# Confirmation that Some Hash Functions Are Not Collision Free

*Shoji Miyaguchi* *Kazuo Ohta* *Masahiko Iwata*

*NTT Communications and Information Processing Laboratories*
*Nippon Telegraph and Telephone Corporation*
*1-2356, Take, Yokosuka-shi, Kanagawa, 238-03 Japan*

**Abstract:** Hash functions are used to compress messages into digital signatures. A hash function has to be collision free; i.e., it must be computationally infeasible to construct different messages which output the same hash-value. This paper shows that five hash functions are not collision free, including the assumptions that an attacker can modify an initial value of the hash function. These hash functions are analyzed from the standpoints of their structure, the complementation property and the weak keys of the block ciphers used in them. As a result, it is clear that many pairs of messages can be created to generate the same hash-values. Therefore, users desiring to use these hash functions should be notified of their weakness.

## 1 Introduction

Digital signature techniques are methods that can confirm the contents of a communication message and its origin [1]. It is recommended to sign a compressed form of the message, the hash-value, in order to enhance digital signature efficiency. Hash functions are nor-

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 326-343, 1991.

mally used for this purpose, especially for long messages. The hash function used to generate the hash-value has to be collision free; i.e., it must be computationally infeasible to construct different messages which output the same hash-value. When a hash function is not collision free, an attacker or malicious sender first signs a message $M$, and then later changes $M$ into a false message $M'$ that yields the same hash-value, and hence the same signature, as message $M$. Therefore, senders can abuse the signature system.

An $n$-bit hash function is a hash function that outputs $n$-bit hash-values. Some existing schemes [3, 4] are 64-bit hash functions, i.e., $n$=64, which include a 64-bit block cipher algorithm [9, 12]. However the birthday attack method [2, 6] can attack any $n$-bit hash function and about $2^{n/2}$ attacks have a success probability of about 0.5. Consequently, the collision free property requires that the length of the hash-value should be at least about 100-bits (128-bits to ensure a sufficient safety margin) to attain the comparable security of a 64-bit block cipher algorithm. Therefore, several $2n$-bit hash functions based on $n$-bit block cipher algorithms were recently proposed [5, 7].

In this paper, five hash functions are analyzed from the standpoints of their structure, the complementation property and the weak keys of the block ciphers used in them. We show that they are not collision free.

A hash-value is calculated from a message and an initial value. Although there are several ways of sharing the initial value between sender and verifier, we will consider the collision free property of the hash functions in the worst case scenario. That is, attacker might be able to modify both the message and the initial value. It is clarified under what conditions the hash functions are collision prone.

## 2 Notation

Hereafter, we use the following notation. Hash function H,

$H = h(M, I)$, is represented as follows:

$H_0 = I$ ( Initial value )

$H_i = \theta(M_i, H_{i-1})$ for $i$ from 1 to $N$

$H = h(M, I) = H_N$ ( Hash-value )

where, $M = M_1 || \ldots || M_i || \ldots || M_N$ : message

$||$ : concatenation, $\phi$ : $n$-zeros

$\theta$ : the iterative function of the hash function

$eK(P)$ : ciphertext block of plaintext block $P$, enciphered by an $n$-bit block cipher using key $K$

$dK(C)$ : plaintext block of ciphertext block $C$, deciphered by an $n$-bit block cipher using key $K$

$X \oplus Y$ : bitwise exclusive-or of data $X$ and $Y$

$X||Y$ : concatenation of data $X$ and $Y$

$\sim X$ : complement of $X$ (All bit inverse of $X$)

## 3 Meyer-Matyas hash function [8]

### 3.1 Algorithm

This is described as:

$H_0 = I$ ( Initial value )

$H_i = \theta_1(M_i, H_{i-1}) = eH_{i-1}(M_i) \oplus M_i$ for $i$ from 1 to $N$

$H = h_1(M, I) = H_N$

$M_i$ , $H_i$ , $I$ : $n$-bit blocks

### 3.2 Consideration of collision prone property

We will describe four kinds of attacks. Three attacks are deterministic and the other one is probabilistic.

#### 3.2.1 Attack 1

We assume that an $n$-bit block cipher satisfies the complementa-

tion property below:

$$e \sim K(\sim P) = \sim eK(P) \tag{1}$$

Then,

$$\begin{aligned}\theta_1(\sim M_i, \sim H_{i-1}) &= e \sim H_{i-1}(\sim M_i) \oplus \sim M_i \\ &= \sim eH_{i-1}(M_i) \oplus \sim M_i \\ &= eH_{i-1}(M_i) \oplus M_i \\ &= \theta_1(M_i, H_{i-1})\end{aligned}$$

holds. Therefore, $h_1(M, I) = h_1(M', \sim I)$ for any given $M$ and $I$, where $M = M_1||M_2||\ldots||M_N$, $M' = (\sim M_1)||M_2||\ldots||M_N$.

The *DES* [9] cipher has the complementation property shown in Equation(1). Thus, the Meyer-Matyas hash function is not collision free if the *DES* cipher is used in its iterative function.

### 3.2.2 Attack 2

When this hash function includes the *DES* cipher in its iterative function, the substantial bit length of $H_i$ is 56. Therefore, an example of the collision prone property is found with $2^{28}$ attacks where the success probability is about 0.5 using the birthday attack [2, 6].

For example, define a message $\xi$ and a mapping $\Psi$ as follows:

$$\xi = M_1||M_2||\ldots||M_{k-1}$$
$$\Psi(\xi) = K_k,$$

where $K_k$ is the substantial bits of $H_{k-1}(k \geq 2)$. Keep both $I$ and $M_k$ constant, apply the birthday attack to $\Psi$ in order to find $\xi$ and $\xi'$ as:

$$\Psi(\xi) = \Psi(\xi') \ , \ \xi \neq \xi'$$

Since $K_k$ is 56-bits long, a pair of $\xi$ and $\xi'$ is found with $2^{28}$ attacks where the success probability is about 0.5. Define $M$ and $M'$ as:

$$M = \xi||M_k||M_{k+1}||\ldots||M_N \ , \quad M' = \xi'||M_k||M_{k+1}||\ldots||M_N.$$

Then, $h_1(M, I) = h_1(M', I)$ holds for any given $I$ and $M_k||\ldots||M_N$ $(k \geq 2)$.

### 3.2.3 Attack 3

We assume that an $n$-bit block cipher has the weak keys, $K_1$ and $K_2$, satisfying Equation(2) for an arbitrary $n$-bit block $K$.

$$eK_2(eK_1(K)) = K \tag{2}$$

Then,

$\theta_1(K, K_1) = eK_1(K) \oplus K$

$\theta_1(eK_1(K), K_2) = eK_2(eK_1(K)) \oplus eK_1(K) = eK_1(K) \oplus K$

The *DES* cipher has the weak keys. Thus, the Meyer-Matyas hash function is collision prone if the *DES* cipher is used in its iterative function. This attack can work well with the *Attack 1.*

### 3.2.4 Attack 4

We assume that an $n$-bit block cipher has the collision keys, $K_x$ and $K_y$ as:

$$eK_x(P) = eK_y(P),\ K_x \neq K_y \text{ for some data block } P$$

Then,

$$\theta_1(P, K_x) = eK_x(P) \oplus P = eK_y(P) \oplus P = \theta_1(P, K_y)$$

The *DES* cipher has the collision keys. An example of collision keys, $K_x$ and $K_y$ is given [6, 11] below in hex.

$P$ = 04 04 04 04 04 04 04 04

$K_x$ = CE 80 6E EE 7C FC D2 EC

$K_y$ = AE 88 38 90 48 74 C6 06

$eK_x(P) = eK_y(P)$ = 15 0E 0B 6F F3 5B 4F 0E

Then, the Meyer-Matyas hash function is collision prone. This attack can work smoothly with the *Attack 1.*

## 4 Davies-Price hash function [4]

### 4.1 Algorithm

This is described as:

$$H_0 = I \text{ ( Initial value )}$$
$$H_i = \theta_2(M_i, H_{i-1})$$
$$= eM_i(H_{i-1}) \oplus H_{i-1} \quad \text{for } i \text{ from 1 to } N$$
$$H = h_2(M, I) = H_N$$

$M_i$ , $H_i$ , $I$ : $n$-bit blocks

### 4.2 Consideration of collision prone property

The basic idea to find collision prone examples will be described below. Find an $n$-bit block $H$ and a message $K$ so as to satisfy:

$$H = \theta_2(K, H) \tag{3}$$

Then, the following relation holds and the hash function is proven to be collision prone:

$$h_2(M, H) = h_2(M', H) = H,$$

where $M = K$ , $M' = K||\ldots||K$.

Furthermore, find an initial value $I$ and a message $K^*$ so as to satisfy:

$$H = \theta_2(K^*, I),$$

where $H$ is the value obtained above. The following relation holds:

$$h_2(M, I) = h_2(M', I) = H,$$

where $M = K^*$ , $M' = K^*||K||\ldots||K$.

#### 4.2.1 Attack 5

Define an $n$-bit block $H$ as follows:

$$H = dK(\phi) \quad \text{for arbitrary } K$$

Then Equation(3) holds. Thus the following relation holds:

$$h_2(M, dK(\phi)) = h_2(M', dK(\phi)) = dK(\phi),$$

where $M = K$, $M' = K||\ldots||K$.

This attack becomes so powerful because it combines the meet-in-the-middle attack [3, 8, 10] that it is used when an initial value is given.

Let $I$ be any given initial value. A pair of $K^*$ and $K$ can be found with $2^{32}$ attacks so as to satisfy the following:

$$eK^*(I) \oplus I = dK(\phi)$$

Then,

$$h_2(M, I) = h_2(M', I) = dK(\phi) \quad \text{for any given } I,$$

where $M = K^*$, $M' = K^*||K||\ldots||K$.

**4.2.2 Attack 6**

We assume that an $n$-bit block cipher satisfies the complementation property of Equation(1). Define an $n$-bit block $H$ as follows:

$$H = \sim d \sim K(\sim \phi) \quad \text{for arbitrary } K$$

Then Equation(3) holds. Thus the following relation holds:

$$\begin{aligned} h_2(M, \sim d \sim K(\sim \phi)) &= h_2(M', \sim d \sim K(\sim \phi)) \\ &= \sim d \sim K(\sim \phi), \end{aligned}$$

where $M = K$, $M' = K||\ldots||K$.

This attack can be extended to the case an initial value is given as well as *Attack 5*.

Let $I$ be any given initial value. A pair of $K^*$ and $K$ can be found with $2^{32}$ attacks so as to satisfy the following [3, 8, 10]:

$$eK^*(I) \oplus I = \sim d \sim K(\sim \phi)$$

Then,

$$h_2(M, I) = h_2(M', I) = \sim d \sim K(\sim \phi),$$

where $M = K^*$, $M' = K^*||K||\ldots||K$.

**4.2.3 Attack 7**

We assume that there is a pair of keys, $K_1$ and $K_2$, in a block cipher satisfying Equation(4).

$$eK_2(eK_1(\phi)) = \phi \tag{4}$$

Note that the weak keys satisfy this equation. Then,

$\theta_2(K_1, \phi) = eK_1(\phi) \oplus \phi = eK_1(\phi)$

$\theta_2(K_2, eK_1(\phi)) = eK_2(eK_1(\phi)) \oplus eK_1(\phi) = eK_1(\phi)$

Thus, $h_2(M, \phi) = h_2(M', eK_1(\phi)) = eK_1(\phi)$,
where $M = K_1||K_2||\ldots||K_2$, $M' = K_2||\ldots||K_2$.

**4.2.4 Attack 8**

We assume that there is a pair of keys, $K_1$ and $K_2$, in a block cipher satisfying Equation(5) and (6).

$$eK_2(eK_1(\sim \phi)) = \sim \phi \tag{5}$$

$$e \sim K_2(\sim eK_1(\sim \phi)) = \sim eK_2(eK_1(\sim \phi)) \tag{6}$$

Note that the weak keys satisfy Equation(5), and if the block cipher has the complementation property of Equation(1), the weak keys also satisfy Equation(6). Then,

$\theta_2(K_1, \sim \phi) = eK_1(\sim \phi) \oplus \sim \phi = \sim eK_1(\sim \phi)$

$\theta_2(\sim K_2, \sim eK_1(\sim \phi)) = e \sim K_2(\sim eK_1(\sim \phi)) \oplus \sim eK_1(\sim \phi)$
$= \sim eK_1(\sim \phi)$

Therefore,

$h_2(M, \sim \phi) = h_2(M', \sim eK_1(\sim \phi)) = \sim eK_1(\sim \phi)$,
where $M = K_1|| \sim K_2||\ldots|| \sim K_2$, $M' = \sim K_2||\ldots|| \sim K_2$.

**4.2.5 Attack 9**

This attack is similar to *Attack 1*, that is, the complementation property of Equation(1) is assumed. Then,

$$\theta_2(\sim K_i, \sim H_{i-1}) = e \sim K_i(\sim H_{i-1}) \oplus \sim H_{i-1}$$
$$= \sim eK_i(H_{i-1}) \oplus \sim H_{i-1} = \theta_2(K_i, H_{i-1})$$

holds. Therefore, $h_2(M, I) = h_2(M', \sim I)$ for any given $I$, where $M = K_1||K_2||\ldots||K_N$, $M' = (\sim K_1)||K_2||\ldots||K_N$.

### 4.3 Summary

The above mentioned results are summarized in *Table 1*. The *DES* cipher has the complementation property of Equation(1) and its weak keys satisfy Equations(4) and (5). If the Davies-Price hash function includes the *DES* cipher, all the examples listed in *Table 1* exist.

## 5 Quisquater-Girault hash function (April version) [5]

In this section, the $2n$-bit hash function presented at Eurocrypt '89 [5] by Quisquater and Girault will be analyzed.

### 5.1 Algorithm

*Figure 1* shows the iterative function, $\theta_3$, of this $2n$-bit hash function. Its procedures are shown below, where $H_i$ and $M_i$ are $2n$-bit blocks, while the others are $n$-bit blocks.

$H_0 = b_{-1}||b_0$ ( Initial value )

$H_i = \theta_3(M_i, H_{i-1})$ for $i$ from 1 to $N$

where

$M_i = m_{2i-1}||m_{2i}$

$w_i = em_{2i-1}(b_{2i-3} \oplus m_{2i}) \oplus m_{2i} \oplus b_{2i-2}$

$b_{2i-1} = em_{2i}(w_i \oplus m_{2i-1}) \oplus m_{2i-1} \oplus b_{2i-3} \oplus b_{2i-2}$

$b_{2i} = w_i \oplus b_{2i-3}$

$H_i = b_{2i-1}||b_{2i}$

$H = h_3(M, I) = H_N$ (Hash-value)

### 5.2 Consideration of collision prone property

Considering a state transition of hash-values for this hash function yields *Figure 2*. Typical examples are as follows:
Assume the key $K$ in a block cipher satisfies Equation(7) and (8):

$$eK(eK(K)) = K \tag{7}$$

$$e \sim K(\sim eK(K)) = \sim eK(eK(K)) \tag{8}$$

Note that the weak keys satisfy Equation(7), and if the block cipher has the complementation property of Equation(1), the weak keys also satisfy Equation(8).

Define $H_0 = \sim \phi || \phi$ and $M_1 = K || \sim K$, then

$$H_1 = \theta_3(M_1, H_0) = \phi || eK(K) \oplus K \tag{9}$$

holds, where Equations(7) and (8) are used.

This state transition is indicated from the state $H_0 (= \sim \phi || \phi)$ to the state $H_1 (= \phi || eK(K) \oplus K)$ using the input $M_1 (= K || \sim K)$. The arrow from $H_0$ to $H_1$ drawn with a straight line means the weak keys and complementation property are necessary.

Define $M_2 = K || K$, then

$$H_2 = \theta_3(M_2, H_1) = \phi || \phi \tag{10}$$

holds, where no condition is necessary.

Define $M_3 = K || K$, then

$$H_3 = \theta_3(M_3, H_2) = \phi || eK(K) \oplus K \tag{11}$$

holds, where Equation(7) is used.

Here, because $H_3 = H_1$ holds, the two states, $H_1$ and $H_2$, are connected and form a loop. There are many initial values other than $\sim \phi || \phi$ but all reduce to the state, $H_1$ or $H_2$, as shown in *Figure 2.*

Moreover, consider the complementation of an arbitrary message block $M_i$. Then

$$\begin{aligned} H_i &= \theta_3(\sim M_i, H_{i-1}) \\ &= \theta_3(\sim m_{2i-1} || \sim m_{2i}, H_{i-1}) = \theta_3(m_{2i-1} || m_{2i}, H_{i-1}) \\ &= \theta_3(M_i, H_{i-1}) \end{aligned}$$

holds, where the complementation property of Equation(1) is used. Therefore, there are two invoking messages between each state in *Figure 2*. One message is always the complement of the other.

### 5.2.1 Attack 10

For any block cipher, the following relation holds:

$h_3(M, \phi || eK_a(K_a) \oplus K_a) = h_3(M', \phi || eK_b(K_b) \oplus K_b) = \phi || \phi$,

where $M = K_a || K_a$, $M' = K_b || K_b$, $K_a$ and $K_b$ are arbitrary $n$-bit blocks, $K_a \neq K_b$.

### 5.2.2 Attack 11

This attack can modify any message component $M_i$ to $\sim M_i$ without changing the initial value and the hash-value. The complementation property of Equation(1) is assumed. Then

$$\theta_3(\sim M_i, H_{i-1}) = \theta_3(M_i, H_{i-1})$$

holds for an arbitrary message block $M_i$. Thus the following relation holds:

$$h_3(M, I) = h_3(M', I) \text{ for any given } M \text{ and } I,$$

where $M = M_1 || \ldots || M_i || \ldots || M_N$,

$M' = M_1 || \ldots || M_{i-1} || \sim M_i || M_{i+1} || \ldots || M_N$.

### 5.2.3 Attack 12

The state transition diagram shown in *Figure 2* allows us to construct many examples of the collision prone property.

For example, when we use the three state transitions, Equations (9), (10), (11), the following relation holds:

$$h_3(M, \sim \phi || \phi) = h_3(M', \sim \phi || \phi) = \phi || \phi,$$

where

$M = K || \sim K || K || K$,

$M' = K || \sim K || K || K || (K || K || K || K) || \ldots || (K || K || K || K)$.

If this hash function includes the *DES* cipher in its iterative function, all the collision prone examples obtained from *Figure 2* exist, because the *DES* cipher has the complementation property and the weak keys.

## 6 Quisquater- Girault hash function (October version) [7]

### 6.1 Algorithm

This scheme was proposed as a modification of the Quisquater-Girault hash function (April version) by originators [7]. In this algorithm, a new message block, $M_{N+1}$, is introduced as a pseudo message block.

$M_1, \ldots, M_N$: real message blocks, where $M_i = m_{2i-1} || m_{2i}$

$M_{N+1}$: a pseudo message block, where $M_{N+1} = m_{2N+1} || m_{2N+2}$

$m_{2N+1} = m_1 \oplus m_2 \oplus \ldots \oplus m_{2N-1} \oplus m_{2N}$

$m_{2N+2} = m_1 + m_2 + \ldots + m_{2N-1} + m_{2N} \bmod (2^n - 1)$

$H_i$, $M_i$, $I$ : $2n$-bit blocks, others : $n$-bit blocks

$H_0 = b_{-1} || b_0$ ( Initial value )

$H_i = \theta_4(M_i, H_{i-1})$ for $i$ from 1 to $N+1$

where

$w_i = em_{2i-1}(b_{2i-3}) \oplus b_{2i-2}$

$b_{2i-1} = em_{2i}(w_i) \oplus b_{2i-3} \oplus b_{2i-2}$

$b_{2i} = w_i \oplus b_{2i-3}$

$H_i = b_{2i-1} || b_{2i}$

$H = h_4(M, I) = H_{N+1}$ ( Hash-value )

### 6.2 Attack 13

For any block cipher,

$$\theta_4(m_1||m_2, a||em_1(a) \oplus a) = \theta_4(m_2||m_1, a||em_2(a) \oplus a) = em_1(a) \oplus em_2(a)||\phi$$

holds, where $a$ is an arbitrary $n$-bit block. Furthermore,

$$m_1 \oplus m_2 \oplus \ldots \oplus m_{2N-1} \oplus m_{2N} = m_2 \oplus m_1 \oplus \ldots \oplus m_{2N-1} \oplus m_{2N},$$

and

$$m_1 + m_2 + \ldots + m_{2N-1} + m_{2N} \bmod (2^n - 1)$$

$= m_2+m_1+\ldots+m_{2N-1}+m_{2N} \bmod (2^n-1)$

hold. Thus the following relation holds:

$$h_4(M, a||em_1(a) \oplus a) = h_4(M', a||em_2(a) \oplus a)$$

where $M = (m_1||m_2)||M_2||\ldots||M_N||M_{N+1}$,

$M' = (m_2||m_1)||M_2||\ldots||M_N||M_{N+1}$.

## 7 2n-bit hash funtion [8]

A $2n$-bit hash function has been proposed that includes an $n$-bit block cipher as the parallel processing element.

### 7.1 Algorithm

This is described as:

$H_0||H'_0 = I||I'$ ( Initial value )

$H_i||H'_i = \theta_5(M_i, H_{i-1}||H'_{i-1})$ for $i$ from 1 to $N$

where

$T_i = eK_i(M_i) \oplus M_i$ where $K_i$ = Adj10 $(H_{i-1})$

$T'_i = eK'_i(M_i) \oplus M_i$ where $K'_i$ = Adj01 $(H'_{i-1})$

$H_i = T_i$[left]$||T'_i$[right] $H'_i = T'_i$[left]$||T_i$[right]

$T_i$[left]: Left half of $T_i$ $T_i$[right]: Right half of $T_i$

$T'_i$[left]: Left half of $T'_i$ $T'_i$[right]: Right half of $T'_i$

$H = h_5(M, I) = H_N||H'_N$ ( Hash-value )

$H_i, H'_i, M_i, I, I'$ : $n$-bit blocks

Here, Adj10($X$) means that: bit positions 2,3 of $X$ are set to '10', and other bits (i.e., bit positions 1(MSB), 4,5,...,64(LSB)) remain unchanged. Adj01($X$) means that: bit positions 2,3 of $X$ are set to '01', and other bits (i.e., bit positions 1,4,5,...,64) remain unchanged.

Paper[8] has the following comment about the initial values:

> *These* (initial values) *can be standardized, or randomly generated by the authenticator. If static origin keys* (initial values) *are used, they are defined here* $I$ = 5252525252525252 in hex, $I'$ = 2525252525252525 in hex.

### 7.2 Attack 14

Find collision keys, $K_x$ and $K_y$, using the birthday attack [2, 6] such that:

$eK_x(P) = eK_y(P), K_x \neq K_y$, for some data block $P$

bit positions 2,3 of $K_x$ are 1,0, bit positions 2,3 of $K_y$ are 0,1.

Then, the following equations hold:

Adj10 $(K_x) = K_x$, Adj01 $(K_y) = K_y$

Adj10 $(\sim K_y) = \sim K_y$, Adj01 $(\sim K_x) = \sim K_x$

We assume the complementation property of Equation(1). Then,

$$H_1 || H_1 = \theta_5(P, K_x || K_y) = \theta_5(\sim P, \sim K_y || \sim K_x).$$

The *DES* cipher has collision keys [11]. Thus, users of the $2n$-bit hash function have to adopt at least the initial values as specified by paper[8].

## 8 Conclusion

The collision free property of hash functions has been analyzed considering hash function structures, the complementation property and the weak keys of the block cipher used in their iterative functions. This paper has shown that five hash functions are not collision free. One of our assumptions is that an attacker can modify the initial value of the hash function. Thus, users desiring to use these hash functions should be notified of their weakness. The authors recommend that the initial value should be standardized to decrease collision-prone cases. We have proposed a new 128-bit hash function, *N-Hash*[13], which seems to be collision free.

### Acknowledgement

The authors would like to thank Dr. Marc Girault with SEPT for various comments on our previous version, and Dr. D. W. Davies for informing us of the initial value requirements of the 2n-bit hash function [8].

## References


[1] Davies,D.W. :"Applying the RSA digital signature to electronic mail, " IEEE Computer, 16, 2, pp. 55-62 ( Feb. 1983 )

[2] Yuval,G. :"How to swindle Rabin," Cryptologia, 3, 3, pp.187-190 (July 1979)

[3] Meyer,C.H. and Matyas,S.M. :"Cryptography : A new dimension in Computer data security," John Willy and Sons, Inc. (1982)

[4] Davies,D.W. and Price,W.L. :"Digital Signatures - An Update," 7th Int. Conf. on Computer Communication, pp.845-849 (1984)

[5] Quisquater, J.J. and Girault,M. :"2n-bit Hash- Functions Using n-bit Symmetric Block Cipher Algorithms," Eurocrypt'89 (Abstract)

[6] Quisquater,J.J. and Delescaille,J.P. :"How easy is collision search? Application to DES," Eurocrypt'89 (Abstract)

[7] Quisquater, J.J. and Girault,M. : Manuscript of "2n-bit Hash-Functions Using n-bit Symmetric Block Cipher Algorithms," Eurocrypt'89 ( for Lecture Note) (October 1989, private correspondence)

[8] Meyer,C.H. and Schilling,M. :"Secure Program Load with Modification Detection Code," Proc. of SECURICOM 88, pp.111-130 (1988)

[9] "Data Encryption Standard," FIPS Pub.46, NBS(1977)

[10] Ohta,K. and Koyama,K. : "A Meet-in-the-Middle Attack against Mixed-Type Digital Signature Methods," Trans. IEICE Japan, J70-D, 2, pp.415-422 (Feb.1987)

[11] Quisquater,J.J. and Delescaille,J.P. :"How easy is collision search? New results and application to DES," Crypto'89 (Abstract)

[12] Miyaguchi,S., Shiraishi,S. and Shimizu,S. :"Fast Data Encipherment Algorithm FEAL-8," Review of the Electrical Communication Laboratories, 36, 4, pp.433-437 (1988)

[13] Miyaguchi,S., Ohta,K. and Iwata,M. :"128-bit Hash Function (N-Hash)," Proc. of SECURICOM 90, pp.123-137 (Mar.1990)

# Table 1. Examples of collision messages in the Davies–Price hash function

| Initial value | Message chain | Hash-value | Note | Attack |
|---|---|---|---|---|
| $dK(\phi)$ | $K\|\|K\|\|K\|\|\ldots$ | $dK(\phi)$ | 1) | 5 |
| given I | $K^*\|\|K\|\|K\|\|\ldots$ | $dK(\phi)$ | 2) | |
| $\sim d\sim K(\sim\phi)$ | $K\|\|K\|\|K\|\|\ldots$ | $\sim d\sim K(\sim\phi)$ | 1),4) | 6 |
| given I | $K^*\|\|K\|\|K\|\|\ldots$ | $\sim d\sim K(\sim\phi)$ | 3),4) | |
| $d\sim K(\sim\phi)$ | $\sim K\|\|K\|\|K\|\|\ldots$ | $\sim d\sim K(\sim\phi)$ | 1),4) | 6, 9 |
| $\phi$ | $K_1\|\|K_2\|\|K_2\|\|\ldots$ | $eK_1(\phi)$ | 5) | 7 |
| $eK_1(\phi)$ | $K_2\|\|K_2\|\|K_2\|\|\ldots$ | $eK_1(\phi)$ | | |
| $\sim eK_1(\phi)$ | $\sim K_2\|\|K_2\|\|K_2\|\|\ldots$ | $eK_1(\phi)$ | 6) | 7, 9 |
| $\sim\phi$ | $K_1\|\|\sim K_2\|\|\sim K_2\|\|\ldots$ | $\sim eK_1(\sim\phi)$ | 7) | 8 |
| $\sim eK_1(\sim\phi)$ | $\sim K_2\|\|\sim K_2\|\|\sim K_2\|\|\ldots$ | $\sim eK_1(\sim\phi)$ | | |
| $eK_1(\sim\phi)$ | $K_2\|\|\sim K_2\|\|\sim K_2\|\|\ldots$ | $\sim eK_1(\sim\phi)$ | 7) | 8, 9 |
| given I and $\sim$I | $K_1\|\|K_2\|\|..\|\|K_N$ and $(\sim K_1)\|\|K_2\|\|..\|\|K_N$ | $H_N$ | 4) | 9 |

Notation:

$H_0$=I (initial value), $C_i$ : message chain

$H_i = eC_i(H_{i-1}) \oplus H_{i-1}$, from i=1 to n

C=eK(P), P=dK(C) : e:enciphering, d:deciphering

K : key, C : ciphertext, P : plaintext, $\phi$ : null data block

$\sim$x : all bit inverse of x, || : concatenation

Notes:

1) K is arbitrary 64-bit data block.

2) K* and K are 64-bit data blocks that satisfy $eK^*(I) \oplus I = dK(\phi)$. A pair of K* and K can be found by the meet-in-the-middle attack using any given initial value I.

3) K* and K are 64-bit data blocks that satisfy $eK^*(I) \oplus I = \sim d\sim K(\sim\phi)$. A pair of K* and K can be found by the meet-in-the-middle attack using any given initial value I.

4) The encipherment algorithm should satisfy the following for massage block K:

$$e\sim K(\sim P) = \sim eK(P)$$

5) The encipherment algorithm should satisfy the following for a pair of keys, $K_1$ and $K_2$:

$$eK_2(eK_1(\phi)) = \phi$$

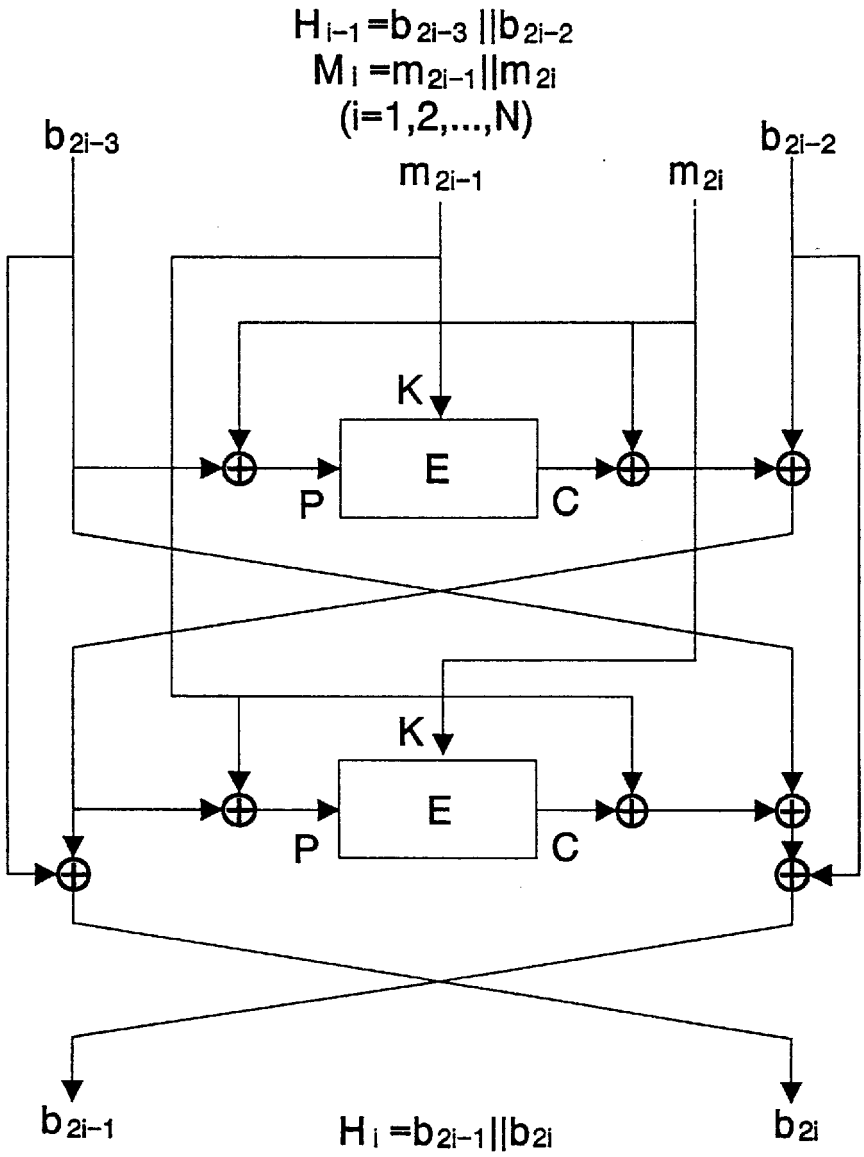
6) The encipherment algorithm should satisfy the following for a pair of keys, $K_1$ and $K_2$:

$$eK_2(eK_1(\phi)) = \phi \quad \text{and} \quad e\sim K_2(\sim eK_1(\phi)) = \sim eK_2(eK_1(\phi))$$

7) The encipherment algorithm should satisfy the following for a pair of keys, $K_1$ and $K_2$:

$$eK_2(eK_1(\sim\phi)) = \sim\phi \quad \text{and} \quad e\sim K_2(\sim eK_1(\sim\phi)) = \sim eK_2(eK_1(\sim\phi))$$

The DES cipher has the properties listed in notes 4)–7).




K : Key input, P : Plaintext input, C : Ciphertext output
E : n-bit block cipher

Figure 1. Iterative function of the Quisquater-Girault hash function (April 1989 version)[5]

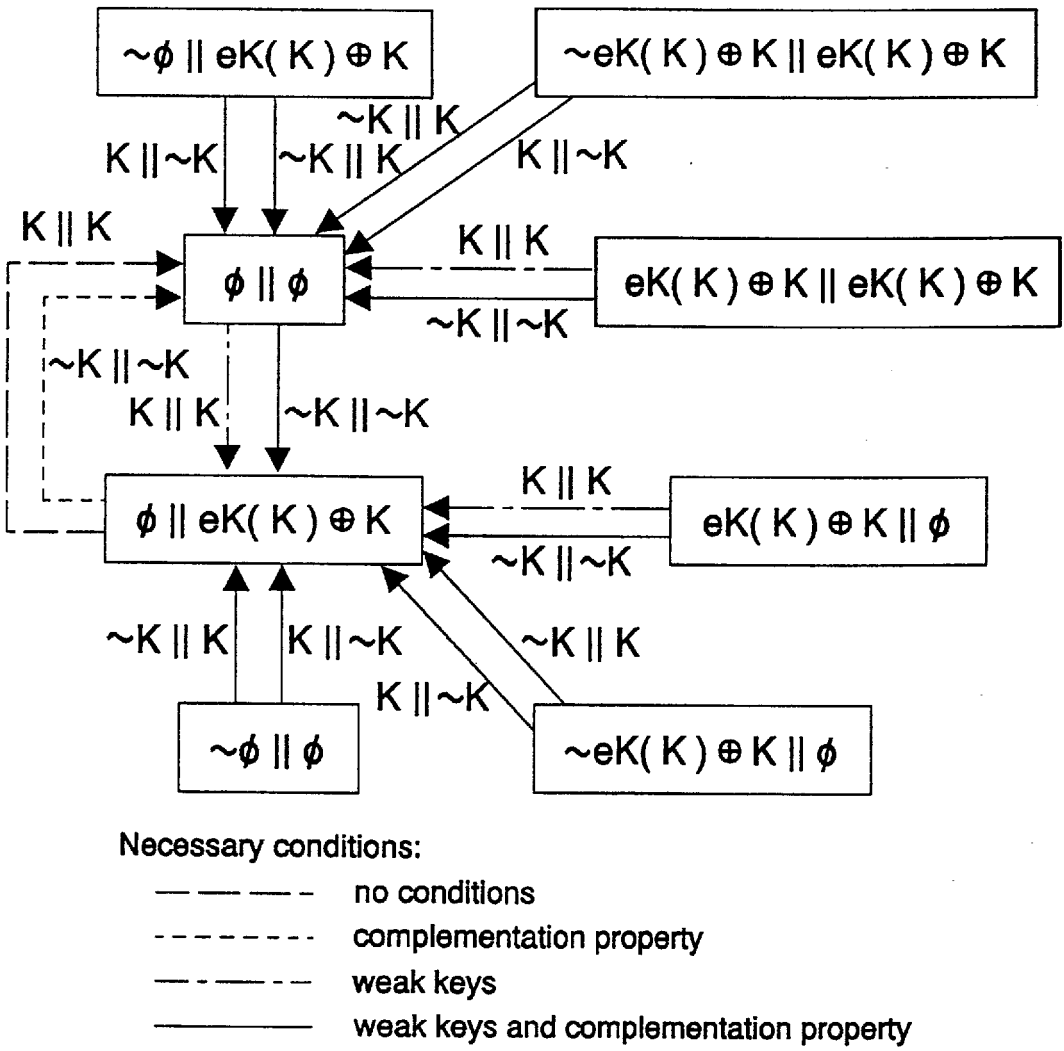



Figure 2. State transition of the Quisquater–Girault hash function (April 1989 version)