## Gröbner Basis Based Cryptanalysis of SHA-1

Makoto Sugita \* Mitsuru Kawazoe <sup>†</sup> Hideki Imai <sup>‡</sup>

**Abstract**— Recently, Wang proposed a new method to cryptanalyze SHA-1 and found collisions of 58-round SHA-1. However many details of Wang's attack are still unpublished, especially, 1) How to find differential paths? 2) How to modify messages properly? For the first issue, some results have already been reported. In our article, we clarify the second issue and give a sophisticated method based on Gröbner basis techniques. We propose two algorithm based on the basic and an improved message modification techniques respectively. The complexity of our algorithm to find a collision for 58-round SHA-1 based on the basic message modification is  $2^{29}$  message modifications and its implementation is equivalent to  $2^{31}$  SHA-1 computation experimentally, whereas Wang's method needs  $2^{34}$  SHA-1 computation. The proposed improved message modification is applied to construct a more sophisticated algorithm to find a collision. The complexity to find a collision for 58-round SHA-1 based on this improved message modification technique is  $2^{8}$  message modifications, but our latest implementation is very slow, equivalent to  $2^{31}$  SHA-1 computation experimentally. However we conjecture that our algorithm can be improved by techniques of error correcting code and Gröbner basis. By using our methods, we have found many collisions for 58-round SHA-1.

Keywords: hash function, SHA-1, Gaussian elimination, Gröbner basis

## 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 [1] has found semi-free start collision of MD5. Later on, Wang [5], [6] has proposed collision attack on SHA-0 whose complexity was estimated to be as  $2^{45}$  SHA-0 computation. Chabaud-Joux [12] independently found 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 reduced SHA-1 have been reported in [10], [11], [9].

Employing the modular differential attack and message modification technique, Wang [4] has found collisions for the following hash functions MD4, MD5, HAVAL-128, RIPEMD, and in [7], [8], 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 [14] and [15], efficient collision search attacks against SHA-0 and 58-round SHA-1 have been reported as well as a complexity evaluation against full SHA-1 claimed to be  $2^{69}$  SHA-1 computation and in the improved approach to be  $2^{63}$ .

In this article, we give a sophisticated method to analyze 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 of boolean functions and to consider message modifications as error-correcting procedures for non-linear codes. For 58-round SHA-1, the complexity of our algorithm using only a basic message modification technique to find a collision is  $2^{29}$  message modifications (equivalent

<sup>\*</sup> IT Security Center, Information-technology Promotion Agency, Japan, 2-28-8 Honkomagome, Bunkyoku Tokyo, 113-6591, Japan, m-sugita@ipa.go.jp

<sup>&</sup>lt;sup>†</sup> 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

<sup>&</sup>lt;sup>‡</sup> 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

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

Table 1: Definition of function  $f_i$ 

to  $2^{31}$  SHA-1 computation experimentally), whereas Wang's method needs  $2^{34}$  SHA-1 computation. We propose an improved algorithm using improved message modification whose complexity to find a collision for 58-round SHA-1 is  $2^8$  message modifications, but our latest implementation is very slow, equivalent to  $2^{31}$ SHA-1 computation experimentally. However we conjecture that our algorithm can be improved by techniques of error correcting code and Gröbner basis. By using our methods, we have found many collisions for 58-round SHA-1 which are different from Wang's result.

# 2 Description of SHA-1 and Wang's analysis

## 2.1 SHA-1 algorithm

The hash function SHA-1 generates 160bit hash result from message of length less than  $2^{64}$  bits. It has Merkle/Damgard structure like other hash functions, and has 160-bit chaining value and 512-bit message block, and initial chaining values (IV) are fixed. From 512-bit block of the padded message, SHA-1 divides it into  $16 \times 32$ -bit words  $(m_0, m_1, \dots, m_{15})$ 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  $i = 16, \dots, 79$ , where  $x \ll n$  denotes *n*-bit left rotation of *x*. Using expanded messages, for  $i = 0, 1, \dots, 79$ ,

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

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

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

#### 2.2 Wang's attack

Wang's attack is summarized as follows.

- Find disturbance vector with low Hamming weight (difference for subtractions modulo 2<sup>32</sup>).
- 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 full-round SHA-1, Wang's attack need to use two iteration. They found collision with two iteration, i.e. each message in the collision includes two message blocks (1024-bit). They gives a set of sufficient conditions so that the differential occurs. Use a message modification technique they greatly improve the collision probability. In [15], they claimed that complexity to find a collision of full-round SHA-1 is 2<sup>69</sup> and in CRYPTO'05 Rump Session, they claimed that they have improved complexity into  $2^{63}$ . In the Rump Session, they claimed that they found new collision path of SHA-1 and described strategies for 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. Message modification follow certain topological order coming from correlations among chaining variable conditions.

Despite they have proposed new method, many details are still unpublished. Not all information are published about their attack, especially, 1) How to find differential paths? 2) How to modify messages properly?

In our analysis, we shall clarify and improve the second issue in the above, and show the effectiveness of our approach via computer experiment.

## 3 Definition and Notation

We take a complete set of representatives of  $\mathbb{Z}/2^{32}\mathbb{Z}$  as  $\{0, 1, 2, \dots, 2^{32} - 1\}$ . So we identifies the ring  $\mathbb{Z}/2^{32}\mathbb{Z}$  as the set  $\{0, 1, 2, \dots, 2^{32} - 1\}$ . 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 identification mapping

 $\mathbb{F}_{2}^{32} \ni (x_{0}, x_{1}, \dots, x_{31}) \mapsto x_{0} 2^{31} + x_{1} 2^{30} + \dots + x_{30} 2^{1} + x_{31} 2^{0} \in \mathbb{Z}/2^{32}\mathbb{Z}.$ 

**Definition 1** Let  $m = (m_0, m_1, \ldots, m_{31}), m' = (m'_0, m'_1, \ldots, m'_{31})$  be vectors of  $\mathbb{F}_2^{32}$ . For a pair m and m', we define the following notation.

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

We define  $\Delta^{\pm}m_j$  by  $\Delta^{\pm}m_j = \Delta^+m_j \oplus \Delta^-m_j$ . Moreover, we define  $\Delta^+m = (\Delta^+m_0, \Delta^+m_1, \dots, \Delta^+m_{31}),$  $\Delta^-m = (\Delta^-m_0, \Delta^-m_1, \dots, \Delta^-m_{31})$ 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 without carry" 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 without carry".

Since a disturbance vector ignores the sign '±', 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 without carry 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 without carry.

**Definition 3** For a message space  $M = \mathbb{Z}/2^{32}\mathbb{Z}$ , we define function  $f: (M \times M) \to M: (x_1, x_2) \mapsto (x_1 - x_2)$  where we consider '-' as subtraction of  $\mathbb{Z}/2^{32}\mathbb{Z}$ . We define differential  $\delta M$  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  $\delta M$ .

We define operator + in  $\delta M$  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  $\delta m$  is very important. When  $\delta m$  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  $\delta M$  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 for SHA-1 is as follows.

1. Find disturbance vector with low Hamming weight from 21-round to final round (in Wang's example of SHA-1, 58 or 80round). 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 differential (difference for subtractions modulo  $2^{32}$ ) so that  $\delta a_{-4} (= \delta e_0 \ll 2), \ \delta a_{-3} (= \delta d_0 \ll 2), \ \delta a_{-2} (\delta c_0 \ll 2), \ \delta a_{-1} (= \delta b_0), \ \delta a_0$  is a local collision. We ignore carry effects here.
- Calculate sufficient conditions on {a<sub>i</sub>}<sub>i=0,1,...,20</sub> considering carry effect by our semi-automatic method.
- 4. Determine advanced sufficient conditions on  $m_i$  by the Gaussian elimination based method.
- 5. Determine our *advanced sufficient conditions*. (Obtained conditions are essentially Wang's sufficient conditions combined with information for message modification technique.)
- 6. Generate a message randomly, and modify it using 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 errorcorrecting for non-linear codes. The method of Step 1 and 2 is based on the essentially same idea of Wang's attack. So we omit the details of Step 1 and 2 and only describe steps after from Step 3.

## 4.1 Sufficient conditions for collisions

For a given disturbance vector (or a given differential without carry) 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 without carry.

## 4.2 How to calculate sufficient conditions on $a_i$ ?

In this step, we may only consider expanded messages by ignoring relations arising from 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. Although it is difficult to calculate full-automatically, our method is semiautomatic one.

## 4.3 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 0-58round by relations of 0-15-round using the Gaussian elimination. Here all relations are considered as equations over  $\mathbb{F}_2$  and an elimination order of  $\{m_{i,j}\}_{i=0,1,\dots,15;j=0,1,\dots,31}$  is given by

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

Execute the Gaussian elimination for the system of equations which consists of all conditions on 0 - 58 round, we obtain a 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 transformation between them is not so complicated.

Experimentally, the best choice of the order is combination of these two orders. Hereafter, we adopt the order of  $\{a_{i,j}\}$  when i =0, 1, 15, 16, and the order of  $\{m_{i,j}\}$  when 1 < i < 15. By using the Gaussian elimination with this order, we reduced a system of equations consists of original sufficient conditions to a reduced row echelon form. Then in spite of original sufficient conditions, we use the obtained system of equations in 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" defined in the next section to original sufficient conditions.

# 4.4 Message modification techniques of $m_i$

In our procedure we use technique of modifying  $\{a_{i,j}\}$  instead of  $\{m_{i,j}\}$ . We note that in [6] and [5], this technique has been explained but not in detail.

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

To find a collision, we start from a random message and then modify it to satisfy sufficient conditions. Message modification technique is used to find a collision for the first 23 rounds.

First we compile a list of controlled relations and control bits associated to first 23rounds. The set of controlled relations consists of advanced sufficient conditions containing  $\{m_{i,j}\}$  and  $\{a_{i,j}\}$ , (i = 0, 1, ..., 15; j = 0, 1, ..., 31). 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 message modification is given as follows.

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

- 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 modified message yields collision or not. If it does not generate collision, return to Step 2. If it generates collision, finish.

The most important issue is that changing the control bit  $a_{i,j}$  may effect 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 the proposed method, we can 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 23 rounds hold.

As we show later, Algorithm 1 improves the complexity of attack on 58-round SHA-1 comparing to Wang's method, but we need further improvement. In the following sections, we propose a more effective algorithm.

## 4.5 Neutral bit, semi-neutral bit and adjuster

By using semi-neutral bits defined below, we can make Algorithm 1 more efficient.

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*.

### 4.6 Improved algorithm 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) *Procedures for message:* 

- 1. Generate  $(a_1, a_2, \cdots, a_{16})$  randomly.
- Using the basic message modification described in Algorithm 1, modify (a<sub>1</sub>, a<sub>2</sub>, ..., a<sub>16</sub>) so that all message conditions and some chaining variable conditions from the 17-th round to the 23-rd round hold. If this step fails, return to Step 1.
- 3. If remaining changing variable conditions from the 17-th round to the 23-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 modify chaining variables using our control sequence, and check whether chaining variable conditions from the 24-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 17-23, there are uncontrolled relations. In the case of our experiment on 58-round SHA-1(see Section 6), there are 5 uncontrolled relations. So, in Algorithm 2, the probability that output of Step 2 pass the test in Step 3 is  $1/2^5$ .

(2) As we show in Section 6, in the case of our experiment on 58-round SHA-1, we use 21 semi-neutral bits and 16 adjusters.

The above proposed algorithm is based on our idea that message modification is analogous to error-correcting procedure for nonlinear codes. (See the next section for more details.) For Step 4 in Algorithm 2, we take a naive trial-and-error method in our latest implementation. We think that if we assemble a list of relations and their control bits for after the 23-rd round, and if we use more techniques from Gröbner basis and error-correcting codes, we can make our algorithm more effective.

## 5 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.

## 5.1 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 ( $58 \le n \le$ 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 R a quotient ring  $\mathbb{F}_2[\mathbf{X}]/J$ . Note that R 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 Ras  $f(\mathbf{X})$ .

For a randomly taken  $(a_1, a_2, \cdots, a_{16}) \in$  $(\mathbb{F}_2^{32})^{16}$ ,  $\mathbf{a} = \{a_{i,j}\}_{i=0,1,\dots,n; j=0,1,\dots,31}$  are determined. We associate this  $\mathbf{a}$  to the ideal in Rgenerated by  $\{X_{i,j} + a_{i,j}\}_{i=0,1,\dots,n;j=0,1,\dots,31}$ . controlled relations are polynomials in  $a_{i,j}$ 's and  $m_{i,j}$ 's. 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  $f({X_{i,j}}) = 0$  where  $f \in R$ . 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.

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  $R_2$  a quotient ring  $R/I_2$ . 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.

- 1. Set r = 0.
- 2. Generate  $(a_1, a_2, \cdots, a_{16}) \in (\mathbb{F}_2^{32})^{16}$  randomly.
- 3. Set i = 0.
- 4. Increment i until  $f_i \not\equiv 0 \mod I$ . If all  $f_i$  are contained in I, go to the final step. If r > M, give up and return to Step 2.
- 5. 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 go to Step 3.
- 6. Solve a system of equations  $\mathcal{T}$  in  $R_2$  by using Gröbner basis algorithm.
- 7. Check whether modified message yields collision or not. If it does not generate collision, return to Step 2. If it generates collision, finish.

We 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  $R_2$ .

## 5.2 Relation between message modification and decoding of error-correcting codes.

Let S be the set of all points in  $F = (\mathbb{F}_2^{32})^{16}$ 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 **a** is analogous to a decoding problem in error-correcting codes. Hence, a basic message modification and a proposed improved message modification including changing semi-neutral bits can be viewed as an errorcorrecting 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.

## 6 Analysis of 58-round SHA-1 based on our method

Now we show the effectiveness of our method by analyzing 58-round SHA-1.

## 6.1 Disturbance vector and Message differential pattern

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 differential without carry associated to the disturbance vector. Constructed one is the same one as Wang obtained in [15]. Explicit form of the differential without carry is as in Table 6.1.

We take  $\{(\Delta^+ m_i, \Delta^- m_i)\}_{i=0,1,2,\dots,57}$  as a message-differential. It is a message-differential without continuous 5-bits.

# 6.2 Sufficient conditions on $\{m_i\}$ and $\{a_i\}$

For the disturbance vector, the differential without carry and the message differential given in the previous step, we give sufficient conditions on 58-round SHA-1. Since it is not written in [15], conditions we give here in Table 3 is the first one which is written in an explicit form.

In Table 3, '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 rewrite all conditions on 0-57-round by 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.

 $m_{15,31} = 1, m_{15,30} = 1, m_{15,29} = 0, m_{15,28} +$ 

i	$\Delta^+ m_i$	$\Delta^{-}m_{i}$	$\Delta^+ a_i$	$\Delta^{-}a_{i}$
58	4	0	Ő	Ō
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
20	1	40000002	0	0
24	1	-0000020	1	0
20	80000041	40000020	1	2
22	40000041	40000002	0	2
20	40000040	2	0	0
10	4000000	22	1	0
18	c00000002	41	2	0
17	40000002	40	2	ő
16	80000001	0	ō	ő
15	20000000	60	1	ő
14	20000001	0	0	ŏ
13	80000040	õ	Ő	$\tilde{2}$
12	0	a0000000	0	0
11	40000000	a0000052	102	80000000
10	40000040	0	0	0
9	40000040	12	8003ff00	40002
8	3	0	1 fe 0000	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

2 1 0	20000000 40000020 20000000	$40000043 \\ 20000012 \\ 0$		60000002 20000000 0	
Table 2 carry c	2: $\{m_i\}$ a of 58-rour	and $\{a_i\}$ c nd SHA-1	of differen	tial with	out

message variable	31 - 24	23 - 16	15 - 8	8 - 0
<i>m</i> <sub>0</sub>	0			
m <sub>1</sub>	-01			-111
m2 m3	0			-1
m4	000			-01-
$m_5$	-11			1-
m <sub>6</sub>	0			0
m7 m2				00
m <sub>8</sub>	-0			-0-11-
m <sub>10</sub>	-0			-0
m <sub>11</sub>	101			-1-11-
$m_{12}$	1-1			
m <sub>13</sub>	0			0
m <sub>15</sub>	0			-11
$m_{16}$	0			0
$m_{17}$	-0			-10-
m18	00			-101
m19 m20	-0			11
m <sub>21</sub>	-0			-01-
m22	01			-010
$m_{23}$	11			10-
m24				0
m25	10			-010
m26	-1			-010-
m28	1			0
$m_{29}$	-1			-10-
m <sub>30</sub>	-0			-10-
<sup>111</sup> 31 max				1-
m32 m33				-0
m34	0			1-
$m_{35}$	0			
m <sub>36</sub>	1			1-
11137 m20	1			
m39	0			-1
m <sub>40</sub>	1			
m41				-1
m42	1			
11143 m 4 A	1			1-
m45				
$m_{46}$	1			
m47	0			
$m_i \ (i \ge 48)$				
1				
chaining variable	31 - 24	23 - 16	15 - 8	8 - 0
chaining variable a0	31 - 24 01100111	23 - 16 01000101	15 - 8 00100011	8 - 0 00000001
chaining variable <u>a_0</u> a_1	31 - 24 01100111 101	23 - 16 01000101	15 - 8 00100011	8 - 0 00000001 -1-a10aa
$\begin{array}{c} \text{chaining} \\ \text{variable} \\ \hline a_0 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \end{array}$	31 - 24 01100111 101 01100	23 - 16 01000101 0-	15 - 8 00100011 a	8 - 0 00000001 -1-a10aa 100010 0a-1a0-0
$\begin{array}{c} \text{chaining} \\ \text{variable} \\ \hline a_0 \\ a_1 \\ \hline a_2 \\ a_3 \\ a_4 \\ \end{array}$	<u>31 - 24</u> 01100111 101 01100 0010 11010	23 - 16 01000101 0- -101a -01	15 - 8 00100011 a 0- 01aaa	8 - 0 00000001 -1-a10aa 100010 0a-1a0-0 0-10-100
$\begin{array}{c} \text{chaining} \\ \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{array}$	31 - 24 01100111 101 01100 10010 10-01a	23 - 16 01000101 0- -101a -01 -1-01-aa	15 - 8 00100011 a 0- 01aaa 00100-	8 - 0 00000001 -1-a10aa 100010 0a-1a0-0 0-10-100 001-1
chaining variable a <sub>1</sub> a <sub>2</sub> a <sub>3</sub> a <sub>4</sub> a <sub>5</sub> a <sub>6</sub>	31 - 24 01100111 101 0010 11010 110-01a 110110	23 - 16 01000101 0- -101a -01 -1-01-aa -a-1001-	15 - 8 00100011 a 0- 01aaa 00100- 01100010	8 - 0 00000001 -1-a10aa 100010 0a-1a0-0 0-10-100 001-1 1-a111-1
chaining variable a <sub>1</sub> a <sub>2</sub> a <sub>3</sub> a <sub>4</sub> a <sub>5</sub> a <sub>6</sub> a <sub>7</sub>	31 - 24 01100111 101 01100 0010 11010 110-01a 110110 -11110 -0.12	23 - 16 01000101 0- -101a -01 -1-01-aa -a-1001- a1a1111- 0000000	15 - 8 00100011 a 01aa 01100- 01100010 -101-001 2001-1	8 - 0 00000001 -1-a10aa 100010 0a-1a0-0 0-10-100 001-1 1-a111-1 10-10 100.0
$\begin{array}{c} \text{chaining} \\ \text{auriable} \\ \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\$	31 - 24 01100111 101 01100 10010 110-01a 110110 -11110 -010 000	23 - 16 01000101 0- -101a -01 -1-01-aa -a-1001- a1a1111- 0000000a 11000100	15 - 8 00100011 a 01aaa 00100- 01100010 -101-001 a001a1 00000000	$\frac{8 - 0}{0000001}$ -1-a10aa 100010 0a-1a0-0 0-10-100 001-1 1-a111-1 10-10 100-0-1- 101-1-1-
$\begin{array}{c} \text{chaining}\\ a_0\\ a_0\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\\ a_8\\ a_9\\ a_{10}\\ \end{array}$	31 - 24 01100111 101 01100 11010 110-01a 110110 -1110 00 0-1	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011	15 - 8 00100011  	$\begin{array}{r} 8 & - & 0 \\ 00000001 \\ -1 - a 10aa \\ 100010 \\ 0a - 1a0 - 0 \\ 0 - 10 - 100 \\ 0 01 - 1 \\ 1 - a 111 - 1 \\ 1 0 - 10 \\ 100 - 0 - 1 \\ 101 - 1 - 1 \\ 00 0 - 1 \end{array}$
chaining variable a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 a10 a11	31 - 24 01100111 101 0010 11010 11-01a 110110 -1110 00 0-1 1-0	23 - 16 01000101 0- -101a -01 a-a-1001- ata1111- 0000000a 11000100 11111011	15 - 8 00100011  01aa 00100- 01100010 -101-001 a001a1 00000000 11100000	8 - 0 0000001 -1-a10aa 100010 0a-1a0-0 0-10-100 00-11 1-a111-1 10-10 100-0-1- 101-1-1- 000-1- 110-
$\begin{array}{c} {\rm chaining} \\ {\rm a0} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \end{array}$	31 - 24 01100111 101 01100 11010 10-01a 110110 -1110 000 0-1 0-1 0-1	23 - 16 01000101 0 -101a -01 -1-01-aa -a-1001- ala1111- 000000a 11000100 11111011 1	15 - 8 00100011 0- 01aa -00100- 01100010 -101-001 a001a1 00000000 11100000 01111110 	8 - 0 0000001 -1-a10aa 100010 0a-1a0-0 0-10-100 001-1 1a111-1 10-10 100-0-1- 101-1-1- 000-1- 110- -1a
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{$	31 - 24 01100111 101 0010 11010 10-01a 110110 -1110 00 0-1 0-1 1-0 1-0 1-0 1-0 1-0	23 - 16 01000101 0- -101a -011 ala1111- 000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aa 0100- 01100010 -101-001 a001a1 00000000 11100000 0111110 	8 - 0 0000001 -1-a10aa 1-00010 0a-1a0-0 0-10-100 00-1-1 1a-111-1 10-10 101-1-1- 00-0-1- 110-1-1 110-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-
$\begin{array}{c} {\rm chaining} \\ {\rm a0} \\ {\rm a0} \\ {\rm a1} \\ {\rm a2} \\ {\rm a3} \\ {\rm a4} \\ {\rm a5} \\ {\rm a6} \\ {\rm a7} \\ {\rm a8} \\ {\rm a9} \\ {\rm a10} \\ {\rm a11} \\ {\rm a12} \\ {\rm a13} \\ {\rm a14} \\ {\rm a15} \end{array}$	31 - 24 01100111 101 01100 11010 110-01a 110110 -1110 0-1 0-1 1-0 1-0 1-0 1-0 0	23 - 16 01000101 0- -101a -01 ala1111- 000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 01111110 	$\begin{array}{c} 8 & - & 0 \\ 00000001 \\ -1-a10aa \\ 100010 \\ 0a-1a0-0 \\ 0-10-100 \\ 001-1 \\ 1-a111-1 \\ 10-10 \\ 100-0-1- \\ 101-1-1- \\ 000-1- \\ 110-1 \\ -1a \\ -101- \\ -11 \\ -10 \\00 \end{array}$
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a}_0 \\ {\rm a}_1 \\ {\rm a}_2 \\ {\rm a}_3 \\ {\rm a}_4 \\ {\rm a}_5 \\ {\rm a}_5 \\ {\rm a}_6 \\ {\rm a}_7 \\ {\rm a}_8 \\ {\rm a}_9 \\ {\rm a}_{10} \\ {\rm a}_{11} \\ {\rm a}_{12} \\ {\rm a}_{13} \\ {\rm a}_{14} \\ {\rm a}_{15} \\ {\rm a}_{16} \end{array}$	31 - 24 01100111 101 00100 110101 11-0110 -11110 -010 00 1-0 1-0 1-0 1-0 0-1 0 1-0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- a1a1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 01111110 	8 - 0 0000001 -1-a10aa 10010 0a-1a0-0 0-10-100 001-1 1-a111-1 100-0-1- 100-0-1- 110-1 -101- -101- -101- -101- -101- -101- -101- -101- -101- -101- 
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ \end{array}$	31 - 24 01100111 101 0010 11010 11-0110 -11110 -010 001 0-1 1-0 1 0-1 -1 -0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- aia1111- 0000000a 11000100 11111001 1 1 1 1 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110 	$\begin{array}{r} 8 & - & 0 \\ 00000001 \\ -1 - a10aa \\ 1 - 00010 \\ 0a-1a0-0 \\ 0-10-100 \\ 001-1 \\ 1 - a111-1 \\ 10-10 \\ 100-0-1- \\ 101-1-1- \\ 000-1- \\ 1101- \\ 1100-1 \\ -1a \\ -101- \\ -1a \\ -101- \\ -101- \\ -101- \\ -101- \\$
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{18$	31 - 24 01100111 101 0010 10-01a 110110 -11110 -00 0-1 1-0 1 0-1 0 0 0 1 0 1-1 1-1	23 - 16 01000101 0- -101a -011 -1-01-aa -a-1001- ata1111- 0000000a 11000100 11111011 1 1 1 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 0111100000 0111110 	8 - 0 0000001 -1-a10aa 100010 0a-1a0-0 0-10-100 001-1 1-a111-1 10-10 100-0-1- 101-1-1- 000-1- 110- -1a -100 -1
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a0} \\ {\rm a1} \\ {\rm a2} \\ {\rm a3} \\ {\rm a4} \\ {\rm a5} \\ {\rm a6} \\ {\rm a7} \\ {\rm a8} \\ {\rm a9} \\ {\rm a10} \\ {\rm a11} \\ {\rm a12} \\ {\rm a13} \\ {\rm a14} \\ {\rm a15} \\ {\rm a16} \\ {\rm a16} \\ {\rm a17} \\ {\rm a18} \\ {\rm a18} \\ {\rm a19} \\ {\rm a20} \end{array}$	31 - 24 01100111 101 01100 11010 110-01a 110110 -1110 0-1 0-1 1-0 1-0 0 -1 -1 	23 - 16 01000101 0- -1011a -011a -1-01-aa -a-1001- ala1111- 000000a 11000100 11111011 1 	15 - 8 00100011 	8 - 0 0000001 -1-a10aa 100010 0a-1a0-0 0-10-100 001-1 1a-111-1 100-0-1- 101-1-1- 000-1- 110-1 110-1 -1a -10 01 0 00- 
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ \end{array}$	31 - 24 01100111 101 00100 110101 110-01a 110110 -010 00 1-0 1-0 0-1 0 1-0 0 -1 0 -1 -0 -1  	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- aia1111- 0000000a 11000100 111111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           10100           000-1-           111           -101-           -101-           -101-          00-          00-          00-          00-          00-          01-          01-          01-          01-          10-          01-
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ \end{array}$	31 - 24 01100111 101 00100 110010 11-0110 -11110 -010 00 1-0 1-0 1-0 1 0-1 1-0 1-1 0-1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           101-11-1           100-0-1-           101-1-1-           1100-1           110-10           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-           -
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ & a_0 \\ & a_1 \\ & a_2 \\ & a_3 \\ & a_4 \\ & a_5 \\ & a_6 \\ & a_7 \\ & a_8 \\ & a_9 \\ & a_{10} \\ & a_{11} \\ & a_{13} \\ & a_{14} \\ & a_{15} \\ & a_{16} \\ & a_{17} \\ & a_{18} \\ & a_{19} \\ & a_{20} \\ & a_{22} \\ & a_{23} \\ \end{array}$	31 - 24 01100111 101 01100 10-01a 11-0110 -11110 -00 0-1 1-0 1-0 1-0 1-1 -0 1-1     	23 - 16 01000101 0- -101a -01 al-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110 01111110  	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1a111-1           10-10           101-1-1-           00-0-1-           110-1           1100           -1a           -1a           -100           -100          00          0          0          0          0          0          0          0          0
$\begin{array}{c} {\rm chaining} \\ {\rm a0} \\ {\rm a0} \\ {\rm a1} \\ {\rm a2} \\ {\rm a3} \\ {\rm a4} \\ {\rm a5} \\ {\rm a6} \\ {\rm a7} \\ {\rm a8} \\ {\rm a9} \\ {\rm a10} \\ {\rm a11} \\ {\rm a12} \\ {\rm a13} \\ {\rm a14} \\ {\rm a15} \\ {\rm a16} \\ {\rm a16} \\ {\rm a17} \\ {\rm a18} \\ {\rm a18} \\ {\rm a20} \\ {\rm a221} \\ {\rm a22} \\ {\rm a23} \\ {\rm a24} \\ {\rm acc} \end{array}$	31 - 24 01100111 101 01100 10-01a 110110 -010 00-1 1-0 1-0 1-0 1-0 1-0 -1 0 -1 -0	23 - 16 01000101 0- -101a -011a -1-01-aa -a-1001- a1a1111- 000000a 11000100 111111011 1 	15 - 8 00100011 a 01aaa -00100- 01100010 -101-001 a001a1 00000000 0111110  	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1a111-1           100-0-1-           101-10-10           000-1-           110-10           100-0-1-           101-11-           000-1-           110           -1a           -10                      0          0          0          0          0          0          0          0          0          0          0          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{26$	31 - 24         01100111         101         01100         110-010         0-10-010         0-1         1-0         1-0         0-1         1-0         1-0         0         1-0         0            0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- a1a111- 0000000a 11000100 11000100 11000100 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           10001-1           1111-           0001-1           -101-           -101-           -101-          01-          00-          00          01
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{22} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ \end{array}$	31 - 24         01100111         101         0010         110011         110011         110011         10-018         11-0110         -0         01         1-0         0-1         1-0         1-0         1-1         1-1         1-1         -0         1-1         -0         -0         -1         -0         -0         -0         -0         -0         -0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-11-           101-1-1-           1011-1           -101-           -101-           -101-           -101-           -101-           -101-          01-          01-          01-          01-          01-          01-          10          01-
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ = & a_0 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\ = & a_4 \\ = & a_5 \\ = & a_6 \\ = & a_7 \\ = & a_6 \\ = & a_7 \\ = & a_8 \\ = & a_9 \\ = & a_1 \\ = & a_2 \\$	31 - 24 01100111 101 01100 10-01a 11-0110 -11110 -00 0-1 1-0 1-0 0 -0 1-1     	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- aia1111- 0000000a 11000100 11111001 1 	15 - 8 00100011 0 01aaa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110  	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           101-1-1-           100-0-1-           101-1-1-           1011-           000-1-           110-0           -1a           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -11          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-          01-
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a0} \\ {\rm a1} \\ {\rm a2} \\ {\rm a3} \\ {\rm a4} \\ {\rm a5} \\ {\rm a6} \\ {\rm a7} \\ {\rm a8} \\ {\rm a9} \\ {\rm a10} \\ {\rm a11} \\ {\rm a12} \\ {\rm a13} \\ {\rm a14} \\ {\rm a15} \\ {\rm a16} \\ {\rm a16} \\ {\rm a17} \\ {\rm a18} \\ {\rm a19} \\ {\rm a20} \\ {\rm a21} \\ {\rm a22} \\$	31 - 24         01100111         101         01100         10-01a         10-01a         10-01a         10-01a         10-01a         10-01a         10-01a         10-0         0-1         1-0         0-1         1-0         1-0         1-1         0	23 - 16 01000101 0- -101a -011a -1-01-aa -a-1001- ala1111- 000000a 11000100 11111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1a111-1           100-0-1-           101-10-10           000-1-           110-0           -1a           -10-1           -10          0-0          0-0          00          00          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a}_{0} \\ {\rm a}_{1} \\ {\rm a}_{2} \\ {\rm a}_{3} \\ {\rm a}_{4} \\ {\rm a}_{5} \\ {\rm a}_{6} \\ {\rm a}_{7} \\ {\rm a}_{8} \\ {\rm a}_{9} \\ {\rm a}_{10} \\ {\rm a}_{11} \\ {\rm a}_{12} \\ {\rm a}_{13} \\ {\rm a}_{14} \\ {\rm a}_{15} \\ {\rm a}_{16} \\ {\rm a}_{17} \\ {\rm a}_{18} \\ {\rm a}_{19} \\ {\rm a}_{20} \\ {\rm a}_{21} \\ {\rm a}_{22} \\ {\rm a}_{22} \\ {\rm a}_{23} \\ {\rm a}_{24} \\ {\rm a}_{25} \\ {\rm a}_{26} \\ {\rm a}_{27} \\ {\rm a}_{28} \\ {\rm a}_{29} \\ {\rm a}_{30} \\ {\rm a}_{21} \\ {\rm a}_{29} \\ {\rm a}_{30} \\ {\rm a}_{21} \\ {\rm a}_{29} \\ {\rm a}_{30} \\ {\rm a}_{21} \\ {\rm a}_{29} \\ {\rm a}_{30} \\ {\rm a}_{21} \\ {\rm a}_{29} \\ {\rm a}_{30} \\ {\rm a}_{21} \\ {\rm a}_{30} \\ {\rm a}_{31} \\ {\rm a$	31 - 24         01100111         101         01100         110-101         110-0110         0-013         110110         -0         1-0         1-0         1-0         0         1-0         0         1-1	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- a1a111- 0000000a 11000100 111111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-10-0           -101           110-1           110-1           -101-           -101-           -101-           -101-          00          00          00          01           <
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{30} \\ a_{31} \\ a_{32} \\ \end{array}$	31 - 24         01100111         101         0010         11010         110-01a         11-0110         -0         1-0         1-0         1-0         1-0         1-0         1-0         0-1         0         1-0         0         0         0         0         0         0	23 - 16 01000101 0- -101a -011a 1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aaa 00100- 0110010 -101-001 a001a1 00000000 11100000 0111110 	8 - 0           00000001           -1-a10aa           100010           0a-1ao-0           0-10-100           00-01-1           1-a111-1           100-0-1-           1011-1           000-1-           110-10           -101-           -101-           -101-           -101-           -101-           -101-          0-0          0          0          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ = & a_0 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\ = & a_4 \\ = & a_5 \\ = & a_6 \\ = & a_7 \\ = & a_6 \\ = & a_7 \\ = & a_8 \\ = & a_9 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\$	31 - 24 01100111 101 01100 11010 110-01a 11-0110 -1110 0 1-0 1-0 0 1-0 1-0 0 -0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ata1111- 0000000a 11000100 11111001 1 	15 - 8 00100011 0- 01aaa 00100- 0110010 1-101-001 a001a1 00000000 11100000 0111110  	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           101-1-1-           100-0-1-           101-1-1-           1011-           000-1-           110-10           -1a           -101-           -101-           -100          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ = & a_0 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\ = & a_4 \\ = & a_5 \\ = & a_6 \\ = & a_7 \\ = & a_8 \\ = & a_9 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\$	31 - 24         01100111         101         01100         110-110         -0-11         0-1         0-1         1-0         0-1         0-1         1-0         0-1         0-1         0         0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 000000a 11000100 11000100 111111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-al0aa           100010           0-10-100           0-10-100           10011           1a111-1           100-0-1-           101-10-10           000-1-           110-10           1000-1-           110-1           -101-           -101-           -101-           -101-          0-0          0-0          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{31} \\ a_{32} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{35} \\ \end{array}$	31 - 24 01100111 101 01100 11010 11-0110 -11110 -00 1-0 1-0 1-0 0 1-0 0 1-0 0  0  	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11000100 11000100 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-10-0           000-1-           110-0           -101-           -101-           -101-          00          00          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{37} \\ a_{36} \\ a_{37} \\ a_{36} \\ a_{35} \\ a_{36} \\ a_{37} \\ a_{37$	31 - 24         01100111         101         0010         11010         110-01a         11-0110         -1         1-0         1-0         1-0         1-0         1-0         1-0         0         1-0         0         0         -1         0         -1         -1         -1         -1         -1         -1	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ata1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-1-1-           000-1-           110-0           -1a2           -10-1           -10-1           -10-1           -10-1           -10-1           -10-1          0-0          0          0          0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ = & a_0 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\ = & a_4 \\ = & a_5 \\ = & a_6 \\ = & a_7 \\ = & a_6 \\ = & a_7 \\ = & a_8 \\ = & a_9 \\ = & a_1 \\ = & a_2 \\$	31 - 24 01100111 101 01100 11010 110-01a 11-0110 -11110 -0 1-0 1-0 1-0 -0	23 - 16 01000101 0- -101a -011a -1-01-aa -a-1001- 11000000a 11000100 11000100 111111011 1 	15 - 8 00100011 	8 - 0           00000001           -1-al0aa           100010           0a-1a0-0           0-101-10           001-1           1a-111-1           100-0-1-           101-1-1-           0001-1           1100           -101           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-          0-          0-          0-
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a0} \\ {\rm a1} \\ {\rm a2} \\ {\rm a3} \\ {\rm a4} \\ {\rm a5} \\ {\rm a6} \\ {\rm a7} \\ {\rm a8} \\ {\rm a9} \\ {\rm a10} \\ {\rm a11} \\ {\rm a12} \\ {\rm a13} \\ {\rm a14} \\ {\rm a15} \\ {\rm a16} \\ {\rm a16} \\ {\rm a17} \\ {\rm a18} \\ {\rm a16} \\ {\rm a16} \\ {\rm a17} \\ {\rm a18} \\ {\rm a19} \\ {\rm a20} \\ {\rm a21} \\ {\rm a22} \\ {\rm a23} \\ {\rm a24} \\ {\rm a22} \\ {\rm a22} \\ {\rm a23} \\ {\rm a33} \\ {\rm a33} \\ {\rm a34} \\ {\rm a35} \\ {\rm a36} \\ {\rm a37} \\ {\rm a38} \\ {\rm a38} \\ {\rm a39} \\ \end{array}$	31 - 24         01100111         101         01100         110-110         0-013         11-0110         -0         0-1         1-0         1-0         0-1         0-1         1-0         0-1         1-0         1-1         0         -0	23 - 16 01000101 0- -101a -01	15 - 8           00100011          0-           01aa          00100-           01100010           a001a1           00000000           0111110	8 - 0           00000001           -1-al0aa           100010           0a-1a0-0           0-10-100           001-1           1a-111-1           100-0-1-           101-11-           0001-1           1100           -1a           -101-           -101-           -101-           -101-           -101-          0-0          0-0          0-0          0-0          0          0          0          0          0          0          0          0          0          0          0          0-          0-          0-          0-          1-          1-          1-          1-          1-          1-
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a}_0 \\ {\rm a}_1 \\ {\rm a}_2 \\ {\rm a}_3 \\ {\rm a}_4 \\ {\rm a}_5 \\ {\rm a}_5 \\ {\rm a}_6 \\ {\rm a}_7 \\ {\rm a}_8 \\ {\rm a}_9 \\ {\rm a}_{10} \\ {\rm a}_{11} \\ {\rm a}_{12} \\ {\rm a}_{13} \\ {\rm a}_{14} \\ {\rm a}_{15} \\ {\rm a}_{16} \\ {\rm a}_{17} \\ {\rm a}_{18} \\ {\rm a}_{19} \\ {\rm a}_{20} \\ {\rm a}_{21} \\ {\rm a}_{22} \\ {\rm a}_{23} \\ {\rm a}_{24} \\ {\rm a}_{25} \\ {\rm a}_{26} \\ {\rm a}_{27} \\ {\rm a}_{28} \\ {\rm a}_{29} \\ {\rm a}_{31} \\ {\rm a}_{32} \\ {\rm a}_{33} \\ {\rm a}_{39} \\ {\rm a}_{40} \end{array}$	31 - 24         01100111         101         01100         110-010         10-01a         11-0110         -00         1-00         1-00         0-10         1-00         1-00        0        0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11100110 1 	15 - 8 00100011 	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-1-1-           000-1-           1100           -101-           -101-           -101-          00          00          01
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{30} \\ a_{31} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{38} \\ a_{38} \\ a_{38} \\ a_{40} \\ a_{41} \\ a_{11} \\ a_{12} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{37} \\ a_{38} \\ a_{38} \\ a_{38} \\ a_{40} \\ a_{41} \\ a_{11} \\ a_{12} \\ a_{23} \\ a_{24} \\ a_{35} \\ a_{36} \\ a_{37} \\ a_{38} \\ a_{40} \\ a_{41} \\ a_{11} \\ a_{12} \\ a_{23} \\ a_{38} \\ a_{39} \\ a_{40} \\ a_{41} \\ a_{41$	31 - 24         01100111         101         0010         110011         110011         110011         10-01a         11-0110         -0         1-0         1-0         1-0         1-0         1-0         1-0         1-1	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- a1a1111- 0000000a 11000100 11111011 1 	15 - 8           00100011          0           01aa          00100-           0110010           -101-001           a001a1           00000000           11100000           01111110	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-1           000-1-           110-0          0-1           -10-1           -10-1           -10-1          0-0          0-0          1          1          1          1          1          1          1          1          1
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ = & a_0 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\ = & a_4 \\ = & a_5 \\ = & a_6 \\ = & a_7 \\ = & a_8 \\ = & a_9 \\ = & a_1 \\ = & a_2 \\ = & a_3 \\$	31 - 24         01100111         101         0100         11010         11010         10-01a         11-0110         -0         0-1         1-0         0-1         0-1         1-0         0-1         0         0         0         -0         -0	23 - 16 01000101 0- -101a -011a -1-01-aa -a-1001- 1000000a 11000100 11111011 1  	15 - 8         00100011	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1a-111-1           100-0-1-           101-100           0001-1           1100           100-0-1-           101-1-1-           0001-1           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-           -101-          0          0-
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ = a_0 \\ = a_1 \\ = a_2 \\ = a_3 \\ = a_4 \\ = a_5 \\ = a_7 \\ = a_8 \\ = a_9 \\ = a_10 \\ = a_11 \\ = a_{12} \\ = a_{13} \\ = a_{22} \\ = a_{23} \\ = a_{23} \\ = a_{23} \\ = a_{24} \\ = a_{25} \\ = a_{26} \\ = a_{27} \\ = a_{28} \\ = a_{29} \\ = a_{29} \\ = a_{20} \\ = a_{21} \\ = a_{22} \\ = a_{23} \\ = a_{24} \\ = a_{26} \\ = a_{27} \\ = a_{28} \\ = a_{29} \\ = a_{29} \\ = a_{30} \\ = a_{31} \\ = a_{32} \\ = a_{33} \\ = a_{34} \\ = a_{35} \\ = a_{36} \\ = a_{37} \\ = a_{38} \\ = a_{39} \\ = a_{40} \\ = a_{41} \\ = a_{42} \\ = a_{43} \\ = a_{44} \\ = a_{$	31 - 24         01100111         101         01100         110-110         0-11110         0-1         0-1         1-0         0-1         0-1         1-0         0-1         0-1         1-0         0-1         0-1         0-1         0-1         0-1         0-1	23 - 16 01000101 0- -101a -01	15 - 8           00100011          0-           01aa          00100-           0110010           1010-001           a001a1           0000000           0111100	8 - 0           00000001           -1-al0aa           100010           0-10-100           001-1           1a111-1           100-0-1-           101-100           0001-1           110-10           1000-1-           1011-1-           000-1-           -101-           -101-           -101-           -101-           -101-          0-0          0-0          0-0          0-1          0-0          0-1          0-1          0-1          0-1          0-1          0-1          0-1          0-1          0-1          0-1          0-1          1-1          1-1          1-1          1-1          1-1          1-1          1-1          1-1          0-1          0-0
$\begin{array}{c} {\rm chaining} \\ {\rm variable} \\ {\rm a}_{0} \\ {\rm a}_{1} \\ {\rm a}_{2} \\ {\rm a}_{3} \\ {\rm a}_{4} \\ {\rm a}_{5} \\ {\rm a}_{6} \\ {\rm a}_{7} \\ {\rm a}_{8} \\ {\rm a}_{9} \\ {\rm a}_{10} \\ {\rm a}_{11} \\ {\rm a}_{12} \\ {\rm a}_{13} \\ {\rm a}_{14} \\ {\rm a}_{15} \\ {\rm a}_{16} \\ {\rm a}_{17} \\ {\rm a}_{18} \\ {\rm a}_{16} \\ {\rm a}_{17} \\ {\rm a}_{18} \\ {\rm a}_{19} \\ {\rm a}_{20} \\ {\rm a}_{21} \\ {\rm a}_{22} \\ {\rm a}_{23} \\ {\rm a}_{24} \\ {\rm a}_{25} \\ {\rm a}_{26} \\ {\rm a}_{27} \\ {\rm a}_{28} \\ {\rm a}_{29} \\ {\rm a}_{23} \\ {\rm a}_{24} \\ {\rm a}_{25} \\ {\rm a}_{26} \\ {\rm a}_{27} \\ {\rm a}_{28} \\ {\rm a}_{29} \\ {\rm a}_{33} \\ {\rm a}_{34} \\ {\rm a}_{34} \\ {\rm a}_{35} \\ {\rm a}_{36} \\ {\rm a}_{37} \\ {\rm a}_{38} \\ {\rm a}_{39} \\ {\rm a}_{40} \\ {\rm a}_{41} \\ {\rm a}_{44} \\ {\rm a}_{45} \\ {\rm a}_{45} \\ \end{array}$	31 - 24         01100111         1010         01100         110-01a         11-0110         -0-1         1-0         1-0         1-0         1-0         1-0         0         0         0         1-0         1-0         0         0         0         0	23 - 16 01000101 0- -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11000100 11000100 	15 - 8           00100011	8 - 0           00000001           -1-a10aa           100010           0a-1a0-0           0-10-100           001-1           1-a111-1           100-0-1-           101-10           000-1-           110-10           -101-           -101-           -101-           -101-           -101-          0-0          00          00          00          0          0          0          10          0          10          10          10          10          10          10          10          10          10          10          10          11          11          11          10          10          10          10          10          10 </th

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

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

 $m_{3,21} + m_{2,26} + m_{2,20} + m_{1,24} + m_{0,28} + m_{0,25} +$  $m_{0,20} = 1, m_{14,21} + m_{12,27} + m_{12,24} + m_{12,22} + \dots$  $m_{11,25} + m_{10,28} + m_{10,27} + m_{10,24} + m_{10,23} + \dots$  $m_{9,28} + m_{9,26} + m_{9,23} + m_{9,21} + m_{8,29} + m_{8,26} +$  $m_{7,29} + m_{7,28} + m_{7,23} + m_{6,29} + m_{6,26} + m_{6,22} + \\$  $m_{5,25} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,23} + m_{4,22} + m_{4,23} + m_{4,22} + m_{4,23} + m_{4,24} + m_{4,24} + m_{4,25} + m_{4,24} + m_{4,24}$  $m_{3,26} + m_{3,25} + m_{3,21} + m_{2,28} + m_{2,23} + m_{1,26} +$  $m_{1,21} + m_{0,25} = 0, m_{14,20} + m_{12,26} + m_{12,23} + m_{$  $m_{12,21} + m_{11,28} + m_{11,24} + m_{10,28} + m_{10,27} +$  $m_{10,26} + m_{10,23} + m_{10,22} + m_{9,27} + m_{9,25} +$  $m_{9,22} + m_{9,20} + m_{8,28} + m_{8,25} + m_{7,28} + m_{7,27} + m_{7,28} + m_{7,28} + m_{7,28} + m_{7,27} + m_{7,28} + m_{7,28}$  $m_{7,22} + m_{6,29} + m_{6,28} + m_{6,25} + m_{6,21} + m_{5,24} +$  $m_{4,27} + m_{4,26} + m_{4,24} + m_{4,22} + m_{4,21} + m_{3,28} + \\$  $m_{3,25} + m_{3,24} + m_{3,20} + m_{2,27} + m_{2,22} + m_{1,25} + \\$  $m_{1,20} + m_{0,28} + m_{0,24} + m_{47,31} = 1, m_{14,5} + \dots$  $m_{8,5} + m_{6,5} = 1, m_{14,4} + m_{12,5} + m_{11,3} + m_{11,2} + \dots$  $m_{10,4} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2} + m_{8,5} +$  $m_{7,2} + m_{6,5} + m_{6,4} + m_{5,4} + m_{5,2} + m_{4,5} + m_{5,2} + m_{4,5} + m_{5,4} + m_{5$  $m_{4,4} + m_{4,0} + m_{3,31} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,5}$  $m_{2,3} + m_{2,2} + m_{1,31} + m_{0,4} + m_{0,3} + m_{0,2} =$  $1, m_{14,3} + m_{11,3} + m_{11,2} + m_{8,2} + m_{7,4} + m_{7,2} +$  $m_{7,1} + m_{6,2} + m_{5,3} + m_{4,0} + m_{3,3} + m_{2,2} + m_{1,31} +$  $m_{1,3} = 0, m_{14,2} + m_{12,5} + m_{12,3} + m_{10,4} + m_{9,2} + m_{10,4} + m_{10,4}$  $m_{7,4} + m_{6,3} + m_{4,5} + m_{4,4} + m_{4,3} + m_{3,2} +$  $m_{2,5} + m_{2,4} + m_{1,2} = 1, m_{14,1} + m_{12,4} + m_{11,2} + m_{11,2} + m_{12,4} + m_{11,2} + m_{12,4} + m_{11,2} + m_{12,4} + m_{12,4}$  $m_{10,2} + m_{9,3} + m_{8,3} + m_{7,2} + m_{6,2} + m_{5,5} + m_{6,2} + m_{5,5} + m_{6,2} + m_{6,2} + m_{6,2} + m_{6,3} + m_{$  $m_{5,2} + m_{4,4} + m_{3,31} + m_{3,4} + m_{3,2} + m_{3,1} + m_{3,2} + m_{3,1} + m_{3,2} + m_{3,1} + m_{3,2} + m_{3,1} + m_{3,2} + m_{$  $m_{2,4} + m_{2,3} + m_{0,3} = 0, m_{14,0} = 0, m_{13,31} =$  $0, m_{13,30} = 0, m_{13,29} + m_{8,29} = 0, m_{13,28} + 0$  $m_{8,28} + m_{2,28} + m_{0,28} = 0, m_{13,27} + m_{11,28} + \dots$  $m_{8,29} + m_{8,27} + m_{6,29} + m_{5,28} + m_{3,28} + m_{2,27} + \\$  $m_{0,27} = 1, m_{13,26} + m_{11,27} + m_{9,28} + m_{8,28} + m_{8$  $m_{8,26} + m_{6,28} + m_{5,27} + m_{3,28} + m_{3,27} + m_{2,26} + \dots$  $m_{1,28} + m_{0,26} = 1, m_{13,24} + m_{12,28} + m_{11,27} + m_{12,28} + m_{$  $m_{11,25} + m_{10,28} + m_{9,27} + m_{9,26} + m_{8,29} + m_{8,26} +$  $m_{8,24} + m_{7,29} + m_{7,28} + m_{6,26} + m_{5,25} + m_{4,28} + m_{6,26} + m_{6,26}$  $m_{3,28} + m_{3,26} + m_{3,25} + m_{2,28} + m_{2,24} + m_{1,28} +$  $m_{1,26} + m_{0,24} = 0, m_{13,23} + m_{12,27} + m_{11,26} + \dots$  $m_{11,24} + m_{10,28} + m_{10,27} + m_{9,26} + m_{9,25} + m_{9,25}$  $m_{8,29} + m_{8,28} + m_{8,25} + m_{8,23} + m_{7,29} + m_{7,28} + m_{7,29} + m_{7,28} + m_{7,29} + m_{7,28} + m_{7,29} + m_{7,29}$  $m_{7,27} + m_{6,25} + m_{5,28} + m_{5,24} + m_{4,28} + m_{4,27} +$  $m_{3,27} + m_{3,25} + m_{3,24} + m_{2,27} + m_{2,23} + m_{1,27} +$  $m_{1,25} + m_{0,28} + m_{0,23} = 0, m_{13,22} + m_{12,26} + \dots$  $m_{11,28} + m_{11,25} + m_{11,23} + m_{10,27} + m_{10,26} +$  $m_{9,28} + m_{9,25} + m_{9,24} + m_{8,28} + m_{8,27} + m_{8,24} +$  $m_{8,22} + m_{7,28} + m_{7,27} + m_{7,26} + m_{6,29} + m_{6,24} + m_{6,24}$  $m_{5,28} + m_{5,27} + m_{5,23} + m_{4,27} + m_{4,26} + m_{3,28} +$  $m_{3,26} + m_{3,24} + m_{3,23} + m_{2,28} + m_{2,26} + m_{2,22} +$  $m_{1,26} + m_{1,24} + m_{0,28} + m_{0,27} + m_{0,22} = 1, m_{13,6} =$  $0, m_{13,5} + m_{12,5} + m_{5,5} + m_{4,5} + m_{2,5} = 0, m_{13,4} + \dots$  $m_{12,5} + m_{11,2} + m_{10,4} + m_{7,4} + m_{5,4} + m_{5,3} + m_{5,4} + m$  $m_{5,2} + m_{4,5} + m_{4,4} + m_{3,31} + m_{2,5} + m_{2,4} + m_{3,31} + m_{$  $m_{2,2} + m_{1,2} = 0, m_{13,3} + m_{8,3} + m_{5,4} + m_{3,4} + \dots$  $m_{2,3} + m_{0,3} = 0, m_{13,2} + m_{10,3} + m_{10,2} + m_{10,1} + m_{10,1}$ 

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

From derived equations, we obtain advanced sufficient conditions on  $\{m_{i,j}\}$ .

### 6.3 control bits and controlled relations

We determine control bits and controlled relations as in Table 4, and Table 5, 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 6) which illustrate advanced sufficient conditions, controlled relations, control bits and semi-neutral bits.

Symbols in Table 6 mean:

- 'a', 'A', 'b', 'B', 'c', 'C': as in Section 6.2.
- 'L' means that it is the leading term of controlled relation of Table 4.
- 'w': adjust  $a_{i,j}$  so that  $m_{i+1,j} = 0$ .
- 'W': adjust  $a_{i,j}$  so that  $m_{i+1,j} = 1$ .
- 'v': adjust  $a_{i,j}$  so that  $m_{i,(j+27 \mod 32)} = 0$ .
- 'V': adjust  $a_{i,j}$  so that  $m_{i,(j+27 \mod 32)} = 1$ .
- 'h': adjust  $a_{i,j}$  so that corresponding controlled relation including  $m_{i+1,j}$  as leading term holds.

message variable	31 - 24	23 - 16	15 - 8	8 - 0
<i>m</i> <sub>0</sub>	0			
m <sub>1</sub> m <sub>2</sub>	-01 L10			011-
m <sub>2</sub>	-L0			-1
$m_4$	000			-01-
m 5 m -	L11			1L
m6 m7	LL			
m_8	LL			00
$m_9$	LOL			-0L11L
m <sub>10</sub>	LOL			-0LL
m11 m12	1L1			F
m <sub>13</sub>	OLLLLL-L	LL		-OLLLLLL
m <sub>14</sub>	LLOLLL-L	LLLL		LLLLLL0
m <sub>15</sub> m <sub>16</sub>	0	LL		-11LLLLL
m16 m17	-0			-10-
m18	00			-101
m <sub>19</sub>	-0			11-
m20 m21	-0			-01-
$m_{22}^{21}$	01			-010
m <sub>23</sub>	11			10-
m24 mar	-1			0
m25 m26	10			-010
m <sub>27</sub>	-1			-010-
m <sub>28</sub>	1			0
m29 m20	-0			-10-
m <sub>31</sub>	-1			0-
m <sub>32</sub>				1-
m33	0			-0
m34 m35	0			1-
m <sub>36</sub>	1			1-
$m_{37}$	1			-0
m <sub>38</sub>	0			
$m_{39}$ $m_{40}$	1			
m41				-1
m42	1			
m43	1			-11-
$m_{45}$				-1-
$m_{46}$	1			
m47	0			
$m_{i}$ (1 > 48)				
chaining	r			
chaining variable	31 - 24	23 - 16	15 - 8	8 - 0
chaining variable a <sub>0</sub>	31 - 24 01100111	23 - 16 01000101	15 - 8 00100011	8 - 0 00000001
$\begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ $	31 - 24 01100111 101VvV 01100vVv	23 - 16 01000101 Y0-	15 - 8 00100011	8 - 0 00000001 -1-a10aa
$\begin{array}{c} \begin{array}{c} & & \\ $	31 - 24 01100111 101VvV 01100vVv 0010Vv	23 - 16 01000101 Y0- -101a	15 - 8 00100011 a 0-	8 - 0 00000001 -1-a10aa 1-w00010 0aX1a0W0
$\begin{array}{c} \begin{array}{c} & & & \\ & & & \\ & $	31 - 24 01100111 101VvV 01100vVv 0010Vv 11010vv-	23 - 16 01000101 Y -101a -01	15 - 8 00100011 a 0- 01aaa	8 - 0 00000001 -1-a10aa 1-w00010 0aX1a0W0 0W10-100
$\begin{array}{c} chaining \\ chaining \\ variable \\ \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ \hline a_4 \\ a_5 \\ c_5 \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 11010vv- 10w01aV- 11V-0110	23 - 16 01000101 Y0 -101a -01 -1-01-aa -ar1001	15 - 8 00100011  	8 - 0 00000001 -1-a10aa 1-w00010 0aX1a0W0 0W10-100 0w01W1 1-as14111
$\begin{array}{c} \begin{array}{c} chaining\\ chaining\\ variable\\ \hline a_0\\ a_1\\ a_2\\ a_3\\ \hline a_4\\ a_5\\ \hline a_6\\ a_7 \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 11010vv- 10w01aV- 11W-0110 w1x-1110	23 - 16 01000101 Y0 -101a -01 -1-01-aa -a-1001- a1a1111-	15 - 8 00100011 	8 - 0 00000001 -1-a10aa 1-w00010 0aX1a0W0 0W10-100 0w-01W1 1-a111W1 10-10
$\begin{array}{c} \begin{array}{c} \dots \\ & (c \in [3]) \\ \hline \\ chaining \\ variable \\ \hline \\ a_0 \\ a_1 \\ \hline \\ a_2 \\ a_3 \\ \hline \\ a_2 \\ a_3 \\ \hline \\ a_4 \\ \hline \\ a_5 \\ \hline \\ a_6 \\ \hline \\ a_7 \\ \hline \\ \\ a_8 \\ \hline \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 11010vv- 10w01aV- 11W-0110 w1x-1110 h0Xvvv10	23 - 16 01000101 Y0 -101a -01 -1-01-aa -a_1001- ala1111- 0000000a	15 - 8 00100011 a 0- 01aaa 0100- 01100010 -101-001 a001a1	8 - 0 00000001 -1-a10aa 1-w00010 0aX1a0W0 0W10-100 0w01W1 1-a111W1 10-10 100X0-1h
$\begin{array}{c} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_9 \\ a_9 \\ a_9 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_9 \\ a_9 \\ a_1 \\ a_2 \\ a_2 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_5 \\ a_6 \\$	31 - 24 01100111 101VvV 01100VV 0010Vv 11010vV- 10w01aV- 11W-0110 w1x-1110 h0Xvvv10 00XVrr-V	23 - 16 01000101 Y0- -101a -01 -1-01-aa -a-1001- ala1111- 0000000a 11000100	15 - 8 00100011  01aa 00100- 01100010 -101-001 a001a1 00000000	8 - 0 00000001 -1-a10aa 1-w00010 0x1a0W0 0W10-100 0w01W1 1-a111W1 10-10 100X0-1h 101-1-1y act vi
$\begin{array}{c} \begin{array}{c} & \dots & & \\ & & chaining \\ & variable \\ & & a_0 \\ & & a_1 \\ & & a_2 \\ & & a_2 \\ & & a_3 \\ & & a_4 \\ & & a_5 \\ & & a_6 \\ & & a_7 \\ & & a_8 \\ & & a_9 \\ & & a_{10} \\ & & a_{11} \end{array}$	31 - 24 01100111 101VvV 01100vVv 01100vV 11010v- 110w01aV- 11W-0110 w1x-1110 h0Xvvv10 00XVrr-V 0w1-rv-v 1w0v-V	23 - 16 01000101 Y0 -101a -01 -1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011	15 - 8 00100011 0- 01aa 00100- 01100010 -101-001 a001a1 00000000 11100000 0111110	8 - 0 0000001 -1-a10aa 1-v00010 0x1a0W0 0W10-100 0w01W1 1-a111W1 10-10 100X0-1h 101-1-1y 00hW0-1h 11x0V
$\begin{array}{c} \begin{array}{c} \dots_{1} & (2 \leq 23) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_{0} \\ a_{1} \\ \hline \\ a_{2} \\ a_{3} \\ \hline \\ a_{4} \\ \hline \\ a_{5} \\ a_{6} \\ \hline \\ a_{7} \\ \hline \\ a_{8} \\ a_{9} \\ \hline \\ a_{10} \\ \hline \\ a_{11} \\ \hline \\ a_{12} \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010-Vv 11010vv- 10w01aV- 11W-0110 w1x-1110 h0Xvvv10 00XVrr-V 0w1-rv-v 1w0V-V 0w1-rV-V	23 - 16 01000101 Y0 -101a -01a -1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1	15 - 8 00100011 	8 - 0 0000001 -1-a10aa 1-w00010 0aX1a0W0 0w01W1 1-a111W1 10-10 100X0-1h 101-1-1y 00hW0-1h 11x0Y -1XWa-Wh
$\begin{array}{c} \begin{array}{c} \dots_{4} & (i \geq 43) \\ \text{chaining} \\ \text{variable} \\ \hline a_{0} \\ a_{1} \\ \hline a_{2} \\ a_{3} \\ \hline a_{4} \\ \hline a_{5} \\ a_{6} \\ \hline a_{7} \\ \hline a_{8} \\ a_{9} \\ \hline a_{10} \\ \hline a_{11} \\ \hline a_{12} \\ \hline a_{13} \end{array}$	31 - 24 01100111 101VvV 01100-Vv 0010Vv 11010vv- 10w01aV- 11W-0110 w1x-1110 h0Xvvv10 00X1r-V 0w1-rv-v 1w0V-V 1w0vv-	23 - 16 01000101 Y0 101a -01 -a-1001- ala1111- 0000000 11000100 11111011 	15 - 8 00100011 0 01aa -00100- 01100010 -101-001 a001a1 00000000 01111100 001111100	8 - 0           00000001           -1-al0aa           1-w00010           0M10-100           0M-01W1           1-al1W1           10-10           100X0-1h           101-1-1y           00bW0-1h           11x0Y           -1XWa-Wh           -1-q0Jy
$\begin{array}{c} \begin{array}{c} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{14} \\ a_{14} \\ a_{14} \\ a_{14} \\ a_{15} \\ a_{16} \\ $	31 - 24 01100111 101VVV 01100vVv 0010Vv 11010vv- 10w01aV- 11W-0110 wix-1110 00XVrr-V 1w0V-V 0w1-rV-V 1w0V-V 0w1-rV-V 1w0V-V 0w1-rV-V 0w1-rV-V	23 - 16 01000101 Y0 -101a -01 ala1111- 0000000a 11000100 111111011 1 rr hh	15 - 8 00100011 0- 01aaa 00100- 01100010 101-001 a001a1 00000000 01111100  01111100000 01111110 	8 - 0           00000001           -1-al0aa           1-w00010           0W10-100           0W01W1           1al1W1           10-10           100X0-1h           101-1-1y           00hW0-1h           11x0'           -1xWa-Wh           -1-qq0Jy           Nihhhhhh
$\begin{array}{c} \begin{array}{c} & \dots & (1 \leq 10) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 110010v- 10w01aV- 11W-0110 w1x-1110 00XVrr-V 0w1-rv-v 0w1-rv-v 1w0v-V 1w0vv- 1rhhvVh 0vvhhhVh	23 - 16 01000101 Y0 01a -011a -01 01aa -a-1001- ala1111- 00000000 11000100 11111011 1 	15 - 8           00100011          0-           01aa           -01000-           01100010           -101-001           a001a1           0000000           11100000           0111110	B         0           00000001         -1-a10aa           -1-a10aa         0.0000001           1-w00010         0.00000000           0010-100         0.0000000           1-a111W1         10-100           100X0-1h         101-1-1y           100X0-1h         11x0Y           -1XWA-Wh         -1-qq01y           NINhh1hh         NNhh0h0
$\begin{array}{c} \begin{array}{c} \dots_{1} (3 \leq 13) \\ \text{chaining} \\ \text{variable} \\ \hline a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ a_{4} \\ a_{5} \\ a_{6} \\ a_{7} \\ a_{8} \\ a_{9} \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ \end{array}$	31 - 24 01100111 101VvV 01100vV 0010Vv 10001aV- 11W-0110 wix-1110 00XVrr-V 001-rv-V 1x0V-V 001-rV-V 1x0vv 1rhhvVh 0vuhhVh Wiwhhhh -0	23 - 16 01000101 Y0 0 -101a -01 a1a1111- 000000a 11000100 11111011 1 hh hhhN hhqNqNN	15 - 8 00100011 0- 01aa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110  qNNNNQN qNNQQMQN NNQNNQQ	B         0           00000001         -1-a10aa           -1-a10aa         0           1-w00010         0           0w10-100         0           0w10-100         0           1-a11W1         1           1-0-101         100X0-1h           101-1-1y         00bW0-1h           11x0Y         -1XWa-Wh           -1XWa-Wh         -1-qq01y           Nihhhihh         NNhh0hh0           qWWhahhh        100-
$\begin{array}{c} \begin{array}{c} \dots_{1} (3 \leq 13) \\ \text{chaining} \\ \text{variable} \\ \hline a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ a_{4} \\ a_{5} \\ a_{6} \\ a_{7} \\ a_{6} \\ a_{7} \\ a_{6} \\ a_{7} \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 10001aV- 10w01aV- 11W-0110 w1x-1110 00XVvr10 00XVrr-V 0w1-rV-v 1w0-v-V 0w1-rV-v 1w0-vv- 1whhNh 0rwhhVh W1whhhh	23 - 16 01000101 Y0 -101a -011a -01 a1a111- 000000a 11111011 1 hhhN hhhhN hhqNqNqN	15 - 8           00100011          0           01aa          00100-           01100010           -101-001           a001a1           00000000           11100000           0111110	S = 0           00000001           -1-a10aa           1=w00010           0aX1a0W0           0M10-100           0w-01W1           1-a111W1           111W1           101-1-1y           00bW0-1h           11x0Y           -1XWa-Wh           -1-qq01y           Nihhhihh           NNhhoho           qWWhahhh          00-
$\begin{array}{c} \begin{array}{c} \dots_{1} (2 \leq 13) \\ \text{chaining} \\ \text{variable} \\ \hline a_{0} \\ a_{1} \\ \hline a_{2} \\ a_{3} \\ \hline a_{4} \\ a_{5} \\ \hline a_{6} \\ \hline a_{7} \\ \hline a_{8} \\ a_{9} \\ \hline a_{10} \\ \hline a_{11} \\ \hline a_{12} \\ \hline a_{13} \\ \hline a_{14} \\ \hline a_{15} \\ \hline a_{16} \\ \hline a_{17} \\ \hline a_{18} \\ \hline a_{19} \\ \hline a_{20} \\ \hline \end{array}$	31 - 24 01100111 101VvV 01100vV 0010Vv 11010vv- 10w01aV- 11W-0110 w1x-1110 00XVvr10 00XVrr-V 0w1-rV-V 1w0V-V 0w1-rV-V 1w0vv- 1rhhvvVh 0rwhhVh W1whhhh -0 1-1 -C	23 - 16 01000101 Y -101a -01 a-1001 a1a1111- 000000a 11111011  hh hhh hhh hhh hhh	15 - 8 00100011 0- 01aa -00100- 01100010 -101-001 a001a1 00000000 11100000 0111110 01111110 000111 qNNNNQN qNNqQNQN NNQNNqQq 	8 - 0           0000001           -1-al0aa           1-w00010           0aXla0W0           0M10-100           0w-01W1           1-al11W1           10-10           100X0-1h           101-1-1y           00hW0-1h           11x0'1           00hW0-1h           11x0'1           00hW0-1h           11x0'1           00hW0-1h           1x0'1           00hW0-1h           1x0'1           Nhhh0hh0           qWWhahhh          0'0-          0'0-
$\begin{array}{c} \begin{array}{c} \begin{array}{c} \dots \\ (1 \\ 2 \\ m) \end{array} \\ \begin{array}{c} \begin{array}{c} \text{chaining} \\ \text{variable} \end{array} \\ \begin{array}{c} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \end{array}$	31 - 24 01100111 101V	23 - 16 01000101 Y0 -101a -01 1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 01111100 01111100 0111110 	8 - 0           00000001           -1-al0aa           1-w00010           0M10-100           0W10-100           0W-01W1           1-al11W1           10-10           100X0-1h           101-1-1y           00hW0-1h           11x00'           -1XWa-Wh           -1-qQ01y           NNhh0hh0           qWWhahhh          00-          00-          00-          0-
$\begin{array}{c} \begin{array}{c} \dots_{1} (2 - 2 - 3) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ \hline \\ a_{4} \\ a_{5} \\ a_{6} \\ \hline \\ a_{7} \\ a_{8} \\ a_{9} \\ a_{10} \\ a_{11} \\ \hline \\ a_{12} \\ a_{13} \\ a_{14} \\ \hline \\ a_{15} \\ a_{16} \\ \hline \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ \hline \\ a_{21} \\ a_{22} \\ \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 110010v- 10w01aV- 11W-0110 w1x-1110 00XVrr-V 1w0-v-V- 1w0-v-V- 1w0-v-V- 1w1v-hhVh 0-v-v- 1-1 1-1 -b 	23 - 16 01000101 Y0 0- -101a -01 -1-01-aa -a-1001- ala1111- 0000000a 11100110 11111011 1 hh hhh hhh hhh hhh	15 - 8           00100011          0-           01aa          00100-           0100010           -101-001           -00101-           0000000           11100000           0111110	B         0           00000001         -1-a10aa           -1-a10aa         1           0x1a0001         0x1a000           0w10-100         0w10-100           0w10-100         0w10-100           1-a111W1         10-10           100X0-1h         101-1-1y           00bW0-1h         11x0Y           -1XWa-Wh         -1-qq01y           Nihhhhh         Nihhhhh           WWhahhh        00-          0        0          0        0          0        0          0
$\begin{array}{c} \begin{array}{c} \dots_{1} (2 - 2 - 3) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ a_{4} \\ a_{5} \\ a_{6} \\ a_{7} \\ a_{8} \\ a_{9} \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 11010vv- 10w01aV- 11W-0110 wix-1110 00XVrr-V 0w1-rV-V 1w0V-V 1w0vv- 1x0vv	23 - 16 01000101 Y0 -101a -011a -1-01-aa -a-1001- ala1111- 0000000 11111011 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 0111110  qNNNNNQN qNNqQNQN NNQNQQAQN NNQNQQAQN NNQNQQAQN	8         0           0000001         -1-a10aa           -1-a10aa         0           1-w00010         0           0aX1a0W0         0           0M10-100         0           0M10-100         0           1-a111W1         1           1-o-01W1         10           100X0-1h         101-11           00H00-1h         11x0Y           -1XWA-Wh         -14WA-Wh           -1XWA-Wh         -1-100          00        00          01        0          01        0          01        0
$\begin{array}{c} \begin{array}{c} \dots_{1} (2 \pm 33) \\ \text{chaining} \\ \text{variable} \\ \hline a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ a_{4} \\ a_{5} \\ a_{6} \\ a_{7} \\ a_{8} \\ a_{9} \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{27} \end{array}$	31 - 24 01100111 101VvV 01100vVv 0010Vv 10010V- 10401aV- 11W-0110 w1x-1110 00XVvr10 00XVrr-V 0w1-rV-V 1w0V-V 0w1-rV-V 1w0vv- 1xhbvVh 0rvhhbVh W1whhhh 0v 1-1 -C -B -B -B	23 - 16 01000101 Y0 -101a -011a -011a 001	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 01111110 01111110 	S         0           00000001         -1-a10aa           -1-a10aa         1           1-w00010         0aX1a0W0           0M10-100         0m(0-100)           1-a111W1         1           1-a111W1         1           1010-010         100X0-1h           1011-1y         00hW0-1h           00hW0-1h         11x0Y           -1XWa-Wh         -1-qq01y           N1hhh1hh         NNhh0h0           QWMahhh        00-          0
$\begin{array}{c} \begin{array}{c} \begin{array}{c}  \\   \\  \\   \\               .$	31 - 24 01100111 101VV 01100vVv 0010Vv 11010vv- 10w01aV- 11W-0110 wix-1110 wix-1110 00XVrr-V 1w0V-V 0w1-rV-V 1w0V-V 1w0V-V 1w1-v-V- 1w0-V-V 1w0V-V  	23 - 16 01000101 Y -101a -01 a-1001 ala1111- 000000a 11111011  hh hhhN hhhN hhhN hhhN	15 - 8 00100011 0- 01aa -00100- 01100010 -101-001 a001a1 00000000 0111110 0111110 01111110 	8 - 0           0000001           -1-a10aa           1-w00010           0aX1a0W0           0M10-100           0w10-100           0w10-100           1-a111W1           1-a111W1           101-1-1y           00hW0-1h           11x01           100hW0-1h           11x01           00hW0-1h           11x01           101-1-1y           00hW0-1h           11x01           11xua-Wh           -1-qq01y           N1hhh1hh          00          0          0          0          0          0
$\begin{array}{c} \begin{array}{c} \dots, \ (i=2,i3)\\ \text{chaining}\\ \text{variable}\\ \hline a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\\ a_8\\ a_6\\ a_7\\ a_8\\ a_9\\ a_{10}\\ a_{11}\\ a_{12}\\ a_{13}\\ a_{14}\\ a_{15}\\ a_{16}\\ a_{17}\\ a_{18}\\ a_{19}\\ a_{20}\\ a_{21}\\ a_{22}\\ a_{23}\\ a_{24}\\ a_{25}\\ a_{26}\\ a_{27}\\ \end{array}$	31 - 24 01100111 101VV 01100-VV 0010Vv 11010vv- 10w01aV- 11W-0110 wix-1110 00XVrr-V 0w1-rv-v 1w0V-V 0w1-rV-V 1w0-V-V 1w0-v-v- 1rhhvvVh 0ruhhVh 0ruhhVh -0 1-1     	23 - 16 01000101 Y0 -101a -01	15 - 8           00100011          0-           01aa          00100-           01010010           -101-001           a001al           00000000           11100000           0111110	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0w10-100         0w10-100           0w10-100         1-a111W1           10-10         100X0-1h           101-1-1y         00bW0-1h           11x0Y         -1XWa-Wh           -1xWa-Wh         -1qq01y           Nihhhihh         WNhhohh0          0        0          0        0          0        0          0        0          0
$\begin{array}{c} \begin{array}{c} \dots, \ (2-20) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_$	31 - 24 31 - 24 01100111 101VvV 01100-VV 10100v-VV 10001aV- 11W-0110 w1x-1110 00XVrr-V 0w1-rv-V 0w1-rv-V 1w0V-V 0w1-rv-V 1w0-v-V	23 - 16 01000101 Y0 0 -101a -01 01 	15 - 8 00100011 0- 01aa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110 00111110 0111111	8         0           00000001         -1-a10aa           -1-a10aa         1           1-w00010         0w10-100           0w10-100         0w10-101           1-a111W1         1           1-a111W1         1           101-1-1y         00M00-1h           1011-1-1y         00M00-1h           11X0Y         -1XWa-Wh           -1-qq01y         Nihhhihh           NNhhhhhh        00          00        00          01        01          01        01
$\begin{array}{c} \begin{array}{c} \dots_{1} (2 \pm 33) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ \hline \\ a_{4} \\ a_{5} \\ a_{6} \\ \hline \\ a_{7} \\ a_{8} \\ a_{9} \\ \hline \\ a_{10} \\ a_{11} \\ \hline \\ a_{12} \\ a_{13} \\ a_{14} \\ \hline \\ a_{15} \\ a_{16} \\ \hline \\ a_{17} \\ a_{18} \\ a_{19} \\ \hline \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{29} \\ a_{30} \\ \end{array}$	31 - 24 31 - 24 01100111 101VvV 01100-Vv 10001aV- 11001aV- 11001aV- 110-0110 vix-1110 00XVrr-V 0v1-rv-V 1v0vV- 1v0-vV- 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v1-v-V 1v0-vV- 1v1-v-V 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v1-v-V 1v1-v-V 1v1-v-V 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1v0-vV- 1v1-v-V 1	23 - 16 01000101 Y0 -101a -011a -01 a1a1111- 000000a 11111011 11000100 111111011 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 0111110  	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0aX1a0W0         0w10-100           0w10-100         0w10-100           1-a11W1         10-101           1-a11W1         111W0           101-1-1Y         00bW0-1h           101-1-1Y         00bW0-1h           11x0Y         -1XWa-Wh           -1XWa-Wh         -1-qq01Y           Wihhhhhhh         Nhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh
$\begin{array}{c} \begin{array}{c} \dots_{1} (2 \pm 33) \\ \text{chaining} \\ \text{variable} \\ \hline a_{0} \\ a_{1} \\ a_{2} \\ a_{3} \\ \hline a_{4} \\ a_{5} \\ a_{6} \\ \hline a_{7} \\ a_{8} \\ a_{9} \\ \hline a_{10} \\ \hline a_{11} \\ a_{12} \\ \hline a_{13} \\ a_{14} \\ \hline a_{15} \\ a_{16} \\ a_{17} \\ \hline a_{18} \\ a_{19} \\ \hline a_{20} \\ a_{21} \\ \hline a_{22} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ \hline a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{30} \\ a_{31} \\ \end{array}$	31 - 24 31 - 24 01100111 101VvV 01100vVv 0010Vv 11010vv- 10001aV- 11W-0110 wix-1110 00XVvr-V 0x1-rV-V 1w0V-V 0w1-rV-V 1w0vV- 1w0vV- 1whhhhh -0v 1-1 -c     	23 - 16 01000101 Y0 -101a -011a -01 ala1111- 000000a 11111011 1 11000100 11111011 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 01111100 01111110 	S         0           00000001         -1-a10aa           -1-a10aa         1           1-w00010         0aX1a0W0           0M10-100         0w10-100           1-a111W1         1           1-a111W1         1           1-a111W1         1           1-a11W1         1           101-1-1y         00bW0-1h           00kW0-1h         11x0Y           11xWawh         -1-qq01y           N1hhh1hh         NNhh0h0           qWMashhh        00-
$\begin{array}{c} \begin{array}{c} \dots, \ (i=2,i5)\\ \text{chaining}\\ \text{variable}\\ \hline a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\\ a_8\\ a_9\\ a_{10}\\ a_{11}\\ a_{12}\\ a_{13}\\ a_{14}\\ a_{15}\\ a_{16}\\ a_{17}\\ a_{18}\\ a_{16}\\ a_{17}\\ a_{18}\\ a_{19}\\ a_{20}\\ a_{21}\\ a_{22}\\ a_{22}\\ a_{23}\\ a_{24}\\ a_{25}\\ a_{26}\\ a_{27}\\ a_{28}\\ a_{29}\\ a_{30}\\ a_{31}\\ a_{32}\\ a_{32}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{32}\\ a_{32}\\ a_{31}\\ a_{32}\\ a_{32}\\ a_{31}\\ a_{32}\\ a_{32}\\ a_{31}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{31}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{31}\\ a_{31}\\ a_{32}\\ a_{31}\\ a_{31$	31 - 24 31 - 24 01100111 101VyV 01100vVv 0010Vv 11000vVv 100018V- 10w018V- 10w018V- 10w018V- 0001-V-V 001-V-V 001-V-V 001-V-V 1w0V-V 001-V-V 1w0V-V 001-V-V 001-V-V 1w0-V-V 0010-V-V 1w0-V-V 0010-V-V 1w0-V-V 0011-V-V 0011-V 0    	23 - 16 01000101 Y0 -101a -01 1-01-aa -a-1001- ala1111- 0000000a 11000100 11111011 1 	15 - 8 00100011 0- 01aa 00100- 0110010 -101-001 a001a1 00000000 11100000 01111110 	8 - 0           0000001           -1-a10aa           1-w00010           0aX1a0W0           0M10-100           0w10-100           0w10-100           1-a111W1           1-a111W1           1-a111W1           1-a11-1y           00hW0-1h           11x0-1           100AX0-1h           11x0y           00hW0-1h           11x0y           00hW0-1h           11x0y           1XWa-Mh           -1-qq01y           N1hhb1hh           NNhb0h0h           qWWaahhh          00-          01          0-          0-          0-          0-          0-          0-          0-          0-          0-          0-
$\begin{array}{c} \begin{array}{c} \dots, \ (i \in 2, i \leq j) \\ \text{chaining} \\ \text{variable} \\ \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{30} \\ a_{31} \\ a_{32} \\ a_{33} \\ a_{32} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{35$	31 - 24 31 - 24 01100111 101VvV 01100-VV 0010Vv 110001aV- 10001aV- 11W-0110 wix-1110 00XVr-V 002Vr-VV 002Vr-VV 100-V-V 002Vr-VV 100-V-V 002Vr-VV 100-VV 002Vr-VV 00	23 - 16 01000101 Y0 -101a -01	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110 0111110 0111110 0111110  	8         0           00000001         -1-a10aa           -1-a10aa         1           1-w00010         0w10-100           0w10-100         0w10-100           1-a111W1         1           1-0101         100X0-1h           101-1-1y         00bW0-1h           11x0Y         -1XWa-Wh           -1-qq01y         Nihhhhh           Nihhhhh        00          0        0
$\begin{array}{c} \begin{array}{c} \dots, \ (2-2,0)\\ \text{chaining}\\ \text{variable}\\ \hline a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\\ a_8\\ a_9\\ a_{10}\\ a_{11}\\ a_{12}\\ a_{13}\\ a_{14}\\ a_{15}\\ a_{16}\\ a_{17}\\ a_{18}\\ a_{19}\\ a_{20}\\ a_{21}\\ a_{22}\\ a_{23}\\ a_{24}\\ a_{25}\\ a_{26}\\ a_{27}\\ a_{28}\\ a_{29}\\ a_{30}\\ a_{31}\\ a_{32}\\ a_{33}\\ a_{34}\\ a_{35}\\ \end{array}$	31 - 24 31 - 24 01100111 101VvV 01100VV 0010Vv 10001aV- 11W-0110 vix-1110 00XVrr-V 0v1-rv-V 0v1-rv-V 1v0-v-V 1v0	23 - 16 01000101 Y0 0 -101a -01 a1010 	15 - 8 00100011 0- 01aa 00100- 01100010 -101-001 a001a1 00000000 11100000 0111100 0000000 11100000 0111111	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0w10-100         0w10-100           0w10-101         1-a111W1           10-101         100X0-1h           101-11-1y         00bW0-1h           101-1-1y         00bW0-1h           11X0Y         -1-qq01y           N1hhh1hh         NNhh0h0           qWWhahhh        0          a-1        0          A1-        0          A-0        0          0-        0-          0-        0-          0-        0-          0-        0-          0-        0-          0-        0-          0-        0-          0-        0-
$\begin{array}{c} \begin{array}{c} \dots, \ (2 & 2 & 3) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{30} \\ a_{31} \\ a_{32} \\ a_{33} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{36} \\ \end{array}$	31 - 24 31 - 24 01100111 101VvV 01100VV 0010Vv 110010V- 10w01aV- 11W-0110 w1x-1110 00XVrr-V 0w1-rV-V 1w0V-V 0w1-rV-V 1w0-vV- 1w0-vV 1w0-vV- 1w	23 - 16 01000101 Y0 -101a -011a -01 a1a1111- 000000a 11111011 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 01111100  	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0aX1a0W0         0M10-100           0mX10-100         0mV0-100           1-a111W1         1-n-0101           1-a111W1         1-n-0-101           100X0-1h         101-1-1y           00hW0-1h         11x0Y           -1XWa-Wh         -1-qq01y           Nihhhihh         Nihhihh           NWhAbhh        00          00        0          01        0          01        0
$\begin{array}{c} \begin{array}{c} \begin{array}{c}  \\   \\  \\   \\              \mbox$	31 - 24 31 - 24 01100111 101VyV 01100-VV 0010Vv 11010v- 10w01aV- 11W-0110 w1x-1110 h0Xvvv10 00X1rr-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-rV-V 1w0-V 0w1-v 1w0-V 0w1-rV-V 0w1-v 1w0-V 0w1-v 0w1-v 1w0-V 0w1-v 0w1-v 1w0-V 0w1-v 1w0-V 0w1-v 0w1	23 - 16 01000101 Y0 -101a -011a -01	15 - 8 00100011 	8 - 0           0000001           -1-a10aa           1-w00010           0aX1a0W0           0M10-100           0M10-100           0M10-100           1-a111W1           1-a111W1           1-a111W1           1-a11W1           1-a11W1           0DW0-1h           11x0Y           1XWawh           -1-qq01y           N1hhh1hh           NNhh0h0           qWhahhh          0-          0-
$\begin{array}{c} \begin{array}{c} \dots, \ (i \in 2, i o) \\ \text{chaining} \\ \text{variable} \\ \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{31} \\ a_{32} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{36} \\ a_{37} \\ a_{38} \\ a_{20} \\ a_{20} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{37} \\ a_{38} \\ a_{36} \\ a_{37} \\ a_{38} \\ a_{20} \\ a_{20} \\ a_{20} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{36} \\ a_{37} \\ a_{38} \\ a_{20} $	31 - 24 31 - 24 01100111 101VyV 01100vVV 0010Vv 110001aV- 11W-0110 wix-1110 00XVr-V 0w1-rv-v 1w0-V-V 0w1-rv-v 1w0-v-V 1w0-v-v- 1w1-rv-v 1w0-v 1w0-v	23 - 16 01000101 Y0 -101a -01	15 - 8           00100011          0-           01aa          00100-           01100010           -101-001           a001-001           a001-001           0000000           01100010	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0w10-100         0w10-100           1-a111W1         10-10           100X0-1h         101-1-1y           100X0-1h         11x0Y           1Ixwa-Wh         -1qq01y           NIhhhihh         WNhhhhh          0        0          0        0          0        0          0        0          0
$\begin{array}{c} \begin{array}{c} \dots, (2-2, 0)\\ \text{chaining}\\ \text{variable}\\ \hline a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\\ a_8\\ a_9\\ a_10\\ a_{11}\\ a_{12}\\ a_{13}\\ a_{14}\\ a_{16}\\ a_{17}\\ a_{18}\\ a_{16}\\ a_{17}\\ a_{18}\\ a_{19}\\ a_{21}\\ a_{22}\\ a_{22}\\ a_{23}\\ a_{24}\\ a_{25}\\ a_{26}\\ a_{27}\\ a_{28}\\ a_{29}\\ a_{30}\\ a_{31}\\ a_{32}\\ a_{33}\\ a_{34}\\ a_{35}\\ a_{38}\\ a_{39}\\ a_{39}\\ a_{40}\\ \end{array}$	31 - 24 31 - 24 01100111 101VvV 01100-VV 0010Vv 110010v- 10v01aV- 11W-0110 wix-1110 00XVrr-V 0v1-rv-V 0v1-rv-V 0v1-rv-V 1v0V-V 0v1-rv-V 1v0-v 1vhvvVh 0v4hhVh -0    	23 - 16 01000101 Y0 -101a -01	15 - 8 00100011 0- 01aaa 0-0100- 01100010 -101-001 a001a1- 00000000 111100000 0111110 0111110  	8         0           00000001         -1-a10aa           -1-a10aa         1           1-w00010         0w10-100           00x1a0w0         0w10-100           1-a111W1         1           1-a111W1         1           100X0-1h         1011-1-1y           100W0-1h         11X0Y           11Xw-Wh         -1-qq01y           N1hh1hh         NNhh0h0           QWWhahhh        0          0        0          0        0
$\begin{array}{c} \begin{array}{c} \dots, \ (2 - 2 - 3) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_4$	31 - 24 31 - 24 01100111 101VvV 01100VV 0010Vv 10001aV- 11W-0110 vix-1110 00XVrr-V 0v1-rv-V 1v0-vV 1v0	23 - 16 01000101 Y0 0 -101a -01 a101 a1a1111- 0000000 11110011 11000100 11111011 	15 - 8 00100011 0- 01aa 00100- 01100010 -101-001 a001a1 00000000 11100000 0111110  	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0aX1a0W0         0w10-100           0w10-100         0w10-100           1-a111W1         1-a111W1           1-a111W1         1-a111W1           1-a111W1         1-a11W1           1-a11W1         1-a11W1           1-a11W1         1-a10W2           101-11Y         00bW0-1h           11X07         1XWa-Wh           -1-qq01Y         Nihhihh           NWhAbhh        00          0-        0          A1-        0          A-0-        0          A-0-        0          0-        0          0-        0          0-        0
$\begin{array}{c} \begin{array}{c} \dots, \ (2 - 2 - 3) \\ \text{chaining} \\ \text{variable} \\ \hline \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \\ a_{17} \\ a_{18} \\ a_{19} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{24} \\ a_{25} \\ a_{26} \\ a_{27} \\ a_{28} \\ a_{29} \\ a_{20} \\ a_{21} \\ a_{22} \\ a_{23} \\ a_{32} \\ a_{33} \\ a_{33} \\ a_{33} \\ a_{33} \\ a_{33} \\ a_{33} \\ a_{34} \\ a_{35} \\ a_{36} \\ a_{37} \\ a_{38} \\ a_{39} \\ a_{40} \\ a_{41} \\ a_{42} \\ a_{41} \\ a_{41} \\ a_{42} \\ a_{41} \\ a_{41} \\ a_{42} \\ a_{41} \\ a_{41} \\ a_{41} \\ a_{42} \\ a_{41} \\ a_{41} \\ a_{41} \\ a_{41} \\ a_{41} \\ a_{42} \\ a_{41} \\ a_{42} \\ a_{41} \\ a_{41}$	31 - 24 31 - 24 01100111 101VyV 01100-VV 0010VV 11010v 10v01aV- 11V-0110 vix-1110 h0Xvvv10 00X1rr-V 1w0-V 1w0-V	23 - 16 01000101 Y0 -101a -01 -101a -01 ala1111- 000000a 11111011 	15 - 8 00100011 0- 01aaa 00100- 01100010 -101-001 a001a1 00000000 11100000 01111100  	8         0           00000001         -1-a10aa           1-w00010         0aX1a0W0           0M10-100         0w10-100           0w10-100         0w10-100           1-a111W1         10101           1-a111W1         1
$\begin{array}{c} \begin{array}{c} \begin{array}{c} \mbox{main rg} \\ \mbox{chain ing} \\ \mbox{variable} \\ \hline \\ a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_4$	31 - 24 31 - 24 01100111 101VyV 01100-VV 0010VV 11010v- 10w01aV- 11W-0110 wix-1110 00XVrr-V 0w1-V-V 0w1-V-V 1w0V-V 0w1-rV-V 1w0V-V 0w1-rV-V 1w0V-V 0w1-rV-V 0w1-rV-V 0w1-rV-V 0w1-rV-V 1w0V-V 0w1-rV-V 0	23 - 16 01000101 Y0 -101a -01 -1-01-aa -01 	15 - 8 00100011 0- 01aaa 0-0100- 01100010 -101-001 a001a1 00000000 11100000 01111110 01111110 	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0w10-100         0w10-100           0w10-100         1-a111W1           10-10         100X0-1h           100X0-1h         11x0Y           1XWA-Wh         -1-qq01y           Nhhhihh        100          0        0          0        A1-          A1-        A1-          A1-        0          A1-        0-
$\begin{array}{c} \begin{array}{c} \begin{array}{c} \mbox{main red} \\ \mbox{main red} \\ \mbox{chain red} \\ \mbox{a r l} \\ a r$	31 - 24 31 - 24 01100111 101V	23 - 16 01000101 Y0 -101a -01	15 - 8 00100011 0- 01aa 00100- 01100010 -101-001 a001a1 00000000 111100000 0111110 00000000 0111110  	8         0           00000001         -1-a10aa           -1-a10aa         1-w00010           0w10-100         0w10-100           1-a111W1         10-10           100X0-1h         101-1-1y           100X0-1h         111/0-10           11X0Y         -1XWa-Wh           -1-qq01y         Nihhhhh           WWhahhh        0-          0-

Table 6: 'Advanced' sufficient condition on  $\{m_{i,j}\}\$  and  $\{a_{i,j}\}\$ 

Control	Control	Controlled relation $r_i$
sequence	bit b.	
s124	$a_{16,7}, a_{15,9}, a_{14,9}$	$a_{23,0} = 0$
<sup>s</sup> 123	$a_{16,9}$	$a_{22,2} + a_{21,2} = 1$
<sup>s</sup> 122	$a_{16,13}, a_{15,15}, a_{15,12}, a_{15,11}$	$a_{22,1} = 1$
<sup>s</sup> 121	<sup>a</sup> 16,10	$a_{21,3} + m_{20,3} = 0$
s120	a16,8	$a_{21,1} = 1$
<sup>\$119</sup>	a16,15, a16,20	$a_{20,3} + m_{19,3} - 1$
\$118 \$117	a16.21	$a_{19,0} = 0$ $a_{18,31} = 1$
<sup>s</sup> 116	a16.19	$a_{18,29} = 1$
s115	a13,4	$a_{18,2} = 0$
s114	a13,3	$a_{18,1} = 0$
<sup>s</sup> 113	a14,15	$a_{17,30} = 0$
<sup>s</sup> 112	a16,31	$m_{15,31} = 1$
\$111 \$110	a16,29	$m_{15,29} = 0$ $m_{15,29} + m_{10,29} + m_{2,20} + m_{7,20} + m_{4,29} + m_{2,29} = 1$
\$100	$a_{16}$ 27, $a_{13}$ 28	$m_{15,26} + m_{10,26} + m_{25,29} + m_{1,29} + m_{4,26} + m_{25,26}$ $m_{15,27} + m_{14,25} + m_{12,28} + m_{12,26} + m_{10,28} + m_{0,27} + m_{0,25} + m_{8,29} + m_{8,28}$
200	10,217 10,20 @10.00	$+m_{7,28} + m_{7,27} + m_{6,26} + m_{5,28} + m_{4,26} + m_{3,25} + m_{2,28} + m_{1,25} + m_{0,28} = 1$
3108	<sup>a</sup> 16,26	$ \begin{array}{c} 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 \end{array} $
<sup>s</sup> 107	$a_{16,25}$	$ \begin{array}{l} 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 \end{array} $
<sup>s</sup> 106	$a_{16,24}$	$ \begin{array}{l} 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} \end{array} $
		$+m_{2,27} + m_{2,25} + m_{2,24} + m_{1,28} + m_{1,27} + m_{0,27} + m_{0,25} = 1$
<sup>s</sup> 105	$a_{16,23}$	$ \begin{array}{l} 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} \end{array} $
\$104	<i>0.1.6.</i> 22	$+m_{3,27} + m_{3,26} + m_{2,26} + m_{2,24} + m_{2,23} + m_{1,27} + m_{1,26} + m_{0,26} + m_{0,24} = 1$
~104	-10,22	$+m_{9,27} + m_{9,26} + m_{8,27} + m_{8,24} + m_{8,23} + m_{7,28} + m_{7,27} + m_{7,23} + m_{6,27}$
		$+m_{6,25} + m_{5,23} + m_{4,28} + m_{4,27} + m_{4,22} + m_{3,26} + m_{2,28} + m_{2,27} + m_{2,25}$
		$+m_{2,23} + m_{2,22} + m_{1,26} + m_{0,25} + m_{0,23} = 0$
<sup>s</sup> 103	<sup>a</sup> 16,6	$m_{15,6} = 1$
\$102		$m_{15,5} = 1$
\$100 \$100	a16.2	$m_{15,4} + m_{12,5} + m_{10,4} + m_{4,5} + m_{4,4} + m_{2,5} + m_{2,4} - 1$ $m_{15,2} + m_{12,5} + m_{11,5} + m_{10,4} + m_{10,2} + m_{8,4} + m_{8,3} + m_{7,3} + m_{5,5}$
100	210,2	$+m_{5,3} + m_{4,5} + m_{4,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{0,3} = 1$
\$99	<sup><i>u</i></sup> 16,1	$m_{15,1} + m_{12,5} + m_{11,3} + m_{11,2} + m_{10,4} + m_{10,2} + m_{9,2} + m_{8,3} + m_{8,2} + m_{5,4} + m_{4,5} + m_{4,4} + m_{4,0} + m_{3,31} + m_{3,4} + m_{3,2} + m_{2,5} + m_{2,4} + m_{2,3}$
		$+m_{1,31} + m_{0,3} = 0$ (3) (3) (3) (3) (3) (3) (3) (3) (3) (3)
<sup>s</sup> 98	a16,0	$m_{15,0} + m_{1,0} = 1$
<sup>\$</sup> 97	$a_{15,30}$	$ \begin{array}{l} 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 \end{array} $
<sup>s</sup> 96	a15,25	$m_{15,30} = 1$
<sup>\$95</sup>	a14,26	$m_{14,31} = 0$
<sup>s</sup> 94	a14,25	$m_{14,30} = 1$
<sup>8</sup> 93	a15,29	$m_{14,29} = 0$ $m_{14,09} + m_{0,09} + m_{0,09} + m_{1,09} = 0$
592 591	a15.28	$m_{14,28} + m_{9,28} + m_{6,29} + m_{3,28} + m_{1,28} = 0$ $m_{14,27} + m_{12,28} + m_{9,27} + m_{7,29} + m_{6,28} + m_{4,28} + m_{3,27} + m_{1,27} = 0$
s90	<sup>a</sup> 15,26	$m_{14,26} + m_{12,27} + m_{10,28} + m_{9,28} + m_{9,26} + m_{7,28} + m_{6,27} + m_{4,28} + m_{4,27}$
	,	$+m_{3,26} + m_{2,28} + m_{1,26} = 1$
<sup>s</sup> 89	$a_{15,24}$	$m_{14,24} + m_{12,27} + m_{12,25} + m_{11,28} + m_{10,27} + m_{10,26} + m_{9,26} + m_{9,24} + m_{8,29}$
		$+m_{7,26} + m_{6,29} + m_{6,25} + m_{5,28} + m_{4,28} + m_{4,26} + m_{4,25} + m_{3,28} + m_{3,24} + m_{2,26} + m_{1,24} + m_{0,28} = 0$
<sup>s</sup> 88	a15,23	$m_{14,23} + m_{12,26} + m_{12,24} + m_{11,27} + m_{10,26} + m_{10,25} + m_{9,28} + m_{9,25} + m_{9,23}$
		$+m_{8,28} + m_{7,25} + m_{6,28} + m_{6,24} + m_{5,27} + m_{4,27} + m_{4,25} + m_{4,24} + m_{3,28} + m_{3,27} + m_{4,27} + m_{4,25} + m_{4,24} + m_{3,28} + m_{3,27} + m_{4,27} + m_{4,27} + m_{4,27} + m_{4,27} + m_{4,28} + m_{3,28} + m_{3,28} + m_{3,27} + m_{4,28} + m_{4,28}$
S87	a15.22	$+m_{3,23} + m_{2,25} + m_{1,28} + m_{1,23} + m_{0,27} - 1$ $m_{14,22} + m_{13,20} + m_{12,25} + m_{12,24} + m_{12,23} + m_{11,28} + m_{11,23} + m_{11,21} + m_{10,27}$
01	10,22	$+m_{9,26} + m_{9,24} + m_{9,23} + m_{8,29} + m_{8,27} + m_{8,26} + m_{8,25} + m_{8,22} + m_{8,20}$
		$+m_{7,26} + m_{7,25} + m_{6,29} + m_{6,23} + m_{6,22} + m_{5,28} + m_{5,25} + m_{5,21} + m_{4,28}$
		$+m_{4,26} + m_{4,25} + m_{4,23} + m_{3,28} + m_{3,24} + m_{3,21} + m_{2,26} + m_{2,20} + m_{1,24}$
800	0.15 24	$\pm m_{0,28} \pm m_{0,25} \pm m_{0,20} = 1$ $m_{14,21} \pm m_{12,27} \pm m_{12,24} \pm m_{12,22} \pm m_{14,27} \pm m_{16,22} \pm m_{16,27} \pm m_{16,27} \pm m_{16,24}$
~86	~15,21	$m_{14,21} + m_{12,24} + m_{12,24} + m_{12,22} + m_{11,25} + m_{10,28} + m_{10,27} + m_{10,24} + m_{10,24} + m_{10,28} + m_{9,28} + m_{9,26} + m_{9,23} + m_{9,21} + m_{8,29} + m_{8,26} + m_{7,26} + m_{7,28}$
		$+m_{7,23} + m_{6,29} + m_{6,26} + m_{6,22} + m_{5,25} + m_{4,28} + m_{4,27} + m_{4,25} + m_{4,23}$
		$+m_{4,22} + m_{3,26} + m_{3,25} + m_{3,21} + m_{2,28} + m_{2,23} + m_{1,26} + m_{1,21} + m_{0,25} = 0$
<sup>s</sup> 85	a15,20	$m_{14,20} + m_{12,26} + m_{12,23} + m_{12,21} + m_{11,28} + m_{11,24} + m_{10,28} + m_{10,27}$
		$+m_{10,26} + m_{10,23} + m_{10,22} + m_{9,27} + m_{9,25} + m_{9,22} + m_{9,20} + m_{8,28} + m_{8,25}$
		$+m_{4,24} + m_{4,22} + m_{4,21} + m_{3,28} + m_{3,25} + m_{3,24} + m_{3,20} + m_{2,27} + m_{2,27} + m_{4,27} + m_{4,26}$
		$+m_{1,20} + m_{0,28} + m_{0,24} + m_{47,31} = 1$

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

Control	Control	Controlled relation $r_i$
sequence	bit	
s <sub>i</sub>	<i>bi</i>	
<sup>s</sup> 84	$a_{15,5}$	$m_{14,5} + m_{8,5} + m_{6,5} = 1$
<sup>s</sup> 83	$a_{15,4}$	$m_{14,4} + m_{12,5} + m_{11,3} + m_{11,2} + m_{10,4} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2}$
		$+m_{8,5}+m_{7,2}+m_{6,5}+m_{6,4}+m_{5,4}+m_{5,2}+m_{4,5}+m_{4,4}+m_{4,0}+m_{3,31}$
		$+m_{3,4} + m_{3,2} + m_{2,5} + m_{2,3} + m_{2,2} + m_{1,31} + m_{0,4} + m_{0,3} + m_{0,2} = 1$
<sup>s</sup> 82	$a_{14,30}$	$m_{14,3} + m_{11,3} + m_{11,2} + m_{8,2} + m_{7,4} + m_{7,2} + m_{7,1} + m_{6,2} + m_{5,3}$
		$+m_{4,0} + m_{3,3} + m_{2,2} + m_{1,31} + m_{1,3} = 0$
<sup>s</sup> 81	$a_{15,2}$	$m_{14,2} + m_{12,5} + m_{12,3} + m_{10,4} + m_{9,2} + m_{7,4} + m_{6,3} + m_{4,5} + m_{4,4}$
	,	$+m_{4,3} + m_{3,2} + m_{2,5} + m_{2,4} + m_{1,2} = 1$
<sup>\$80</sup>	a15.1	$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_{7,2} + $
	,-	$m_{5,2} + m_{4,4} + m_{3,31} + m_{3,4} + m_{3,2} + m_{3,1} + m_{2,4} + m_{2,3} + m_{0,3} = 0$
<sup>\$79</sup>	$a_{14.27}$	$m_{14,0} = 0$
\$78	a13.26	$m_{13,31} = 0$
\$77	a13 25	$m_{13,30} = 0$
\$76	a14 20	$m_{12,20} + m_{2,20} = 0$
\$75	a14.29	$m_{12} \circ m_{22} \circ m$
874	<i>a</i> 12,20	$13,25 + 5,25 + 2,25 + 0,25 + m_{2},27 + m_{2},00 + m_{5},00 + m_$
874 870	a13,22	$m_{13,27} + m_{11,28} + m_{8,29} + m_{8,27} + m_{6,29} + m_{5,28} + m_{3,28} + m_{2,27} + m_{0,27} - 1$
373	a13,21	$m_{13,26} + m_{11,27} + m_{9,28} + m_{8,28} + m_{8,26} + m_{6,28} + m_{5,27} + m_{3,28} + m_{3,27}$
		$+m_{2,26} + m_{1,28} + m_{0,26} - 1$
<sup>\$72</sup>	$a_{14,24}$	$m_{13,24} + m_{12,28} + m_{11,27} + m_{11,25} + m_{10,28} + m_{9,27} + m_{9,26} + m_{8,29} + m_{8,26}$
		$+m_{8,24} + m_{7,29} + m_{7,28} + m_{6,26} + m_{5,25} + m_{4,28} + m_{3,28} + m_{3,26} + m_{3,25} + m_{2,28}$
		$+m_{2,24} + m_{1,28} + m_{1,26} + m_{0,24} = 0$
<sup>s</sup> 71	$a_{14,23}$	$m_{13,23} + m_{12,27} + m_{11,26} + m_{11,24} + m_{10,28} + m_{10,27} + m_{9,26} + m_{9,25} + m_{8,29} + m_{10,27} + m_{10,2$
		$m_{8,28} + m_{8,25} + m_{8,23} + m_{7,29} + m_{7,28} + m_{7,27} + m_{6,25} + m_{5,28} + m_{5,24} + m_{4,28}$
		$+m_{4,27} + m_{3,27} + m_{3,25} + m_{3,24} + m_{2,27} + m_{2,23} + m_{1,27} + m_{1,25} + m_{0,28} + m_{0,23} = 0$
<sup>s</sup> 70	$a_{14,22}$	$m_{13,22} + m_{12,26} + m_{11,28} + m_{11,25} + m_{11,23} + m_{10,27} + m_{10,26} + m_{9,28} + m_{9,25}$
		$+m_{9,24} + m_{8,28} + m_{8,27} + m_{8,24} + m_{8,22} + m_{7,28} + m_{7,27} + m_{7,26} + m_{6,29} + m_{6,24}$
		$+m_{5,28} + m_{5,27} + m_{5,23} + m_{4,27} + m_{4,26} + m_{3,28} + m_{3,26} + m_{3,24} + m_{3,23} + m_{2,28}$
		$+m_{2,26} + m_{2,22} + m_{1,26} + m_{1,24} + m_{0,28} + m_{0,27} + m_{0,22} = 1$
<sup>s</sup> 69	a13,0	$m_{13,6} = 0$
<sup>s</sup> 68	$a_{14,5}$	$m_{13,5} + m_{12,5} + m_{5,5} + m_{4,5} + m_{2,5} = 0$
<sup>s</sup> 67	$a_{14,4}$	$m_{13,4} + m_{12,5} + m_{11,2} + m_{10,4} + m_{7,4} + m_{5,4} + m_{5,3} + m_{5,2} + m_{4,5} + m_{4,4} + m_{3,31}$
	,	$+m_{2,5} + m_{2,4} + m_{2,2} + m_{1,2} = 0$
<sup>s</sup> 66	$a_{14,3}$	$m_{13,3} + m_{8,3} + m_{5,4} + m_{3,4} + m_{2,3} + m_{0,3} = 0$
<sup>8</sup> 65	a13.28	$m_{13,2} + m_{10,3} + m_{10,2} + m_{10,1} + m_{9,2} + m_{8,2} + m_{7,4} + m_{7,2} + m_{4,0} + m_{3,4} + m_{3,3}$
		$+m_{3,2} + m_{2,3} + m_{2,2} + m_{1,31} + m_{1,2} + m_{0,3} = 0$
<sup>s</sup> 64	a14.1	$m_{13,1} + m_{10,2} + m_{9,3} + m_{8,3} + m_{7,4} + m_{7,2} + m_{6,2} + m_{5,3} + m_{5,2} + m_{4,0} + m_{3,4}$
Ŭ.	1 1,1	$+m_3 + m_2 + m_1 + m_1 + m_1 = 0$

Control	Control	Controlled relation $r_i$
sequence	bit	
s <sub>i</sub>	$b_i$	
<sup>s</sup> 63	$a_{14,0}$	$m_{13,0} + m_{1,31} = 1$
<sup>s</sup> 62	$a_{12,26}$	$m_{12,31} = 1$
<sup>s</sup> 61	$a_{13,30}$	$m_{12,30} \equiv 0$
<sup>s</sup> 60	$a_{12,24}$	$m_{12,29} = 1$
<sup>s</sup> 59	$a_{12,27}$	$m_{12,0} + m_{4,0} + m_{3,0} + m_{1,31} + m_{1,0} = 0$
<sup>s</sup> 58	$a_{11,26}$	$m_{11,31} = 1$
<sup>\$57</sup>	$a_{12,30}$	$m_{11,30} = 0$
<sup>s</sup> 56	$a_{11,24}$	$m_{11,29} = 1$
<sup>s</sup> 55	$a_{12,5}$	$m_{11,6} = 1$
<sup>s</sup> 54	a11,0	$m_{11,6} = 1$
s53	$a_{12,4}$	$m_{11,4} = 1$
<sup>s</sup> 52	$a_{12,1}$	$m_{11,1} = 1$
<sup>s</sup> 51	$a_{12,0}$	$m_{11,0} + m_{1,31} = 0$
<sup>s</sup> 50	$a_{10,26}$	$m_{10,31} = 0$
s49	$a_{11,30}$	$m_{10,30} = 0$
<sup>s</sup> 48	$a_{10,24}$	$m_{10,29} = 0$
<sup>s</sup> 47	$a_{11,5}$	$m_{10,6} = 0$
<sup>s</sup> 46	$a_{10,0}$	$m_{10,5} + m_{4,5} + m_{2,5} = 0$
s45	$a_{10,27}$	$m_{10,0} + m_{4,0} + m_{1,0} = 0$
$s_{44}$	$a_{9,26}$	$m_{9,31} + m_{3,31} + m_{3,0} + m_{1,0} = 1$
<sup>s</sup> 43	$a_{9,25}$	$m_{9,30} = 0$
<sup>s</sup> 42	$a_{10,30}$	$m_{9,30} = 0$
<sup>s</sup> 41	$a_{9,24}$	$m_{9,29} = 1$
s40	$a_{9,0}$	$m_{9,6} = 0$
s39	$^{a_{4,8}}$	$m_{9,6} = 0$
s38	$a_{10,5}$	$m_{9,5} + m_{8,5} + m_{6,5} + m_{3,5} = 0$
<sup>s</sup> 37	$a_{10,4}$	$m_{9,4} = 1$
<sup>s</sup> 36	$a_{9,28}$	$m_{9,1} = 1$
s35	$a_{9,27}$	$m_{9,0} + m_{3,0} + m_{1,0} = 0$
<sup>s</sup> 34	$a_{8,26}$	$m_{8,31} = 0$
<sup>s</sup> 33	$a_{9,29}$	$m_{8,30} = 1$
<sup>s</sup> 32	$a_{8,28}$	$m_{8,1} = 0$
<sup>s</sup> 31	$a_{8,27}$	$m_{8,0} = 0$
s30	a8,31	$m_{7,31} + m_{3,31} + m_{1,31} + m_{1,0} = 0$
<sup>s</sup> 29	$a_{8,29}$	$m_{7,30} = 1$
<sup>s</sup> 28	$a_{8,4}$	$m_{7,5} = 1$
<sup>s</sup> 27	$a_{6,6}$	$m_{7,5} = 1$

Control	Control	Controlled relation $r_i$
sequence	bit	
$s_i$	$b_i$	
<sup>s</sup> 26	$a_{8,0}$	$m_{7,0} + m_{3,0} = 0$
<sup>s</sup> 25	$a_{7,31}$	$m_{6,31} = 0$
<sup>s</sup> 24	$a_{7,29}$	$m_{6,30} = 0$
<sup>s</sup> 23	$a_{3,26}$	$m_{5,31} + m_{3,31} = 0$
<sup>s</sup> 22	$a_{5,25}$	$m_{5,30} = 1$
s21	$a_{6,29}$	$m_{5,29} = 1$
<sup>s</sup> 20	$a_{6,1}$	$m_{5,1} = 1$
<sup>s</sup> 19	$a_{3,27}$	$m_{5,0} + m_{3,0} + m_{1,31} = 1$
<sup>s</sup> 18	$a_{4,26}$	$m_{4,31} = 0$
<sup>s</sup> 17	$a_{4,25}$	$m_{4,30} = 0$
<sup>s</sup> 16	$a_{5,29}$	$m_{4,29} = 0$
<sup>s</sup> 15	$a_{5,6}$	$m_{4,6} = 0$
<sup>s</sup> 14	$a_{5,1}$	$m_{4,1} = 1$
<sup>s</sup> 13	$a_{3,25}$	$m_{3,30} = 1$
<sup>s</sup> 12	$a_{3,24}$	$m_{3,29} = 0$
<sup>s</sup> 11	$a_{4,6}$	$m_{3,6} = 1$
<sup>s</sup> 10	$a_{2,26}$	$m_{2,31} = 0$
<i>s</i> 9	$a_{2,25}$	$m_{2,30} = 1$
<sup>s</sup> 8	$a_{2,24}$	$m_{2,29} = 0$
s7	$a_{3,5}$	$m_{2,6} = 1$
<sup>s</sup> 6	$a_{2,6}$	$m_{2,6} = 1$
<sup>s</sup> 5	$a_{3,1}$	$m_{2,1} = 1$
<sup>s</sup> 4	$a_{2,5}$	$m_{1,5} = 0$
<sup>s</sup> 3	$a_{1,28}$	$m_{1,1} = 1$
<sup>s</sup> 2	$a_{1,25}$	$m_{1,30} = 0$
<sup>s</sup> 1	$a_{1,24}$	$m_{1,29} = 1$
<sup>s</sup> 0	a1,23	$m_{1,29} = 1$

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

- '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.

In this case, the set of bits corresponding to 'q' is exactly same to the set of *adjusters*.

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  $\{m_{i,j}\}_{i=0,1,\dots,15; j=0,1,\dots,31}$  according to the order defined as  $m'_{i',i'} \leq m_{i,j}$  if  $i' \leq i$  or (i' =i and  $j' \leq j$ ). By the proposed method we have succeeded in modifying message so that all sufficient conditions on message  $\{m_{i,j}\}$  and some sufficient conditions on chaining variable  $\{a_{ij}\}$  of first 23 rounds. Still 34 conditions remain as listed below:  $a_{17,3} = 1, a_{17,2} =$  $0, a_{17,1} = 0, a_{26,1} = 1, a_{27,0} = 1, a_{29,1} = 0, a_{30,1} = 0$  $0, a_{33,1} = 1, a_{37,1} = 1, a_{39,1} = 0, a_{41,1} = 0, a_{43,1} =$  $0, a_{20,30} + a_{18,0} = 1, a_{21,30} + a_{20,0} = 0, a_{24,30} + a_{20,0} = 0, a_{24,30} + a_{20,30} + a_{20,3$  $a_{22,0} = 0, a_{25,30} + a_{24,0} = 1, a_{25,3} + a_{24,3} =$  $0, a_{26,2} + a_{25,2} = 1, a_{28,30} + a_{26,0} = 0, a_{28,3} + a_{2$  $a_{27,3} = 1, a_{29,30} + a_{28,0} = 1, a_{29,3} + a_{28,3} =$  $1, a_{32,3} + a_{31,3} = 1, a_{36,3} + a_{35,3} = 1, a_{38,3} + a_{38,3} = 1, a_{38,3} + a_{38$  $a_{37,3} = 1, a_{39,31} + a_{38,1} = 1, a_{40,3} + a_{39,3} =$  $1, a_{40,31} + a_{38,1} = 1, a_{41,31} + a_{40,1} = 1, a_{42,31} + a_{40,1} = 1, a_{42,31} + a_{40,31} + a_{40,3$  $a_{40,1} = 1, a_{43,31} + a_{42,1} = 1, a_{42,3} + a_{41,3} =$  $1, a_{44,31} + a_{42,1} = 1, a_{45,31} + a_{44,1} = 1.$ 

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 basic message modification (used in Step 2 of Algorithm 2) is  $1/2^5$ .

To adjust other 29 conditions, we use semineutral bits as we described in Algorithm 2.

### 6.4 New Collisions

Using Algorithm 2 (essentially, using semineutral bits showed in Table 6 to adjust the above remaining 29 conditions), we found many collisions of 58-round SHA-1 as follows. As we show in Table 6, we have 21 semi-neutral bits and 16 adusters. Here we show some of new collisions we found. They are new collisions different from Wang's result. For other examples of new collisions, see [13].

- $m = 0x1ead6636319fe59e4ea7ddcbc7961642 \\ 0ad9523af98f28db0ad135d0e4d62aec \\ 6c2da52c3c7160b606ec74b2b02d545e \\ bdd9e4663f1563194f497592dd1506f9$
- $\begin{array}{lll} m' &=& 0x3ead6636519fe5ac2ea7dd88e7961602 \\ && ead95278998f28d98ad135d1e4d62acc \\ && 6c2da52f7c7160e446ec74f2502d540c \\ && 1dd9e466bf1563596f497593fd150699 \end{array}$
- $m = 0x16507a963da18c5f4195d14bd55695ea \\ 0cb08092f79649bb0717a22658c119fc \\ 5a36c1f8b960383b08929187ae9842fa \\ b690d8710452419d585d012edcaf0278$
- $\begin{array}{lll} m' &=& 0x36507a965da18c6d2195d108f55695aa \\ & ecb080d0979649b98717a22758c119dc \\ & 5a36c1fbf9603869489291c74e9842a8 \\ & 1690d871845241dd785d012ffcaf0218 \end{array}$

#### 6.5 Complexity

When we use the basic message modification which we described in Algorithm 1, the complexity to find a collision for 58-round SHA-1 is  $2^{29}$  message modifications (equivalent to  $2^{31}$  SHA-1 computation experimentally) because there 29 remaining conditions after message modifications, whereas Wang's method needs  $2^{34}$  message modifications and  $2^{34}$  SHA-1 computation.

Now we consider the complexity when we use the improved message modification proposed as Algorithm 2. Since there are 5 remaining conditions which should be tested in Step 3, the probability that the output of Step 2 pass the test of Step 3 is  $1/2^5$ . And since there are 29 remaining conditions after Step 3 and we have 21 semi-neutral bits, the probability that the modified message in Step 4 pass the final test of Step 4 is  $1/2^8$ . Hence when we use Algorithm 2, we have the complexity to find a collision for 58-round SHA-1 is  $2^8$  message modifications experimentally, because Step 4 is a dominant part of the algorithm. However, the real complexity to find a collision for 58-round SHA-1 in our latest implementation is  $2^{31}$  SHA-1 computation, i.e. one improved message modification is  $2^{23}$  heavier than the one of Algorithm 1. However, using sophisticated techniques of error correcting code (list decoding, iterative decoding, etc.) and Gröbner basis, it can be faster. Similarly, in the case of full-round SHA-1, we can use the same technique. The problem is that number of semi-neutral bits is much smaller than the case 58-round SHA-1. In this case one message modification is much heavier than the case of 58-round SHA-1. Implementation of such sophisticated technique is the future problem.

## 7 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. Particularly, via the computer experiments employing 58-round SHA-1 we have shown, by finding new collisions, that our algorithm is a very efficient one. The proposed method improves the complexity of finding collision for 58-round SHA-1 from 2<sup>34</sup> SHA-1 computation to  $2^{31}$ . The complexity can be reduced to  $2^8$ message modification by using our improved message modification technique, even though complexity of one message modification appears as a high one implying a request for employment of the more sophisticated methods for error-correcting and Gröbner basis.

## Acknowledgement The authors would

like to thank Prof. Adi Shamir and Prof. Miodrag Mihaljevic for giving many useful comments on our manuscript.

## References

- Hans Dobbertin, "Cryptanalysis of MD4." Fast Software Encryption 1996: 53-69
- [2] X. Y. Wang etc, "An Attack on Hash Function HAVAL-128," Science in China Series E.
- [3] L. C. K. Hui, X. Y. Wang etc, The Differential Analysis of Skipjack Vari-

ants from the first Round, Advance in Cryptography–CHINACRYPT'2002, Science Publishing House.

- [4] Xiaoyun Wang, "Collisions for Some Hash Functions MD4, MD5,HAVAL-128,RIPEMD," Rump Session in Crypto'04, E-print.
- [5] X. Y. Wang, "The Improved Collision attack on SHA-0", 1998.
- [6] X. Y. Wang, "The Collision attack on SHA-0," 1997.
- [7] Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, Xiuyuan Yu "Cryptanalysis of the Hash Functions MD4 and RIPEMD." EUROCRYPT 2005: 1-18
- [8] Xiaoyun Wang, Hongbo Yu: How to Break MD5 and Other Hash Functions. EUROCRYPT 2005: 19-35
- [9] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, William Jalby "Collisions of SHA-0 and Reduced SHA-1." EUROCRYPT 2005: 36-57
- [10] Eli Biham, Rafi Chen "Near-Collisions of SHA-0." CRYPTO 2004: 290-305
- [11] Antoine Joux, "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions." CRYPTO 2004: 306-316
- [12] Florent Chabaud, Antoine Joux "Differential Collisions in SHA-0." CRYPTO 1998: 56-71
- [13] M. Sugita, M. Kawazoe and H. Imai "Gröbner basis based cryptoanalysis of SHA-1", IACR Cryptology ePrint Archive 2006/098, http://eprint.iacr.org/2006/098,
- [14] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin, "Efficient Collision Search Attacks on SHA-0," CRYPTO2005 1-16
- [15] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, "Finding Collisions in the Full SHA-1," CRYPTO 2005, 17-36

# Appendix: How to find good message differential

As we stated in Section 2, a choice of "differential without carry" is very important. Here we show how to find good "differential without carry" and good "message differential" with low Hamming weight.

Our strategy is as follows.

- Find a message differential in which difference appears only on continuing 4bits. 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. 1, Fig. 2. By our experiments, Wang's disturbance vector seems a best possible one.

i	$\Delta^+ m$	$\Delta^{-}m$	i	$\Delta^+ m$	$\Delta^{-}m$
0	20000000	0	29	2	40000040
1	40000020	20000012	30	40000002	40
2	20000000	40000043	31	2	40000000
3	20000000	40	32	0	2
4	e0000040	2	33	40	0
5	0	60000002	34	80000000	2
6	80000001	0	35	80000000	0
7	0	20	36	0	80000002
8	3	0	37	40	80000000
9	40000040	12	38	0	0
10	40000040	0	39	80000000	40
11	40000000	a0000052	40	0	80000000
12	0	a0000000	41	0	40
13	80000040	0	42	0	80000000
14	20000001	0	43	0	40
15	20000000	60	44	0	80000002
16	80000001	0	45	0	0
17	40000002	40	46	0	80000000
18	c0000002	41	47	80000000	0
19	40000000	22	48	0	0
20	0	3	49	0	0
21	40000040	2	50	0	0
22	80000041	40000002	51	0	0
23	2	c0000020	52	0	0
24	1	0	53	0	0
25	0	40000002	54	0	0
26	40000041	80000002	55	0	0
27	42	40000020	56	0	0
28	1	8000000	57	0	0

Table. A message-differential of continuous 4-round



Figure 1: Finding good disturbance vector (I)



Figure 2: Finding good disturbance vector (II)