Towards Optimally Secure Double Block Length Hash Functions with Rate 1*

Zheng Gong, Xuejia Lai and Kefei Chen
Department of Computer Science and Engineering
Shanghai Jiaotong University, China
neoyan@sjtu.edu.cn,{lai-xj,chen-kf}@cs.sjtu.edu.cn

Abstract

In this paper, the security of double block length hash functions with rate 1 which based on a block cipher with a block length of n-bit and a key length of $2n$-bit is reconsidered. First, two concrete attacks are designed to break Hirose's two examples which were left as an open problem. Next, attacks are presented on a general class of double block length hash functions with rate 1, which disclose there exist uncovered flaws in the former analysis by Satoh *et al.* and Hirose. Some refined conditions are proposed for ensuring this class of the rate-1 hash functions to be optimally secure. Finally, the security results are extended to a new class of double block length hash functions with rate 1.

Key words. Cryptanalysis, Block cipher, Double block length Hash function.

1 Introduction

Cryptographic hash function $H : \{0,1\}^* \rightarrow \{0,1\}^\ell$ is defined as an easily computable algorithm which uniformly maps an arbitrary-length message to a fixed-length output hash value. In practice, most of hash functions are either explicitly or implicitly composed from block ciphers. The advantages

*This paper is supported by NSFC under the grants 60573032, 90604036 and National 863 Projects 2006AA01Z422

of the block-cipher-based designs are that one can conveniently choose a widely accepted block cipher(i.e., DES, IDEA, AES, etc) to construct the round function, and also the latest cryptanalysis results on such block cipher can be used to avoid the potential weakness in the algorithm. Discussion of hash functions constructed from n-bit block ciphers is divided into *single block length*(SBL) and *double block length*(DBL) hash functions, where single and double are related to the output range of the block cipher used in the hash function. Assume that equal or greater than 2^{64} operations(encryption or decryption) are infeasible, the objective of SBL hash functions is to just provide *one-wayness* for cipher of block length near $n = 64$, while fail to *collision resistance* since a doubled 128-bit length range is required to resist the birthday paradox attack. The motivation for double block length is to combine two n-bit block ciphers to obtain a sufficient output range for collision resistance. One such algorithm is MDC-2, which was developed by Brachtl *et al.*[3] for use in combination with DES. It is believed that the complexities for (second) preimage and collision attacks on MDC-2 are about $2^{3n/2}$ and 2^n, respectively. A DBL hash function H is said to be *optimally secure*, if any adversary with non-negligible successful probability must spend the computation costs greater or equal to brute-force attacks, which requires the complexities of collision and (second) preimage attacks are no less than 2^{2n} and 2^n, respectively.

Although double block length can realize collision resistance, the objective of DBL hash functions is a decrease in speed. The *rate* of a block-cipher-based hash function is defined as the number of n-bit message blocks processed per encryption or decryption for the measurement of the efficiency. The rate of MDC-2 is only 1/2, which implies that MDC-2 is at least twice as slow as the underlying block cipher. To improve the efficiency, many DBL hash functions with rate 1 were proposed[4, 8, 16, 23]. Unfortunately, some reviews show the critical results that the proposed schemes with rate 1 unlikely achieve optimally secure. In [10], Knudsen *et al.* presented the attacks on a large class of DBL hash functions with rate 1 such that the key length is equal to the block length n-bit. In particular, the attacks break the proposed schemes in [4, 8, 16]. Still, many advanced block ciphers (i.e., AES, RC5, Blowfish, etc) support variants of key length motivates renewed interest in finding good ways to construct an DBL hash function as secure as MDC-2. Many instructive examples were proposed recently, i.e., [6, 12, 14, 15]. But all these schemes are less than rate-1, which means they are still not efficient. In [19], Satoh *et al.* presented the attacks on a general class of DBL hash functions with rate 1 where the key length is double to the

block length, which break the proposed scheme in [23]. In particular, Satoh *et al.* described a necessary condition for this general class of the rate-1 hash functions to be optimally secure. Recently, Hirose[7] gave a comment on Satoh *et al.*'s result [19] and it is shown that there exists a missed case in their analysis. Moreover, Hirose left two examples in this case as an open problem to make it clear whether they are optimally secure.

Our Contributions. Consider the security of double block length hash functions with rate 1 where the key length is double to the block length, our contributions are three-folds. First, we present two concrete attacks on Hirose's two examples which are left as an open problem in [7]. The attacks show the fact that the two schemes are not optimally collision resistant. Based on this negative result, then we investigate the security of a general class of DBL hash functions with rate 1 which is defined by Satoh *et al.*[19] to find whether there exists an optimally secure DBL hash function with rate 1. Some refined conditions for this class of DBL hash functions to be optimally secure are proposed after the analysis. Unfortunately, the results also show that Hirose's two example are failed to be optimally (second) preimage resistant. Finally, the security results are extended to a new class of DBL hash functions with rate 1 where one block cipher used in the round function has the key length is equal to the block length and the other is doubled. Prior to this paper, there is no rigorous analysis on the half-baked cases proposed by Satoh *et al.*[19] and Hirose[7] to decide whether they are as secure as MDC-2.

Organization. The remainder of this paper is organized as follows. In Section 2, some definitions and the former results on DBL hash functions with rate 1 are reviewed. In Section 3, first two concrete attacks are presented on Hirose's two examples. Then attacks are described on a general class of DBL hash functions with rate 1. Section 4 describes an extended result on a new class of DBL hash functions with rate 1. The conclusion is given in the last section.

2 Preliminaries

In this section, the notions and definitions are reviewed for the following analysis. Let the symbol $\oplus$ be the bitwise exclusive OR. For binary sequences a and b, $a||b$ denotes their concatenation. Let IV be the initial value. For double block length hash function, the i-th input message M_i

can be looked as a concatenation of the $2n$-bit length blocks such that $M^i = m_1^i||m_2^i||\cdots||m_t^i$, where $t = |M^i|/2n$ and $m_j^i = m_{j,1}^i||m_{j,1}^i, j \in \{0,t\}$. The function $Rank(\cdot)$ returns the rank of an input matrix. The same terminology and abbreviations in different definitions are the same meaning, except there are special claims in the context.

2.1 Block-Cipher-Based Hash Functions

Let κ, n, ℓ be numbers. A *block cipher* is a keyed function $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$. For each $k \in \{0,1\}^\kappa$, the function $E_k(\cdot) = E(k,\cdot)$ denotes a permutation on $\{0,1\}^n$. If E is a block cipher then E^{-1} is its inverse, where $E_k^{-1}(y) = x$ such that $E_k(x) = y$. Let $\texttt{Bloc}(\kappa, n)$ be the family of all block ciphers $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$. To avoid trivial extension attacks, we assume that any block cipher $E \in \texttt{Bloc}$ has no *fixed-point* such that $E_k(x) = k$ or x or $E_k^{-1}(y) = y$ or k and length strengthening technique[5, 13] is explicitly implemented in the constructions. A *block-cipher-based* hash function is a hash function $H : \{0,1\}^* \to \{0,1\}^\ell$ by implementing $E \in \texttt{Bloc}(\kappa, n)$ in the round function of H. If $\ell = n$, then H is called a single block length(SBL) hash function, i.e., the PGV hash functions[17]. If $\ell = 2n$, then H is called a double block length(DBL) hash function, i.e., MDC-2[3], Parallel-DM[4], QG-I, and LOKI-DBH[10]. The *rate* is used to measure the efficiency of a block-cipher-based hash function, which is defined as follows.

Definition 1 *Let $H : \{0,1\}^* \to \{0,1\}^\ell$ be a hash function and $E \in \texttt{Bloc}(\kappa, n)$ is a block cipher used in the round function of H. If the round function performs T times encryption or decryption of E to process totally ℓ bits long message block, the rate of the hash function H equals $\frac{\ell}{T \cdot n}$.*

2.2 Security Definitions

Since data integrity is a fundamental component for the real-life cryptographic applications(i.e., data or entity authentication, public-key encryption and digital signature), a *secure* hash function must resist the following attacks to protect the integrity.

Attacks on hash functions. For block-cipher-based hash functions, there are three standard attacks which are called collision attack, preimage attack and second preimage attack. A limitation is that the standard attacks only consider the situation that initial value IV is fixed.

Definition 2 *Let $H : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}$ be a family of hash functions where $\mathcal{K} \in \{0,1\}^\kappa, \mathcal{Y} \in \{0,1\}^\ell$. Let M be a message belongs to message space $\mathcal{M} \in \{0,1\}^*$. By considering whether IV is fixed or not, three standard attacks and three extended attacks are defined as follows.*

1. *The preimage attack (Pre) is that given IV and h, find a message M such that $h = H(IV, M)$.*
2. *The free-start preimage attack (fPre) is that given IV and h, find IV' and M such that $h = H(IV', M)$.*
3. *The second preimage attack (Sec) is that given IV and a message M, find another message $M' \neq M$ such that $H(IV, M) = H(IV, M')$.*
4. *The free-start second preimage attack (fSec) is that given IV and a message M, find IV' and another message $M' \neq M$ such that $H(IV, M) = H(IV', M')$.*
5. *The collision attack (Coll) is that given an initial value IV, find $M \neq M'$ such that $H(IV, M) = H(IV, M')$.*
6. *The free-start collision attack (fColl) is that find $IV \neq IV'$ and messages M, M' such that $H(IV, M) = H(IV', M')$.*

The above attacks are from [9]. Similar definitions can be found in [11]. Compare with the standard attacks, the extended attacks are also meaningful since they would be a complete examination on minimizing potential flaws in a class of hash function. To rigorously analyze the security of a hash function at the presents of adversary, a widely accepted security model will be reviewed before the analysis.

Ideal Cipher Model. Ideal cipher model is a well-known model for the security analysis of block-cipher-based hash functions, which is dating back to Shannon [20] and has been frequently used for the security analysis of various hash functions[1, 11, 17]. Let $H : \{0,1\}^* \to \{0,1\}^\ell$ be a hash function and $E \in \texttt{Bloc}(\kappa, n)$ be a block cipher used in the round function of H. An adversary is given access to the encryption oracle E and the decryption oracle E^{-1}. The i-th query-response is defined as a four-tuple $(\sigma_i, k_i, x_i, y_i)$ where $k_i \in \{0,1\}^\kappa, x_i, y_i \in \{0,1\}^n$. If $\sigma_i = 1$ then the adversary queries (k_i, x_i) and gets response $y_i = E_{k_i}(x_i)$, otherwise he queries (k_i, y_i)

and gets response $x_i = E_{k_i}^{-1}(y_i)$. Since $E_k(\cdot)$ is a permutation on $\{0,1\}^n$, it holds that

$$Pr[E_{k_i}(x_i) = y_i] = Pr[E_{k_i}^{-1}(y_i) = x_i] = \frac{1}{n}.$$

In the ideal cipher model, one measures the complexity of an attack, on which finding a collision, preimage or second preimage, is based on the total number of encryptions and decryptions the adversary queries. Generally, all repetition queries will be ignored, i.e., if adversary asks a query $E_k(x)$ and this returns y, then he does not repeat the query or ask the inverse $E_k^{-1}(y)$. Such trivial queries does not help anything at the view of adversary. The block cipher in this model is variously named "Shannon oracle model", "Black-box model", or "Ideal cipher model". Since the last name is more often called, it will be used throughout the paper.

Recently, Black[2] exhibited a negative result on the ideal cipher model that there exists a block cipher based hash function that is provably secure in the ideal cipher model but trivially insecure when instantiated by any block cipher. The scheme is quite artificial and unnatural. Thus far, as in the ideal cipher model analog, no block cipher based hash function proven secure has been broken after instantiation. Like schemes in the random oracle model, a hash function is proven secure in the ideal cipher model is still reliable, unless one uses the unnatural design for the goal from the beginning.

2.3 Results on Fast DBL Hash Functions

By assuming the key length κ of block cipher $E \in \texttt{Bloc}(\kappa, n)$ used in round function is equal to the block length n-bit, Knudsen *et al.* [10] presented attacks on a class of DBL hash functions with rate 1. The general form of this class is described as follows.

$$\begin{cases} h_i = E_A(B) \oplus C, \\ g_i = E_X(Y) \oplus Z. \end{cases} \tag{1}$$

For all hash functions of rate 1 defined by (1)(denoted by FDBL-I), (A, B, C) are linear combinations of the n-bit vectors $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$, (X, Y, Z)

are linear combinations of the n-bit vectors $(h_i, h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$.

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \underbrace{\begin{pmatrix} L_l & L_r \end{pmatrix}}_{L} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}, \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \underbrace{\begin{pmatrix} R_l & R_r \end{pmatrix}}_{R} \cdot \begin{pmatrix} h_i \\ h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}. \tag{2}$$

If h_i and g_i can be computed independently, the hash function is called *parallel*, otherwise is called *serial*. Knudsen *et al.*[10] proved that all hash functions in FDBL-I are not optimally secure.

Theorem 1 *For the rate-1 iterated hash function with the form* (1)*(FDBL-I), where (at least) one of* $h_i \in \{0,1\}^n$ *and* $g_i \in \{0,1\}^n$ *in the hash function has the form of a (secure) single block length hash function, there exist second preimage attacks with complexities of about* 3×2^n*, primage attacks with complexities of about* 4×2^n*, and collision attacks with complexities of about* $3 \times 2^{n/2}$.

In AES algorithm, key length can be 128,196,256-bit while block length is 128-bit. This property motivates interest in finding good ways to turn a block cipher into an optimally secure fast DBL hash function whose block length and key length are not limited to the same n-bit. By considering the block cipher $E \in \texttt{Bloc}(\kappa, n)$ where $\kappa = 2n$, Satoh *et al.*[19] proposed a new family of DBL hash functions with rate 1 defined by the general form as follows.

$$\begin{cases} h_i = E_{A||B}(C) \oplus D, \\ g_i = E_{W||X}(Y) \oplus Z. \end{cases} \tag{3}$$

For all hash functions of rate 1 defined by (3) (denoted by FDBL-II), both (A, B, C, D) and (W, X, Y, Z) are linear combinations of the n-bit vectors $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$. Those linear combinations can be represented as

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \underbrace{\begin{pmatrix} L_l & L_r \end{pmatrix}}_{L} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}, \begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \underbrace{\begin{pmatrix} R_l & R_r \end{pmatrix}}_{R} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}, \tag{4}$$

where L_l and L_r denote 4×2 binary submatrices of L. Let L_r^i denote the 3×2 submatrices of L_r such that the i-th row of L_r are deleted, respectively. Similarly, L_l^i denote the 3×2 submatrices of L_l such that the i-th row of L_l are deleted, respectively. Matrix L is said to be *exceptional* if $Rank(L) = 4$ and $Rank(L_r^3) = Rank(L_r^4) = 2$[19].

In [19], Satoh *et al.* stated attacks on this kind of DBL hash functions whose round functions do not satisfy the property "exceptional".

Theorem 2 *For the rate-1 iterated hash function with the form* (3)*(FDBL-II), if L is not exceptional, there exist the preimage, the second preimage and the collision attacks with complexities of about* 4×2^n, 3×2^n *and* $3 \times 2^{n/2}$, *respectively.*

In particular, Satoh *et al.*[19] showed attacks on a subclass of DBL hash functions with rate 1 in FDBL-II.

Theorem 3 *For the rate-1 double block length hash functions in FDBL-II with the round function h:*

$$\begin{cases} h_i = E_{A||B}(C) \oplus D, \\ g_i = E_{A||B}(C) \oplus F. \end{cases} \tag{5}$$

where (A, B, C, D, F) *is linear combinations of* $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$ *and* $E \in \texttt{Bloc}(2n, n)$. *Then, there exist (second) preimage attacks with complexities of about* 2×2^n, *and collision attacks with complexities of about* $2 \times 2^{n/2}$.

The rate 1 hash functions defined by (5) can be looked as one subclass of FDBL-II, where $W = A, X = B$ and $Y = C$.

In [7], Hirose gave a comment on the analysis by Satoh *et al.*[19]. The comment shows there exist the rate-1 DBL hash functions whose round functions do not satisfy the property "exceptional" but still no meaningful attacks are found. For convincing of this result, an example (denoted by HDBL-1) was proposed in [7] as follows.

HDBL-1: Let HDBL-1:$\{0,1\}^* \to \{0,1\}^{2n}$ be a double block length hash function and $E \in \texttt{Bloc}(2n, n)$ is the block cipher used in the round function of H. The round function has the following:

$$\begin{cases} h_i = E_{m_{i,1}||m_{i,2}}(h_{i-1} \oplus g_{i-1}) \oplus h_{i-1} \oplus g_{i-1}, \\ g_i = E_{m_{i,1}||m_{i,2}}(h_{i-1}) \oplus h_{i-1}. \end{cases} \tag{6}$$

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}}_{L} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_{i,1} \\ m_{i,2} \end{pmatrix}, \begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}}_{R} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_{i,1} \\ m_{i,2} \end{pmatrix} \quad (7)$$

Furthermore, an exceptional example (denoted by HDBL-2) was also proposed in [7].

HDBL-2: Let HDBL-2:$\{0,1\}^* \to \{0,1\}^{2n}$ be a double block length hash function and $E \in \texttt{Bloc}(2n, n)$ is the block cipher used in the round function of H. The round function has the following:

$$\begin{cases} h_i = E_{m_{i,1}||m_{i,2}}(h_{i-1}) \oplus g_{i-1}, \\ g_i = E_{m_{i,1}||m_{i,2}}(g_{i-1}) \oplus h_{i-1}. \end{cases} \quad (8)$$

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}}_{L} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_{i,1} \\ m_{i,2} \end{pmatrix}, \begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}}_{R} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_{i,1} \\ m_{i,2} \end{pmatrix} \quad (9)$$

Both HDBL-1 and HDBL-2 are the instances of FDBL-II. Based on the results given by Knudsen *et al.*[10] and Satoh *et al.*[19], Hirose[7] revised the conditions for the rate-1 hash functions in FDBL-II which are possibly to be optimally collision resistant.

Definition 3 *For any rate-1 iterated hash function in FDBL-II, if it is optimally collision resistant, then it must be in one of the two types:*

1. *Both L and R are exceptional,*
2. *$Rank(L) = Rank(R) = 3$, $c \oplus d = \lambda_1 a \oplus \lambda_2 b$ and $y \oplus z = \lambda_3 w \oplus \lambda_4 x$, for some $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \{0,1\}$, and the upper right 2×2 submatrices of L and R are both non-singular.*

In [7], Hirose claimed that the above conditions are not sufficient but just necessary for the property of optimal collision resistance. It was left as an open problem if the two plausible examples HDBL-1 and HDBL-2 are really optimally secure.

3 Security Analysis of FDBL-II

Here the security of the rate-1 hash functions in FDBL-II is reconsidered. A synthetic analysis is presented which exploits the fact that the former results[7, 19] on the security of FDBL-II are not exact. In particular, two concrete attacks are presented to disclose that both HDBL-1 and HDBL-2 are failed to be optimally collision resistant.

3.1 Attacks on Hirose's Two Examples

In [19], Satoh *et al.* suggested that any rate-1 hash function in FDBL-II will not to be optimally secure if its round function does not satisfy the *exceptional* property. Towards this approach, Hirose[7] gave a comment on Satoh *et al.*'s result, and said there exist optimally secure hash functions in FDBL-II whose round functions do not satisfy the exceptional property. Moreover, Hirose proposed two two rate-1 hash functions in FDBL-II (HDBL-1 and HDBL-2, described in Section 2.4) which are *plausible* secure. HDBL-1 satisfies the exceptional property while HDBL-2 does not(Both of them satisfy Hirose's necessary conditions in Definition 3). In this section, two concrete attacks are presented on these two examples which were left as an open problem. First, some definitions are given for the analysis. Let $E(\cdot) \in \texttt{Bloc}(2n, n)$ be an encryption function and $E^{-1}(\cdot)$ is its inverse. Let $M^i = m_1^i||m_2^i||\cdots||m_t^i$ be the i-th input message where the $2n$-bit length block $m_j^i = m_{j,1}^i||m_{j,2}^i, j \in \{1, t\}$. Let IV be the initial value and $h_0||g_0 = IV$. $\mathcal{A}$ denotes the adversary in the ideal cipher model.

Theorem 4 *Let HDBL-1 be a hash function defined by the form* (6)*,*

$$\begin{cases} h_i = E_{m_{i,1}||m_{i,2}}(h_{i-1} \oplus g_{i-1}) \oplus h_{i-1} \oplus g_{i-1}, \\ g_i = E_{m_{i,1}||m_{i,2}}(h_{i-1}) \oplus h_{i-1}, \end{cases}$$

then there exists a collision attack on the hash function with complexity about $4 \times 2^{n/2}$*.*

Proof. By using the idea of the *fixed-point* attack, a collision attack on the HDBL-1 hash function can be constructed in the following steps.

1. $\mathcal{A}$ chooses a message $M = m_1||m_2||\cdots||m_{i-2}$ and a block m_i.

2. For $j = 1, 2, \cdots, 2^{n/2}$, $\mathcal{A}$ processes:
   (a) uniformly and randomly chooses a block m_{i-1}^j,
   (b) computes $(h_{i-1}^j, g_{i-1}^j) \leftarrow$HDBL-1$(IV, M||m_{i-1}^j)$,
   (c) updates the set $S_j = S_{j-1} \cup \{m_{i-1}^j, h_{i-1}^j, g_{i-1}^j, h_i^j\}$. The set $S_{2^{n/2}}$ is the complete view of $\mathcal{A}$.
   (d) checks if there exist $h_{i-1}^j = h_{i-1}^l$ and $g_{i-1}^j = g_{i-1}^l$ where $l < j$. If true $\mathcal{A}$ returns $(M||m_{i-1}^j, M||m_{i-1}^l)$ as the collision pairs and aborts.
3. For $j = 1, 2, \cdots, 2^{n/2}$, $\mathcal{A}$ checks if $\{m_{i-1}^j, h_{i-1}^j, g_{i-1}^j, h_i^j\} \in S_{2^{n/2}}$ satisfies the following equations

$$\begin{cases} h_{i-1}^j = E_{m_i}(h_{i-1}^j \oplus g_{i-1}^j) \oplus h_{i-1}^j \oplus g_{i-1}^j, \\ g_{i-1}^j = E_{m_i}(h_{i-1}^j) \oplus h_{i-1}^j. \end{cases} \tag{10}$$

   If true $\mathcal{A}$ obtains $\{m_{i-1}^j, h_{i-1}^j, g_{i-1}^j, h_i^j\} \in S_{2^{n/2}}$ and breaks the loop. If all $\{m_{i-1}^j, h_{i-1}^j, g_{i-1}^j, h_i^j\} \in S_{2^{n/2}}$ are failed, then $\mathcal{A}$ returns false and aborts.
4. If $\mathcal{A}$ does not abort after the above steps, $\mathcal{A}$ returns a fourth-tuple $(m_{i-1}^j, m_i, h_{i-1}^j, g_{i-1}^j)$.

The attack will be succeeded in polynomial time with a non-negligible probability. If $\mathcal{A}$ aborts in Step 2, then there should be a collision pairs $(M||m_{i-1}, M||m'_{i-1}) \in S_{2^{n/2}}$ such that

$$\text{HDBL-1}(IV, M||m_{i-1}^j) = \text{HDBL-1}(IV, M||m_{i-1}^l).$$

If $\mathcal{A}$ does not abort in Step 2, then all $(h_{i-1}^j, g_{i-1}^j) \in S_{2^{n/2}}$ are uniformly distributed. Since the equations (10) can be combined as

$$h_{i-1}^j = E_{m_i}(h_{i-1}^j \oplus g_{i-1}^j) \oplus E_{m_i}(h_{i-1}^j),$$

due to the birthday paradox, there exists $\{m_{i-1}^j, m_i, h_{i-1}^j, g_{i-1}^j, h_i^j\} \in S_{2^{n/2}}$ which satisfies the above equation with a non-negligible probability. Since HDBL-1$(h_{i-1}^j||g_{i-1}^j, m_i) = (h_{i-1}^j, g_{i-1}^j)$, a collision pairs can be derived from the fixed-point such that

$$\text{HDBL-1}(IV, M||m_{i-1}^j) = \text{HDBL-1}(IV, M||m_{i-1}^j||m_i).$$

It is easy to see that both Step 2 and 3 require $2 \times O(2^{n/2})$ operations. Thus the total complexity of the attack is $4 \times O(2^{n/2})$. So the theorem holds. □

Similar to HDBL-1, a collision attack can also be found in the HDBL-2 hash function. The attack is described in the following theorem.

Theorem 5 *Let HDBL-2 be a hash function defined by the form* (8),

$$\begin{cases} h_i = E_{m_{i,1}||m_{i,2}}(h_{i-1}) \oplus g_{i-1}, \\ g_i = E_{m_{i,1}||m_{i,2}}(g_{i-1}) \oplus h_{i-1}. \end{cases}$$

then there exists a collision attack on the hash function with complexity about $4 \times 2^{n/2}$.

Proof. By using the method of the *meet-in-the-middle* attack, an adversary $\mathcal{A}$ can find a collision in HDBL-2 from the following steps.

1. $\mathcal{A}$ chooses a message $M = m_1||m_2||\cdots||m_{i-2}$, then computes $(h_{i-2}, g_{i-2}) \leftarrow$ HDBL-2(IV, M).
2. For $j = 1, 2, \cdots, 2^{n/2}$, $\mathcal{A}$ processes:
   (a) uniformly and randomly chooses a block m_{i-1}^j,
   (b) if $E_{m_{i-1}^j}(h_{i-2}) \oplus g_{i-2} = E_{m_{i-1}^j}(g_{i-2}) \oplus h_{i-2}$ which implies $h_{i-1} = g_{i-1} = E_{m_{i-1}^j}(g_{i-2}) \oplus h_{i-2}$, then obtains $(m_{i-1}^j, h_{i-1}, g_{i-1})$ and breaks the loop. Else $\mathcal{A}$ repeats the procedure.
   (c) If all m_{i-1}^j are failed, $\mathcal{A}$ returns false and aborts.
3. With the received values $(m_{i-1}^j, h_{i-1}, g_{i-1})$ in Step 2, $\mathcal{A}$ randomly chooses two blocks m_i, m_i', and checks if $E_{m_i}(h_{i-1}) \oplus g_{i-1} = E_{m_i'}(g_{i-1}) \oplus h_{i-1}$ holds. If the result is false, $\mathcal{A}$ makes different choices of (m_i, m_i') and repeats the check.
4. $\mathcal{A}$ returns a triple-tuple (m_{i-1}^j, m_i, m_i') after the above steps. A collision can be easily derived from the return value such that

$$\text{HDBL-2}(IV, M||m_{i-1}^j||m_i) = \text{HDBL-2}(M||m_{i-1}^j||m_i').$$

Due to the birthday paradox, Step 2 requires $2 \times O(2^{n/2})$ for finding m_{i-1}^j satisfies the condition with a non-negligible probability. The same goes to Step 3 for finding the blocks (m_i, m_i'). Thus the total complexity of the attack is about $4 \times O(2^{n/2})$. So the theorem holds. □

Since HDBL-1 satisfies the second condition in Definition 3, and HDBL-2 satisfies the exceptional property, which are the two conditions given by Hirose[7], the two concrete attacks disclose there exist uncovered flaws in the former security results on the rate-1 hash functions in FDBL-II which are defined by Satoh *et al.*[19] and Hirose[7].

3.2 The Exact Security of FDBL-II

In this section, the exact conditions for the rate-1 hash functions in FDBL-II to be optimally secure are analyzed. For ease of the reader, the general form of FDBL-II is recalled here.

$$\begin{cases} h_i = E_{A||B}(C) \oplus D, \\ g_i = E_{W||X}(Y) \oplus Z. \end{cases}$$

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \underbrace{\begin{pmatrix} L_l & L_r \end{pmatrix}}_{L} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}, \begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \underbrace{\begin{pmatrix} R_l & R_r \end{pmatrix}}_{R} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}.$$

By using the similar methods for the general attacks on the rate-1 hash functions in FDBL-I[10], the general attacks on FDBL-II are described in the following theorem.

Theorem 6 *For any hash function H in FDBL-II with the form (3), if T operations are required to find a block $m_i = m_{i,1}||m_{i,2}$ for any given value of (h_{i-1}, g_{i-1}), such that the resulting four-tuple $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$ yields the fixed value for h_i (or g_i or $h_i \oplus g_i$), then there exist collision, preimage, and second preimage attacks on the hash function with complexities $(T+3) \times 2^{n/2}$, $(T+3) \times 2^n$, and $(T+3) \times 2^n$, respectively.*

Proof. An attacker $\mathcal{A}$ starts the attacks by choosing arbitrary message $M = m_1||m_2||\cdots||m_{i-2}$, and by computing the values of (h_{i-2}, g_{i-2}) iteratively from the initial value $IV = h_0||g_0$. The initial operations for the values of (h_{i-2}, g_{i-2}) can be ignored if $i \ll 2^{n/2}$.

For (second) preimage attacks, $\mathcal{A}$ searches for two blocks m_{i-1} and m_i such that the fixed hash value (h_i, g_i) is hit. First, $\mathcal{A}$ computes the pair (h_{i-1}, g_{i-1}) from the given values (h_{i-2}, g_{i-2}) and $(m_{i-1,1}, m_{i-1,2})$. Secondly, $\mathcal{A}$ finds a block $(m_{i,1}, m_{i,2})$ such that the resulting four-tuple $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$ yields the fixed value for h_i(or g_i or $h_i \oplus g_i$). This step costs T times of encryption or decryption. Finally $\mathcal{A}$ computes the value of g_i(or h_i) from the tuple $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$. If the value does not hit, $\mathcal{A}$ will repeat the above steps at most 2^n times. Due to the pigeonhole principle, the probability of finding the preimage in the above procedure is non-negligible. The total complexity of these (second) preimage attacks is about $(T+3) \times 2^n$.

For collision attacks, $\mathcal{A}$ searches for a pair of the blocks (m_{i-1}, m_i) and (m'_{i-1}, m'_i) which yield the same hash value (h_i, g_i). First, $\mathcal{A}$ chooses a value of h_i. Then $\mathcal{A}$ proceeds $2^{n/2}$ times in the same way as the preimage attack. Due to the birthday paradox, the probability of finding the collision in the above procedure is non-negligible. The total complexity of these collision attacks is about $(T+3) \times 2^{n/2}$. So the theorem holds. □

In [7], a comment is proved that the attacks given by Satoh *et al.*[19] do not work on some hash functions as is expected even the underlying round function does not satisfy the exceptional property, i.e., the counter-example HDBL-1. Let (a, b, c, d) be the values of (A, B, C, D) used in the computations of h_i. In [19], the attacker chooses random triple (a, b, c) such that $c = \alpha \cdot a \oplus \beta \cdot b$ and computes $d = E_{a||b}(c) \oplus h_i$. Hirose said if $c = \alpha \cdot a \oplus \beta b \oplus d$, the attacker cannot compute d by $E_{a||b}(c) \oplus h_i$. Therefore, besides both L and R are exceptional, a new condition for the rate-1 hash functions in FDBL-II to be optimally secure is defined by Hirose [7] as the second condition described in Definition 3. Due to the two concrete attacks defined in Section 3.2, HDBL-1 and HDBL-2 are two counter-example of the two conditions given by Hirose[7]. Moreover, Since HDBL-2 is an instance of FDBL-II with the exceptional property, it means that the exceptional property does not directly imply the optimal security. Thus the result given by Satoh *et al.*[19] is not precise too. To ensure what conditions should be imposed on a hash function to achieve the optimal security, the security of the rate-1 hash functions in FDBL-II is reconsidered by the following attacks.

First, the attacks break the optimal collision and the (second) preimage resistances are described as follows.

Lemma 1 *For any hash function H in FDBL-II with the form (3), if the rank of L(or R) is less than three, then there exist collision, preimage, and*

second preimage attacks on the hash function with complexities of about $4 \times 2^{n/2}$, 3×2^n, *and* 3×2^n, *respectively.*

Proof. Consider the general form of FDBL-II. Since the rank of L(or R) is at most two and h_i depends on a subspace of $(m_{i,1}, m_{i,2}, h_{i-1}, g_{i-1})$, it follows that an attacker can has at least one dimensional of freedom to find the values of $m_{i,1}$(or $m_{i,2}$ or $m_{i,1} \oplus m_{i,2}$) yielding the given hash value (h_i, g_i). Based on the attacks defined by Theorem 6, it is easily to prove that $T \simeq 0$ in the (second) preimage attack, and $T \simeq 1$ in the collision attack. □

Lemma 2 *For any hash function* H *in FDBL-II with the form (3), if the rank of* L_r^3*(or* L_r^4 *or* R_r^3 *or* R_r^4*) is less than two, then there exist collision, preimage, and second preimage attacks on the hash function with complexities of about* $4 \times 2^{n/2}$, 3×2^n, *and* 3×2^n, *respectively.*

Proof. Consider the general form of FDBL-II. If either L_r^3 or L_r^4 is less than two, then the key $A||B$ of $E_{A||B}(C)$ depends on one dimensional of $(m_{i,1}, m_{i,2})$(or $m_{i,1} \oplus m_{i,2}$). Let (a, b, c, d) be the values of (A, B, C, D) used in the computations of h_i. By computing $d = E_{a||b}(c) \oplus h_i$(in case of L_r^4 is less than two) or $c = E_{a||b}^{-1}(d \oplus h_i)$(in case of L_r^3 is less than two), an attacker can decide the value of $m_{i,1}$(or $m_{i,2}$) from the hash values of $(h_{i-1}, g_{i-1}, h_i, g_i)$. Based on the attacks defined by Theorem 6, it is easily to prove that $T \simeq 0$ in the (second) preimage attack, and $T \simeq 1$ in the collision attack. Same result holds if either R_r^3 or R_r^4 is less than two. □

Then the attacks that break the optimal collision resistance were described as follows.

Theorem 7 *For any hash function* H *in FDBL-II with the form (3), if* $D \oplus h_{i-1} \neq 0$ *and* $D \oplus h_{i-1} \neq C$, *and* $Z \oplus g_{i-1} \neq 0$ *and* $Z \oplus g_{i-1} \neq Y$, *then there exists a collision attack on the hash function with complexity of about* $4 \times 2^{n/2}$.

Proof. Consider the general form of FDBL-II. An attacker $\mathcal{A}$ start the attacks by choosing arbitrary messages $M = m_1||m_2|| \cdots ||m_{t-2}$ and a block m_t, and by computing the values of (h_{t-2}, g_{t-2}) iteratively from the given initial value $IV = h_0||g_0$. For $j = 1, 2, \cdots, 2^{n/2}$, $\mathcal{A}$ uniformly and randomly selects the value of m_{t-1}^j, computes (h_{t-1}^j, g_{t-1}^j) from $(m_{t-1}^j, h_{t-2}, g_{t-2})$ and

updates the set $S_j = S_{j-1} \cup m_{t-1}^j, h_{t-1}^j, g_{t-1}^j$. Thus $S_{2^{n/2}}$ is the complete view of $\mathcal{A}$ after $2^{n/2}$ times. Since $D \oplus h_{i-1} \neq 0$ and $D \oplus h_{i-1} \neq C$, and $Z \oplus g_{i-1} \neq 0$ and $Z \oplus g_{i-1} \neq Y$, one can construct the following equations from the general form of FDBL-II.

$$\begin{cases} h_{i-1} = E_{A||B}(C) \oplus D, \\ g_{i-1} = E_{W||X}(Y) \oplus Z. \end{cases}$$

$\mathcal{A}$ searches the set $S^{2^{n/2}}$ to find (h_{i-1}, g_{i-1}) satisfy the above equations on the block m_t. Since $|h_i| = |g_i| = n$, due to the birthday paradox, the probability that such values can be found in the set $S^{2^{n/2}}$ is non-negligible probability. □

The attack on HDBL-1 is an instance of Theorem 7.

Theorem 8 *For any hash function H in FDBL-II with the form (3), if $h_{i-1} = g_{i-1}$ implies $h_i = g_i$, then there exists a collision attack on the hash function with complexity of about $4 \times 2^{n/2}$.*

Proof. Consider the general form of FDBL-II. An attacker $\mathcal{A}$ start the attacks by choosing arbitrary messages $M = m_1||m_2|| \cdots ||m_{t-2}$, and by computing the values of (h_{t-2}, g_{t-2}) iteratively from the given initial value $IV = h_0||g_0$. With the values of (h_{t-2}, g_{t-2}), $\mathcal{A}$ proceeds $2^{n/2}$ times to find a block m_{t-1} which satisfies $E_{a||b}(c) \oplus d = E_{w||x}(y) \oplus z$. Then $\mathcal{A}$ proceeds $2^{n/2}$ times to find two blocks (m_t, m_t') where $E_{a||b}(c) \oplus d = E_{a'||b'}(c') \oplus d'$. It is easily to prove that $H(IV, M||m_{t-1}||m_t) = H(IV, M||m_{t-1}||m_t')$. The total complexity of the above procedure is $4 \times 2^{n/2}$. □

The attack on HDBL-2 is an instance of Theorem 8.

Then the attacks that break optimal (second) preimage resistance were described as follows.

Theorem 9 *For any hash function H in FDBL-II with the form (3), if the rank of L_l^3 (or L_l^4 or R_l^3 or R_l^4) is less than two, then there exists a (second) preimage attack on the hash function with complexity of about $2 \times 2^{3n/2}$.*

Proof. Consider the general form of FDBL-II. If either L_l^3 or L_l^4 is less than two, then the key $A||B$ of $E_{A||B}(C)$ depends on one dimensional of

(h_{i-1}, g_{i-1})(or $h_{i-1} \oplus g_{i-1}$). Let (a, b, c, d) be the values of (A, B, C, D) used in the computations of h_i. By computing $d = E_{a||b}(c) \oplus h_i$(in case of L_l^4 is less than two) or $c = E_{a||b}^{-1}(d \oplus h_i)$(in case of L_l^3 is less than two).

An attacker $\mathcal{A}$ start the attacks by choosing arbitrary messages $M = m_1||m_2||\cdots||m_{i-2}$, and by computing the values of (h_{i-2}, g_{i-2}) iteratively from the given initial value $IV = h_0||g_0$.

1. For $j = 1, 2, \cdots, 2^{n/2}$, $\mathcal{A}$ processes:
   (a) randomly chooses a block m_{i-1} and computes (h_{i-1}, g_{i-1}).
   (b) randomly chooses a block m_i and check if (m_i, h_{i-1}, g_{i-1}) fixes the value h_i(or g_i).
2. Then $\mathcal{A}$ repeats Step 1 for 2^n times, check if there exists the value of (m_i, h_{i-1}, g_{i-1}) fixes the value g_i(or h_i).

It is easy to see the attack will succeed with a non-negligible probability due to the birthday paradox holds in Step 1 and the pigeonhole principle holds in Step 2. The total complexity is about $(2 \times 2^{n/2} + 2) \times 2^n \simeq 2 \times 2^{3n/2}$. Same result holds if either R_l^3 or R_l^4 is less than two. □

We note that both HDBL-1 and HDBL-2 are failed to be optimally (second) preimage resistance due to Theorem 9.

Subsequently, the complexities of free-start attacks on the rate-1 hash functions in FDBL-II can be easily deduced from the above results.

Lemma 3 *For any hash function H in FDBL-II with the form (3), if one of the ranks of L and R is less than four, then there exist free-start collision and free-start (second) preimage attacks on the hash function with complexities of about $2 \times 2^{n/2}$ and 2×2^n, respectively.*

Based on the above results, more exact security conditions for the rate-1 hash functions in FDBL-II to be optimally secure are listed as follows.

Corollary 1 *For the rate-1 hash functions in FDBL-II, if the round function matches one of the following conditions*

1. *The ranks of L and R are less than three,*

2. *The rank of* L_r^3*(or* L_r^4 *or* R_r^3 *or* R_r^4*) is less than two,*

3. *The rank of* L_l^3*(or* L_l^4 *or* R_l^3 *or* R_l^4*) is less than two,*

4. $h_{i-1} = g_{i-1}$ *implies* $h_i = g_i$*,*

5. $D \oplus h_{i-1} \neq 0$ *and* $D \oplus h_{i-1} \neq C$*, and* $Z \oplus g_{i-1} \neq 0$ *and* $Z \oplus g_{i-1} \neq Y$*,*

then there exist collision, preimage and second preimage attacks with non-negligible successful probability must spend the computation costs less or equal to break MDC-2.

4 A New Class of Fast DBL Hash Functions

Based on FDBL-I and FDBL-II, a new class of fast DBL hash functions named FDBL-III can be defined as follows. Hash functions in FDBL-III can be constructed on a block cipher $E \in \texttt{Bloc}(\kappa, n)$ with variants of key length where $\kappa = n$ or $\kappa = 2n$.

Definition 4 *Let* $E \in \texttt{Bloc}(\kappa, n)$ *be a block cipher with variants of key length where* $\kappa = n$ *or* $\kappa = 2n$*. A new class of DBL hash functions with rate 1 (denoted by FDBL-III) can be constructed as follows.*

$$\begin{cases} h_i = E_A(B) \oplus C, \\ g_i = E_{W||X}(Y) \oplus Z. \end{cases} \tag{11}$$

Both (A, B, C) and (W, X, Y, Z) are linear combinations of the n-bit vectors $(h_{i-1}, g_{i-1}, m_{i,1}, m_{i,2})$. Those linear combinations can be represented as

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \underbrace{\begin{pmatrix} L_l & L_r \end{pmatrix}}_{L} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}, \begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \underbrace{\begin{pmatrix} R_l & R_r \end{pmatrix}}_{R} \cdot \begin{pmatrix} h_{i-1} \\ g_{i-1} \\ m_i^1 \\ m_i^2 \end{pmatrix}, \tag{12}$$

By implementing the similar attacks on FDBL-II, one can easily derive the following results on FDBL-III.

Lemma 4 *For any hash function H in FDBL-III with the form (11), if the rank of L(or R) is less than three, then there exist collision, preimage, and second preimage attacks on the hash function with complexities of about $4 \times 2^{n/2}$, 3×2^n, and 3×2^n, respectively.*

Lemma 5 *For any hash function in FDBL-III with the form (11), if the rank of L_r^2(or L_r^3 or R_r^2 or R_r^3) is less than two, then there exist collision, preimage, and second preimage attacks on the hash function with complexities of about $4 \times 2^{n/2}$, 3×2^n, and 3×2^n, respectively.*

Lemma 6 *For any hash function in FDBL-III with the form (11), if the rank of L_l^2(or L_l^3 or R_l^2 or R_l^3) is less than two, then there exists a (second) preimage attack on the hash function with complexity of about $2 \times 2^{3n/2}$.*

Lemma 7 *For any hash function H in FDBL-III with the form (11), if $C \oplus h_{i-1} \neq 0$ and $C \oplus h_{i-1} \neq B$, and $Z \oplus g_{i-1} \neq 0$ and $Z \oplus g_{i-1} \neq Y$, then there exists a collision attack on the hash function with complexity of about $4 \times 2^{n/2}$.*

Lemma 8 *For any hash function H in FDBL-III with the form (11), if $h_{i-1} = g_{i-1}$ implies $h_i = g_i$, then there exists a collision attack on the hash function with complexity of about $4 \times 2^{n/2}$.*

The rate-1 hash functions in FDBL-III can also be constructed from two different block ciphers where $E_1 \in \texttt{Bloc}(n, n)$ and $E_2 \in \texttt{Bloc}(2n, n)$, which enlarges the candidates for the design.

5 Conclusion

In this paper, new attacks have been described on FDBL-II [7, 19]. In particular, the attacks proved Hirose's two examples are not optimally secure against collision, preimage and second preimage attacks. Based on the former results, the security of FDBL-II has been reconsidered and the conditions for optimally secure are given. Moreover, the security results are extended to a new class of the rate-1 hash functions (FDBL-III) based on FDBL-I and FDBL-II. These cryptanalysis results are practical and helpful to find the rate-1 DBL hash functions to be optimally secure in FDBL-II

and FDBL-III. By considering the security conditions on FDBL-II, Hirose's two examples can be improved as follows.

1. Improved HDBL-1

$$\begin{cases} h_i = E_{m_i^1 \oplus g_{i-1} || m_i^2}(h_{i-1}) \oplus h_{i-1} \\ g_i = E_{m_i^1 || m_i^2 \oplus h_{i-1}}(h_{i-1} \oplus g_{i-1}) \oplus h_{i-1} \oplus g_{i-1} \end{cases}$$

2. Improved HDBL-2

$$\begin{cases} h_i = E_{m_i^1 || m_i^2 \oplus g_{i-1}}(h_{i-1}) \oplus h_{i-1} \oplus g_{i-1} \\ g_i = E_{m_i^1 \oplus g_{i-1} || m_i^2}(h_{i-1} \oplus g_{i-1}) \oplus h_{i-1} \end{cases}$$

Future work is to make it clear whether there exists a subclass of the rate-1 hash functions in FDBL-II or FDBL-III which can be formally proved optimally secure against collision, preimage and second preimage attacks in the ideal cipher model. Another interesting work is to compare the performances between FDBL-II and FDBL-III.

References

[1] J. Black, P. Rogaway and T. Shrimpton. Black-Box Analysis of the Black-Cipher-Based Hash-Function Constructions from PGV. *Advances in Cryptology - CRYPTO'02*. LNCS 2442, pp. 320-335. 2002.

[2] J. Black. The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function. *FSE 2006*, LNCS 4047, pp. 328-340, 2006.

[3] B.O. Brachtl, D. Coppersmith, M.M. Hyden, S.M. Matyas, C.H. Meyer, J. Oseas, S. Pilpel and M. Schilling. *Data Authentication Using Modification Detection Codes Based on a Publick One Way Encryption Function*. U.S. Patent Number 4,908,861, March 13, 1990.

[4] L. Brown, J. Pieprzyk, and J. Seberry. LOKI-a cryptographic primitive for authentication and secrecy applications. In J. Seberry and J. Pieprzyk, editors, *Advances in Cryptology-Proc. AusCrypt'90*, LNCS 453, pp. 229-236, Springer-Verlag, Berlin, 1990.

[5] I. Damgard. A Design Principle for Hash Functions, *Advances in Cryptology, Cyrpto'89*, LNCS 435, pp. 416-427. 1989.

[6] S. Hirose. Some Plausible Constructions of Double-Block-Length Hash Functions. In *FSE 2006*, LNCS 4047, pp. 210-225, 2006.

[7] S. Hirose. A Security Analysis of Double-Block-Length Hash Functions with the Rate 1. *IEICE Trans. Fundamentals*, Vol. E89-A, NO.10, pp. 2575-2582, Oct 2006.

[8] W. Hohl, X. Lai, T. Meier, and C. Waldvogel. Security of iterated hash function based on block ciphers. In *CRYPTO'93*, LNCS 773, pp. 379-390, 1994.

[9] L.R. Knudsen. Block Ciphers-Analysis, Design and Applications. *Ph. D. thesis*, Aarthus University, 1994.

[10] L. R. Knudsen, X. Lai, and B. Preneel. Attacks on fast double block length hash functions. *Journal of Cryptology*, 11(1):59-72, 1998.

[11] X. Lai and J. L. Massey. Hash Functions Based on Block Ciphers. In *Advances in Cryptology-Eurocrypt'92*, LNCS 658, pp. 55-70. 1993.

[12] S. Lucks. A Failure-Friendly Design Principle for Hash Functions. In *ASIACRYPT 2005*, LNCS 3788, pp. 474-494. 2005.

[13] R.C. Merkle. One way hash functions and DES, *Advances in Cryptology, Crypto'89*, LNCS 435, pp. 428-446. 1989.

[14] M. Nandi. Design of Iteration on Hash Functions and Its Cryptanalysis. *PhD thesis*, Indian Statistical Institute, 2005.

[15] M. Nandi. Towards optimal double-length hash functions. *INDOCRYPT 2005*, LNCS 3797, pages 77C89, 2005.

[16] B. Preneel, A, Bosselaers, R. Govaerts and J. Vandewalle. Collision-free Hash-functions Based on Blockcipher Algorithms. In *Proceeding of 1989 International Carnahan Conference on Security Technology*, pp. 203-210, 1989.

[17] B. Preneel, R. Govaerts and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. In *Advances in Cryptology - CRYPTO'93*, LNCS 773, pp. 368-378. 1994.

[18] P. Rogaway and T. Shrimpton. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance and Collision Resistance. In *FSE 2004*, LNCS 3017, pp. 371-388, 2004.

[19] T. Satoh, M. Haga, and K. Kurosawa. Towards Secure adn Fast Hash Functions. *IEICE Trans. Fundamentals*, Vol. E82-A, NO.1, pp. 55-62, Jan, 1999.

[20] C. Shannon. Communication theory of secrecy systems. Bell Systems Techincal Journal, 28(4): pages 656-715, 1949.

[21] X. Wang, Y. Yin and H. Yu. Finding Collision in the Full SHA-1. In *CRYPTO'05*, LNCS 3621, pp. 17-36, 2005.

[22] X. Wang and H. Yu. How to Break MD5 and Other Hash Functions. In *EUROCRYPT'05*, LNCS 3494, pp.19-35, 2005.

[23] X. Yi and K.Y. Lam. A New Hash Function Based on Block Cipher. In *ACISP'97 Information Security and Privacy*, LNCS 1270, pp. 139-146, Springer-Verlag, 1997.