it is difficult to calculate full-automatically.

5.2 Gaussian elimination and advanced sufficient conditions

Here we consider to analyze n-round SHA-1 ($58 \leq n \leq 80$). In order to calculate the sufficient condition on $\{m_{i,j}\}_{i=0,1,\cdots,n;j=0,1,\ldots,31}$, we must take into account that $\Delta^+ m_{i,j} = 1$ implies $m_{i,j} = 0$ and $\Delta^- m_{i,j} = 1$ implies $m_{i,j} = 1$. This is done manually.

Moreover we also consider the relations derived from the key expansion

$$m_i = (m_{i-3} \oplus m_{i-8} \oplus m_{i-14} \oplus m_{i-16}) \lll 1$$

and we can rewrite all conditions on m_i in all rounds into relations of $0-15$-round by using the Gaussian elimination. Here all relations are considered as equations over $\mathbb{F}_2$ and an elimination order of $\{m_{i,j}\}_{i=0,1,\ldots,15;j=0,1,\ldots,31}$ is given by

$$m'_{i',j'} \leq m_{i,j} \text{ if } i' \leq i \text{ or } (i' = i \text{ and } j' \leq j).$$

Execute the Gaussian elimination for the system of equations which consists of all conditions on all rounds, we obtain reduced conditions only on $0-15$-round.

The important thing is that $m_{i,j}$ can be viewed as a polynomial on $a_{k,l}$, $(k \leq i+1)$, because $m_{i,j}$ can be viewed as a boolean function on $a_{k,l}$, $(k \leq i+1)$ by the definition of SHA-1. So it is useful to consider an elimination order of $\{a_{i,j}\}$. We can consider an elimination order of $\{a_{i,j}\}_{i=0,1,\ldots,15;j=0,1,\ldots,31}$ by

$a'_{i',j'} \leq a_{i,j}$ if $i' \leq i$ or ($i' = i$ and $j' \leq j$).

These two orders are different but approximately similar because a transformation between them is not so complicated.

Basically, we use the order of $\{a_{i,j}\}$ but not all relations can be sorted in a theoretical way, so experimentally we adjust the order in some relations. By using the Gaussian elimination with the order, we reduce a system of equations via original sufficient conditions to a reduced row echelon form. Then in spite of original sufficient conditions, we use the obtained system of equations in a reduced row echelon form as new sufficient conditions. We call them advanced sufficient conditions. On the other hand, for conditions on $\{a_{i,j}\}$, we construct advanced sufficient conditions by adding the information on "control bits", "semi-neutral bits" and "adjusters" defined in the next section to original sufficient conditions.

6 Message modification techniques of m_i

To find a collision, we start from a random message and then modify it to satisfy sufficient conditions. A technique to modify a message appropriately is called *message modification*, which was firstly introduced by Wang. Here we introduce an *improved message modification* technique.

We call Wang's message modification the *conventional message modification* and use it to have a "pre-collision", that is, a collision from the first round to a restricted round. Then we use our improved message modification to find a real collision.

6.1 Conventional message modification.

First we describe the conventional message modification. We note that in [14] and [15], this technique has been explained but not in detail.

In our procedure we use technique of modifying $\{a_{i,j}\}$ instead of $\{m_{i,j}\}$. When $(a_0, b_0, c_0, d_0, e_0)$ is fixed, it is clear that $(m_0, m_1, \cdots, m_{15})$ corresponds to $(a_1, a_2, \cdots, a_{16})$ bijectively, which implies that modification of $\{a_{i,j}\}$ is theoretically equivalent to modification of $\{m_{i,j}\}$ in the case of SHA-1.

In our method, the conventional message modification is used to find a collision in first R rounds for some R. The bound R is determined by the number of total rounds of a considered version of SHA-1. We can take $R = 23$ in the case of 58-round of SHA-1 and $R = 26$ in the case of the full SHA-1.

First we compile a list of controlled relations and control bits associated to the first R-rounds. The set of controlled relations consists of advanced sufficient conditions containing $\{m_{i,j}\}$ $(i \leq 15)$ and $\{a_{i,j}\}$ $(i \leq 30)$. Control bits are determined for each controlled relation. Control bits are chosen among $a_{i,j}$ which appears in a leading term or a term 'near' leading term in $m_{i,j}$, where $m_{i,j}$ is considered as a boolean function on $a_{i,j}$'s.

If a controlled relation is not satisfied by a current message, we adjust the message by changing values of control bits associated to the controlled relation. In the list, controlled relations are listed following the elimination order used in the Gaussian elimination. Each controlled relation with control bits associated to it is labeled by s_i where i denotes the order in the list.

By using the above setting, a basic procedure for the conventional message modification is given as follows.

Algorithm 1 (Conventional Message Modification) *Procedures for message modification: Preset the maximal number of trials M and the maximal round R.*

1. *Set* $r = 0$.

2. *Generate* $(a_1, a_2, \cdots, a_{16})$ *randomly.*
3. *Set* $i = 0$.
4. *Increment* i *until the controlled relation* r_i *of* s_i *is not satisfied. If all relations are satisfied go to final step. If* $r > M$*, give up and return to Step 2.*
5. *Adjust control bits* $a_{i,j}$ *of* s_i *so that corresponding controlled relation and sufficient condition on* $\{a_{i,j}\}$ *hold. After adjusting, set* $i = 0$ *and* $r = r + 1$ *and go to Step 3 and repeat the process until all controlled relations hold.*
6. *If all controlled relations are satisfied, check whether all sufficient conditions on the message* $\{m_{i,j}\}$ *and all sufficient conditions on the chaining variable* $\{a_{ij}\}$ *of 1-R round hold or not. If they hold then finish, otherwise return to the first step.*

The most important issue is that changing the control bit $a_{i,j}$ may affect the controlled relation $r_k (k < i)$ of previous step. In such situation, we have to go back to $i = k$ and correct controlled relations again.

By using the conventional message modification, we modify a message so that all sufficient conditions on the message $\{m_{i,j}\}$ and all sufficient conditions on the chaining variable $\{a_{ij}\}$ of first R rounds hold.

6.2 Neutral bit, semi-neutral bit and adjuster

To adjust remaining conditions after R-round ($R = 23$ for the 58-round SHA-1 and $R = 26$ for the full SHA-1), we use *semi-neutral bits* and *adjusters* defined below.

Assume that message conditions and some chaining variable conditions are satisfied. If changing some bit of chaining variable does not affect these conditions, the bit is called a neutral bit, following Wang's terminology. To adjust a message to satisfy remaining conditions, it is useful to use neutral bits. But in the case of SHA-1, there are not enough neutral bits. Here we introduce a notion of semi-neutral bits, a generalization of neutral bits. Assume again that message conditions and some chaining variable conditions are satisfied. If an effect of changing a bit of chaining variable can be easily eliminated so that all conditions previously satisfied are satisfied, we call the bit as a *semi-neutral bit*. Effects of changing semi-neutral bits can be eliminated by controlling a little number of bits. We call such bit an *adjuster*.

The choice of a set of semi-neutral bits and adjusters is not unique. So we should choose it heuristically.

6.3 Improved message modification to find collisions of SHA-1

Using semi-neutral bits and adjusters, we construct a more efficient algorithm to find collisions of SHA-1.

A new procedure to find collisions of SHA-1 is as follows.

Algorithm 2 (Improved Message Modification for SHA-1) *Procedures for message:*

1. *Generate* $(a_1, a_2, \cdots, a_{16})$ *randomly.*
2. *Using the conventional message modification described in Algorithm 1, modify* $(a_1, a_2, \cdots, a_{80})$ *so that all message conditions and some chaining variable conditions from the 17-th round to the R-th round hold. If this step fails, return to Step 1.*
3. *If remaining chaining variable conditions from the 17-th round to the R-th round are not satisfied, return to Step 1 and repair until all conditions are satisfied (It can be satisfied probabilistically).*
4. *Change values of semi-neutral bits and adjusters and check whether chaining variable conditions from the R-th round to the final round are satisfied.*
5. *Repeat all procedure above until all chaining variable conditions are satisfied.*

Remark 1. (1) In round 17-R, there are uncontrolled relations. In the case of our experiment on the 58-round SHA-1, there are 5 uncontrolled relations where $R = 23$. In the case of the full SHA-1, there are 26 uncontrolled relations where $R = 26$.

(2) As we show in Section 8, in the case of our experiment on the full SHA-1, we use 10 semi-neutral bits and 8 adjusters. The procedure in Step 4 is equivalent to solve a system of polynomial equations via sufficient conditions with semi-neutral bits and adjusters as unknown variables. So we can use Gröbner basis technique in Step 4. In Section 6.4, we give algebraic description for the above algorithm related to Gröbner basis and error-correcting codes.

6.4 Algebraic Description of Message Modification and the Relation to Error-Correcting Codes

Here we give another point of view which may be useful for further improvements.

Algebraic Description of message modification. We can explain Algorithm 2 in terms of ideals of a polynomial ring and Gröbner basis. Here we consider n-round SHA-1 ($58 \leq n \leq 80$).

Let $\mathbb{F}_2[\mathbf{X}]$ be a polynomial ring over $\mathbb{F}_2$ with variables $X_{i,j}$, $i = 0, 1, \ldots, n$ and $j = 0, 1, \ldots, 31$. Let J be an ideal in $\mathbb{F}_2[\mathbf{X}]$ generated by $\{X_{i,j}^2 + X_{i,j}\}_{i=0,1,\ldots,n;j=0,1,\ldots,31}$ and B_n a quotient ring $\mathbb{F}_2[\mathbf{X}]/J$. Note that B_n represents the set of all boolean functions with variables $X_{i,j}$, $i = 0, 1, \ldots, n$ and $j = 0, 1, \ldots, 31$. For the simplicity of notation, we write an element in B_n as $f(\mathbf{X})$.

For a randomly taken $(a_1, a_2, \cdots, a_{16}) \in (\mathbb{F}_2^{32})^{16}$, $\mathbf{a} = \{a_{i,j}\}_{i=0,1,\ldots,n;j=0,1,\ldots,31}$ are determined. We associate this $\mathbf{a}$ to the ideal in B_n generated by $\{X_{i,j} + a_{i,j}\}_{i=0,1,\ldots,n;j=0,1,\ldots,31}$. Since $m_{i,j}$ is determined by $a_{i,j}$'s, we may consider those relations as functions on $a_{i,j}$'s. Moreover, since controlled relations are equations via boolean functions, they can be expressed as polynomials on $a_{i,j}$'s. So by replacing $a_{i,j}$ by the variable $X_{i,j}$, we may consider controlled relations are equations in the form $f(\mathbf{X}) = 0$ where $f \in B_n$. Put $g_{i,j} = X_{i,j} + a_{i,j}$ for each i, j, let I be an ideal generated by $g_{i,j}$'s and let $(f_1, f_2, \ldots)$ an ordered set of polynomials associated to the list of controlled relations. Controlled relation and control bits in the list are replaced by f_i's and $g_{i,j}$. We call f_i a control equation and we call $g_{i,j}$ corresponding a control bit a control polynomial. Note that all control relations f_i are in a subring $\mathbb{F}_2[\{X_{i,j}\}_{i=0,1,\ldots,R;j=0,1,\ldots,31}]$ where R is determined by n, $R = 23$ when $n = 58$ and $R = 26$ when $n = 80$ for example.

Let $T := \{f_j\}$ be the set of all conditions in a table of advanced sufficient conditions on which changing semi-neutral bits affect. Let N be the set of all semi-neutral bits and adjusters. Put $P := \{(i, j) \mid a_{i,j} \in N\}$ and let I_2 be the ideal generated by all polynomials $g_{i,j} = X_{i,j} + a_{i,j}$ for $(i, j) \notin P$ and let $\bar{B}_n$ a quotient ring B_n/I_2. For each f_j in T, let $\bar{f}_j$ be an equation $f_j \mod I_2$ and let $\mathcal{T}$ a system of equations which consists of all $\bar{f}_j$.

Then, Algorithm 2 is described as follows.

Algorithm 3 *Procedures for message modification: Preset the maximal number of trials M and the control bound R.*

1. *Set $r = 0$ and generate $(a_1, a_2, \cdots, a_{16}) \in (\mathbb{F}_2^{32})^{16}$ randomly.*
2. *Set $i = 0$.*
3. *Increment i until $f_i \not\equiv 0 \mod I$. If all f_i are contained in I, go to Step 5. If $r > M$, give up and return to Step 1.*
4. *For control polynomials $\{g_{j,l}\}$ associated to f_i, replace appropriate $g_{j,l}(X_{j,l})$ by $g_{j,l}(X_{j,l} + 1)$ in I to satisfy $f_i \equiv 0 \mod I$. After adjusting, set $r = r + 1$ and return to Step 2.*
5. *If $f \equiv 0 \mod I$ for all polynomial $f(\mathbf{X})$ associated to sufficient conditions till R round, go to Step 6. Otherwise, return to Step 1.*
6. *Solve a system of equations $\mathcal{T}$ in R_2 by using Gröbner basis algorithm.*
7. *Check whether a modified message yields collision or not. If it does not generate collision, return to Step 1. If it generates collision, finish.*

Note that in the above algorithm, an ideal I is replaced by a new one in Step 2. We also remark that in a system of polynomial equation considered in Step 6 in the above algorithm, most of equations coming from controlled relations are trivial, that is, $\bar{f}_i \equiv 0$ in R_2.

Relation between message modification and decoding of error-correcting codes. Let S be the set of all points in $F = \left(\mathbb{F}_2^{32}\right)^{16}$ satisfying advanced sufficient conditions on $\{a_{i,j}\}$. Note that S is a non-linear subset of F because there are non-linear conditions. Then, for a given $\mathbf{a} \in F$ which is not necessarily contained in S, to find an element in S by modifying $\mathbf{a}$ is analogous to a decoding problem in error-correcting codes. Hence, a conventional message modification and a proposed improved message modification including changing semi-neutral bits can be viewed as an error-correcting process for a non-linear code S in F. More precisely, for a non-linear code S in F, an error-correction can be achieved by manipulating control bits and semi-neutral bits.

7 Analysis of the 58-round SHA-1 based on our method

In the case of the 58-round SHA-1, the conventional message modification (Step 2 in Algorithm 2) is applied to 1-23 round.

The complexity of the attack for the 58-round SHA-1 is given as follows. After Step 2, there are 5 uncontrolled relations in round 17-23. So the probability that output of Step 2 pass the test in Step 3 is $1/2^5$. For after 23-round, there are 29 remaining conditions. To adjust these 29 conditions, we use 21 semi-neutral bits and 16 adjusters. Hence the total complexity is improved to $2^5+2^{29-21} \sim 2^8$ message modifications(equivalent to 2^{31} SHA-1 computation with our latest implementation, experimentally), whereas Wang's method needs 2^{34} SHA-1 computation.

Here we show the result on 58-round SHA-1.

Disturbance vector and Message differential path. We start from the disturbance vector which is the same as the one Wang gave. (Of course, our method is applicable to other disturbance vectors.) Then we construct a differential associated to the disturbance vector. Constructed one is the same one as Wang obtained in [11]. Explicit form of the differential is given in Table 2.

Sufficient conditions, the result of Gaussian elimination, control bits and controlled relations. We show sufficient conditions on 58-round SHA-1 (Table 3), the result of Gaussian eliminations, a table of control bits and controlled relations (Table 4, 5), and advanced sufficient conditions (Table 6) in the following pages. In the following table,

- '`a`' means $a_{i,j} = a_{i-1,j}$,
- '`A`' means $a_{i,j} = a_{i-1,j} + 1$,
- '`b`' means $a_{i,j} = a_{i-1,(j+2 \mod 32)}$,
- '`B`' means $a_{i,j} = a_{i-1,(j+2 \mod 32)} + 1$,
- '`c`' means $a_{i,j} = a_{i-2,(j+2 \mod 32)}$
- '`C`' means $a_{i,j} = a_{i-2,(j+2 \mod 32)} + 1$.
- '`L`' means the leading term of controlled relation of Table 9, 10, 11 and 12.
- '`w`', '`W`': adjust $a_{i,j}$ so that $m_{i+1,j} = 0, 1$, respectively.
- '`v`', '`V`': adjust $a_{i,j}$ so that $m_{i,(j+27 \mod 32)} = 0, 1$, respectively.
- '`h`': adjust $a_{i,j}$ so that corresponding controlled relation including $m_{i+1,j}$ as leading term holds.
- '`r`' means to adjust $a_{i,j}$ so that corresponding controlled relation including $m_{i,(j+27 \mod 32)}$ as leading term holds.
- '`x`', '`y`': adjust $a_{i+1,j-1}$, $a_{i,j-1}$ so that $m_{i,j} = 0$, respectively.
- '`X`', '`Y`': adjust $a_{i+1,j-1}$, $a_{i,j-1}$ so that $m_{i,j} = 1$, respectively.
- '`N`': semi-neutral bit.

i	$\Delta^+ m_i$	$\Delta^- m_i$	$\Delta^+ a_i$	$\Delta^- a_i$
58	4	0	0	0
57	0	0	0	0
56	0	0	0	0
55	0	0	0	0
54	0	0	0	0
53	0	0	0	0
52	0	0	0	0
51	0	0	0	0
50	0	0	0	0
49	0	0	0	0
48	0	0	0	0
47	80000000	0	0	0
46	0	80000000	0	0
45	0	0	0	0
44	0	80000002	0	0
43	0	40	2	0
42	0	80000000	0	0
41	0	40	2	0
40	0	80000000	0	0
39	80000000	40	2	0
38	0	0	0	0
37	40	80000000	0	2
36	0	80000002	0	0
35	80000000	0	0	0
34	80000000	2	0	0
33	40	0	0	2
32	0	2	0	0
31	2	40000000	0	0
30	40000002	40	2	0
29	2	40000040	2	0
28	1	80000000	0	0
27	42	40000020	0	1
26	40000041	80000002	0	2
25	0	40000002	0	0
24	1	0	0	0
23	2	c0000020	1	0
22	80000041	40000002	0	2
21	40000040	2	0	2
20	0	3	0	0
19	40000000	22	1	0
18	c0000002	41	2	0
17	40000002	40	2	0
16	80000001	0	0	0
15	20000000	60	1	0
14	20000001	0	0	0
13	80000040	0	0	2
12	0	a0000000	0	0
11	40000000	a0000052	102	80000000
10	40000040	0	0	0
9	40000040	12	8003ff00	40002
8	3	0	1fe0000	2000000
7	0	20	209	100180
6	80000001	0	1008000	4000
5	0	60000002	10100600	08080801
4	e0000040	2	8012	4024
3	20000000	40	201	0
2	20000000	40000043	80000014	60000002
1	40000020	20000012	40000000	20000000
0	20000000	0	0	0

Table 2. $\{m_i\}$ and $\{a_i\}$ of differential of 58-round SHA-1

message variable	31 - 24	23 - 16	15 - 8	8 - 0
m_0	--0-----	--------	--------	--------
m_1	-01-----	--------	--------	--01--1-
m_2	-10-----	--------	--------	-1----11
m_3	--0-----	--------	--------	-1------
m_4	000-----	--------	--------	-0----1-
m_5	-11-----	--------	--------	------1-
m_6	0-------	--------	--------	-------0
m_7	--------	--------	--------	--1-----
m_8	--------	--------	--------	------00
m_9	-0------	--------	--------	-0-1--1-
m_{10}	-0------	--------	--------	-0------
m_{11}	101-----	--------	--------	-1-1--1-
m_{12}	1-1-----	--------	--------	--------
m_{13}	0-------	--------	--------	-0------
m_{14}	--0-----	--------	--------	-------0
m_{15}	--0-----	--------	--------	-11-----
m_{16}	0-------	--------	--------	-------0
m_{17}	-0------	--------	--------	-1----0-
m_{18}	00------	--------	--------	-1----01
m_{19}	-0------	--------	--------	--1---1-
m_{20}	--------	--------	--------	------11
m_{21}	-0------	--------	--------	-0----1-
m_{22}	01------	--------	--------	-0----10
m_{23}	11------	--------	--------	--1---0-
m_{24}	--------	--------	--------	-------0
m_{25}	-1------	--------	--------	------1-
m_{26}	10------	--------	--------	-0----10
m_{27}	-1------	--------	--------	-01---0-
m_{28}	1-------	--------	--------	-------0
m_{29}	-1------	--------	--------	-1----0-
m_{30}	-0------	--------	--------	-1----0-
m_{31}	-1------	--------	--------	------0-
m_{32}	--------	--------	--------	------1-
m_{33}	--------	--------	--------	-0------
m_{34}	0-------	--------	--------	------1-
m_{35}	0-------	--------	--------	--------
m_{36}	1-------	--------	--------	------1-
m_{37}	1-------	--------	--------	-0------
m_{38}	--------	--------	--------	--------
m_{39}	0-------	--------	--------	-1------
m_{40}	1-------	--------	--------	--------
m_{41}	--------	--------	--------	-1------
m_{42}	1-------	--------	--------	--------
m_{43}	--------	--------	--------	-1------
m_{44}	1-------	--------	--------	------1-
m_{45}	--------	--------	--------	--------
m_{46}	1-------	--------	--------	--------
m_{47}	0-------	--------	--------	--------
m_i $(i \geq 48)$	--------	--------	--------	--------

chaining variable	31 - 24	23 - 16	15 - 8	8 - 0
a_0	01100111	01000101	00100011	00000001
a_1	101-----	--------	--------	-1-a10aa
a_2	01100---	------0-	----a---	1--00010
a_3	0010----	-10---1a	------0-	0a-1a0-0
a_4	11010---	-01-----	01aaa---	0-10-100
a_5	10-01a--	-1-01-aa	--00100-	0---01-1
a_6	11--0110	-a-1001-	01100010	1-a111-1
a_7	-1--1110	a1a1111-	-101-001	1---0-10
a_8	-0----10	0000000a	a001a1--	100-0-1-
a_9	00------	11000100	00000000	101-1-1-
a_{10}	0-1-----	11111011	11100000	00--0-1-
a_{11}	1-0-----	-------1	01111110	11----0-
a_{12}	0-1-----	--------	--------	-1--a---
a_{13}	1-0-----	--------	--------	-1---01-
a_{14}	1-------	--------	--------	-1---1--
a_{15}	0-------	--------	--------	----0--0
a_{16}	-1------	--------	--------	----a---
a_{17}	-0------	--------	--------	----100-
a_{18}	1-1-----	--------	--------	-----00-
a_{19}	--------	--------	--------	-------0
a_{20}	-C------	--------	--------	----A---
a_{21}	-b------	--------	--------	----a-1-
a_{22}	--------	--------	--------	-----A1-
a_{23}	--------	--------	--------	-------0
a_{24}	-c------	--------	--------	--------
a_{25}	-B------	--------	--------	----a---
a_{26}	--------	--------	--------	-----A1-
a_{27}	--------	--------	--------	-------1
a_{28}	-c------	--------	--------	----A---
a_{29}	-B------	--------	--------	----A-0-
a_{30}	--------	--------	--------	------0-
a_{31}	--------	--------	--------	--------
a_{32}	--------	--------	--------	----A---
a_{33}	--------	--------	--------	------1-
a_{34}	--------	--------	--------	--------
a_{35}	--------	--------	--------	--------
a_{36}	--------	--------	--------	----A---
a_{37}	--------	--------	--------	------1-
a_{38}	--------	--------	--------	----A---
a_{39}	B-------	--------	--------	------0-
a_{40}	C-------	--------	--------	----A---
a_{41}	B-------	--------	--------	------0-
a_{42}	C-------	--------	--------	----A---
a_{43}	B-------	--------	--------	------0-
a_{44}	C-------	--------	--------	--------
a_{45}	B-------	--------	--------	--------
a_i $(i \geq 46)$	--------	--------	--------	--------

Table 3. Sufficient condition on $\{m_{ij}\}$ and $\{a_{i,j}\}$ of 58-round SHA-1

– 'q' : adjust $a_{i,j}$ so that relations after 17-round hold.

In this case, the set of bits corresponding to 'q' is exactly same to the set of *adjuster*s. The result of Gaussian elimination is as follows.

$m_{15,31} = 1,\ m_{15,30} = 1,\ m_{15,29} = 0,\ m_{15,28} + m_{10,28} + m_{8,29} + m_{7,29} + m_{4,28} + m_{2,28} = 1,$

$m_{15,27} + m_{14,25} + m_{12,28} + m_{12,26} + m_{10,28} + m_{9,27} + m_{9,25} + m_{8,29} + m_{8,28} + m_{7,28} + m_{7,27} + m_{6,26} + m_{5,28} + m_{4,26} + m_{3,25} + m_{2,28} + m_{1,25} + m_{0,28} = 1,$

$m_{15,26} + m_{10,28} + m_{10,26} + m_{8,28} + m_{8,27} + m_{7,27} + m_{6,29} + m_{5,27} + m_{4,26} + m_{2,27} + m_{2,26} + m_{0,27} = 1,$

$m_{15,25} + m_{11,28} + m_{10,27} + m_{10,25} + m_{9,28} + m_{8,27} + m_{8,26} + m_{7,26} + m_{6,29} + m_{6,28} + m_{5,26} + m_{4,25} + m_{3,28} + m_{2,28} + m_{2,26} + m_{2,25} + m_{1,28} + m_{0,28} + m_{0,26} = 0,$

$m_{15,24} + m_{12,28} + m_{11,27} + m_{10,26} + m_{10,24} + m_{9,28} + m_{9,27} + m_{8,29} + m_{8,26} + m_{8,25} + m_{7,25} + m_{6,29} + m_{6,28} + m_{6,27} + m_{5,25} + m_{4,28} + m_{4,24} + m_{3,28} + m_{3,27} + m_{2,27} + m_{2,25} + m_{2,24} + m_{1,28} + m_{1,27} + m_{0,27} + m_{0,25} = 1,$

$m_{15,23} + m_{12,28} + m_{12,27} + m_{11,26} + m_{10,25} + m_{10,23} + m_{9,27} + m_{9,26} + m_{8,28} + m_{8,25} + m_{8,24} + m_{7,29} + m_{7,24} + m_{6,28} + m_{6,27} + m_{6,26} + m_{5,24} + m_{4,27} + m_{4,23} + m_{3,27} + m_{3,26} + m_{2,26} + m_{2,24} + m_{2,23} + m_{1,27} + m_{1,26} + m_{0,26} + m_{0,24} = 1,$

$m_{15,22} + m_{14,25} + m_{12,28} + m_{12,27} + m_{11,25} + m_{10,27} + m_{10,24} + m_{10,22} + m_{9,28} + m_{9,27} + m_{9,26} + m_{8,27} + m_{8,24} + m_{8,23} + m_{7,28} + m_{7,27} + m_{7,23} + m_{6,27} + m_{6,25} + m_{5,23} + m_{4,28} + m_{4,27} + m_{4,22} + m_{3,26} + m_{2,28} + m_{2,27} + m_{2,25} + m_{2,23} + m_{2,22} + m_{1,26} + m_{0,25} + m_{0,23} = 0,$

$m_{15,6} = 1,\ m_{15,5} = 1,\ m_{15,4} + m_{12,5} + m_{10,4} + m_{4,5} + m_{4,4} + m_{2,5} + m_{2,4} = 1,$

$m_{15,3} + m_{12,2} + m_{10,2} + m_{8,3} + m_{7,3} + m_{7,2} + m_{5,3} + m_{4,2} + m_{3,4} + m_{3,2} + m_{2,3} + m_{2,2} + m_{1,2} + m_{0,3} = 0,$

$m_{15,2} + m_{12,5} + m_{11,5} + m_{10,4} + m_{10,2} + m_{8,4} + m_{8,3} + m_{7,3} + m_{5,5} + m_{5,3} + m_{4,5} + m_{4,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{0,3} = 1,$

$m_{15,1} + m_{12,5} + m_{11,3} + m_{11,2} + m_{10,4} + m_{10,2} + m_{9,2} + m_{8,3} + m_{8,2} + m_{5,4} + m_{4,5} + m_{4,4} + m_{4,0} + m_{3,31} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,4} + m_{2,3} + m_{1,31} + m_{0,3} = 0,$

$m_{15,0} + m_{1,0} = 1,\ m_{14,31} = 0,\ m_{14,30} = 1,\ m_{14,29} = 0,\ m_{14,28} + m_{9,28} + m_{6,29} + m_{3,28} + m_{1,28} = 0,$

$m_{14,27} + m_{12,28} + m_{9,27} + m_{7,29} + m_{6,28} + m_{4,28} + m_{3,27} + m_{1,27} = 0,$

$m_{14,26} + m_{12,27} + m_{10,28} + m_{9,28} + m_{9,26} + m_{7,28} + m_{6,27} + m_{4,28} + m_{4,27} + m_{3,26} + m_{2,28} + m_{1,26} = 1,$

$m_{14,24} + m_{12,27} + m_{12,25} + m_{11,28} + m_{10,27} + m_{10,26} + m_{9,26} + m_{9,24} + m_{8,29} + m_{7,26} + m_{6,29} + m_{6,25} + m_{5,28} + m_{4,28} + m_{4,26} + m_{4,25} + m_{3,28} + m_{3,24} + m_{2,26} + m_{1,24} + m_{0,28} = 0,$

$m_{14,23} + m_{12,26} + m_{12,24} + m_{11,27} + m_{10,26} + m_{10,25} + m_{9,28} + m_{9,25} + m_{9,23} + m_{8,28} + m_{7,25} + m_{6,28} + m_{6,24} + m_{5,27} + m_{4,27} + m_{4,25} + m_{4,24} + m_{3,28} + m_{3,27} + m_{3,23} + m_{2,25} + m_{1,28} + m_{1,23} + m_{0,27} = 1,$

$m_{14,22} + m_{13,20} + m_{12,25} + m_{12,24} + m_{12,23} + m_{11,28} + m_{11,23} + m_{11,21} + m_{10,27} + m_{9,26} + m_{9,24} + m_{9,23} + m_{8,29} + m_{8,27} + m_{8,26} + m_{8,25} + m_{8,22} + m_{8,20} + m_{7,26} + m_{7,25} + m_{6,29} + m_{6,23} + m_{6,22} + m_{5,28} + m_{5,25} + m_{5,21} + m_{4,28} + m_{4,26} + m_{4,25} + m_{4,23} + m_{3,28} + m_{3,24} + m_{3,21} + m_{2,26} + m_{2,20} + m_{1,24} + m_{0,28} + m_{0,25} + m_{0,20} = 1,$

$m_{14,21} + m_{12,27} + m_{12,24} + m_{12,22} + m_{11,25} + m_{10,28} + m_{10,27} + m_{10,24} + m_{10,23} + m_{9,28} + m_{9,26} + m_{9,23} + m_{9,21} + m_{8,29} + m_{8,26} + m_{7,29} + m_{7,28} + m_{7,23} + m_{6,29} + m_{6,26} + m_{6,22} + m_{5,25} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,23} + m_{4,22} + m_{3,26} + m_{3,25} + m_{3,21} + m_{2,28} + m_{2,23} + m_{1,26} + m_{1,21} + m_{0,25} = 0,$

$m_{14,20} + m_{12,26} + m_{12,23} + m_{12,21} + m_{11,28} + m_{11,24} + m_{10,28} + m_{10,27} + m_{10,26} + m_{10,23} + m_{10,22} + m_{9,27} + m_{9,25} + m_{9,22} + m_{9,20} + m_{8,28} + m_{8,25} + m_{7,28} + m_{7,27} + m_{7,22} + m_{6,29} + m_{6,28} + m_{6,25} + m_{6,21} + m_{5,24} + m_{4,27} + m_{4,26} + m_{4,24} + m_{4,22} + m_{4,21} + m_{3,28} + m_{3,25} + m_{3,24} + m_{3,20} + m_{2,27} + m_{2,22} + m_{1,25} + m_{1,20} + m_{0,28} + m_{0,24} + m_{47,31} = 1,$

$m_{14,5} + m_{8,5} + m_{6,5} = 1,$

$m_{14,4} + m_{12,5} + m_{11,3} + m_{11,2} + m_{10,4} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2} + m_{8,5} + m_{7,2} + m_{6,5} + m_{6,4} + m_{5,4} + m_{5,2} + m_{4,5} + m_{4,4} + m_{4,0} + m_{3,31} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{1,31} + m_{0,4} + m_{0,3} + m_{0,2} = 1,$

$m_{14,3} + m_{11,3} + m_{11,2} + m_{8,2} + m_{7,4} + m_{7,2} + m_{7,1} + m_{6,2} + m_{5,3} + m_{4,0} + m_{3,3} + m_{2,2} + m_{1,31} + m_{1,3} = 0,$

$m_{14,2} + m_{12,5} + m_{12,3} + m_{10,4} + m_{9,2} + m_{7,4} + m_{6,3} + m_{4,5} + m_{4,4} + m_{4,3} + m_{3,2} + m_{2,5} + m_{2,4} + m_{1,2} = 1,$

$m_{14,1} + m_{12,4} + m_{11,2} + m_{10,2} + m_{9,3} + m_{8,3} + m_{7,2} + m_{6,2} + m_{5,5} + m_{5,2} + m_{4,4} + m_{3,31} + m_{3,4} + m_{3,2} + m_{3,1} + m_{2,4} + m_{2,3} + m_{0,3} = 0,$

$m_{14,0} = 0,\ m_{13,31} = 0,\ m_{13,30} = 0,\ m_{13,29} + m_{8,29} = 0,\ m_{13,28} + m_{8,28} + m_{2,28} + m_{0,28} = 0,$

$m_{13,27} + m_{11,28} + m_{8,29} + m_{8,27} + m_{6,29} + m_{5,28} + m_{3,28} + m_{2,27} + m_{0,27} = 1,$

$m_{13,26} + m_{11,27} + m_{9,28} + m_{8,28} + m_{8,26} + m_{6,28} + m_{5,27} + m_{3,28} + m_{3,27} + m_{2,26} + m_{1,28} + m_{0,26} = 1,$

$m_{13,24} + m_{12,28} + m_{11,27} + m_{11,25} + m_{10,28} + m_{9,27} + m_{9,26} + m_{8,29} + m_{8,26} + m_{8,24} + m_{7,29} + m_{7,28} + m_{6,26} + m_{5,25} + m_{4,28} + m_{3,28} + m_{3,26} + m_{3,25} + m_{2,28} + m_{2,24} + m_{1,28} + m_{1,26} + m_{0,24} = 0,$

$m_{13,23} + m_{12,27} + m_{11,26} + m_{11,24} + m_{10,28} + m_{10,27} + m_{9,26} + m_{9,25} + m_{8,29} + m_{8,28} + m_{8,25} + m_{8,23} + m_{7,29} + m_{7,28} + m_{7,27} + m_{6,25} + m_{5,28} + m_{5,24} + m_{4,28} + m_{4,27} + m_{3,27} + m_{3,25} + m_{3,24} + m_{2,27} + m_{2,23} + m_{1,27} + m_{1,25} + m_{0,28} + m_{0,23} = 0,$

$m_{13,22} + m_{12,26} + m_{11,28} + m_{11,25} + m_{11,23} + m_{10,27} + m_{10,26} + m_{9,28} + m_{9,25} + m_{9,24} + m_{8,28} + m_{8,27} + m_{8,24} + m_{8,22} + m_{7,28} + m_{7,27} + m_{7,26} + m_{6,29} + m_{6,24} + m_{5,28} + m_{5,27} + m_{5,23} + m_{4,27} + m_{4,26} + m_{3,28} + m_{3,26} + m_{3,24} + m_{3,23} + m_{2,28} + m_{2,26} + m_{2,22} +$

$m_{1,26} + m_{1,24} + m_{0,28} + m_{0,27} + m_{0,22} = 1,$
$m_{13,6} = 0,\ m_{13,5} + m_{12,5} + m_{5,5} + m_{4,5} + m_{2,5} = 0,$
$m_{13,4} + m_{12,5} + m_{11,2} + m_{10,4} + m_{7,4} + m_{5,4} + m_{5,3} + m_{5,2} + m_{4,5} + m_{4,4} + m_{3,31} + m_{2,5} + m_{2,4} + m_{2,2} + m_{1,2} = 0,$
$m_{13,3} + m_{8,3} + m_{5,4} + m_{3,4} + m_{2,3} + m_{0,3} = 0,$
$m_{13,2} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2} + m_{8,2} + m_{7,4} + m_{7,2} + m_{4,0} + m_{3,4} + m_{3,3} + m_{3,2} + m_{2,3} + m_{2,2} + m_{1,31} + m_{1,2} + m_{0,3} = 0,$
$m_{13,1} + m_{10,2} + m_{9,3} + m_{8,3} + m_{7,4} + m_{7,2} + m_{6,2} + m_{5,3} + m_{5,2} + m_{4,0} + m_{3,4} + m_{3,2} + m_{2,3} + m_{2,2} + m_{1,31} + m_{0,3} = 0,$
$m_{13,0} + m_{1,31} = 1,\ m_{12,31} = 1,\ m_{12,30} = 0,\ m_{12,29} = 1,$
$m_{12,0} + m_{4,0} + m_{3,0} + m_{1,31} + m_{1,0} = 0,\ m_{11,31} = 1,\ m_{11,30} = 0,\ m_{11,29} = 1,\ m_{11,6} = 1,\ m_{11,4} = 1,\ m_{11,1} = 1,$
$m_{11,0} + m_{1,31} = 0,\ m_{10,31} = 0,\ m_{10,30} = 0,\ m_{10,29} = 0,\ m_{10,6} = 0,\ m_{10,5} + m_{4,5} + m_{2,5} = 0,$
$m_{10,0} + m_{4,0} + m_{1,0} = 0,\ m_{9,31} + m_{3,31} + m_{3,0} + m_{1,0} = 1,\ m_{9,30} = 0,\ m_{9,29} = 1,\ m_{9,6} = 0,$
$m_{9,5} + m_{8,5} + m_{6,5} + m_{3,5} = 0,\ m_{9,4} = 1,\ m_{9,1} = 1,\ m_{9,0} + m_{3,0} + m_{1,0} = 0,\ m_{8,31} = 0,\ m_{8,30} = 1,\ m_{8,1} = 0,$
$m_{8,0} = 0,\ m_{7,31} + m_{3,31} + m_{1,31} + m_{1,0} = 0,\ m_{7,30} = 1,\ m_{7,5} = 1,\ m_{7,0} + m_{3,0} = 0,\ m_{6,31} = 0,\ m_{6,30} = 0,\ m_{6,0} = 0,$
$m_{5,31} + m_{3,31} = 0,\ m_{5,30} = 1,\ m_{5,29} = 1,\ m_{5,1} = 1,\ m_{5,0} + m_{3,0} + m_{1,31} = 1,\ m_{4,31} = 0,\ m_{4,30} = 0,\ m_{4,29} = 0,$
$m_{4,6} = 0,\ m_{4,1} = 1,\ m_{3,30} = 1,\ m_{3,29} = 0,\ m_{3,6} = 1,\ m_{2,31} = 0,\ m_{2,30} = 1,\ m_{2,29} = 0,\ m_{2,6} = 1,\ m_{2,1} = 1,$
$m_{2,0} = 1,\ m_{1,30} = 0,\ m_{1,29} = 1,\ m_{1,5} = 0,\ m_{1,4} = 1,\ m_{1,1} = 1,\ m_{0,31} = 0,\ m_{0,30} = 0,\ m_{0,29} = 0$

The result of the Conventional Message Modification After Step 2 in Algorithm 2, still 34 conditions remain as listed below:
$a_{17,3} = 1, a_{17,2} = 0, a_{17,1} = 0, a_{26,1} = 1, a_{27,0} = 1, a_{29,1} = 0, a_{30,1} = 0, a_{33,1} = 1, a_{37,1} = 1, a_{39,1} = 0, a_{41,1} = 0, a_{43,1} = 0, a_{20,30} + a_{18,0} = 1, a_{21,30} + a_{20,0} = 0, a_{24,30} + a_{22,0} = 0, a_{25,30} + a_{24,0} = 1, a_{25,3} + a_{24,3} = 0, a_{26,2} + a_{25,2} = 1, a_{28,30} + a_{26,0} = 0, a_{28,3} + a_{27,3} = 1, a_{29,30} + a_{28,0} = 1, a_{29,3} + a_{28,3} = 1, a_{32,3} + a_{31,3} = 1, a_{36,3} + a_{35,3} = 1, a_{38,3} + a_{37,3} = 1, a_{39,31} + a_{38,1} = 1, a_{40,3} + a_{39,3} = 1, a_{40,31} + a_{38,1} = 1, a_{41,31} + a_{40,1} = 1, a_{42,31} + a_{40,1} = 1, a_{43,31} + a_{42,1} = 1, a_{42,3} + a_{41,3} = 1, a_{44,31} + a_{42,1} = 1, a_{45,31} + a_{44,1} = 1.$

Among the above conditions, there are five conditions $a_{17,3} = 1$, $a_{17,2} = 0$, $a_{17,1=0}$, $a_{20,30} + a_{18,0} = 1$, $a_{21,30} + a_{20,0} = 0$ which are related to only first 23 rounds. The probability that these five conditions are satisfied after the conventional message modification (Step 2 of Algorithm 2) is $1/2^5$. For other 29 conditions, we adjust by using 21 semi-neutral bits and 11 adjusters after Step 3 in Algorithm 2.

New Collisions New collisions we found are listed in the following.

$$\begin{aligned} m &= 0x1ead6636319fe59e4ea7ddcbc79616420ad9523af98f28db0ad135d0e4d62aec \\ &\quad 6c2da52c3c7160b606ec74b2b02d545ebdd9e4663f1563194f497592dd1506f9 \\ m' &= 0x3ead6636519fe5ac2ea7dd88e7961602ead95278998f28d98ad135d1e4d62acc \\ &\quad 6c2da52f7c7160e446ec74f2502d540c1dd9e466bf1563596f497593fd150699 \end{aligned}$$

$$\begin{aligned} m &= 0x16507a963da18c5f4195d14bd55695ea0cb08092f79649bb0717a22658c119fc \\ &\quad 5a36c1f8b960383b08929187ae9842fab690d8710452419d585d012edcaf0278 \\ m' &= 0x36507a965da18c6d2195d108f55695aaecb080d0979649b98717a22758c119dc \\ &\quad 5a36c1fbf9603869489291c74e9842a81690d871845241dd785d012ffcaf0218 \end{aligned}$$

$$\begin{aligned} m &= 0x1eae299630efec5e5d2c494b573f8eea11ef20b27b4fbd1b0713f0585a1e1bbe \\ &\quad 6d332488a82958be0a108f32a67a37dabeab1d0c2c8ec4bd4b947b3ccd389b6d \\ m' &= 0x3eae299650efec6c3d2c4908773f8eaaf1ef20f01b4fbd198713f0595a1e1b9e \\ &\quad 6d33248be82958ec4a108f72467a37881eab1d0cac8ec4fd6b947b3ded389b0d \end{aligned}$$

Control sequence s_i	Control bit b_i	Controlled relation r_i
s_{124}	$a_{16,7}$, $a_{15,9}$, $a_{14,9}$	$a_{23,0} = 0$
s_{123}	$a_{16,9}$	$a_{22,2} + a_{21,2} = 1$
s_{122}	$a_{16,13}$, $a_{15,15}$, $a_{15,12}$, $a_{15,11}$	$a_{22,1} = 1$
s_{121}	$a_{16,10}$	$a_{21,3} + m_{20,3} = 0$
s_{120}	$a_{16,8}$	$a_{21,1} = 1$
s_{119}	$a_{16,15}$, $a_{16,20}$	$a_{20,3} + m_{19,3} = 1$
s_{118}	$a_{16,17}$	$a_{19,0} = 0$
s_{117}	$a_{16,21}$	$a_{18,31} = 1$
s_{116}	$a_{16,19}$	$a_{18,29} = 1$
s_{115}	$a_{13,4}$	$a_{18,2} = 0$
s_{114}	$a_{13,3}$	$a_{18,1} = 0$
s_{113}	$a_{14,15}$	$a_{17,30} = 0$
s_{112}	$a_{16,31}$	$m_{15,31} = 1$
s_{111}	$a_{16,29}$	$m_{15,29} = 0$
s_{110}	$a_{16,28}$	$m_{15,28} + m_{10,28} + m_{8,29} + m_{7,29} + m_{4,28} + m_{2,28} = 1$
s_{109}	$a_{16,27}$, $a_{13,28}$	$m_{15,27} + m_{14,25} + m_{12,28} + m_{12,26} + m_{10,28} + m_{9,27} + m_{9,25} + m_{8,29} + m_{8,28} + m_{7,28} + m_{7,27} + m_{6,26} + m_{5,28} + m_{4,26} + m_{3,25} + m_{2,28} + m_{1,25} + m_{0,28} = 1$
s_{108}	$a_{16,26}$	$m_{15,26} + m_{10,28} + m_{10,26} + m_{8,28} + m_{8,27} + m_{7,27} + m_{6,29} + m_{5,27} + m_{4,26} + m_{2,27} + m_{2,26} + m_{0,27} = 1$
s_{107}	$a_{16,25}$	$m_{15,25} + m_{11,28} + m_{10,27} + m_{10,25} + m_{9,28} + m_{8,27} + m_{8,26} + m_{7,26} + m_{6,29} + m_{6,28} + m_{5,26} + m_{4,25} + m_{3,28} + m_{2,28} + m_{2,26} + m_{2,25} + m_{1,28} + m_{0,28} + m_{0,26} = 0$
s_{106}	$a_{16,24}$	$m_{15,24} + m_{12,28} + m_{11,27} + m_{10,26} + m_{10,24} + m_{9,28} + m_{9,27} + m_{8,29} + m_{8,26} + m_{8,25} + m_{7,25} + m_{6,29} + m_{6,28} + m_{6,27} + m_{5,25} + m_{4,28} + m_{4,24} + m_{3,28} + m_{3,27} + m_{2,27} + m_{2,25} + m_{2,24} + m_{1,28} + m_{1,27} + m_{0,27} + m_{0,25} = 1$
s_{105}	$a_{16,23}$	$m_{15,23} + m_{12,28} + m_{12,27} + m_{11,26} + m_{10,25} + m_{10,23} + m_{9,27} + m_{9,26} + m_{8,28} + m_{8,25} + m_{8,24} + m_{7,29} + m_{7,24} + m_{6,28} + m_{6,27} + m_{6,26} + m_{5,24} + m_{4,27} + m_{4,23} + m_{3,27} + m_{3,26} + m_{2,26} + m_{2,24} + m_{2,23} + m_{1,27} + m_{1,26} + m_{0,26} + m_{0,24} = 1$
s_{104}	$a_{16,22}$	$m_{15,22} + m_{14,25} + m_{12,28} + m_{12,27} + m_{11,25} + m_{10,27} + m_{10,24} + m_{10,22} + m_{9,28} + m_{9,27} + m_{9,26} + m_{8,27} + m_{8,24} + m_{8,23} + m_{7,28} + m_{7,27} + m_{7,23} + m_{6,27} + m_{6,25} + m_{5,23} + m_{4,28} + m_{4,27} + m_{4,22} + m_{3,26} + m_{2,28} + m_{2,27} + m_{2,25} + m_{2,23} + m_{2,22} + m_{1,26} + m_{0,25} + m_{0,23} = 0$
s_{103}	$a_{16,6}$	$m_{15,6} = 1$
s_{102}	$a_{16,5}$	$m_{15,5} = 1$
s_{101}	$a_{16,4}$	$m_{15,4} + m_{12,5} + m_{10,4} + m_{4,5} + m_{4,4} + m_{2,5} + m_{2,4} = 1$
s_{100}	$a_{16,2}$	$m_{15,2} + m_{12,5} + m_{11,5} + m_{10,4} + m_{10,2} + m_{8,4} + m_{8,3} + m_{7,3} + m_{5,5} + m_{5,3} + m_{4,5} + m_{4,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{0,3} = 1$
s_{99}	$a_{16,1}$	$m_{15,1} + m_{12,5} + m_{11,3} + m_{11,2} + m_{10,4} + m_{10,2} + m_{9,2} + m_{8,3} + m_{8,2} + m_{5,4} + m_{4,5} + m_{4,4} + m_{4,0} + m_{3,31} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,4} + m_{2,3} + m_{1,31} + m_{0,3} = 0$
s_{98}	$a_{16,0}$	$m_{15,0} + m_{1,0} = 1$
s_{97}	$a_{15,30}$	$m_{15,3} + m_{12,2} + m_{10,2} + m_{8,3} + m_{7,3} + m_{7,2} + m_{5,3} + m_{4,2} + m_{3,4} + m_{3,2} + m_{2,3} + m_{2,2} + m_{1,2} + m_{0,3} = 0$
s_{96}	$a_{15,25}$	$m_{15,30} = 1$
s_{95}	$a_{14,26}$	$m_{14,31} = 0$
s_{94}	$a_{14,25}$	$m_{14,30} = 1$
s_{93}	$a_{15,29}$	$m_{14,29} = 0$
s_{92}	$a_{15,28}$	$m_{14,28} + m_{9,28} + m_{6,29} + m_{3,28} + m_{1,28} = 0$
s_{91}	$a_{15,27}$	$m_{14,27} + m_{12,28} + m_{9,27} + m_{7,29} + m_{6,28} + m_{4,28} + m_{3,27} + m_{1,27} = 0$
s_{90}	$a_{15,26}$	$m_{14,26} + m_{12,27} + m_{10,28} + m_{9,28} + m_{9,26} + m_{7,28} + m_{6,27} + m_{4,28} + m_{4,27} + m_{3,26} + m_{2,28} + m_{1,26} = 1$
s_{89}	$a_{15,24}$	$m_{14,24} + m_{12,27} + m_{12,25} + m_{11,28} + m_{10,27} + m_{10,26} + m_{9,26} + m_{9,24} + m_{8,29} + m_{7,26} + m_{6,29} + m_{6,25} + m_{5,28} + m_{4,28} + m_{4,26} + m_{4,25} + m_{3,28} + m_{3,24} + m_{2,26} + m_{1,24} + m_{0,28} = 0$
s_{88}	$a_{15,23}$	$m_{14,23} + m_{12,26} + m_{12,24} + m_{11,27} + m_{10,26} + m_{10,25} + m_{9,28} + m_{9,25} + m_{9,23} + m_{8,28} + m_{7,25} + m_{6,28} + m_{6,24} + m_{5,27} + m_{4,27} + m_{4,25} + m_{4,24} + m_{3,28} + m_{3,27} + m_{3,23} + m_{2,25} + m_{1,28} + m_{1,23} + m_{0,27} = 1$
s_{87}	$a_{15,22}$	$m_{14,22} + m_{13,20} + m_{12,25} + m_{12,24} + m_{12,23} + m_{11,28} + m_{11,23} + m_{11,21} + m_{10,27} + m_{9,26} + m_{9,24} + m_{9,23} + m_{8,29} + m_{8,27} + m_{8,26} + m_{8,25} + m_{8,22} + m_{8,20} + m_{7,26} + m_{7,25} + m_{6,29} + m_{6,23} + m_{6,22} + m_{5,28} + m_{5,25} + m_{5,21} + m_{4,28} + m_{4,26} + m_{4,25} + m_{4,23} + m_{3,28} + m_{3,24} + m_{3,21} + m_{2,26} + m_{2,20} + m_{1,24} + m_{0,28} + m_{0,25} + m_{0,20} = 1$
s_{86}	$a_{15,21}$	$m_{14,21} + m_{12,27} + m_{12,24} + m_{12,22} + m_{11,25} + m_{10,28} + m_{10,27} + m_{10,24} + m_{10,23} + m_{9,28} + m_{9,26} + m_{9,23} + m_{9,21} + m_{8,29} + m_{8,26} + m_{7,29} + m_{7,28} + m_{7,23} + m_{6,29} + m_{6,26} + m_{6,22} + m_{5,25} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,23} + m_{4,22} + m_{3,26} + m_{3,25} + m_{3,21} + m_{2,28} + m_{2,23} + m_{1,26} + m_{1,21} + m_{0,25} = 0$
s_{85}	$a_{15,20}$	$m_{14,20} + m_{12,26} + m_{12,23} + m_{12,21} + m_{11,28} + m_{11,24} + m_{10,28} + m_{10,27} + m_{10,26} + m_{10,23} + m_{10,22} + m_{9,27} + m_{9,25} + m_{9,22} + m_{9,20} + m_{8,28} + m_{8,25} + m_{7,28} + m_{7,27} + m_{7,22} + m_{6,29} + m_{6,28} + m_{6,25} + m_{6,21} + m_{5,24} + m_{4,27} + m_{4,26} + m_{4,24} + m_{4,22} + m_{4,21} + m_{3,28} + m_{3,25} + m_{3,24} + m_{3,20} + m_{2,27} + m_{2,22} + m_{1,25} + m_{1,20} + m_{0,28} + m_{0,24} + m_{47,31} = 1$

Table 4. Control bit and controlled relations of 58-round SHA-1 (I)

Control sequence s_i	Control bit b_i	Controlled relation r_i
s_{84}	$a_{15,5}$	$m_{14,5} + m_{8,5} + m_{6,5} = 1$
s_{83}	$a_{15,4}$	$m_{14,4} + m_{12,5} + m_{11,3} + m_{11,2} + m_{10,4} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2}$ $+m_{8,5} + m_{7,2} + m_{6,5} + m_{6,4} + m_{5,4} + m_{5,2} + m_{4,5} + m_{4,4} + m_{4,0} + m_{3,31}$ $+m_{3,4} + m_{3,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{1,31} + m_{0,4} + m_{0,3} + m_{0,2} = 1$
s_{82}	$a_{14,30}$	$m_{14,3} + m_{11,3} + m_{11,2} + m_{8,2} + m_{7,4} + m_{7,2} + m_{7,1} + m_{6,2} + m_{5,3}$ $+m_{4,0} + m_{3,3} + m_{2,2} + m_{1,31} + m_{1,3} = 0$
s_{81}	$a_{15,2}$	$m_{14,2} + m_{12,5} + m_{12,3} + m_{10,4} + m_{9,2} + m_{7,4} + m_{6,3} + m_{4,5} + m_{4,4}$ $+m_{4,3} + m_{3,2} + m_{2,5} + m_{2,4} + m_{1,2} = 1$
s_{80}	$a_{15,1}$	$m_{14,1} + m_{12,4} + m_{11,2} + m_{10,2} + m_{9,3} + m_{8,3} + m_{7,2} + m_{6,2} + m_{5,5}+$ $m_{5,2} + m_{4,4} + m_{3,31} + m_{3,4} + m_{3,2} + m_{3,1} + m_{2,4} + m_{2,3} + m_{0,3} = 0$
s_{79}	$a_{14,27}$	$m_{14,0} = 0$
s_{78}	$a_{13,26}$	$m_{13,31} = 0$
s_{77}	$a_{13,25}$	$m_{13,30} = 0$
s_{76}	$a_{14,29}$	$m_{13,29} + m_{8,29} = 0$
s_{75}	$a_{14,28}$	$m_{13,28} + m_{8,28} + m_{2,28} + m_{0,28} = 0$
s_{74}	$a_{13,22}$	$m_{13,27} + m_{11,28} + m_{8,29} + m_{8,27} + m_{6,29} + m_{5,28} + m_{3,28} + m_{2,27} + m_{0,27} = 1$
s_{73}	$a_{13,21}$	$m_{13,26} + m_{11,27} + m_{9,28} + m_{8,28} + m_{8,26} + m_{6,28} + m_{5,27} + m_{3,28} + m_{3,27}$ $+m_{2,26} + m_{1,28} + m_{0,26} = 1$
s_{72}	$a_{14,24}$	$m_{13,24} + m_{12,28} + m_{11,27} + m_{11,25} + m_{10,28} + m_{9,27} + m_{9,26} + m_{8,29} + m_{8,26}$ $+m_{8,24} + m_{7,29} + m_{7,28} + m_{6,26} + m_{5,25} + m_{4,28} + m_{3,28} + m_{3,26} + m_{3,25} + m_{2,28}$ $+m_{2,24} + m_{1,28} + m_{1,26} + m_{0,24} = 0$
s_{71}	$a_{14,23}$	$m_{13,23} + m_{12,27} + m_{11,26} + m_{11,24} + m_{10,28} + m_{10,27} + m_{9,26} + m_{9,25} + m_{8,29} +$ $m_{8,28} + m_{8,25} + m_{8,23} + m_{7,29} + m_{7,28} + m_{7,27} + m_{6,25} + m_{5,28} + m_{5,24} + m_{4,28}$ $+m_{4,27} + m_{3,27} + m_{3,25} + m_{3,24} + m_{2,27} + m_{2,23} + m_{1,27} + m_{1,25} + m_{0,28} + m_{0,23} = 0$
s_{70}	$a_{14,22}$	$m_{13,22} + m_{12,26} + m_{11,28} + m_{11,25} + m_{11,23} + m_{10,27} + m_{10,26} + m_{9,28} + m_{9,25}$ $+m_{9,24} + m_{8,28} + m_{8,27} + m_{8,24} + m_{8,22} + m_{7,28} + m_{7,27} + m_{7,26} + m_{6,29} + m_{6,24}$ $+m_{5,28} + m_{5,27} + m_{5,23} + m_{4,27} + m_{4,26} + m_{3,28} + m_{3,26} + m_{3,24} + m_{3,23} + m_{2,28}$ $+m_{2,26} + m_{2,22} + m_{1,26} + m_{1,24} + m_{0,28} + m_{0,27} + m_{0,22} = 1$
s_{69}	$a_{13,0}$	$m_{13,6} = 0$
s_{68}	$a_{14,5}$	$m_{13,5} + m_{12,5} + m_{5,5} + m_{4,5} + m_{2,5} = 0$
s_{67}	$a_{14,4}$	$m_{13,4} + m_{12,5} + m_{11,2} + m_{10,4} + m_{7,4} + m_{5,4} + m_{5,3} + m_{5,2} + m_{4,5} + m_{4,4} + m_{3,31}$ $+m_{2,5} + m_{2,4} + m_{2,2} + m_{1,2} = 0$
s_{66}	$a_{14,3}$	$m_{13,3} + m_{8,3} + m_{5,4} + m_{3,4} + m_{2,3} + m_{0,3} = 0$
s_{65}	$a_{13,28}$	$m_{13,2} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2} + m_{8,2} + m_{7,4} + m_{7,2} + m_{4,0} + m_{3,4} + m_{3,3}$ $+m_{3,2} + m_{2,3} + m_{2,2} + m_{1,31} + m_{1,2} + m_{0,3} = 0$
s_{64}	$a_{14,1}$	$m_{13,1} + m_{10,2} + m_{9,3} + m_{8,3} + m_{7,4} + m_{7,2} + m_{6,2} + m_{5,3} + m_{5,2} + m_{4,0} + m_{3,4}$ $+m_{3,2} + m_{2,3} + m_{2,2} + m_{1,31} + m_{0,3} = 0$

s_i	b_i	r_i
s_{63}	$a_{14,0}$	$m_{13,0} + m_{1,31} = 1$
s_{62}	$a_{12,26}$	$m_{12,31} = 1$
s_{61}	$a_{13,30}$	$m_{12,30} = 0$
s_{60}	$a_{12,24}$	$m_{12,29} = 1$
s_{59}	$a_{12,27}$	$m_{12,0} + m_{4,0} + m_{3,0} + m_{1,31} + m_{1,0} = 0$
s_{58}	$a_{11,26}$	$m_{11,31} = 1$
s_{57}	$a_{12,30}$	$m_{11,30} = 0$
s_{56}	$a_{11,24}$	$m_{11,29} = 1$
s_{55}	$a_{12,5}$	$m_{11,6} = 1$
s_{54}	$a_{11,0}$	$m_{11,6} = 1$
s_{53}	$a_{12,4}$	$m_{11,4} = 1$
s_{52}	$a_{12,1}$	$m_{11,1} = 1$
s_{51}	$a_{12,0}$	$m_{11,0} + m_{1,31} = 0$
s_{50}	$a_{10,26}$	$m_{10,31} = 0$
s_{49}	$a_{11,30}$	$m_{10,30} = 0$
s_{48}	$a_{10,24}$	$m_{10,29} = 0$
s_{47}	$a_{11,5}$	$m_{10,6} = 0$
s_{46}	$a_{10,0}$	$m_{10,5} + m_{4,5} + m_{2,5} = 0$
s_{45}	$a_{10,27}$	$m_{10,0} + m_{4,0} + m_{1,0} = 0$
s_{44}	$a_{9,26}$	$m_{9,31} + m_{3,31} + m_{3,0} + m_{1,0} = 1$
s_{43}	$a_{9,25}$	$m_{9,30} = 0$
s_{42}	$a_{10,30}$	$m_{9,30} = 0$
s_{41}	$a_{9,24}$	$m_{9,29} = 1$
s_{40}	$a_{9,0}$	$m_{9,6} = 0$
s_{39}	$a_{4,8}$	$m_{9,6} = 0$
s_{38}	$a_{10,5}$	$m_{9,5} + m_{8,5} + m_{6,5} + m_{3,5} = 0$
s_{37}	$a_{10,4}$	$m_{9,4} = 1$
s_{36}	$a_{9,28}$	$m_{9,1} = 1$
s_{35}	$a_{9,27}$	$m_{9,0} + m_{3,0} + m_{1,0} = 0$
s_{34}	$a_{8,26}$	$m_{8,31} = 0$
s_{33}	$a_{9,29}$	$m_{8,30} = 1$
s_{32}	$a_{8,28}$	$m_{8,1} = 0$
s_{31}	$a_{8,27}$	$m_{8,0} = 0$
s_{30}	$a_{8,31}$	$m_{7,31} + m_{3,31} + m_{1,31} + m_{1,0} = 0$

s_i	b_i	r_i
s_{29}	$a_{8,29}$	$m_{7,30} = 1$
s_{28}	$a_{8,4}$	$m_{7,5} = 1$
s_{27}	$a_{6,6}$	$m_{7,5} = 1$
s_{26}	$a_{8,0}$	$m_{7,0} + m_{3,0} = 0$
s_{25}	$a_{7,31}$	$m_{6,31} = 0$
s_{24}	$a_{7,29}$	$m_{6,30} = 0$
s_{23}	$a_{3,26}$	$m_{5,31} + m_{3,31} = 0$
s_{22}	$a_{5,25}$	$m_{5,30} = 1$
s_{21}	$a_{6,29}$	$m_{5,29} = 1$
s_{20}	$a_{6,1}$	$m_{5,1} = 1$
s_{19}	$a_{3,27}$	$m_{5,0} + m_{3,0} + m_{1,31} = 1$
s_{18}	$a_{4,26}$	$m_{4,31} = 0$
s_{17}	$a_{4,25}$	$m_{4,30} = 0$
s_{16}	$a_{5,29}$	$m_{4,29} = 0$
s_{15}	$a_{5,6}$	$m_{4,6} = 0$
s_{14}	$a_{5,1}$	$m_{4,1} = 1$
s_{13}	$a_{3,25}$	$m_{3,30} = 1$
s_{12}	$a_{3,24}$	$m_{3,29} = 0$
s_{11}	$a_{4,6}$	$m_{3,6} = 1$
s_{10}	$a_{2,26}$	$m_{2,31} = 0$
s_9	$a_{2,25}$	$m_{2,30} = 1$
s_8	$a_{2,24}$	$m_{2,29} = 0$
s_7	$a_{3,5}$	$m_{2,6} = 1$
s_6	$a_{2,6}$	$m_{2,6} = 1$
s_5	$a_{3,1}$	$m_{2,1} = 1$
s_4	$a_{2,5}$	$m_{1,5} = 0$
s_3	$a_{1,28}$	$m_{1,1} = 1$
s_2	$a_{1,25}$	$m_{1,30} = 0$
s_1	$a_{1,24}$	$m_{1,29} = 1$
s_0	$a_{1,23}$	$m_{1,29} = 1$

Table 5. Control bit and controlled relations of 58-round SHA-1 (II)(III)(IV)

message variable	31 - 24	23 - 16	15 - 8	8 - 0
m_0	--0-----	--------	--------	--------
m_1	-01-----	--------	--------	--01--1-
m_2	L10-----	--------	--------	-1----11
m_3	-L0-----	--------	--------	-1------
m_4	000-----	--------	--------	-0----1-
m_5	L11-----	--------	--------	------1L
m_6	0L------	--------	--------	-------0
m_7	LL------	--------	--------	--1----L
m_8	LL------	--------	--------	------00
m_9	L0L-----	--------	--------	-0L1--1L
m_{10}	L0L-----	--------	--------	-0L----L
m_{11}	101-----	--------	--------	-1-1--1L
m_{12}	1L1-----	--------	--------	-------L
m_{13}	0LLLLL-L	LL------	--------	-0LLLLLL
m_{14}	LL0LLL-L	LLLL----	--------	--LLLLL0
m_{15}	LL0LLLLL	LL------	--------	-11LLLLL
m_{16}	0-------	--------	--------	-------0
m_{17}	-0------	--------	--------	-1----0-
m_{18}	00------	--------	--------	-1----01
m_{19}	-0------	--------	--------	--1---1-
m_{20}	--------	--------	--------	------11
m_{21}	-0------	--------	--------	-0----1-
m_{22}	01------	--------	--------	-0----10
m_{23}	11------	--------	--------	--1---0-
m_{24}	--------	--------	--------	-------0
m_{25}	-1------	--------	--------	------1-
m_{26}	10------	--------	--------	-0----10
m_{27}	-1------	--------	--------	-01---0-
m_{28}	1-------	--------	--------	-------0
m_{29}	-1------	--------	--------	-1----0-
m_{30}	-0------	--------	--------	-1----0-
m_{31}	-1------	--------	--------	------0-
m_{32}	--------	--------	--------	------1-
m_{33}	--------	--------	--------	-0------
m_{34}	0-------	--------	--------	------1-
m_{35}	0-------	--------	--------	--------
m_{36}	1-------	--------	--------	------1-
m_{37}	1-------	--------	--------	-0------
m_{38}	--------	--------	--------	--------
m_{39}	0-------	--------	--------	-1------
m_{40}	1-------	--------	--------	--------
m_{41}	--------	--------	--------	-1------
m_{42}	1-------	--------	--------	--------
m_{43}	--------	--------	--------	-1------
m_{44}	1-------	--------	--------	------1-
m_{45}	--------	--------	--------	--------
m_{46}	1-------	--------	--------	--------
m_{47}	0-------	--------	--------	--------
m_i $(i \geq 48)$	--------	--------	--------	--------

chaining variable	31 - 24	23 - 16	15 - 8	8 - 0
a_0	01100111	01000101	00100011	00000001
a_1	101V--vV	Y-------	--------	-1-a10aa
a_2	01100vVv	------0-	----a---	1-w00010
a_3	0010--Vv	-10---1a	------0-	0aX1a0W0
a_4	11010vv-	-01-----	01aaa---	0W10-100
a_5	10w01aV-	-1-01-aa	--00100-	0w--01W1
a_6	11W-0110	-a-1001-	01100010	1-a111W1
a_7	w1x-1110	a1a1111-	-101-001	1---0-10
a_8	h0Xvvv10	0000000a	a001a1--	100X0-1h
a_9	00XVrr-V	11000100	00000000	101-1-1y
a_{10}	0w1-rv-v	11111011	11100000	00hW0-1h
a_{11}	1w0--V-V	-------1	01111110	11x---0Y
a_{12}	0w1-rV-V	--------	--------	-1XWa-Wh
a_{13}	1w0--vv-	-rr-----	--------	-1-qq01y
a_{14}	1rhhvvVh	hh------	qNNNNNqN	N1hhh1hh
a_{15}	0rwhhhVh	hhhh---N	qNNqqNqN	NNhh0hh0
a_{16}	W1whhhhh	hhqNqNqN	NNqNNqqq	qWWhahhh
a_{17}	-0------	--------	--------	----100-
a_{18}	1-1-----	--------	--------	-----00-
a_{19}	--------	--------	--------	-------0
a_{20}	-C------	--------	--------	----A---
a_{21}	-b------	--------	--------	----a-1-
a_{22}	--------	--------	--------	-----A1-
a_{23}	--------	--------	--------	-------0
a_{24}	-c------	--------	--------	--------
a_{25}	-B------	--------	--------	----a---
a_{26}	--------	--------	--------	-----A1-
a_{27}	--------	--------	--------	-------1
a_{28}	-c------	--------	--------	----A---
a_{29}	-B------	--------	--------	----A-0-
a_{30}	--------	--------	--------	------0-
a_{31}	--------	--------	--------	--------
a_{32}	--------	--------	--------	----A---
a_{33}	--------	--------	--------	------1-
a_{34}	--------	--------	--------	--------
a_{35}	--------	--------	--------	--------
a_{36}	--------	--------	--------	----A---
a_{37}	--------	--------	--------	------1-
a_{38}	--------	--------	--------	----A---
a_{39}	B-------	--------	--------	------0-
a_{40}	C-------	--------	--------	----A---
a_{41}	B-------	--------	--------	------0-
a_{42}	C-------	--------	--------	----A---
a_{43}	B-------	--------	--------	------0-
a_{44}	C-------	--------	--------	--------
a_{45}	B-------	--------	--------	--------
a_i $(i \geq 46)$	--------	--------	--------	--------

Table 6. 'Advanced' sufficient conditions on $\{m_{i,j}\}$ and $\{a_{i,j}\}$ for the 58-round SHA-1

$$m = 0x1a9d9116b33b165e51f5734bd7761b4319b8bf12fa65c2f30b46c73c66e1f76f$$
$$585d297cb97102171ad29716b4e2f5d7aa5b68fa132f8b185f254eaad13145e5$$
$$m' = 0x3a9d9116d33b166c31f57308f7761b03f9b8bf509a65c2f18b46c73d66e1f74f$$
$$585d297ff97102455ad2975654e2f5850a5b68fa932f8b587f254eabf1314585$$

$$m = 0x1a4e6f36bcf6cb9e5380d8cb482719cb134c7b2a6aeccefb0bb249bcdfa35ba9$$
$$623b26c02ed018bb0f0a4fbca21ec47bac46d7b629647720525006c6c4abc561$$
$$m' = 0x3a4e6f36dcf6cbac3380d8886827198bf34c7b680aeccef98bb249bddfa35b89$$
$$623b26c36ed018e94f0a4ffc421ec4290c46d7b6a9647760725006c7e4abc501$$

8 Analysis of the full SHA-1 based on our method

For the full SHA-1, Wang's attack tries to find a two-block collision, which is called a two-iteration attack. Here we analyze a two-iteration attack based on our method. We note that our current result is only for an attack on the first block, but our method would be efficient for an attack on the second block.

8.1 Disturbance vector and Message differential

We start from a partial information of a disturbance vector and messge differential given by Wang et al. and construct a message differential for the full SHA-1. Here we correct Wang's message differential by changing $\Delta a^+_{14,31}$ and $\Delta a^-_{14,31}$. As we stated in Section 3, it is important to choose $\Delta^+ m$, $\Delta^- m$, $\Delta^+ a$ and $\Delta^- a$ carefully because a bad choice of plus/minus leads an indeterminate system of equations as a result of Gaussian elimination. We can construct a system of equations which gives conditions to take appropriate signature. We have to follow conditions given by such system of equations. For this reason, we have to correct Wang's message differential. We show a message differential we constructed in Table 7.

8.2 Sufficient conditions on $\{m_i\}$ and $\{a_i\}$

For the disturbance vector, the differential and the message differential given in the previous step, we give sufficient conditions on the full SHA-1. We show obtained conditions in Table 8.

In Table 8, 'a' means $a_{i,j} = a_{i-1,j}$, 'A' means $a_{i,j} = a_{i-1,j} + 1$, 'b' means $a_{i,j} = a_{i-1,(j+2 \mod 32)}$, 'B' means $a_{i,j} = a_{i-1,(j+2 \mod 32)} + 1$, 'c' means $a_{i,j} = a_{i-2,(j+2 \mod 32)}$ and 'C' means $a_{i,j} = a_{i-2,(j+2 \mod 32)} + 1$.

By the Gaussian elimination, we reduce all conditions on $\{m_i\}$ for $0-80$-round to relations of $0-15$-round. An elimination order of $\{m_{i,j}\}_{i=0,1,\ldots,15;j=0,1,\ldots,31}$ we use here is: $m'_{i',j'} \leq m_{i,j}$ if $i' \leq i$ or ($i' = i$ and $j' \leq j$). The result of Gaussian elimination is as follows. There are 167 conditions on $\{m_{i,j}\}$.

$m_{15,31} = 0$, $m_{15,30} = 1$, $m_{15,29} = 1$, $m_{15,28} + m_{10,28} + m_{4,28} + m_{2,28} = 0$, $m_{15,27} + m_{10,27} + m_{8,28} + m_{4,27} + m_{2,28} + m_{2,27} + m_{0,28} = 1$, $m_{15,26} + m_{10,28} + m_{10,26} + m_{8,28} + m_{8,27} + m_{7,27} + m_{5,27} + m_{4,26} + m_{2,27} + m_{2,26} + m_{0,27} = 0$, $m_{15,25} + m_{11,28} + m_{10,27} + m_{10,25} + m_{9,28} + m_{8,27} + m_{8,26} + m_{7,26} + m_{5,26} + m_{4,25} + m_{3,28} + m_{2,28} + m_{2,26} + m_{2,25} + m_{1,28} + m_{0,28} + m_{0,26} = 0$, $m_{15,24} + m_{12,28} + m_{11,27} + m_{10,26} + m_{10,24} + m_{9,28} + m_{9,27} + m_{8,26} + m_{8,25} + m_{7,25} + m_{6,27} + m_{5,25} + m_{4,28} + m_{4,24} + m_{3,28} + m_{3,27} + m_{2,27} + m_{2,25} + m_{2,24} + m_{1,28} + m_{1,27} + m_{0,27} + m_{0,25} = 1$, $m_{15,23} + m_{12,28} + m_{12,27} + m_{11,26} + m_{10,25} + m_{10,23} + m_{9,27} + m_{9,26} + m_{8,28} + m_{8,25} + m_{8,24} + m_{7,24} + m_{7,0} + m_{6,27} + m_{6,26} + m_{5,24} + m_{4,27} + m_{4,23} + m_{3,27} + m_{3,26} + m_{2,26} + m_{2,24} + m_{2,23} + m_{1,30} + m_{1,27} + m_{1,26} + m_{1,0} + m_{0,26} + m_{0,24} = 0$, $m_{15,22} + m_{12,27} + m_{12,26} + m_{11,25} + m_{10,28} + m_{10,24} + m_{10,22} + m_{9,28} + m_{9,26} + m_{9,25} + m_{8,27} + m_{8,24} + m_{8,23} + m_{7,23} + m_{6,27} +$

	$\Delta^{\pm} m$	$\Delta^{+} m$	$\Delta^{-} m$
$i = 0$	$a0000003$	00000001	$a0000002$
$i = 1$	20000030	20000020	00000010
$i = 2$	60000000	60000000	00000000
$i = 3$	$e000002a$	40000000	$a000002a$
$i = 4$	20000043	20000042	00000001
$i = 5$	$b0000040$	$a0000000$	10000040
$i = 6$	$d0000053$	$d0000042$	00000011
$i = 7$	$d0000022$	$d0000000$	00000022
$i = 8$	20000000	00000000	20000000
$i = 9$	60000032	20000030	40000002
$i = 10$	60000043	60000041	00000002
$i = 11$	20000040	00000000	20000040
$i = 12$	$e0000042$	$c0000000$	20000042
$i = 13$	60000002	00000002	60000000
$i = 14$	80000001	00000001	80000000
$i = 15$	00000020	00000020	00000000
$i = 16$	00000003	00000002	00000001
$i = 17$	40000052	00000002	40000050
$i = 18$	40000040	00000000	40000040
$i = 19$	$e0000052$	00000002	$e0000050$
$i = 20$	$a0000000$	00000000	$a0000000$
$i = 21$	80000040	80000000	00000040
$i = 22$	20000001	00000001	20000000
$i = 23$	20000060	00000000	20000060
$i = 24$	80000001	00000000	80000001
$i = 25$	40000042	00000000	40000042
$i = 26$	$c0000043$	40000041	80000002
$i = 27$	40000022	00000002	40000020
$i = 28$	00000003	00000001	00000002
$i = 29$	40000042	40000042	00000000
$i = 30$	$c0000043$	00000002	$c0000041$
$i = 31$	$c0000022$	00000020	$c0000002$
$i = 32$	00000001	00000000	00000001
$i = 33$	40000002	40000002	00000000
$i = 34$	$c0000043$	$c0000003$	00000040
$i = 35$	40000062	40000000	00000062
$i = 36$	80000001	00000001	80000000
$i = 37$	40000042	00000042	40000000
$i = 38$	40000042	40000000	00000042
$i = 39$	40000002	00000002	40000000
$i = 40$	00000002	00000000	00000002
$i = 41$	00000040	00000040	00000000
$i = 42$	80000002	80000002	00000000
$i = 43$	80000000	00000000	80000000
$i = 44$	80000002	80000002	00000000
$i = 45$	80000040	80000000	00000040
$i = 46$	00000000	00000000	00000000
$i = 47$	80000040	80000000	00000040
$i = 48$	80000000	80000000	00000000
$i = 49$	00000040	00000000	00000040
$i = 50$	80000000	80000000	00000000
$i = 51$	00000040	00000000	00000040
$i = 52$	80000002	00000000	80000002
$i = 53$	00000000	00000000	00000000
$i = 54$	80000000	00000000	80000000
$i = 55$	80000000	80000000	00000000
$i = 56$	00000000	00000000	00000000
$i = 57$	00000000	00000000	00000000
$i = 58$	00000000	00000000	00000000
$i = 59$	00000000	00000000	00000000
$i = 60$	00000000	00000000	00000000
$i = 61$	00000000	00000000	00000000
$i = 62$	00000000	00000000	00000000
$i = 63$	00000000	00000000	00000000
$i = 64$	00000000	00000000	00000000
$i = 65$	00000000	00000000	00000000
$i = 66$	00000004	00000004	00000000
$i = 67$	00000080	00000000	00000080
$i = 68$	00000004	00000004	00000000
$i = 69$	00000009	00000009	00000000
$i = 70$	00000101	00000001	00000100
$i = 71$	00000009	00000008	00000001
$i = 72$	00000012	00000012	00000000
$i = 73$	00000202	00000002	00000200
$i = 74$	$0000001a$	00000018	00000002
$i = 75$	00000124	00000004	00000120
$i = 76$	$0000040c$	$0000040c$	00000000
$i = 77$	00000026	00000002	00000024
$i = 78$	$0000004a$	00000002	00000048
$i = 79$	$0000080a$	00000808	00000002
$i = 80$	00000000	00000000	00000000

	$\Delta^{\pm} a$	$\Delta^{+} a$	$\Delta^{-} a$
$i = 0$	00000000	00000000	00000000
$i = 1$	$e0000001$	$a0000000$	40000001
$i = 2$	20000004	20000000	00000004
$i = 3$	$c07fff84$	$803fff84$	40400000
$i = 4$	$800030e2$	$800010a0$	00002042
$i = 5$	$084080b0$	08008020	00400090
$i = 6$	$80003a00$	$00001a00$	80002000
$i = 7$	$0fff8001$	08000001	$07ff8000$
$i = 8$	00000008	00000008	00000000
$i = 9$	80000101	80000100	00000001
$i = 10$	00000002	00000002	00000000
$i = 11$	00000100	00000000	00000100
$i = 12$	00000002	00000002	00000000
$i = 13$	00000000	00000000	00000000
$i = 14$	00000000	00000000	00000000
$i = 15$	00000001	00000001	00000000
$i = 16$	00000000	00000000	00000000
$i = 17$	80000002	80000002	00000000
$i = 18$	00000002	00000002	00000000
$i = 19$	80000002	80000002	00000000
$i = 20$	00000000	00000000	00000000
$i = 21$	00000002	00000002	00000000
$i = 22$	00000000	00000000	00000000
$i = 23$	00000003	00000003	00000000
$i = 24$	00000000	00000000	00000000
$i = 25$	00000002	00000002	00000000
$i = 26$	00000002	00000000	00000002
$i = 27$	00000001	00000001	00000000
$i = 28$	00000000	00000000	00000000
$i = 29$	00000002	00000000	00000002
$i = 30$	00000002	00000002	00000000
$i = 31$	00000001	00000000	00000001
$i = 32$	00000000	00000000	00000000
$i = 33$	00000000	00000000	00000000
$i = 34$	00000002	00000002	00000000
$i = 35$	00000003	00000003	00000000
$i = 36$	00000000	00000000	00000000
$i = 37$	00000002	00000000	00000002
$i = 38$	00000002	00000002	00000000
$i = 39$	00000000	00000000	00000000
$i = 40$	00000000	00000000	00000000
$i = 41$	00000002	00000000	00000002
$i = 42$	00000000	00000000	00000000
$i = 43$	00000000	00000000	00000000
$i = 44$	00000000	00000000	00000000
$i = 45$	00000002	00000002	00000000
$i = 46$	00000000	00000000	00000000
$i = 47$	00000002	00000002	00000000
$i = 48$	00000000	00000000	00000000
$i = 49$	00000002	00000002	00000000
$i = 50$	00000000	00000000	00000000
$i = 51$	00000002	00000002	00000000
$i = 52$	00000000	00000000	00000000
$i = 53$	00000000	00000000	00000000
$i = 54$	00000000	00000000	00000000
$i = 55$	00000000	00000000	00000000
$i = 56$	00000000	00000000	00000000
$i = 57$	00000000	00000000	00000000
$i = 58$	00000000	00000000	00000000
$i = 59$	00000000	00000000	00000000
$i = 60$	00000000	00000000	00000000
$i = 61$	00000000	00000000	00000000
$i = 62$	00000000	00000000	00000000
$i = 63$	00000000	00000000	00000000
$i = 64$	00000000	00000000	00000000
$i = 65$	00000000	00000000	00000000
$i = 66$	00000000	00000000	00000000
$i = 67$	00000004	00000004	00000000
$i = 68$	00000000	00000000	00000000
$i = 69$	00000000	00000000	00000000
$i = 70$	00000008	00000008	00000000
$i = 71$	00000000	00000000	00000000
$i = 72$	00000000	00000000	00000000
$i = 73$	00000010	00000010	00000000
$i = 74$	00000000	00000000	00000000
$i = 75$	00000008	00000008	00000000
$i = 76$	00000020	00000000	00000020
$i = 77$	00000000	00000000	00000000
$i = 78$	00000000	00000000	00000000
$i = 79$	00000040	00000000	00000040
$i = 80$	00000000	00000000	00000000

Table 7. A message differential for the full SHA-1

message variable	31 - 24	23 - 16	15 - 8	8 - 0
m_0	1-1-----	--------	--------	------10
m_1	--0-----	--------	--------	--01----
m_2	-00-----	--------	--------	--------
m_3	101-----	--------	--------	--1-1-1-
m_4	--0-----	--------	--------	-0----01
m_5	0-01----	--------	--------	-1------
m_6	00-0----	--------	--------	-0-1--01
m_7	00-0----	--------	--------	--1---1-
m_8	--1-----	--------	--------	--------
m_9	-10-----	--------	--------	--00--1-
m_{10}	-00-----	--------	--------	-0----10
m_{11}	--1-----	--------	--------	-1------
m_{12}	001-----	--------	--------	-1----1-
m_{13}	-11-----	--------	--------	------0-
m_{14}	1-------	--------	--------	-------0
m_{15}	--------	--------	--------	--0-----
m_{16}	--------	--------	--------	------01
m_{17}	-1------	--------	--------	-1-1--0-
m_{18}	-1------	--------	--------	-1------
m_{19}	111-----	--------	--------	-1-1--0-
m_{20}	1-1-----	--------	--------	--------
m_{21}	0-------	--------	--------	-1------
m_{22}	--1-----	--------	--------	-------0
m_{23}	--1-----	--------	--------	-11-----
m_{24}	1-------	--------	--------	-------1
m_{25}	-1------	--------	--------	-1----1-
m_{26}	10------	--------	--------	-0----10
m_{27}	-1------	--------	--------	--1---0-
m_{28}	--------	--------	--------	------10
m_{29}	-0------	--------	--------	-0----0-
m_{30}	11------	--------	--------	-1----01
m_{31}	11------	--------	--------	--0---1-
m_{32}	--------	--------	--------	-------1
m_{33}	-0------	--------	--------	------0-
m_{34}	00------	--------	--------	-1----00
m_{35}	-0------	--------	--------	-11---1-
m_{36}	1-------	--------	--------	-------0
m_{37}	-1------	--------	--------	-0----0-
m_{38}	-0------	--------	--------	-1----1-
m_{39}	-1------	--------	--------	------0-
m_{40}	--------	--------	--------	------1-
m_{41}	--------	--------	--------	-0------
m_{42}	0-------	--------	--------	------0-
m_{43}	1-------	--------	--------	--------
m_{44}	0-------	--------	--------	------0-
m_{45}	0-------	--------	--------	-1------
m_{46}	--------	--------	--------	--------
m_{47}	0-------	--------	--------	-1------
m_{48}	0-------	--------	--------	--------
m_{49}	--------	--------	--------	-1------
m_{50}	0-------	--------	--------	--------
m_{51}	--------	--------	--------	-1------
m_{52}	1-------	--------	--------	------1-
m_{53}	--------	--------	--------	--------
m_{54}	1-------	--------	--------	--------
m_{55}	0-------	--------	--------	--------
m_{56}	--------	--------	--------	--------
m_{57}	--------	--------	--------	--------
m_{58}	--------	--------	--------	--------
m_{59}	--------	--------	--------	--------
m_{60}	--------	--------	--------	--------
m_{61}	--------	--------	--------	--------
m_{62}	--------	--------	--------	--------
m_{63}	--------	--------	--------	--------
m_{64}	--------	--------	--------	--------
m_{65}	--------	--------	--------	--------
m_{66}	--------	--------	--------	-----0--
m_{67}	--------	--------	--------	1-------
m_{68}	--------	--------	--------	-----0--
m_{69}	--------	--------	--------	----0--0
m_{70}	--------	--------	-------1	-------0
m_{71}	--------	--------	--------	----0--1
m_{72}	--------	--------	--------	---0--0-
m_{73}	--------	--------	------1-	------0-
m_{74}	--------	--------	--------	---00-1-
m_{75}	--------	--------	-------1	--1--0--
m_{76}	--------	--------	-----0--	----00--
m_{77}	--------	--------	--------	--1--10-
m_{78}	--------	--------	--------	-1--1-0-
m_{79}	--------	--------	----0---	----0-1-
m_{80}	--------	--------	--------	--------

chaining variable	31 - 24	23 - 16	15 - 8	8 - 0
a_0	01100111	01000101	00100011	00000001
a_1	010----0	-0-01-0-	10-0-10-	---a0101
a_2	-100---1	0aa10a1a	01a1a011	1--a11a1
a_3	01011---	-1000000	00000000	01--a0a1
a_4	0-101--a	---10000	00101000	010---10
a_5	0-0101-1	-1-11110	00111-00	10010100
a_6	1-0a1a0a	a0a1aaa-	--10010-	--01-0--
a_7	--0-0111	11111111	111-010-	0-0-0110
a_8	-10---01	11110000	010-111-	1---000-
a_9	00----11	11111111	111----0	----1-01
a_{10}	-11-----	--------	-----a--	-1--1-0-
a_{11}	100-----	--------	-------1	-1--0---
a_{12}	--------	--------	--------	-1----0-
a_{13}	0-------	--------	--------	-1---0--
a_{14}	1-------	--------	--------	-----1--
a_{15}	--------	--------	--------	----0--0
a_{16}	-1------	--------	--------	----1-A-
a_{17}	00------	--------	--------	----0-0-
a_{18}	1-1-----	--------	--------	----a-0-
a_{19}	0-b-----	--------	--------	------0-
a_{20}	--0-----	--------	--------	----a---
a_{21}	--b-----	--------	--------	------0-
a_{22}	--------	--------	--------	----aa--
a_{23}	--------	--------	--------	------00
a_{24}	-c------	--------	--------	----a---
a_{25}	-B------	--------	--------	----a-0-
a_{26}	--------	--------	--------	-----A1-
a_{27}	--------	--------	--------	-------0
a_{28}	-C------	--------	--------	----a---
a_{29}	-b------	--------	--------	----a-1-
a_{30}	--------	--------	--------	-----A0-
a_{31}	--------	--------	--------	-------1
a_{32}	-c------	--------	--------	--------
a_{33}	-b------	--------	--------	----a---
a_{34}	--------	--------	--------	----AA0-
a_{35}	--------	--------	--------	------00
a_{36}	-c------	--------	--------	----A---
a_{37}	-B------	--------	--------	----A-1-
a_{38}	--------	--------	--------	------0-
a_{39}	--------	--------	--------	--------
a_{40}	B-------	--------	--------	----A---
a_{41}	--------	--------	--------	------1-
a_{42}	C-------	--------	--------	--------
a_{43}	B-------	--------	--------	--------
a_{44}	--------	--------	--------	----A---
a_{45}	--------	--------	--------	------0-
a_{46}	C-------	--------	--------	----A---
a_{47}	B-------	--------	--------	------0-
a_{48}	C-------	--------	--------	----A---
a_{49}	B-------	--------	--------	------0-
a_{50}	C-------	--------	--------	----A---
a_{51}	B-------	--------	--------	------0-
a_{52}	C-------	--------	--------	--------
a_{53}	B-------	--------	--------	--------
a_{54}	--------	--------	--------	--------
a_{55}	--------	--------	--------	--------
a_{56}	--------	--------	--------	--------
a_{57}	--------	--------	--------	--------
a_{58}	--------	--------	--------	--------
a_{59}	--------	--------	--------	--------
a_{60}	--------	--------	--------	--------
a_{61}	--------	--------	--------	--------
a_{62}	--------	--------	--------	--------
a_{63}	--------	--------	--------	--------
a_{64}	--------	--------	--------	--------
a_{65}	--------	--------	--------	--------
a_{66}	--------	--------	--------	---A----
a_{67}	--------	--------	--------	-----0--
a_{68}	--------	--------	--------	-------C
a_{69}	--------	--------	--------	--A---B-
a_{70}	--------	--------	--------	----0---
a_{71}	--------	--------	--------	------C-
a_{72}	--------	--------	--------	-A----B-
a_{73}	--------	--------	--------	---0----
a_{74}	--------	--------	--------	--A--C--
a_{75}	--------	--------	--------	A---0B--
a_{76}	--------	--------	--------	--1---C-
a_{77}	--------	--------	--------	----C-B-
a_{78}	--------	--------	--------	----b---
a_{79}	--------	--------	--------	-1------
a_{80}	--------	--------	--------	--------

Table 8. Sufficient conditions for the full SHA-1

$$m_{6,26}+m_{6,25}+m_{5,23}+m_{4,28}+m_{4,26}+m_{4,22}+m_{3,26}+m_{3,25}+m_{2,28}+m_{2,25}+m_{2,23}+m_{2,22}+m_{1,26}+m_{1,25}+m_{0,25}+m_{0,23}=0,$$
$$m_{15,21}+m_{12,28}+m_{12,26}+m_{12,25}+m_{11,28}+m_{11,24}+m_{10,27}+m_{10,23}+m_{10,21}+m_{9,28}+m_{9,27}+m_{9,25}+m_{9,24}+m_{8,26}+m_{8,23}+m_{8,22}+$$
$$m_{7,27}+m_{7,22}+m_{6,26}+m_{6,25}+m_{6,24}+m_{5,22}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,21}+m_{3,25}+m_{3,24}+m_{2,27}+m_{2,24}+m_{2,22}+m_{2,21}+m_{1,28}+m_{1,25}+$$
$$m_{1,24}+m_{0,28}+m_{0,24}+m_{0,22}=0,\ m_{15,20}+m_{12,28}+m_{12,27}+m_{12,25}+m_{12,24}+m_{11,28}+m_{11,27}+m_{11,23}+m_{10,26}+m_{10,22}+m_{10,20}+$$
$$m_{9,28}+m_{9,27}+m_{9,26}+m_{9,24}+m_{9,23}+m_{8,28}+m_{8,25}+m_{8,22}+m_{8,21}+m_{7,26}+m_{7,21}+m_{6,25}+m_{6,24}+m_{6,23}+m_{5,27}+m_{5,21}+m_{4,27}+$$
$$m_{4,26}+m_{4,24}+m_{4,20}+m_{3,24}+m_{3,23}+m_{2,26}+m_{2,23}+m_{2,21}+m_{2,20}+m_{1,28}+m_{1,27}+m_{1,24}+m_{1,23}+m_{0,28}+m_{0,27}+m_{0,23}+m_{0,21}=1,$$
$$m_{15,19}+m_{12,27}+m_{12,26}+m_{12,24}+m_{12,23}+m_{11,27}+m_{11,26}+m_{11,22}+m_{10,25}+m_{10,21}+m_{10,19}+m_{9,27}+m_{9,26}+m_{9,25}+m_{9,23}+m_{9,22}+$$
$$m_{8,28}+m_{8,27}+m_{8,24}+m_{8,21}+m_{8,20}+m_{7,25}+m_{7,20}+m_{7,0}+m_{6,24}+m_{6,23}+m_{6,22}+m_{5,27}+m_{5,26}+m_{5,20}+m_{4,26}+m_{4,25}+m_{4,23}+m_{4,19}+$$
$$m_{3,23}+m_{3,22}+m_{2,25}+m_{2,22}+m_{2,20}+m_{2,19}+m_{1,30}+m_{1,28}+m_{1,27}+m_{1,26}+m_{1,23}+m_{1,22}+m_{1,0}+m_{0,27}+m_{0,26}+m_{0,22}+m_{0,20}=1,$$
$$m_{15,18}+m_{12,26}+m_{12,25}+m_{12,23}+m_{12,22}+m_{11,26}+m_{11,25}+m_{11,21}+m_{10,24}+m_{10,20}+m_{10,18}+m_{9,28}+m_{9,26}+m_{9,25}+m_{9,24}+$$
$$m_{9,22}+m_{9,21}+m_{8,28}+m_{8,27}+m_{8,26}+m_{8,23}+m_{8,20}+m_{8,19}+m_{7,24}+m_{7,19}+m_{6,27}+m_{6,23}+m_{6,22}+m_{6,21}+m_{5,27}+m_{5,26}+$$
$$m_{5,25}+m_{5,19}+m_{4,25}+m_{4,24}+m_{4,22}+m_{4,18}+m_{3,22}+m_{3,21}+m_{2,28}+m_{2,24}+m_{2,21}+m_{2,19}+m_{2,18}+m_{1,27}+m_{1,26}+m_{1,25}+$$
$$m_{1,22}+m_{1,21}+m_{0,26}+m_{0,25}+m_{0,21}+m_{0,19}=0,\ m_{15,17}+m_{12,25}+m_{12,24}+m_{12,22}+m_{12,21}+m_{11,25}+m_{11,24}+m_{11,20}+m_{10,23}+$$
$$m_{10,19}+m_{10,17}+m_{9,28}+m_{9,27}+m_{9,25}+m_{9,24}+m_{9,23}+m_{9,21}+m_{9,20}+m_{8,27}+m_{8,26}+m_{8,25}+m_{8,22}+m_{8,19}+m_{8,18}+m_{7,27}+$$
$$m_{7,23}+m_{7,18}+m_{6,27}+m_{6,26}+m_{6,22}+m_{6,21}+m_{6,20}+m_{5,26}+m_{5,25}+m_{5,24}+m_{5,18}+m_{4,24}+m_{4,23}+m_{4,21}+m_{4,17}+m_{3,21}+m_{3,20}+$$
$$m_{2,28}+m_{2,27}+m_{2,23}+m_{2,20}+m_{2,18}+m_{2,17}+m_{1,26}+m_{1,25}+m_{1,24}+m_{1,21}+m_{1,20}+m_{0,28}+m_{0,25}+m_{0,24}+m_{0,20}+m_{0,18}=0,$$
$$m_{15,16}+m_{13,11}+m_{12,28}+m_{12,27}+m_{12,24}+m_{12,20}+m_{12,19}+m_{12,15}+m_{11,27}+m_{11,25}+m_{11,24}+m_{11,23}+m_{11,21}+m_{11,17}+m_{11,14}+$$
$$m_{11,12}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,23}+m_{10,22}+m_{10,19}+m_{10,15}+m_{9,27}+m_{9,25}+m_{9,24}+m_{9,22}+m_{9,20}+m_{9,19}+m_{9,18}+m_{9,17}+$$
$$m_{9,14}+m_{9,13}+m_{8,28}+m_{8,27}+m_{8,25}+m_{8,24}+m_{8,21}+m_{8,20}+m_{8,18}+m_{8,16}+m_{8,13}+m_{8,11}+m_{7,26}+m_{7,24}+m_{7,21}+m_{7,20}+m_{7,16}+m_{7,15}+$$
$$m_{7,0}+m_{6,23}+m_{6,22}+m_{6,21}+m_{6,19}+m_{6,18}+m_{6,13}+m_{5,27}+m_{5,20}+m_{5,19}+m_{5,16}+m_{5,12}+m_{4,28}+m_{4,26}+m_{4,25}+m_{4,15}+m_{3,26}+m_{3,24}+$$
$$m_{3,22}+m_{3,21}+m_{3,20}+m_{3,18}+m_{3,17}+m_{3,15}+m_{3,13}+m_{3,12}+m_{2,27}+m_{2,26}+m_{2,24}+m_{2,20}+m_{2,19}+m_{2,16}+m_{2,15}+m_{2,11}+m_{1,30}+m_{1,28}+$$
$$m_{1,27}+m_{1,26}+m_{1,25}+m_{1,24}+m_{1,22}+m_{1,20}+m_{1,19}+m_{1,18}+m_{1,15}+m_{1,13}+m_{1,0}+m_{0,28}+m_{0,26}+m_{0,24}+m_{0,21}+m_{0,20}+m_{0,16}+m_{0,11}=$$
$$1,\ m_{15,15}+m_{13,14}+m_{12,26}+m_{12,24}+m_{12,23}+m_{12,20}+m_{12,19}+m_{12,18}+m_{11,24}+m_{11,23}+m_{11,20}+m_{11,18}+m_{11,17}+m_{11,15}+m_{10,28}+$$
$$m_{10,27}+m_{10,26}+m_{10,22}+m_{10,19}+m_{10,18}+m_{10,17}+m_{10,15}+m_{9,28}+m_{9,25}+m_{9,23}+m_{9,22}+m_{9,20}+m_{9,19}+m_{9,18}+m_{9,17}+m_{9,16}+m_{8,27}+$$
$$m_{8,25}+m_{8,24}+m_{8,19}+m_{8,17}+m_{8,14}+m_{7,26}+m_{7,24}+m_{7,23}+m_{7,21}+m_{7,20}+m_{7,19}+m_{7,18}+m_{7,16}+m_{7,0}+m_{6,27}+m_{6,26}+m_{6,24}+m_{6,23}+$$
$$m_{6,21}+m_{6,20}+m_{6,19}+m_{6,18}+m_{6,16}+m_{5,26}+m_{5,24}+m_{5,20}+m_{5,19}+m_{5,16}+m_{5,15}+m_{4,27}+m_{4,26}+m_{4,25}+m_{4,23}+m_{4,22}+m_{4,21}+m_{4,18}+$$
$$m_{4,15}+m_{3,28}+m_{3,27}+m_{3,25}+m_{3,24}+m_{3,22}+m_{3,21}+m_{3,20}+m_{3,19}+m_{3,16}+m_{3,15}+m_{2,27}+m_{2,26}+m_{2,23}+m_{2,21}+m_{2,20}+m_{2,16}+m_{2,15}+$$
$$m_{2,14}+m_{1,30}+m_{1,26}+m_{1,25}+m_{1,24}+m_{1,23}+m_{1,22}+m_{1,21}+m_{1,19}+m_{1,16}+m_{1,0}+m_{0,24}+m_{0,20}+m_{0,19}+m_{0,18}+m_{0,16}+m_{0,14}=0,$$
$$m_{15,14}+m_{13,14}+m_{12,26}+m_{12,24}+m_{12,21}+m_{12,19}+m_{11,27}+m_{11,24}+m_{11,21}+m_{11,20}+m_{11,15}+m_{10,27}+m_{10,22}+m_{10,21}+m_{10,20}+$$
$$m_{10,19}+m_{10,18}+m_{10,16}+m_{10,14}+m_{9,28}+m_{9,26}+m_{9,25}+m_{9,24}+m_{9,22}+m_{9,18}+m_{9,16}+m_{8,28}+m_{8,26}+m_{8,24}+m_{8,22}+m_{8,20}+m_{8,15}+$$
$$m_{8,14}+m_{7,26}+m_{7,23}+m_{7,19}+m_{7,18}+m_{7,15}+m_{7,0}+m_{6,27}+m_{6,25}+m_{6,24}+m_{6,21}+m_{6,19}+m_{6,18}+m_{6,17}+m_{6,16}+m_{5,27}+m_{5,21}+m_{5,20}+$$
$$m_{5,19}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,23}+m_{4,21}+m_{4,20}+m_{4,19}+m_{4,14}+m_{3,25}+m_{3,24}+m_{3,22}+m_{3,21}+m_{3,20}+m_{3,17}+m_{3,16}+m_{3,15}+$$
$$m_{2,27}+m_{2,24}+m_{2,23}+m_{2,18}+m_{2,17}+m_{2,15}+m_{1,30}+m_{1,26}+m_{1,25}+m_{1,23}+m_{1,22}+m_{1,17}+m_{1,16}+m_{1,0}+m_{0,26}+m_{0,25}+m_{0,24}+m_{0,23}+$$
$$m_{0,21}+m_{0,20}+m_{0,19}+m_{0,17}+m_{0,15}+m_{0,14}=1,\ m_{15,12}+m_{12,27}+m_{12,20}+m_{12,19}+m_{12,17}+m_{12,16}+m_{11,28}+m_{11,27}+m_{11,26}+m_{11,25}+$$
$$m_{11,20}+m_{11,19}+m_{11,15}+m_{10,27}+m_{10,25}+m_{10,24}+m_{10,18}+m_{10,14}+m_{10,12}+m_{9,27}+m_{9,23}+m_{9,22}+m_{9,20}+m_{9,19}+m_{9,18}+m_{9,16}+$$
$$m_{9,15}+m_{8,28}+m_{8,27}+m_{8,26}+m_{8,24}+m_{8,22}+m_{8,21}+m_{8,20}+m_{8,17}+m_{8,14}+m_{8,13}+m_{7,26}+m_{7,25}+m_{7,24}+m_{7,23}+m_{7,22}+m_{7,18}+m_{7,13}+$$
$$m_{7,0}+m_{6,27}+m_{6,26}+m_{6,25}+m_{6,24}+m_{6,22}+m_{6,21}+m_{6,17}+m_{6,16}+m_{6,15}+m_{5,26}+m_{5,24}+m_{5,21}+m_{5,20}+m_{5,19}+m_{5,13}+m_{4,25}+m_{4,24}+$$
$$m_{4,19}+m_{4,18}+m_{4,16}+m_{4,12}+m_{3,28}+m_{3,27}+m_{3,25}+m_{3,16}+m_{3,15}+m_{2,28}+m_{2,23}+m_{2,22}+m_{2,18}+m_{2,15}+m_{2,13}+m_{2,12}+m_{1,30}+$$
$$m_{1,21}+m_{1,20}+m_{1,19}+m_{1,16}+m_{1,15}+m_{1,0}+m_{0,28}+m_{0,27}+m_{0,23}+m_{0,20}+m_{0,19}+m_{0,15}+m_{0,13}=1,\ m_{15,7}+m_{15,6}+m_{9,6}+m_{8,2}+$$
$$m_{7,6}+m_{7,3}+m_{6,5}+m_{6,3}+m_{5,5}+m_{5,4}+m_{5,2}+m_{5,1}+m_{4,4}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,3}+m_{1,1}+m_{0,3}+m_{0,2}+m_{79,11}=1,$$
$$m_{15,5}=0,\ m_{15,4}+m_{7,3}+m_{7,2}+m_{6,5}+m_{6,3}+m_{5,4}+m_{5,3}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,30}+m_{1,3}+m_{1,1}+m_{0,3}=0,$$
$$m_{15,3}+m_{7,3}+m_{7,2}+m_{7,0}+m_{6,5}+m_{5,5}+m_{5,4}+m_{5,2}+m_{5,1}+m_{4,3}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,30}+m_{1,1}+m_{0,3}=0,$$
$$m_{15,2}+m_{7,3}+m_{7,2}+m_{7,0}+m_{6,5}+m_{6,3}+m_{5,5}+m_{5,4}+m_{5,1}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,3}+m_{1,2}+m_{1,1}+$$
$$m_{0,3}+m_{0,2}=0,\ m_{15,1}+m_{8,2}+m_{7,3}+m_{7,2}+m_{7,0}+m_{5,3}+m_{4,2}+m_{3,4}+m_{2,2}+m_{1,2}+m_{0,4}+m_{0,2}=0,\ m_{15,0}+m_{1,30}=1,$$
$$m_{14,31}=1,\ m_{14,30}=1,\ m_{14,29}=0,\ m_{14,28}+m_{9,28}+m_{3,28}+m_{1,28}=1,\ m_{14,27}+m_{12,28}+m_{9,27}+m_{4,28}+m_{3,27}+m_{1,27}=1,$$
$$m_{14,26}+m_{12,27}+m_{10,28}+m_{9,28}+m_{9,26}+m_{6,27}+m_{4,28}+m_{4,27}+m_{3,26}+m_{2,28}+m_{1,26}=1,\ m_{14,25}+m_{12,28}+m_{12,26}+m_{10,28}+$$
$$m_{10,27}+m_{9,27}+m_{9,25}+m_{7,27}+m_{6,26}+m_{4,27}+m_{4,26}+m_{3,25}+m_{2,27}+m_{1,25}=1,\ m_{14,24}+m_{12,27}+m_{12,25}+m_{11,28}+m_{10,27}+$$
$$m_{10,26}+m_{9,26}+m_{9,24}+m_{7,26}+m_{6,25}+m_{4,28}+m_{4,26}+m_{4,25}+m_{3,28}+m_{3,24}+m_{2,26}+m_{1,24}+m_{0,28}=0,\ m_{14,23}+m_{12,26}+m_{12,24}+$$
$$m_{11,27}+m_{10,26}+m_{10,25}+m_{9,28}+m_{9,25}+m_{9,23}+m_{8,28}+m_{7,25}+m_{6,24}+m_{5,27}+m_{4,27}+m_{4,25}+m_{4,24}+m_{3,28}+m_{3,27}+m_{3,23}+$$
$$m_{2,25}+m_{1,28}+m_{1,23}+m_{0,27}=1,\ m_{14,22}+m_{12,28}+m_{12,25}+m_{12,23}+m_{11,26}+m_{10,28}+m_{10,25}+m_{10,24}+m_{9,27}+m_{9,24}+m_{9,22}+$$
$$m_{8,27}+m_{7,24}+m_{6,27}+m_{6,23}+m_{5,26}+m_{4,28}+m_{4,26}+m_{4,24}+m_{4,23}+m_{3,27}+m_{3,26}+m_{3,22}+m_{2,24}+m_{1,27}+m_{1,22}+m_{0,26}=1,$$
$$m_{14,21}+m_{12,27}+m_{12,24}+m_{12,22}+m_{11,25}+m_{10,28}+m_{10,27}+m_{10,24}+m_{10,23}+m_{9,28}+m_{9,26}+m_{9,23}+m_{9,21}+m_{8,26}+m_{7,23}+$$

$$m_{6,26}+m_{6,22}+m_{5,25}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,23}+m_{4,22}+m_{3,26}+m_{3,25}+m_{3,21}+m_{2,28}+m_{2,23}+m_{1,26}+m_{1,21}+m_{0,25}=1,$$
$$m_{14,20}+m_{12,26}+m_{12,23}+m_{12,21}+m_{11,28}+m_{11,24}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,23}+m_{10,22}+m_{9,27}+m_{9,25}+m_{9,22}+m_{9,20}+m_{8,28}+$$
$$m_{8,25}+m_{7,27}+m_{7,22}+m_{6,25}+m_{6,21}+m_{5,24}+m_{4,27}+m_{4,26}+m_{4,24}+m_{4,22}+m_{4,21}+m_{3,28}+m_{3,25}+m_{3,24}+m_{3,20}+m_{2,27}+m_{2,22}+$$
$$m_{1,25}+m_{1,20}+m_{0,28}+m_{0,24}=0,\ m_{14,19}+m_{12,25}+m_{12,22}+m_{12,20}+m_{11,28}+m_{11,27}+m_{11,23}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,25}+$$
$$m_{10,22}+m_{10,21}+m_{9,28}+m_{9,26}+m_{9,24}+m_{9,21}+m_{9,19}+m_{8,27}+m_{8,24}+m_{7,27}+m_{7,26}+m_{7,21}+m_{6,27}+m_{6,24}+m_{6,20}+m_{5,23}+m_{4,28}+$$
$$m_{4,26}+m_{4,25}+m_{4,23}+m_{4,21}+m_{4,20}+m_{3,27}+m_{3,24}+m_{3,23}+m_{3,19}+m_{2,26}+m_{2,21}+m_{1,28}+m_{1,24}+m_{1,19}+m_{0,28}+m_{0,27}+m_{0,23}=1,$$
$$m_{14,18}+m_{13,14}+m_{12,28}+m_{12,26}+m_{12,22}+m_{12,21}+m_{12,19}+m_{12,18}+m_{11,27}+m_{11,26}+m_{11,24}+m_{11,20}+m_{11,17}+m_{11,15}+m_{10,27}+$$
$$m_{10,25}+m_{10,24}+m_{10,22}+m_{10,20}+m_{10,19}+m_{10,18}+m_{9,28}+m_{9,27}+m_{9,26}+m_{9,25}+m_{9,23}+m_{9,21}+m_{9,18}+m_{9,17}+m_{9,16}+m_{8,26}+m_{8,20}+$$
$$m_{8,19}+m_{8,16}+m_{8,14}+m_{7,27}+m_{7,26}+m_{7,24}+m_{7,23}+m_{7,19}+m_{7,18}+m_{7,0}+m_{6,27}+m_{6,25}+m_{6,21}+m_{6,19}+m_{6,16}+m_{5,26}+m_{5,23}+m_{5,20}+$$
$$m_{5,19}+m_{5,15}+m_{4,27}+m_{4,26}+m_{4,24}+m_{4,23}+m_{4,22}+m_{4,20}+m_{4,18}+m_{3,27}+m_{3,26}+m_{3,25}+m_{3,24}+m_{3,23}+m_{3,21}+m_{3,20}+m_{3,16}+m_{3,15}+$$
$$m_{2,27}+m_{2,23}+m_{2,18}+m_{2,14}+m_{1,30}+m_{1,27}+m_{1,26}+m_{1,25}+m_{1,23}+m_{1,21}+m_{1,16}+m_{1,0}+m_{0,27}+m_{0,24}+m_{0,23}+m_{0,20}+m_{0,19}+m_{0,14}=$$
$$1,\ m_{14,17}+m_{12,27}+m_{12,23}+m_{12,20}+m_{12,18}+m_{11,27}+m_{11,26}+m_{11,25}+m_{11,21}+m_{10,28}+m_{10,26}+m_{10,25}+m_{10,24}+m_{10,23}+m_{10,20}+$$
$$m_{10,19}+m_{9,26}+m_{9,24}+m_{9,22}+m_{9,19}+m_{9,17}+m_{8,28}+m_{8,25}+m_{8,22}+m_{7,27}+m_{7,25}+m_{7,24}+m_{7,19}+m_{6,27}+m_{6,26}+m_{6,25}+m_{6,22}+$$
$$m_{6,18}+m_{5,27}+m_{5,26}+m_{5,21}+m_{4,28}+m_{4,27}+m_{4,26}+m_{4,24}+m_{4,23}+m_{4,21}+m_{4,19}+m_{4,18}+m_{3,28}+m_{3,25}+m_{3,22}+m_{3,21}+m_{3,17}+m_{2,28}+$$
$$m_{2,24}+m_{2,19}+m_{1,28}+m_{1,26}+m_{1,22}+m_{1,17}+m_{0,26}+m_{0,25}+m_{0,21}=1,\ m_{14,16}+m_{12,26}+m_{12,22}+m_{12,19}+m_{12,17}+m_{11,26}+m_{11,25}+$$
$$m_{11,24}+m_{11,20}+m_{10,28}+m_{10,27}+m_{10,25}+m_{10,24}+m_{10,23}+m_{10,22}+m_{10,19}+m_{10,18}+m_{9,28}+m_{9,25}+m_{9,23}+m_{9,21}+m_{9,18}+m_{9,16}+$$
$$m_{8,27}+m_{8,24}+m_{8,21}+m_{7,27}+m_{7,26}+m_{7,24}+m_{7,23}+m_{7,18}+m_{7,0}+m_{6,27}+m_{6,26}+m_{6,25}+m_{6,24}+m_{6,21}+m_{6,17}+m_{5,26}+m_{5,25}+m_{5,20}+$$
$$m_{4,28}+m_{4,27}+m_{4,26}+m_{4,25}+m_{4,23}+m_{4,22}+m_{4,20}+m_{4,18}+m_{4,17}+m_{3,28}+m_{3,27}+m_{3,24}+m_{3,21}+m_{3,20}+m_{3,16}+m_{2,28}+m_{2,27}+m_{2,23}+$$
$$m_{2,18}+m_{1,30}+m_{1,28}+m_{1,27}+m_{1,25}+m_{1,21}+m_{1,16}+m_{1,0}+m_{0,25}+m_{0,24}+m_{0,20}=0,\ m_{14,15}+m_{12,25}+m_{12,21}+m_{12,18}+m_{12,16}+$$
$$m_{11,25}+m_{11,24}+m_{11,23}+m_{11,19}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,24}+m_{10,23}+m_{10,22}+m_{10,21}+m_{10,18}+m_{10,17}+m_{9,28}+m_{9,27}+m_{9,24}+$$
$$m_{9,22}+m_{9,20}+m_{9,17}+m_{9,15}+m_{8,28}+m_{8,26}+m_{8,23}+m_{8,20}+m_{7,26}+m_{7,25}+m_{7,23}+m_{7,22}+m_{7,17}+m_{6,26}+m_{6,25}+m_{6,24}+m_{6,23}+$$
$$m_{6,20}+m_{6,16}+m_{5,25}+m_{5,24}+m_{5,19}+m_{4,28}+m_{4,27}+m_{4,26}+m_{4,25}+m_{4,24}+m_{4,22}+m_{4,21}+m_{4,19}+m_{4,17}+m_{4,16}+m_{3,27}+m_{3,26}+$$
$$m_{3,23}+m_{3,20}+m_{3,19}+m_{3,15}+m_{2,28}+m_{2,27}+m_{2,26}+m_{2,22}+m_{2,17}+m_{1,27}+m_{1,26}+m_{1,24}+m_{1,20}+m_{1,15}+m_{0,24}+m_{0,23}+m_{0,19}=0,$$
$$m_{14,13}+m_{13,14}+m_{12,27}+m_{12,26}+m_{12,24}+m_{12,23}+m_{12,22}+m_{12,19}+m_{12,18}+m_{12,16}+m_{12,14}+m_{11,28}+m_{11,24}+m_{11,23}+m_{11,21}+$$
$$m_{11,20}+m_{11,15}+m_{10,28}+m_{10,25}+m_{10,24}+m_{10,20}+m_{10,18}+m_{10,16}+m_{10,15}+m_{9,25}+m_{9,22}+m_{9,21}+m_{9,18}+m_{9,17}+m_{9,16}+m_{9,15}+$$
$$m_{9,13}+m_{8,28}+m_{8,26}+m_{8,24}+m_{8,23}+m_{8,21}+m_{8,20}+m_{8,19}+m_{8,18}+m_{8,16}+m_{8,14}+m_{7,27}+m_{7,25}+m_{7,21}+m_{7,19}+m_{7,18}+m_{7,15}+m_{7,0}+$$
$$m_{6,26}+m_{6,25}+m_{6,24}+m_{6,22}+m_{6,18}+m_{6,16}+m_{6,14}+m_{5,27}+m_{5,20}+m_{5,19}+m_{5,17}+m_{5,15}+m_{4,27}+m_{4,24}+m_{4,22}+m_{4,20}+m_{4,18}+m_{4,17}+$$
$$m_{4,15}+m_{4,14}+m_{3,27}+m_{3,22}+m_{3,20}+m_{3,17}+m_{3,16}+m_{3,15}+m_{3,13}+m_{2,27}+m_{2,26}+m_{2,24}+m_{2,23}+m_{2,18}+m_{2,15}+m_{2,14}+m_{1,30}+$$
$$m_{1,28}+m_{1,26}+m_{1,24}+m_{1,22}+m_{1,21}+m_{1,16}+m_{1,13}+m_{1,0}+m_{0,28}+m_{0,26}+m_{0,24}+m_{0,23}+m_{0,21}+m_{0,20}+m_{0,19}+m_{0,17}+m_{0,14}=0,$$
$$m_{14,12}+m_{13,11}+m_{12,28}+m_{12,27}+m_{12,26}+m_{12,23}+m_{12,22}+m_{12,21}+m_{12,19}+m_{12,18}+m_{12,13}+m_{11,28}+m_{11,27}+m_{11,25}+m_{11,22}+$$
$$m_{11,20}+m_{11,19}+m_{11,17}+m_{11,16}+m_{11,14}+m_{11,12}+m_{10,28}+m_{10,26}+m_{10,25}+m_{10,24}+m_{10,21}+m_{10,20}+m_{10,16}+m_{10,14}+m_{9,28}+$$
$$m_{9,27}+m_{9,26}+m_{9,24}+m_{9,23}+m_{9,21}+m_{9,19}+m_{9,18}+m_{9,13}+m_{9,12}+m_{8,28}+m_{8,26}+m_{8,25}+m_{8,23}+m_{8,16}+m_{8,13}+m_{8,11}+m_{7,24}+$$
$$m_{7,23}+m_{7,21}+m_{7,19}+m_{7,17}+m_{7,16}+m_{7,15}+m_{7,14}+m_{7,0}+m_{6,26}+m_{6,25}+m_{6,21}+m_{6,18}+m_{6,17}+m_{5,27}+m_{5,24}+m_{5,23}+m_{5,22}+$$
$$m_{5,21}+m_{5,20}+m_{5,19}+m_{5,17}+m_{5,12}+m_{4,27}+m_{4,24}+m_{4,21}+m_{4,20}+m_{4,19}+m_{4,18}+m_{4,15}+m_{4,14}+m_{4,13}+m_{3,28}+m_{3,26}+m_{3,23}+$$
$$m_{3,22}+m_{3,21}+m_{3,20}+m_{3,19}+m_{3,18}+m_{3,16}+m_{3,15}+m_{3,13}+m_{2,25}+m_{2,23}+m_{2,22}+m_{2,20}+m_{2,19}+m_{2,17}+m_{2,15}+m_{2,14}+m_{2,11}+$$
$$m_{1,30}+m_{1,26}+m_{1,24}+m_{1,22}+m_{1,21}+m_{1,18}+m_{1,17}+m_{1,15}+m_{1,13}+m_{1,12}+m_{1,0}+m_{0,28}+m_{0,26}+m_{0,23}+m_{0,19}+m_{0,17}+m_{0,11}=0,$$
$$m_{14,5}=0,\ m_{14,4}+m_{5,5}+m_{3,4}=0,\ m_{14,3}+m_{8,2}+m_{7,3}+m_{7,0}+m_{6,5}+m_{6,3}+m_{6,2}+m_{5,5}+m_{5,4}+m_{5,2}+m_{4,2}+m_{2,5}+m_{2,4}+$$
$$m_{2,3}+m_{2,1}+m_{1,2}+m_{1,1}+m_{1,0}+m_{0,4}+m_{0,3}+m_{0,2}=0,\ m_{14,2}+m_{8,2}+m_{7,2}+m_{5,4}+m_{5,2}+m_{5,1}+m_{4,2}+m_{2,1}+m_{1,1}+m_{0,4}=0,$$
$$m_{14,1}+m_{8,2}+m_{7,3}+m_{7,2}+m_{6,5}+m_{6,3}+m_{5,4}+m_{5,3}+m_{5,2}+m_{5,1}+m_{4,2}+m_{3,4}+m_{3,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,3}+m_{0,3}+m_{0,2}=0,$$
$$m_{14,0}=0,\ m_{13,31}=1,\ m_{13,30}=1,\ m_{13,29}=1,\ m_{13,28}+m_{8,28}+m_{2,28}+m_{0,28}=1,\ m_{13,27}+m_{11,28}+m_{8,27}+m_{3,28}+m_{2,27}+m_{0,27}=0,$$
$$m_{13,26}+m_{11,27}+m_{9,28}+m_{8,28}+m_{8,26}+m_{5,27}+m_{3,28}+m_{3,27}+m_{2,26}+m_{1,28}+m_{0,26}=0,\ m_{13,25}+m_{11,28}+m_{11,26}+m_{9,28}+$$
$$m_{9,27}+m_{8,27}+m_{8,25}+m_{6,27}+m_{5,26}+m_{3,27}+m_{3,26}+m_{2,25}+m_{1,27}+m_{0,25}=1,\ m_{13,24}+m_{12,28}+m_{11,27}+m_{11,25}+m_{10,28}+$$
$$m_{9,27}+m_{9,26}+m_{8,26}+m_{8,24}+m_{6,26}+m_{5,25}+m_{4,28}+m_{3,28}+m_{3,26}+m_{3,25}+m_{2,28}+m_{2,24}+m_{1,28}+m_{1,26}+m_{0,24}=0,$$
$$m_{13,23}+m_{12,27}+m_{11,26}+m_{11,24}+m_{10,28}+m_{10,27}+m_{9,26}+m_{9,25}+m_{8,28}+m_{8,25}+m_{8,23}+m_{7,27}+m_{6,25}+m_{5,24}+m_{4,28}+m_{4,27}+$$
$$m_{3,27}+m_{3,25}+m_{3,24}+m_{2,27}+m_{2,23}+m_{1,27}+m_{1,25}+m_{0,28}+m_{0,23}=1,\ m_{13,22}+m_{12,26}+m_{11,28}+m_{11,25}+m_{11,23}+m_{10,27}+$$
$$m_{10,26}+m_{9,28}+m_{9,25}+m_{9,24}+m_{8,28}+m_{8,27}+m_{8,24}+m_{8,22}+m_{7,27}+m_{7,26}+m_{6,24}+m_{5,27}+m_{5,23}+m_{4,27}+m_{4,26}+m_{3,28}+m_{3,26}+$$
$$m_{3,24}+m_{3,23}+m_{2,28}+m_{2,26}+m_{2,22}+m_{1,26}+m_{1,24}+m_{0,28}+m_{0,27}+m_{0,22}=1,\ m_{13,21}+m_{12,25}+m_{11,27}+m_{11,24}+m_{11,22}+m_{10,28}+$$
$$m_{10,26}+m_{10,25}+m_{9,28}+m_{9,27}+m_{9,24}+m_{9,23}+m_{8,27}+m_{8,26}+m_{8,23}+m_{8,21}+m_{7,27}+m_{7,26}+m_{7,25}+m_{6,23}+m_{5,27}+m_{5,26}+m_{5,22}+$$
$$m_{4,26}+m_{4,25}+m_{3,28}+m_{3,27}+m_{3,25}+m_{3,23}+m_{3,22}+m_{2,27}+m_{2,25}+m_{2,21}+m_{1,28}+m_{1,25}+m_{1,23}+m_{0,27}+m_{0,26}+m_{0,21}=0,$$
$$m_{13,20}+m_{12,28}+m_{12,24}+m_{11,28}+m_{11,26}+m_{11,23}+m_{11,21}+m_{10,28}+m_{10,27}+m_{10,25}+m_{10,24}+m_{9,27}+m_{9,26}+m_{9,23}+$$
$$m_{9,22}+m_{8,26}+m_{8,25}+m_{8,22}+m_{8,20}+m_{7,26}+m_{7,25}+m_{7,24}+m_{6,27}+m_{6,22}+m_{5,26}+m_{5,25}+m_{5,21}+m_{4,25}+m_{4,24}+m_{3,28}+$$
$$m_{3,27}+m_{3,26}+m_{3,24}+m_{3,22}+m_{3,21}+m_{2,26}+m_{2,24}+m_{2,20}+m_{1,27}+m_{1,24}+m_{1,22}+m_{0,28}+m_{0,26}+m_{0,25}+m_{0,20}=0,$$

$$m_{13,19}+m_{12,27}+m_{12,23}+m_{11,27}+m_{11,25}+m_{11,22}+m_{11,20}+m_{10,27}+m_{10,26}+m_{10,24}+m_{10,23}+m_{9,26}+m_{9,25}+m_{9,22}+m_{9,21}+m_{8,28}+m_{8,25}+m_{8,24}+m_{8,21}+m_{8,19}+m_{7,25}+m_{7,24}+m_{7,23}+m_{7,0}+m_{6,26}+m_{6,21}+m_{5,27}+m_{5,25}+m_{5,24}+m_{5,20}+m_{4,28}+m_{4,24}+m_{4,23}+m_{3,27}+m_{3,26}+m_{3,25}+m_{3,23}+m_{3,21}+m_{3,20}+m_{2,28}+m_{2,25}+m_{2,23}+m_{2,19}+m_{1,30}+m_{1,26}+m_{1,23}+m_{1,21}+m_{1,0}+m_{0,28}+m_{0,27}+m_{0,25}+m_{0,24}+m_{0,19}=0,\ m_{13,18}+m_{12,28}+m_{12,26}+m_{12,22}+m_{11,28}+m_{11,26}+m_{11,24}+m_{11,21}+m_{11,19}+m_{10,26}+m_{10,25}+m_{10,23}+m_{10,22}+m_{9,25}+m_{9,24}+m_{9,21}+m_{9,20}+m_{8,27}+m_{8,24}+m_{8,23}+m_{8,20}+m_{8,18}+m_{7,27}+m_{7,24}+m_{7,23}+m_{7,22}+m_{6,27}+m_{6,25}+m_{6,20}+m_{5,27}+m_{5,26}+m_{5,24}+m_{5,23}+m_{5,19}+m_{4,27}+m_{4,23}+m_{4,22}+m_{3,28}+m_{3,26}+m_{3,25}+m_{3,24}+m_{3,22}+m_{3,20}+m_{3,19}+m_{2,27}+m_{2,24}+m_{2,22}+m_{2,18}+m_{1,25}+m_{1,22}+m_{1,20}+m_{0,28}+m_{0,27}+m_{0,26}+m_{0,24}+m_{0,23}+m_{0,18}=1,\ m_{13,17}+m_{12,27}+m_{12,25}+m_{12,21}+m_{11,27}+m_{11,25}+m_{11,23}+m_{11,20}+m_{11,18}+m_{10,25}+m_{10,24}+m_{10,22}+m_{10,21}+m_{9,24}+m_{9,23}+m_{9,20}+m_{9,19}+m_{8,26}+m_{8,23}+m_{8,22}+m_{8,19}+m_{8,17}+m_{7,27}+m_{7,26}+m_{7,23}+m_{7,22}+m_{7,21}+m_{6,26}+m_{6,24}+m_{6,19}+m_{5,26}+m_{5,25}+m_{5,23}+m_{5,22}+m_{5,18}+m_{4,28}+m_{4,26}+m_{4,22}+m_{4,21}+m_{3,28}+m_{3,27}+m_{3,25}+m_{3,24}+m_{3,23}+m_{3,21}+m_{3,19}+m_{3,18}+m_{2,28}+m_{2,26}+m_{2,23}+m_{2,21}+m_{2,17}+m_{1,28}+m_{1,24}+m_{1,21}+m_{1,19}+m_{0,27}+m_{0,26}+m_{0,25}+m_{0,23}+m_{0,22}+m_{0,17}=1,\ m_{13,16}+m_{12,28}+m_{12,26}+m_{12,24}+m_{12,20}+m_{11,26}+m_{11,24}+m_{11,22}+m_{11,19}+m_{11,17}+m_{10,28}+m_{10,24}+m_{10,23}+m_{10,21}+m_{10,20}+m_{9,28}+m_{9,23}+m_{9,22}+m_{9,19}+m_{9,18}+m_{8,25}+m_{8,22}+m_{8,21}+m_{8,18}+m_{8,16}+m_{7,27}+m_{7,26}+m_{7,25}+m_{7,22}+m_{7,21}+m_{7,20}+m_{6,27}+m_{6,25}+m_{6,23}+m_{6,18}+m_{5,25}+m_{5,24}+m_{5,22}+m_{5,21}+m_{5,17}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,21}+m_{4,20}+m_{3,27}+m_{3,26}+m_{3,24}+m_{3,23}+m_{3,22}+m_{3,20}+m_{3,18}+m_{3,17}+m_{2,27}+m_{2,25}+m_{2,22}+m_{2,20}+m_{2,16}+m_{1,28}+m_{1,27}+m_{1,23}+m_{1,20}+m_{1,18}+m_{0,28}+m_{0,26}+m_{0,25}+m_{0,24}+m_{0,22}+m_{0,21}+m_{0,16}=1,\ m_{13,15}+m_{13,14}+m_{12,27}+m_{12,26}+m_{12,25}+m_{12,24}+m_{12,23}+m_{12,22}+m_{12,19}+m_{12,18}+m_{11,28}+m_{11,25}+m_{11,24}+m_{11,23}+m_{11,22}+m_{11,21}+m_{11,20}+m_{11,18}+m_{11,17}+m_{11,16}+m_{11,15}+m_{10,27}+m_{10,26}+m_{10,23}+m_{10,21}+m_{10,20}+m_{10,18}+m_{9,28}+m_{9,27}+m_{9,26}+m_{9,22}+m_{9,20}+m_{9,18}+m_{9,16}+m_{8,24}+m_{8,23}+m_{8,21}+m_{8,19}+m_{8,17}+m_{8,16}+m_{8,15}+m_{8,14}+m_{7,27}+m_{7,26}+m_{7,23}+m_{7,21}+m_{7,18}+m_{7,0}+m_{6,27}+m_{6,25}+m_{6,24}+m_{6,23}+m_{6,22}+m_{6,21}+m_{6,17}+m_{6,16}+m_{5,26}+m_{5,24}+m_{5,22}+m_{5,21}+m_{5,19}+m_{5,16}+m_{5,15}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,24}+m_{4,23}+m_{4,20}+m_{4,18}+m_{3,28}+m_{3,27}+m_{3,26}+m_{3,24}+m_{3,23}+m_{3,20}+m_{3,19}+m_{3,18}+m_{3,17}+m_{3,15}+m_{2,28}+m_{2,27}+m_{2,26}+m_{2,25}+m_{2,24}+m_{2,23}+m_{2,21}+m_{2,20}+m_{2,19}+m_{2,18}+m_{2,15}+m_{2,14}+m_{1,30}+m_{1,27}+m_{1,25}+m_{1,22}+m_{1,21}+m_{1,19}+m_{1,18}+m_{1,17}+m_{1,16}+m_{1,0}+m_{0,27}+m_{0,26}+m_{0,25}+m_{0,22}+m_{0,21}+m_{0,19}+m_{0,15}+m_{0,14}=1,\ m_{13,13}+m_{12,25}+m_{12,23}+m_{12,21}+m_{12,17}+m_{11,27}+m_{11,23}+m_{11,21}+m_{11,19}+m_{11,16}+m_{11,14}+m_{10,28}+m_{10,25}+m_{10,21}+m_{10,20}+m_{10,18}+m_{10,17}+m_{9,28}+m_{9,27}+m_{9,25}+m_{9,20}+m_{9,19}+m_{9,16}+m_{9,15}+m_{8,28}+m_{8,22}+m_{8,19}+m_{8,18}+m_{8,15}+m_{8,13}+m_{7,26}+m_{7,24}+m_{7,23}+m_{7,22}+m_{7,19}+m_{7,18}+m_{7,17}+m_{6,27}+m_{6,25}+m_{6,24}+m_{6,22}+m_{6,20}+m_{6,15}+m_{5,27}+m_{5,26}+m_{5,25}+m_{5,22}+m_{5,21}+m_{5,19}+m_{5,18}+m_{5,14}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,24}+m_{4,22}+m_{4,18}+m_{4,17}+m_{3,28}+m_{3,26}+m_{3,24}+m_{3,23}+m_{3,21}+m_{3,20}+m_{3,19}+m_{3,17}+m_{3,15}+m_{3,14}+m_{2,26}+m_{2,24}+m_{2,22}+m_{2,19}+m_{2,17}+m_{2,13}+m_{1,28}+m_{1,25}+m_{1,24}+m_{1,20}+m_{1,17}+m_{1,15}+m_{0,28}+m_{0,25}+m_{0,23}+m_{0,22}+m_{0,21}+m_{0,19}+m_{0,18}+m_{0,13}=0,\ m_{13,5}+m_{7,2}+m_{6,2}+m_{5,5}+m_{5,2}+m_{4,4}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,30}+m_{1,0}=1,\ m_{13,4}+m_{5,5}+m_{3,4}+m_{2,4}+m_{0,4}=0,\ m_{13,3}+m_{6,2}+m_{5,3}+m_{5,2}+m_{5,1}+m_{4,2}+m_{3,2}+m_{2,4}+m_{2,2}+m_{2,1}+m_{1,0}+m_{0,2}=1,\ m_{13,2}+m_{8,2}+m_{7,0}+m_{5,3}+m_{2,2}+m_{1,30}+m_{0,2}=0,\ m_{13,1}=0,\ m_{13,0}+m_{1,30}=1,\ m_{12,31}=0,\ m_{12,30}=0,\ m_{12,29}=1,\ m_{12,6}=1,\ m_{12,5}+m_{7,2}+m_{6,2}+m_{5,2}+m_{4,5}+m_{4,4}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,30}+m_{1,0}=1,\ m_{12,4}+m_{4,4}=0,\ m_{12,3}+m_{7,3}+m_{7,2}+m_{6,3}+m_{5,3}+m_{5,2}+m_{5,1}+m_{4,3}+m_{3,2}+m_{2,2}+m_{2,1}+m_{1,1}+m_{0,4}=0,\ m_{12,2}+m_{7,3}+m_{6,3}+m_{5,3}+m_{4,3}+m_{3,2}+m_{2,2}+m_{1,3}+m_{1,2}+m_{1,0}+m_{0,4}=1,\ m_{12,1}=1,\ m_{12,0}=1,\ m_{11,31}=0,\ m_{11,30}=0,\ m_{11,29}=1,\ m_{11,6}=1,\ m_{11,5}+m_{8,4}+m_{3,4}=0,\ m_{11,4}+m_{7,3}+m_{7,2}+m_{7,0}+m_{6,5}+m_{6,3}+m_{5,3}+m_{5,2}+m_{5,1}+m_{4,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,3}+m_{1,2}+m_{1,1}+m_{0,3}+m_{0,2}=1,\ m_{11,3}+m_{7,0}+m_{1,30}=0,\ m_{11,2}+m_{8,2}+m_{7,3}+m_{7,2}+m_{7,0}+m_{5,5}+m_{5,4}+m_{5,2}+m_{4,2}+m_{3,4}+m_{3,2}+m_{2,4}+m_{1,30}+m_{1,2}+m_{0,4}+m_{0,2}=1,\ m_{11,1}=1,\ m_{11,0}+m_{1,30}=1,\ m_{10,31}=1,\ m_{10,30}=0,\ m_{10,29}=0,\ m_{10,6}=0,\ m_{10,5}+m_{4,5}+m_{2,5}=1,\ m_{10,4}+m_{7,3}+m_{6,5}+m_{6,3}+m_{6,2}+m_{5,4}+m_{5,3}+m_{5,2}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,4}+m_{1,3}+m_{1,1}+m_{1,0}+m_{0,3}=1,\ m_{10,3}+m_{7,3}+m_{7,0}+m_{6,5}+m_{5,5}+m_{5,4}+m_{5,3}+m_{5,1}+m_{3,4}+m_{3,2}+m_{2,5}+m_{2,2}+m_{2,1}+m_{1,30}+m_{1,1}+m_{0,3}=0,\ m_{10,2}+m_{7,3}+m_{7,0}+m_{6,5}+m_{6,3}+m_{6,2}+m_{5,5}+m_{5,3}+m_{3,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{1,30}+m_{1,3}+m_{1,1}+m_{0,4}+m_{0,3}+m_{0,2}=0,\ m_{10,1}=1,\ m_{10,0}=0,\ m_{9,31}=1,\ m_{9,30}=1,\ m_{9,29}=0,\ m_{9,5}=0,\ m_{9,4}=0,\ m_{9,3}+m_{8,2}+m_{7,3}+m_{7,0}+m_{6,5}+m_{6,3}+m_{6,2}+m_{5,5}+m_{5,4}+m_{5,2}+m_{4,2}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,3}+m_{1,2}+m_{1,1}+m_{1,0}+m_{0,4}+m_{0,3}+m_{0,2}=0,\ m_{9,2}+m_{8,2}+m_{6,5}+m_{6,3}+m_{5,4}+m_{5,3}+m_{5,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,30}+m_{1,3}+m_{1,2}+m_{1,1}+m_{0,4}+m_{0,3}=0,\ m_{9,1}=1,\ m_{9,0}=0,\ m_{8,31}=0,\ m_{8,30}=1,\ m_{8,29}=1,\ m_{8,3}+m_{7,3}+m_{7,2}+m_{7,0}+m_{6,3}+m_{5,4}+m_{5,3}+m_{3,4}+m_{3,2}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,30}+m_{1,3}+m_{0,2}=0,\ m_{8,1}+m_{7,3}+m_{6,5}+m_{6,3}+m_{5,3}+m_{3,4}+m_{3,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{1,3}+m_{1,1}+m_{0,4}+m_{0,3}+m_{0,2}=0,\ m_{8,0}=0,\ m_{7,31}=0,\ m_{7,30}=0,\ m_{7,29}=0,\ m_{7,28}=0,\ m_{7,5}=1,\ m_{7,4}+m_{7,2}+m_{5,4}+m_{5,3}+m_{5,2}+m_{3,2}+m_{2,2}+m_{0,4}=1,\ m_{7,1}=1,\ m_{6,31}=0,\ m_{6,30}=0,\ m_{6,29}=0,\ m_{6,28}=0,\ m_{6,6}=0,\ m_{6,4}=1,\ m_{6,1}=0,\ m_{6,0}=1,\ m_{5,31}=0,\ m_{5,30}=0,\ m_{5,29}=0,\ m_{5,28}=1,\ m_{5,6}=1,\ m_{5,0}+m_{1,30}+m_{1,0}=0,\ m_{4,31}=0,\ m_{4,30}=0,\ m_{4,29}=0,\ m_{4,6}=0,\ m_{4,1}=0,\ m_{4,0}=1,\ m_{3,31}=1,\ m_{3,30}=0,\ m_{3,29}=1,\ m_{3,5}=1,\ m_{3,3}=1,\ m_{3,1}=1,\ m_{3,0}+m_{1,0}=0,\ m_{2,31}=1,\ m_{2,30}=0,\ m_{2,29}=0,\ m_{2,0}+m_{1,30}=1,\ m_{1,31}+m_{1,30}=1,\ m_{1,29}=0,\ m_{1,5}=0,\ m_{1,4}=1,\ m_{0,31}=1,\ m_{0,30}=0,\ m_{0,29}=1,\ m_{0,1}=1,\ m_{0,0}=0.$$

8.3 Control bits and controlled relations

We determine control bits and controlled relations as in Table 9, 10, 11 and 12 where a control sequence denotes a pair of a control bit and a controlled relation.

Now we summarize our advanced sufficient conditions on $\{m_{i,j}\}$and $\{a_{i,j}\}$ by showing two tables (Table 13). Symbols in Table 13 mean:

- 'a', 'A', 'b', 'B', 'c', 'C': as in Section 8.2.
- 'L' means the leading term of controlled relation of Table 9, 10, 11 and 12.
- 'w', 'W': adjust $a_{i,j}$ so that $m_{i+1,j} = 0, 1$, respectively.
- 'v', 'V': adjust $a_{i,j}$ so that $m_{i,(j+27 \mod 32)} = 0, 1$, respectively.
- 'h': adjust $a_{i,j}$ so that corresponding controlled relation including $m_{i+1,j}$ as leading term holds.
- 'r' means to adjust $a_{i,j}$ so that corresponding controlled relation including $m_{i,(j+27 \mod 32)}$ as leading term holds.
- 'x', 'y': adjust $a_{i+1,j-1}$, $a_{i,j-1}$ so that $m_{i,j} = 0$, respectively.
- 'X', 'Y': adjust $a_{i+1,j-1}$, $a_{i,j-1}$ so that $m_{i,j} = 1$, respectively.
- 'N': semi-neutral bit.
- 'q' : adjust $a_{i,j}$ so that relations after 17-round hold.
- 'F' : etc.

By using our advanced sufficient conditions on $\{a_{i,j}\}$ and Algorithm 1 which is used as Step 2 in Algorithm 2, we can adjust the value of $\{m_{i,j}\}_{i=0,1,\cdots,15;j=0,1,\cdots,31}$ according to the order defined as $m'_{i',j'} \leq m_{i,j}$ if $i' \leq i$ or ($i' = i$ and $j' \leq j$). By the proposed method we can modify a message so that all sufficient conditions on message $\{m_{i,j}\}$ and some sufficient conditions on chaining variable $\{a_{ij}\}$ of first 26 rounds. Still 73 conditions remain. 9 of those are conditions only for 0-26 round. These 9 conditions are as listed in the following.

Result of the Conventional Message Modification. After Step 2 in Algorithm 2, there are following 9 conditions in round 17-26.
$a_{17,3} = 0$, $a_{18,3} + a_{17,3} = 0$, $a_{22,2} + a_{21,2} = 0$, $a_{23,1} = 0$, $a_{24,30} + a_{22,0} = 0$, $a_{24,3} + a_{23,3} = 0$, $a_{25,30} + a_{24,0} = 1$, $a_{25,1} = 0$, $a_{26,1} = 1$.

Remaining conditions after Step 3. After Step 3 in Algorithm 2, there are following 64 remaining conditions on $\{a_{i,j}\}$.

$a_{27,0} = 0$, $a_{28,30} + a_{26,0} = 1$, $a_{28,3} + a_{27,3} = 0$, $a_{29,30} + a_{28,0} = 0$, $a_{29,3} + a_{28,3} = 0$, $a_{29,1} = 1$, $a_{30,1} = 0$, $a_{31,0} = 1$, $a_{32,30} + a_{30,0} = 0$, $a_{33,30} + a_{32,0} = 0$, $a_{33,3} + a_{32,3} = 0$, $a_{34,3} + a_{33,3} = 1$, $a_{34,2} + a_{33,2} = 1$, $a_{34,1} = 0$, $a_{35,1} = 0$, $a_{35,0} = 0$, $a_{36,30} + a_{34,0} = 0$, $a_{36,3} + a_{35,3} = 1$, $a_{37,30} + a_{36,0} = 1$, $a_{37,3} + a_{36,3} = 1$, $a_{37,1} = 1$, $a_{38,1} = 0$, $a_{40,31} + a_{39,1} = 1$, $a_{40,3} + a_{39,3} = 1$, $a_{41,1} = 1$, $a_{42,31} + a_{40,1} = 1$, $a_{43,31} + a_{42,1} = 1$, $a_{44,3} + a_{43,3} = 1$, $a_{45,1} = 0$, $a_{46,31} + a_{44,1} = 1$, $a_{46,3} + a_{45,3} = 1$, $a_{47,31} + a_{46,1} = 1$, $a_{47,1} = 0$, $a_{48,31} + a_{46,1} = 1$, $a_{48,3} + a_{47,3} = 1$, $a_{49,31} + a_{48,1} = 1$, $a_{49,1} = 0$, $a_{50,31} + a_{48,1} = 1$, $a_{50,3} + a_{49,3} = 1$, $a_{51,31} + a_{50,1} = 1$, $a_{51,1} = 0$, $a_{52,31} + a_{50,1} = 1$, $a_{53,31} + a_{52,1} = 1$, $a_{66,4} + a_{65,4} = 1$, $a_{67,2} = 0$, $a_{68,0} + a_{66,2} = 1$, $a_{69,5} + a_{68,5} = 1$, $a_{69,0} + a_{68,2} = 1$, $a_{70,3} = 0$, $a_{71,1} + a_{69,3} = 1$, $a_{72,6} + a_{71,6} = 1$, $a_{72,1} + a_{71,3} = 1$, $a_{73,4} = 0$, $a_{74,5} + a_{73,5} = 1$, $a_{74,2} + a_{72,4} = 1$, $a_{75,7} + a_{74,7} = 1$, $a_{75,3} = 0$, $a_{75,2} + a_{74,4} = 1$, $a_{76,5} = 1$, $a_{76,1} + a_{74,3} = 1$, $a_{77,3} + a_{75,5} = 1$, $a_{77,1} + a_{76,3} = 1$, $a_{78,3} + a_{77,5} = 0$, $a_{79,6} = 1$.

Now there are 64 remaining conditions on $\{a_{i,j}\}$ for 27-80 round. To adjust these 64 conditions, we use semi-neutral bits as we described in Algorithm 2. In this case, we use 10 semi-neutral bits (corresponding to 'N' in Table 13) and 8 *adjuster*s which are the bits 1-bit-left to 'N'.

8.4 Complexity

Now we consider the complexity when we use the improved message modification proposed as Algorithm 2. Since there are 9 remaining conditions in round 17-26 which should be tested in Step 3, the probability that the output of Step 2 pass the test of Step 3 is $1/2^9$. And since there are 64 remaining conditions on $\{a_{i,j}\}$ after Step 3 and we have 10 semi-neutral bits, the probability that the

ctrl. seq.	control bits	controlled relation
s_{168}	$a_{15,8}$	$a_{30,2} + a_{29,2} = 1$
s_{167}	$a_{16,6}$	$a_{26,2} + a_{25,2} = 1$
s_{166}	$a_{15,7}$	$a_{25,3} + a_{24,3} = 0$
s_{165}	$a_{13,7}$	$a_{24,3} + a_{23,3} = 0$
s_{164}	$a_{13,9}$	$a_{23,0} = 0$
s_{163}	$a_{16,10}$	$a_{22,3} + a_{21,3} = 0$
s_{162}	$a_{16,11}$	$a_{21,29} + a_{20,31} = 0$
s_{161}	$a_{16,8}$	$a_{21,1} = 0$
s_{160}	$a_{16,9}$	$a_{20,29} = 0$
s_{159}	$a_{15,10}$	$a_{20,3} + a_{19,3} = 0$
s_{158}	$a_{15,11}$	$a_{19,31} = 0$
s_{157}	$a_{15,9}$	$a_{19,29} + a_{18,31} = 0$
s_{156}	$a_{14,8}$	$a_{19,1} = 0$
s_{155}	$a_{14,11}$	$a_{18,31} = 1$
s_{154}	$a_{15,14}$	$a_{18,29} = 1$
s_{153}	$a_{13,8}$	$a_{18,1} = 0$
s_{152}	$a_{13,11}$	$a_{17,31} = 0$
s_{151}	$a_{13,10}$	$a_{17,30} = 0$
s_{150}	$a_{13,13}$	$a_{17,1} = 0$
s_{149}	$a_{16,31}$	$m_{15,31} = 0$
s_{148}	$a_{16,29}$	$m_{15,29} = 1$
s_{147}	$a_{16,28}$	$m_{15,28} + m_{10,28} + m_{4,28} + m_{2,28} = 0$
s_{146}	$a_{16,27}$	$m_{15,27} + m_{10,27} + m_{8,28} + m_{4,27} + m_{2,28} + m_{2,27} + m_{0,28} = 1$
s_{145}	$a_{16,26}$	$m_{15,26} + m_{10,28} + m_{10,26} + m_{8,28} + m_{8,27} + m_{7,27} + m_{5,27} + m_{4,26} + m_{2,27} + m_{2,26} + m_{0,27} = 0$
s_{144}	$a_{16,25}$	$m_{15,25} + m_{11,28} + m_{10,27} + m_{10,25} + m_{9,28} + m_{8,27} + m_{8,26} + m_{7,26} + m_{5,26} + m_{4,25} + m_{3,28} + m_{2,28} + m_{2,26} + m_{2,25} + m_{1,28} + m_{0,28} + m_{0,26} = 0$
s_{143}	$a_{16,24}$	$m_{15,24} + m_{12,28} + m_{11,27} + m_{10,26} + m_{10,24} + m_{9,28} + m_{9,27} + m_{8,26} + m_{8,25} + m_{7,25} + m_{6,27} + m_{5,25} + m_{4,28} + m_{4,24} + m_{3,28} + m_{3,27} + m_{2,27} + m_{2,25} + m_{2,24} + m_{1,28} + m_{1,27} + m_{0,27} + m_{0,25} = 1$
s_{142}	$a_{16,23}$	$m_{15,23} + m_{12,28} + m_{12,27} + m_{11,26} + m_{10,25} + m_{10,23} + m_{9,27} + m_{9,26} + m_{8,28} + m_{8,25} + m_{8,24} + m_{7,24} + m_{7,0} + m_{6,27} + m_{6,26} + m_{5,24} + m_{4,27} + m_{4,23} + m_{3,27} + m_{3,26} + m_{2,26} + m_{2,24} + m_{2,23} + m_{1,30} + m_{1,27} + m_{1,26} + m_{1,0} + m_{0,26} + m_{0,24} = 0$
s_{141}	$a_{16,22}$	$m_{15,22} + m_{12,27} + m_{12,26} + m_{11,25} + m_{10,28} + m_{10,24} + m_{10,22} + m_{9,28} + m_{9,26} + m_{9,25} + m_{8,27} + m_{8,24} + m_{8,23} + m_{7,23} + m_{6,27} + m_{6,26} + m_{6,25} + m_{5,23} + m_{4,28} + m_{4,26} + m_{4,22} + m_{3,26} + m_{3,25} + m_{2,28} + m_{2,25} + m_{2,23} + m_{2,22} + m_{1,26} + m_{1,25} + m_{0,25} + m_{0,23} = 0$
s_{140}	$a_{16,21}$	$m_{15,21} + m_{12,28} + m_{12,26} + m_{12,25} + m_{11,28} + m_{11,24} + m_{10,27} + m_{10,23} + m_{10,21} + m_{9,28} + m_{9,27} + m_{9,25} + m_{9,24} + m_{8,26} + m_{8,23} + m_{8,22} + m_{7,27} + m_{7,22} + m_{6,26} + m_{6,25} + m_{6,24} + m_{5,22} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,21} + m_{3,25} + m_{3,24} + m_{2,27} + m_{2,24} + m_{2,22} + m_{2,21} + m_{1,28} + m_{1,25} + m_{1,24} + m_{0,28} + m_{0,24} + m_{0,22} = 0$
s_{139}	$a_{16,20}$	$m_{15,20} + m_{12,28} + m_{12,27} + m_{12,25} + m_{12,24} + m_{11,28} + m_{11,27} + m_{11,23} + m_{10,26} + m_{10,22} + m_{10,20} + m_{9,28} + m_{9,27} + m_{9,26} + m_{9,24} + m_{9,23} + m_{8,28} + m_{8,25} + m_{8,22} + m_{8,21} + m_{7,26} + m_{7,21} + m_{6,25} + m_{6,24} + m_{6,23} + m_{5,27} + m_{5,21} + m_{4,27} + m_{4,26} + m_{4,24} + m_{4,20} + m_{3,24} + m_{3,23} + m_{2,26} + m_{2,23} + m_{2,21} + m_{2,20} + m_{1,28} + m_{1,27} + m_{1,24} + m_{1,23} + m_{0,28} + m_{0,27} + m_{0,23} + m_{0,21} = 1$
s_{138}	$a_{16,19}$	$m_{15,19} + m_{12,27} + m_{12,26} + m_{12,24} + m_{12,23} + m_{11,27} + m_{11,26} + m_{11,22} + m_{10,25} + m_{10,21} + m_{10,19} + m_{9,27} + m_{9,26} + m_{9,25} + m_{9,23} + m_{9,22} + m_{8,28} + m_{8,27} + m_{8,24} + m_{8,21} + m_{8,20} + m_{7,25} + m_{7,20} + m_{7,0} + m_{6,24} + m_{6,23} + m_{6,22} + m_{5,27} + m_{5,26} + m_{5,20} + m_{4,26} + m_{4,25} + m_{4,23} + m_{4,19} + m_{3,23} + m_{3,22} + m_{2,25} + m_{2,22} + m_{2,20} + m_{2,19} + m_{1,30} + m_{1,28} + m_{1,27} + m_{1,26} + m_{1,23} + m_{1,22} + m_{1,0} + m_{0,27} + m_{0,26} + m_{0,22} + m_{0,20} = 1$
s_{137}	$a_{16,18}$	$m_{15,18} + m_{12,26} + m_{12,25} + m_{12,23} + m_{12,22} + m_{11,26} + m_{11,25} + m_{11,21} + m_{10,24} + m_{10,20} + m_{10,18} + m_{9,28} + m_{9,26} + m_{9,25} + m_{9,24} + m_{9,22} + m_{9,21} + m_{8,28} + m_{8,27} + m_{8,26} + m_{8,23} + m_{8,20} + m_{8,19} + m_{7,24} + m_{7,19} + m_{6,27} + m_{6,23} + m_{6,22} + m_{6,21} + m_{5,27} + m_{5,26} + m_{5,25} + m_{5,19} + m_{4,25} + m_{4,24} + m_{4,22} + m_{4,18} + m_{3,22} + m_{3,21} + m_{2,28} + m_{2,24} + m_{2,21} + m_{2,19} + m_{2,18} + m_{1,27} + m_{1,26} + m_{1,25} + m_{1,22} + m_{1,21} + m_{0,26} + m_{0,25} + m_{0,21} + m_{0,19} = 0$
s_{136}	$a_{16,17}$	$m_{15,17} + m_{12,25} + m_{12,24} + m_{12,22} + m_{12,21} + m_{11,25} + m_{11,24} + m_{11,20} + m_{10,23} + m_{10,19} + m_{10,17} + m_{9,28} + m_{9,27} + m_{9,25} + m_{9,24} + m_{9,23} + m_{9,21} + m_{9,20} + m_{8,27} + m_{8,26} + m_{8,25} + m_{8,22} + m_{8,19} + m_{8,18} + m_{7,27} + m_{7,23} + m_{7,18} + m_{6,27} + m_{6,26} + m_{6,22} + m_{6,21} + m_{6,20} + m_{5,26} + m_{5,25} + m_{5,24} + m_{5,18} + m_{4,24} + m_{4,23} + m_{4,21} + m_{4,17} + m_{3,21} + m_{3,20} + m_{2,28} + m_{2,27} + m_{2,23} + m_{2,20} + m_{2,18} + m_{2,17} + m_{1,26} + m_{1,25} + m_{1,24} + m_{1,21} + m_{1,20} + m_{0,28} + m_{0,25} + m_{0,24} + m_{0,20} + m_{0,18} = 0$
s_{135}	$a_{16,16}$	$m_{15,16} + m_{13,11} + m_{12,28} + m_{12,27} + m_{12,24} + m_{12,20} + m_{12,19} + m_{12,15} + m_{11,27} + m_{11,25} + m_{11,24} + m_{11,23} + m_{11,21} + m_{11,17} + m_{11,14} + m_{11,12} + m_{10,28} + m_{10,27} + m_{10,26} + m_{10,23} + m_{10,22} + m_{10,19} + m_{10,15} + m_{9,27} + m_{9,25} + m_{9,24} + m_{9,22} + m_{9,20} + m_{9,19} + m_{9,18} + m_{9,17} + m_{9,14} + m_{9,13} + m_{8,28} + m_{8,27} + m_{8,25} + m_{8,24} + m_{8,21} + m_{8,20} + m_{8,18} + m_{8,16} + m_{8,13} + m_{8,11} + m_{7,26} + m_{7,24} + m_{7,21} + m_{7,20} + m_{7,16} + m_{7,15} + m_{7,0} + m_{6,23} + m_{6,22} + m_{6,21} + m_{6,19} + m_{6,18} + m_{6,13} + m_{5,27} + m_{5,20} + m_{5,19} + m_{5,16} + m_{5,12} + m_{4,28} + m_{4,26} + m_{4,25} + m_{4,15} + m_{3,26} + m_{3,24} + m_{3,22} + m_{3,21} + m_{3,20} + m_{3,18} + m_{3,17} + m_{3,15} + m_{3,13} + m_{3,12} + m_{2,27} + m_{2,26} + m_{2,24} + m_{2,20} + m_{2,19} + m_{2,16} + m_{2,15} + m_{2,11} + m_{1,30} + m_{1,28} + m_{1,27} + m_{1,26} + m_{1,25} + m_{1,24} + m_{1,22} + m_{1,20} + m_{1,19} + m_{1,18} + m_{1,15} + m_{1,13} + m_{1,0} + m_{0,28} + m_{0,26} + m_{0,24} + m_{0,21} + m_{0,20} + m_{0,16} + m_{0,11} = 1$
s_{134}	$a_{16,15}$	$m_{15,15} + m_{13,14} + m_{12,26} + m_{12,24} + m_{12,23} + m_{12,20} + m_{12,19} + m_{12,18} + m_{11,24} + m_{11,23} + m_{11,20} + m_{11,18} + m_{11,17} + m_{11,15} + m_{10,28} + m_{10,27} + m_{10,26} + m_{10,22} + m_{10,19} + m_{10,18} + m_{10,17} + m_{10,15} + m_{9,28} + m_{9,25} + m_{9,23} + m_{9,22} + m_{9,20} + m_{9,19} + m_{9,18} + m_{9,17} + m_{9,16} + m_{8,27} + m_{8,25} + m_{8,24} + m_{8,19} + m_{8,17} + m_{8,14} + m_{7,26} + m_{7,24} + m_{7,23} + m_{7,21} + m_{7,20} + m_{7,19} + m_{7,18} + m_{7,16} + m_{7,0} + m_{6,27} + m_{6,26} + m_{6,24} + m_{6,23} + m_{6,21} + m_{6,20} + m_{6,19} + m_{6,18} + m_{6,16} + m_{5,26} + m_{5,24} + m_{5,20} + m_{5,19} + m_{5,16} + m_{5,15} + m_{4,27} + m_{4,26} + m_{4,25} + m_{4,23} + m_{4,22} + m_{4,21} + m_{4,18} + m_{4,15} + m_{3,28} + m_{3,27} + m_{3,25} + m_{3,24} + m_{3,22} + m_{3,21} + m_{3,20} + m_{3,19} + m_{3,16} + m_{3,15} + m_{2,27} + m_{2,26} + m_{2,23} + m_{2,21} + m_{2,20} + m_{2,16} + m_{2,15} + m_{2,14} + m_{1,30} + m_{1,26} + m_{1,25} + m_{1,24} + m_{1,23} + m_{1,22} + m_{1,21} + m_{1,19} + m_{1,16} + m_{1,0} + m_{0,24} + m_{0,20} + m_{0,19} + m_{0,18} + m_{0,16} + m_{0,14} = 0$
s_{133}	$a_{16,14}$	$m_{15,14} + m_{13,14} + m_{12,26} + m_{12,24} + m_{12,21} + m_{12,19} + m_{11,27} + m_{11,24} + m_{11,21} + m_{11,20} + m_{11,15} + m_{10,27} + m_{10,22} + m_{10,21} + m_{10,20} + m_{10,19} + m_{10,18} + m_{10,16} + m_{10,14} + m_{9,28} + m_{9,26} + m_{9,25} + m_{9,24} + m_{9,22} + m_{9,18} + m_{9,16} + m_{8,28} + m_{8,26} + m_{8,24} + m_{8,22} + m_{8,20} + m_{8,15} + m_{8,14} + m_{7,26} + m_{7,23} + m_{7,19} + m_{7,18} + m_{7,15} + m_{7,0} + m_{6,27} + m_{6,25} + m_{6,24} + m_{6,21} + m_{6,19} + m_{6,18} + m_{6,17} + m_{6,16} + m_{5,27} + m_{5,21} + m_{5,20} + m_{5,19} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,23} + m_{4,21} + m_{4,20} + m_{4,19} + m_{4,14} + m_{3,25} + m_{3,24} + m_{3,22} + m_{3,21} + m_{3,20} + m_{3,17} + m_{3,16} + m_{3,15} + m_{2,27} + m_{2,24} + m_{2,23} + m_{2,18} + m_{2,17} + m_{2,15} + m_{1,30} + m_{1,26} + m_{1,25} + m_{1,23} + m_{1,22} + m_{1,17} + m_{1,16} + m_{1,0} + m_{0,26} + m_{0,25} + m_{0,24} + m_{0,23} + m_{0,21} + m_{0,20} + m_{0,19} + m_{0,17} + m_{0,15} + m_{0,14} = 1$
s_{132}	$a_{16,12}$	$m_{15,12} + m_{12,27} + m_{12,20} + m_{12,19} + m_{12,17} + m_{12,16} + m_{11,28} + m_{11,27} + m_{11,26} + m_{11,25} + m_{11,20} + m_{11,19} + m_{11,15} + m_{10,27} + m_{10,25} + m_{10,24} + m_{10,18} + m_{10,14} + m_{10,12} + m_{9,27} + m_{9,23} + m_{9,22} + m_{9,20} + m_{9,19} + m_{9,18} + m_{9,16} + m_{9,15} + m_{8,28} + m_{8,27} + m_{8,26} + m_{8,24} + m_{8,22} + m_{8,21} + m_{8,20} + m_{8,17} + m_{8,14} + m_{8,13} + m_{7,26} + m_{7,25} + m_{7,24} + m_{7,23} + m_{7,22} + m_{7,18} + m_{7,13} + m_{7,0} + m_{6,27} + m_{6,26} + m_{6,25} + m_{6,24} + m_{6,22} + m_{6,21} + m_{6,17} + m_{6,16} + m_{6,15} + m_{5,26} + m_{5,24} + m_{5,21} + m_{5,20} + m_{5,19} + m_{5,13} + m_{4,25} + m_{4,24} + m_{4,19} + m_{4,18} + m_{4,16} + m_{4,12} + m_{3,28} + m_{3,27} + m_{3,25} + m_{3,16} + m_{3,15} + m_{2,28} + m_{2,23} + m_{2,22} + m_{2,18} + m_{2,15} + m_{2,13} + m_{2,12} + m_{1,30} + m_{1,21} + m_{1,20} + m_{1,19} + m_{1,16} + m_{1,15} + m_{1,0} + m_{0,28} + m_{0,27} + m_{0,23} + m_{0,20} + m_{0,19} + m_{0,15} + m_{0,13} = 1$

Table 9. Control bits and controlled relations for the full SHA-1 (I)

ctrl. seq.	control bits	controlled relation
s_{131}	$a_{16,7}$	$m_{15,7}+m_{15,6}+m_{9,6}+m_{8,2}+m_{7,6}+m_{7,3}+m_{6,5}+m_{6,3}+m_{5,5}+m_{5,4}+m_{5,2}+m_{5,1}+m_{4,4}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,3}+m_{1,1}+m_{0,3}+m_{0,2}+m_{79,11}=1$
s_{130}	$a_{16,5}$	$m_{15,5}=0$
s_{129}	$a_{16,4}$	$m_{15,4}+m_{7,3}+m_{7,2}+m_{6,5}+m_{6,3}+m_{5,4}+m_{5,3}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,30}+m_{1,3}+m_{1,1}+m_{0,3}=0$
s_{128}	$a_{16,2}$	$m_{15,2}+m_{7,3}+m_{7,2}+m_{7,0}+m_{6,5}+m_{6,3}+m_{5,5}+m_{5,4}+m_{5,1}+m_{4,2}+m_{3,2}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,3}+m_{1,2}+m_{1,1}+m_{0,3}+m_{0,2}=0$
s_{127}	$a_{16,0}$	$m_{15,0}+m_{1,30}=1$
s_{126}	$a_{13,20}$	$m_{15,3}+m_{7,3}+m_{7,2}+m_{7,0}+m_{6,5}+m_{5,5}+m_{5,4}+m_{5,2}+m_{5,1}+m_{4,3}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,30}+m_{1,1}+m_{0,3}=0$
s_{125}	$a_{13,18}$	$m_{15,1}+m_{8,2}+m_{7,3}+m_{7,2}+m_{7,0}+m_{5,3}+m_{4,2}+m_{3,4}+m_{2,2}+m_{1,2}+m_{0,4}+m_{0,2}=0$
s_{124}	$a_{13,15}$	$m_{15,30}=1$
s_{123}	$a_{15,31}$	$m_{14,31}=1$
s_{122}	$a_{15,30}$	$m_{14,30}=1$
s_{121}	$a_{15,29}$	$m_{14,29}=0$
s_{120}	$a_{15,28}$	$m_{14,28}+m_{9,28}+m_{3,28}+m_{1,28}=1$
s_{119}	$a_{15,27}$	$m_{14,27}+m_{12,28}+m_{9,27}+m_{4,28}+m_{3,27}+m_{1,27}=1$
s_{118}	$a_{15,26}$	$m_{14,26}+m_{12,27}+m_{10,28}+m_{9,28}+m_{9,26}+m_{6,27}+m_{4,28}+m_{4,27}+m_{3,26}+m_{2,28}+m_{1,26}=1$
s_{117}	$a_{15,25}$	$m_{14,25}+m_{12,28}+m_{12,26}+m_{10,28}+m_{10,27}+m_{9,27}+m_{9,25}+m_{7,27}+m_{6,26}+m_{4,27}+m_{4,26}+m_{3,25}+m_{2,27}+m_{1,25}=1$
s_{116}	$a_{15,24}$	$m_{14,24}+m_{12,27}+m_{12,25}+m_{11,28}+m_{10,27}+m_{10,26}+m_{9,26}+m_{9,24}+m_{7,26}+m_{6,25}+m_{4,28}+m_{4,26}+m_{4,25}+m_{3,28}+m_{3,24}+m_{2,26}+m_{1,24}+m_{0,28}=0$
s_{115}	$a_{15,23}$	$m_{14,23}+m_{12,26}+m_{12,24}+m_{11,27}+m_{10,26}+m_{10,25}+m_{9,28}+m_{9,25}+m_{9,23}+m_{8,28}+m_{7,25}+m_{6,24}+m_{5,27}+m_{4,27}+m_{4,25}+m_{4,24}+m_{3,28}+m_{3,27}+m_{3,23}+m_{2,25}+m_{1,28}+m_{1,23}+m_{0,27}=1$
s_{114}	$a_{15,22}$	$m_{14,22}+m_{12,28}+m_{12,25}+m_{12,23}+m_{11,26}+m_{10,28}+m_{10,25}+m_{10,24}+m_{9,27}+m_{9,24}+m_{9,22}+m_{8,27}+m_{7,24}+m_{6,27}+m_{6,23}+m_{5,26}+m_{4,28}+m_{4,26}+m_{4,24}+m_{4,23}+m_{3,27}+m_{3,26}+m_{3,22}+m_{2,24}+m_{1,27}+m_{1,22}+m_{0,26}=1$
s_{113}	$a_{15,21}$	$m_{14,21}+m_{12,27}+m_{12,24}+m_{12,22}+m_{11,25}+m_{10,28}+m_{10,27}+m_{10,24}+m_{10,23}+m_{9,28}+m_{9,26}+m_{9,23}+m_{9,21}+m_{8,26}+m_{7,23}+m_{6,26}+m_{6,22}+m_{5,25}+m_{4,28}+m_{4,27}+m_{4,25}+m_{4,23}+m_{4,22}+m_{3,26}+m_{3,25}+m_{3,21}+m_{2,28}+m_{2,23}+m_{1,26}+m_{1,21}+m_{0,25}=1$
s_{112}	$a_{15,20}$	$m_{14,20}+m_{12,26}+m_{12,23}+m_{12,21}+m_{11,28}+m_{11,24}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,23}+m_{10,22}+m_{9,27}+m_{9,25}+m_{9,22}+m_{9,20}+m_{8,28}+m_{8,25}+m_{7,27}+m_{7,22}+m_{6,25}+m_{6,21}+m_{5,24}+m_{4,27}+m_{4,26}+m_{4,24}+m_{4,22}+m_{4,21}+m_{3,28}+m_{3,25}+m_{3,24}+m_{3,20}+m_{2,27}+m_{2,22}+m_{1,25}+m_{1,20}+m_{0,28}+m_{0,24}=0$
s_{111}	$a_{15,19}$	$m_{14,19}+m_{12,25}+m_{12,22}+m_{12,20}+m_{11,28}+m_{11,27}+m_{11,23}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,25}+m_{10,22}+m_{10,21}+m_{9,28}+m_{9,26}+m_{9,24}+m_{9,21}+m_{9,19}+m_{8,27}+m_{8,24}+m_{7,27}+m_{7,26}+m_{7,21}+m_{6,27}+m_{6,24}+m_{6,20}+m_{5,23}+m_{4,28}+m_{4,26}+m_{4,25}+m_{4,23}+m_{4,21}+m_{4,20}+m_{3,27}+m_{3,24}+m_{3,23}+m_{3,19}+m_{2,26}+m_{2,21}+m_{1,28}+m_{1,24}+m_{1,19}+m_{0,28}+m_{0,27}+m_{0,23}=1$
s_{110}	$a_{15,18}$	$m_{14,18}+m_{13,14}+m_{12,28}+m_{12,26}+m_{12,22}+m_{12,21}+m_{12,19}+m_{12,18}+m_{11,27}+m_{11,26}+m_{11,24}+m_{11,20}+m_{11,17}+m_{11,15}+m_{10,27}+m_{10,25}+m_{10,24}+m_{10,22}+m_{10,20}+m_{10,19}+m_{10,18}+m_{9,28}+m_{9,27}+m_{9,26}+m_{9,25}+m_{9,23}+m_{9,21}+m_{9,18}+m_{9,17}+m_{9,16}+m_{8,26}+m_{8,20}+m_{8,19}+m_{8,16}+m_{8,14}+m_{7,27}+m_{7,26}+m_{7,24}+m_{7,23}+m_{7,19}+m_{7,18}+m_{7,0}+m_{6,27}+m_{6,25}+m_{6,21}+m_{6,19}+m_{6,16}+m_{5,26}+m_{5,23}+m_{5,20}+m_{5,19}+m_{5,15}+m_{4,27}+m_{4,26}+m_{4,24}+m_{4,23}+m_{4,22}+m_{4,20}+m_{4,18}+m_{3,27}+m_{3,26}+m_{3,25}+m_{3,24}+m_{3,23}+m_{3,21}+m_{3,20}+m_{3,16}+m_{3,15}+m_{2,27}+m_{2,23}+m_{2,18}+m_{2,14}+m_{1,30}+m_{1,27}+m_{1,26}+m_{1,25}+m_{1,23}+m_{1,21}+m_{1,16}+m_{1,0}+m_{0,27}+m_{0,24}+m_{0,23}+m_{0,20}+m_{0,19}+m_{0,14}=1$
s_{109}	$a_{15,17}$	$m_{14,17}+m_{12,27}+m_{12,23}+m_{12,20}+m_{12,18}+m_{11,27}+m_{11,26}+m_{11,25}+m_{11,21}+m_{10,28}+m_{10,26}+m_{10,25}+m_{10,24}+m_{10,23}+m_{10,20}+m_{10,19}+m_{9,26}+m_{9,24}+m_{9,22}+m_{9,19}+m_{9,17}+m_{8,28}+m_{8,25}+m_{8,22}+m_{7,27}+m_{7,25}+m_{7,24}+m_{7,19}+m_{6,27}+m_{6,26}+m_{6,25}+m_{6,22}+m_{6,18}+m_{5,27}+m_{5,26}+m_{5,21}+m_{4,28}+m_{4,27}+m_{4,26}+m_{4,24}+m_{4,23}+m_{4,21}+m_{4,19}+m_{4,18}+m_{3,28}+m_{3,25}+m_{3,22}+m_{3,21}+m_{3,17}+m_{2,28}+m_{2,24}+m_{2,19}+m_{1,28}+m_{1,26}+m_{1,22}+m_{1,17}+m_{0,26}+m_{0,25}+m_{0,21}=1$
s_{108}	$a_{15,16}$	$m_{14,16}+m_{12,26}+m_{12,22}+m_{12,19}+m_{12,17}+m_{11,26}+m_{11,25}+m_{11,24}+m_{11,20}+m_{10,28}+m_{10,27}+m_{10,25}+m_{10,24}+m_{10,23}+m_{10,22}+m_{10,19}+m_{10,18}+m_{9,28}+m_{9,25}+m_{9,23}+m_{9,21}+m_{9,18}+m_{9,16}+m_{8,27}+m_{8,24}+m_{8,21}+m_{7,27}+m_{7,26}+m_{7,24}+m_{7,23}+m_{7,18}+m_{7,0}+m_{6,27}+m_{6,26}+m_{6,25}+m_{6,24}+m_{6,21}+m_{6,17}+m_{5,26}+m_{5,25}+m_{5,20}+m_{4,28}+m_{4,27}+m_{4,26}+m_{4,25}+m_{4,23}+m_{4,22}+m_{4,20}+m_{4,18}+m_{4,17}+m_{3,28}+m_{3,27}+m_{3,24}+m_{3,21}+m_{3,20}+m_{3,16}+m_{2,28}+m_{2,27}+m_{2,23}+m_{2,18}+m_{1,30}+m_{1,28}+m_{1,27}+m_{1,25}+m_{1,21}+m_{1,16}+m_{1,0}+m_{0,25}+m_{0,24}+m_{0,20}=0$
s_{107}	$a_{15,15}$	$m_{14,15}+m_{12,25}+m_{12,21}+m_{12,18}+m_{12,16}+m_{11,25}+m_{11,24}+m_{11,23}+m_{11,19}+m_{10,28}+m_{10,27}+m_{10,26}+m_{10,24}+m_{10,23}+m_{10,22}+m_{10,21}+m_{10,18}+m_{10,17}+m_{9,28}+m_{9,27}+m_{9,24}+m_{9,22}+m_{9,20}+m_{9,17}+m_{9,15}+m_{8,28}+m_{8,26}+m_{8,23}+m_{8,20}+m_{7,26}+m_{7,25}+m_{7,23}+m_{7,22}+m_{7,17}+m_{6,26}+m_{6,25}+m_{6,24}+m_{6,23}+m_{6,20}+m_{6,16}+m_{5,25}+m_{5,24}+m_{5,19}+m_{4,28}+m_{4,27}+m_{4,26}+m_{4,25}+m_{4,24}+m_{4,22}+m_{4,21}+m_{4,19}+m_{4,17}+m_{4,16}+m_{3,27}+m_{3,26}+m_{3,23}+m_{3,20}+m_{3,19}+m_{3,15}+m_{2,28}+m_{2,27}+m_{2,26}+m_{2,22}+m_{2,17}+m_{1,27}+m_{1,26}+m_{1,24}+m_{1,20}+m_{1,15}+m_{0,24}+m_{0,23}+m_{0,19}=0$
s_{106}	$a_{15,13}$	$m_{14,13}+m_{13,14}+m_{12,27}+m_{12,26}+m_{12,24}+m_{12,23}+m_{12,22}+m_{12,19}+m_{12,18}+m_{12,16}+m_{12,14}+m_{11,28}+m_{11,24}+m_{11,23}+m_{11,21}+m_{11,20}+m_{11,15}+m_{10,28}+m_{10,25}+m_{10,24}+m_{10,20}+m_{10,18}+m_{10,16}+m_{10,15}+m_{9,25}+m_{9,22}+m_{9,21}+m_{9,18}+m_{9,17}+m_{9,16}+m_{9,15}+m_{9,13}+m_{8,28}+m_{8,26}+m_{8,24}+m_{8,23}+m_{8,21}+m_{8,20}+m_{8,19}+m_{8,18}+m_{8,16}+m_{8,14}+m_{7,27}+m_{7,25}+m_{7,21}+m_{7,19}+m_{7,18}+m_{7,15}+m_{7,0}+m_{6,26}+m_{6,25}+m_{6,24}+m_{6,22}+m_{6,18}+m_{6,16}+m_{6,14}+m_{5,27}+m_{5,20}+m_{5,19}+m_{5,17}+m_{5,15}+m_{4,27}+m_{4,24}+m_{4,22}+m_{4,20}+m_{4,18}+m_{4,17}+m_{4,15}+m_{4,14}+m_{3,27}+m_{3,22}+m_{3,20}+m_{3,17}+m_{3,16}+m_{3,15}+m_{3,13}+m_{2,27}+m_{2,26}+m_{2,24}+m_{2,23}+m_{2,18}+m_{2,15}+m_{2,14}+m_{1,30}+m_{1,28}+m_{1,26}+m_{1,24}+m_{1,22}+m_{1,21}+m_{1,16}+m_{1,13}+m_{1,0}+m_{0,28}+m_{0,26}+m_{0,24}+m_{0,23}+m_{0,21}+m_{0,20}+m_{0,19}+m_{0,17}+m_{0,14}=0$
s_{105}	$a_{15,12}$	$m_{14,12}+m_{13,11}+m_{12,28}+m_{12,27}+m_{12,26}+m_{12,23}+m_{12,22}+m_{12,21}+m_{12,19}+m_{12,18}+m_{12,13}+m_{11,28}+m_{11,27}+m_{11,25}+m_{11,22}+m_{11,20}+m_{11,19}+m_{11,17}+m_{11,16}+m_{11,14}+m_{11,12}+m_{10,28}+m_{10,26}+m_{10,25}+m_{10,24}+m_{10,21}+m_{10,20}+m_{10,16}+m_{10,14}+m_{9,28}+m_{9,27}+m_{9,26}+m_{9,24}+m_{9,23}+m_{9,21}+m_{9,19}+m_{9,18}+m_{9,13}+m_{9,12}+m_{8,28}+m_{8,26}+m_{8,25}+m_{8,23}+m_{8,16}+m_{8,13}+m_{8,11}+m_{7,24}+m_{7,23}+m_{7,21}+m_{7,19}+m_{7,17}+m_{7,16}+m_{7,15}+m_{7,14}+m_{7,0}+m_{6,26}+m_{6,25}+m_{6,21}+m_{6,18}+m_{6,17}+m_{5,27}+m_{5,24}+m_{5,23}+m_{5,22}+m_{5,21}+m_{5,20}+m_{5,19}+m_{5,17}+m_{5,12}+m_{4,27}+m_{4,24}+m_{4,21}+m_{4,20}+m_{4,19}+m_{4,18}+m_{4,15}+m_{4,14}+m_{4,13}+m_{3,28}+m_{3,26}+m_{3,23}+m_{3,22}+m_{3,21}+m_{3,20}+m_{3,19}+m_{3,18}+m_{3,16}+m_{3,15}+m_{3,13}+m_{2,25}+m_{2,23}+m_{2,22}+m_{2,20}+m_{2,19}+m_{2,17}+m_{2,15}+m_{2,14}+m_{2,11}+m_{1,30}+m_{1,26}+m_{1,24}+m_{1,22}+m_{1,21}+m_{1,18}+m_{1,17}+m_{1,15}+m_{1,13}+m_{1,12}+m_{1,0}+m_{0,28}+m_{0,26}+m_{0,23}+m_{0,19}+m_{0,17}+m_{0,11}=0$
s_{104}	$a_{15,5}$	$m_{14,5}=0$
s_{103}	$a_{15,4}$	$m_{14,4}+m_{5,5}+m_{3,4}=0$
s_{102}	$a_{9,2}$	$m_{14,3}+m_{8,2}+m_{7,3}+m_{7,0}+m_{6,5}+m_{6,3}+m_{6,2}+m_{5,5}+m_{5,4}+m_{5,2}+m_{4,2}+m_{2,5}+m_{2,4}+m_{2,3}+m_{2,1}+m_{1,2}+m_{1,1}+m_{1,0}+m_{0,4}+m_{0,3}+m_{0,2}=0$
s_{101}	$a_{15,2}$	$m_{14,2}+m_{8,2}+m_{7,2}+m_{5,4}+m_{5,2}+m_{5,1}+m_{4,2}+m_{2,1}+m_{1,1}+m_{0,4}=0$
s_{100}	$a_{15,1}$	$m_{14,1}+m_{8,2}+m_{7,3}+m_{7,2}+m_{6,5}+m_{6,3}+m_{5,4}+m_{5,3}+m_{5,2}+m_{5,1}+m_{4,2}+m_{3,4}+m_{3,2}+m_{2,5}+m_{2,3}+m_{2,2}+m_{2,1}+m_{1,3}+m_{0,3}+m_{0,2}=0$

Table 10. Control bits and controlled relations for the full SHA-1 (II)

ctrl. seq.	control bits	controlled relation
s_{99}	$a_{13,22}$	$m_{14,0} = 0$
s_{98}	$a_{13,26}$	$m_{13,31} = 1$
s_{97}	$a_{14,30}$	$m_{13,30} = 1$
s_{96}	$a_{14,29}$	$m_{13,29} = 1$
s_{95}	$a_{14,28}$	$m_{13,28} + m_{8,28} + m_{2,28} + m_{0,28} = 1$
s_{94}	$a_{14,27}$	$m_{13,27} + m_{11,28} + m_{8,27} + m_{3,28} + m_{2,27} + m_{0,27} = 0$
s_{93}	$a_{14,26}$	$m_{13,26}+m_{11,27}+m_{9,28}+m_{8,28}+m_{8,26}+m_{5,27}+m_{3,28}+m_{3,27}+m_{2,26}+m_{1,28}+m_{0,26} = 0$
s_{92}	$a_{14,25}$	$m_{13,25} + m_{11,28} + m_{11,26} + m_{9,28} + m_{9,27} + m_{8,27} + m_{8,25} + m_{6,27} + m_{5,26} + m_{3,27} + m_{3,26} + m_{2,25} + m_{1,27} + m_{0,25} = 1$
s_{91}	$a_{14,24}$	$m_{13,24} + m_{12,28} + m_{11,27} + m_{11,25} + m_{10,28} + m_{9,27} + m_{9,26} + m_{8,26} + m_{8,24} + m_{6,26} + m_{5,25} + m_{4,28} + m_{3,28} + m_{3,26} + m_{3,25} + m_{2,28} + m_{2,24} + m_{1,28} + m_{1,26} + m_{0,24} = 0$
s_{90}	$a_{14,23}$	$m_{13,23} + m_{12,27} + m_{11,26} + m_{11,24} + m_{10,28} + m_{10,27} + m_{9,26} + m_{9,25} + m_{8,28} + m_{8,25} + m_{8,23} + m_{7,27} + m_{6,25} + m_{5,24} + m_{4,28} + m_{4,27} + m_{3,27} + m_{3,25} + m_{3,24} + m_{2,27} + m_{2,23} + m_{1,27} + m_{1,25} + m_{0,28} + m_{0,23} = 1$
s_{89}	$a_{14,22}$	$m_{13,22} + m_{12,26} + m_{11,28} + m_{11,25} + m_{11,23} + m_{10,27} + m_{10,26} + m_{9,28} + m_{9,25} + m_{9,24} + m_{8,28} + m_{8,27} + m_{8,24} + m_{8,22} + m_{7,27} + m_{7,26} + m_{6,24} + m_{5,27} + m_{5,23} + m_{4,27} + m_{4,26} + m_{3,28} + m_{3,26} + m_{3,24} + m_{3,23} + m_{2,28} + m_{2,26} + m_{2,22} + m_{1,26} + m_{1,24} + m_{0,28} + m_{0,27} + m_{0,22} = 1$
s_{88}	$a_{14,21}$	$m_{13,21} + m_{12,25} + m_{11,27} + m_{11,24} + m_{11,22} + m_{10,28} + m_{10,26} + m_{10,25} + m_{9,28} + m_{9,27} + m_{9,24} + m_{9,23} + m_{8,27} + m_{8,26} + m_{8,23} + m_{8,21} + m_{7,27} + m_{7,26} + m_{7,25} + m_{6,23} + m_{5,27} + m_{5,26} + m_{5,22} + m_{4,26} + m_{4,25} + m_{3,28} + m_{3,27} + m_{3,25} + m_{3,23} + m_{3,22} + m_{2,27} + m_{2,25} + m_{2,21} + m_{1,28} + m_{1,25} + m_{1,23} + m_{0,27} + m_{0,26} + m_{0,21} = 0$
s_{87}	$a_{14,20}$	$m_{13,20} + m_{12,28} + m_{12,24} + m_{11,28} + m_{11,26} + m_{11,23} + m_{11,21} + m_{10,28} + m_{10,27} + m_{10,25} + m_{10,24} + m_{9,27} + m_{9,26} + m_{9,23} + m_{9,22} + m_{8,26} + m_{8,25} + m_{8,22} + m_{8,20} + m_{7,26} + m_{7,25} + m_{7,24} + m_{6,27} + m_{6,22} + m_{5,26} + m_{5,25} + m_{5,21} + m_{4,25} + m_{4,24} + m_{3,28} + m_{3,27} + m_{3,26} + m_{3,24} + m_{3,22} + m_{3,21} + m_{2,26} + m_{2,24} + m_{2,20} + m_{1,27} + m_{1,24} + m_{1,22} + m_{0,28} + m_{0,26} + m_{0,25} + m_{0,20} = 0$
s_{86}	$a_{14,19}$	$m_{13,19} + m_{12,27} + m_{12,23} + m_{11,27} + m_{11,25} + m_{11,22} + m_{11,20} + m_{10,27} + m_{10,26} + m_{10,24} + m_{10,23} + m_{9,26} + m_{9,25} + m_{9,22} + m_{9,21} + m_{8,28} + m_{8,25} + m_{8,24} + m_{8,21} + m_{8,19} + m_{7,25} + m_{7,24} + m_{7,23} + m_{7,0} + m_{6,26} + m_{6,21} + m_{5,27} + m_{5,25} + m_{5,24} + m_{5,20} + m_{4,28} + m_{4,24} + m_{4,23} + m_{3,27} + m_{3,26} + m_{3,25} + m_{3,23} + m_{3,21} + m_{3,20} + m_{2,28} + m_{2,25} + m_{2,23} + m_{2,19} + m_{1,30} + m_{1,26} + m_{1,23} + m_{1,21} + m_{1,0} + m_{0,28} + m_{0,27} + m_{0,25} + m_{0,24} + m_{0,19} = 0$
s_{85}	$a_{14,18}$	$m_{13,18} + m_{12,28} + m_{12,26} + m_{12,22} + m_{11,28} + m_{11,26} + m_{11,24} + m_{11,21} + m_{11,19} + m_{10,26} + m_{10,25} + m_{10,23} + m_{10,22} + m_{9,25} + m_{9,24} + m_{9,21} + m_{9,20} + m_{8,27} + m_{8,24} + m_{8,23} + m_{8,20} + m_{8,18} + m_{7,27} + m_{7,24} + m_{7,23} + m_{7,22} + m_{6,27} + m_{6,25} + m_{6,20} + m_{5,27} + m_{5,26} + m_{5,24} + m_{5,23} + m_{5,19} + m_{4,27} + m_{4,23} + m_{4,22} + m_{3,28} + m_{3,26} + m_{3,25} + m_{3,24} + m_{3,22} + m_{3,20} + m_{3,19} + m_{2,27} + m_{2,24} + m_{2,22} + m_{2,18} + m_{1,25} + m_{1,22} + m_{1,20} + m_{0,28} + m_{0,27} + m_{0,26} + m_{0,24} + m_{0,23} + m_{0,18} = 1$
s_{84}	$a_{14,17}$	$m_{13,17} + m_{12,27} + m_{12,25} + m_{12,21} + m_{11,27} + m_{11,25} + m_{11,23} + m_{11,20} + m_{11,18} + m_{10,25} + m_{10,24} + m_{10,22} + m_{10,21} + m_{9,24} + m_{9,23} + m_{9,20} + m_{9,19} + m_{8,26} + m_{8,23} + m_{8,22} + m_{8,19} + m_{8,17} + m_{7,27} + m_{7,26} + m_{7,23} + m_{7,22} + m_{7,21} + m_{6,26} + m_{6,24} + m_{6,19} + m_{5,26} + m_{5,25} + m_{5,23} + m_{5,22} + m_{5,18} + m_{4,28} + m_{4,26} + m_{4,22} + m_{4,21} + m_{3,28} + m_{3,27} + m_{3,25} + m_{3,24} + m_{3,23} + m_{3,21} + m_{3,19} + m_{3,18} + m_{2,28} + m_{2,26} + m_{2,23} + m_{2,21} + m_{2,17} + m_{1,28} + m_{1,24} + m_{1,21} + m_{1,19} + m_{0,27} + m_{0,26} + m_{0,25} + m_{0,23} + m_{0,22} + m_{0,17} = 1$
s_{83}	$a_{14,16}$	$m_{13,16} + m_{12,28} + m_{12,26} + m_{12,24} + m_{12,20} + m_{11,26} + m_{11,24} + m_{11,22} + m_{11,19} + m_{11,17} + m_{10,28} + m_{10,24} + m_{10,23} + m_{10,21} + m_{10,20} + m_{9,28} + m_{9,23} + m_{9,22} + m_{9,19} + m_{9,18} + m_{8,25} + m_{8,22} + m_{8,21} + m_{8,18} + m_{8,16} + m_{7,27} + m_{7,26} + m_{7,25} + m_{7,22} + m_{7,21} + m_{7,20} + m_{6,27} + m_{6,25} + m_{6,23} + m_{6,18} + m_{5,25} + m_{5,24} + m_{5,22} + m_{5,21} + m_{5,17} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,21} + m_{4,20} + m_{3,27} + m_{3,26} + m_{3,24} + m_{3,23} + m_{3,22} + m_{3,20} + m_{3,18} + m_{3,17} + m_{2,27} + m_{2,25} + m_{2,22} + m_{2,20} + m_{2,16} + m_{1,28} + m_{1,27} + m_{1,23} + m_{1,20} + m_{1,18} + m_{0,28} + m_{0,26} + m_{0,25} + m_{0,24} + m_{0,22} + m_{0,21} + m_{0,16} = 1$
s_{82}	$a_{14,15}$	$m_{13,15} + m_{13,14} + m_{12,27} + m_{12,26} + m_{12,25} + m_{12,24} + m_{12,23} + m_{12,22} + m_{12,19} + m_{12,18} + m_{11,28} + m_{11,25} + m_{11,24} + m_{11,23} + m_{11,22} + m_{11,21} + m_{11,20} + m_{11,18} + m_{11,17} + m_{11,16} + m_{11,15} + m_{10,27} + m_{10,26} + m_{10,23} + m_{10,21} + m_{10,20} + m_{10,18} + m_{9,28} + m_{9,27} + m_{9,26} + m_{9,22} + m_{9,20} + m_{9,18} + m_{9,16} + m_{8,24} + m_{8,23} + m_{8,21} + m_{8,19} + m_{8,17} + m_{8,16} + m_{8,15} + m_{8,14} + m_{7,27} + m_{7,26} + m_{7,23} + m_{7,21} + m_{7,18} + m_{7,0} + m_{6,27} + m_{6,25} + m_{6,24} + m_{6,23} + m_{6,22} + m_{6,21} + m_{6,17} + m_{6,16} + m_{5,26} + m_{5,24} + m_{5,22} + m_{5,21} + m_{5,19} + m_{5,16} + m_{5,15} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,24} + m_{4,23} + m_{4,20} + m_{4,18} + m_{3,28} + m_{3,27} + m_{3,26} + m_{3,24} + m_{3,23} + m_{3,20} + m_{3,19} + m_{3,18} + m_{3,17} + m_{3,15} + m_{2,28} + m_{2,27} + m_{2,26} + m_{2,25} + m_{2,24} + m_{2,23} + m_{2,21} + m_{2,20} + m_{2,19} + m_{2,18} + m_{2,15} + m_{2,14} + m_{1,30} + m_{1,27} + m_{1,25} + m_{1,22} + m_{1,21} + m_{1,19} + m_{1,18} + m_{1,17} + m_{1,16} + m_{1,0} + m_{0,27} + m_{0,26} + m_{0,25} + m_{0,22} + m_{0,21} + m_{0,19} + m_{0,15} + m_{0,14} = 1$
s_{81}	$a_{14,13}$	$m_{13,13} + m_{12,25} + m_{12,23} + m_{12,21} + m_{12,17} + m_{11,27} + m_{11,23} + m_{11,21} + m_{11,19} + m_{11,16} + m_{11,14} + m_{10,28} + m_{10,25} + m_{10,21} + m_{10,20} + m_{10,18} + m_{10,17} + m_{9,28} + m_{9,27} + m_{9,25} + m_{9,20} + m_{9,19} + m_{9,16} + m_{9,15} + m_{8,28} + m_{8,22} + m_{8,19} + m_{8,18} + m_{8,15} + m_{8,13} + m_{7,26} + m_{7,24} + m_{7,23} + m_{7,22} + m_{7,19} + m_{7,18} + m_{7,17} + m_{6,27} + m_{6,25} + m_{6,24} + m_{6,22} + m_{6,20} + m_{6,15} + m_{5,27} + m_{5,26} + m_{5,25} + m_{5,22} + m_{5,21} + m_{5,19} + m_{5,18} + m_{5,14} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,24} + m_{4,22} + m_{4,18} + m_{4,17} + m_{3,28} + m_{3,26} + m_{3,24} + m_{3,23} + m_{3,21} + m_{3,20} + m_{3,19} + m_{3,17} + m_{3,15} + m_{3,14} + m_{2,26} + m_{2,24} + m_{2,22} + m_{2,19} + m_{2,17} + m_{2,13} + m_{1,28} + m_{1,25} + m_{1,24} + m_{1,20} + m_{1,17} + m_{1,15} + m_{0,28} + m_{0,25} + m_{0,23} + m_{0,22} + m_{0,21} + m_{0,19} + m_{0,18} + m_{0,13} = 0$
s_{80}	$a_{14,5}$	$m_{13,5} + m_{7,2} + m_{6,2} + m_{5,5} + m_{5,2} + m_{4,4} + m_{2,3} + m_{2,2} + m_{2,1} + m_{1,30} + m_{1,0} = 1$
s_{79}	$a_{14,4}$	$m_{13,4} + m_{5,5} + m_{3,4} + m_{2,4} + m_{0,4} = 0$
s_{78}	$a_{14,3}$	$m_{13,3} + m_{6,2} + m_{5,3} + m_{5,2} + m_{5,1} + m_{4,2} + m_{3,2} + m_{2,4} + m_{2,2} + m_{2,1} + m_{1,0} + m_{0,2} = 1$
s_{77}	$a_{9,4}$	$m_{13,2} + m_{8,2} + m_{7,0} + m_{5,3} + m_{2,2} + m_{1,30} + m_{0,2} = 0$
s_{76}	$a_{14,1}$	$m_{13,1} = 0$
s_{75}	$a_{14,0}$	$m_{13,0} + m_{1,30} = 1$
s_{74}	$a_{12,26}$	$m_{12,31} = 0$
s_{73}	$a_{13,30}$	$m_{12,30} = 0$
s_{72}	$a_{13,29}$	$m_{12,29} = 1$
s_{71}	$a_{8,8}$	$m_{12,6} = 1$
s_{70}	$a_{13,5}$	$m_{12,5} + m_{7,2} + m_{6,2} + m_{5,2} + m_{4,5} + m_{4,4} + m_{2,5} + m_{2,3} + m_{2,2} + m_{2,1} + m_{1,30} + m_{1,0} = 1$
s_{69}	$a_{13,4}$	$m_{12,4} + m_{4,4} = 0$
s_{68}	$a_{13,3}$	$m_{12,3}+m_{7,3}+m_{7,2}+m_{6,3}+m_{5,3}+m_{5,2}+m_{5,1}+m_{4,3}+m_{3,2}+m_{2,2}+m_{2,1}+m_{1,1}+m_{0,4} = 0$
s_{67}	$a_{12,28} \cdot a_{4,2}$	$m_{12,2} + m_{7,3} + m_{6,3} + m_{5,3} + m_{4,3} + m_{3,2} + m_{2,2} + m_{1,3} + m_{1,2} + m_{1,0} + m_{0,4} = 1$
s_{66}	$a_{13,1}$	$m_{12,1} = 1$
s_{65}	$a_{13,0}$	$m_{12,0} = 1$
s_{64}	$a_{12,31}$	$m_{11,31} = 0$
s_{63}	$a_{12,30}$	$m_{11,30} = 0$
s_{62}	$a_{12,29}$	$m_{11,29} = 1$
s_{61}	$a_{7,8}$	$m_{11,6} = 1$
s_{60}	$a_{12,5}$	$m_{11,5} + m_{8,4} + m_{3,4} = 0$
s_{59}	$a_{12,4}$	$m_{11,4} + m_{7,3} + m_{7,2} + m_{7,0} + m_{6,5} + m_{6,3} + m_{5,3} + m_{5,2} + m_{5,1} + m_{4,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{2,1} + m_{1,3} + m_{1,2} + m_{1,1} + m_{0,3} + m_{0,2} = 1$
s_{58}	$a_{12,3}$	$m_{11,3} + m_{7,0} + m_{1,30} = 0$

Table 11. Control bits and controlled relations for the full SHA-1 (III)

ctrl. seq.	control bits	controlled relation
s_{57}	$a_{12,2}$	$m_{11,2} + m_{8,2} + m_{7,3} + m_{7,2} + m_{7,0} + m_{5,5} + m_{5,4} + m_{5,2} + m_{4,2} + m_{3,4} + m_{3,2} + m_{2,4} + m_{1,30} + m_{1,2} + m_{0,4} + m_{0,2} = 1$
s_{56}	$a_{11,28}$	$m_{11,1} = 1$
s_{55}	$a_{12,0}$	$m_{11,0} + m_{1,30} = 1$
s_{54}	$a_{10,26}$	$m_{10,31} = 1$
s_{53}	$a_{10,25}$	$m_{10,30} = 0$
s_{52}	$a_{10,24}$	$m_{10,29} = 0$
s_{51}	$a_{6,8}$	$m_{10,6} = 0$
s_{50}	$a_{11,5}$	$m_{10,5} + m_{4,5} + m_{2,5} = 1$
s_{49}	$a_{11,4}$	$m_{10,4} + m_{7,3} + m_{6,5} + m_{6,3} + m_{6,2} + m_{5,4} + m_{5,3} + m_{5,2} + m_{4,2} + m_{3,2} + m_{2,5} + m_{2,4} + m_{1,3} + m_{1,1} + m_{1,0} + m_{0,3} = 1$
s_{48}	$a_{6,1}$	$m_{10,3} + m_{7,3} + m_{7,0} + m_{6,5} + m_{5,5} + m_{5,4} + m_{5,3} + m_{5,1} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,2} + m_{2,1} + m_{1,30} + m_{1,1} + m_{0,3} = 0$
s_{47}	$a_{11,2}$	$m_{10,2} + m_{7,3} + m_{7,0} + m_{6,5} + m_{6,3} + m_{6,2} + m_{5,5} + m_{5,3} + m_{3,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{1,30} + m_{1,3} + m_{1,1} + m_{0,4} + m_{0,3} + m_{0,2} = 0$
s_{46}	$a_{11,1}$	$m_{10,1} = 1$
s_{45}	$a_{11,0}$	$m_{10,0} = 0$
s_{44}	$a_{10,31}$	$m_{9,31} = 1$
s_{43}	$a_{10,28}$	$m_{9,29} = 0$
s_{42}	$a_{10,5}$	$m_{9,5} = 0$
s_{41}	$a_{10,4}$	$m_{9,4} = 0$
s_{40}	$a_{3,4}, a_{3,5}$	$m_{9,3} + m_{8,2} + m_{7,3} + m_{7,0} + m_{6,5} + m_{6,3} + m_{6,2} + m_{5,5} + m_{5,4} + m_{5,2} + m_{4,2} + m_{2,5} + m_{2,4} + m_{2,3} + m_{2,1} + m_{1,3} + m_{1,2} + m_{1,1} + m_{1,0} + m_{0,4} + m_{0,3} + m_{0,2} = 0$
s_{39}	$a_{10,2}$	$m_{9,2} + m_{8,2} + m_{6,5} + m_{6,3} + m_{5,4} + m_{5,3} + m_{5,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{2,1} + m_{1,30} + m_{1,3} + m_{1,2} + m_{1,1} + m_{0,4} + m_{0,3} = 0$
s_{38}	$a_{9,28}$	$m_{9,1} = 1$
s_{37}	$a_{10,0}$	$m_{9,0} = 0$
s_{36}	$a_{8,26}$	$m_{8,31} = 0$
s_{35}	$a_{9,29}$	$m_{8,29} = 1$
s_{34}	$a_{8,0}$	$m_{8,3} + m_{7,3} + m_{7,2} + m_{7,0} + m_{6,3} + m_{5,4} + m_{5,3} + m_{3,4} + m_{3,2} + m_{2,4} + m_{2,3} + m_{2,1} + m_{1,30} + m_{1,3} + m_{0,2} = 0$
s_{33}	$a_{6,3}, a_{1,5}$	$m_{8,1} + m_{7,3} + m_{6,5} + m_{6,3} + m_{5,3} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{1,3} + m_{1,1} + m_{0,4} + m_{0,3} + m_{0,2} = 0$
s_{32}	$a_{8,27}$	$m_{8,0} = 0$
s_{31}	$a_{8,31}$	$m_{7,31} = 0$
s_{30}	$a_{8,28}$	$m_{7,28} = 0$
s_{29}	$a_{8,5}$	$m_{7,5} = 1$
s_{28}	$a_{8,4}$	$m_{7,4} + m_{7,2} + m_{5,4} + m_{5,3} + m_{5,2} + m_{3,2} + m_{2,2} + m_{0,4} = 1$
s_{27}	$a_{3,25}$	$m_{7,1} = 1$
s_{26}	$a_{7,31}$	$m_{6,31} = 0$
s_{25}	$a_{7,30}$	$m_{6,30} = 0$
s_{24}	$a_{2,31}$	$m_{6,29} = 0$
s_{23}	$a_{7,28}$	$m_{6,28} = 0$
s_{22}	$a_{7,6}$	$m_{6,6} = 0$
s_{21}	$a_{7,4}$	$m_{6,4} = 1$
s_{20}	$a_{5,25}$	$m_{5,31} = 0$
s_{19}	$a_{6,30}$	$m_{5,30} = 0$
s_{18}	$a_{5,23}$	$m_{5,28} = 1$
s_{17}	$a_{6,6}$	$m_{5,6} = 1$
s_{16}	$a_{6,0}$	$m_{5,0} + m_{1,30} + m_{1,0} = 0$
s_{15}	$a_{4,26}$	$m_{4,31} = 0$
s_{14}	$a_{5,30}$	$m_{4,30} = 0$
s_{13}	$a_{4,23}$	$m_{4,29} = 0$
s_{12}	$a_{3,26}$	$m_{3,31} = 1$
s_{11}	$a_{4,30}$	$m_{3,30} = 0$
s_{10}	$a_{3,24}$	$m_{3,29} = 1$
s_{9}	$a_{4,4}, a_{1,7}$	$m_{3,5} = 1$
s_{8}	$a_{4,3}$	$m_{3,3} = 1$
s_{7}	$a_{1,27}$	$m_{3,0} + m_{1,0} = 0$
s_{6}	$a_{2,26}$	$m_{2,31} = 1$
s_{5}	$a_{2,25}$	$m_{2,30} = 0$
s_{4}	$a_{1,25}$	$m_{2,0} + m_{1,30} = 1$
s_{3}	$a_{2,5}$	$m_{1,5} = 0$
s_{2}	$a_{1,26}$	$m_{1,31} + m_{1,30} = 1$
s_{1}	$a_{1,23}$	$m_{1,29} = 0$

Table 12. Control bits and controlled relations for the full SHA-1 (IV)

message variable	31 - 24	23 - 16	15 - 8	8 - 0
m_0	1-1-----	--------	--------	------10
m_1	L-0-----	--------	--------	--01----
m_2	L00-----	--------	--------	-------L
m_3	101-----	--------	--------	--1-1-1L
m_4	LL0-----	--------	--------	-0----01
m_5	0L01----	--------	--------	-1-----L
m_6	00L0----	--------	--------	-0-1--01
m_7	00-0----	--------	--------	--1L--1-
m_8	L-1-----	--------	--------	----L--L
m_9	L10-----	--------	--------	--00-L1L
m_{10}	L00-----	--------	--------	-0LLL10
m_{11}	LL1-----	--------	--------	-1LLLLL
m_{12}	001-----	--------	--------	-1LLL-1L
m_{13}	L11LLLL	LLLLLLL	L-L-----	--LLL0L
m_{14}	1LLLLLL	LLLLLLL	L-LL----	--LLLL0
m_{15}	LLLLLLL	LLLLLLL	LL-L----	L-0LLLL
m_{16}	--------	--------	--------	------01
m_{17}	-1------	--------	--------	-1-1--0-
m_{18}	-1------	--------	--------	-1------
m_{19}	111-----	--------	--------	-1-1--0-
m_{20}	1-1-----	--------	--------	--------
m_{21}	0-------	--------	--------	-1------
m_{22}	--1-----	--------	--------	-------0
m_{23}	--1-----	--------	--------	-11-----
m_{24}	1-------	--------	--------	-------1
m_{25}	-1------	--------	--------	-1---1-
m_{26}	10------	--------	--------	-0----10
m_{27}	-1------	--------	--------	--1---0-
m_{28}	--------	--------	--------	------10
m_{29}	-0------	--------	--------	-0----0-
m_{30}	11------	--------	--------	-1----01
m_{31}	11------	--------	--------	--0---1-
m_{32}	--------	--------	--------	-------1
m_{33}	-0------	--------	--------	------0-
m_{34}	00------	--------	--------	-1----00
m_{35}	-0------	--------	--------	-11---1-
m_{36}	1-------	--------	--------	-------0
m_{37}	-1------	--------	--------	-0----0-
m_{38}	-0------	--------	--------	-1----1-
m_{39}	-1------	--------	--------	------0-
m_{40}	--------	--------	--------	------1-
m_{41}	--------	--------	--------	-0------
m_{42}	0-------	--------	--------	------0-
m_{43}	1-------	--------	--------	--------
m_{44}	0-------	--------	--------	------0-
m_{45}	0-------	--------	--------	-1------
m_{46}	--------	--------	--------	--------
m_{47}	0-------	--------	--------	-1------
m_{48}	0-------	--------	--------	--------
m_{49}	--------	--------	--------	-1------
m_{50}	0-------	--------	--------	--------
m_{51}	--------	--------	--------	-1------
m_{52}	1-------	--------	--------	------1-
m_{53}	--------	--------	--------	--------
m_{54}	1-------	--------	--------	--------
m_{55}	0-------	--------	--------	--------
m_{56}	--------	--------	--------	--------
m_{57}	--------	--------	--------	--------
m_{58}	--------	--------	--------	--------
m_{59}	--------	--------	--------	--------
m_{60}	--------	--------	--------	--------
m_{61}	--------	--------	--------	--------
m_{62}	--------	--------	--------	--------
m_{63}	--------	--------	--------	--------
m_{64}	--------	--------	--------	--------
m_{65}	--------	--------	--------	--------
m_{66}	--------	--------	--------	-----0--
m_{67}	--------	--------	--------	1-------
m_{68}	--------	--------	--------	-----0--
m_{69}	--------	--------	--------	----0--0
m_{70}	--------	--------	-------1	-------0
m_{71}	--------	--------	--------	----0--1
m_{72}	--------	--------	--------	---0--0-
m_{73}	--------	--------	------1-	------0-
m_{74}	--------	--------	--------	---00-1-
m_{75}	--------	--------	-------1	--1--0--
m_{76}	--------	--------	-----0--	----00--
m_{77}	--------	--------	--------	--1--10-
m_{78}	--------	--------	--------	-1--1-0-
m_{79}	--------	--------	----0---	----0-1-
m_{80}	--------	--------	--------	--------

chaining variable	31 - 24	23 - 16	15 - 8	8 - 0
a_0	01100111	01000101	00100011	00000001
a_1	010-FrF0	y0-01-0-	10-0-10-	F-Fa0101
a_2	F100-Vv1	0aai0a1a	01a1a011	1-wa11a1
a_3	0101iVFV	-1000000	00000000	01FFa0a1
a_4	0w101v-a	y--10000	00101000	010XWF10
a_5	0w0101y1	V1-11110	00111-00	10010100
a_6	1w0a1a0a	a0a1aaa-	--10010F	-W01F0Fh
a_7	ww0w0111	11111111	111-010F	0w0W0110
a_8	w10wvv01	11110000	010-111F	1-Wh000F
a_9	00WV--11	11111111	111----0	---F1F01
a_{10}	W11x-Vvv	--------	-----a--	-1ww1h0w
a_{11}	100V----	--------	-------1	-1hh0hWw
a_{12}	wwWF-v--	--------	--------	-1hhhh0h
a_{13}	0wW--V--	-F-F-F--	FNqNqqqq	q1hhh0WW
a_{14}	1WWhhhhh	hhhhhhhh	hNhNqNNq	NNhhh1wh
a_{15}	WWwhhhhh	hhhhhhhh	hqhhqqqq	qNwh0hh0
a_{16}	w1Whhhhh	hhhhhhhh	hhNhqqqq	hqwh1hAh
a_{17}	00------	--------	--------	----0-0-
a_{18}	1-1-----	--------	--------	----a-0-
a_{19}	0-b-----	--------	--------	------0-
a_{20}	--0-----	--------	--------	----a---
a_{21}	--b-----	--------	--------	------0-
a_{22}	--------	--------	--------	----aa--
a_{23}	--------	--------	--------	------00
a_{24}	-c------	--------	--------	----a---
a_{25}	-B------	--------	--------	----a-0-
a_{26}	--------	--------	--------	-----A1-
a_{27}	--------	--------	--------	-------0
a_{28}	-C------	--------	--------	----a---
a_{29}	-b------	--------	--------	----a-1-
a_{30}	--------	--------	--------	-----A0-
a_{31}	--------	--------	--------	-------1
a_{32}	-c------	--------	--------	--------
a_{33}	-b------	--------	--------	----a---
a_{34}	--------	--------	--------	----AA0-
a_{35}	--------	--------	--------	------00
a_{36}	-c------	--------	--------	----A---
a_{37}	-B------	--------	--------	----A-1-
a_{38}	--------	--------	--------	------0-
a_{39}	--------	--------	--------	--------
a_{40}	B-------	--------	--------	----A---
a_{41}	--------	--------	--------	------1-
a_{42}	C-------	--------	--------	--------
a_{43}	B-------	--------	--------	--------
a_{44}	--------	--------	--------	----A---
a_{45}	--------	--------	--------	------0-
a_{46}	C-------	--------	--------	----A---
a_{47}	B-------	--------	--------	------0-
a_{48}	C-------	--------	--------	----A---
a_{49}	B-------	--------	--------	------0-
a_{50}	C-------	--------	--------	----A---
a_{51}	B-------	--------	--------	------0-
a_{52}	C-------	--------	--------	--------
a_{53}	B-------	--------	--------	--------
a_{54}	--------	--------	--------	--------
a_{55}	--------	--------	--------	--------
a_{56}	--------	--------	--------	--------
a_{57}	--------	--------	--------	--------
a_{58}	--------	--------	--------	--------
a_{59}	--------	--------	--------	--------
a_{60}	--------	--------	--------	--------
a_{61}	--------	--------	--------	--------
a_{62}	--------	--------	--------	--------
a_{63}	--------	--------	--------	--------
a_{64}	--------	--------	--------	--------
a_{65}	--------	--------	--------	--------
a_{66}	--------	--------	--------	---A----
a_{67}	--------	--------	--------	-----0--
a_{68}	--------	--------	--------	-------C
a_{69}	--------	--------	--------	--A----B
a_{70}	--------	--------	--------	----0---
a_{71}	--------	--------	--------	------C-
a_{72}	--------	--------	--------	-A----B-
a_{73}	--------	--------	--------	---0----
a_{74}	--------	--------	--------	--A--C--
a_{75}	--------	--------	--------	A---0B--
a_{76}	--------	--------	--------	--1---C-
a_{77}	--------	--------	--------	----C-B-
a_{78}	--------	--------	--------	----b---
a_{79}	--------	--------	--------	-1------
a_{80}	--------	--------	--------	--------

Table 13. Advanced sufficient conditions on $\{m_{i,j}\}$ and $\{a_{i,j}\}$ with semi-neutral bits for the full SHA-1

modified message in Step 4 pass the final test of Step 4 is $1/2^{54}$. Hence when we use Algorithm 2, we have the complexity to find a collision for the full SHA-1 is 2^{54} message modifications experimentally, because Step 4 is a dominant part of the algorithm. As stated in [9], we can relax 3 conditions from the above remaining conditions. Hence the total complexity is reduced to 2^{51} message modification, though symbolic computations are very slow at this moment.

8.5 An example of a partial result of Algorithm 2.

We show an example of a message $m = (m_0, m_1, \ldots, m_{15})$ obtained by Algorithm 2.

$$m = aa740c82\ 9f91e819\ 84c3e50f\ a898306b\ 1e5b4111\ 1867d96b\ 0616ea95\ 014a2f32$$
$$7ae92980\ d5e4d6c6\ 9d49d0ba\ 3b8087d3\ 32717277\ edcec899\ dc537498\ 63bca615$$

The above m satisfies all message conditions of 0-80 rounds and all chaining variable conditions of 0-28 rounds.

9 A concluding note

This paper yields an improved method for cryptanalysis of SHA-1 which originates from an explanation of the mathematical basis for Wang's attack and its improvement. We provide the detailed procedures which are based on a novel message modification technique. The proposed method improves the complexity of an attack against 58-round SHA-1 and we found many new collisions. Moreover, the complexity of the first iteration in a two-iteration attack against the full SHA-1 is reduced from 2^{62} message modification to 2^{51}.

References

1. E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, W. Jalby, "Collisions of SHA-0 and Reduced SHA-1" EUROCRYPT 2005, 36-57.
2. E. Biham, R. Chen, "Near-Collisions of SHA-0", CRYPTO 2004, 290-305.
3. F. Chabaud, A. Joux, "Differential Collisions in SHA-0", CRYPTO 1998, 56-71.
4. H. Dobbertin, "Cryptanalysis of MD4", Fast Software Encryption 1996, 53-69.
5. L. C. K. Hui, X. Wang, K. P. Chow, W. W. Tsang, C. F. Chong, H. W. Chan, "The Differential Analysis of Skipjack Variants from the first Round", Advance in Cryptography–CHINACRYPT2002, Science Publishing House.
6. A. Joux, "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions", CRYPTO 2004, 306-316.
7. X. Wang, X. Lai, D. Feng, H. Chen, X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD", EUROCRYPT 2005, 1-18.
8. X. Wang, D. Feng, X. Yu, "An Attack on Hash Function HAVAL-128", Science in China Series F **48**(2005), 545-556.
9. X. Wang, A. C. Yao, F. Yao, "Cryptanalysis on SHA-1", Proceedings of Cryptographic Hash Workshop, 2005,
10. X. Wang, Y. L. Yin, H. Yu, "New Collision Search for SHA-1", CRYPTO 2005, in Rump Session Presentation by Adi Shamir's "Recent Progress on SHA-1",
11. X. Wang, Y. L. Yin, H. Yu, "Finding Collisions in the Full SHA-1", CRYPTO 2005, 17-36.
12. X. Wang, H. Yu, "How to Break MD5 and Other Hash Functions", EUROCRYPT 2005, 19-35.
13. X. Wang, H. Yu, Y. L. Yin, "Efficient Collision Search Attacks on SHA-0", CRYPTO2005, 1-16.
14. X. Wang, "The Collision attack on SHA-0", 1997.
15. X. Wang, "The Improved Collision attack on SHA-0", 1998.
16. X. Wang, "Collisions for Some Hash Functions MD4, MD5, HAVAL-128, RIPEMD", Rump Session in Crypto'04, E-print.
17. X. Wang, "Cryptanalysis of Hash Functions and Potential Dangers", RSA Conference 2006, San Jose, USA,

Appendix: How to find good message differential with low hamming weight? - Our strategy

As we stated in Section 2, a choice of "differential" is very important. Here we show how to find good "differential'.

Our strategy is as follows.

- Find a message differential in which difference appears only on continuing 4-bits. There are a few message differential patterns which have values only on 3- or 4- bits.
- Find another message-differentials of continuing 4-bit by shifting the one obtained in the previous step.
- Substitute message-differentials into each round and combine them (adding a disturbance vector) and obtain a 'better' message differential.

If we start from Wang's message-differential with continuing 4-bit, we have the results as in Fig. **??**, Fig. **??**. By our experiments, Wang's disturbance vector for 58-round SHA-1 seems a best possible one.

i	$\Delta^+ m$	$\Delta^- m$	i	$\Delta^+ m$	$\Delta^- m$	i	$\Delta^+ m$	$\Delta^- m$
0	20000000	0	20	0	3	40	0	80000000
1	40000020	20000012	21	40000040	2	41	0	40
2	20000000	40000043	22	80000041	40000002	42	0	80000000
3	20000000	40	23	2	c0000020	43	0	40
4	e0000040	2	24	1	0	44	0	80000002
5	0	60000002	25	0	40000002	45	0	0
6	80000001	0	26	40000041	80000002	46	0	80000000
7	0	20	27	42	40000020	47	80000000	0
8	3	0	28	1	80000000	48	0	0
9	40000040	12	29	2	40000040	49	0	0
10	40000040	0	30	40000002	40	50	0	0
11	40000000	a0000052	31	2	40000000	51	0	0
12	0	a0000000	32	0	2	52	0	0
13	80000040	0	33	40	0	53	0	0
14	20000001	0	34	80000000	2	54	0	0
15	20000000	60	35	80000000	0	55	0	0
16	80000001	0	36	0	80000002	56	0	0
17	40000002	40	37	40	80000000	57	0	0
18	c0000002	41	38	0	0			
19	40000000	22	39	80000000	40			

Table. A message-differential for 58-round SHA-1 of continuous 4-round

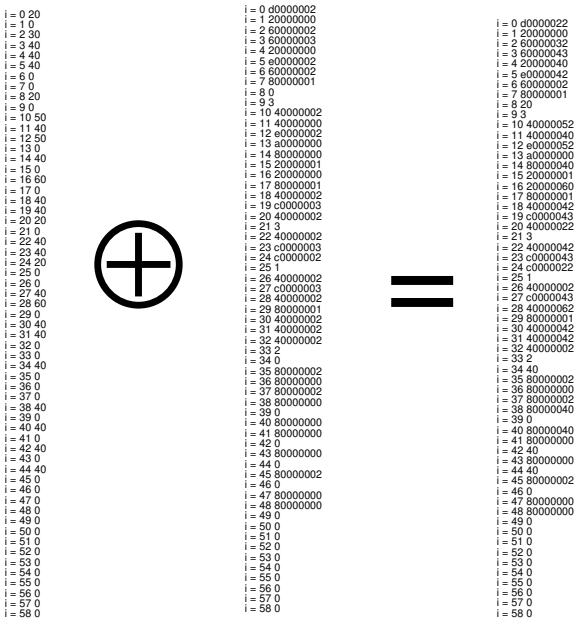

Fig. 1. Finding good disturbance vector (I)

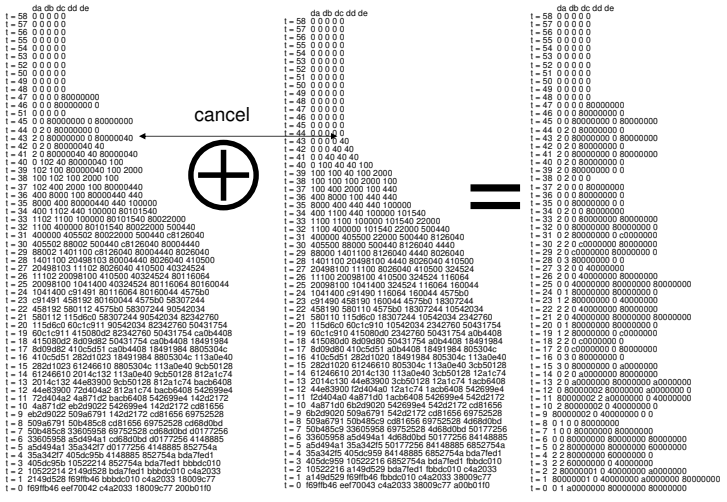

Fig. 2. Finding good disturbance vector (II)