Musings on the Wang *et al.* MD5 Collision

Philip Hawkes[1], Michael Paddon[1], and Gregory G. Rose[1]

Qualcomm Australia, Level 3, 230 Victoria Rd, Gladesville, NSW 2111, Australia
{phawkes,mwp,ggr}@qualcomm.com

Abstract. Wang et al [12] caused great excitement at CRYPTO2004 when they announced a collision for MD5 [11]. This paper is examines the internal differences and conditions required for the attack to be successful. There are a large number of conditions that must be satisfied, thus indicating Wang at al. have found a clever way to generate message pairs for which the conditions are satisfied. The large number of conditions suggests that an attacker cannot use these differentials to cause second pre-image attacks with complexity less than generic attacks. Initial examination also suggests that an attacker cannot cause such collisions for HMAC-MD5 [9] with complexity less than generic attacks.
Keywords: MD5, collision.

Disclaimer: This document notes some observations of the authors regarding the collisions generated by Wang et al.. We do not claim to have any new discoveries in this paper. However, we hope that this paper provides a useful explanation until the time when Wang et al. publish a detailed analysis of their discoveries. This is a very rough description and is not intended as a publication. There has been a focus more on content than presentation.

1 Introduction

The cryptographic hash algorithm MD5 [11] needs little introduction. The MD5 collision found by X. Wang, D. Feng, X. Lai and H. Yu [12] is almost as well known as MD5 itself!

Following the announcement of the MD5 collision, we spent some time studying the MD5 collision in order to glean useful hints for our ongoing analysis of SHA-2 family [5]. At first, the collision seemed to difficult to comprehend: the XOR-based differences have high weight (which seemed counter-intuitive) and the addition-based differences do not seem to follow any obvious pattern. We are still amazed that someone found this sequences of differences! It will be enlightening to see how it was discovered.

The collision uses a differential that is spread over a length of two message blocks. The first block difference results in a small difference in the state, and the second block difference cancels the introduced difference. For each of these blocks, the internal differentials are very similar. Unfortunately, we have only had sufficient time to fully document the internal differential for the first block.

Tables in Appendix B contain the details of the internal differential for the second block, but without any explanatory text.

This paper is arranged as follows. Section 3 contains some basic notation, with Section 3 containing a description of the MD5 algorithm. We use an unorthodox description, as it better suits our analysis and (I think) leads to a better understanding of the algorithm. Section 4 describes the sequence of addition-based differences that form the internal differential for the first block. Section 4 also considers the conditions required for the cyclic rotation to produce the correct add-differences. Section 5 considers the conditions required for the non-linear functions f_t to produce the correct add-differences. By combining the conditions stated in Section 4 and Section 5, we can determine the complexity for various attacks. The Appendices contains tables with the details of the internal differential for the first and second block.

Our results indicate that the differential can be used for:

- a collision attack with complexity $2^{42.2}$;
- a second pre-image attack with complexity 2^{285};
- a 2^{128} complexity collision attack on HMAC-MD5 with unknown key;
- a $2^{42.2}$ complexity collision attack on HMAC-MD5 with known key;

Given how fast Wang at al. can generate a collision (1 hour) it seems likely that they have founds some additional tricks to use for finding collisions.

2 Notation

MD5 is based on 32-bit words. Within each word, the most significant bit (MSB) is the leftmost bit while the least significant bit (LSB) is the rightmost bit. Where words must be formed from octet-oriented data, MD5 uses Least Significant Byte first (little endian, c.f. Intel 80386), whereas SHA algorithms [3] use Most Significant Byte first (big endian, c.f. SPARC).

The i-th bit of a word a is denoted $a[i]$. MD5 uses three bit-wise operators: "$\wedge$" represents the bitwise AND operation with $(a \wedge b)[i] = a[i] \wedge b[i]$, $0 \leq i \leq 31$; "$\vee$" represents the bitwise OR operation with $(a \vee b)[i] = a[i] \vee b[i]$, $0 \leq i \leq 31$; and "$\oplus$" represents the bitwise exclusive-OR operation with $(a \oplus b)[i] = a[i] \oplus b[i]$, $0 \leq i \leq 31$. MD5 also uses addition modulo 2^{32}, which is denoted using "+". Subtraction modulo 2^{32} is denoted using "−".

The bit-wise complement of x (equal to $2^{32} - 1 - x$) is denoted $\overline{x}$. The function $ROTL^r(X)$ produces a word of the same size as X, but with the bits rotated cyclically to the left by r positions. That is, if $Y = ROTL^r(X)$, then $Y[i] = X[i - r (\text{mod } 32)]$, $0 \leq i \leq 31$.

In a situation where we want to consider several bit positions $X[a]$, $X[b]$, $X[c]$, $X[d]$ of value X simultaneously, then we may combine these values into a vector $(X[a], X[b], X[c], X[d])$ and use the notation:

$$X[a, b, c, d] = (X[a], X[b], X[c], X[d]).$$

We always write the bits in descending order. If some bits are adjacent we may combine them, for example:

$$X[a-b,c] = (X[a], X[a-1], \ldots, X[b+1], X[b], X[c]).$$

If we want to say that a set of bit positions are set to a specific value, then we may write, for example

$$X[a-b,c] = 1, \quad \Leftrightarrow \\ X[a] = 1; X[a-1] = 1, \ldots, X[b+1] = 1; X[b] = 1; X[c] = 1.$$

3 Description of MD5

I shall use an unorthodox description for MD5 (the description is unorthodox in comparison to [11]).
Padding: The message is padded and has its length in bits appended to make a multiple of 512 bits.

Parsing: The padded message is parsed into 512-bit blocks, $M^{(1)}, \ldots, M^{(N)}$. Each 512-bit input block is expressed as sixteen 32-bit words $M_0^{(i)}, \ldots, M_{15}^{(i)}$.

Message Expansion: The message expansion is applied to each message block individually. This is similar in principal to the key scheduling for a modern block cipher. The message expansion results in a series of 64 words $\{W_t\}$:

$$W_t = \begin{cases} M_t^{(i)}, & 0 \le t \le 15; \\ M_{1+5t(\mathrm{mod} 16)}^{(i)}, & 16 \le t \le 31; \\ M_{5+3t(\mathrm{mod} 16)}^{(i)}, & 32 \le t \le 47; \\ M_{7t(\mathrm{mod} 16)}^{(i)}, & 48 \le t \le 63. \end{cases}$$

Note that for each r, $0 \le r \le 3$, the values of $\{W_{16r+0}, \ldots, W_{16r+15}\}$ form a permutation of the message block words.

Register Update:

The hash function maintains 4 words of state for the intermediate hash value $IHV^{(i)}[0]$, $IHV^{(i)}[1]$, $IHV^{(i)}[2]$, $IHV^{(i)}[3]$, where $IHV^{(i)}$ denotes the value of the intermediate hash value before hashing the i-th 512-bit block. The 4 words $IHV^{(0)}[j]$ are initialized to pre-determined constants.

The algorithm has a working register with 4 words of state Q_t, Q_{t-1}, Q_{t-2}, Q_{t-3}. These values are initialized to

$$Q_0 = IHV^{(i)}[1], Q_{-1} = IHV^{(i)}[2], Q_{-2} = IHV^{(i)}[3], Q_{-3} = IHV^{(i)}[0].$$

The unusual order of initialization is due to our description of the algorithm, but it is still an accurate translation of the algorithm.

Following initialization, 64 rounds of the round function are applied to the expanded input sequence $\{W_t\}$. The round function modifies the register based on the values of an input word $W_t \in GF(^{32})$, a rotation amount denoted $S(t) \in [0, 31]$, and a pre-determined constant word $AC_t \in GF(2^{32})$. The rotation amounts $S(t)$ can be seen in Table 1. The constant words AC_t are found in the MD5 specification [11]. The compression function uses addition modulo 2^{32}, left rotation by the amount $S(t)$ and a round-dependent nonlinear function $f_t(X, Y, Z)$ where:

$$f_t(X,Y,Z) = \begin{cases} F(X,Y,Z) = (X \wedge Y) \oplus (\overline{X} \wedge Z), & 0 \leq t \leq 15; \\ G(X,Y,Z) = (Z \wedge X) \oplus (\overline{Z} \wedge Y), & 16 \leq t \leq 31; \\ H(X,Y,Z) = X \oplus Y \oplus Z, & 32 \leq t \leq 47; \\ I(X,Y,Z) = Y \oplus (X \vee \overline{Z}), & 48 \leq t \leq 63. \end{cases}$$

All the inputs and outputs of these round-dependent functions are 32-bit values.

The compression function modifies the register as follows:

$$T_t = f_t(Q_t, Q_{t-1}, Q_{t-2}) + Q_{t-3} + AC_t + W_t;$$
$$R_t = ROTL^{S(t)}(T_t); \quad Q_{t+1} = Q_t + R_t.$$

After all 64 input words have been input to the register, the resulting values of the state are added modulo 2^{32} to the initialized values of the state, according to the Davies-Meyer construction [10]:

$$IHV^{(i+1)}[1] = IHV^{(i)}[1] + Q_{64}, \; IHV^{(i+1)}[2] = IHV^{(i)}[2] + Q_{63},$$
$$IHV^{(i+1)}[3] = IHV^{(i)}[3] + Q_{62}, \; IHV^{(i+1)}[0] = IHV^{(i)}[0] + Q_{61}.$$

These values become the new intermediate hash value. If this is the last message block, the new intermediate hash value is output as the resulting message digest. Otherwise, the algorithm proceeds to updating the register using the next message block.

4 The Differentials

We concentrate mainly on add-differences $\delta X = X^* - X \pmod{2^{32}}$: add-differences are so-called because the differences are formed relative to the modular addition group operation. We also look at XOR-differences $\Delta X = X^* \oplus X$, as both differences are useful. As noted in [5], if $\Delta X = \lambda$, then δX can be determined if $X[i]$ is known for every $i < 31$ such that $\lambda[i] = 1$.[1] That is, if the attacker predicts the bits of X at the positions where $\widehat{\lambda}[i] = 1$, then the attacker also predicts δX.

4.1 Message Expansion

The collision uses a pair of messages with each message consisting of two message blocks of data with the first message containing the blocks $M|N$ and

[1] The attacker need not guess $X[31]$ to determine δX, since differences in the most significant bit always contribute an add-difference of 2^{31}.

the second message containing blocks M^*, N^*. When parsed into 32-bit words, $M_0, \ldots, M_{15} | N_0, \ldots, N_{15}$ and $M_0^*, \ldots, M_{15}^* | N_0^*, \ldots, N_{15}^*$, these values satisfy:

$$\begin{array}{c} M_4^* - M_4 = 2^{31},\ M_{11}^* - M_{11} = 2^{15},\ M_{14}^* - M_{14} = 2^{31},\ M_i^* = M_i \text{ otherwise}, \\ N_4^* - N_4 = 2^{31},\ N_{11}^* - N_{11} = -2^{15},\ N_{14}^* - N_{14} = 2^{31},\ N_i^* = N_i \text{ otherwise}. \end{array}$$

The message expansion transforms the message block into the input word sequence W_t, $0 \le t \le 63$. For the first message blocks M and M^*, the attacker has:

$$\begin{aligned} W_4^* - W_4 = W_{23}^* - W_{23} = W_{37}^* - W_{37} = W_{60}^* - W_{60} &= -2^{31}, \\ W_{11}^* - W_{11} = W_{18}^* - W_{18} = W_{34}^* - W_{34} = W_{61}^* - W_{61} &= +2^{15}, \\ W_{14}^* - W_{14} = W_{25}^* - W_{25} = W_{35}^* - W_{35} = W_{50}^* - W_{50} &= -2^{31}, \end{aligned}$$

and $W_i^* = W_i$ otherwise. For the second message blocks N and N^*, the attacker has:

$$\begin{aligned} W_4^* - W_4 = W_{23}^* - W_{23} = W_{37}^* - W_{37} = W_{60}^* - W_{60} &= -2^{31}, \\ W_{11}^* - W_{11} = W_{18}^* - W_{18} = W_{34}^* - W_{34} = W_{61}^* - W_{61} &= -2^{15}, \\ W_{14}^* - W_{14} = W_{25}^* - W_{25} = W_{35}^* - W_{35} = W_{50}^* - W_{50} &= -2^{31}, \end{aligned}$$

and $W_i^* = W_i$ otherwise.

4.2 First Block of the Differential

It may be easiest to read through the description of the first few rounds to get an idea of how the notation works. I have only looked in detail at the differential for the first blocks (M and M^*).

Due to the structure of the MD5 round function, add-differences propagate through most of the round function with little trouble.

$$\begin{aligned} \delta T_t &= \delta f_t(Q_t, Q_{t-1}, Q_{t-2}) + \delta Q_{t-3} + \delta W_t, \\ \delta Q_{t+1} &= \delta Q_t + \delta R_t. \end{aligned}$$

Furthermore, the difference δR_t can be expressed as $\delta R_t = ROTL^{S(t)}(\delta T_t)$ with high probability. Table 1 on page 6 describes the differential, showing the values of δQ_t, $\delta f_t(Q_t, Q_{t-1}, Q_{t-2})$, δQ_{t-3}, δW_t, δT_t, $S(t)$ and δR_t.

Notation. The columns headed by δQ_t, $\delta f_t(Q_t, Q_{t-1}, Q_{t-2})$, δQ_{t-3}, δW_t, δT_t, and δR_t describe the add-differences between the appropriate values, for example $\delta Q_t = Q_t^* - Q_t \pmod{2^{32}}$. To describe the add-differences in such a small space,

- a difference of the form $+2^j$ is denoted $\overset{+}{j}$, and
- a difference of the form -2^j is denoted $\overset{-}{j}$.

t	δQ_t	δf_t	δQ_{t-3}	δW_t	δT_t	$S(t)$	δR_t
0-3	-	-	-	-	-	.	-
4	-	-	-	$\overset{-}{31}$	$\overset{-}{31}$	7	$\overset{-}{6}$
5	$\overset{-}{6}$	$\overset{+}{19},\overset{+}{11}$	-	-	$\overset{+}{19},\overset{+}{11}$	12	$\overset{+}{31},\overset{+}{23}$
6	$\overset{\pm}{31},\overset{+}{23},\overset{-}{6}$	$\overset{-}{14},\overset{-}{10}$	-	-	$\overset{-}{15},\overset{+}{14},\overset{-}{10}$	17	$\overset{+}{31},\overset{-}{27},\overset{-}{0}$
7	$\overset{-}{27},\overset{+}{23},\overset{-}{6},\overset{-}{0}$	$\overset{-}{27},\overset{-}{25},\overset{+}{16},\overset{+}{10},\overset{+}{5},\overset{-}{2}$	-	-	$\overset{-}{27},\overset{-}{25},\overset{+}{16},\overset{+}{10},\overset{+}{5},\overset{-}{2}$	22	$\overset{+}{27},\overset{-}{24},\overset{-}{17},\overset{-}{15},\overset{+}{6},\overset{+}{1}$
8	$\overset{-}{23},\overset{-}{17},\overset{-}{15},\overset{+}{0}$	$\overset{\pm}{31},\overset{-}{24},\overset{+}{16},\overset{+}{10},\overset{+}{8},\overset{+}{6}$	$\overset{-}{6}$	-	$\overset{-}{31},\overset{-}{24},\overset{+}{16},\overset{+}{10},\overset{+}{8}$	7	$\overset{-}{31},\overset{+}{23},\overset{+}{17},\overset{+}{15},\overset{-}{6}$
9	$\overset{\pm}{31},\overset{-}{6},\overset{+}{0}$	$\overset{\pm}{31},\overset{+}{26},\overset{-}{23},\overset{-}{20},\overset{+}{6},\overset{+}{0}$	$\overset{\pm}{31},\overset{+}{23},\overset{-}{6}$	-	$\overset{+}{26},\overset{-}{20},\overset{+}{0}$	12	$\overset{+}{12},\overset{+}{6},\overset{-}{0}$
10	$\overset{+}{31},\overset{+}{12}$	$\overset{-}{23},\overset{+}{13},\overset{+}{6},\overset{+}{0}$	$\overset{-}{27},\overset{+}{23},\overset{-}{6},\overset{-}{0}$	-	$\overset{-}{27},\overset{+}{13}$	17	$\overset{+}{30},\overset{-}{12}$
11	$\overset{+}{31},\overset{+}{30}$	$\overset{-}{8},\overset{-}{0}$	$\overset{-}{23},\overset{-}{17},\overset{-}{15},\overset{+}{0}$	$\overset{+}{15}$	$\overset{-}{23},\overset{-}{17},\overset{-}{8}$	22	$\overset{-}{30},\overset{-}{13},\overset{-}{7}$
12	$\overset{+}{31},\overset{-}{13},\overset{-}{7}$	$\overset{+}{31},\overset{+}{17},\overset{+}{7}$	$\overset{-}{31},\overset{-}{6},\overset{+}{0}$	-	$\overset{+}{17},\overset{+}{6},\overset{+}{0}$	7	$\overset{+}{24},\overset{+}{13},\overset{+}{7}$
13	$\overset{+}{31},\overset{+}{24}$	$\overset{+}{31},\overset{-}{13}$	$\overset{+}{31},\overset{+}{12}$	-	$\overset{-}{12}$	12	$\overset{-}{24}$
14	$\overset{+}{31}$	$\overset{+}{31},\overset{+}{18}$	$\overset{+}{31},\overset{+}{30}$	$\overset{-}{31}$	$\overset{-}{30},\overset{+}{18}$	17	$\overset{-}{15},\overset{+}{3}$
15	$\overset{+}{31},\overset{-}{15},\overset{+}{3}$	$\overset{+}{31},\overset{+}{25}$	$\overset{+}{31},\overset{-}{13},\overset{-}{7}$	-	$\overset{+}{25},\overset{-}{13},\overset{-}{7}$	22	$\overset{-}{29},\overset{+}{15},\overset{-}{3}$
16	$\overset{+}{31},\overset{-}{29}$	$\overset{+}{31}$	$\overset{+}{31},\overset{+}{24}$	-	$\overset{+}{24}$	5	$\overset{+}{29}$
17	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31}$	-	-	9	-
18	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31},\overset{-}{15},\overset{+}{3}$	$\overset{+}{15}$	$\overset{+}{3}$	14	$\overset{+}{17}$
19	$\overset{+}{31},\overset{+}{17}$	$\overset{+}{31}$	$\overset{+}{31},\overset{-}{29}$	-	$\overset{-}{29}$	20	$\overset{-}{17}$
20-21	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31}$	-	-	.	-
22	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31},\overset{+}{17}$	-	$\overset{+}{17}$	14	$\overset{+}{31}$
23	-	-	$\overset{+}{31}$	$\overset{-}{31}$	-	20	-
24	-	$\overset{+}{31}$	$\overset{+}{31}$	-	-	5	-
25	-	-	$\overset{+}{31}$	$\overset{-}{31}$	-	9	-
26-33	-	-	-	-	-	.	-
34	-	-	-	$\overset{+}{15}$	$\overset{+}{15}$	16	$\overset{+}{31}$
35	$\overset{+}{31}$	$\overset{-}{31}$	-	$\overset{-}{31}$	-	23	-
36	$\overset{+}{31}$	-	-	-	-	4	-
37	$\overset{+}{31}$	$\overset{+}{31}$		$\overset{-}{31}$	-	11	-
38-49	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	-	-	.	-
50	$\overset{-}{31}$		$\overset{-}{31}$	$\overset{-}{31}$	-	15	-
51-59	$\overset{-}{31}$	$\overset{+}{31}$	$\overset{\pm}{31}$	-	-	.	-
60	$\overset{+}{31}$		$\overset{-}{31}$	$\overset{-}{31}$	-	6	-
61	$\overset{-}{31}$	$\overset{-}{31}$	$\overset{-}{31}$	$\overset{+}{15}$	$\overset{+}{15}$	10	$\overset{+}{25}$
62-63	$\overset{\pm}{31},\overset{+}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	-	-	.	-

Table 1. The first block of the differential. Recall that $\delta Q_t = \delta Q_{t-1} + \delta R_{t-1}$, $\delta T_t = \delta f_t + \delta Q_{t-3} + \delta W_t$, and (most of the time) $\delta R_t = ROTL^{S(t)}(\delta T_t)$.

The total add-difference is obtained by adding the differences together. The column headed by $S(t)$ shows the rotation amount for that round. The propagation of differences through the f_t function is discussed in Section 5.

Conditions of T_t. For Section 4 we consider only the restrictions on T_t that are necessary to ensure that the rotation of T_t (that is R_t) provides the correct add-difference. The restrictions fall into one of three categories:

- A given add-difference *must not* propagate XOR-differences past the bit position in T_t that is rotated to bit $R_t[31]$ otherwise the rotation will carry that difference to the lower order bits, thus resulting in the wrong add-difference in R_t.
- A given add-difference *must* propagate XOR-differences past a certain bit position in T_t, to ensure that the rotation will carry that difference to the lower order bits, in order to obtain the correct add-difference in R_t.
- In some cases, an add-difference would propagate XOR-differences past bit 31 (if it were possible). For example, if $T_t[j] = 0$, $25 \leq j \leq 31$ and the attacker wanted the add-difference -2^{25}, then the second message must have $T_t^*[j] = 1$, $25 \leq j \leq 31$. Injecting this add-difference to T_t propagates the difference up to bit 31, and would propagate further (if T_t had consisted of more bits). When rotated by, for example $S(t) = 12$, the attacker may desire that the resulting difference is $\delta R_t = -2^{25+12 \pmod{32}} = -2^5$. In stead, the attacker will get

  $$\delta R_t = \sum_{j=25}^{31} +2^{j+12 \pmod{32}} = \sum_{j=5}^{31} +2^j.$$

  This is not what the attacker wanted at all. To prevent this, the attacker needed to ensure that injecting this add-difference to T_t would not propagate pas bit 31 (if T_t had consisted of more bits). The attacker needed at least one of the bit positions $25 \leq j \leq 31$ to have $T_t[j] = 1$, as this would stop the difference propagating past this pit position.

Rather than explaining this reasoning every time these situations occur, we may simply state:

- $\delta = (\pm 2^j)$ must not propagate past bit k;
- $\delta = (\pm 2^j)$ must propagate past bit k; or
- $\delta = (\pm 2^j)$ must propagate past bit 31;

according to the corresponding category above.

4.3 Description of the First Block of the Differential

Rounds 0 to 3: $\delta Q_t = 0$ and $\delta W_t = 0$: thus $\delta T_t = \delta R_t = \delta Q_{t+1} = 0$.

Round 4: $\delta Q_4 = 0$.

- $\delta W_4 = +2^{31}$.

- Thus $\delta T_4 = -2^{31}$.
- **Conditions on T_4:**
  - $T_4[31] = 1$, to change add-difference $(+2^{31})$ to (-2^{31}).
- Since $S(4) = 7$, this results in $\delta R_4 = -2^{31+7=6} = -2^6$.
- Thus $\delta Q_5 = \delta Q_4 + \delta R_4 = (0) + (-2^6) = -2^6$.

Round 5: $\delta Q_5 = -2^6$.

- $\delta f_5 = +2^{19} + 2^{11}$.
- Thus $\delta T_5 = +2^{19} + 2^{11}$.
- **Conditions on T_5:**
  - $\delta = (+2^{19} + 2^{11})$ must not propagate past bit 19.
- Since $S(5) = 12$, this results in

$$\delta R_5 = +2^{19+12=31} + 2^{11+12=23} = +2^{31} + 2^{23}.$$

- Thus $\delta Q_6 = \delta Q_5 + \delta R_5 = (-2^6) + (+2^{31} + 2^{23}) = \pm 2^{31} + 2^{23} - 2^6$.

Round 6: $\delta Q_6 = \pm 2^{31} + 2^{23} - 2^6$.

- $\delta f_6 = -2^{14} - 2^{10}$.
- Thus $\delta T_6 = -2^{14} - 2^{10}$.
- **Conditions on T_6:**
  - $\delta = (-2^{14})$ *must* propagate to at least bit 15 in order for the rotation to cause *desired* bit differences in lower order bits. Thus, we can write $\delta T_6 = -2^{15} + 2^{14} - 2^{10}$.
  - $\delta = (-2^{10})$ must not propagate past bit 14.
- Since $S(6) = 17$, this results in $\delta R_6 = -2^{15+17=0} + 2^{14+17=1} - 2^{10+17=27} = +2^{31} - 2^{27} - 2^0$.
- Thus

$$\begin{aligned}\delta Q_7 = \delta Q_6 + \delta R_6 &= (\pm 2^{31} + 2^{23} - 2^6) + (+2^{31} - 2^{27} - 2^0)\\ &= -2^{27} + 2^{23} - 2^6 - 2^0,\end{aligned}$$

  noting that the add-differences $(\pm 2^{31})$ and $(+2^{31})$ have cancelled out.

Round 7: $\delta Q_7 = -2^{27} + 2^{23} - 2^6 - 2^0$.

- $\delta f_7 = -2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2$.
- Thus $\delta T_7 = -2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2$.
- **Conditions on T_7:**
  - $\delta = (-2^{27} - 2^{25} + 2^{16})$ must not propagate past bit 31.
  - $\delta = (-2^2)$ must not propagate past bit 9.
  - $\delta = (+2^{10} + 2^5)$ *must* propagate to at least bit 11 and have $\Delta T_7[10] = 0$ in order for the rotation to cause *desired* bit differences in lower order bits. Thus, we can write

$$(+2^{10} + 2^5) = +2^{11} - 2^9 - 2^8 - 2^7 - 2^6 - 2^5.$$

  - In the given collision, $T_7[27, 25, 9-5, 2] = 1$, and $T_7[16, 11] = 0$, so these conditions are satisfied.

- Since $S(7) = 22$, this results in

$$\begin{aligned}\delta R_7 &= -2^{27+22=17} - 2^{25+22=15} + 2^{16+22=6} + 2^{11+22=1} - 2^{2+22=24} \\ &\quad + \underbrace{(-2^{9+22=31} - 2^{8+22=30} - 2^{7+22=29} - 2^{6+22=28} - 2^{5+22=27})}_{=+2^{27}} \\ &= +2^{27} - 2^{24} - 2^{17} - 2^{15} + 2^{6} + 2^{1}.\end{aligned}$$

- Thus

$$\begin{aligned}\delta Q_8 &= \delta Q_7 + \delta R_7 \\ &= (-2^{27} + 2^{23} - 2^{6} - 2^{0}) + (+2^{27} - 2^{24} - 2^{17} - 2^{15} + 2^{6} + 2^{1}) \\ &= (-2^{24} + 2^{23}) - 2^{17} - 2^{15} + (+2^{1} - 2^{0}) \\ &= -2^{23} - 2^{17} - 2^{15} + 2^{0},\end{aligned}$$

  noting that:
  - the add-differences (-2^{27}) and $(+2^{27})$ have cancelled out;
  - the add-differences (-2^{6}) and $(+2^{6})$ have cancelled out;
  - add-differences (-2^{24}) and $(+2^{23})$ combine as (-2^{23}); and
  - add-differences $(+2^{1})$ and (-2^{0}) combine as $(+2^{0})$.

Round 8: $\delta Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^{0}$.

- $\delta f_8 = \pm 2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^{8} + 2^{6}$.
- $\delta Q_{t-3} = \delta Q_5 = -2^{6}$.
- Thus

$$\begin{aligned}\delta T_8 &= (+2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^{8} + 2^{6}) + (-2^{-6}) \\ &= -2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^{8},\end{aligned}$$

  noting that:
  - the add-differences (-2^{6}) and $(+2^{6})$ have cancelled out.
- **Conditions on T_6:**
  - $T_6[31] = 1$, to ensure add-difference $(\pm 2^{31})$ is really (-2^{31}).
  - $\delta = (-2^{24} + 2^{16} + 2^{10} + 2^{8})$ must not propagate past bit 24.
- Since $S(8) = 7$, this results in

$$\begin{aligned}\delta R_8 &= -2^{31+7=6} - 2^{24+7=31} + 2^{16+7=23} + 2^{10+7=17} + 2^{8+7=15} \\ &= -2^{31} + 2^{23} + 2^{17} + 2^{15} - 2^{6}.\end{aligned}$$

- Thus

$$\begin{aligned}\delta Q_9 &= \delta Q_8 + \delta R_8 \\ &= (-2^{23} - 2^{17} - 2^{15} + 2^{0}) + (-2^{31} + 2^{23} + 2^{17} + 2^{15} - 2^{6}) \\ &= -2^{31} - 2^{6} + 2^{0}.\end{aligned}$$

  noting that:
  - the add-differences (-2^{23}) and $(+2^{23})$ have cancelled out;

  - the add-differences (-2^{17}) and $(+2^{17})$ have cancelled out; and
  - the add-differences (-2^{15}) and $(+2^{15})$ have cancelled out.

Round 9: $\delta Q_9 = -2^{31} - 2^{6} + 2^{0}$.

- $\delta f_9 = \pm 2^{31} + 2^{26} - 2^{23} - 2^{20} + 2^{6} + 2^{0}$.
- $\delta Q_{t-3} = \delta Q_6 = +2^{31} + 2^{23} - 2^{6}$.
- Thus

$$\begin{aligned}\delta T_9 &= (\pm 2^{31} + 2^{26} - 2^{23} - 2^{20} + 2^{6} + 2^{0}) + (+2^{31} + 2^{23} - 2^{6})\\ &= +2^{26} - 2^{20} + 2^{0},\end{aligned}$$

  noting that:
  - $(\pm 2^{31})$ and $(+2^{31})$ have cancelled out;
  - (-2^{23}) and $(+2^{23})$ have cancelled out; and
  - $(+2^{6})$ and (-2^{6}) have cancelled out.
- **Conditions on T_t:**
  - $\delta = (+2^{26} - 2^{20})$ must not propagate past bit 31.
  - $\delta = (+2^{0})$ must not propagate past bit 19.
- Since $S(9) = 12$, this results in

$$\begin{aligned}\delta R_9 &= +2^{26+12=6} - 2^{20+12=0} + 2^{0+12=12}\\ &= +2^{12} + 2^{6} - 2^{0}.\end{aligned}$$

- Thus $\delta Q_{10} = \delta Q_9 + \delta R_9 = (-2^{31} - 2^{6} + 2^{0}) + (+2^{12} + 2^{6} - 2^{0}) = -2^{31} + 2^{12}$, noting that:
  - (-2^{6}) and $(+2^{6})$ have cancelled out; and
  - $(+2^{0})$ and (-2^{0}) have cancelled out.

Round 10: $\delta Q_{10} = +2^{31} + 2^{12}$.

- $\delta f_{10} = -2^{23} + 2^{13} + 2^{6} + 2^{0}$.
- $\delta Q_{t-3} = \delta Q_7 = -2^{27} + 2^{23} - 2^{6} - 2^{0}$.
- Thus

$$\begin{aligned}\delta T_{10} &= (-2^{23} + 2^{13} + 2^{6} + 2^{0}) + (-2^{27} + 2^{23} - 2^{6} - 2^{0})\\ &= -2^{27} + 2^{13},\end{aligned}$$

  - (-2^{23}) and $(+2^{23})$ have cancelled out;
  - (-2^{6}) and $(+2^{6})$ have cancelled out; and
  - $(+2^{0})$ and (-2^{0}) have cancelled out.
- **Conditions on T_t:**
  - $\delta = (-2^{27})$ must not propagate past bit 31.
  - $\delta = (+2^{13})$ must not propagate past bit 14.
- Since $S(10) = 17$, this results in

$$\delta R_{10} = +2^{27+17=12} - 2^{13+17=30} = +2^{30} - 2^{12}.$$

- Thus $\delta Q_{11} = \delta Q_{10} + \delta R_{10} = (+2^{31} + 2^{12}) + (+2^{30} - 2^{12}) = +2^{31} + 2^{30}$, noting that

- $(+2^{12})$ and (-2^{12}) have cancelled out.

Round 11: $\delta Q_{11} = +2^{31} + 2^{30}$.

- $\delta f_{11} = -2^{8} - 2^{0}$.
- $\delta Q_{t-3} = \delta Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^{0}$.
- $\delta W_{11} = \delta M_{11} = +2^{15}$.
- Thus

$$\begin{aligned}\delta T_{11} &= (-2^{8} - 2^{0}) + (-2^{23} - 2^{17} - 2^{15} + 2^{0}) + (+2^{15})\\ &= -2^{23} - 2^{17} - 2^{8},\end{aligned}$$

  noting that:
  - (-2^{15}) and $(+2^{15})$ have cancelled out; and (-2^{0}) and $(+2^{0})$ have cancelled out.
- **Conditions on T_t:**
  - $\delta = (-2^{23} - 2^{17})$ must not propagate past bit 31.
  - $\delta = (-2^{8})$ must not propagate past bit 9.
- Since $S(11) = 22$, this results in

$$\delta R_{11} = -2^{23+22=13} - 2^{17+22=7} - 2^{8+22=20} = -2^{30} - 2^{13} - 2^{7}.$$

- Thus

$$\begin{aligned}\delta Q_{12} = \delta Q_{11} + \delta R_{11} &= (+2^{31} + 2^{30}) + (-2^{30} - 2^{13} - 2^{7})\\ &= +2^{31} - 2^{13} - 2^{7},\end{aligned}$$

  noting that
  - $(+2^{30})$ and (-2^{30}) have cancelled out.

Round 12: $\delta Q_{12} = +2^{31} - 2^{13} - 2^{7}$.

- $\delta f_{12} = +2^{31} + 2^{17} + 2^{7}$.
- $\delta Q_{t-3} = \delta Q_9 = -2^{31} - 2^{6} + 2^{0}$.
- Thus

$$\begin{aligned}\delta T_{12} &= (+2^{31} + 2^{17} + 2^{7}) + (-2^{31} - 2^{6} + 2^{0})\\ &= -2^{16} + 2^{6} + 2^{0},\end{aligned}$$

  noting that:
  - $(+2^{31})$ and (-2^{31}) have cancelled out; and
  - $(+2^{7})$ and (-2^{6}) have combined to become $(+2^{6})$.
- **Conditions on T_t:**
  - $\delta = (-2^{16} + 2^{6} + 2^{0})$ must not propagate past bit 24.
- Since $S(12) = 7$, this results in

$$\delta R_{12} = -2^{16+7=23} + 2^{6+7=13} + 2^{0+7=7} = +2^{24} + 2^{13} + 2^{7}.$$

- Thus

$$\begin{aligned}\delta Q_{13} &= \delta Q_{12} + \delta R_{12} = (+2^{31} - 2^{13} - 2^{7}) + (+2^{24} + 2^{13} + 2^{7}) \\ &= +2^{31} + 2^{24},\end{aligned}$$

  noting that:
  - (-2^{13}) and $(+2^{13})$ have cancelled out; and
  - (-2^{7}) and $(+2^{7})$ have cancelled out.

Round 13: $\delta Q_{13} = +2^{31} + 2^{24}$.
- $\delta f_{13} = +2^{31} - 2^{13}$.
- $\delta Q_{t-3} = \delta Q_{10} = +2^{31} + 2^{12}$.
- Thus $\delta T_{13} = (+2^{31} - 2^{13}) + (+2^{31} + 2^{12}) = -2^{12}$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out; and
  - (-2^{13}) and $(+2^{12})$ have combined to become (-2^{12}).
- **Conditions on T_t:**
  - $\delta = (-2^{12})$ must not propagate past bit 19.
- Since $S(13) = 12$, this results in $\delta R_{13} = -2^{12+12=24} = -2^{24}$.
- Thus $\delta Q_{14} = \delta Q_{13} + \delta R_{13} = (+2^{31} + 2^{24}) + (-2^{24}) = +2^{31}$, noting that:
  - $(+2^{24})$ and (-2^{24}) have cancelled out.

Round 14: $\delta Q_{14} = +2^{31}$.
- $\delta f_{14} = +2^{31} + 2^{18}$.
- $\delta Q_{t-3} = \delta Q_{11} = +2^{31} + 2^{30}$.
- $\delta W_{14} = \delta M_{14} = -2^{31}$.
- $\delta T_{14} = (+2^{31} + 2^{18}) + (+2^{31} + 2^{30}) + (-2^{31}) = -2^{30} + 2^{18}$, noting that:
  - $(+2^{31})$, $(+2^{31} + 2^{30})$ and (-2^{31}) combine to become (-2^{30}).
- **Conditions on T_t:**
  - $\delta = (-2^{30} + 2^{18})$ must not propagate past bit 31.
- Since $S(14) = 17$, this results in

$$\delta R_{14} = -2^{30+17=15} + 2^{18+17=3} = -2^{15} + 2^{3}.$$

- Thus $\delta Q_{15} = \delta Q_{14} + \delta R_{14} = (+2^{31}) + (-2^{15} + 2^{3}) = +2^{31} - 2^{15} + 2^{3}$.

Round 15: $\delta Q_{15} = +2^{31} - 2^{15} + 2^{3}$.
- $\delta f_{15} = +2^{31} + 2^{25}$.
- $\delta Q_{t-3} = \delta Q_{12} = +2^{31} - 2^{13} - 2^{7}$.
- $\delta T_{15} = (+2^{31} + 2^{25}) + (+2^{31} - 2^{13} - 2^{7}) = +2^{25} - 2^{13} - 2^{7}$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.
- **Conditions on T_t:**
  - $\delta = (+2^{25} - 2^{13})$ must not propagate past bit 31.
  - $\delta = (-2^{7})$ must not propagate past bit 9.
- Since $S(15) = 22$, this results in

$$\delta R_{15} = +2^{25+22=15} - 2^{13+22=3} - 2^{7+22=29} = -2^{29} + 2^{15} - 2^{3}.$$

– Thus

$$\begin{aligned}\delta Q_{16} = \delta Q_{15} + \delta R_{15} &= (+2^{31} - 2^{15} + 2^{3}) + (-2^{29} + 2^{15} - 2^{3}) \\ &= +2^{31} - 2^{29},\end{aligned}$$

noting that:
- (-2^{15}) and $(+2^{15})$ have cancelled out; and
- $(+2^{3})$ and (-2^{3}) have cancelled out.

The differential becomes easier from here-on.

Round 16: $\delta Q_{16} = +2^{31} - 2^{29}$.
- $\delta f_{16} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{13} = +2^{31} + 2^{24}$.
- Thus $\delta T_{16} = (+2^{31}) + (+2^{31} + 2^{24}) = +2^{24}$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.
- **Conditions on T_t:**
  - $\delta = (+2^{24})$ must not propagate past bit 26.
- Since $S(16) = 5$, this results in $\delta R_{16} = +2^{24+5=29} = +2^{29}$.
- Thus $\delta Q_{17} = \delta Q_{16} + \delta R_{16} = (+2^{31} - 2^{29}) + (+2^{29}) = +2^{31}$, noting that:
  - (-2^{29}) and $(+2^{29})$ have cancelled out.

Round 17: $\delta Q_{17} = +2^{31}$.
- $\delta f_{17} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{14} = +2^{31}$.
- Thus $\delta T_{17} = (+2^{31}) + (+2^{31}) = 0$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{17} = 0$.
- Thus $\delta Q_{18} = \delta Q_{17} + \delta R_{17} = (+2^{31}) + (0) = +2^{31}$.

Round 18: $\delta Q_{18} = +2^{31} - 2^{29}$.
- $\delta f_{18} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{15} = +2^{31} - 2^{15} + 2^{3}$.
- $\delta W_{18} = \delta M_{11} = +2^{15}$.
- Thus $\delta T_{18} = (+2^{31}) + (+2^{31} - 2^{15} + 2^{3}) + (+2^{15}) = (+2^{3})$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out; and
  - (-2^{15}) and $(+2^{15})$ have cancelled out.
- **Conditions on T_t:**
  - $\delta = (+2^{3})$ must not propagate past bit 17.
- Since $S(18) = 14$, this results in $\delta R_{18} = +2^{3+14=17} = +2^{17}$.
- Thus $\delta Q_{19} = \delta Q_{18} + \delta R_{18} = (+2^{31}) + (+2^{17}) = +2^{31} + 2^{17}$.

Round 19: $\delta Q_{19} = +2^{31} + 2^{17}$.
- $\delta f_{19} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{14} = +2^{31} - 2^{29}$.
- Thus $\delta T_{19} = (+2^{31}) + (+2^{31} - 2^{29}) = -2^{29}$, noting that
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.

- **Conditions on T_t:**
  - $\delta = (-2^{29})$ must not propagate past bit 31.
- Since $S(19) = 20$, this results in $\delta R_{19} = -2^{29+20=17} = -2^{17}$.
- Thus $\delta Q_{20} = \delta Q_{19} + \delta R_{19} = (+2^{31} + 2^{17}) + (-2^{17}) = +2^{31}$, noting that:
  - $(+2^{17})$ and (-2^{17}) have cancelled out.

Round 20 and 21 $\delta Q_t = +2^{31}$.
- $\delta f_t = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{17} = +2^{31}$.
- Thus $\delta T_t = (+2^{31}) + (+2^{31}) = 0$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.
- **Conditions on T_t:** none.
- $\delta R_t = 0$.
- Thus $\delta Q_{t+1} = \delta Q_t + \delta R_t = (+2^{31}) + (0) = +2^{31}$.

Round 22: $\delta Q_{22} = +2^{31}$.
- $\delta f_{22} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{19} = +2^{31} + 2^{17}$.
- Thus $\delta T_{22} = (+2^{31}) + (+2^{31} + 2^{17}) = +2^{17}$, noting that
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.
- **Conditions on T_t:**
  - $\delta = (+2^{17})$ must not propagate past bit 17.
- Since $S(22) = 14$, this results in $\delta R_{19} = +2^{17+14=31} = +2^{31}$.
- Thus $\delta Q_{23} = \delta Q_{22} + \delta R_{22} = (+2^{31}) + (+2^{31}) = 0$, noting that
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.

Round 23: $\delta Q_{23} = 0$.
- $\delta f_{23} = 0$.
- $\delta Q_{t-3} = \delta Q_{20} = +2^{31}$.
- $\delta W_{23} = \delta M_4 = -2^{31}$.
- Thus $\delta T_{23} = (+2^{31}) + (-2^{31}) = 0$, noting that:
  - $(+2^{31})$ and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{23} = 0$.
- Thus $\delta Q_{24} = \delta Q_{23} + \delta R_{23} = (0) + (0) = 0$.

Round 24: $\delta Q_{24} = 0$.
- $\delta f_{24} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{21} = +2^{31}$.
- Thus $\delta T_{24} = (+2^{31}) + (+2^{31}) = 0$, noting that:
  - $(+2^{31})$ and $(+2^{31})$ have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{24} = 0$.
- Thus $\delta Q_{25} = \delta Q_{24} + \delta R_{24} = 0$.

Round 25: $\delta Q_{25} = 0$.
- $\delta f_{25} = 0$.
- $\delta Q_{t-3} = \delta Q_{19} = +2^{31}$.

- $\delta W_{25} = \delta M_{14} = -2^{31}$.
- Thus $\delta T_{25} = (+2^{31}) + (-2^{31}) = 0$, noting that
  - $(+2^{31})$ and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{25} = 0$.
- Thus $\delta Q_{26} = \delta Q_{25} + \delta R_{25} = 0$.

Round 26 to 33: $\delta Q_t = 0$.

- $\delta f_t = \delta Q_{t-3} = \delta W_t = 0$.
- Thus $\delta T_t = \delta R_t = 0$, and $\delta Q_{t+1} = \delta Q_t + \delta R_t = 0$.
- **Conditions on T_t:** none

Round 34: $\delta Q_{34} = 0$.

- $\delta f_{34} = 0$.
- $\delta Q_{t-3} = \delta Q_{31} = 0$.
- $\delta W_{34} = \delta M_{11} = +2^{15}$.
- Thus $\delta T_{34} = (0) + (+2^{15}) = +2^{15}$.
- **Conditions on T_t:**
  - $\delta = (+2^{15})$ must not propagate past bit 15.
- Since $S(34) = 16$, this results in $\delta R_{34} = +2^{15+16=31} = +2^{31}$.
- Thus $\delta Q_{35} = \delta Q_{34} + \delta R_{34} = (0) + (+2^{31}) = +2^{31}$.

Round 35: $\delta Q_{35} = +2^{31}$.

- $\delta f_{35} = -2^{31}$.
- $\delta Q_{t-3} = \delta Q_{32} = 0$.
- $\delta W_{35} = \delta M_{14} = -2^{31}$.
- Thus $\delta T_{35} = (-2^{31}) + (-2^{31}) = 0$, noting that:
  - (-2^{31}) and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{35} = 0$.
- Thus $\delta Q_{36} = \delta Q_{35} + \delta R_{35} = (+2^{31}) + (0) = +2^{31}$.

Round 36: $\delta Q_{36} = +2^{31}$.

- $\delta f_{36} = 0$,
- $\delta Q_{t-3} = \delta Q_{33} = 0$.
- Thus $\delta T_{36} = \delta R_{36} = 0$.
- **Conditions on T_t:** none
- Thus $\delta Q_{37} = \delta Q_{36} + \delta R_{36} = (+2^{31}) + (0) = +2^{31}$.

Round 37: $\delta Q_{37} = +2^{31}$.

- $\delta f_{37} = +2^{31}$.
- $\delta Q_{t-3} = \delta Q_{34} = 0$.
- $\delta W_{37} = \delta M_4 = -2^{31}$.
- Thus $\delta T_{37} = (-2^{31}) + (-2^{31}) = 0$, noting that:
  - (-2^{31}) and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{37} = 0$.
- Thus $\delta Q_{38} = \delta Q_{37} + \delta R_{37} = (+2^{31}) + (0) = +2^{31}$.

Rounds 38 to 49: $\delta Q_t = \pm 2^{31}$.
- $\delta f_t = \pm 2^{31}$.
- $\delta Q_{t-3} = \pm 2^{31}$.
- Thus $\delta T_t = (\pm 2^{31}) + (\pm 2^{31}) = 0$, noting that:
  - $(\pm 2^{31})$ and $(\pm 2^{31})$ have cancelled out.
- **Conditions on T_t:** none
- $\delta R_t = 0$.
- Thus $\delta Q_{t+1} = \delta Q_t + \delta R_t = (\pm 2^{31}) + (0) = \pm 2^{31}$.

Round 50: $\delta Q_{50} = -2^{31}$.
- $\delta f_{50} = 0$.
- $\delta Q_{t-3} = \delta Q_{47} = -2^{31}$.
- $\delta W_{50} = \delta M_{14} = -2^{31}$.
- Thus $\delta T_{50} = (-2^{31}) + (-2^{31}) = 0$, noting that:
  - (-2^{31}) and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{50} = 0$.
- Thus $\delta Q_{51} = \delta Q_{50} + \delta R_{50} = (-2^{31}) + (0) = -2^{31}$.

Rounds 51 to 59: $\delta Q_t = -2^{31}$.
- $\delta f_t = +2^{31}$.
- $\delta Q_{t-3} = \pm 2^{31}$.
- Thus $\delta T_t = (-2^{31}) + (\pm 2^{31}) = 0$, noting that:
  - (-2^{31}) and $(\pm 2^{31})$ have cancelled out.
- **Conditions on T_t:** none
- $\delta R_t = 0$.
- Thus $\delta Q_{t+1} = \delta Q_t + \delta R_t = (-2^{31}) + (0) = \pm 2^{31}$.

Round 60: $\delta Q_{60} = +2^{31}$.
- $\delta f_{60} = 0$.
- $\delta Q_{t-3} = \delta Q_{57} = -2^{31}$.
- $\delta W_{60} = \delta M_4 = -2^{31}$.
- Thus $\delta T_{60} = (-2^{31}) + (-2^{31}) = 0$, noting that:
  - (-2^{31}) and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_{60} = 0$.
- Thus $\delta Q_{61} = \delta Q_{60} + \delta R_{60} = (+2^{31}) + (0) = -2^{31}$.

Round 61: $\delta Q_{61} = -2^{31}$.
- $\delta f_{61} = -2^{31}$.
- $\delta Q_{t-3} = \delta Q_{58} = -2^{31}$.
- $\delta W_{61} = \delta M_{11} = +2^{15}$.
- Thus $\delta T_{61} = (-2^{31}) + (-2^{31}) + (+2^{15}) = +2^{15}$, noting that:
  - (-2^{31}) and (-2^{31}) have cancelled out.
- **Conditions on T_t:**
  - $\delta = (+2^{15})$ must not propagate past bit 21.
- Since $S(61) = 10$, this results in $\delta R_{61} = +2^{15+10=25} = +2^{25}$.
- Thus $\delta Q_{62} = \delta Q_{61} + \delta R_{61} = (+2^{31}) + (0) = +2^{31} + 2^{25}$.

Rounds 62 to 63: $\delta Q_t = \pm 2^{31} + 2^{25}$.

- $\delta f_t = \pm 2^{31}$.
- $\delta Q_{t-3} = \pm 2^{31}$.
- Thus $\delta T_t = (\pm 2^{31}) + (\pm 2^{31}) = 0$, noting that:
  - (-2^{31}) and (-2^{31}) have cancelled out.
- **Conditions on T_t:** none
- $\delta R_t = 0$.
- Thus $\delta Q_{t+1} = \delta Q_t + \delta R_t = (\pm 2^{31} + 2^{25}) + (0) = \pm 2^{31} + 2^{25}$.

The differential in the first block finishes with

$$\begin{aligned}
\varDelta Q_{61} &= \pm 2^{31},\\
\varDelta Q_{62} &= \pm 2^{31} + 2^{25},\\
\varDelta Q_{62} &= \pm 2^{31} + 2^{25},\\
\varDelta Q_{62} &= \pm 2^{31} + 2^{25},
\end{aligned}$$

and thus:

$$\begin{aligned}
\delta IHV^{(1)}[0] = \delta IHV^{(0)}[0] + \delta Q_{61} &= (0) + (\pm 2^{31}) &&= \pm\, 2^{31},\\
\delta IHV^{(1)}[1] = \delta IHV^{(0)}[1] + \delta Q_{64} &= (0) + (\pm 2^{31} + 2^{25}) &&= \pm\, 2^{31} + 2^{25},\\
\delta IHV^{(1)}[2] = \delta IHV^{(0)}[2] + \delta Q_{63} &= (0) + (\pm 2^{31} + 2^{25}) &&= \pm\, 2^{31} + 2^{25},\\
\delta IHV^{(1)}[3] = \delta IHV^{(0)}[3] + \delta Q_{62} &= ((0) + (\pm 2^{31} + 2^{25}) &&= \pm\, 2^{31} + 2^{25}.
\end{aligned}$$

The differential in the second block begins with

$$\begin{aligned}
\delta IHV^{(1)}[0] &= \pm 2^{31},\\
\delta IHV^{(1)}[1] &= \pm 2^{31} + 2^{25},\\
\delta IHV^{(1)}[2] &= \pm 2^{31} + 2^{25},\\
\delta IHV^{(1)}[3] &= \pm 2^{31} + 2^{25}.
\end{aligned}$$

Table 16 in Appendix B.1 shows the sequence of add-differences in the second block. The differential in the second block finishes up with

$$\begin{aligned}
\delta Q_{61} &= \pm 2^{31},\\
\delta Q_{62} &= \pm 2^{31} - 2^{25},\\
\delta Q_{63} &= \pm 2^{31} - 2^{25},\\
\delta Q_{64} &= \pm 2^{31} - 2^{25}.
\end{aligned}$$

There is no explanation of the differential through the second block as the explanation is quite similar to that for the first block. Thus:

$$\begin{aligned}
\delta IHV^{(2)}[0] &= \delta IHV^{(1)}[0] + \delta Q_{61} = (\pm 2^{31}) + (\pm 2^{31}) = 0,\\
\delta IHV^{(2)}[1] &= \delta IHV^{(1)}[1] + \delta Q_{64} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31} - 2^{25}) = 0,\\
\delta IHV^{(2)}[2] &= \delta IHV^{(1)}[2] + \delta Q_{63} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31} - 2^{25}) = 0,\\
\delta IHV^{(2)}[3] &= \delta IHV^{(1)}[3] + \delta Q_{62} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31} - 2^{25}) = 0.
\end{aligned}$$

t	δ	Max	Requirements	Probabilities	
				Small	≈ 1
4	$(+2^{31})$	> 31	$T_4[31] = 1$	2^{-1}	
5	$(+2^{19} + 2^{11})$	≤ 19	$T_5[19] = 0,$	2^{-1}	
			$0 \in T_5[11 - 18]$		$(1 - 2^{-8})$
6	(-2^{14})	> 14	$T_6[14] = 0$	2^{-1}	
	(-2^{10})	≤ 14	$1 \in T_6[13 - 10]]$		$(1 - 2^{-5})$
7	$(-2^{27} - 2^{25} + 2^{16})$	≤ 31	$1 \in T_7[31 - 27],$		$(1 - 2^{-5})$
			$1 \in T_7[26, 25],$	$(1 - 2^{-2})$	
			$0 \in T_7[24 - 16]$		$(1 - 2^{-9})$
	(-2^2)	≤ 9	$1 \in T_7[9 - 2]$		$(1 - 2^{-8})$
	$(+2^{10} + 2^5)$	$\Delta T_7[10] = 0$	$T_7[9 - 5] = 1$	2^{-5}	
8	$+2^{31}$	> 31	$T_8[31] = 1$	2^{-1}	
	$(-2^{24} + 2^{16} + 2^{10} + 2^8)$	≤ 24	$T_8[24] = 1,$	2^{-1}	
			$0 \in T_8[23 - 16],$		$(1 - 2^{-8})$
			$0 \in T_7[15 - 10],$		$(1 - 2^{-6})$
			$0 \in T_7[9, 8]$	$(1 - 2^{-2})$	
9	$(+2^{26} - 2^{20})$	≤ 31	$0 \in T_9[31 - 26],$		$(1 - 2^{-6})$
			$1 \in T_9[25 - 20]$		$(1 - 2^{-6})$
	$(+2^0)$	≤ 19	$0 \in T_9[19 - 2]$		$(1 - 2^{-18})$
10	(-2^{27})	≤ 31	$1 \in T_{10}[31 - 27]$		$(1 - 2^{-5})$
	$(+2^{13})$	≤ 14	$0 \in T_{10}[14, 12]$	$(1 - 2^{-3})$	
11	$(-2^{23} - 2^{17})$	≤ 31	$1 \in T_{11}[31, 23],$		$(1 - 2^{-9})$
			$1 \in T_{11}[22, 17]$		$(1 - 2^{-6})$
	(-2^8)	≤ 9	$1 \in T_{11}[9, 8]$	$(1 - 2^{-2})$	
12	$(-2^{16} + 2^6 + 2^0)$	≤ 24	$1 \in T_{12}[24 - 16],$		$(1 - 2^{-9})$
			$0 \in T_{12}[15 - 6]$		$(1 - 2^{-10})$
			$0 \in T_{12}[5 - 2]$	$(1 - 2^{-4})$	
13	(-2^{12})	≤ 19	$1 \in T_{13}[19 - 12]$		$(1 - 2^{-8})$
14	$(-2^{30} + 2^{18})$	≤ 31	$1 \in T_{14}[31, 30],$	$(1 - 2^{-2})$	
			$0 \in T_{14}[29 - 18]$		$(1 - 2^{-12})$
15	$(+2^{25} - 2^{13})$	≤ 31	$0 \in T_{15}[31 - 25],$		$(1 - 2^{-12})$
			$1 \in T_{15}[24 - 13]$		$(1 - 2^{-12})$
	(-2^7)	≤ 9	$1 \in T_{15}[9, 8, 7]$	$(1 - 2^{-3})$	
16	$(+2^{24})$	≤ 24	$T_{16}[24] = 0$	2^{-1}	
18	$(+2^3)$	≤ 17	$0 \in T_{18}[17 - 3]$		$(1 - 2^{-15})$
19	(-2^{29})	≤ 31	$1 \in T_{19}[31 - 29]$	$(1 - 2^{-3})$	
22	$(+2^{17})$	≤ 17	$T_{22}[17] = 0$	2^{-1}	
34	$(+2^{15})$	≤ 15	$T_{23}[15] = 0$	2^{-1}	
61	$(+2^{15})$	≤ 21	$0 \in T_{15}[21 - 15]$		$(1 - 2^{-7})$
			Total	$2^{-15.6}$	

Table 2. Conditions on T_t for the first block of the differential. Only those rounds with conditions are shown.

4.4 Summary of Conditions on T_t

In Table 2, the conditions on the carry propagation for δT_t have been collected, turned into conditions of the values $T_t[j]$ (the values during the first message), and then translated into a probability. The product of these probabilities is $2^{-15.6}$. That is, for a random message, the conditions on T_t are satisfied with probability $2^{-15.6}$.

Suppose we define a"T_t-good" message M to be a message such that the conditions on T_t in the first 16 rounds satisfied. You can see from the table that most of the conditions on T_t occur in the first 16 rounds. This is useful, because an attacker has full, independent control over the value of T_t for all of these rounds. Hence, the attacker can easily generate T_t-good" message M. For each T_t-good message, the probability of the conditions being satisfied is the product of the probabilities for rounds 16 to 63. This probability is $2^{-3.2} \approx 1/9$, so the attacker can assume that one in 9 of the T_t-good messages will also satisfy the conditions in the remaining rounds.

5 Conditions for Propagation of the Differences Through the f_t Functions

Tables 3, 6, 7 and 8 provide more details on the propagation of the differences through the f_t functions.

- Table 3 corresponds to the rounds 0 to 15, with function $f_t = F$.
- Table 6 corresponds to the rounds 16 to 31, with function $f_t = G$.
- Table 7 corresponds to the rounds 32 to 47, with function $f_t = H$.
- Table 8 corresponds to the rounds 48 to 63, with function $f_t = I$.

We use the following notation:

$$\nabla X[i] = \begin{cases} 0, & \text{if } X^*[i] = X[i] = 0; \\ 1, & \text{if } X^*[i] = X[i] = 1; \\ \text{“.”}, & \text{if } X^*[i] = X[i] \text{, but the value is not specified;} \\ + \text{ or } +1, & \text{if } X^*[i] - X[i] = +1; \\ - \text{ or } -1, & \text{if } X^*[i] - X[i] = -1; \\ \pm \text{ or } \pm 1, & \text{if } X^*[i] - X[i] = \pm 1 \text{: that is } X^*[i] = \overline{X[i]}. \end{cases}$$

- We may write $X[i] = 0/1$ to to mean that $X[i] = 0$ and $X^*[i] = 1$. This is the same as $\nabla X[i] = +1$.
- We may write $X[i] = 1/0$ to to mean that $X[i] = 1$ and $X^*[i] = 0$. This is the same as $\nabla X[i] = -1$.

5.1 Rounds 0 to 15 of the First Block

Rounds 0 to 4: The attacker has

- $\delta Q_3 = 0$,

t	δQ_t	∇Q_t	∇f_t	δf_t
0-4	-	....	....	-
5	$\overset{-}{6}$	.........-++++++++++++++++......	............+.......+...........	$\overset{+}{19}, \overset{+}{11}$
6	$\overset{\pm}{31}, \overset{+}{23}, \overset{-}{6}$	±.......+................-......	.........-+++++++.++++..........	$\overset{-}{14}, \overset{-}{10}$
7	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	±+++++---...........-+++++-+++++	....-.-........+.....+....+..-..	$\overset{-}{27}, \overset{-}{25}, \overset{+}{16}, \overset{+}{10}, \overset{+}{5}, \overset{-}{2}$
8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	........-..-+++-+..............+	±......-.......+.....+.+.+......	$\overset{\pm}{31}, \overset{-}{24}, \overset{+}{16}, \overset{+}{1.}, \overset{+}{8}, \overset{+}{6}$
9	$\overset{\pm}{31}, \overset{-}{6}, \overset{+}{0}$	±......................-++....+-	±....+..-..-.............+.....+	$\overset{\pm}{31}, \overset{+}{26}, \overset{-}{23}, \overset{-}{2.}, \overset{+}{6}, \overset{+}{0}$
10	$\overset{\pm}{31}, \overset{+}{12}$	±.................+-............	........-.........+......+.....+	$\overset{-}{23}, \overset{+}{13}, \overset{+}{6}, \overset{+}{0}$
11	$\overset{\pm}{31}, \overset{+}{30}$	±+..............................	.......................-.......-	$\overset{-}{8}, \overset{-}{0}$
12	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$	±...........-++++++....-+.......	±...........+--.........+.......	$\overset{\pm}{31}, \overset{+}{17}, \overset{+}{7}$
13	$\overset{\pm}{31}, \overset{+}{24}$	±.....+-........................	±...........-++++++.............	$\overset{\pm}{31}, \overset{-}{13}$
14	$\overset{\pm}{31}$	±...............................	±............+..................	$\overset{\pm}{31}, \overset{+}{18}$
15	$\overset{\pm}{31}, \overset{-}{15}, \overset{+}{3}$	±...............-...........+...	±.....+.........................	$\overset{\pm}{31}, \overset{+}{25}$

Table 3. Propagation of differences through the f_t functions in the first 16 rounds of the first block for the example collision given by Wang et al.. Note that $f_t = (Q_t \wedge Q_{t-1}) \oplus (\overline{Q_t} \wedge Q_{t-2})$ for these rounds.

- $\delta Q_4 = 0$, and
- $\delta Q_5 = 0$.

The attacker wants $\delta f_5 = 0$. No conditions required.

	δ	∇
Q_{t-2}		....
Q_{t-1}		....
Q_t		....
f_t		....

Round 5: The attacker has

- $\delta Q_3 = 0$,
- $\delta Q_4 = 0$, and
- $\delta Q_5 = -2^6$.

The attacker wants $\delta f_5 = +2^{19} + 2^{11}$.

Obtaining Correct ΔQ_t: The only way to obtain $\delta f_5 = +2^{19} + 2^{11}$ from these differences is if the difference (-2^6) in Q_5 is propagated into higher order bits via the carries. That is, the attacker needs $Q_5[j] = 0$, $6 \leq j \leq 19$. In the collision of Wang et al., the value of Q_5 has $Q_5[21-6] = 0$ and $Q_5[22] = 1$, as shown below. Although we could consider the case with $Q_5[19-6] = 0$ and $Q_5[20] = 1$ (which is more probable) we are satisfied with the conditions $Q_5[21-6] = 0$ and $Q_5[22] = 1$ (for the moment).

	δ	∇
Q_3		....
Q_4		....
Q_5	$\bar{6}$	.........-++++++++++++++++......
f_5	$\overset{+}{19}, \overset{+}{11}$	............+.......+...........

Conditions to get correct ΔQ_t:

- $Q_5[21-6]=0$;
- $Q_5[22]=1$.

Obtaining Correct δf_t: The "best" way to get the difference $\delta f_5 = +2^{19} + 2^{11}$ is to use the differences in $Q_5[19]$ and $Q_5[11]$ to result in a differences $\nabla f_5[19,11] =$"+". By "best" we: mean that this requires the fewest conditions be applied.

Constant bits of Q_5: $\Delta Q_5[j]=0$ for $j \in [31-23, 5-0]$, where the function either

- selects $f_5[j]=Q_4[j]$ and $f_5^*[j]=Q_4^*[j]$ (when $Q_5[j]]=1$), or
- selects $f_5[j]=Q_3[j]$ and $f_5^*[j]=Q_3^*[j]$ (when $Q_5[j]=0$).

We deduce that:

- For bits $j \in [31-23, 5-0]$, $\Delta Q_4[j]=0$ and $\Delta Q_3[j]=0$, and thus $f_t=0$. No conditions required for these bits.
- *Conditions from constant bits of Q_5:* none.

Non-Constant bits of Q_5:

$\nabla Q_5[j]=+1,\ j \in [21-6]$: $Q_5[j]=0/1, \Rightarrow f_5[j]=Q_3[j]/Q_4^*[j]$.

- For $j \in [21,20,18-12,10-6]$, $f_5^*[j]=f_5[j]$, requires $Q_4^*[j]=Q_4[j]=Q_3[j]$.
- For $j \in [19,11]$, $f_5^*[j]-f_5[j]=+1$, requires $Q_4^*[j]-Q_3[j]=Q_4[j]-Q_3[j]=+1$ which implies that $Q_4[j]=1$ and $Q_3[j]=0$.

$\nabla Q_5[j]=-1,\ j \in [22]$: $Q_5[j]=1/0, \Rightarrow f_5[j]=Q_4[j]/Q_3^*[j]$.

- $f_5^*[22]=f_5[22]$, requires $Q_3^*[22]=Q_3[22]=Q_4[22]$.

Conditions from non-constant bits of Q_5:

- $Q_4[19,11]=1$;
- $Q_3[19,11]=0$;
- $Q_3[21,20,18-12,10-6]=Q_4[21,20,18-12,10-6]$. We indicate this equality by placing a "v" in the corresponding bit positions in Q_3 (like an arrow pointing down to say "The value of this bit must be equal to the value of the bit below") and placing a "^" in Q_4 (like an arrow pointing up to say "The value of this bit must be equal to the value of the bit above.")

Summary of Requirements resulting from this round:

- $Q_5[21-6]=0$;
- $Q_5[22]=1$;
- $Q_4[19,11]=1$;
- $Q_3[19,11]=0$;
- $Q_3[21,20,18-12,10-6]=Q_4[21,20,18-12,10-6]$.

t	Cumulative Conditions on Q_t
3	`.........vvv0vvvvvvv0vvvvv......`
4	`........0^^^1^^^^^^^1^^^^^......`
5	`........010000000000000000......`

Round 6: The attacker has

- $\delta Q_4 = 0$,
- $\delta Q_5 = -2^6$, and
- $\delta Q_6 = -+2^{31} + 2^{23} - 2^6$.

The attacker wants $\delta f_6 = -2^{14} - 2^{10}$.

<u>Obtaining Correct ΔQ_t:</u>

- No conditions on bit 31 at this stage.
- Otherwise, it is best if the add-differences do not propagate. Thus, for the difference $(+2^{23})$ we want $Q_6[23] = 1$, and for the difference (-2^6) we want $Q_6[6] = 1$.

	δ	∇
Q_4	-	`................................`
Q_5	$\overset{-}{6}$	`.........-++++++++++++++++......`
Q_6	$\overset{\pm}{31}, \overset{+}{23}, \overset{-}{6}$	`±.......+................-......`
f_6	$\overset{-}{14}, \overset{-}{10}$	`.........-+++++++.++++..........`

This value of ∇f_6 provides the correct add-difference $(-2^{14} - 2^{10})$, since:

$$\begin{aligned}
\delta f_6 = \sum_{j=0}^{31} (f_6^*[j] - f_6[j]) 2^j \;&=\; -2^{22} + \left(\sum_{j=15}^{21} +2^j \right) + \left(\sum_{j=10}^{13} +2^j \right) \\
= \underbrace{\left(-2^{22} + \left(\sum_{j=14}^{21} +2^j \right) \right)}_{=-2^{14}} &+ \underbrace{\left(-2^{14} + \left(\sum_{j=10}^{13} +2^j \right) \right)}_{=-2^{10}} \\
= -2^{14} - 2^{10}.&
\end{aligned}$$

Conditions to get correct ΔQ_t:

- $Q_6[23] = 0$;
- $Q_6[6] = 1$;

<u>Obtaining Correct δf_t:</u>

Constant bits of Q_6: $\Delta Q_6[j] = 0$, $j \in [30-24, 22-7, 5-0]$; where the function either

- selects $f_6[j] = Q_5[j]$ and $f_6^*[j] = Q_5^*[j]$ (when $Q_6[j]] = 1$), or
- selects $f_6[j] = Q_4[j]$ and $f_6^*[j] = Q_4^*[j]$ (when $Q_6[j] = 0$).

We deduce that,

- To obtain $\Delta f_6[22-15, 13-10] = 1$, requires $Q_6[22-15, 13-10] = 1$.

- To obtain $\Delta f_6[14,9,8,7]$, requires $Q_6[14,9,8,7] = 0$.
- For bits $j \in [30-24, 5-0]$, $\Delta Q_5[j] = 0$ and $\Delta Q_4[j] = 0$, and thus $f_t = 0$. No conditions required for these bits.
- *Conditions from constant bits of Q_6:*
  - $Q_6[22-15, 13-10] = 1$.
  - $Q_6[14,9,8,7] = 0$.

Non-Constant bits of Q_6:

$\nabla Q_6[j] = +1,\ j \in [23]$: $Q_6[j] = 0/1, \Rightarrow f_6[j] = Q_4[j]/Q_4^*[j]$.

- $f_6^*[23] = f_6[23]$, requires $Q_5^*[23] = Q_5[23] = Q_4[23]$.

$\nabla Q_6[j] = -1,\ j \in [6]$: $Q_6[j] = 1/0, \Rightarrow f_6[j] = Q_5[j]/Q_4^*[j]$.

- $f_6^*[6] = f_6[6]$, requires $Q_4^*[6] = Q_5[6] = 1$, since $Q_5[6] = 0$ has already been specified ($\nabla Q_5[6] =$"+").

$\nabla Q_6[31] = \pm 1$:

- $f_6^*[31] = f_6[31]$, requires $Q_5[31] = Q_4[31]$.

Conditions from non-constant bits of Q_6:

- $Q_5[31,23] = Q_4[31,23]$;
- $Q_4[6] = 0$.

Summary of Requirements resulting from this round:

- $Q_6[22-15, 13-10, 6] = 1$;
- $Q_6[23,14,9,8,7] = 0$;
- $Q_4[6] = 0$;
- $Q_5[31,23] = Q_4[31,23]$.

Note that the condition $Q_4[6] = 0$ combines with the condition $Q_4[6] = Q_3[6]$ required for f_5, and thus $Q_3[6] = 0$. A by-product of this requirement is that $f_5[6] = f_4[6] = 0$.

t	Cumulative Conditions on Q_t
3	.........vvv0vvvvvvv0vvvv0......
4	v.......v^^^1^^^^^^^1^^^^0......
5	^.......^10000000000000000......
6	........011111111011110001......

Round 7: The attacker has

- $\delta Q_5 = -2^6$,
- $\delta Q_6 = \pm 2^{31} + 2^{23} - 2^6$, and
- $\delta Q_7 = -2^{27} + 2^{23} - 2^6 - 2^0$.

The attacker wants $\delta f_7 = -2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2$.

Obtaining Correct ΔQ_t:

- Obtaining difference $(+2^{25})$ in f_7 requires the difference $(+2^{23})$ in Q_7 to propagated to at least bit 26. This requires $Q_7[25-23] = 1$.
- Obtaining difference $(+2^{26})$ in f_9 requires the difference $(+2^{23})$ in Q_7 to propagated to bit 26. This requires $Q_7[26] = 0$.
- Obtaining difference $(+2^{10})$ in f_8 will require the difference (-2^6) in Q_7 to propagated to bit 11. This requires $Q_7[11] = 1$, $Q_7[10-6] = 0$.
- Obtaining difference $(+2^5)$ in f_7 will require the difference (-2^0) in Q_7 to propagated to bit 5. This requires $Q_7[5] = 1$, $Q_7[4-0] = 0$.

- The example of Wang et al. has the difference (-2^{27}) in Q_7 propagating to bit 31. At first glance, this does not seem to be necessary, as it results in a large additional number of conditions. We consider two cases:
  - *Case One:* where the carry propagates and thus $Q_7[30-27]=0$; and
  - *Case Two:* where there is no carry propagation and thus $Q_7[27]=1$.

Case One: $Q_7[30-27]=0$*; carry propagation as in example of Wang et al.*

	δ	∇
Q_5	$\overset{-}{6}$	.........−++++++++++++++++......
Q_6	$\overset{\pm}{31},\overset{+}{23},\overset{-}{6}$	±.......+................−......
Q_7	$\overset{\pm}{31},\overset{-}{27},\overset{+}{23},\overset{-}{6},\overset{-}{0}$	±+++++−−−...........−+++++−+++++
f_7	$\overset{-}{27},\overset{-}{25},\overset{+}{16},\overset{+}{10},\overset{+}{5},\overset{-}{2}$	....−.−........+.....+....+..−..

Case Two: $Q_7[27]=1$*; no carry propagation.*

	δ	∇
Q_5	$\overset{-}{6}$	.........−++++++++++++++++......
Q_6	$\overset{+}{31},\overset{+}{23},\overset{-}{6}$	±.......+................−......
Q_7	$\overset{\pm}{31},\overset{-}{27},\overset{+}{23},\overset{-}{6},\overset{-}{0}$	....−+−−−...........−+++++−+++++
f_7	$\overset{-}{27},\overset{-}{25},\overset{+}{16},\overset{+}{10},\overset{+}{5},\overset{-}{2}$	....−.−........+.....+....+..−..

Conditions to get correct ΔQ_t*:*
- $Q_7[26,10-6,4-0]=0$;
- $Q_7[25-23,11,5]=1$.
- *Case One:* $Q_7[31-27]=0$.
- *Case Two:* $Q_7[27]=1$.

Obtaining Correct δf_t:

Constant bits of Q_7: $\Delta Q_7[j]=0$, $j\in[22-12]$, where the function either
- selects $f_7[j]=Q_6[j]$ and $f_7^*[j]=Q_6^*[j]$ (when $Q_7[j]]=1$), or
- selects $f_7[j]=Q_5[j]$ and $f_7^*[j]=Q_5^*[j]$ (when $Q_7[j]=0$).

We deduce that:
- To obtain $\Delta f_7[16]=+1$, requires $Q_7[16]=0$.
- To obtain $\Delta f_7[22-17,15-12]=0$, requires $Q_7[22-17,15-12]=1$.

Case Two: add $\Delta Q_7[j]=0$, $j\in[31-28]$.
- To obtain $\Delta f_7[31]=0$, requires $Q_7[31]=0$.
- No conditions for bits $j\in[30,29,28]$.
- *Conditions from constant bits of* Q_7*:*
  - $Q_7[16]=0$;
  - $Q_7[22-17,15-12]=1$;
  - *Case Two:* $Q_7[31]=0$.

Non-Constant bits of Q_7:

$\nabla Q_7[j]=+1$, $j\in[26,10-6,4-0]$: $Q_7[j]=0/1,\Rightarrow f_7[j]=Q_5[j]/Q_6^*[j]$.

- For the bits $j \in [26,4,3,1,0]$: $f_7^*[j] = f_7[j]$ requires $Q_6^*[j] = Q_6[j] = Q_5[j]$.
- For $j \in [2]$, $f_7^*[j] - f_7[j] = -1$ requires $Q_6^*[j] - Q_5[j] = -1$, which implies that $Q_6[j] = 0$ and $Q_5[j] = 1$.
- $f_7^*[10] - f_7[10] = +1$ requires $Q_6^*[10] - Q_5[10] = +1$, which implies that $Q_6[10] = 1$, and $Q_5[10] = 0$.
- For $j \in [9,8]$, $f_7^*[j] = f_7[j]$ requires $Q_6^*[j] = Q_5[j]$, which implies that $Q_6[j] = 0$, since $Q_5[j] = 0$ has already been specified ($\nabla Q_5[j] =$"+").
- *Case One:* add $\nabla Q_7[j] = +1$, $j \in [31-27]$.
  - For the bits $j \in [30,29,28]$: $f_7^*[j] = f_7[j]$ requires $Q_6^*[j] = Q_6[j] = Q_5[j]$.
  - $f_7^*[31] = f_7[31]$ requires $Q_6^*[31] = Q_5[31] = 1$, since $Q_6^*[31] = 1$ has already been specified ($\nabla Q_6[31] =$"+").
  - For $j \in [27]$, $f_7^*[j] - f_7[j] = -1$ requires $Q_6^*[j] - Q_5[j] = -1$, which implies that $Q_6[j] = 0$ and $Q_5[j] = 1$.

$\underline{\nabla Q_7[j] = -1,\ j \in [23-25,11,5]:}$ $Q_7[j] = 1/0, \Rightarrow f_7[j] = Q_6[j]/Q_5^*[j]$.

- $f_7^*[25] - f_7[25] = -1$, requires $Q_5^*[25] - Q_6[25] = Q_5[25] - Q_6[25] = -1$, since $\Delta Q_6[25] = \Delta Q_5[25] = 0$. Thus $Q_6[25] = 1$ and $Q_5[25] = 0$.
- $f_7^*[24] = f_7[24]$, requires $Q_5^*[24] = Q_6[24] \Rightarrow Q_5[24] = Q_6[24]$.
- $f_7^*[23] = f_7[23]$, requires $Q_5^*[23] = Q_6[23] \Rightarrow Q_5[23] = 0$, since $Q_6[23] = 0$, has already been specified.
- $f_7^*[11] = f_7[11]$, requires $Q_5^*[11] = Q_6[11] \Rightarrow Q_6[11] = 1$, since $Q_5[11] = 1$, has already been specified.
- $f_7^*[5] - f_7[5] = +1$, requires $Q_5^*[5] - Q_6[5] = Q_5[5] - Q_6[5] = +1$, since $\Delta Q_6[5] = \Delta Q_5[5] = 0$. Thus $Q_6[5] = 0$ and $Q_5[5] = 1$.
- *Case Two:* add $\nabla Q_7[27] = -1$.
  - $f_7^*[27] - f_7[27] = -1$ requires $Q_5^*[27] - Q_6[27] = -1$, which implies that $Q_5[27] = 0$ and $Q_6[27] = 1$.

$\underline{\nabla Q_7[31] = \pm 1:}$ *Case One* only. Need $f_7^*[31] = f_7[31]$.

- $\nabla(Q_7[31], Q_6[31]) = (+,+)$: $f_7^*[31] = Q_6^*[31] = 1, \Rightarrow f_7[31] = Q_5[31] = 1$.
- $\nabla(Q_7[31], Q_6[31]) = (+,-)$: $f_7^*[31] = Q_6^*[31] = 0, \Rightarrow f_7[31] = Q_5[31] = 0$.
- $\nabla(Q_7[31], Q_6[31]) = (-,+)$: $f_7[31] = Q_6[31] = 0, \Rightarrow f_7^*[31] = Q_5[31] = 0$.
- $\nabla(Q_7[31], Q_6[31]) = (-,-)$: $f_7[31] = Q_6[31] = 1, \Rightarrow f_7^*[31] = Q_5[31] = 1$.
- These conditions are summarized by $Q_5[31] = Q_6[31] \oplus Q_7[31]$.

Conditions from non-constant bits of Q_7:

- $Q_5[5,2] = 1$;
- $Q_5[25,23,10] = 0$;
- $Q_6[25,11,10] = 1$;
- $Q_6[9,8,5,2] = 0$;
- $j \in [30-28,26,24,4,3,1,0]$, $Q_6[j] = Q_5[j]$.
- *Case One:*
  - $Q_5[31,27] = 1$;
  - $Q_6[27] = 0$;
  - $j \in [30,29,28]$, $Q_6[j] = Q_5[j]$.
- *Case Two:*
  - $Q_5[27] = 0$;

- $Q_6[27] = 1$.

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_5[25,23] &= Q_6[9,8,5,2] &&= Q_7[26,16,10-6,4-0] = 0; \\ Q_5 5,2] &= Q_6[25,11,10] &&= Q_7[25-17,15-11,5] \;\; = 1; \end{aligned}$$

$$Q_6[26,24,4,3,1,0] = Q_5[26,24,4,3,1,0].$$

Case One: Additional Conditions

$$\begin{aligned} Q_7[31-27] &= 0; \\ Q_5[31] &= \overline{Q_6[31] \oplus Q_7[31]}; \\ Q_6[30,29,28] &= Q_5[30,29,28]. \end{aligned}$$

Note that the condition on $Q_5[31]$ combines with the condition $Q_5[31] = Q_4[31]$ required for f_6, to define $Q_4[31]$.

t	Cumulative Conditions on Q_t: *Case One*
4	`C.......0^^^1^^^^^^^1^^^^0......`
5	`Cvvv1v0v0100000000000000001vv1vv`
6	`B^^^0^1^01111111101111000010^^0^^`
7	`A00000111111111011111000001000000`
	$C = \overline{A \oplus B}$

Case Two: Additional Conditions

$$\begin{aligned} Q_6[27] &= Q_7[27] = 1; \\ Q_5[27] &= Q_7[31] = 0. \end{aligned}$$

Note that the condition $Q_5[31] = 0$ combines with the condition $Q_5[31] = Q_4[31]$ required for f_6, to define $Q_4[31] = 0$.

t	Cumulative Conditions on Q_t: *Case Two*
4	`0.......0^^^1^^^^^^^1^^^^0......`
5	`0...0v0v0100000000000000001vv1vv`
6	`....1^1^01111111101111000010^^0^^`
7	`1...10111111111011111000001000000`

Round 8: The attacker has

- $\delta Q_6 = \pm 2^{31} + 2^{23} - 2^{6}$,
- $\delta Q_7 = -2^{27} + 2^{23} - 2^{6} - 2^{0}$, and
- $\delta Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^{0}$.

The attacker wants $\delta f_7 = +2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^{8} + 2^{6}$.

Obtaining Correct $\varDelta Q_t$:

- Obtaining difference (-2^{20}) in f_9 requires the difference (-2^{17}) in Q_8 to propagate to bit 20. This requires $Q_8[20] = 1$ and $Q_8[19,18,17] = 0$.
- Obtaining difference $(+2^{16})$ in f_8 requires the difference (-2^{15}) in Q_8 to propagate to bit 16. This requires $Q_8[16] = 1$ and $Q_8[15] = 0$.

- Otherwise, it is best if the add-differences do not propagate. Thus, for the difference (-2^{23}) we want $Q_8[23] = 1$, and for the difference $(+2^0)$ we want $Q_8[0] = 0$.
- It is now possible to obtain $\nabla f_8[31, 16, 10, 8, 6] =$"+" and $\nabla f_8[24] =$"-".

Case One: (See explanation of Round 7).

	δ	∇
Q_6	$\overset{\pm}{31}, \overset{+}{23}, \overset{-}{6}$	`±.......+................-......`
Q_7	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	`±+++++---...........-+++++-+++++`
Q_8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	`........-..-+++-+..............+`
f_8	$\overset{\pm}{31}, \overset{-}{24}, \overset{+}{16}, \overset{+}{10}, \overset{+}{8}, \overset{+}{6}$	`±......-.......+.....+.+.+......`

Case Two: (See explanation of Round 7).

	δ	∇
Q_6	$\overset{\pm}{31}, \overset{+}{23}, \overset{-}{6}$	`±.......+................-......`
Q_7	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	`....-+---...........-+++++-+++++`
Q_8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	`........-..-+++-+..............+`
f_8	$\overset{\pm}{31}, \overset{-}{24}, \overset{+}{16}, \overset{+}{10}, \overset{+}{8}, \overset{+}{6}$	`±......-.......+.....+.+.+......`

Conditions to get correct ΔQ_t:

- $Q_8[19, 18, 17, 15, 0] = 0$;
- $Q_8[23, 20, 16] = 1$.

Obtaining Correct δf_t:

Constant bits of Q_8: $\Delta Q_8[j] = 0$, for $j \in [27 - 24, 22, 21, 14 - 1]$, where the function either

- selects $f_8[j] = Q_7[j]$ and $f_8^*[j] = Q_7^*[j]$ (when $Q_8[j]] = 1$), or
- selects $f_8[j] = Q_6[j]$ and $f_8^*[j] = Q_6^*[j]$ (when $Q_8[j] = 0$).

We deduce that:

- For $j \in [27, 26, 25, 11, 9, 7, 5 - 1]$, $\Delta f_8[j] = 0$, requires $Q_8[j] = 0$.
- For $j \in [10, 8, 6]$, $\nabla f_8[j] = +1$, requires $Q_8[j] = 1$.
- $\nabla f_8[24] = -1$, requires $Q_8[24] = 1$.
- No conditions are required for bits $j \in [22, 21, 14, 13, 12]$.
- *Case One:*
  - The attacker obtains $\nabla f_8[31] = \pm 1$, irrespective of the value of $Q_8[31]$, so this results in no conditions.
  - For $j \in [30, 29, 28]$, $\Delta f_8[j] = 0$, requires $Q_8[j] = 0$.
- *Case Two:*
  - $\nabla f_8[31] = \pm 1$, requires $Q_8[j] = 0$.
  - No conditions are required for bits $j \in [30, 29, 28]$.
- *Conditions from constant bits of Q_8:*
  - $Q_8[27, 26, 25, 11, 9, 7, 5 - 1] = 0$;
  - $Q_8[24, 10, 8, 6] = 1$.

- *Case One:* $Q_8[30,29,28]=0$.
- *Case Two:* $Q_8[31]=0$.

Non-Constant bits of Q_8:

$\underline{\nabla Q_8[j]=+1,\ j\in[19,18,17,15,0]}$: $Q_8[j]=0/1, \Rightarrow f_8[j]=Q_6[j]/Q_6^*[j]$.
- For the bits $j\in[19,18,17,15]$, $f_8^*[j]=f_8[j]$, requires $Q_7^*[j]=Q_7[j]=Q_6[j]$.
- $f_8^*[0]=f_8[0]$, requires $Q_6[0]=Q_7^*[0]=1$, since $Q_7^*[0]=1$, is already specified ($\varDelta Q_7[0]=+1$).

$\underline{\nabla Q_8[j]=-1,\ j\in[23,20,16]}$: $Q_8[j]=1/0, \Rightarrow f_8[j]=Q_7[j]/Q_6^*[j]$.
- The values $Q_6^*[23]=1$ and $Q_7[23]=1$ are already specified, resulting in $f_8^*[23]=f_8[23]=1$.
- $f_8^*[20]=f_8[20]$, requires $Q_6^*[20]=Q_6[20]=Q_7[20]$.
- $f_8^*[16]-f_8[16]=+1$, requires $Q_6^*[16]-Q_7[16]=+1$, and thus $Q_6^*[16]=Q_6[16]=1$ and $Q_7[16]=Q_7^*[16]=0$.

Conditions from non-constant bits of Q_8:
- $Q_6[16,0]=1$;
- $Q_7[16]=0$;
- $j\in[20-17,15]$, $Q_7[j]=Q_6[j]$.

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_7[16] &= Q_8[27,26,25,19,18,17,15,11,9,7,5-0]=0;\\ Q_6[16,0]=Q_7[0] &= Q_8[24,23,20,16,10,8,6] \qquad\qquad =1;\\ Q_6[20-17,15] &= Q_7[20-17,15]. \end{aligned}$$

Note that the condition $Q_6[0]=1$ combines with the condition $Q_5[0]=Q_6[0]$ required for f_7, and thus we obtain $Q_5[0]=1$. Interestingly, the conditions:

$$\begin{gathered} Q_6[20-17,15]=Q_7[20-17,15];\\ Q_7[16]=0; \quad Q_6[16]=1; \end{gathered}$$

were already satisfied as a consequence of previous independent requirements for f_6 and f_7. Alternatively, one could say that the other requirements stipulated the values of $\varDelta f_8[20-15]$.

Case One: Additional Conditions: $Q_8[30,29,28]=0$.

t	Cumulative Conditions on Q_t: *Case One*
5	`Cvvv1v0v010000000000000000001vv1v1`
6	`B^^^0^1^0111111110111100010^^0^1`
7	`A00000111111111011111000001000000`
8	`.00000011..100010...010101000000`
	$C=\overline{A\oplus B}$

Case Two: Additional Condition: $Q_8[31]=0$.

t	Cumulative Conditions on Q_t: *Case Two*
5	`0...0v0v010000000000000000001vv1v1`
6	`....1^1^0111111110111100010^^0^1`
7	`1...10111111111011111000001000000`
8	`0...00011..100010...010101000000`

Round 9: The attacker has

- $\delta Q_7 = -2^{27} + 2^{23} - 2^6 - 2^0$,
- $\delta Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^0$, and
- $\delta Q_9 = -2^{31} - 2^6 + 2^0$.

The attacker wants $\delta f_9 = \pm 2^{31} + 2^{26} - 2^{23} - 2^{20} + 2^6 + 2^0$.

Obtaining Correct $\varDelta Q_t$:

- Obtaining difference (-2^8) in f_{11} requires the difference (-2^6) in Q_9 to propagate to bit 8 exactly. This requires $Q_9[8] = 1$ and $Q_9[7, 6] = 0$.
- Obtaining difference (-2^0) in f_{11} requires the difference (2^0) in Q_9 to have $\nabla Q_9[0] =$“−”. This requires the addition to propagate to at least bit 1. It is best if the add-difference does not propagate further. Thus, we add conditions $Q_9[1] = 0$ and $Q_9[0] = 1$.
- No conditions for bit 31?
- It is now possible to obtain the add-difference by using $\nabla f_9[31] = \pm$, $\nabla f_9[26, 6, 0] =$“+” and $\nabla f_9[23, 20] =$“−”.

Case One: (See explanation of Round 7).

	δ	∇
Q_7	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	±+++++−−−...........−+++++−+++++
Q_8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	........−..−+++−+..............+
Q_9	$\overset{\pm}{31}, \overset{-}{6}, \overset{+}{0}$	±......................−++....+−
f_9	$\overset{\pm}{31}, \overset{+}{26}, \overset{-}{23}, \overset{-}{20}, \overset{+}{6}, \overset{+}{0}$	±....+..−..−.............+.....+

Case Two: (See explanation of Round 7).

	δ	∇
Q_7	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	....−+−−−...........−+++++−+++++
Q_8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	........−..−+++−+..............+
Q_9	$\overset{\pm}{31}, \overset{-}{6}, \overset{+}{0}$	±......................−++....+−
f_9	$\overset{\pm}{31}, \overset{+}{26}, \overset{-}{23}, \overset{-}{20}, \overset{+}{6}, \overset{+}{0}$	±....+..−..−.............+.....+

Conditions to get correct $\varDelta Q_t$:

- $Q_9[7, 6, 1] = 0$;
- $Q_9[8, 0] = 1$.

Obtaining Correct δf_t:

Constant bits of Q_9: $\varDelta Q_9[j] = 0$, for $j \in [30-9, 5-2]$, where the function either

- selects $f_9[j] = Q_8[j]$ and $f_9^*[j] = Q_8^*[j]$ (when $Q_9[j]] = 1$), or
- selects $f_9[j] = Q_7[j]$ and $f_9^*[j] = Q_7^*[j]$ (when $Q_9[j] = 0$).

We deduce that:

- The attacker obtains $\nabla f_9[23] = -1$, irrespective of the value of $Q_9[23]$, so this results in no conditions.
- For $j \in [27, 25, 24, 11, 10, 9, 5-2]$, $\varDelta f_9[j] = 0$, requires $Q_9[j] = 1$ to select from Q_8 rather than Q_7.

- For $j \in [19-15]$, $\Delta f_9[j] = 0$, requires $Q_9[j] = 0$ to select from Q_7 rather than Q_8.
- $\nabla f_9[26] = +1$, requires $Q_9[26] = 0$.
- $\nabla f_9[20] = +1$, requires $Q_9[20] = 1$.
- No conditions are required for bits $j \in [22, 21, 14-12]$.
- *Case One:*
  - For $j \in [30, 29, 28]$, $\Delta f_9[j] = 0$, requires $Q_9[j] = 1$ to select from Q_8 rather than Q_7.
- *Case Two:*
  - No conditions are required for bits $j \in [30, 29, 28]$.
- *Conditions from constant bits of Q_9:*
  - $Q_9[26, 19-15] = 0$;
  - $Q_9[27, 25, 24, 20, 11, 10, 9, 5-2] = 1$.
  - *Case One:* $Q_9[30, 29, 28] = 1$.

Non-Constant bits of Q_9:

$\underline{\nabla Q_9[j] = +1,\ j \in [7, 6, 1]:}$ $Q_9[j] = 0/1, \Rightarrow f_9[j] = Q_7[j]/Q_8^*[j]$.

- For the bits $j \in [7, 1]$, $f_9^*[j] = f_9[j]$, requires $Q_8^*[j] = Q_7[j] = 0$, since $Q_7[j] = 0$, is already specified ($\Delta Q_7[j] = +1$). Thus, $Q_8[j] = 0$, $j \in [7, 1]$.
- $f_9^*[6] - f_9[6] = +1$, requires $Q_8^*[6] - Q_7[6] = +1$, and hence $Q_8^*[6] = 1$, since $Q_7^*[6] = 0$, is already specified ($\Delta Q_7[6] = +1$).

$\underline{\nabla Q_9[j] = -1,\ j \in [8, 0]:}$ $Q_9[j] = 1/0, \Rightarrow f_9[j] = Q_8[j]/Q_7^*[j]$.

- $f_9^*[8] = f_9[8]$, requires $Q_7^*[8] = Q_8[8] = 1$, since $Q_7^*[8] = 1$, is already specified ($\Delta Q_7[8] = +1$).
- The values $\Delta Q_9[0] = -1$, $Q_8[0] = Q_7[0] = +1$, are already specified, resulting in $\Delta f_9^*[0] = +1$.

$\underline{\nabla Q_9[31] = \pm 1:}$ Need $\nabla f_9[31] = \pm 1$.

- *Case One.*
  - $\nabla(Q_9[31], Q_7[31]) = (+,+)$: $f_9[31] = Q_7[31] = 0, \Rightarrow Q_8[31] = 1$.
  - $\nabla(Q_9[31], Q_7[31]) = (+,-)$: $f_9[31] = Q_7[31] = 1, \Rightarrow Q_8[31] = 0$.
  - $\nabla(Q_9[31], Q_7[31]) = (-,+)$: $f_9^*[31] = Q_7^*[31] = 1, \Rightarrow Q_8[31] = 0$.
  - $\nabla(Q_9[31], Q_7[31]) = (-,-)$: $f_9^*[31] = Q_7^*[31] = 0, \Rightarrow Q_8[31] = 1$.
  - These conditions are summarized by $Q_8[31] = \overline{Q_7[31] \oplus Q_8[31]}$.
- *Case Two:* $\nabla Q_7[31] = 1$, $\nabla Q_8[31] = 0$, and $\nabla Q_7[31] = \pm 1$, implies $\nabla f_9 = \pm 1$. No additional conditions.

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_8[7,1] = Q_9[26, 19-15] &= 0; \\ Q_8[8,6] = Q_9[27, 25, 24, 20, 11-8, 5-2, 0] &= 1; \end{aligned}$$

Interestingly, the conditions:

$$Q_8[7, 1] = 0; \;\; Q_8[8, 6] = 1;$$

were already satisfied as a consequence of previous independent requirements for f_8. Alternatively, one could say that the other requirements stipulated the values of $f_9[8,7,6,1]$. *Case One:* Additional Conditions:

$$Q_9[30,29,28] = 1;$$
$$Q_8[31] = \overline{Q_7[31] \oplus Q_8[31]}$$

t	Cumulative Conditions on Q_t: *Case One*
6	`B^^^0^1^0111111110111100010^^0^1`
7	`A0000011111111101111100000100000`
8	`D0000011..100010...010101000000`
9	`E1111011...100000.....1100111101`
	$E = \overline{A \oplus D}$

Case Two: Additional Conditions: none.

t	Cumulative Conditions on Q_t: *Case Two*
6	`....1^1^0111111110111100010^^0^1`
7	`1...1011111111101111100000100000`
8	`0...00011..100010...010101000000`
9	`....1011...100000.....1100111101`

Round 10: The attacker has

- $\delta Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^0$,
- $\delta Q_9 = \pm 2^{31} - 2^6 + 2^0$, and
- $\delta Q_{10} = \pm 2^{31} + 2^{12}$.

The attacker wants $\delta f_{10} = -2^{23} + 2^{13} + 2^6 + 2^0$.

<u>**Obtaining Correct ΔQ_t:**</u>

- Obtaining difference $(+2^{13})$ in f_{10} requires the difference $(+2^{12})$ in Q_{10} to propagate to bit 13 exactly. This requires $Q_{10}[13] = 0$, $Q_{10}[12] = 1$.
- It is now possible to obtain $\nabla f_{10}[13,6,0] =$"+" and $\nabla f_{10}[23] =$"–".

	δ	∇
Q_8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	`........-..-+++-+..............+`
Q_9	$\overset{\pm}{31}, \overset{-}{6}, \overset{+}{0}$	`±......................-++....+-`
Q_{10}	$\overset{\pm}{31}, \overset{+}{12}$	`±.................+-............`
f_{10}	$\overset{-}{23}, \overset{+}{13}, \overset{+}{6}, \overset{+}{0}$	`........-.........+......+.....+`

Conditions to get correct ΔQ_t:

- $Q_{10}[13] = 0$;
- $Q_{10}[12] = 1$.

<u>**Obtaining Correct δf_t:**</u>

Constant bits of Q_{10}: $\Delta Q_{10}[j] = 0$, for $j \in [30-14, 11-0]$, where the function either

- selects $f_{10}[j] = Q_9[j]$ and $f^*_{10}[j] = Q^*_9[j]$ (when $Q_{10}[j]] = 1$), or

- selects $f_{10}[j] = Q_8[j]$ and $f^*_{10}[j] = Q^*_8[j]$ (when $Q_{10}[j] = 0$).

We deduce that:

- For $j \in [20-15]$, $\varDelta f_{10}[j] = 0$, requires $Q_{10}[j] = 1$.
- For $j \in [8,7,1]$, $\varDelta f_{10}[j] = 0$, requires $Q_{10}[j] = 0$.
- $\varDelta f_{10}[23] = -1$, requires $Q_{10}[23] = 0$.
- $\varDelta f_{10}[6] = +1$, requires $Q_{10}[6] = 1$.
- $\varDelta f_{10}[0] = +1$, requires $Q_{10}[0] = 0$.
- No conditions are required for bits $j \in [30-24, 14, 11-9, 5-2]$.
- *Conditions from constant bits of* Q_{10}*:*
  - $Q_{10}[23, 8, 7, 1, 0] = 0$;
  - $Q_{10}[20-15, 6] = 1$.

Non-Constant bits of Q_{10}:

$\underline{\nabla Q_{10}[j] = +1,\ j \in [13]}$: $Q_{10}[j] = 0/1, \Rightarrow f_{10}[j] = Q_8[j]/Q^*_8[j]$.

- $f^*_{10}[13] - f_{10}[13] = +1$, requires $Q^*_9[13] - Q_8[13] = +1$, which implies that $Q^*_9[13] = Q_9[13] = 1$ and $Q^*_8[13] = Q_8[13] = 0$.

$\underline{\nabla Q_{10}[j] = -1,\ j \in [12]}$: $Q_{10}[j] = 1/0, \Rightarrow f_{10}[j] = Q_9[j]/Q^*_8[j]$.

- $f^*_{10}[12] = f_{10}[12]$, requires $Q^*_8[12] = Q_8[12] = Q_9[12]$.

$\underline{\nabla Q_{10}[31] = \pm 1}$:

- $\nabla(Q_{10}[31], Q_9[31]) = (+,+)$: $f^*_{10}[31] = Q^*_9[31] = 1, \Rightarrow Q_8[31] = 1$.
  - *Case Two* is impossible in this case since $Q_8[31] = 0$ already specified.
- $\nabla(Q_{10}[31], Q_9[31]) = (+,-)$: $f^*_{10}[31] = Q^*_9[31] = 0, \Rightarrow Q_8[31] = 0$.
- $\nabla(Q_{10}[31], Q_9[31]) = (-,+)$: $f_{10}[31] = Q_9[31] = 0, \Rightarrow Q_8[31] = 0$.
- $\nabla(Q_{10}[31], Q_9[31]) = (-,-)$: $f_{10}[31] = Q_9[31] = 1, \Rightarrow Q_8[31] = 1$.
  - *Case Two* is impossible in this case since $Q_8[31] = 0$ already specified.
- These conditions are summarized by:
  - *Case One:* $Q_{10}[31] = \overline{Q_8[31] \oplus Q_9[31]}$.
  - *Case Two:* $Q_{10}[31] = \overline{Q_9[31]}$.

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_8[13] &= Q_{10}[23, 13, 8, 7, 1, 0] = 0; \\ Q_9[13] &= Q_{10}[20-15, 12, 6] \quad = 1; \\ Q_8[12] &= Q_9[12]. \end{aligned}$$

Case One: Additional Conditions:

$$Q_{10}[31] = \overline{Q_8[31] \oplus Q_9[31]} = Q_7[31].$$

t	Cumulative Conditions on Q_t: *Case One*
7	`A00000111111111011111000001000000`
8	`D00000011..100010.0v010101000000`
9	`E1111011...100000.1^..1100111101`
10	`A.......0..111111101...001....00`
	$E = \overline{A \oplus D}$

Case Two: Additional Conditions: $Q_{10}[31] = \overline{Q_9[31]}$.

t	Cumulative Conditions on Q_t: *Case Two*
7	`1...10111111111101111100000100000`
8	`0...00011..100010.0v010101000000`
9	`F...1011...100000.1^..1100111101`
10	`G.......0..111111101...001....00`
	$G = \overline{F}$

Round 11: The attacker has

- $\delta Q_9 = \pm 2^{31} - 2^6 + 2^0$,
- $\delta Q_{10} = \pm 2^{31} + 2^{12}$, and
- $\delta Q_{11} = \pm 2^{31} + 2^{30}$.

The attacker wants $\delta f_{11} = -2^8 - 2^0$.

Obtaining Correct $\varDelta Q_t$:

- It is already possible to obtain $\nabla f_{11}[8, 0] =$"`-`".
- The difference $\delta Q_{11} = \pm 2^{31} + 2^{30}$ could be

  $\nabla Q_{11} =$ `.-...`, with $\varDelta Q_{11}[31] = 0$ or

  $\nabla Q_{11} =$ $\pm$`+...`, with $\varDelta Q_{11}[31] = 1$.

  In the first case, $Q_{11}[31]$ will select either:
  - $f_{11}[31] = Q_9[31]/Q_9[31]$, and $\nabla f_{11}[31] = \nabla Q_9[31] = \pm$; or
  - $f_{11}[31] = Q_{10}[31]/Q_{10}[31]$, and $\nabla f_{11}[31] = \nabla f_{10}[31] = \pm$.

  Since we need $\varDelta f_{11}[31] = 0$, this eliminates the first case. Therefore, the attacker needs $\nabla Q_{11} = \pm$`+`.... That is, the attacker needs $Q_{11}[30] = 0$.

	δ	∇
Q_9	$\overset{\pm}{31}, \overset{-}{6}, \overset{+}{0}$	$\pm$`......................-++....+-`
Q_{10}	$\overset{\pm}{31}, \overset{+}{12}$	$\pm$`.................+-............`
Q_{11}	$\overset{+}{31}, \overset{+}{30}$	$\pm$`+..............................`
f_{11}	$\overset{-}{8}, \overset{-}{0}$	`.......................-.......-`

Conditions to get correct $\varDelta Q_t$:

- $Q_{11}[30] = 0$.

Obtaining Correct δf_t:

Constant bits of Q_{11}: $\varDelta Q_{11}[j] = 0$, for $j \in [29 - 0]$, where the function either

- selects $f_{11}[j] = Q_{10}[j]$ and $f^*_{11}[j] = Q^*_{10}[j]$ (when $Q_{11}[j]] = 1$), or
- selects $f_{11}[j] = Q_9[j]$ and $f^*_{11}[j] = Q^*_9[j]$ (when $Q_{11}[j] = 0$).

We deduce that:

- For $j \in [13, 12]$, $\varDelta f_{11}[j] = 0$, requires $Q_{11}[j] = 0$.
- For $j \in [7, 6, 1]$, $\varDelta f_{11}[j] = 0$, requires $Q_{11}[j] = 1$.
- For $j \in [8, 0]$, $\nabla f_{11}[j] = +1$, requires $Q_{11}[j] = 0$.
- No conditions are required for bits $j \in [29 - 14, 11 - 9, 5 - 2]$.
- *Conditions from constant bits of Q_{11}:*
  - $Q_{11}[13, 12, 8, 0] = 0$;

- $Q_{11}[7, 6, 1] = 1$.

Non-Constant bits of Q_{11}:

$\nabla Q_{11}[j] = +1,\ j \in [30]$: $Q_{11}[j] = 0/1, \Rightarrow f_{11}[j] = Q_9[j]/Q_9^*[j]$.

– $f_{11}^*[30] = f_{11}[30]$, requires $Q_9^*[30] = Q_9[30] = Q_{10}[30]$.

$\nabla Q_{11}[31] = \pm 1$: Note $\nabla Q_{10}[31] = \pm 1$, $\nabla Q_{10}[31] = \pm 1$. Attacker wants $f_{11}^*[31] = f_{11}[31]$

– $\nabla Q_{11}[31] =$"+": $Q_{11}[j] = 0/1, \Rightarrow f_{11}[j] = Q_9[j]/Q_{10}^*[j]$. Thus, $f_{11}^*[31] = f_{11}[31]$ requires $Q_{10}^*[31] = Q_9[31]$. We require $Q_{10}[31] = \overline{Q_9[31]}$.

– $\nabla Q_{11}[31] =$"–": $Q_{11}[j] = 1/0, \Rightarrow f_{11}[j] = Q_{10}[j]/Q_9^*[j]$. Thus, $f_{11}^*[31] = f_{11}[31]$ requires $Q_9^*[31] = Q_{10}[31]$. Similarly, we require $Q_{10}[31] = \overline{Q_9[31]}$.

– In either case, the requirement is $Q_{10}[31] = \overline{Q_9[31]}$.

Conditions from non-constant bits of Q_{11}:

– $Q_9[30] = Q_{10}[30]$;

– $Q_{10}[31] = \overline{Q_9[31]}$.

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_{11}[13, 12, 8, 0] &= 0; \\ Q_{11}[7, 6, 1] &= 1; \\ Q_9^*[30] &= Q_{10}[30]. \\ Q_{10}[31] &= \overline{Q_9[31]}. \end{aligned}$$

Note that the condition $Q_9^*[30] = Q_{10}[30]$ combines with the condition $Q_9^*[30] = 1$ required for f_9, and thus we obtain $Q_{10}[30] = 1$.

Case One: The condition $Q_{10}[31] = \overline{Q_9[31]}$ combines with the condition: $Q_8[31] = \overline{Q_9[31] \oplus Q_{10}[31]}$ required for *Case One* in f_{10}, and we thus obtain $Q_8[31] = 0$.

t	Cumulative Conditions on Q_t: *Case One*
8	`000000011..100010.0v010101000000`
9	`E1111011...100000.1^..1100111101`
10	`A1......0..111111101...001....00`
11	`.0....vv..........00...011....10`
	$E = \overline{A}$

Case Two: The condition $Q_{10}[31] = \overline{Q_9[31]}$ is already satisfied.

t	Cumulative Conditions on Q_t: *Case Two*
8	`0...00011..100010.0v010101000000`
9	`F...1011...100000.1^..1100111101`
10	`G1......0..111111101...001....00`
11	`.0................00...011....10`
	$G = \overline{F}$

Interestingly, the conditions on the MSB are identical for Q_8, Q_9 and Q_{10} for both *Case One* and *Case Two.*

Round 12: The attacker has

- $\delta Q_{10} = \pm 2^{31} + 2^{12}$,
- $\delta Q_{11} = \pm 2^{31} + 2^{30}$, and
- $\delta Q_{12} = \pm 2^{31} - 2^{13} - 2^{7}$.

The attacker wants $\delta f_{12} = \pm 2^{31} + 2^{17} + 2^{7}$.

Obtaining Correct ΔQ_t:

- Obtaining difference $(+2^{18})$ in f_{14} requires the difference (-2^{13}) in Q_{12} to propagate to bit 19 exactly. It is best if the add-difference does not propagate further. Thus, we add conditions $Q_{12}[19] = 1$ and $Q_{12}[18 - 13] = 0$.
- Since $Q_{11}[7] = 1$ and $Q_{11}[7] = 0$ are already specified, the only way to get $\nabla f_{12}[7] =$"+" is to have $\nabla Q_{12}[7] =$"+". This means that the difference (-2^{7}) must propagate to at least bit 8. It is best if the add-difference does not propagate further. Thus, we add conditions $Q_{12}[8] = 1$ and $Q_{12}[7] = 0$.
- Note that $Q_{10}[19, 18, 17] = 1$, is already specified. It is impossible to get $\nabla f_{12}[j] =$"+" for the bit positions 17 and 18 since $f_{12}[j] = Q_{10}[j] = 1$ is selected for both bit positions. The only way to get the difference $(+2^{17})$ is to have
  - $\nabla f_{12}[17] =$"-" by specifying $Q_{11}[17] = 0$;
  - $\nabla f_{12}[18] =$"-" by specifying $Q_{11}[18] = 0$; and
  - $\nabla f_{12}[19] =$"+" by specifying $Q_{11}[19] = 0$.

	δ	∇
Q_{10}	$\overset{\pm}{31}, \overset{+}{12}$	±.................+-............
Q_{11}	$\overset{\pm}{31}, \overset{+}{30}$	±+..............................
Q_{12}	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$	±...........-++++++....-+.......
f_{12}	$\overset{\pm}{31}, \overset{+}{17}, \overset{+}{7}$	±...........+--.........+.......

Conditions to get correct ΔQ_t:

- $Q_{12}[18 - 13, 7] = 0$;
- $Q_{12}[19, 8] = 1$;
- $Q_{11}[19, 18, 17] = 0$.

Obtaining Correct δf_t:

Constant bits of Q_{12}: $\Delta Q_{12}[j] = 0$, for $j \in [30 - 20, 12 - 9, 6 - 0]$:

- $Q_{12}[j] = 1$, selects $f_{12}[j] = Q_{11}[j]$ and $f^*_{12}[j] = Q^*_{11}[j]$, or
- $Q_{12}[j] = 0$, selects $f_{12}[j] = Q_{10}[j]$ and $f^*_{12}[j] = Q^*_{10}[j]$.

We deduce that:

- $\Delta f_{12}[30] = 0$, requires $Q_{12}[30] = 0$.
- $\Delta f_{12}[12] = 0$, requires $Q_{12}[12] = 1$.
- No conditions are required for bits $j \in [30 - 20, 11, 10, 9, 6 - 0]$.
- *Conditions from constant bits of Q_{12}:*
  - $Q_{12}[30] = 0$;
  - $Q_{12}[12] = 1$.

Non-Constant bits of Q_{12}:

Bits [19-17] are discussed under heading “Obtaining Correct ΔQ_t.”

$\underline{\nabla Q_{12}[j] = +1,\ j \in [16-13, 7]:}$ $Q_{12}[j] = 0/1, \Rightarrow f_{12}[j] = Q_{10}[j]/Q^*_{10}[j]$.

- For the bits $j \in [16, 15, 14, 7]$, $f^*_{12}[j] = f_{12}[j]$, requires $Q^*_{11}[j] = Q_{11}[j] = Q_{10}[j]$.
- $f^*_{12}[13] = f_{12}[13]$, requires $Q^*_{11}[13] = Q_{10}[13] = 0$, since $Q_{10}[13] = 0$, is already specified ($\Delta Q_{10}[13] = +1$). Thus, $Q_{11}[13] = 0$.

$\underline{\nabla Q_{12}[j] = -1,\ j \in [8]:}$ $Q_{12}[j] = 1/0, \Rightarrow f_{12}[j] = Q_{11}[j]/Q^*_{10}[j]$.

- $f^*_{12}[8] = f_{12}[8]$, requires $Q^*_{10}[8] = Q_{10}[8] = Q_{11}[8]$.

$\underline{\nabla Q_{12}[31] = \pm 1:}$ Note $\nabla Q_{10}[31] = \pm 1$, $\nabla Q_{11}[31] = \pm 1$. Attacker wants $f^*_{12}[31] = \overline{f_{12}[31]}$.

- $\nabla Q_{12}[31]$ =“+”: $Q_{12}[j] = 0/1, \Rightarrow f_{12}[j] = Q_{10}[j]/Q^*_{11}[j]$. To obtain $f^*_{12}[31] = \overline{f_{12}[31]}$ requires $Q^*_{11}[31] = \overline{Q_{10}[31]}$. That is, $Q_{11}[31] = Q_{10}[31]$.
- $\nabla Q_{12}[31]$ =“–”: $Q_{12}[j] = 1/0, \Rightarrow f_{12}[j] = Q_{11}[j]/Q^*_{10}[j]$. To obtain $f^*_{12}[31] = \overline{f_{12}[31]}$ requires $Q^*_{10}[31] = \overline{Q_{11}[31]}$. That is, $Q_{11}[31] = Q_{10}[31]$.
- In either case, the requirement is $Q_{11}[31] = Q_{10}[31]$.

Conditions from non-constant bits of Q_{12}:

- $Q_{10}[31, 16, 15, 14, 8, 7] = Q_{11}[31, 16, 15, 14, 8, 7]$;
- $Q_{11}[13] = 0$;

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_{11}[19, 18, 17, 13] &= Q_{12}[30, 18-13, 7] = 0; \\ Q_{10}[19, 18, 17] &= Q_{12}[19, 12, 8] \quad = 1; \\ Q_{10}[31, 16, 15, 14, 8, 7] &= Q_{11}[31, 16, 15, 14, 8, 7]. \end{aligned}$$

The conditions:

$$Q_{10}[19, 18, 17] = 1; \quad Q_{11}[13] = 0; \quad Q_{10}[8, 7] = Q_{11}[8, 7].$$

were already satisfied as a consequence of previous independent requirements for f_{10} and f_{11}. Alternatively, one could say that the other requirements stipulated the values of $f_{12}[19, 18, 17, 13, 8, 7]$. Note that the condition $Q_{10}[16, 15] = Q_{11}[16, 15]$, combines with the condition $Q_{10}[16, 15] = 1$, required for f_{10}, and thus we obtain $Q_{11}[16, 15] = 1$.

Case One:

t	Cumulative Conditions on Q_t: *Case One*
9	`E1111011...100000.1^..1100111101`
10	`A1......0..111111101...001....00`
11	`A0..........000...00...011....10`
12	`.0..........10000001...10.......`
	$E = \overline{A}$

Case Two:

t	Cumulative Conditions on Q_t: *Case Two*
9	F...1011...100000.1^..1100111101
10	G1......0..111111101...001....00
11	G0..........000...00...011....10
12	.0..........10000001...10.......
	$G = \overline{F}$

Round 13: The attacker has

- $\delta Q_{11} = \pm 2^{31} + 2^{30}$,
- $\delta Q_{12} = \pm 2^{31} - 2^{13} - 2^{7}$, and
- $\delta Q_{13} = \pm 2^{31} + 2^{24}$.

The attacker wants $\delta f_{13} = \pm 2^{31} - 2^{13}$.

Obtaining Correct ΔQ_t:

- Obtaining difference $(+2^{25})$ in f_{15} requires the difference $(+2^{24})$ in Q_{13} to propagate to bit 25 exactly. Thus, we add conditions $Q_{13}[25] = 0$ and $Q_{13}[24] = 1$.
- The difference (-2^{13}) can be obtained by specifying values of $Q_{13}[19-13]$ so that f_{13} selects the bits that produce the difference (-2^{13}) in Q_{12}. We look at this below.

	δ	∇
Q_{11}	$\overset{\pm}{31}, \overset{+}{30}$	±+..............................
Q_{12}	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$	±...........−++++++....−+.......
Q_{13}	$\overset{\pm}{31}, \overset{+}{24}$	±.....+−........................
f_{13}	$\overset{\pm}{31}, \overset{-}{13}$	±...........−++++++.............

Conditions to get correct ΔQ_t:

- $Q_{13}[25] = 0$;
- $Q_{13}[24] = 1$.

Obtaining Correct δf_t:

Constant bits of Q_{13}: $\Delta Q_{13}[j] = 0$, for $j \in [30-26, 23-0]$:

- $Q_{13}[j] = 1$, selects $f_{13}[j] = Q_{12}[j]$ and $f^*_{13}[j] = Q^*_{12}[j]$, or
- $Q_{13}[j] = 0$, selects $f_{13}[j] = Q_{11}[j]$ and $f^*_{13}[j] = Q^*_{11}[j]$.

We deduce that:

- $\Delta f_{13}[30] = 0$, requires $Q_{13}[30] = 1$.
- For $j \in [8, 7]$, $\Delta f_{13}[j] = 0$, requires $Q_{13}[j] = 0$.
- To produce the difference (-2^{13}) we must have $\nabla f_{13}[19] = -1$ and $\nabla f_{13}[j] = +1$:
  - $\nabla f_{13}[19] = -1$, requires $Q_{13}[19] = 1$.
  - For $j \in [18-13]$, $\nabla f_{13}[j] = +1$, requires $Q_{13}[j] = 1$.
- No conditions are required for bits $j \in [29-26, 23-20, 12-9, 6-0]$.
- *Conditions from constant bits of Q_{13}:*
  - $Q_{13}[8, 7] = 0$;

- $Q_{13}[30, 19-13] = 1$.

Non-Constant bits of Q_{13}:

$\nabla Q_{13}[j] = +1,\ j \in [25]$: $Q_{13}[j] = 0/1, \Rightarrow f_{13}[j] = Q_{11}[j]/Q^*_{11}[j]$.
 – $f^*_{13}[25] = f_{13}[25]$, requires $Q^*_{12}[25] = Q_{12}[25] = Q_{11}[25]$.

$\nabla Q_{13}[j] = -1,\ j \in [24]$: $Q_{13}[j] = 1/0, \Rightarrow f_{13}[j] = Q_{12}[j]/Q^*_{11}[j]$.
 – $f^*_{13}[24] = f_{13}[24]$, requires $Q^*_{11}[24] = Q_{11}[24] = Q_{12}[24]$.

$\nabla Q_{13}[31] = \pm1$: Note $\nabla Q_{11}[31] = \pm1$, $\nabla Q_{12}[31] = \pm1$. Attacker wants $f^*_{13}[31] = \overline{f_{13}[31]}$. As for Round 12, the requirement is $Q_{12}[31] = Q_{11}[31]$.

Conditions from non-constant bits of Q_{13}:
 – $Q_{11}[31, 25, 24] = Q_{12}[31, 25, 24]$;

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_{13}[25, 8, 7] &= 0; \\ Q_{13}[30, 24, 19-13] &= 1; \\ Q_{11}[31, 25, 24] &= Q_{12}[31, 25, 24]. \end{aligned}$$

It is no longer useful to distinguish between *Case One* and *Case Two*; we show the conditions on the same table from hereon.

t	Cumulative Conditions on Q_t
11	A0....vv....000...00...011....10
12	A0....^^....10000001...10.......
13	.1....01....1111111....00.......

Round 14: The attacker has
 – $\delta Q_{12} = \pm 2^{31} - 2^{13} - 2^7$,
 – $\delta Q_{13} = \pm 2^{31} + 2^{24}$, and
 – $\delta Q_{14} = \pm 2^{31}$.
The attacker wants $\delta f_{14} = \pm 2^{31} + 2^{18}$.
Obtaining Correct ΔQ_t: No conditions required.

	δ	∇
Q_{12}	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$	±...........-++++++....-+.......
Q_{13}	$\overset{\pm}{31}, \overset{+}{24}$	±.....+-........................
Q_{14}	$\overset{\pm}{31}$	±...............................
f_{14}	$\overset{\pm}{31}, \overset{+}{18}$	±............+..................

Conditions to get correct ΔQ_t: none
Obtaining Correct δf_t:
Constant bits of Q_{14}: $\Delta Q_{14}[j] = 0$, for $j \in [30-0]$:
 – $Q_{14}[j] = 1$, selects $f_{14}[j] = Q_{13}[j]$ and $f^*_{14}[j] = Q^*_{13}[j]$, or
 – $Q_{14}[j] = 0$, selects $f_{14}[j] = Q_{12}[j]$ and $f^*_{14}[j] = Q^*_{12}[j]$.
We deduce that:

- For $j \in [25, 24]$, $\Delta f_{14}[j] = 0$, requires $Q_{14}[j] = 0$.
- For $j \in [19, 17-13, 8, 7]$, $\Delta f_{14}[j] = 0$, requires $Q_{14}[j] = 1$.
- $\Delta f_{14}[18] = +1$, requires $Q_{14}[18] = 0$.
- No conditions are required for bits $j \in [30-26, 23-20, 12-9, 6-0]$.
- *Conditions from constant bits of Q_{14}:*
  - $Q_{14}[25, 24, 18] = 0$;
  - $Q_{14}[19, 17-13, 8, 7] = 1$.

Non-Constant bits of Q_{14}:

$\underline{\nabla Q_{14}[31] = \pm 1}$: Note $\nabla Q_{12}[31] = \pm 1$, $\nabla Q_{13}[31] = \pm 1$. Attacker wants $f^*_{14}[31] = \overline{f_{14}[31]}$. As for Round 12, the requirement is $Q_{13}[31] = Q_{12}[31]$.

Conditions from non-constant bits of Q_{14}:

- $Q_{12}[31] = Q_{13}[31]$;

Summary of Requirements resulting from this round:

$$\begin{aligned} Q_{14}[25, 24, 18] &= 0; \\ Q_{14}[19, 17-13, 8, 7] &= 1; \\ Q_{12}[31] &= Q_{13}[31]. \end{aligned}$$

t	Cumulative Conditions on Q_t
11	A0....vv....000...00...011....10
12	A0....^^....10000001...10.......
13	A1....01....1111111....00.......
14	......00....1011111....11.......

Round 15: The attacker has

- $\delta Q_{13} = \pm 2^{31} + 2^{24}$,
- $\delta Q_{14} = \pm 2^{31}$, and
- $\delta Q_{15} = \pm 2^{31} - 2^{15} + 2^{3}$.

The attacker wants $\delta f_{15} = \pm 2^{31} + 2^{25}$.

Obtaining Correct ΔQ_t:

- It is best if the add-differences do not propagate. Thus, for the difference (-2^{15}) we want $Q_{15}[15] = 1$, and for the difference $(+2^3)$ we want $Q_{15}[3] = 0$.

	δ	∇
Q_{13}	$\overset{\pm}{31}, \overset{+}{24}$	±.....+-........................
Q_{14}	$\overset{\pm}{31}$	±...............................
Q_{15}	$\overset{\pm}{31}, \overset{-}{15}, \overset{+}{3}$	±...............-...........+...
f_{15}	$\overset{\pm}{31}, \overset{+}{25}$	±.....+.........................

Conditions to get correct ΔQ_t:

- $Q_{15}[3] = 0$;
- $Q_{15}[15] = 1$.

Obtaining Correct δf_t:

Constant bits of Q_{15}: $\Delta Q_{15}[j] = 0$, for $j \in [30-16, 14-4, 2, 1, 0]$:

- $Q_{15}[j] = 1$, selects $f_{15}[j] = Q_{14}[j]$ and $f^*_{15}[j] = Q^*_{14}[j]$, or
- $Q_{15}[j] = 0$, selects $f_{15}[j] = Q_{13}[j]$ and $f^*_{15}[j] = Q^*_{13}[j]$.

We deduce that:

- $\Delta f_{15}[24] = 0$, requires $Q_{15}[24] = 1$.
- $\Delta f_{15}[25] = +1$, requires $Q_{15}[25] = 0$.
- No conditions are required for bits $j \in [30-26, 23-16, 14-4, 2, 1, 0]$.
- *Conditions from constant bits of Q_{15}:*
  - $Q_{15}[25] = 0$;
  - $Q_{15}[24] = 1$.

Non-Constant bits of Q_{15}:

$\nabla Q_{15}[j] = +1$, $j \in [3]$: $Q_{15}[j] = 0/1, \Rightarrow f_{15}[j] = Q_{13}[j]/Q^*_{14}[j]$.

- $f^*_{15}[3] = f_{15}[3]$, requires $Q^*_{14}[3] = Q_{14}[3] = Q_{13}[3]$.

$\nabla Q_{15}[j] = -1$, $j \in [15]$: $Q_{15}[j] = 1/0, \Rightarrow f_{15}[j] = Q_{14}[j]/Q^*_{13}[j]$.

- $f^*_{15}[15] = f_{15}[15]$, requires $Q^*_{13}[15] = Q_{13}[15] = Q_{14}[15]$.

$\nabla Q_{15}[31] = \pm 1$: Note $\nabla Q_{13}[31] = \pm 1$, $\nabla Q_{14}[31] = \pm 1$. Attacker wants $f^*_{15}[31] = \overline{f_{15}[31]}$. As for Round 12, the requirement is $Q_{14}[31] = Q_{13}[31]$.

Conditions from non-constant bits of Q_{15}:

- $Q_{13}[31, 15, 3] = Q_{14}[31, 15, 3]$;

Summary of Requirements resulting from this round:

$$Q_{15}[25, 3] = 0; \quad Q_{15}[24, 15] = 1;$$
$$Q_{13}[31, 15, 3] = Q_{14}[31, 15, 3].$$

These conditions are added to Table 3. Interestingly, the condition: $Q_{13}[15] = Q_{14}[15]$. was already satisfied as a consequence of previous independent requirements for f_{13} and f_{14}. Alternatively, one could say that the other requirements stipulated the value of $f_{15}[15]$.

t	Cumulative Conditions on Q_t
13	`A1....01....1111111....00...v...`
14	`A.....00....1011111....11...^...`
15	`..1...01........1...........0...`

t	Conditions on Q_t for Rounds 0-15: *Case One*
3	`.........vvv0vvvvvvv0vvvv0......`
4	`C.......0^^^1^^^^^^^1^^^^0......`
5	`Cvvv1v0v0100000000000000001vv1v1`
6	`B^^^0^1^0111111110111100010^^0^1`
7	`A0000011111111101111100000100000`
8	`000000011..100010.0v010101000000`
9	`E1111011...100000.1^..1100111101`
10	`A1......0..111111101...001....00`
11	`A0....vv....000...00...011....10`
12	`A0....^^....10000001...10.......`
13	`A1....01....1111111....00...v...`
	$C = \overline{A \oplus B}$, $E = \overline{A}$

Table 4. Summary of the conditions required to get the correct propagation of differences through f_t for rounds 0 to 15. The values of Q_{14} and Q_{15} will have additional conditions imposed by Rounds 16 and 17, so they are not shown here. These conditions are for *Case One*, that has the same conditions as the example by Wang et al.

t	Conditions on Q_t for Rounds 0-15: *Case Two*
3	`.........vvv0vvvvvvv0vvvv0......`
4	`0.......0^^^1^^^^^^^1^^^^0......`
5	`0...0v0v0100000000000000001vv1v1`
6	`....1^1^0111111110111100010^^0^1`
7	`1...1011111111101111100000100000`
8	`0...00011..100010.0v010101000000`
9	`F...1011...100000.1^..1100111101`
10	`G1......0..111111101...001....00`
11	`G0....vv....000...00...011....10`
12	`G0....^^....10000001...10.......`
13	`G1....01....1111111....00...v...`
	$G = \overline{F}$

Table 5. Summary of the conditions required to get the correct propagation of differences through f_t for rounds 0 to 15. The values of Q_{14} and Q_{15} will have additional conditions imposed by Rounds 16 and 17, so they are not shown here. These conditions are for *Case Two*.

5.2 Rounds 16 to 34 of the First Block

t	δQ_t	∇Q_t	∇f_t	δf_t
14	$\overset{\pm}{31}$	`±.0...00....1011111....11...1...`		
15	$\overset{\pm}{31}, \overset{-}{15}, \overset{+}{3}$	`±.1...01........-...........+...`		
16	$\overset{\pm}{31}, \overset{-}{29}$	`±.-.............v...........v...`	`±.1...0.........v...........v...`	$\overset{\pm}{31}$
17	$\overset{\pm}{31}$	`±.v...........0.^...........^...`	`±...............^...........^...`	$\overset{\pm}{31}$
18	$\overset{\pm}{31}$	`±.^...........1.................`	`±...............................`	$\overset{\pm}{31}$
19	$\overset{\pm}{31}, \overset{+}{17}$	`±.............+.................`	`±.............1.................`	$\overset{\pm}{31}$
20	$\overset{\pm}{31}$	`±.............v.................`	`±.............v.................`	$\overset{+}{31}$
21	$\overset{\pm}{31}$	`±.............^.................`	`±.............^.................`	$\overset{+}{31}$
22	$\overset{\pm}{31}$	`±...............................`	`±...............................`	$\overset{\pm}{31}$
23	-	`0...............................`	`0...............................`	-
24	-	`1...............................`	`±...............................`	$\overset{\pm}{31}$
25-32	-	`................................`	`................................`	-

Table 6. Propagation of differences through the f_t functions for rounds 16 to 32 of the first block. Note $f_t = (Q_{t-2} \wedge Q_t) \oplus (\overline{Q_{t-2}} \wedge Q_{t-1})$ for these rounds.

In rounds 16 to 31, the function changes so that it is now the value of Q_{t-2} that is selecting either Q_t (when $Q_{t-2} = 1$) or Q_t (when $Q_{t-2} = 1$).

These rounds will be easier to describe because the only differences in f_t only occur in the MSB.

Round 16: The attacker has

- $\delta Q_{14} = \pm 2^{31}$,
- $\delta Q_{15} = \pm 2^{31} - 2^{15} + 2^{3}$, and
- $\delta Q_{16} = \pm 2^{31} - 2^{29}$.

The attacker wants $\delta f_{16} = \pm 2^{31}$.

Obtaining Correct ΔQ_t:

- It is best if the add-differences do not propagate. Thus, for the difference (-2^{29}) we want $Q_{16}[29] = 1$.

	δ	∇
Q_{14}	$\overset{\pm}{31}$	`±...............................`
Q_{15}	$\overset{\pm}{31}, \overset{-}{15}, \overset{+}{3}$	`±...............-...........+...`
Q_{16}	$\overset{\pm}{31}, \overset{-}{29}$	`±.-.............................`
f_{16}	$\overset{\pm}{31}$	`±...............................`

Conditions to get correct ΔQ_t:
- $Q_{16}[29] = 1$.

$\underline{\textbf{Obtaining Correct } \delta f_t\textbf{:}}$
Constant bits of Q_{14}: $\Delta Q_{14}[j] = 0$, for $j \in [30 - 0]$:
- $Q_{14}[j] = 1$ selects $f_{16}[j] = Q_{16}[j]$ and $f^*_{16}[j] = Q^*_{16}[j]$, or
- $Q_{14}[j] = 0$ selects $f_{16}[j] = Q_{15}[j]$ and $f^*_{16}[j] = Q^*_{15}[j]$.

We deduce that:
- $\Delta f_{16}[29] = 0$, requires $Q_{14}[29] = 0$.
- For $j \in [15, 3]$, $\Delta f_{16}[j] = 0$, requires $Q_{14}[j] = 1$.
- No conditions are required for bits $j \in [30, 28 - 16, 14 - 3, 2, 1, 0]$.
- *Conditions from constant bits of Q_{16}:*
  - $Q_{14}[29] = 0$;
  - $Q_{14}[15, 3] = 1$.

Non-Constant bits of Q_{14}:
$\underline{\nabla Q_{14}[31] = \pm 1\text{:}}$ Note $\nabla Q_{15}[31] = \pm 1$, $\nabla Q_{16}[31] = \pm 1$. Attacker wants $f^*_{16}[31] = \overline{f_{16}[31]}$.
- $\nabla Q_{14}[31] \underline{\ =\text{“+”}\text{:}}$ $Q_{14}[j] = 0/1, \Rightarrow$ $\underline{f_{16}[j]\ } = Q_{15}[j]/Q^*_{16}[j]$. To obtain $f^*_{16}[31] = \overline{f_{16}[31]}$ requires $Q^*_{16}[31] = \overline{Q_{15}[31]}$. That is, $Q_{15}[31] = Q_{16}[31]$.
- $\nabla Q_{14}[31] \underline{\ =\text{“–”}\text{:}}$ $Q_{14}[j] = 1/0, \Rightarrow$ $\underline{f_{16}[j]\ } = Q_{16}[j]/Q^*_{15}[j]$. To obtain $f^*_{16}[31] = \overline{f_{16}[31]}$ requires $Q^*_{15}[31] = \overline{Q_{16}[31]}$. That is, $Q_{15}[31] = Q_{16}[31]$.
- In either case, the requirement is $Q_{15}[31] = Q_{16}[31]$.

Conditions from non-constant bits of Q_{16}:
- $Q_{15}[31] = Q_{16}[31]$.

Summary of Requirements resulting from this round:

$$Q_{14}[29] = 0; \quad Q_{14}[15, 3] = 1$$
$$Q_{15}[31] = Q_{16}[31].$$

Interestingly, the condition $Q_{14}[15] = 1$, was already satisfied as a consequence of previous independent requirements for f_{10}. Alternatively, one could say that the other requirements stipulated the values of $f_{16}[15]$. Note that the condition $Q_{14}[3] = 1$ combines with the condition $Q_{13}[3] = Q_{14}[3]$ required for f_{15}, and thus we obtain $Q_{13}[3] = 1$.

t	Cumulative Conditions on Q_t
13	`A1....01....1111111....00...1...`
14	`A.....00....1011111....11...1...`
15	`H.1...01........1...........0...`
16	`H.1.............................`

Round 17: The attacker has
- $\delta Q_{15} = \pm 2^{31} - 2^{15} + 2^{03}$,
- $\delta Q_{16} = \pm 2^{31} - 2^{29}$, and
- and $\delta Q_{17} = \pm 2^{31}$.

The attacker wants $\delta f_{17} = \pm 2^{31}$.
$\underline{\textbf{Obtaining Correct } \Delta Q_t\textbf{:}}$ Already good.

	δ	∇
Q_{15}	$\overset{\pm}{31}, \overset{-}{15}, \overset{+}{3}$	±...............-...........+...
Q_{16}	$\overset{\pm}{31}, \overset{-}{29}$	±.-.............................
Q_{17}	$\overset{\pm}{31}$	±...............................
f_{17}	$\overset{\pm}{31}$	±...............................

Conditions to get correct $\mathit{\Delta} Q_t$: none.
Obtaining Correct δf_t:
Constant bits of Q_{15}: $\mathit{\Delta} Q_{15}[j] = 0$, for $j \in [30-17, 14-44, 2, 1, 0]$:

- $Q_{15}[j] = 1$ selects $f_{17}[j] = Q_{17}[j]$ and $f^*_{17}[j] = Q^*_{17}[j]$, or
- $Q_{15}[j] = 0$ selects $f_{17}[j] = Q_{16}[j]$ and $f^*_{17}[j] = Q^*_{16}[j]$.

We deduce that:

- $\mathit{\Delta} f_{17}[29] = 0$, requires $Q_{15}[29] = 1$.
- No conditions are required for bits $j \in [30, 28-16, 14-4, 2, 1, 0]$.
- *Conditions from constant bits of Q_{17}:*
  - $Q_{15}[29] = 1$.

Non-Constant bits of Q_{15}:
$\nabla Q_{15}[j] = +1$, $j \in [3]$: $Q_{15}[j] = 0/1, \Rightarrow f_{17}[j] = Q_{16}[j]/Q^*_{17}[j]$.

- $f^*_{17}[3] = f_{17}[3]$, requires $Q^*_{17}[3] = Q_{17}[3] = Q_{16}[3]$.

$\nabla Q_{15}[j] = -1$, $j = 15$: $Q_{15}[j] = 1/0, \Rightarrow f_{17}[j] = Q_{17}[j]/Q^*_{16}[j]$.

- $f^*_{17}[15] = f_{17}[15]$, requires $Q^*_{16}[15] = Q_{16}[15] = Q_{17}[15]$.

$\nabla Q_{15}[31] = \pm 1$: Note $\nabla Q_{16}[31] = \pm 1$, $\nabla Q_{17}[31] = \pm 1$. Attacker wants $f^*_{17}[31] = \overline{f_{17}[31]}$. As for Round 16, the attacker requires $Q_{16}[31] = Q_{17}[31]$.

Conditions from non-constant bits of Q_{17}:

- $Q_{16}[31, 15, 3] = Q_{17}[31, 15, 3]$.

Summary of Requirements resulting from this round:

$$Q_{15}[29] = 1;$$
$$Q_{16}[31, 15, 3] = Q_{17}[31, 15, 3].$$

Note that the condition $Q_{15}[29] = 1$ was already specified.

t	Cumulative Conditions on Q_t
15	`H.1...01........1...........0...`
16	`H.1.............v...........v...`
17	`H...............^...........^...`

Round 18: The attacker has

- $\delta Q_{16} = \pm 2^{31} - 2^{29}$,
- $\delta Q_{17} = \pm 2^{31}$, and
- $\delta Q_{18} = \pm 2^{31}$.

The attacker wants $\delta f_{18} = +2^{31}$.
Obtaining Correct $\mathit{\Delta} Q_t$: Already Good.

	δ	∇
Q_{16}	$\overset{\pm}{31},\overset{-}{29}$	`±.-.............................`
Q_{17}	$\overset{\pm}{31}$	`±...............................`
Q_{18}	$\overset{\pm}{31}$	`±...............................`
f_{18}	$\overset{\pm}{31}$	`±...............................`

Conditions to get correct ΔQ_t: none.

Obtaining Correct δf_t:

Constant bits of Q_{16}: $\Delta Q_{16}[j] = 0$, for $j \in [30, 28{-}0]$, and since $\Delta Q_{18}[j] = \Delta Q_{18}[j] = 0$ at these bit positions, it follows that $\Delta f_{18}[j] = 0$ at these bit positions.

- *Conditions from constant bits of Q_{18}:* none.

Non-Constant bits of Q_{16}:

$\nabla Q_{16}[29] = -1$=: $Q_{16}[29] = 1/0, \Rightarrow f_{18}[29] = Q_{18}[29]/Q^*_{17}[29]$.

- $f^*_{18}[29] = f_{18}[29]$, requires $Q^*_{17}[29] = Q_{17}[29] = Q_{18}[29]$.

$\nabla Q_{16}[31] = \pm 1$: Note $\nabla Q_{17}[31] = \pm 1$, $\nabla Q_{18}[31] = \pm 1$. Attacker wants $f^*_{18}[31] = \overline{f_{18}[31]}$. As for Round 16, the attacker requires $Q_{17}[31] = Q_{18}[31]$.

Conditions from non-constant bits of Q_{18}:

- $Q_{17}[31, 29] = Q_{18}[31, 29]$.

Summary of Requirements resulting from this round:

$$Q_{17}[31, 29] = Q_{18}[31, 29].$$

t	Cumulative Conditions on Q_t
16	`H.1.............v...........v...`
17	`H.v.............^...........^...`
18	`H.^.............................`

Round 19: The attacker has

- $\delta Q_{17} = \pm 2^{31}$,
- $\delta Q_{18} = \pm 2^{31}$, and
- $\delta Q_{19} = \pm 2^{31} + 2^{17}$.

The attacker wants $\delta f_{19} = \pm 2^{31}$.

Obtaining Correct ΔQ_t:

- It is best if the add-differences do not propagate. Thus, for the difference $(+2^{17})$ we want $Q_{19}[17] = 0$.

	δ	∇
Q_{17}	$\overset{\pm}{31}$	`±...............................`
Q_{18}	$\overset{\pm}{31}$	`±...............................`
Q_{19}	$\overset{\pm}{31},\overset{+}{17}$	`±..............+................`
f_{19}	$\overset{\pm}{31}$	`±...............................`

Conditions to get correct $\varDelta Q_t$:
- $Q_{19}[17] = 0$.

Obtaining Correct δf_t:
Constant bits of Q_{17}: $\varDelta Q_{17}[j] = 0$, for $j \in [30 - 0]$:
- $Q_{17}[j]] = 1$ selects $f_{19}[j] = Q_{19}[j]$ and $f^*_{19}[j] = Q^*_{19}[j]$, or
- $Q_{17}[j] = 0$ selects $f_{19}[j] = Q_{18}[j]$ and $f^*_{19}[j] = Q^*_{18}[j]$.

We deduce that:
- $\varDelta f_{19}[17] = 0$, requires $Q_{17}[17] = 0$.
- No conditions are required for bits $j \in [30 - 18, 16 - 0]$.
- *Conditions from constant bits of Q_{19}:*
  - $Q_{17}[17] = 0$;

Non-Constant bits of Q_{17}:
$\nabla Q_{17}[31] = \pm 1$: Note $\nabla Q_{18}[31] = \pm 1$, $\nabla Q_{19}[31] = \pm 1$. Attacker wants $f^*_{19}[31] = \overline{f_{19}[31]}$. As for Round 16, the attacker requires $Q_{18}[31] = Q_{19}[31]$.

Conditions from non-constant bits of Q_{19}:
- $Q_{18}[31] = Q_{19}[31]$.

Summary of Requirements resulting from this round:

$$Q_{19}[17] = Q_{17}[17] = 0;$$
$$Q_{18}[31] = Q_{19}[31].$$

t	Cumulative Conditions on Q_t
16	`H.1.............v...........v...`
17	`H.v...........0.^...........^...`
18	`H.^.............................`
19	`H.............0.................`

Round 20: The attacker has
- $\delta Q_{18} = \pm 2^{31}$,
- $\delta Q_{19} = \pm 2^{31} + 2^{17}$, and
- $\delta Q_{20} = \pm 2^{31}$.

The attacker wants $\delta f_{20} = \pm 2^{31}$.
Obtaining Correct $\varDelta Q_t$: Already good.

	δ	∇
Q_{18}	$\overset{\pm}{31}$	`±...............................`
Q_{19}	$\overset{\pm}{31}, \overset{+}{17}$	`±..............+................`
Q_{20}	$\overset{\pm}{31}$	`±...............................`
f_{20}	$\overset{\pm}{31}$	`±...............................`

Conditions to get correct $\varDelta Q_t$: none.
Obtaining Correct δf_t:
Constant bits of Q_{18}: $\varDelta Q_{18}[j] = 0$, for $j \in [30 - 0]$:

- $Q_{18}[j]] = 1$ selects $f_{20}[j] = Q_{20}[j]$ and $f^*_{20}[j] = Q^*_{20}[j]$, or
- $Q_{18}[j] = 0$ selects $f_{20}[j] = Q_{19}[j]$ and $f^*_{20}[j] = Q^*_{19}[j]$.

We deduce that:

- $\Delta f_{20}[17] = 0$, requires $Q_{18}[17] = 1$.
- No conditions are required for bits $j \in [30-18, 16-0]$.
- *Conditions from constant bits of Q_{20}:*
  - $Q_{18}[17] = 1$.

Non-Constant bits of Q_{18}:
<u>$\nabla Q_{18}[31] = +1$.</u> <u>$\nabla Q_{18}[31] = \pm 1$:</u> Note $\nabla Q_{19}[31] = \pm 1$, $\nabla Q_{20}[31] = \pm 1$. Attacker wants $f^*_{20}[31] = \overline{f_{20}[31]}$. As for Round 16, the attacker requires $Q_{19}[31] = Q_{20}[31]$.

Conditions from non-constant bits of Q_{20}:

- $Q_{19}[31] = Q_{20}[31]$.

Summary of Requirements resulting from this round:

$$Q_{18}[17] = 1, Q_{19}[31] = Q_{20}[31].$$

t	Cumulative Conditions on Q_t
18	H.^...........1.................
19	H.............0.................
20	H...............................

Round 21: The attacker has

- $\delta Q_{19} = \pm 2^{31} + 2^{17}$,
- $\delta Q_{20} = \pm 2^{31}$, and
- $\delta Q_{21} = \pm 2^{31}$.

The attacker wants $\delta f_{21} = \pm 2^{31}$.
<u>**Obtaining Correct ΔQ_t:**</u> Already good.

	δ	∇
Q_{19}	$\overset{\pm}{31}, \overset{+}{17}$	±.............+.................
Q_{20}	$\overset{\pm}{31}$	±...............................
Q_{21}	$\overset{\pm}{31}$	±...............................
f_{21}	$\overset{\pm}{31}$	±...............................

Conditions to get correct ΔQ_t: none.
<u>**Obtaining Correct δf_t:**</u>
Constant bits of Q_{19}: $\Delta Q_{19}[j] = 0$, for $j \in [30-18, 16-0]$, and since $\Delta Q_{21}[j] = \Delta Q_{21}[j] = 0$ at these bit positions, it follows that $\Delta f_{21}[j] = 0$ at these bit positions.

- *Conditions from constant bits of Q_{21}:* none.

Non-Constant bits of Q_{19}:
<u>$\nabla Q_{19}[j] = +1$, $j \in [17]$:</u> $Q_{19}[j] = 0/1, \Rightarrow f_{21}[j] = Q_{20}[j]/Q^*_{21}[j]$.

– $f^*_{21}[17] = f_{21}[17]$, requires $Q^*_{21}[17] = Q_{21}[17] = Q_{20}[17]$.

$\nabla Q_{19}[31] = \pm 1$: Note $\nabla Q_{20}[31] = \pm 1$, $\nabla Q_{21}[31] = \pm 1$. Attacker wants $f^*_{21}[31] = \overline{f_{21}[31]}$. As for Round 16, the attacker requires $Q_{20}[31] = Q_{21}[31]$.

Conditions from non-constant bits of Q_{21}*:*

– $Q_{20}[31, 17] = Q_{21}[31, 17]$.

Summary of Requirements resulting from this round:

$$Q_{20}[31, 17] = Q_{21}[31, 17].$$

t	Cumulative Conditions on Q_t
19	`H.............0.................`
20	`H.............v.................`
21	`H.............^.................`

Round 22: The attacker has

– $\delta Q_{20} = \pm 2^{31}$,

– $\delta Q_{21} = \pm 2^{31}$, and

– $\delta Q_{22} = \pm 2^{31}$.

The attacker wants $\delta f_{22} = \pm 2^{31}$.

Obtaining Correct ΔQ_t: Already good.

	δ	∇
Q_{20}	± 31	±...............................
Q_{21}	± 31	±...............................
Q_{22}	± 31	±...............................
f_{22}	± 31	±...............................

Conditions to get correct ΔQ_t: none.

Obtaining Correct δf_t:

Constant bits of Q_{20}: $\Delta Q_{20}[j] = 0$, for $j \in [30 - 0]$, and since $\Delta Q_{22}[j] = \Delta Q_{22}[j] = 0$, at these bit positions, it follows that $\Delta f_{22}[j] = 0$ at these bit positions.

– *Conditions from constant bits of* Q_{22}*:* none.

Non-Constant bits of Q_{20}:

$\nabla Q_{20}[31] = \pm 1$: Note $\nabla Q_{21}[31] = \pm 1$, $\nabla Q_{22}[31] = \pm 1$. Attacker wants $f^*_{22}[31] = \overline{f_{22}[31]}$. As for Round 16, the attacker requires $Q_{21}[31] = Q_{22}[31]$.

Conditions from non-constant bits of Q_{22}*:*

– $Q_{21}[31.] = Q_{22}[31.]$.

t	Cumulative Conditions on Q_t
20	`H.............v.................`
21	`H.............^.................`
22	`H...............................`

Round 23: The attacker has

- $\delta Q_{21} = \pm 2^{31}$,
- $\delta Q_{22} = \pm 2^{31}$, and
- $\delta Q_{23} = 0$.

The attacker wants $\delta f_{23} = 0$.

Obtaining Correct ΔQ_t: no differences.

	δ	∇
Q_{21}	± 31	±...............................
Q_{22}	± 31	±...............................
Q_{23}		....
f_{23}		....

Conditions to get correct ΔQ_t: none.

Obtaining Correct δf_t:

Constant bits of Q_{21}: $\Delta Q_{21}[j] = 0$, for $j \in [30 - 0]$, and since $\Delta Q_{23}[j] = \Delta Q_{23}[j] = 0$ at these bit positions, it follows that $\Delta f_{23}[j] = 0$ at these bit positions.

- *Conditions from constant bits of Q_{23}:*
  - $Q_{21}[29] = 0$;
  - $Q_{21}[15, 3] = 1$.

Non-Constant bits of Q_{21}:

$\nabla Q_{21}[31] = \pm 1$: Note $\nabla Q_{22}[31] = \pm 1$ but $\Delta Q_{23}[31] = 0$. Attacker wants $f^*_{23}[31] = f_{23}[31]$.

- $\nabla Q_{21}[31] =$"+": $Q_{21}[j] = 0/1, \Rightarrow f_{23}[j] = Q_{22}[j]/Q^*_{23}[j]$ where $Q^*_{23}[j] = Q_{23}[j]$. To obtain $f^*_{23}[31] = f_{23}[31]$ requires $Q_{23}[31] = Q_{22}[31]$. That is, $Q_{22}[31] = Q_{21}[31]$.
- $\nabla Q_{21}[31] =$"–": $Q_{21}[j] = 1/0, \Rightarrow f_{23}[j] = Q_{23}[j]/Q^*_{22}[j]$. To obtain $f^*_{23}[31] = \overline{f_{23}[31]}$ requires $Q^*_{22}[31] = Q_{23}[31]$. That is, $Q_{23}[31] = \overline{Q_{22}[31]}$.
- In either case, the requirement is $Q_{23}[31] = Q_{21}[31] \oplus Q_{22}[31]$. However, since we already know that $Q_{21}[31] \oplus Q_{22}[31]$ from the conditions for f_{22}, we conclude that $Q_{23}[31] = 0$.

Conditions from non-constant bits of Q_{23}:

- $Q_{22}[31] = 0$.

Summary of Requirements resulting from this round:

$$Q_{23}[31] = 0.$$

t	Cumulative Conditions on Q_t
20	H.............v.................
21	H.............^.................
22	H...............................
23	0...............................

Round 24: The attacker has

- $\delta Q_{22} = \pm 2^{31}$,
- $\delta Q_{23} = 0$, and
- $\delta Q_{24} = 0$.

The attacker wants $\delta f_{24} = \pm 2^{31}$.

Obtaining Correct $\varDelta Q_t$: Already good.

	δ	∇
Q_{22}	±31	±...............................
Q_{23}		....
Q_{24}		....
f_{24}	±31	±...............................

Conditions to get correct $\varDelta Q_t$: none

Obtaining Correct δf_t:

Constant bits of Q_{22}: $\varDelta Q_{22}[j] = 0$, for $j \in [30 - 0]$, and since $\varDelta Q_{24}[j] = \varDelta Q_{24}[j] = 0$ at these bit positions, it follows that $\varDelta f_{24}[j] = 0$ at these bit positions.

- *Conditions from constant bits of Q_{24}:*
  - $Q_{22}[29] = 0$;
  - $Q_{22}[15, 3] = 1$.

Non-Constant bits of Q_{22}:

$\nabla Q_{22}[31] = \pm 1$: Note $\varDelta Q_{23}[31] = \nabla Q_{24}[31] = 0$.

- Getting $\nabla f_{24}[31] = \pm 1$ will require $Q_{24}[31] = \overline{Q_{23}[31]}$.

Conditions from non-constant bits of Q_{24}:

- $Q_{24}[31] = \overline{Q_{23}[31]}$.

Summary of Requirements resulting from this round:

$$Q_{24}[31] = \overline{Q_{23}[31]}.$$

Note that the condition $Q_{24}[31] = \overline{Q_{23}[31]}$ combines with the condition $Q_{23}[31] = 0$ required for f_{23}, and thus we obtain $Q_{24}[31] = 1$.

t	Cumulative Conditions on Q_t
22	`H...............................`
23	`0...............................`
24	`1...............................`

Rounds 25 to 32: The attacker has

- $\delta Q_{t-2} = 0$,
- $\delta Q_{t-1} = 0$, and
- $\delta Q_t = 0$.

The attacker wants $\delta f_t = 0$.

Obtaining Correct ΔQ_t: no differences.

	δ	∇
Q_{t-2}		....
Q_{t-1}		....
Q_t		....
f_t		....

New Conditions imposed by these rounds: none.

5.3 Rounds 32 to 47 of the First Block

From here-on it is rather easy. Certainly, rounds 32 to 47 are very simple to explain.

Since $f_t = Q_t \oplus Q_{t-1} \oplus Q_{t-2}$, it follows that $\Delta f_t = \Delta Q_t \oplus \Delta Q_{t-1} \oplus \Delta Q_{t-2}$. Thus, Δf_t is dictated by the XOR differences in Q_{t-2}, Q_{t-1}, and Q_t.

In these rounds, only differences in Q_t occur in the MSB. The sign of an MSB difference is important only if the difference goes through the rotation and becomes a difference in a less significant bit in R_t. However, in these rounds, these MSB differences are cancelled by an MSB difference in either f_t, Q_{t-3} or W_t, so $\Delta R_t = 0$. Consequently, for these rounds, the "sign" of MSB difference is irrelevant.

t	δQ_t	∇Q_t	∇f_t	δf_t
32-34	-	....	....	-
35	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{-}{31}$
36	$\overset{\pm}{31}$	±...............................	....	-
37-47	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$

Table 7. Propagation of differences through the f_t functions for rounds 16 to 31 of the first block. Note $f_t = Q_t \ \oplus \ Q_{t-1} \ \oplus \ Q_{t-2}$.

Round 35: The attacker has $\delta Q_{32} = 0$, $\delta Q_{34} = 0$ and $\delta Q_{35} = \pm 2^{31}$: (in Wang et al.'s example, they have $\delta Q_{35} = +2^{31}$) The attacker will get $\delta f_{35} = \pm 2^{31}$: (in Wang et al.'s example, they have $\delta f_{35} = -2^{31}$)

	δ	∇
Q_{32}	0	....
Q_{34}	0	....
Q_{35}	$\pm 2^{31}$	±...............................
f_{35}	$\pm 2^{31}$	±...............................

Round 36: The attacker has $\delta Q_{34} = 0$, $\delta Q_{35} = \pm 2^{31}$ and $\delta Q_{36} = \pm 2^{31}$: (in Wang et al.'s example, they have $\delta Q_{35} = +2^{31}$ and $\delta Q_{36} = +2^{31}$) The attacker will get $\delta f_{36} = 0$.

	δ	∇
Q_{34}	0	....
Q_{35}	$\pm 2^{31}$	±...............................
Q_{36}	$\pm 2^{31}$	±...............................
Q_{36}	0	....

Round 37-47: The attacker has $\delta Q_{t-2} = \pm 2^{31}$, $\delta Q_{t-1} = \pm 2^{31}$ and $\delta Q_t = \pm 2^{31}$: The attacker will get $\delta f_t = \pm 2^{31}$.

	δ	∇
Q_{t-2}	$\pm 2^{31}$	±...............................
Q_{t-1}	$\pm 2^{31}$	±...............................
Q_t	$\pm 2^{31}$	±...............................
f_t	$\pm 2^{31}$	±...............................

Summary of Rounds 32 to 47: – There are no conditions imposed during these rounds.

5.4 Rounds 48 to 63 of the First Block

The final 16 rounds are a bit tricky again because of the non-linearity in the function f_t. For these rounds, the sequential order of +'s and -'s in $\{\nabla Q_t[31]\}$ is quite important, as the sequence determines where $f_t[31]$ will have differences. The differences in $f_t[31]$ must occur for the correct values of t, otherwise the differences in $f_t[31]$, $Q_{t-3}[31]$ and $W_t[31]$ will not cancel out, and the difference in T_t will introduce differences in undesirable bit positions (after the rotation). As we shall see, in order to get the correct sequence of XOR-differences $\{\Delta f_t[31]\}$, the sequence of +'s and -'s in $\{\nabla Q_t[31]\}$ is completely determined by the values of $\nabla Q_{46}[31]$ and $\nabla Q_{47}[31]$. Since $\nabla Q_{46}[31] \in \{\texttt{+},\texttt{-}\}$ and $\nabla Q_{47}[31] \in \{\texttt{+},\texttt{-}\}$, it follows that there are 4 possible sequences of +'s and -'s in $\{\nabla Q_t[31]\}$. These four possible sequences are shown in Table 8. In the example of Wang et al., they have $\nabla Q_{46} = +2^{31}$ and $\nabla Q_{47} = -2^{31}$, shown in the fourth to sixth columns in Table 8.

Furthermore, the MSB of Q_t, Q_{t-1} and Q_{t-2} is specified for all of these rounds (since $\nabla Q_t[31] = \pm 2^{31}$), so the difference in the MSB of f_t is already specified. The first two columns of Table 9 show the values of $\nabla f_t[31]$ when $\nabla Q_{t-2}[31] \in \pm 2^{31}$, $\nabla Q_{t-1}[31] \in \pm 2^{31}$, and $\nabla Q_t[31] \in \pm 2^{31}$.

t	δQ_t	∇Q_t	∇f_t	δQ_t	∇Q_t	∇f_t	δQ_t	∇Q_t	∇f_t	δQ_t	∇Q_t	∇f_t
46	$+2^{31}$	+......		$+2^{31}$	+......		-2^{31}	-......		-2^{31}	-......	
47	$+2^{31}$	+......		-2^{31}	-......		$+2^{31}$	+......		-2^{31}	-......	
48	$+2^{31}$	+......	-......	$+2^{31}$	+......	+......	-2^{31}	-......	-......	-2^{31}	-......	+......
49	$+2^{31}$	+......	-......	-2^{31}	-......	-......	$+2^{31}$	+......	+......	-2^{31}	-......	+......
50	-2^{31}	-......	1......	-2^{31}	-......	0......	$+2^{31}$	+......	0......	$+2^{31}$	+......	1......
51	$+2^{31}$	+......	+......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	-2^{31}	-......	-......
52	-2^{31}	-......	-......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	$+2^{31}$	+......	+......
53	$+2^{31}$	+......	+......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	-2^{31}	-......	-......
54	-2^{31}	-......	-......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	$+2^{31}$	+......	+......
55	$+2^{31}$	+......	+......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	-2^{31}	-......	-......
56	-2^{31}	-......	-......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	$+2^{31}$	+......	+......
57	$+2^{31}$	+......	+......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	-2^{31}	-......	-......
58	-2^{31}	-......	-......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	$+2^{31}$	+......	+......
59	$+2^{31}$	+......	+......	-2^{31}	-......	+......	$+2^{31}$	+......	-......	-2^{31}	-......	-......
60	$+2^{31}$	+.....0	0......	$+2^{31}$	+.....0	1......	-2^{31}	-.....0	1......	-2^{31}	-.....0	0......
61	$+2^{31}$	+.....1	-......	-2^{31}	-.....1	-......	$+2^{31}$	+.....1	+......	-2^{31}	-.....1	+......
62	$+2^{31}+2^{25}$	+.....+	-.....0	$+2^{31}+2^{25}$	+.....+	+.....0	$-2^{31}+2^{25}$	-.....+	-.....0	$-2^{31}+2^{25}$	-.....+	+.....0
63	$+2^{31}+2^{25}$	+.....+	-.....0	$-2^{31}+2^{25}$	-.....+	-.....0	$+2^{31}+2^{25}$	+.....+	+.....0	$-2^{31}+2^{25}$	-.....+	+.....0

Table 8. The four possible sequences for the p propagation of differences through the f_t functions in the last 16 rounds of the first block. Only the 7 most significant bits are shown.

Most of the differences in these rounds occur only in the MSB (that is, bit 31). The first two columns of Table 9 show the values of $\nabla f_t[31]$ when $\nabla Q_{t-2}[31] \in \pm 2^{31}$, $\nabla Q_{t-1}[31] \in \pm 2^{31}$, and $\nabla Q_t[31] \in \pm 2^{31}$. The only other differences occur in bit $Q_{62}[25]$ and $Q_{63}[25]$. The attacker wants to obtain $\Delta f_{62}[25] = \Delta f_{63}[25] = 0$ and must choose the values of $Q_{60}[25]$ and $Q_{61}[25]$ appropriately. The last two columns of Table 9 show of values $\nabla f_{62}[25]$ and $\nabla f_{63}[25]$ for the possible combinations $\nabla Q_{60}[25] \in \{0,1\}$ and $\nabla Q_{61}[25] \in \{0,1\}$. This table is sufficient to determine what values of values for ∇Q_t will produce the correct outputs from f_t.

Round 48: The attacker has $\delta Q_{46} = \pm 2^{31}$, $\delta Q_{47} = \pm 2^{31}$, and $\delta Q_{48} = \pm 2^{31}$. The attacker wants $\delta f_{48} = \pm 2^{31}$. Table 9 indicates that

- obtaining $\Delta f_{48}[31] = 0$, requires $\nabla Q_{48}[31] = \nabla Q_{48}[31]$, and provides $\nabla f_{48}[31] = -\nabla Q_{47}[31]$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{46}	$+2^{31}$	+...	$+2^{31}$	+...	-2^{31}	-...	-2^{31}	-...
Q_{47}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
Q_{48}	$+2^{31}$	+...	$+2^{31}$	+...	-2^{31}	-...	-2^{31}	-...
f_{48}	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...

Bit 31		Bit 25	
$\nabla(Q_{t-2}, Q_{t-1}, Q_t)$	∇f_t		
+,+,+	-	$\nabla(Q_{60}, Q_{61}, Q_{62})$	$\nabla f_{62}[j]$
+,+,-	1	0,0,+	1
+,-,+	+	0,1,+	0
+,-,-	0	1,0,+	+
-,+,+	0	1,1,+	-
-,+,-	-	$\nabla(Q_{61}, Q_{62}, Q_{63})$	$\nabla f_{63}[j]$
-,-,+	1	0,+,+	-
-,-,-	+	1,+,+	0

Table 9. Propagation of differences through the f_t functions in the last 32 rounds of the first block.

Round 49: The attacker has $\delta Q_{47} = \pm 2^{31}$, $\delta Q_{48} = \pm 2^{31}$, and $\delta Q_{49} = \pm 2^{31}$. The attacker wants $\delta f_{49} = \pm 2^{31}$. Table 9 indicates that

- obtaining $\Delta f_{49}[31] = 0$, requires $\nabla Q_{49}[31] = \nabla Q_{49}[31]$, and provides $\nabla f_{49}[31] = -\nabla Q_{48}[31]$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{47}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
Q_{48}	$+2^{31}$	+...	$+2^{31}$	+...	-2^{31}	-...	-2^{31}	-...
Q_{49}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
f_{49}	-2^{31}	-...	-2^{31}	-...	$+2^{31}$	+...	$+2^{31}$	+...

Round 50: The attacker has $\delta Q_{48} = \pm 2^{31}$, $\delta Q_{49} = \pm 2^{31}$, and $\delta Q_{50} = \pm 2^{31}$. The attacker wants $\delta f_{50} = 0$. Table 9 indicates that

- obtaining $\Delta f_{50}[31] = 0$, requires $\nabla Q_{50}[31] = -\nabla Q_{50}[31]$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{48}	$+2^{31}$	+...	$+2^{31}$	+...	-2^{31}	-...	-2^{31}	-...
Q_{49}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
Q_{50}	-2^{31}	-...	-2^{31}	-...	$+2^{31}$	+...	$+2^{31}$	+...
f_{50}		1...		0...		0...		1...

A by-product is that $\nabla f_{50}[31] = 1$.

Rounds 51 to 59: The attacker has $\delta Q_{t-2} = \pm 2^{31}$, $\delta Q_{t-1} = \pm 2^{31}$, and $\delta Q_t = \pm 2^{31}$. The attacker wants $\delta f_t = \pm 2^{31}$. Table 9 indicates that

- obtaining $\Delta f_t[31] = 1$, requires $\nabla Q_t[31] = \nabla Q_t[31]$, and results in $\nabla f_t[31] = -\nabla Q_{t-1}[31]$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$											
	$+,+$			$+,-$			$-,+$			$-,-$		
	δ	∇	∇f_t	δ	∇	∇f_t	δ	∇	∇f_t	δ	∇	∇f_t
Q_{49}	$+2^{31}$	+...		-2^{31}	-...		$+2^{31}$	+...		-2^{31}	-...	
Q_{50}	-2^{31}	-...		-2^{31}	-...		$+2^{31}$	+...		$+2^{31}$	+...	
Q_{51}	$+2^{31}$	+...	+	-2^{31}	-...	+	$+2^{31}$	+...	-	-2^{31}	-...	-
Q_{52}	-2^{31}	-...	-	-2^{31}	-...	+	$+2^{31}$	+...	-	$+2^{31}$	+...	+
Q_{53}	$+2^{31}$	+...	+	-2^{31}	-...	+	$+2^{31}$	+...	-	-2^{31}	-...	-
Q_{54}	-2^{31}	-...	-	-2^{31}	-...	+	$+2^{31}$	+...	-	$+2^{31}$	+...	+
Q_{55}	$+2^{31}$	+...	+	-2^{31}	-...	+	$+2^{31}$	+...	-	-2^{31}	-...	-
Q_{56}	-2^{31}	-...	-	-2^{31}	-...	+	$+2^{31}$	+...	-	$+2^{31}$	+...	+
Q_{57}	$+2^{31}$	+...	+	-2^{31}	-...	+	$+2^{31}$	+...	-	-2^{31}	-...	-
Q_{58}	-2^{31}	-...	-	-2^{31}	-...	+	$+2^{31}$	+...	-	$+2^{31}$	+...	+
Q_{59}	$+2^{31}$	+...	+	-2^{31}	-...	+	$+2^{31}$	+...	-	-2^{31}	-...	-

Rounds 60: The attacker has $\delta Q_{58} = \pm 2^{31}$, $\delta Q_{59} = \pm 2^{31}$, and $\delta Q_{60} = \pm 2^{31}$. The attacker wants $\delta f_{60} = 0$. Table 9 indicates that

- obtaining $\Delta f_{60}[31] = 0$, requires $\nabla Q_{60}[31] = -\nabla Q_{60}[31]$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{58}	-2^{31}	-...	-2^{31}	-...	$+2^{31}$	+...	$+2^{31}$	+...
Q_{59}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
Q_{60}	$+2^{31}$	+...	$+2^{31}$	+...	-2^{31}	-...	-2^{31}	-...
f_{60}		0...		1...		1...		0...

Rounds 61: The attacker has $\delta Q_{59} = \pm 2^{31}$, $\delta Q_{60} = \pm 2^{31}$, and $\delta Q_{61} = \pm 2^{31}$. The attacker wants $\delta f_{61} = \pm 2^{31}$. Table 9 indicates that

- obtaining $\Delta f_{61}[31] = 0$, requires $\nabla Q_{61}[31] = \nabla Q_{61}[31]$, and provides $\nabla f_{61}[31] = -\nabla Q_{60}[31]$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{59}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
Q_{60}	$+2^{31}$	+...	$+2^{31}$	+...	-2^{31}	-...	-2^{31}	-...
Q_{61}	$+2^{31}$	+...	-2^{31}	-...	$+2^{31}$	+...	-2^{31}	-...
f_{61}	-2^{31}	-...	-2^{31}	-...	$+2^{31}$	+...	$+2^{31}$	+...

Round 62: The attacker has $\delta Q_{60} = \pm 2^{31}$, $\delta Q_{61} = \pm 2^{31}$, and $\delta Q_{62} = \pm 2^{31} + 2^{25}$. The attacker wants $\delta f_{62} = \pm 2^{31}$.

- The first thing to notice is that the smallest number of requirements will be imposed if the add-difference ($+2^{25}$) does not propagate to other bits: that is, the smallest number of requirements will be imposed if $\nabla Q_{62} = \pm.....+$. This imposes the condition $Q_{62}[25] = 0$.

Table 9 indicates that

- obtaining $\varDelta f_{62}[31] = 1$, requires $\nabla Q_{62}[31] = \nabla Q_{62}[31]$, and provides $\nabla f_{62}[31] = -\nabla Q_{61}[31]$;
- obtaining $\varDelta f_{62}[25] = 0$, requires $Q_{60}[25] = 0$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{60}	$+2^{31}$	+.....0	$+2^{31}$	+.....0	-2^{31}	-.....0	-2^{31}	-.....0
Q_{61}	$+2^{31}$	+......	-2^{31}	-......	$+2^{31}$	+......	-2^{31}	-......
Q_{62}	$+2^{31}+2^{25}$	+.....+	$+2^{31}+2^{25}$	+.....+	$-2^{31}+2^{25}$	-.....+	$-2^{31}+2^{25}$	-.....+
f_{62}	-2^{31}	-......	$+2^{31}$	+......	-2^{31}	-......	$+2^{31}$	+......

Round 63: The attacker has $\delta Q_{61} = \pm 2^{31}$, $\delta Q_{62} = \pm 2^{31} + 2^{25}$, and $\delta Q_{63} = \pm 2^{31} + 2^{25}$. The attacker wants $\delta f_{63} = \pm 2^{31}$.

- The first thing to notice is that the smallest number of requirements will be imposed if the add-difference ($+2^{25}$) does not propagate to other bits: that is, the smallest number of requirements will be imposed if $\nabla Q_{63} = \pm$.....+. This imposes the condition $Q_{63}[25] = 0$.

Table 9 indicates that

- obtaining $\varDelta f_{63}[31] = 1$, requires $\nabla Q_{63}[31] = \nabla Q_{63}[31]$, and provides $\nabla f_{63}[31] = -\nabla Q_{62}[31]$;
- obtaining $\varDelta f_{63}[25] = 0$, requires $Q_{61}[25] = 1$.

	$\nabla Q_{46}[31], \nabla Q_{47}[31]$							
	$+,+$		$+,-$		$-,+$		$-,-$	
	δ	∇	δ	∇	δ	∇	δ	∇
Q_{61}	$+2^{31}$	+.....1	-2^{31}	-.....1	$+2^{31}$	+.....1	-2^{31}	-.....1
Q_{62}	$+2^{31}+2^{25}$	+.....+	$+2^{31}+2^{25}$	+.....+	$-2^{31}+2^{25}$	-.....+	$-2^{31}+2^{25}$	-.....+
Q_{63}	$+2^{31}+2^{25}$	+.....+	$-2^{31}+2^{25}$	-.....+	$+2^{31}+2^{25}$	+.....+	$-2^{31}+2^{25}$	-.....+
f_{63}	-2^{31}	-......	-2^{31}	-......	$+2^{31}$	+......	$+2^{31}$	+......

A by-product is that $\nabla f_{63}[25] = \nabla f_{62}[25] = 0$.

Summary of Rounds 48 to 63: The four possibilities can be described by defining the choices $I = Q_{46}[31] \in \{0, 1\}$, $J = Q_{47}[31] \in \{0, 1\}$, and a related value $K = \overline{I}$.

t	Q_t
46	`I...............................`
47	`J...............................`
48	`I...............................`
49	`J...............................`
50	`K...............................`
51	`J...............................`
52	`K...............................`
53	`J...............................`
54	`K...............................`
55	`J...............................`
56	`K...............................`
57	`J...............................`
58	`K...............................`
59	`J...............................`
60	`I.....0.........................`
61	`J.....1.........................`
62	`I.....0.........................`
63	`J.....0.........................`

Table 10. Summary of conditions on Rounds 48 to 63: $I = Q_{46}[31] \in \{0, 1\}$, $J = Q_{47}[31] \in \{0, 1\}$, $K = \overline{I}$.

- There are four possible sequences of additive differences, each specified by the values of $\nabla Q_{46}[31]$ and $\nabla Q_{46}[31]$. Each sequence has the same number of conditions.
- Each of the four sequences requires specific values for $Q_t[31]$, $48 \leq t \leq 63$ and specific values for $Q_t[25]$, $60 \leq t \leq 63$.
- This is a total of 20 conditions on the internal state for these rounds.
- The probability of a random message satisfying one of these set of 20 conditions is $4 \times 2^{-20} = 2^{-18}$.

5.5 Summary of Conditions for Propagation through f_t

Tables 12 and 12 show the conditions on Q_t in order to for the differential to propagate through f_t correctly:

- *Case One*: For a given choice of the values A, B, H, I, J, the total number of conditions is 282. Thus, for a random message, the probability is 2^{-277} that all the conditions for this differential are satisfied (since there are five variables).

t	Conditions on Q_t			
	Case One	Eq	Def	None
3	.........vvv0vvvvvvv0vvvv0......	13v	3	16
4	C.......0^^^1^^^^^^^1^^^^0......	13^	5	11
5	Cvvv1v0v0100000000000000001vv1v1	8v	24	
6	B^^^0^1^0111111110111100010^^0^1	8^	24	
7	A0000011111111101111100000100000		32	
8	000000011..100010.0v010101000000	1v	28	3
9	E1111011...100000.1^..1100111101	1^	25	6
10	A1......0..111111101...001....00		17	15
11	A0....vv....000...00...011....10	2v	15	15
12	A0....^^....10000001...10.......	2^	12	18
13	A1....01....1111111....00...1...		14	18
14	A.0...00....1011111....11...1...		14	18
15	H.1...01........1...........0...		6	26
		Eq	Def	Combined
	Subtotal $0 \leq t \leq 15$: *Case One*	24	219	243
	Case Two	Eq	Def	None
3	.........vvv0vvvvvvv0vvvv0......	13v	3	16
4	0.......0^^^1^^^^^^^1^^^^0......	13^	5	11
5	0...0v0v0100000000000000001vv1v1	5v	24	3
6	....1^1^0111111110111100010^^0^1	5^	23	4
7	1...1011111111101111100000100000		29	2
8	0...00011..100010.0v010101000000	1v	25	6
9	E...1011...100000.1^..1100111101	1^	22	9
10	A1......0..111111101...001....00		17	15
11	A0....vv....000...00...011....10	2v	15	15
12	A0....^^....10000001...10.......	2^	12	18
13	A1....01....1111111....00...1...		14	18
14	A.0...00....1011111....11...1...		14	18
15	H.1...01........1...........0...		6	26
		Eq	Def	Combined
	Subtotal $0 \leq t \leq 15$: *Case Two*	21	209	230

Table 11. Conditions for on Q_t, $15 \leq t \leq 32$ in the first block. There are two variables with two possibilities each: $A \in \{0,1\}$, $B \in \{0,1\}$, with $C = \overline{A \oplus B}$, $E = \overline{A}$. The column headed by "Eq" contains the number of equality relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. When computing subtotals, the column headed by "Comb." contains the combination of equality relationships and definitions.

t	Conditions on Q_t	Eq	Def	None
14	`A.0...00....1011111....11...1...`			
15	`H.1...01........1...........0...`			
16	`H.1.............v...........v...`	2v	2	28
17	`H.v...........0.^...........^...`	1v,2^	2	27
18	`H.^...........1.................`	1^	2	29
19	`H.............0.................`		2	30
20	`H.............v.................`	1v	1	30
21	`H.............^.................`	1^	1	30
22	`H...............................`		1	31
23	`0...............................`		1	31
24	`1...............................`		1	31
25-45	`................................`			32
46	`I...............................`		1	31
47	`J...............................`		1	31
48	`I...............................`		1	31
49	`J...............................`		1	31
50	`K...............................`		1	31
51	`J...............................`		1	31
52	`K...............................`		1	31
53	`J...............................`		1	31
54	`K...............................`		1	31
55	`J...............................`		1	31
56	`K...............................`		1	31
57	`J...............................`		1	31
58	`K...............................`		1	31
59	`J...............................`		1	31
60	`I.....0.........................`		2	30
61	`J.....1.........................`		2	30
62	`I.....0.........................`		2	30
63	`J.....0.........................`		2	30
		Eq	Def	Combined
	Sub-total: $16 \leq t \leq 31$	4	13	17
	Sub-total: $32 \leq t \leq 47$	-	2	2
	Sub-total: $48 \leq t \leq 63$	-	20	20
	SubTotal: $16 \leq t \leq 63$ (This Table)	4	35	
	Sub-total: $-2 \leq t \leq 15$: *Case One*	24	219	243
	Sub-total: $-2 \leq t \leq 15$: *Case Two*	21	209	230
	Total: $-2 \leq t \leq 63$: *Case One*	28	254	282
	Total: $-2 \leq t \leq 63$: *Case Two*	25	244	269

Table 12. Conditions for on Q_t, $15 \leq t \leq 32$ in the first block. There are three new variables with two possibilities each: $H \in \{0, 1\}$, $I \in \{0, 1\}$, and $J \in \{0, 1\}$, with $K = \overline{I}$. The column headed by "Eq" contains the number of equality relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. In the last few rows, the column headed by "Comb." contains the combination of equality relationships and definitions.

- *Case Two*: For a given choice of the values A, H, I, J, the total number of conditions is 269. Thus, for a random message, the probability is 2^{-265} that all the conditions for this differential are satisfied (since there are only four variables for *Case Two*).
- This eliminates the possibility of a second pre-image attack.
- A vast majority of the conditions occur in the first 16 rounds.
- Only 39 conditions occur in the last 48 rounds.

I define an"f_t-good" message M to be a message such that the conditions required for f_t in the first 16 rounds are satisfied. You can see from the table that most of the conditions on f_t occur in the first 16 rounds. This is useful, because an attacker has full, independent control over the value of f_t for all of these rounds. Hence, the attacker can easily generate an f_t-good" message M. For each f_t-good message, the probability of the conditions being satisfied is the product of the probabilities for rounds 16 to 63. This probability is 2^{-39}, so the attacker can assume that one in 2^{39} of the f_t-good messages will also satisfy the conditions in the remaining rounds.

The attacker may easily produce first message blocks that are both T_t-good (see Section 4.4)and f_t good. The probability that tone such message block satisfies the requirements for all rounds is: $2^{-39} \cdot 2^{-3.2} \approx 2^{-42}$. Given how fast Wang at al. can generate a collision (1 hour) it seems likely that they are using additional tricks.

Appendix B provides the details of the internal differential for the second block.

- For a given choice of the values A, B, H, I, J, the total number of conditions is 323. Thus, for a random message, the probability is 2^{-318} that all the conditions for this differential are satisfied (since there are five variables).
- Eight of these conditions apply to the intermediate has value $IHV^{(1)}$. This may means that some intermediate values are not acceptable, even though they satisfy the conditions for the first block.
- A vast majority of the conditions occur in the first 16 rounds.
- Once again, only 39 conditions occur in the last 48 rounds.

The attacker can easily produce second message blocks that are both T_t-good and f_t good. The probability that one such message block satisfies the requirements for all rounds is the same as the probability for the first block: 2^{-42}. The total complexity is the sum of the complexity for finding the first message block and the complexity of find the second message block. This complexity is 2^{43}.

5.6 Applications of the Differential

- The differential allows a collision attack on the MD5 hash function with complexity $2^{42.2}$;
- A second pre-image attack based on this differential has complexity 2^{265}. So this differential does not lead to second pre-image attack on the MD5 hash function.

- Regarding HMAC-MD5 with unknown key: it seems that the attack must guess the entire state in order to get the conditions to be satisfied. Maybe there is a slight advantage to using this differential, but I doubt it. I suspect that this differential does not lead to a collision attack on HMAC-MD5.
- Regarding HMAC-MD5 with known key: in most cases the attacker does not know the key, but there are uses of MAC functions where the MAC must resist collisions even when the key is known. If the key is known, then complexity of finding a collision is at most as difficult as finding a collision in MD5 hash function. If the attacker can control the key being used, then the attacker can find a good starting point in the middle of the differential and work outwards to find a suitable initial value ($IHV^{(0)}$) that provides many collisions. The attacker can then choose to use this key.

A little observation: If the attacker can control the appropriate bits up to round 20, then there are only 25 conditions for f_t left (with 2 variables I and J). Also, the probability of satisfying the conditions on T_t increases to 2^{-2}. So the complexity becomes 2^{25} which is possible in one hour. (*Disclaimer: we do not know if it is possible for the attacker to control the appropriate bits up to round 20*).

6 Conclusion

The Wang et al. MD5 collision makes sophisticated use of differences in the carry bits in the modular addition. Features of their attack include a complicated differential for in the first round of compression, with simple differentials (in the most significant bit) for the remaining rounds. The collision uses differences in two blocks for which each block has similar internal differentials. The first block difference one to introduce a small difference into the state, and the second block difference cancels the introduced difference.

References

1. Eli Biham, Rafi Chen *New results on SHA-0 and SHA-1* Short talk presented at CRYPTO 2004 Rump Session, 2004.
2. F. Chabaud and A. Joux, *Differential Collisions in SHA-0,* Advances in Cryptology-CRYPTO'98, Lecture Notes in Computer Science, vol.1462, pp.56-71, Springer-Verlag, 1998.
3. National Institute of Standards and Technology, *Federal Information Processing Standards (FIPS) Publication 180-2, Secure Hash Standard (SHS),* February, 2004.
4. H. Gilbert and H. Hanschuh, *Security Analysis of SHA-256 and sisters,* Selected Areas in Cryptography, SAC 2003, Canada, Lecture Notes in Computer Science, vol. 3006, M. Matsui and R. Zuccheratopp (Eds.), pp. 175-193, Springer, 2004.
5. P. Hawkes, M. Paddon and G. Rose, *On Corrective Patterns for the SHA-2 Family,* Cryptology ePrint Archive, Report 2004/207, see `http://eprint.iacr.org/`, 2004.
6. International Organization for Standardization, *Data Cryptographic Techniques-Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm,* ISO/IEC 9797, 1989.

7. A. Joux, *Multicollisions in Iterated Hash Functions,* Advances in Cryptology - CRYPTO 2004, Lecture Notes in Computer Science, vol. 3152, M. Franklin (Ed.), pp. 306-316, Springer, 2004.
8. A. Joux, *Collisions in SHA-0,* Short talk presented at CRYPTO 2004 Rump Session, 2004.
9. H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication,* Internet RFC 2104, February 1997.
10. A. Menezes, P.van Oorschot and A. Vanstone *Handbook of Applied Cryptography,* CRC Press series on Discrete Nathematics and its Applications, CRC Press LLC, 1997.
11. R. Rivest, *The MD5 Message-Digest Algorithm,* Internet RFC 1321, April 1992.
12. X. Wang, D. Feng, X. Lai and H. Yu, *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD,* Cryptology ePrint Archive, Report 2004/199, see `http://eprint.iacr.org/`, 2004.

A Details for First Block

A.1 Sequence of Addition Differences

See Table 1 on page 6.

A.2 Conditions on Bit Positions

See Tables 11 and 12 on pages 58 and 59.

A.3 Values of ∇Q_t and ∇f_t at All Bit Positions

Tables 13, 14, 15 and 16 list the values of ∇Q_t and ∇f_t at all bit positions of the first block of the example collision given by Wang et al.

t	δQ_t	∇Q_t	∇f_t	δf_t
-3		01100111010001010010001100000001		
-2		00010000001100100101010001110110		
-1		10011000101110101101110011111110		
0		11101111110011011010101110001001	10011000101110101101110011111110	
1		00010011101110001100111111110110	10001011100010101001101110001000	
2		01001100100110100110010010001101	10100011110111011100111110000100	
3		00000010001001110011001100110011	00010001100110101110110011000101	
4		10110111001011110011101100111000	01001010101101110111011110110101	
5	$\overset{-}{6}$	100010000-++++++++++++++++100101	100000100010+1110011+01100110010	$\overset{+}{19}, \overset{+}{11}$
6	$\overset{+}{31}, \overset{+}{23}, \overset{-}{6}$	+0000010+1111111101111000-000001	101101010-+++++++0++++1100111001	$\overset{-}{14}, \overset{-}{10}$
7	$\overset{-}{27} +, \overset{-}{23}, \overset{-}{6}, \overset{-}{0}$	++++++---11111101111-+++++-+++++	1000-0-00111111+10111+0000+00-01	$\overset{-}{27}, \overset{-}{25}, \overset{+}{16}, \overset{+}{10}, \overset{+}{5}, \overset{-}{2}$
8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	00000001-01-+++-+00101010100000+	+000001-1111111+10111+0+0+000001	$\overset{+}{31}, \overset{-}{24}, \overset{+}{16}, \overset{+}{10}, \overset{+}{8}, \overset{+}{6}$
9	$\overset{-}{31}, \overset{-}{6}, \overset{+}{1}, \overset{-}{0}$	-1111011101100000011111-++1111+-	+0000+01-11-1110110101010+00000+	$\overset{+}{31}, \overset{+}{26}, \overset{-}{23}, \overset{-}{20}, \overset{+}{6}, \overset{+}{0}$
10	$\overset{+}{31}, \overset{+}{13}, \overset{-}{12}$	+11100110111111111+-100001100100	01110011-011000000+111010+10010+	$\overset{-}{23}, \overset{+}{13}, \overset{+}{6}, \overset{+}{0}$
11	$\overset{+}{31}, \overset{+}{30}$	++011110011100011100111011010010	11110011111100011111100-0110110-	$\overset{-}{8}, \overset{-}{0}$
12	$\overset{+}{31}, \overset{-}{13}, \overset{-}{7}$	+00000101010-++++++1111-+0100111	+11100110111+--111001110+1000010	$\overset{+}{31}, \overset{+}{17}, \overset{+}{7}$
13	$\overset{+}{31}, \overset{+}{24}$	+11100+-010111111111010000001000	+00011100010-++++++1111011010010	$\overset{+}{31}, \overset{-}{13}$
14	$\overset{+}{31}$	+0010100110010111111010111111000	+001001001101+111111111000001111	$\overset{+}{31}, \overset{+}{18}$
15	$\overset{+}{31}, \overset{-}{15}, \overset{+}{3}$	+111000101011101-00010100010+000	+00100+0010010111111010000101000	$\overset{+}{31}, \overset{+}{25}$

Table 13. Values of ∇Q_t and ∇f_t at all bit positions for rounds 0 to 15 of the first block of the collision provided by Wang et al..

t	δQ_t	∇Q_t	∇f_t	δf_t
14	$\overset{+}{31}$	+0010100110010111111010111111000		
15	$\overset{+}{31}, \overset{-}{15}, \overset{+}{3}$	+111000101011101-00010100010+000		
16	$\overset{+}{31}, \overset{-}{29}$	+0-01101100010111000001100110100	+0111101000100001101110010101111	$+2^{31}$
17	$\overset{+}{31}$	+1101111000111001110111100100110	+1101101100111101000101100110100	$\overset{+}{31}$
18	$\overset{+}{31}$	+1110101100011100100100000101000	+1100111100111100110110000100010	$\overset{+}{31}$
19	$\overset{+}{31}, \overset{+}{17}$	+1100101111111+00101111010001110	+1110101100111100100111000001110	$\overset{+}{31}$
20	$\overset{+}{31}$	+0010001110101010101101001101010	+0010001111101000101111010101110	$\overset{+}{31}$
21	$\overset{+}{31}$	+1101001101010011110001011001010	+1110001101010010100001011101010	$\overset{+}{31}$
22	$\overset{+}{31}$	+1110010101100011011001110100100	+1111000101110011011001010100000	$\overset{+}{31}$
23		01111110011111010111100001001001	01111010001110010111000101101100	
24		10011011010111010011000111010010	+0011110010111010111100111001001	$\overset{+}{31}$
25		00101111000000010000001000100111	10101111000000010000000110010011	
26		01111100101101101100111111010110	00111100000101000000001111110111	
27		10001011000011101001001011101110	01011011101101101100111111110110	
28		11001011101100101011110100011010	11001011101110101001110100111010	
29		01011000110111011000100011000010	01001000101111001010110111010010	
30		01010011100110111001110001010011	01010011110111111001110011010010	
31		10011111001100000001000001001010	00011011000100100001010001010011	

Table 14. Values of ∇Q_t and ∇f_t at all bit positions for rounds 16 to 31 of the first block of the collision provided by Wang et al..

t	δQ_t	∇Q_t	∇f_t	δf_t
30		01010011100110111001110001010011		
31		10011111001100000001000001001010		
32		10001111001001011101000110010000	01000011100011100101110110001001	
33		00001101011011000010101110000100	00011101011110011110101001011110	
34		11101110110000000110101101111001	01101100100010011001000101101101	
35	$\overset{+}{31}$	+11000101011111100111111100010001	-00000010001001101111111111101100	$\overset{-}{31}$
36	$\overset{+}{31}$	+00100110011111110101100111001000	100111110100000001111100010001100	
37	$\overset{+}{31}$	+111100011101110111111100111010101	+00010010110111001101101100000000	$\overset{+}{31}$
38	$\overset{-}{31}$	-0010100100001011000110011010011011	-1111111010101001101111001000010010	$\overset{-}{31}$
39	$\overset{-}{31}$	-11110001111000101101111100100010	+00101001001101000011101100001000100	$\overset{+}{31}$
40	$\overset{-}{31}$	-01001101010011010000000001010111	-10010101101001001100011101001100110	$\overset{-}{31}$
41	$\overset{+}{31}$	+11010010001000101101101110101110111	+0110111010001101000001010100010010	$\overset{+}{31}$
42	$\overset{-}{31}$	-0111100010110110111001110100001001	+1110011111011001001111000100001001	$\overset{+}{31}$
43	$\overset{-}{31}$	-01010011011110000001001001100111	+1111100111101100000110000010001001	$\overset{+}{31}$
44	$\overset{-}{31}$	-00000000110111101010000101111101	-0010101100010000011000101111011011	$\overset{-}{31}$
45	$\overset{+}{31}$	+0110010100101011000101000001010010	+001101101000110110010001101000000	$\overset{+}{31}$
46	$\overset{+}{31}$	+10010111101000001111111001111111	-1111001001010101010010110001000000	$\overset{-}{31}$
47	$\overset{-}{31}$	-011100000110111100111010000010000	-1000001011100100110100000110001001	$\overset{-}{31}$

Table 15. Values of ∇Q_t and ∇f_t at all bit positions for rounds 32 to 47 of the first block of the collision provided by Wang et al..

t	δQ_t	∇Q_t	∇f_t	δf_t
46	$\overset{+}{31}$	+10010111101000001111111100111111		
47	$\overset{-}{31}$	-01110000011011110011101000000100		
48	$\overset{+}{31}$	+0010110001111100011000100101010	+0001110000010000010110011101110	$\overset{+}{31}$
49	$\overset{-}{31}$	-1111111010000001111010001110111	-1101001111101101100011111010101	$\overset{-}{31}$
50	$\overset{-}{31}$	-10010000100101010000000010000000	00010110100010110011101010100010	
51	$\overset{-}{31}$	-1010100110111011011011100001010	+0011100101101010011111100001010	$\overset{+}{31}$
52	$\overset{-}{31}$	-0100100110110010001011110110100	+11000110010000001100100011110101	$\overset{+}{31}$
53	$\overset{-}{31}$	-0011101011100110010010110011111	+0011011101010100111101001001011	$\overset{+}{31}$
54	$\overset{-}{31}$	-0001011010011101111110011011110	+1000110000111011101100101000000	$\overset{+}{31}$
55	$\overset{-}{31}$	-0111111111101000100110000011000	+1110100101100100010001010100110	$\overset{+}{31}$
56	$\overset{-}{31}$	-0011110000000001100101111100111	+1000001010001011000011111111111	$\overset{+}{31}$
57	$\overset{-}{31}$	-1000011011101110001110001111100	+1011101011111110111010000011000	$\overset{+}{31}$
58	$\overset{-}{31}$	-0100001101101000111010110000100	+0100010100010000110100111100000	$\overset{+}{31}$
59	$\overset{-}{31}$	-0100000010110101101011101101110	+0011101011011101000001001101011	$\overset{+}{31}$
60	$\overset{+}{31}$	+10111011010111111111111110010011	11111111101101010010100010010101	
61	$\overset{-}{31}$	-11010110001001101110000000100011	-0100010000110001000011100100000	$\overset{-}{31}$
62	$\overset{+}{31}, \overset{+}{25}$	+00100+0100100110110100110010000	+1011001110000000001100111011111	$\overset{+}{31}$
63	$\overset{-}{31}, \overset{+}{25}$	-00100+1010010111111111101010110	-0000101011111001001011001001110	$\overset{-}{31}$

Table 16. Values of ∇Q_t and ∇f_t at all bit positions for rounds 48 to 63 of the first block of the collision provided by Wang et al.

B All Details for the Second Block

B.1 Sequence of Add-Differences

The differential in the second block begins with

$$\begin{aligned} \delta Q_{-3} &= \delta IHV^{(1)}[0] = \pm 2^{31}, \\ \delta Q_{0} &= \delta IHV^{(1)}[1] = \pm 2^{31} + 2^{25}, \\ \delta Q_{-1} &= \delta IHV^{(1)}[2] = \pm 2^{31} + 2^{25}, \\ \delta Q_{-2} &= \delta IHV^{(1)}[3] = \pm 2^{31} + 2^{25}. \end{aligned}$$

Table 16 shows the sequence of add-differences in the second block. The differential in the second block finishes up with

$$\begin{aligned} \delta Q_{61} &= \pm 2^{31}, \\ \delta Q_{62} &= \pm 2^{31} - 2^{25}, \\ \delta Q_{63} &= \pm 2^{31} - 2^{25}, \\ \delta Q_{64} &= \pm 2^{31} - 2^{25}. \end{aligned}$$

Thus:

$$\begin{array}{ll} \delta IHV^{(2)}[0] & = \delta IHV^{(1)}[0] + \Delta Q_{61} = (\pm 2^{31}) + (\pm 2^{31}) \qquad\qquad\qquad = 0, \\ \delta IHV^{(2)}[1] & = \delta IHV^{(1)}[1] + \Delta Q_{64} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31} - 2^{25}) = 0, \\ \delta IHV^{(2)}[2] & = \delta IHV^{(1)}[2] + \Delta Q_{63} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31} - 2^{25}) = 0, \\ \delta IHV^{(2)}[3] & = \delta IHV^{(1)}[3] + \Delta Q_{62} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31} - 2^{25}) = 0. \end{array}$$

t	δQ_t	δf_t	δQ_{t-3}	δW_t	δT_t	$S(t)$	δR_t
0	$\overset{\pm}{31}, \overset{+}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			7	
1	$\overset{\pm}{31}, \overset{+}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}, \overset{+}{25}$		$\overset{+}{25}$	12	$\overset{+}{5}$
2	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{5}$	$\overset{+}{25}$	$\overset{\pm}{31}, \overset{+}{25}$		$\overset{+}{31}, \overset{+}{26}$	17	$\overset{+}{16}, \overset{+}{11}$
3	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{16}, \overset{+}{11}, \overset{+}{5}$	$\overset{\pm}{31}, \overset{-}{27}, \overset{+}{25}, \overset{-}{21}, \overset{-}{11}$	$\overset{\pm}{31}, \overset{+}{25}$		$\overset{-}{26}, \overset{-}{21}, \overset{-}{11}$	22	$\overset{-}{16}, \overset{-}{11}, \overset{-}{1}$
4	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{5}, \overset{-}{1}$	$\overset{+}{30}, \overset{+}{26}, \overset{-}{18}, \overset{-}{3}, \overset{+}{1}$	$\overset{\pm}{31}, \overset{+}{25}$	$\overset{\pm}{31}$	$\overset{+}{30}, \overset{+}{26}, \overset{+}{25}, \overset{-}{18}, \overset{+}{2}, \overset{+}{1}$	7	$\overset{-}{25}, \overset{+}{10}, \overset{-}{8}, \overset{+}{5}, \overset{+}{1}, \overset{+}{0}$
5	$\overset{\pm}{31}, \overset{+}{10}, \overset{-}{8}, \overset{+}{6}, \overset{+}{0}$	$\overset{+}{30}, \overset{+}{28}, \overset{-}{26}, \overset{-}{25}, \overset{-}{20}, \overset{-}{8}, \overset{-}{5}, \overset{-}{4}$	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{5}$		$\overset{-}{30}, \overset{+}{28}, \overset{-}{26}, \overset{-}{20}, \overset{-}{8}, \overset{-}{4}$	12	$\overset{-}{20}, \overset{-}{16}, \overset{-}{10}, \overset{+}{8}, \overset{-}{6}, \overset{-}{0}$
6	$\overset{\pm}{31}, \overset{-}{20}, \overset{-}{16}$	$\overset{-}{25}, \overset{-}{21}, \overset{-}{16}, \overset{-}{11}, \overset{-}{10}, \overset{-}{5}, \overset{+}{3}$	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{16}, \overset{+}{11}, \overset{+}{5}$		$\overset{-}{31}, \overset{-}{21}, \overset{-}{10}, \overset{+}{3}$	17	$\overset{-}{27}, \overset{+}{20}, \overset{+}{16}, \overset{-}{6}$
7	$\overset{\pm}{31}, \overset{-}{27}, \overset{-}{6}$	$\overset{\pm}{31}, \overset{-}{27}, \overset{+}{16}$	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{5}, \overset{-}{1}$		$\overset{-}{27}, \overset{+}{25}, \overset{+}{16}, \overset{+}{5}, \overset{-}{1}$	22	$\overset{+}{27}, \overset{-}{23}, \overset{-}{17}, \overset{+}{15}, \overset{+}{6}$
8	$\overset{\pm}{31}, \overset{-}{23}, \overset{-}{17}, \overset{+}{15}$	$\overset{+}{25}, \overset{+}{16}, \overset{-}{6}$	$\overset{\pm}{31}, \overset{+}{10}, \overset{-}{7}, \overset{-}{6}, \overset{+}{0}$		$\overset{-}{31}, \overset{+}{25}, \overset{+}{16}, \overset{+}{9}, \overset{+}{8}, \overset{+}{0}$	7	$\overset{+}{23}, \overset{+}{16}, \overset{+}{15}, \overset{+}{6}, \overset{+}{0}$
9	$\overset{\pm}{31}, \overset{+}{6}, \overset{+}{0}$	$\overset{\pm}{31}, \overset{-}{26}, \overset{+}{16}, \overset{+}{0}$	$\overset{\pm}{31}, \overset{-}{20}, \overset{-}{16}$		$\overset{-}{26}, \overset{-}{20}, \overset{+}{0}$	12	$\overset{+}{12}, \overset{-}{6}, \overset{-}{0}$
10	$\overset{\pm}{31}, \overset{+}{12}$	$\overset{\pm}{31}, \overset{+}{6}$	$\overset{\pm}{31}, \overset{-}{27}, \overset{-}{6}$		$\overset{-}{27}$	17	$\overset{-}{12}$
11	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}, \overset{-}{23}, \overset{-}{17}, \overset{+}{15}$	$\overset{-}{15}$	$\overset{-}{23}, \overset{-}{17}$	22	$\overset{-}{13}, \overset{-}{7}$
12	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$	$\overset{\pm}{31}, \overset{+}{17}$	$\overset{\pm}{31}, \overset{+}{6}, \overset{+}{0}$		$\overset{+}{17}, \overset{+}{6}, \overset{+}{0}$	7	$\overset{+}{24}, \overset{+}{13}, \overset{+}{7}$
13	$\overset{\pm}{31}, \overset{+}{24}$	$\overset{\pm}{31}, \overset{-}{13}$	$\overset{\pm}{31}, \overset{+}{12}$		$\overset{-}{12}$	12	$\overset{-}{24}$
14	$\overset{\pm}{31}$	$\overset{+}{30}, \overset{+}{18}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{+}{30}, \overset{+}{18}$	17	$\overset{+}{15}, \overset{+}{3}$
15	$\overset{\pm}{31}, \overset{+}{15}, \overset{+}{3}$	$\overset{\pm}{31}, \overset{-}{25}$	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$		$\overset{-}{25}, \overset{-}{13}, \overset{-}{7}$	22	$\overset{-}{29}, \overset{-}{15}, \overset{-}{3}$
16	$\overset{\pm}{31}, \overset{-}{29}$	$\overset{\pm}{31}$	$\overset{\pm}{31}, \overset{+}{24}$		$\overset{+}{24}$	5	$\overset{+}{29}$
17	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			9	
18	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}, \overset{+}{15}, \overset{+}{3}$	$\overset{-}{15}$	$\overset{+}{3}$	14	$\overset{+}{17}$
19	$\overset{\pm}{31}, \overset{+}{17}$	$\overset{\pm}{31}$	$\overset{\pm}{31}, \overset{-}{29}$		$\overset{-}{29}$	20	$\overset{-}{17}$
20-21	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			.	
22	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}, \overset{+}{17}$		$\overset{+}{17}$	14	$\overset{\pm}{31}$
23			$\overset{\pm}{31}$	$\overset{\pm}{31}$		20	
24		$\overset{\pm}{31}$	$\overset{\pm}{31}$			5	
25			$\overset{\pm}{31}$	$\overset{\pm}{31}$		9	
26-33						.	
34				$\overset{-}{15}$	$\overset{-}{15}$	16	$\overset{\pm}{31}$
35	$\overset{\pm}{31}$	$\overset{\pm}{31}$		$\overset{\pm}{31}$		23	
36	$\overset{\pm}{31}$					4	
37	$\overset{\pm}{31}$	$\overset{\pm}{31}$		$\overset{\pm}{31}$		11	
38-49	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			.	
50	$\overset{\pm}{31}$		$\overset{\pm}{31}$	$\overset{\pm}{31}$		15	
51-59	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			.	
60	$\overset{\pm}{31}$		$\overset{\pm}{31}$	$\overset{\pm}{31}$		6	
61	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{-}{15}$	$\overset{-}{15}$	10	$\overset{-}{25}$
62-63	$\overset{\pm}{31}, \overset{-}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$				

Table 17. Sequence of add-differences for rounds 16 to 63 of the second block. Recall that $\delta Q_t = \delta Q_{t-1} + \delta R_{t-1}$, $\delta T_t = \delta f_t + \delta Q_{t-3} + \delta W_t$, and (most of the time) $\delta R_t = ROTL^{S(t)}(\delta T_t)$.

B.2 Sequence of XOR-Differences in Q_t and f_t

Tables 18 and 19 show the XOR-differences in Q_t in f_t in order to get the add-differences in f_t from the corresponding bits in Q_t, ${}_{t-1}$ and Q_{t-2}. The sign of $\nabla Q_t[31]$ is not shown here, as this is determined by the function f_t.

t	δQ_t	∇Q_t	∇f_t	δf_t
-3	$\overset{\pm}{31}$	±...............................		
-2	$\overset{\pm}{31}, \overset{+}{25}$	±.....+.........................		
-1	$\overset{\pm}{31}, \overset{+}{25}$	±....+-.........................		
0	$\overset{\pm}{31}, \overset{+}{25}$	±.....+.........................	±...............................	$\overset{\pm}{31}$
1	$\overset{\pm}{31}, \overset{+}{25}$	±.....+.........................	±...............................	$\overset{\pm}{31}$
2	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{5}$	±.....+...................+.....	......+.........................	$\overset{+}{25}$
3	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{16}, \overset{+}{11}, \overset{+}{5}$	±-----...+-----...+-...+--.....	±...-.+...-.........-...........	$\overset{\pm}{31}, \overset{-}{27}, \overset{+}{25}, \overset{-}{21}, \overset{-}{11}$
4	$\overset{\pm}{31}, \overset{+}{25}, \overset{+}{5}, \overset{-}{1}$	±....+-...................+-+++.	±.----.......-...............++.	$\overset{+}{30}, \overset{+}{26}, \overset{-}{18}, \overset{+}{2}, \overset{+}{1}$
5	$\overset{\pm}{31}, \overset{+}{9}, \overset{+}{6}, \overset{+}{0}$	±..................+---++-.....+	±.--.--....-...........-..--....	$\overset{+}{30}, \overset{+}{27}, \overset{+}{25}, \overset{-}{20}, \overset{-}{8}, \overset{-}{6}, \overset{+}{4}$
6	$\overset{\pm}{31}, \overset{-}{20}, \overset{-}{16}$	±.........-+..-+................	......-...-...-+....--...-+.+...	$\overset{-}{25}, \overset{-}{21}, \overset{-}{16}, \overset{-}{11}, \overset{-}{10}, \overset{-}{5}, \overset{+}{3}$
7	$\overset{\pm}{31}, \overset{-}{27}, \overset{-}{6}$	±..-+.................-+++......	±...-..........+................	$\overset{\pm}{31}, \overset{-}{27}, \overset{+}{16}$
8	$\overset{\pm}{31}, \overset{-}{23}, \overset{-}{17}, \overset{+}{15}$	±....-+++.....-+-...............	......+........+......-+++......	$\overset{+}{25}, \overset{+}{16}, \overset{-}{6}$
9	$\overset{\pm}{31}, \overset{+}{6}, \overset{+}{0}$	±.....................+---....+-	±....-.........+...............+	$\overset{\pm}{31}, \overset{-}{26}, \overset{+}{16}, \overset{+}{0}$
10	$\overset{\pm}{31}, \overset{+}{12}$	±..................+............	±.....................+---......	$\overset{\pm}{31}, \overset{+}{6}$
11	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
12	$\overset{\pm}{31}, \overset{-}{13}, \overset{-}{7}$	±...........-++++++.....-.......	±............+-.................	$\overset{\pm}{31}, \overset{+}{17}$
13	$\overset{\pm}{31}, \overset{+}{24}$	±+------........................	±...........-++++++.............	$\overset{\pm}{31}, \overset{-}{13}$
14	$\overset{\pm}{31}$	±...............................	.+...........+..................	$\overset{+}{30}, \overset{+}{18}$
15	$\overset{\pm}{31}, \overset{+}{15}, \overset{+}{3}$	±...............+...........+...	±.....-.........................	$\overset{\pm}{31}, \overset{-}{25}$

Table 18. Sequence of XOR-Differences in Q_t and f_t for rounds 0 to 15 of the second block.

t	δQ_t	∇Q_t	∇f_t	δf_t
16	$\overset{\pm}{31}, \overset{-}{29}$	±.-.............................	±...............................	$\overset{\pm}{31}$
17-18	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
19	$\overset{\pm}{31}, \overset{+}{17}$	±.............+.................	±...............................	$\overset{\pm}{31}$
20-22	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
23		....	....	
24		....	±...............................	$\overset{\pm}{31}$
25-34		....	....	
35	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
36	$\overset{\pm}{31}$	±...............................	....	
37-49	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
50	$\overset{\pm}{31}$	±...............................	....	
51-59	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
61	$\overset{\pm}{31}$	±...............................	....	
60	$\overset{\pm}{31}$	±...............................	±...............................	$\overset{\pm}{31}$
62	$\overset{\pm}{31}, \overset{-}{25}$	±.....-.........................	±...............................	$\overset{\pm}{31}$
63	$\overset{\pm}{31}, \overset{-}{25}$	±....-+.........................	±...............................	$\overset{\pm}{31}$

Table 19. Sequence of XOR-Differences in Q_t and f_t for rounds 16 to 63 of the second block.

B.3 Conditions on Bit Positions

Tables 20 and 21 detail the conditions on the internal values Q_t, $-2 \leq t \leq 53$ in order for the collision to occur. The conditions on Q_{-2}, Q_{-1} and Q_0 correspond to conditions on the intermediate hash value $IHV^{(1)}$.

t	Conditions on Q_t	Eq	Def	None
-2	A.....0.........................		2	30
-1	A....01.........................		3	29
0	A....00...................v.....	1v	3	28
1	Bvvv010...1vvvvv...v0...v1^.....	10v,1^	7	14
2	B^^^110...0^^^^^...^1...^10vv00.	2v,10^	10	10
3	B011111...011111...01vv1011^^11v	3v,2^	21	6
4	B011101...000100...00^^00001000^	3^	23	6
5	A100101...101111...0111001010000		26	6
6	A..0010v1.10..101..0110001010110	1v	24	7
7	B..1011^1.00..011..1111000....v1	1v,1^	19	11
8	B..001000.11..101..v..1111....^0	1v,1^	17	13
9	B..111000.....010..^..0111....01	1^	16	15
10	B....1111...v0111100..1111....00	1v	18	13
11	Bvvvvvvv....^1011100..1111....11	7v,1^	14	10
12	B^^^^^^^....10000001....1.......	7^	10	15
13	A0111111....1111111.....0...1...		17	15
14	A1000000....1011111.....1...1...		17	15
15	C1111101........0...........0...		10	22
		Eq	Def	Combined
	Sub-total: $-2 \leq t \leq 15$	27	257	

Table 20. Conditions on ∇Q_t, $-2 \leq t \leq 15$, of the second block to get the correct propagation of differences through f_t. The attacker can allow $A \in \{0,1\}$, $C \in \{0,1\}$ with $B = \overline{A}$. The column headed by "Eq" contains the number of relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. In the last row, the column headed by "Comb." contains the combination of equality relationships and definitions. Note the conditions on Q_{-2},Q_{-1}, Q_0 apply to the intermediate hash value $IHV^{(1)}$.

t	Conditions on Q_t	Eq	Def	None
14	`A1000000....1011111.....1...1...`			
15	`C1111101........0...........0...`			
16	`C.1.............v...........v...`	2v	2	28
17	`C.v...........0.^...........^...`	2^,1v	2	27
18	`C.^...........1.................`	1^	2	29
19	`C.............0.................`		2	30
20	`C.............v.................`	1v	1	30
21	`C.............^.................`	1^	1	30
22	`C...............................`		1	31
23	`0...............................`		1	31
24	`1...............................`		1	31
25-31	`................................`			32
32-45	`................................`			32
46	`I...............................`		1	31
47	`J...............................`		1	31
48	`I...............................`		1	31
49	`J...............................`		1	31
50	`K...............................`		1	31
51	`J...............................`		1	31
52	`K...............................`		1	31
53	`J...............................`		1	31
54	`K...............................`		1	31
55	`J...............................`		1	31
56	`K...............................`		1	31
57	`J...............................`		1	31
58	`K...............................`		1	31
59	`J...............................`		1	31
60	`I.....0.........................`		2	30
61	`J.....1.........................`		2	30
62	`I.....1.........................`		2	30
63	`J.....1.........................`		2	30
		Eq	Def	Combined
	Sub-total: $16 \leq t \leq 31$	4	13	
	Sub-total: $32 \leq t \leq 47$	-	2	
	Sub-total: $48 \leq t \leq 63$	-	20	
	SubTotal: $16 \leq t \leq 63$ (This Table)	4	35	
	Sub-total: $-2 \leq t \leq 15$ (Table 20)	27	257	
	Total: $-2 \leq t \leq 63$	31	292	323

Table 21. Conditions on ∇Q_t, $16 \leq t \leq 63$, of the second block to get the correct propagation of differences through f_t. There are two new variables with two possibilities each: $I \in \{0, 1\}$, and $J \in \{0, 1\}$, with $K = \overline{I}$. The column headed by "Eq" contains the number of equality relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. In the last few rows, the column headed by "Comb." contains the combination of equality relationships and definitions.

B.4 Values of ∇Q_t and ∇f_t at All Bit Positions

Tables 22, 23, 24 and 25 list the values of ∇Q_t and ∇f_t at all bit positions of the second block of the example collision given by Wang et al.

t	δQ_t	∇Q_t	∇f_t	δf_t
-3	$\overset{+}{31}$	+10100100101100010010011001001OO		
-2	$\overset{+}{31}, \overset{+}{25}$	+01000+011000101101111110000001 10		
-1	$\overset{+}{31}, \overset{+}{25}$	+0101+-000000110110111000101010 0		
0	$\overset{+}{31}, \overset{+}{25}$	+01100+0100100111101011111001010	+0100000010001101111110001000100	$\overset{+}{31}$
1	$\overset{-}{31}, \overset{+}{25}$	-10001+0001100111001001011010111	+0101010000101111101111011000010	$\overset{+}{31}$
2	$\overset{-}{31}, \overset{+}{25}, \overset{+}{5}$	-10011+1100100110011111111+11001	111101+0000100111101001011010011	$\overset{+}{25}$
3	$\overset{-}{31}, \overset{+}{25}, \overset{+}{16}, \overset{+}{11}, \overset{+}{5}$	-+-----101+-----101+-101+--11110	-100-1+100-100110011-11111011001	$\overset{-}{31}, \overset{-}{27}, \overset{+}{25}, \overset{-}{21}, \overset{-}{11}$
4	$\overset{-}{31}, \overset{+}{25}, \overset{+}{5}, \overset{-}{1}$	-0111+-001000100111001000 0+-+++0	-1----1111010-111011111111011++1	$\overset{+}{30}, \overset{+}{26}, \overset{-}{18}, \overset{+}{2}, \overset{+}{1}$
5	$\overset{+}{31}, \overset{+}{9}, \overset{+}{6}, \overset{+}{0}$	+100101100101111101+---++-01000+	-0--1--0010-01001010010-00--1110	$\overset{+}{30}, \overset{+}{27}, \overset{+}{25}, \overset{-}{20}, \overset{-}{8}, \overset{-}{6}, \overset{+}{4}$
6	$\overset{+}{31}, \overset{-}{20}, \overset{-}{16}$	+010010010-+00-+1100110001010110	100110-001-001-+1010--000-+1+000	$\overset{-}{25}, \overset{-}{21}, \overset{-}{16}, \overset{-}{11}, \overset{-}{10}, \overset{-}{5}, \overset{+}{3}$
7	$\overset{-}{31}, \overset{-}{27}, \overset{-}{6}$	-01-+11011000101100111-+++100101	+110-1011010101+1010110001010100	$\overset{+}{31}, \overset{-}{27}, \overset{+}{16}$
8	$\overset{-}{31}, \overset{-}{23}, \overset{-}{17}, \overset{+}{15}$	-0000-+++11100-+-101011111110000	101001+01100000+100111-+++100110	$\overset{+}{25}, \overset{+}{16}, \overset{-}{6}$
9	$\overset{-}{31}, \overset{+}{6}, \overset{+}{0}$	-111110001111001001110+---0110+-	-0000-101111010+100101111111010+	$\overset{-}{31}, \overset{-}{26}, \overset{+}{16}, \overset{+}{0}$
10	$\overset{-}{31}, \overset{+}{12}$	-0001111100010111 10+101111111100	-0001100011110010001 11+---011000	$\overset{-}{31}, \overset{+}{6}$
11	$\overset{-}{31}$	-0001111001011011100011111010011	-1111111010110011111101111011000	$\overset{-}{31}$
12	$\overset{-}{31}, \overset{-}{13}, \overset{-}{7}$	-00011110000-++++++10111-0110000	-000111110001+-11100111111011100	$\overset{-}{31}, \overset{+}{17}$
13	$\overset{+}{31}, \overset{+}{24}$	++------0100111111111101000011010	-00011110010-++++++1011111010001	$\overset{-}{31}, \overset{-}{13}$
14	$\overset{+}{31}$	+1000000111110111111001010111100	1+00111101001+1111110111 00011000	$\overset{+}{30}, \overset{+}{18}$
15	$\overset{+}{31}, \overset{+}{15}, \overset{+}{3}$	+111110101010001+01011001011+111	+10000-0010111111111001010111100	$\overset{+}{31}, \overset{-}{25}$

Table 22. Values of ∇Q_t and ∇f_t at all bit positions for $0 \leq t \leq 15$, in the second block.

t	δQ_t	∇Q_t	∇f_t	δf_t
14	$\overset{+}{31}$	+10000001111101111111001010111100		
15	$\overset{+}{31}, \overset{+}{15}, \overset{+}{3}$	+11111010101001+01011001011+111		
16	$\overset{+}{31}, \overset{-}{29}$	+0-011100001000011011101101011110	+01111010001000011011100101011111	$\overset{+}{31}$
17	$\overset{+}{31}$	+00011010101100010011110100011111	+00011110101000011011101100011111	$\overset{+}{31}$
18	$\overset{+}{31}$	+00010101011001000010101011111101	+00010110101100000010111001011101	$\overset{+}{31}$
19	$\overset{+}{31}, \overset{+}{17}$	+1100101010111+1100110000100010 0	+00001111111101010011001011101 00	$\overset{+}{31}$
20	$\overset{+}{31}$	+00010111000110010100110001110000	+11011111100110110001100001110000	$\overset{+}{31}$
21	$\overset{+}{31}$	+00101011111000110001000110001000	+00011111101000110101110011111000	$\overset{+}{31}$
22	$\overset{+}{31}$	+00000010111001001100110011100100	+00101010111000100101110111101000	$\overset{+}{31}$
23		00011111111011011111010000111000	00010101111000111110011000110010	
24		11010110011010110000001000100111	+00111101110111110010010001010100	$\overset{+}{31}$
25		00011010011000101100001010101111	11011010011000101100001000101111	
26		01000111111110110001001110011101	01001110011010111100001010001101	
27		01010010011001001010000110111110	01010111111110011001000110111110	
28		01010110111000110111010110011011	01010110111001111011000110111011	
29		01110111001001111100111101101100	01010110101001111101010100101101	
30		11001011111100110001110010001100	01100011111001111001111011101100	
31		11011111010010000100011111100111	11011111110100000101011111100100	

Table 23. Values of ∇Q_t and ∇f_t at all bit positions for $16 \leq t \leq 31$, in the second block.

t	δQ_t	∇Q_t	∇f_t	δf_t
30		110010111111100110001110010001100		
31		11011111010010000100011111100111		
32		11001110101100100110001001111111	11011010000010010011100100010100	
33		10110001010001010011110110100100	10100000101111110001100000111100	
34		11001011110110110011000100010001	10110100001011000110111011001010	
35	$\overset{-}{31}$	-0110000001001111000111000111000	-1001010101110011000001010001101	$\overset{-}{31}$
36	$\overset{+}{31}$	+00101001101111110011110000010100	01101111001000111000001100111101	
37	$\overset{+}{31}$	+01011110000111000000110000101010	-00010111111011010111111000000110	$\overset{-}{31}$
38	$\overset{-}{31}$	-0001000100111011011011110000100	-0110011010011001000011110111010	$\overset{-}{31}$
39	$\overset{-}{31}$	-1110011110000011010000101100100	+1010100010100100001101011001010	$\overset{+}{31}$
40	$\overset{-}{31}$	-0101100001100101111000011100001	-1010111011011101110011000000001	$\overset{-}{31}$
41	$\overset{+}{31}$	+1111010111101100101010111101010	+0100101000001010000010001101111	$\overset{+}{31}$
42	$\overset{-}{31}$	-0000010011100100111000100110101	+1010100101101101101010000111110	$\overset{+}{31}$
43	$\overset{-}{31}$	-0001101111101000110001111110010	+1110101011100000100011100101101	$\overset{+}{31}$
44	$\overset{-}{31}$	-0101111101110101111001000110001	-0100000001111001110000011110110	$\overset{-}{31}$
45	$\overset{-}{31}$	-0110110000010001011011011001111	-0010100010001100010011100001100	$\overset{-}{31}$
46	$\overset{-}{31}$	-0110011010000010101010110101001	-0101010111100110001000101010111	$\overset{-}{31}$
47	$\overset{+}{31}$	+1110001101101111001000111011010	+1110100111111100111001010111100	$\overset{+}{31}$

Table 24. Values of ∇Q_t and ∇f_t at all bit positions for $32 \leq t \leq 47$, in the second block.

t	δQ_t	∇Q_t	∇f_t	δf_t
46	$\overset{-}{31}$	-01100110100000101010101101010 01		
47	$\overset{+}{31}$	+1110001101101111001000111011010		
48	$\overset{-}{31}$	-0001101001001101001000010100100	-0111100000010010010101100101100	$\overset{-}{31}$
49	$\overset{+}{31}$	+1100011001010101000010111110001	+1100010010011000111111101010001	$\overset{+}{31}$
50	$\overset{+}{31}$	+0001010101001000001000110010010	00011001110101111111101000101010	
51	$\overset{+}{31}$	+0110000010100100001100100101001	-0110110011100110110101010111101	$\overset{-}{31}$
52	$\overset{+}{31}$	+0100001100110111011111010011001	-1000101100010011110011111010100	$\overset{-}{31}$
53	$\overset{+}{31}$	+0011000011010101101101111110011	-1111110011101000100000101101110	$\overset{-}{31}$
54	$\overset{+}{31}$	+0000010011111101000110110101000	-1000110000101000000101100001110 1	$\overset{-}{31}$
55	$\overset{+}{31}$	+0001000011100010110011000101010	-1101101100010111110101110000110	$\overset{-}{31}$
56	$\overset{+}{31}$	+1000001111101111000101100010011	-1110101100001101001110101111101	$\overset{-}{31}$
57	$\overset{+}{31}$	+0001000001111110101100001010000	-0111110010010000101001011000110	$\overset{-}{31}$
58	$\overset{+}{31}$	+1110110100011010110011011011010	-1110110101100100010111010101110	$\overset{-}{31}$
59	$\overset{+}{31}$	+1110111000110110110101101100101	-0000001010101101000100100110101	$\overset{-}{31}$
60	$\overset{-}{31}$	-1100000001010110101000010100010	10011110011000001011001011000010	
61	$\overset{+}{31}$	+1000011101010101000001011111011	+0101011110001011100011001011001	$\overset{+}{31}$
62	$\overset{-}{31}, \overset{-}{25}$	-10100-10101101000001001111101001	-0011100011101000010110100000110	$\overset{-}{31}$
63	$\overset{+}{31}, \overset{-}{25}$	+1110-+10101111100100011011010 00	+0101110000001010111011010000101	$\overset{+}{31}$

Table 25. Values of ∇Q_t and ∇f_t at all bit positions for rounds $48 \leq t \leq 63$, in the second block.