PAPER Special Section on Information Theory and Its Applications

# A Security Analysis of Double-Block-Length Hash Functions with the Rate 1*

**Shoichi HIROSE**[†a)], ***Member***

**SUMMARY** In this article, the security of double-block-length hash functions with the rate 1 is analyzed, whose compression functions are composed of block ciphers with their key length twice larger than their block length. First, the analysis by Satoh, Haga and Kurosawa is investigated, and it is shown that there exists a case uncovered by their analysis. Second, a large class of compression functions are defined, and it is shown that they are at most as secure as those of single-block-length hash functions. Finally, some candidate hash functions are given which are possibly optimally collision-resistant.

***key words:*** *cryptographic hash function, double-block-length hash function, compression function*

## 1. Introduction

A cryptographic hash function is a function which maps an input of arbitrary length to an output of fixed length. It is one of the most important primitives in cryptography [17] and should satisfy preimage resistance, second-preimage resistance and collision resistance. Informally, preimage resistance means that, given an output, it is infeasible to obtain an input which produces the output. Second-preimage resistance means that, given an input, it is infeasible to obtain another input which produces the same output as the given input. Collision resistance means that it is infeasible to obtain two distinct inputs which produce the same output. For simplicity, a cryptographic hash function is called a hash function in this article.

A hash function usually consists of iteration of a compression function with fixed input/output length and is called an iterated hash function. Compression-function constructions are classified into two types: using block ciphers and from scratch. The topic of this article is the former. It is expected to minimize design and implementation effort with secure block ciphers. Its major drawback is slow processing speed. However, it is compensated by fast block ciphers such as AES. Furthermore, some recent work has pointed out weakness of customized hash functions such as MD5 and SHA-1 [1], [21]–[23]. Thus, hash functions composed of block ciphers may become more important.

Hash functions composed of block ciphers are classified into two categories: single-block-length (SBL) and double-block-length (DBL). A SBL hash function is a hash function whose output length is equal to the block length. The output length of a DBL hash function is twice larger than the block length. It is well-known that the birthday attack can find a collision of a hash function with the complexity $O(2^{\ell/2})$, where $\ell$ is the output length of the hash function. The block length of widely used block ciphers is 64 or 128. Thus, SBL hash functions are no longer secure in terms of collision resistance.

In this article, we analyze the security of a large class of DBL hash functions. They are based on block ciphers whose key length is twice larger than the block length and their rates are 1. For this kind of DBL hash functions, a detailed analysis is given by Satoh, Haga and Kurosawa [20]. They stated that no effective attacks were found for the DBL hash functions satisfying the property called "exceptional" defined by them.

In this paper, first, their analysis is reviewed, and it is shown that there exists a case uncovered by their analysis. This result implies that there exist DBL hash functions whose compression functions do not satisfy the property "exceptional" and on which no effective attacks are found.

Second, a large class of compression functions are defined, and it is shown that they are at most as secure as those of single-block-length hash functions. Thus, even if there exist optimally collision-resistant DBL hash functions of this type, it cannot be proved based solely on collision resistance of their compression functions owing to Merkle and Damgård.

Finally, some candidate hash functions are given which are possibly optimally collision-resistant. However, it is still an open question if they really optimally collision-resistant.

The paper is organized as follows. Some definitions are introduced and mathematical facts are described in Sect. 2. The analysis by Satoh, Haga and Kurosawa is investigated in Sect. 3. In Sect. 4, the analysis of compression functions is described. Some candidate hash functions are given which are possibly optimally collision-resistant in Sect. 5. Finally, Sect. 6 concludes the paper.

### 1.1 Related Work

For DBL hash functions, many schemes have been presented [3], [7]–[9], [11]–[13], [15], [16], [18], [19]. Among them, three DBL hash functions composed of DES [18] have been shown to be optimally collision-resistant in the ideal-cipher model: the complexity of any collision-finding al-

Manuscript received January 13, 2006.
Manuscript revised April 11, 2006.
Final manuscript received May 25, 2006.

[†]The author is with the Faculty of Engineering, The University of Fukui, Fukui-shi, 910-8507 Japan.

*This is a modified version of [6] in References.

a) E-mail: hirose@fuee.fukui-u.ac.jp

DOI: 10.1093/ietfec/e89–a.10.2575

gorithm for them is $\Omega(2^{\ell/2})$, where $\ell$ is the output length. However, their rates are at most 0.276 and they are not efficient. Recently, other constructions of DBL hash functions have been given in [7], [8], [16], [19]. They are composed of block ciphers whose key length is larger than the block length. Their rates are still low and at most 1/2. Optimal collision resistance of these schemes are implied by optimal collision resistance of their compression functions owing to Merkle and Damgård [4], [18].

Knudsen, Lai and Preneel [14] discussed the security of DBL hash functions with the rate 1 based on $(n, n)$ block ciphers. An $(m, \kappa)$ block cipher is a block cipher with its block length $m$ and its key length $\kappa$. Hohl, Lai, Meier and Waldvogel [9] discussed the security of compression functions of DBL hash functions with the rate $1/2$. On the other hand, the security of DBL hash functions with the rate 1 based on $(n, 2n)$ block ciphers was discussed by Satoh, Haga and Kurosawa [20] and by Hattori, Hirose and Yoshida [6]. This article is a revised and generalized version of [6]. A slightly larger class of DBL hash functions are discussed and proofs are largely simplified in Sect. 4. Moreover, Sect. 5 is added.

Recently, Black, Cochran and Shrimpton [2] showed that it is impossible to construct a highly efficient block-cipher-based hash function provably secure in the black-box model. A block-cipher-based hash function is highly efficient if it makes exactly one block-cipher call for each message block and all block-cipher calls use a single key.

## 2. Preliminaries

$\mathbb{N}$ denotes the set of natural numbers. $\oplus$ denotes the bitwise exclusive OR. For binary sequences $a$ and $b$, $a||b$ denotes their concatenation.

### 2.1 Block Ciphers

A block cipher is a keyed function which maps an $m$-bit plaintext to an $m$-bit ciphertext. Let $\kappa, m \in \mathbb{N}$. An $(m, \kappa)$ block cipher is a mapping $E : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^m$. For each $k \in \{0,1\}^\kappa$, the function $E_k(\cdot) = E(k, \cdot)$ is a one-to-one mapping from $\{0,1\}^m$ to $\{0,1\}^m$. $\{0,1\}^\kappa$ and $\{0,1\}^m$ in the domain $\{0,1\}^\kappa \times \{0,1\}^m$ and $\{0,1\}^m$ in the range are called the key space, the plaintext space, and the ciphertext space, respectively. $m$ is called the block length and $\kappa$ is called the key length.

### 2.2 Hash Functions

A hash function is a mapping from the set of all binary sequences to the set of binary sequences of some fixed length. A hash function is denoted by $h : \{0,1\}^* \to \{0,1\}^\ell$, where $\{0,1\}^* = \bigcup_{i \geq 0} \{0,1\}^i$.

A hash function $h : \{0,1\}^* \to \{0,1\}^\ell$ usually consists of a compression function $f : \{0,1\}^\ell \times \{0,1\}^{\ell'} \to \{0,1\}^\ell$ and an initial value $IV \in \{0,1\}^\ell$. $h$ is computed by the iterated application of $f$ to the given input. Thus, $h$ is called an iterated hash function. The output of the hash function $h$ for an input $M \in \{0,1\}^*$, $h(M)$, is calculated as follows. $M$ is called a message.

1. Some unambiguous padding is applied to the message $M$. The length of the padded message is a multiple of $\ell'$. It is divided into the blocks $M_1, M_2, \ldots, M_n$, where $M_i \in \{0,1\}^{\ell'}$ for $i = 1, 2, \ldots, n$.
2. $H_i = f(H_{i-1}, M_i)$ is calculated for $i = 1, 2, \ldots, n$, where $H_i \in \{0,1\}^\ell$ and $H_0 = IV$. $H_n$ is the output of $h$ for the message $M$, that is, $H_n = h(M)$. If the initial value should be specified, the equation is described as $H_n = h(H_0, M)$.

### 2.3 Properties Required for Hash Functions

For a hash function $h$, there exist many pairs $(M, \hat{M})$ such that $h(M) = h(\hat{M})$ and $M \neq \hat{M}$. For the cryptographic use, $h$ must satisfy the following properties.

**Preimage resistance** Given a hash value $H$, it is computationally infeasible to find a message $M$ such that $h(M) = H$.

**Second-preimage resistance** Given a message $M$, it is computationally infeasible to find a message $\hat{M}$ such that $h(M) = h(\hat{M})$ and $M \neq \hat{M}$.

**Collision resistance** It is computationally infeasible to find a pair of messages, $M$ and $\hat{M}$, such that $h(M) = h(\hat{M})$ and $M \neq \hat{M}$.

### 2.4 Attacks on Hash Functions

The following attacks [14] are against the properties listed in Sect. 2.3.

**The preimage attack** Given an initial value $H_0$ and a hash value $H$, find a message $M$ such that $H = h(H_0, M)$.

**The second-preimage attack** Given an initial value $H_0$ and a message $M$, find a message $\hat{M}$ such that $h(H_0, M) = h(H_0, \hat{M})$ and $M \neq \hat{M}$.

**The free-start preimage attack** Given a hash value $H$, find an initial value $H_0$ and a message $M$ such that $h(H_0, M) = H$.

**The free-start second-preimage attack** Given an initial value $H_0$ and a message $M$, find an initial value $\hat{H}_0$ and a message $\hat{M}$ such that $h(H_0, M) = h(\hat{H}_0, \hat{M})$ and $(H_0, M) \neq (\hat{H}_0, \hat{M})$.

**The collision attack** Given an initial value $H_0$, find two messages $M$, $\hat{M}$ such that $h(H_0, M) = h(H_0, \hat{M})$ and $M \neq \hat{M}$.

**The semi-free-start collision attack** Find an initial value $H_0$ and two messages $M$, $\hat{M}$ such that $h(H_0, M) = h(H_0, \hat{M})$ and $M \neq \hat{M}$.

**The free-start collision attack** Find two initial values $H_0$, $\hat{H}_0$ and two messages $M$, $\hat{M}$ such that $h(H_0, M) = h(\hat{H}_0, \hat{M})$ and $(H_0, M) \neq (\hat{H}_0, \hat{M})$.

The following two facts [5] are often used to estimate the amount of computation of the attacks.

**Proposition 1:** Suppose that a sample of size $r$ is drawn from a set of $N$ elements with replacement. If $r, N \to \infty$, then the probability that a given element is drawn converges to $1 - \exp(-r/N)$.

**Proposition 2** (Birthday Paradox): Suppose that a sample of size $r$ is drawn from a set of $N$ elements with replacement. If $r, N \to \infty$ and $r$ is $O(\sqrt{N})$, then the probability that there is at least one coincidence converges to $1 - \exp(-r^2/(2N))$.

### 2.5 Hash Functions Composed of Block Ciphers

Let $h : \{0,1\}^* \to \{0,1\}^\ell$ be an iterated hash function and $E : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^m$ be a block cipher used in the compression function of $h$. If $\ell = m$, then $h$ is called an SBL hash function. If $\ell = 2m$, then $h$ is called a DBL hash function.

Let $\sigma$ be the number of the calls of the block cipher used in the compression function. Let $\ell' = |M_i|$. Then, the rate is defined as $\ell'/(\sigma m)$ and is used as a measure of efficiency.

### 2.6 The Ideal-Cipher Model

In the ideal-cipher model, a block cipher is assumed to be random, that is, $E_k : \{0,1\}^m \to \{0,1\}^m$ is a random permutation for each $k \in \{0,1\}^\kappa$. Two oracles, $E$ and $E^{-1}$, are available. The encryption oracle $E$ returns $E_k(x)$ on an input $(k, x)$. The decryption oracle $E^{-1}$, on an input $(k, y)$, returns $x$ such that $E_k(x) = y$.

In this model, the complexity of an attack is the required number of encryptions and decryptions of the block cipher. This is the number of the queries to the oracles.

## 3. A Comment on the Analysis by Satoh, Haga and Kurosawa

Satoh, Haga and Kurosawa [20] have analyzed the security of the DBL hash functions with the rate 1, whose compression functions are defined as follows.

**Definition 1:** Let $M_i = (M_i^1, M_i^2) \in \{0,1\}^{2m}$ be a message block, where $M_i^1, M_i^2 \in \{0,1\}^m$. The compression function $(H_i, G_i) = f(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$ is defined by the two functions $f_{\mathrm{U}}, f_{\mathrm{L}}$ such as

$$H_i = f_{\mathrm{U}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E_{A\|B}(C) \oplus D,$$
$$G_i = f_{\mathrm{L}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E_{W\|X}(Y) \oplus Z,$$

where $H_j, G_j \in \{0,1\}^m$ for $j = i-1, i$ and $E$ is an $(m, 2m)$ block cipher. $A, B, C, D, W, X, Y, Z \in \{0,1\}^m$ and $A, B, C, D$ and $W, X, Y, Z$ are represented by linear combinations of $H_{i-1}, G_{i-1}, M_i^1, M_i^2$ such as

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = U \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix} \text{ and } \begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = L \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix},$$

where both $U$ and $L$ are $4 \times 4$ binary matrices[†]. Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}$ denote the row vectors of $U$ and let $\boldsymbol{w}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ denote the row vectors of $L$.

In this section, their analysis is reconsidered. It is shown that there exists a case uncovered by their analysis.

### 3.1 Analysis by Satoh, Haga and Kurosawa

Satoh, Haga and Kurosawa presented effective attacks against hash functions whose compression functions does not satisfy the property called "exceptional" defined in their paper. This property is defined as follows.

**Definition 2:** Let $Q$ be a $4 \times 4$ binary matrix. Let $Q_{\mathrm{rh}}$ be the $4 \times 2$ submatrix of $Q$, where $Q_{\mathrm{rh}}$ consists of the right half elements of $Q$. Let $Q_{\mathrm{rh}}^3$ be the $3 \times 2$ submatrix of $Q_{\mathrm{rh}}$ such that the third row of $Q_{\mathrm{rh}}$ is deleted. Let $Q_{\mathrm{rh}}^4$ be the $3 \times 2$ submatrix of $Q_{\mathrm{rh}}$ such that the fourth row of $Q_{\mathrm{rh}}$ is deleted. $Q$ is called "exceptional" if $\mathrm{rank}(Q) = 4$ and $\mathrm{rank}(Q_{\mathrm{rh}}^3) = \mathrm{rank}(Q_{\mathrm{rh}}^4) = 2$.

The following claim is Theorem 16 in their paper.

**Claim 1:** Let $h$ be a DBL hash function with the rate 1, whose compression function is specified in Definition 1. Suppose that at least one of $U$ and $L$ is not "exceptional." Then, there exist second-preimage and preimage attacks on $h$ with about $4 \times 2^m$ complexity. Furthermore, there exists a collision attack on $h$ with about $3 \times 2^{m/2}$ complexity.

### 3.2 A Comment

In this section, it is shown that the attacks by Satoh, Haga and Kurosawa do not work on some hash functions as is expected though their compression functions do not satisfy "exceptional."

Without loss of generality, we assume that $U$ is not "exceptional." Let $N_2$ be the $2 \times 2$ submatrix of $U_{\mathrm{rh}}$, where $N_2$ consists of the upper half elements of $U_{\mathrm{rh}}$. Satoh et al. presented their proof of Claim 1 for two cases: (i) $\mathrm{rank}(U) = 3$ and $\mathrm{rank}(N_2) = 2$ and (ii) $\mathrm{rank}(U) = 4$. The first case is investigated in the remaining part. Their proof proceeds as follows.

Since $\mathrm{rank}(N_2) = 2$, one can find (by elementary row operations) $\alpha, \beta \in \{0,1\}$ such that

$$U' = \begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{b} \\ \boldsymbol{c} \\ \boldsymbol{d} \oplus \alpha\boldsymbol{a} \oplus \beta\boldsymbol{b} \end{pmatrix} = \begin{pmatrix} N_1 & N_2 \\ N_3' & N_4' \end{pmatrix},$$

where

$$N_4' = \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}.$$

[†]In [20], $W$, $X$, $Y$, $Z$ are represented by some (not necessarily linear) combinations of $H_{i-1}, G_{i-1}, M_i^1, M_i^2$. However, it does not matter whether the combination is linear or not in the discussion of this section.

Let

$$\begin{pmatrix} A \\ B \\ C \\ D' \end{pmatrix} = U' \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}.$$

Then, $D' = 0$, $H_{i-1}$, $G_{i-1}$ or $H_{i-1} \oplus G_{i-1}$.

Subsequently, they stated in their proofs that $\boldsymbol{c} = \lambda_1 \boldsymbol{a} \oplus \lambda_2 \boldsymbol{b}$ when $D' \neq 0$. However, in general, there may be a case that $\boldsymbol{c} = \lambda_1 \boldsymbol{a} \oplus \lambda_2 \boldsymbol{b} \oplus \boldsymbol{d}$ when $D' \neq 0$. Furthermore, in this case, their attack for the case that $\mathrm{rank}(U) = 3$, $\mathrm{rank}(N_2) = 2$, and $D' \neq 0$ cannot be applied.

In their attack, the adversary chooses random triples $(A, B, C)$ such that $C = \lambda_1 A \oplus \lambda_2 B$ and computes $D = E_{A\|B}(C) \oplus H_i$. Then the adversary computes $D' = D \oplus \alpha A \oplus \beta B$. However, if $\boldsymbol{c} = \lambda_1 \boldsymbol{a} \oplus \lambda_2 \boldsymbol{b} \oplus \boldsymbol{d}$, $C$ is calculated by $A$, $B$ and $D$. Therefore, the adversary cannot compute $D$ by $E_{A\|B}(C) \oplus H_i$.

## 4. Collision-Resistance of Compression Functions

Let $\mathcal{H}$ be the set of DBL hash functions composed of the compression functions in Definition 1 satisfying

- Both $U$ and $L$ are "exceptional," or
- $\mathrm{rank}(U) = \mathrm{rank}(L) = 3$, $\boldsymbol{c} \oplus \boldsymbol{d} = \lambda_1 \boldsymbol{a} \oplus \lambda_2 \boldsymbol{b}$ for some $\lambda_1, \lambda_2 \in \{0, 1\}$, $\boldsymbol{y} \oplus \boldsymbol{z} = \lambda_3 \boldsymbol{w} \oplus \lambda_4 \boldsymbol{x}$ for some $\lambda_3, \lambda_4 \in \{0, 1\}$, and the upper right $2 \times 2$ submatrices of $U$ and $L$ are both non-singular.

From the results by Satoh, Haga and Kurosawa and the discussion in Sect. 3, there may exist some $h \in \mathcal{H}$ such that the complexity of any second-preimage/preimage attack on $h$ is $\omega(2^m)$ and the complexity of any collision attack on $h$ is $\omega(2^{m/2})$.

For collision resistance, Merkle [18] and Damgård [4] independently showed that, from any algorithm for the collision attack on a hash function, an algorithm for the free-start collision attack on its compression function is constructed. The complexity of the latter algorithm is almost equal to that of the former one. Thus, if there exists no effective free-start collision attack on a compression function, then there exists no effective collision attack on the hash function composed of the compression function.

In this section, however, it is shown that there exist effective free-start collision attacks with the complexity $O(2^{m/2})$ on all compression functions in Definition 1. Thus, it is impossible to prove collision resistance of DBL hash functions composed of the compression functions in Definition 1 based on the result of Merkle and Damgård.

Actually, for a larger class of compression functions than in Definition 1, free-start collision attacks with the complexity $O(2^{m/2})$ are presented. Effective free-start second-preimage attacks are also presented. Their complexity is $O(2^m)$.

**Definition 3:** Let $M_i = (M_i^1, M_i^2) \in \{0, 1\}^{2m}$ be a message block, where $M_i^1, M_i^2 \in \{0, 1\}^m$. The compression function $(H_i, G_i) = f(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$ is defined by the two functions $f_{\mathrm{U}}, f_{\mathrm{L}}$ such as

$$H_i = f_{\mathrm{U}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = {E^{\mathrm{U}}}_{A\|B}(C) \oplus D,$$
$$G_i = f_{\mathrm{L}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2, H_i) = {E^{\mathrm{L}}}_{W\|X}(Y) \oplus Z,$$

where $H_j, G_j \in \{0, 1\}^m$ for $j = i - 1, i$ and both $E^{\mathrm{U}}$ and $E^{\mathrm{L}}$ are $(m, 2m)$ block ciphers. $A, B, C, D, W, X, Y, Z \in \{0, 1\}^m$ and $A, B, C, D$ and $W, X, Y, Z$ are represented by linear combinations of $H_{i-1}, G_{i-1}, M_i^1, M_i^2$ and $H_i$ as follows:

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = U \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = L \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix} \oplus v H_i, \tag{2}$$

where $U$ and $L$ are $4 \times 4$ binary matrices and $v \in \{0, 1\}^4$ is a column vector. Let $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ and $\boldsymbol{d}$ denote the row vectors of $U$ and let $\boldsymbol{w}$, $\boldsymbol{x}$, $\boldsymbol{y}$ and $\boldsymbol{z}$ denote the row vectors of $L$.

It is easy to see that Definition 3 coincides with Definition 1 if $E^{\mathrm{U}} = E^{\mathrm{L}}$ and $v = (0, 0, 0, 0)^{\mathrm{T}}$. If $v = (0, 0, 0, 0)^{\mathrm{T}}$, then the compression function is said to be in the parallel type. Otherwise, it is said to be in the serial type.

**Theorem 1:** Let $f$ be a compression function in Definition 3. Then, there exists a free-start collision attack on $f$ with the complexity at most about $2 \times 2^{m/2}$. There also exists a free-start second-preimage attack on $f$ with the complexity at most about $2 \times 2^m$.

This theorem is proved for the following cases: (i) $\mathrm{rank}(U) = 4$, (ii) $\mathrm{rank}(U) = 3$, and (iii) $\mathrm{rank}(U) \leq 2$.

**Lemma 1:** Let $f$ be a compression function in Definition 3. Suppose that $\mathrm{rank}(U) = 4$. Then, there exists a free-start collision attack on $f$ with the complexity at most about $2 \times 2^{m/2}$. There also exists a free-start second-preimage attack with the complexity at most about $2 \times 2^m$.

(Proof) Case (a). Suppose that $\mathrm{rank}(L) \geq 3$. Since $\mathrm{rank}(U) = 4$, from (1),

$$\begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix} = U^{-1} \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix}. \tag{3}$$

*The free-start second-preimage attack.* The adversary $\mathcal{A}$ proceeds as follows.

S0. $\mathcal{A}$ computes the output $(H_i, G_i)$ for the given input $(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$.

S1. $\mathcal{A}$ chooses $2^m$ random 3-tuples $(\tilde{A}, \tilde{B}, \tilde{C})$ and computes $\tilde{D} = {E^{\mathrm{U}}}_{\tilde{A}\|\tilde{B}}(\tilde{C}) \oplus H_i$. Since the block cipher is assumed to be random, $\tilde{D}$ is also random.

S2. For each 4-tuple $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$, $\mathcal{A}$ computes $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ with (3). Since $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ is random, $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ is also random.

S3. For each $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$, $\mathcal{A}$ computes $(\tilde{W}, \tilde{X}, \tilde{Y}, \tilde{Z})$ with (2) and computes $\tilde{G}_i = E^{\mathrm{L}}_{\tilde{W}\|\tilde{X}}(\tilde{Y}) \oplus \tilde{Z}$.

Since $\mathrm{rank}(L) \geq 3$, $(\boldsymbol{w}, \boldsymbol{x}) \neq (\boldsymbol{0}, \boldsymbol{0})$. Thus, at least one of $\tilde{W}$ and $\tilde{X}$ is expressed by a linear combination of $\tilde{H}_{i-1}$, $\tilde{G}_{i-1}$, $\tilde{M}_i^1$ and $\tilde{M}_i^2$. Since $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ is random, $E^{\mathrm{L}}_{\tilde{W}\|\tilde{X}}(\tilde{Y})$ is random, and $\tilde{G}_i$ is also random. Thus, according to Proposition 1, $\mathcal{A}$ can find $\tilde{G}_i$ such that $G_i = \tilde{G}_i$ with probability about 0.63. The total complexity is about $2 \times 2^m$.

*The free-start collision attack.* $\mathcal{A}$ chooses arbitrary $H_i$. Then, it chooses $2^{m/2}$ random 3-tuples $(\tilde{A}, \tilde{B}, \tilde{C})$ and computes $\tilde{G}_i$ in the same way as in the S1–S3 above. According to Proposition 2, $\mathcal{A}$ can find a collision of $f_{\mathrm{L}}$ with probability about 0.39. The total complexity is about $2 \times 2^{m/2}$.

Case (b). Suppose that $\mathrm{rank}(L) \leq 2$. Since $\mathrm{rank}(U) = 4$, at most two row vectors of $U$ can be represented by some linear combinations of the row vectors of $L$.

*The free-start second-preimage attack.*

S0. $\mathcal{A}$ computes the output $(H_i, G_i)$ for the given input $(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$. Let

$$\begin{pmatrix} W^* \\ X^* \\ Y^* \\ Z^* \end{pmatrix} = L \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}.$$

S1. $\mathcal{A}$ chooses $2^m$ random 4-tuples $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ such that

$$\begin{pmatrix} W^* \\ X^* \\ Y^* \\ Z^* \end{pmatrix} = L \begin{pmatrix} \tilde{H}_{i-1} \\ \tilde{G}_{i-1} \\ \tilde{M}_i^1 \\ \tilde{M}_i^2 \end{pmatrix}.$$

S2. For each $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$, $\mathcal{A}$ computes $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ with (1) and computes $\tilde{H}_i = E^{\mathrm{U}}_{\tilde{A}\|\tilde{B}}(\tilde{C}) \oplus \tilde{D}$.

In the above process, since at least one of $\tilde{A}$ and $\tilde{B}$ or both $\tilde{C}$ and $\tilde{D}$ are random, $\tilde{H}_i = E^{\mathrm{U}}_{\tilde{A}\|\tilde{B}}(\tilde{C}) \oplus \tilde{D}$ is also random. Thus, according to Proposition 1, $\mathcal{A}$ can find $\tilde{H}_i$ such that $H_i = \tilde{H}_i$ with probability about 0.63. The total complexity is about $2^m$.

*The free-start collision attack.* $\mathcal{A}$ chooses $2^{m/2}$ random 4-tuples $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ such that

$$L \begin{pmatrix} \tilde{H}_{i-1} \\ \tilde{G}_{i-1} \\ \tilde{M}_i^1 \\ \tilde{M}_i^2 \end{pmatrix}$$

is constant. Then, according to Proposition 2, $\mathcal{A}$ can find a collision of $f_{\mathrm{U}}$ with probability about 0.39. This collision is also a collision of $f_{\mathrm{L}}$. The total complexity is about $2^{m/2}$. □

**Lemma 2:** Let $f$ be a compression function in Definition 3. Suppose that $\mathrm{rank}(U) = 3$. Then, there exists a free-start collision attack on $f$ with the complexity at most about $2^{m/2}$. There also exists a free-start second-preimage attack on $f$ with the complexity at most about $2^m$.

(Proof) Case (a). Suppose that at most two row vectors of $L$ can be represented by some linear combinations of the row vectors of $U$.

*The free-start second-preimage attack.*

S0. $\mathcal{A}$ computes the output $(H_i, G_i)$ for the given input $(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$. Let

$$\begin{pmatrix} A^* \\ B^* \\ C^* \\ D^* \end{pmatrix} = U \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}.$$

S1. $\mathcal{A}$ computes $2^m$ 4-tuples $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ such that

$$\begin{pmatrix} A^* \\ B^* \\ C^* \\ D^* \end{pmatrix} = U \begin{pmatrix} \tilde{H}_{i-1} \\ \tilde{G}_{i-1} \\ \tilde{M}_i^1 \\ \tilde{M}_i^2 \end{pmatrix}.$$

S2. For each $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$, $\mathcal{A}$ computes $(\tilde{W}, \tilde{X}, \tilde{Y}, \tilde{Z})$ with (2) and computes $\tilde{G}_i = E^{\mathrm{L}}_{\tilde{W}\|\tilde{X}}(\tilde{Y}) \oplus \tilde{Z}$.

In the above process, since at least one of $\tilde{W}$ and $\tilde{X}$ or both $\tilde{Y}$ and $\tilde{Z}$ take all values in $\{0,1\}^m$, $E^{\mathrm{L}}_{\tilde{W}\|\tilde{X}}(\tilde{Y}) \oplus \tilde{Z}$ is random. Thus, according to Proposition 1, $\mathcal{A}$ can find $\tilde{G}_i$ such that $G_i = \tilde{G}_i$ with probability about 0.63. The total complexity is about $2^m$.

*The free-start collision attack.* $\mathcal{A}$ chooses $2^{m/2}$ random 4-tuples $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ such that

$$U \begin{pmatrix} \tilde{H}_{i-1} \\ \tilde{G}_{i-1} \\ \tilde{M}_i^1 \\ \tilde{M}_i^2 \end{pmatrix}$$

is constant. After that, it computes $\tilde{G}_i$ in the same way as in the S2 above. According to Proposition 2, $\mathcal{A}$ can find a collision of $f_{\mathrm{L}}$ with probability about 0.39. The total complexity is about $2^{m/2}$.

Case (b). Suppose that both $\boldsymbol{y}$ and $\boldsymbol{z}$ are represented by some linear combinations of the row vectors of $U$ and that either $\boldsymbol{w}$ or $\boldsymbol{x}$ cannot be represented by any linear combination of the row vectors of $U$. Then, the free-start second-preimage/collision attacks of Case (a) can be applied since at least one of $\tilde{W}$ and $\tilde{X}$ take all values in $\{0,1\}^m$ and $E^{\mathrm{L}}_{\tilde{W}\|\tilde{X}}(\tilde{Y}) \oplus \tilde{Z}$ is random. Their complexities are about $2^m$ and $2^{m/2}$, respectively.

Case (c). Suppose that $\boldsymbol{w}$, $\boldsymbol{x}$ and $\boldsymbol{y}$ are represented by some linear combinations of the row vectors of $U$ and that $\boldsymbol{z}$ cannot be represented by any linear combination of the row vectors of $U$.

*The free-start second-preimage attack.*

S0. $\mathcal{A}$ computes the output $(H_i, G_i)$ for the given input $(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$.
S1. $\mathcal{A}$ chooses $2^m$ random 4-tuples $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ (only three of them are randomly chosen since $\mathrm{rank}(U) = 3$) and finds $(A', B', C', D')$ such that $H_i = E^{\mathrm{U}}{}_{A'\|B'}(C') \oplus D'$.
S2. $\mathcal{A}$ computes $(W', X', Y')$ from $(A', B', C', D')$ and $H_i$. Then, he computes $Z' = E^{\mathrm{L}}{}_{W'\|X'}(Y') \oplus G_i$.
S3. $\mathcal{A}$ computes a second preimage $(H'_{i-1}, G'_{i-1}, M_i^1, M_i^2)$ from $(A', B', C', D')$, $Z'$ and $H_i$.

In the above process, $\mathcal{A}$ can find the second preimage with probability about 0.63. The complexity is about $2^m$.

*The free-start collision attack.*

S1. $\mathcal{A}$ chooses $2^{m/2}$ random 4-tuples $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ and finds a pair $(A', B', C', D')$ and $(A'', B'', C'', D'')$ which produce the same output of $f_{\mathrm{U}}$. Let $H_i$ be the output.
S2. $\mathcal{A}$ computes $(W', X', Y')$ and $(W'', X'', Y'')$ from $(A', B', C', D')$ and $(A'', B'', C'', D'')$ and $H_i$, respectively. Then, $\mathcal{A}$ chooses arbitrary $G_i$ and computes $Z' = E^{\mathrm{L}}{}_{W'\|X'}(Y') \oplus G_i$ and $Z'' = E^{\mathrm{L}}{}_{W''\|X''}(Y'') \oplus G_i$.
S3. $\mathcal{A}$ computes $(H'_{i-1}, G'_{i-1}, M^{1\prime}{}_i, M^{2\prime}{}_i)$ from $(A', B', C', D')$, $Z'$ and $H_i$, and $(H''_{i-1}, G''_{i-1}, M^{1\prime\prime}{}_i, M^{2\prime\prime}{}_i)$ from $(A'', B'', C'', D'')$, $Z''$ and $H_i$.

In the above process, $\mathcal{A}$ can find a collision with probability about 0.39. The complexity is about $2^{m/2}$.

Case (d). Suppose that $\boldsymbol{w}$, $\boldsymbol{x}$ and $\boldsymbol{z}$ are represented by some linear combinations of the row vectors of $U$ and that $\boldsymbol{y}$ cannot be represented by any linear combination of the row vectors of $U$.

*The free-start second-preimage attack.*

S0. $\mathcal{A}$ computes the output $(H_i, G_i)$ for the given input $(H_{i-1}, G_{i-1}, M_i^1, M_i^2)$.
S1. $\mathcal{A}$ chooses $2^m$ random 4-tuples $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ and finds $(A', B', C', D')$ such that $H_i = E^{\mathrm{U}}{}_{A'\|B'}(C') \oplus D'$.
S2. $\mathcal{A}$ computes $(W', X', Z')$ from $(A', B', C', D')$ and $H_i$. Then, he computes $Y' = E^{\mathrm{L}\,-1}{}_{W'\|X'}(Z' \oplus G_i)$.
S3. $\mathcal{A}$ computes a second preimage $(H'_{i-1}, G'_{i-1}, M^{1\prime}{}_i, M^{2\prime}{}_i)$ from $(A', B', C', D')$, $Y'$ and $H_i$.

In the above process, $\mathcal{A}$ can find the second preimage with probability about 0.63. The complexity is about $2^m$.

*The free-start collision attack.*

S1. $\mathcal{A}$ chooses $2^{m/2}$ random 4-tuples $(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ and finds a pair $(A', B', C', D')$ and $(A'', B'', C'', D'')$ which produce the same output of $f_{\mathrm{U}}$. Let $H_i$ be the output.
S2. $\mathcal{A}$ computes $(W', X', Z')$ and $(W'', X'', Z'')$ from $(A', B', C', D')$ and $(A'', B'', C'', D'')$ and $H_i$, respectively. Then, $\mathcal{A}$ chooses arbitrary $G_i$ and computes $Y' = E^{\mathrm{L}\,-1}{}_{W'\|X'}(Z' \oplus G_i)$ and $Y'' = E^{\mathrm{L}\,-1}{}_{W''\|X''}(Z'' \oplus G_i)$.
S3. $\mathcal{A}$ computes $(H'_{i-1}, G'_{i-1}, M^{1\prime}{}_i, M^{2\prime}{}_i)$ from $(A', B', C', D')$, $Y'$ and $H_i$, and $(H''_{i-1}, G''_{i-1}, M^{1\prime\prime}{}_i, M^{2\prime\prime}{}_i)$ from $(A'', B'', C'', D'')$, $Y''$ and $H_i$.

In the above process, $\mathcal{A}$ can find a collision with probability about 0.39. The complexity is about $2^{m/2}$.

Case (e). Suppose that all of the row vectors of $L$ are represented by some linear combinations of the row vectors of $U$. In this case, it is easy to find many $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ corresponding to a fixed $(A, B, C, D)$ and $(W, X, Y, Z)$. □

**Lemma 3:** Let $f$ be a compression function in Definition 3. Suppose that $\mathrm{rank}(U) \leq 2$. Then, there exists a free-start collision attack on $f$ with the complexity at most about $2^{m/2}$. There also exists a free-start second-preimage attack on $f$ with the complexity at most about $2^m$.

(Proof) If at most two of the row vectors of $L$ can be represented by some linear combinations of the row vectors of $U$, then the free-start second-preimage/collision attacks of Case (a) in Lemma 2 can be applied. Their complexities are about $2^m$ and $2^{m/2}$, respectively.

If three or more row vectors of $L$ can be represented by some linear combinations of the row vectors of $U$, then it is easy to find many $(\tilde{H}_{i-1}, \tilde{G}_{i-1}, \tilde{M}_i^1, \tilde{M}_i^2)$ corresponding to fixed $(A, B, C, D)$ and $(W, X, Y, Z)$ since $\mathrm{rank}(U) \leq 2$. □

## 5. Remarks

Let $f$ be a compression function in Definition 3 with $v = 0$ (parallel type). From the results by Satoh, Haga and Kurosawa [20] and the discussions so far, if any optimally collision-resistant hash function can be composed of $f$, then $f$ must be in one of the following two types:

T-I. Both $U$ and $L$ are "exceptional,"
T-II. $\mathrm{rank}(U) = \mathrm{rank}(L) = 3$, $\boldsymbol{c} \oplus \boldsymbol{d} = \lambda_1 \boldsymbol{a} \oplus \lambda_2 \boldsymbol{b}$ for some $\lambda_1, \lambda_2 \in \{0, 1\}$, $\boldsymbol{y} \oplus \boldsymbol{z} = \lambda_3 \boldsymbol{w} \oplus \lambda_4 \boldsymbol{x}$ for some $\lambda_3, \lambda_4 \in \{0, 1\}$, and the upper right $2 \times 2$ submatrices of $U$ and $L$ are both non-singular.

Here is an example of a compression function, with which it is impossible to construct an optimally collision-resistant hash function.

**Example 1:** Let $f_1$ be a compression function in Definition 3 such that

$$H_i = f_{1\mathrm{U}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E^{\mathrm{U}}{}_{M_i^1\|M_i^2}(H_{i-1}) \oplus H_{i-1},$$
$$G_i = f_{1\mathrm{L}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E^{\mathrm{L}}{}_{M_i^1\|M_i^2}(G_{i-1}) \oplus G_{i-1}.$$

Then,

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}$$

$$\begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}.$$

It is easy to see that $f_1$ is in T-II. Notice that $H_i$ does not depend on $G_{i-1}$ and that $G_i$ does not depend on $H_{i-1}$. Namely, the hash function $h_1$ composed of $f_1$ is simply a concatenation of two independent iterated hash functions:

$$h_1((H_0, G_0), M) = h_{1\mathrm{U}}(H_0, M) \| h_{1\mathrm{L}}(G_0, M),$$

where the compression functions of $h_{1\mathrm{U}}$ and $h_{1\mathrm{L}}$ are $f_{1\mathrm{U}}$ and $f_{1\mathrm{L}}$, respectively. Thus, we can find a collision with the time complexity $O(m2^{m/2})$ [10]. We can find a set of $O(2^{m/2})$ distinct messages which are mapped to the same output by $h_{1\mathrm{U}}$ with the time complexity $O(m2^{m/2})$ using Joux's multicollision attack. The set contains a pair of messages which are mapped to the same output by $h_{1\mathrm{L}}$.

On the other hand, this attack does not seem to work for the following compression functions $f_2$ and $f_3$: $f_2$ is in T-II and $f_3$ is in T-I.

**Example 2:** Let $f_2$ be a compression function in Definition 3 such that

$$\begin{aligned} H_i &= f_{2\mathrm{U}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) \\ &= E^{\mathrm{U}}{}_{M_i^1 \| M_i^2}(H_{i-1} \oplus G_{i-1}) \oplus H_{i-1} \oplus G_{i-1}, \\ G_i &= f_{2\mathrm{L}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E^{\mathrm{L}}{}_{M_i^1 \| M_i^2}(H_{i-1}) \oplus H_{i-1}. \end{aligned}$$

Then,

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}$$

$$\begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}.$$

**Example 3:** Let $f_3$ be a compression function in Definition 3 such that

$$\begin{aligned} H_i &= f_{3\mathrm{U}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E^{\mathrm{U}}{}_{M_i^1 \| M_i^2}(H_{i-1}) \oplus G_{i-1}, \\ G_i &= f_{3\mathrm{L}}(H_{i-1}, G_{i-1}, M_i^1, M_i^2) = E^{\mathrm{L}}{}_{M_i^1 \| M_i^2}(G_{i-1}) \oplus H_{i-1}. \end{aligned}$$

Then,

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}$$

$$\begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} H_{i-1} \\ G_{i-1} \\ M_i^1 \\ M_i^2 \end{pmatrix}.$$

It is an open question if optimally collision-resistant DBL hash functions are composed of $f_2$ or $f_3$.

## 6. Conclusion

In this article, we have analyzed the security of the DBL hash functions with the rate 1. Many of them are at most as secure as SBL hash functions composed of the same block ciphers. Furthermore, even if there exists optimally collision-resistant DBL hash functions among them, it cannot be implied only by the collision resistance of their compression functions.

Future work is to make it clear if there exist optimally collision-resistant DBL hash functions in T-I or T-II given in Sect. 5.

### References

[1] E. Biham and R. Chen, "Near-collisions of SHA-0," CRYPTO 2004 Proc., LNCS 3152, pp.290–305, 2004.
[2] J. Black, M. Cochran, and T. Shrimpton, "On the impossibility of highly efficient blockcipher-based hash functions," EUROCRYPT 2005 Proc., LNCS 3494, pp.526–541, 2005.
[3] B.O. Brachtl, D. Coppersmith, M.M. Hyden, S.M. Matyas, Jr., C.H.W. Meyer, J. Oseas, S. Pilpel, and M. Schilling, "Data authentication using modification detection codes based on a public one-way encryption function," U.S. Patent # 4,908,861, March 1990.
[4] I. Damgård, "A design principle for hash functions," CRYPTO'89 Proc., LNCS 435, pp.416–427, 1990.
[5] M. Girault, R. Cohen, and M. Campana, "A generalized birthday attack," EUROCRYPTO'88 Proc., LNCS 330, pp.129–156, 1988.
[6] M. Hattori, S. Hirose, and S. Yoshida, "Analysis of double block length hash functions," Proc. 9th IMA International Conference on Cryptography and Coding, LNCS 2898, pp.290–302, 2003.
[7] S. Hirose, "Provably secure double-block-length hash functions in a black-box model," Proc. 7th Internatinal Conference on Information Security and Cryptology (ICISC 2004), LNCS 3506, pp.330–342, 2005.
[8] S. Hirose, "Some plausible constructions of double-block-length hash functions," Preproceedings of the 13th Fast Software Encryption Workshop (FSE 2006), pp.231–246, 2006.
[9] W. Hohl, X. Lai, T. Meier, and C. Waldvogel, "Security of iterated hash functions based on block ciphers," CRYPTO'93 Proc., LNCS 773, pp.379–390, 1994.
[10] A. Joux, "Multicollisions in iterated hash functions, Application to cascaded constructions," CRYPTO 2004 Proc., LNCS 3152, pp.306–316, 2004.
[11] L. Knudsen and B. Preneel, "Hash functions based on block ciphers and quaternary codes," ASIACRYPT'96 Proc., LNCS 1163, pp.77–90, 1996.
[12] L. Knudsen and B. Preneel, "Fast and secure hashing based on codes," CRYPTO'97 Proc., LNCS 1294, pp.485–498, 1997.
[13] L. Knudsen and B. Preneel, "Construction of secure and fast hash functions using nonbinary error-correcting codes," IEEE Trans. Inf. Theory, vol.48, no.9, pp.2524–2539, 2002.
[14] L.R. Knudsen, X. Lai, and B. Preneel, "Attacks on fast double block length hash functions," J. Cryptol., vol.11, no.1, pp.59–72, 1998.
[15] X. Lai and J.L. Massey, "Hash function based on block ciphers," EUROCRYPT'92 Proc., LNCS 658, pp.55–70, 1993.
[16] S. Lucks, "A failure-friendly design principle for hash functions," ASIACRYPT 2005 Proc., LNCS 3788, pp.474–494, 2005.
[17] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[18] R.C. Merkle, "One way hash functions and DES," CRYPTO'89 Proc., LNCS 435, pp.428–446, 1990.
[19] M. Nandi, "Towards optimal double-length hash functions," Proc.

6th International Conference on Cryptology in India (INDOCRYPT 2005), LNCS 3797, pp.77–89, 2005.
[20] T. Satoh, M. Haga, and K. Kurosawa, "Towards secure and fast hash functions," IEICE Trans. Fundamentals, vol.E82-A, no.1, pp.55–62, Jan. 1999.
[21] X. Wang, Y.L. Yin, and H. Yu, "Finding collisions in the full SHA-1," CRYPTO 2005 Proc., LNCS 3621, pp.17–36, 2005.
[22] X. Wang and H. Yu, "How to break MD5 and other hash functions," EUROCRYPT 2005 Proc., LNCS 3494, pp.19–35, 2005.
[23] X. Wang, H. Yu, and Y.L. Yin, "Efficient collision search attacks on SHA-0," CRYPTO 2005 Proc., LNCS 3621, pp.1–16, 2005.

**Shoichi Hirose** received the B.E., M.E. and D.E. degrees in information science from Kyoto University, Kyoto, Japan, in 1988, 1990 and 1995, respectively. From 1990 to 1998, he was a research associate at Faculty of Engineering, Kyoto University. From 1998 to 2005, he was a lecturer at Graduate School of Informatics, Kyoto University. From 2005, he is an associate professor at Faculty of Engineering, The University of Fukui. His current interests include cryptography and information security. He received Young Engineer Award from IEICE in 1997. He is a member of IACR, ACM, IEEE and IPSJ.