IEICE TRANS. INF. & SYST., VOL.E99–D, NO.4 APRIL 2016

PAPER Special Section on Information and Communication System Security

A New Scheme of Blockcipher Hash*,**

Rashed MAZUMDER[†a)], ***Nonmember and*** **Atsuko MIYAJI**[†,††,†††b)], ***Member***

SUMMARY A cryptographic hash is an important tool in the area of a modern cryptography. It comprises a compression function, where the compression function can be built by a scratch or blockcipher. There are some familiar schemes of blockcipher compression function such as Weimar, Hirose, Tandem, Abreast, Nandi, ISA-09. Interestingly, the security proof of all the mentioned schemes are based on the ideal cipher model (ICM), which depends on ideal environment. Therefore, it is desired to use such a proof technique model, which is close to the real world such as weak cipher model (WCM). Hence, we proposed an $(n, 2n)$ blockcipher compression function, which is secure under the ideal cipher model, weak cipher model and extended weak cipher model (ext.WCM). Additionally, the majority of the existing schemes need multiple key schedules, where the proposed scheme and the Hirose-DM follow single key scheduling property. The efficiency-rate of our scheme is $r = 1/2$. Moreover, the number of blockcipher call of this scheme is 2 and it runs in parallel.

key words: *cryptographic hash, blockcipher, ideal cipher model, weak cipher model, collision and preimage resistance*

1. Introduction

A cryptographic hash is defined as a module that takes an arbitrary length of data and produces a fixed size of data [1]. In the modern cryptography, a cryptographic hash has enormous applications. It is widely used in the digital signatures, message authentication, password verification and file/data identifier [1]–[4], [21], [24]. It consists of a compression function, where the blockcipher or scratch can be used [3], [4], [14]–[16]. Therefore, the blockcipher compression function is being focused here because of better security bound and higher efficiency than that of the scratch based compression function [5]–[10]. Additionally, the blockcipher compression function is suitable for encryption of a constrained device due to direct implementation of the blockcipher rather than the encryption function [3], [4], [10]–[12]. There are some well known properties of the cryptographic compression function such as collision resistance, preimage resistance, efficiency rate, key scheduling and number of blockcipher call, where these properties identify the efficacy and fame of the blockcipher based cryptographic compression function [1]–[3]. Usually, the collision resistance means, it is infeasible to find two inputs where outputs will collide. However, the efficiency rate is defined as $r = |m|/(n \times \#E)$, where $|m|$ = length of message, n = block-length, $\#E$ = number of blockcipher call [3], [4]. If a single key is used for each iteration of encryption, it is called single key scheduling (KS = 1) [3], [4]. Additionally, it is also needed to evaluate the number of blockcipher call ($\#E$) for a single message encryption [3], [4]. Generally, it is desired that r will be close to 1 and the value of KS and $\#E$ will be minimum for any better scheme of blockcipher compression function. There are two basic classifications of the blockcipher compression function such as (n, n) and $(n, 2n)$ blockcipher (n = block, key length) [1], [2], [17], [18]. However, the $(n, 2n)$ blockcipher compression function is suitable in application level because of higher security bound [21], [23], [24].

Motivation. There are some familiar schemes of $(n, 2n)$ blockcipher compression function such as Weimar, Hirose, Abreast, Tandem, Nandi and ISA-09. However, the security proof technique of these schemes depend on the ideal cipher model [3], [4], [15], [16], [23], [24]. Usually, the security proof of any crypto-system depends on cryptographic model, where this model is defined on the basis of certain assumptions, primitives, and environments [17]–[20], [33]. Hence, the security proof of a cryptographic compression function generally depends on the ideal assumptions, which is called ICM or Shanon model [17], [18]. As a security model, the ICM works well and easy to understand. But it totally depends on the ideal environment, where the adversarial power is limited [19], [20]. For example, the adversary can make only two types of query such as forward $\left(E^f\right)$ and backward $\left(E^b\right)$ query for finding collision attack [19], [20], [22]. Under this tight circumstance, Hirose et. al. [20] formalized the concept of the weak ideal compression function to the weak cipher model. However, Liscov point out the issue of the weak ideal compression function independently at first in 2006 [19], where the adversary is allowed to make total three types of query such as E^f, E^b and E^k (key-disclosure query). Therefore, the adversary of WCM is stronger than that of the ICM (details in [17], [19], [20]).

Still there is a limitation for the adversary under the

Manuscript received June 4, 2015.
Manuscript revised October 11, 2015.
Manuscript publicized January 13, 2016.

[†]The authors are with the JAIST, Nomi-shi, 923–1292 Japan.
[††]The author is with Graduate School of Engineering, Osaka University, Suita-shi, 565–0871 Japan.
[†††]The author is with Japan Science and Technology Agency (JST) CREST, Kawaguchi-shi, 332–0012 Japan.

*This paper was presented at AINA 2015 [31].

**This study is partly supported by Grant-in-Aid for Scientific Research (C) (15K00183) and (15K00189) and Japan Science and Technology Agency (JST), Infrastructure Development for Promoting International S&T Cooperation.

a) E-mail: s1420213@jaist.ac.jp
b) E-mail: miyaji@jaist.ac.jp, miyaji@comm.eng.osaka-u.ac.jp

DOI: 10.1587/transinf.2015ICP0028

Table 1 The result of existing blockcipher compression functions

				Security Proof Technique		
Scheme name	**CF**	**KS**	r	**ICM**	**WCM**	**ext. WCM**
MR (This paper), [31]	$3n \to 2n$	1	1/2	√	√	√
Weimar [3]	$3n \to 2n$	2	1/2	√	N.Y.	N.Y.
Hirose [3], [4]	$3n \to 2n$	1	1/2	√	N.Y.	N.Y.
Abreast [3], [15]	$3n \to 2n$	2	1/2	√	N.Y.	N.Y.
Tandem [3], [16]	$3n \to 2n$	2	1/2	√	N.Y.	N.Y.
Nandi [23]	$4n \to 2n$	3	2/3	√	N.Y.	N.Y.
ISA-09 [24]	$4n \to 2n$	3	2/3	√	N.Y.	N.Y.

CF = Compression function, KS =Key scheduling, Efficiency rate = r
ICM, WCM, ext.WCM = Ideal, Weak, extended weak (cipher model)
N.Y. = Not yet

Table 2

$\mathcal{A} \to^{allowed}$ for Game. **Game** (G): $[x, x'] \mid x \neq x' \wedge H(x) = H(x')$	ICM	WCM	ext. WCM
	Allow, $\mathcal{A} \to E^f / E^b$ for G	Allow, $\mathcal{A} \to E^f$ for G then, $\mathcal{A} \to E^b$ for G then, $\mathcal{A} \to E^k$ for G	Allow, $\mathcal{A} \to E^f / E^b // E^k$ for G

WCM model. Though the adversary can make three types of query but it is only allowed to make a single type of query under a single instance. For example, the adversary is allowed to make only forward query for a single game (Table 2 and Fig. 1). After ending of this game, it will be allowed for backward query or key-disclosure query. On the other hand, the adversary can make two types of query under the ICM but it is allowed for both query under a single instance (Table 2 and Fig. 1). That's why, we think to extend the weak cipher model, where the adversary can make three types of query for any game under a single instance like the ICM (Table 2 and Fig. 1).

In the perspective of the efficiency, the efficiency rate of Hirose-DM is 1/2 and it follows single key scheduling (Table 1). However, the collision security bound of Hirose-DM is less than that of the Weimar-DM [3], [4]. On the contrary, the Weimar-DM needs multiple key scheduling (Table 1). Usually, the number of gates will be increased if any scheme needs multiple key scheduling (details in [10], [31]). The efficiency rate of the Nandi and ISA-09 are 2/3 but the collision security bound are less than that of the Weimar and Hirose-DM [3], [4]. Additionally, the Nandi and ISA-09 need multiple key scheduling (KS = 3). Therefore, there is a scope for a new scheme which can provide higher collision security bound under the ICM, WCM and ext.WCM model. Moreover, the new scheme will satisfy single key scheduling property and higher efficiency rate.

Our Contribution: According to the motivational section, we can claim that our proposed scheme is secure under the three types of security model. Secondly, it follows single key scheduling and it's number of blockcipher call is 2. Additionally, the efficiency rate of proposed scheme is 1/2.

In the perspective of security bound, we use three kinds of security model such as the ICM, WCM and ext.WCM. The ICM depends on the ideal environment, which is far

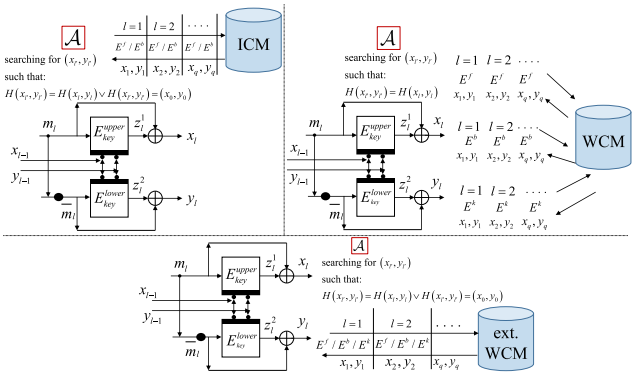

Fig. 1 Security proof model

from the real world [34]. Usually, the adversarial behaviour is limited under the ideal environment. Therefore, though the security bound is good under the ICM but it doesn't reflect the real world scenario [30], [34]. For example, the adversary can make query for plaintext and ciphertext under the ICM. Hence, there is a gap for key-disclosure query, which is being injected into the WCM [17]–[20]. As a result, the WCM is close to the real world, where the adversary gets better freedom than that of the ICM. That's why, it is desire to satisfy the security of blockcipher compression function under the WCM. However, the WCM is better than the ICM, but still it is not close enough to the real world. According to the definition of the WCM, we find that though the adversary can make three types of query but it is restricted for only one type of query under a single instance. As an example, the adversary can make only plaintext query for a single instance. Hence, it can start for the ciphertext or key-disclosure query process after ending the plaintext query process. That's why, we proposed here the ext.WCM, where the adversary can make any type of query under a single instance. Therefore, the ext.WCM goes more close to the real world than that of the WCM.

2. Preliminaries

2.1 Ideal Cipher Model (ICM)

The ideal cipher oracle is denoted by E, where it has n-bit block and k-bit key. If K, M, C is a set of key, message and ciphertext space, then $E_k(\cdot) \mid k \in K$ is an operation of a random permutation. The Block_n^k is a set of all blockciphers from where E is selected randomly. Under the ICM, two types of query are available to an adversary, where the adversary $\mathcal{A}$ can ask either E^f (forward query) or E^b (backward query) to the blockcipher oracle under a single instance (Table 2 and Fig. 1). The adversary gets a value of ciphertext $[E_k(m) = c \mid (k \in K, m \in M, c \in C)]$ for the E^f and oppositely it gets plaintext for the E^b. It is assumed that the adversary never makes a duplicate query [17], [18], [22].

2.2 Weak Cipher Model (WCM)

The weak cipher model [19], [20] is an extension of the

ICM. The assumption and primitive is more weaker than the ICM. The adversary can make the query of E^f and E^b as like the ICM. Additionally, a key-disclosure $\left(E^k\right)$ query can be asked by the adversary, where $E(m,c)=k$. The WCM environment also ensures that no duplicate query will be executed. Though the adversary can make three types of query but it is restricted to only one type of query for a single instance (Table 2 and Fig. 1).

2.3 Extended Weak Cipher Model (ext.WCM)

An extended weak cipher model (ext.WCM) has been introduced in this paper. It follows the basic properties of the ICM/WCM. It adds a new feature for making the adversary powerful, where the adversary can ask any type of query for a single instance (Table 2 and Fig. 1). Additionally, the assumptions of the ext.WCM is weaker than the ICM and WCM. Under the ext.WCM, the adversary gets a set of message and corresponding encrypted message (ciphertext) based on a key. However, the query process is based on non-adaptive. The blockcipher oracle is defined as ${}^{ext.}WCM^{k,m,c}(\cdot)$, where the adversary can ask and gets a set of key (k), message (m) and ciphertext (c).

2.4 Collision Resistance

It is difficult for an adversary to find a pair of distinct inputs, such that the hash output will be same. In notational form, it can be deduced as $H(in_1)=H(in_2)$, when $in_1 \neq in_2$ [$in_{1,2}$ = input, $H(\cdot)$ = Hash output]. It is assumed that the adversarial advantage will be measured by the number of executed queries from the oracle [3], [16], [27]–[29]. Additionally, it is assumed that the adversary doesn't make any similar query such as $E^f_{k_1}(m_1)=c_1 \rightarrow^{\times} \left(E^b_{k_1}(c_1)=m_1\right)$, where c = ciphertext, m = message and k = key.

The compression function of cryptographic hash is defined as F, where the blockcipher (E) is replaced into F. According to the adversarial point of view, the function of adversary is to find a collision under the F such as:

$$\begin{aligned}&\text{func}_F^{\text{coll}}(\mathcal{A}) = \\ &(x,y,m),(x',y',m') \leftarrow \mathcal{A}^{\text{ICM,WCM,}^{\text{ext.}}\text{WCM}} \\ &\text{if, } F(x,y,m)=F(x',y',m') \wedge \{(x,y,m)\neq(x',y',m')\} \\ &\text{then return 1, else 0}\end{aligned}$$

where,

$$\left[\begin{array}{l} x,y,x',y' = \text{chaining value,} \\ m,m' = \text{message,} \\ \text{ICM,WCM,}^{\text{ext.}}\text{WCM= oracle model} \end{array}\right]$$

If $\mathcal{A}$ finds a collision under the F then $\text{func}_F^{\text{coll}}(\mathcal{A})$ returns 1. Let, $\text{Adv}_F^{\text{coll}}(\mathcal{A})$ is probability of the function of $\text{func}_F^{\text{coll}}(\mathcal{A})$. Therefore, $\text{Adv}_F^{\text{coll}}(q)=\max_{\mathcal{A}}\left\{\text{Adv}_F^{\text{coll}}(\mathcal{A})\right\}$, where $\mathcal{A}$ can make at most q, $(q \geq 1)$ pairs of queries [17], [18], [30].

3. Definition of Scheme

The proposed scheme follows the two calls of blockcipher

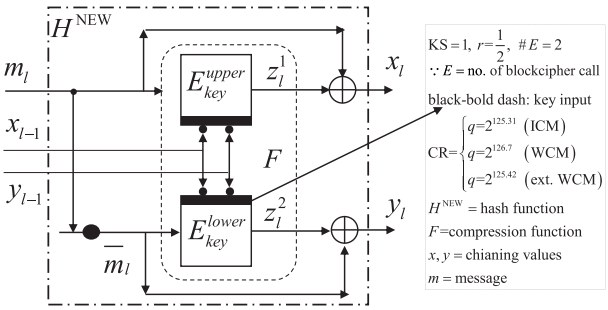

Fig. 2 Block diagram of the proposed scheme

call, where the key scheduling is single. It satisfies the class of $(n, 2n)$ blockcipher because of key size is double of the block-length. It runs under the Matyas Meyer Oseas mode (MMO). The definition and block diagram of this scheme are notified in Definition 1 and Fig. 2.

Definition 1. Let $E \in Block_n^k$ be a blockcipher, where k = key length and n = block-length. The H^{NEW} is a hash that is constructed by F. Let $F=\{0,1\}^n \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ be a blockcipher (E) based compression function. In this scheme, two independent blockciphers will be used for a single iteration such as E^{upper}_{key} and E^{lower}_{key}. Therefore, the final output of H^{NEW} will be:

$$\begin{aligned}&H^{NEW}(x_{l-1},y_{l-1},m_l)=x_l,\ y_l \\ &\text{such that,} \\ &x_l=z_l^1 \oplus m_l,\ \ y_l=z_l^2 \oplus \bar{m}_l \\ &\text{where,} \\ &\quad z_l^1 \leftarrow E^{upper}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(m),\ \ z_l^2 \leftarrow E^{lower}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(\bar{m})\end{aligned}$$

$$\left[x_l, y_l = \text{chaining value},\ m_l = \text{message},\ z_l^1, z_l^2 = \text{output}\right]$$

4. Security Proof of Collision Resistance Under the ICM

An adversary $\mathcal{A}$ can make two types of query such as forward query $\left(E^f\right)$ and backward query $\left(E^b\right)$ [17], [18], [22]. Under the ICM, a game will be defined as $Game^{coll}_{ICM}$ (Algorithm 1), where the adversary $\mathcal{A}$ will try to find (x,y,m) and (x',y',m'). Therefore, the adversary will win iff $H^{NEW}(x,y,m)=H^{NEW}(x',y',m')$ where, $(x,y,m)\neq(x',y',m')$. Additionally, the $Game^{coll}_{ICM}$ will be categorized into three sub-games with their tasks into Table 3. Hence, the adversary $\mathcal{A}$ will play through these three subgames for getting success, where the first subgame stands for dual queries. Under this subgame, the adversary will try to find two different queries for a collision. Secondly, the subgame of $subGame^{coll}_{sole,ICM}$ will be responsible for finding a collision within a single query. Finally, a collision through the initial chaining values will be followed by the third subgame.

Theorem 1: Let H^{NEW} be a two calls of $2n$ bit key blockcipher compression function. The task of adversary $\mathcal{A}$ is to find a collision under the compression function $F\left(H^{NEW}\right)$. Hence, after q pairs of queries, the advantage of $\mathcal{A}$ will be

Table 3 Branches of $Game^{coll}_{ICM}$

Branch name	Condition
$subGame^{coll}_{dual,ICM}$	$(x_l, y_l, m_l) \neq (x_{l'}, y_{l'}, m_{l'}) \wedge$ $H^{NEW}(x_l, y_l, m_l) = H^{NEW}(x_{l'}, y_{l'}, m_{l'})$
$subGame^{coll}_{sole,ICM}$	$x_l = y_l$, when $H^{NEW}(x_{l-1}, y_{l-1}, m_l) = (x_l, y_l)$
$subGame^{coll}_{pri,ICM}$	$(x_l, y_l) = (x_0, y_0)$, when $H^{NEW}(x_{l-1}, y_{l-1}, m_l) = (x_l, y_l)$

bounded by:

$$\mathrm{Adv}^{ICM^{coll}}_{H^{NEW}}(q) \leq \frac{q^2+q}{(2^n-2q)^2} + \frac{2q}{(2^n-2q)}$$

Proof: We allow an adversary $\mathcal{A}$ to ask any relevant query but assume that $\mathcal{A}$ never makes any duplicate query through E^f or E^b. It can ask upto l-th queries, where $l \leq q$.

$subGame^{coll}_{dual,ICM}$. The adversary $\mathcal{A}$ uses the ICM oracle for E^f or E^b query. At first, the adversary will check whether the most recent query made collision with the previous any queries or not. Let the current iteration is l, where the outputs are x_l, y_l. For example, $l'|(l' < l \leq q)$ is previously executed any iteration and the corresponding output are $x_{l'}, y_{l'}$. If $(x_l, y_l) = (x_{l'}, y_{l'})$, a trigger will be defined and the $subGame^{coll}_{dual,ICM}$ will be over. Otherwise, the adversary $\mathcal{A}$ will store the x_l, y_l into the query database (Q) and run for next iteration.

Let the outcome of l'-th iteration are $x_{l'} \leftarrow E^{upper}_{\bar{x}_{l'-1}\|\bar{y}_{l'-1}}(m_{l'}) \oplus m_{l'}$ and $y_{l'} \leftarrow E^{lower}_{\bar{x}_{l'-1}\|\bar{y}_{l'-1}}(\bar{m}_{l'}) \oplus \bar{m}_{l'}$. For an iteration of $l|(l' < l \leq q)$, the output are $x_l \leftarrow E^{upper}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(m_l) \oplus m_l$ and $y_l \leftarrow E^{lower}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(\bar{m}_l) \oplus \bar{m}_l$. If $(x_{l'}, y_{l'})$ and (x_l, y_l) collides each other then a trigger will be defined as $tri^{coll}_{dual,ICM}$. However, the x_l, y_l come from the set size $2^n - (2l-2)$ and $2^n - (2l-1)$. Hence, under the trigger of $tri^{coll}_{dual,ICM}$ the probability will be $l - 1/(2^n - (2l-2)) \times (2^n - (2l-1))$. More explicitly, under the $subGame^{coll}_{dual,ICM}$ through $tri^{coll}_{dual,ICM}$, the following states are responsible for collision:

$$\{(x_l = x_{l'}) \wedge (x_l = y_{l'})\} \vee \{(y_l = y_{l'}) \wedge (y_l = x_{l'})\} \quad (1)$$

where,

$$x_l = E^{upper}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(m_l) \oplus m_l, x_{l'} = E^{upper}_{\bar{x}_{l'-1}\|\bar{y}_{l'-1}}(m_{l'}) \oplus m_{l'}$$
$$y_l = E^{lower}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(\bar{m}_l) \oplus \bar{m}_l, y_{l'} = E^{lower}_{\bar{x}_{l'-1}\|\bar{y}_{l'-1}}(\bar{m}_{l'}) \oplus \bar{m}_{l'}$$

Therefore, the probability of collision under the l-th query will be $\Pr\left[Tri^{coll}_{dual,ICM}\right] = \Pr\left[tri^{coll}_{2,dual,ICM}, \cdots, tri^{coll}_{q,dual,ICM}\right]$, which implies that,

$$\sum_{l=2}^{q} \Pr[Tri^{coll}_{l,dual,ICM}] = \sum_{l=2}^{q} \frac{2(l-1)}{(2^n-2l-2)(2^n-2l-1)}$$
$$\leq \sum_{l=2}^{q} \frac{2(l-1)}{(2^n-2l)^2} \leq \frac{q^2}{(2^n-2q)^2} \quad (2)$$

$subGame^{coll}_{sole,ICM}$. The $subGame^{coll}_{sole,ICM}$ is responsible for finding a collision within l-th iteration of query, where $l \leq q$. Assume that, at the point of l-th iteration, the output are x_l and y_l. Therefore, there is a chance for creating a collision when $x_l = y_l$. If collision occurs, a trigger $\left(tri^{coll}_{sole,ICM}\right)$ will be called. Therefore, the probability of collision under the subgame $\left(subGame^{coll}_{sole,ICM}\right)$ through $tri^{coll}_{sole,ICM}$ is $\Pr\left[Tri^{coll}_{sole,ICM}\right] = \Pr\left[tri^{coll}_{1,sole,ICM}, tri^{coll}_{2,sole,ICM}, \ldots, tri^{coll}_{q,sole,ICM}\right]$. After q pairs of queries, it implies that,

$$\sum_{l=1}^{q} \Pr[Tri^{coll}_{l,sole,ICM}] = \sum_{l=1}^{q} \frac{1}{(2^n-2l-2)(2^n-2l-1)}$$
$$\leq \sum_{l=1}^{q} \frac{1}{(2^n-2l)^2} \leq \frac{q}{(2^n-2q)^2} \quad (3)$$

Algorithm 1 $\left(Game^{coll}_{ICM}\right)$

```
Initailization : l = 0, q = 2^n, Q : Empty query database
procedure Game^coll_ICM
    Execution: E^f or E^b
    Answer: from ICM oracle
    E^f/E^b → x_l = (z^1_l ⊕ m_l) = E^upper_{x̄_{l-1}‖ȳ_{l-1}}(m_l) ⊕ m_l
    E^f/E^b → y_l = (z^2_l ⊕ m̄_l) = E^lower_{x̄_{l-1}‖ȳ_{l-1}}(m̄_l) ⊕ m̄_l
    switch (input) do
        case 1
            assert(subGame^coll_dual,ICM)
            if l' < l ≤ q then
                searching for (x_l', y_l') from Q
                if {(x_l, y_l) = (x_l', y_l')} → A wins then
                    call: collision event tri^coll_dual,ICM
                    break: from subGame^coll_dual,ICM
                end if
            else
                store: (x_l, y_l) → Q
            end if
        case 2
            assert(subGame^coll_sole,ICM)
            if {(l ≤ q) ∧ (x_l = y_l)} → A wins then
                call: collision event tri^coll_sole,ICM
                break:from subGame^coll_sole,ICM
            else
                store: (x_l, y_l) → Q
            end if
        case 3
            assert(subGame^coll_pre,ICM)
            if {(l ≤ q) ∧ (x_l, y_l) = (x_0, y_0)} → A wins then
                call: collision event tri^coll_pri,ICM
                break: from subGame^coll_pri,ICM
            else
                store: (x_l, y_l) → Q
            end if
end procedure
```

$subGame^{coll}_{pri,ICM}$. Usually, the initial vectors or chaining values need to provide at the beginning of encryption process. Therefore, the generated output can be collide with the initial or primary values at the any phase of l. For example, in the iteration of $l|(l \leq q)$, the outcome are $x_l = E^{upper}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(m_l) \oplus m_l$ and $y_l = E^{lower}_{\bar{x}_{l-1}\|\bar{y}_{l-1}}(\bar{m}_l) \oplus$

$\bar{m}_l$. If collision occurs for x_0, y_0 and x_l, y_l, a trigger will be defined as $tri^{coll}_{pri,ICM}$ and query process will be terminated from the $subGame^{coll}_{pri,ICM}$. Hence, the probability of collision under l-th query will be $\Pr\left[Tri^{coll}_{pri,ICM}\right] = \Pr\left[tri^{coll}_{1,pri,ICM}, tri^{coll}_{2,pri,ICM}, \ldots, tri^{coll}_{q,pri,ICM}\right]$. After q pairs of queries, it implies that,

$$\sum_{l=1}^{q} \Pr[Tri^{coll}_{l,pri,ICM}] = \sum_{l=1}^{q} \frac{2}{(2^n - 2l)} \leq \frac{2q}{(2^n - 2q)} \tag{4}$$

Adding 2, 3 and 4, Theorem 1 will be satisfied.

5. Security Proof of Collision Resistance Under the WCM

An adversary $\mathcal{A}$ will make an additional query E^k with E^f and E^b under the WCM, where E^k is defined as a key-disclosure query [19], [20]. According to the WCM, the adversary $\mathcal{A}$ will make any relevant query with non-repetition. A $Game^{coll}_{WCM}$ (Algorithm 2) will be defined for finding collision under the WCM. The target of the adversary $\mathcal{A}$ is to find X, Y such that $H(X) = H(Y)$, where X, Y = input, H = hash outout. Additionally, the $Game^{coll}_{WCM}$ will be classified into three subgames (Table 4), where $subGame^{coll}_{forw(E^f),WCM}$ is defined for finding collision through ciphertext and $subGame^{coll}_{back(E^b),WCM}$ is used for exploring plaintext. Additionally, the adversary $\mathcal{A}$ will execute the game of $subGame^{coll}_{key(E^k),WCM}$ for getting collision through the key-disclosure query.

Theorem 2: Let H^{NEW} be a two calls of $2n$ bit key, blockcipher hash function. It invokes the blockcipher based compression function F, where the advantage of the adversary $\mathcal{A}$ is to find collision under H^{NEW} (F). Therefore, after q pairs of queries, the adversarial advantage will be bounded by:

$$\mathrm{Adv}^{WCM^{coll}}_{H^{NEW}}(q) \leq \frac{3q(q-1)}{2^{2n}}$$

Proof: Let $\mathcal{A}$ be the adversary that can make query upto l-th queries, where $l \leq q$. The collision probability of these three subgames will be evaluated under the adversary $\mathcal{A}$ in the following way.

$subGame^{coll}_{forw(E^f),WCM}$. The adversary $\mathcal{A}$ will execute the $subGame^{coll}_{forw(E^f),WCM}$, where a forward query returns the query result and stores a pair of output into the Q. There are three basic phases under the $subGame^{coll}_{forw(E^f),WCM}$ such as making query, checking and trigger/store. In the first phase, the adversary is allowed to make query through E^f under the WCM. Then in second phase, $\mathcal{A}$ checks whether the last output pair collides with the previous any query pair. The third phase depends on the second phase where a trigger will be called if collision occurs. On the contrary, the output pair will be stored into Q and the adversary will be allowed for next query. For example, the adversary $\mathcal{A}$ gets a pair of outputs $(x_{l'}, y_{l'})$ at the l'-th iteration. Let there is an another iteration of $l|\,(l' < l)$, where output pair will be x_l, y_l. If $(x_l, y_l) = (x_{l'}, y_{l'})$ then a collision will be occurred and a trigger $\left(tri^{coll}_{E^f,WCM}\right)$ will be called. However, the sets of queries are:

$$\begin{aligned}
&E^f \rightarrow^{WCM} (l' < q):\\
&\quad x_{l'} = z^1_{l'} \oplus m_{l'} = E^{upper}_{\tilde{x}_{l'-1},\tilde{y}_{l'-1}}(m_{l'}) \oplus m_{l'},\\
&\quad y_{l'} = z^2_{l'} \oplus \bar{m}_{l'} = E^{lower}_{\tilde{x}_{l'-1},\tilde{y}_{l'-1}}(\bar{m}_{l'}) \oplus \bar{m}_{l'}\\
&E^f \rightarrow^{WCM} (l' < l < q):\\
&\quad x_l = z^1_l \oplus m_l = E^{upper}_{\tilde{x}_{l-1},\tilde{y}_{l-1}}(m_l) \oplus m_l,\\
&\quad y_l = z^2_l \oplus \bar{m}_l = E^{lower}_{\tilde{x}_{l-1},\tilde{y}_{l-1}}(\bar{m}_l) \oplus \bar{m}_l
\end{aligned}$$

Hence, the conditions of collision are:

$$\left\{ \begin{array}{l} \left(z^1_{l'} \oplus m_{l'} = z^1_l \oplus m_l\right) \vee \\ \left(z^2_{l'} \oplus \bar{m}_{l'} = z^1_l \oplus m_l\right) \end{array} \right\} \wedge \left\{ \begin{array}{l} \left(z^1_{l'} \oplus m_{l'} = z^2_l \oplus \bar{m}_l\right) \vee \\ \left(z^2_{l'} \oplus \bar{m}_{l'} = z^2_l \oplus \bar{m}_l\right) \end{array} \right\} \tag{5}$$

From 5, the collision probability will be:

$$\sum_{l=2}^{q} \Pr[Tri^{coll}_{l,E^f,WCM}] = \sum_{l=2}^{q} \frac{2(l-1)}{(2^n - 2l)^2}$$

$$\leq \sum_{l=2}^{q} \frac{2(l-1)}{(2^n)^2} \leq \frac{q(q-1)}{2^{2n}} \tag{6}$$

$subGame^{coll}_{back(E^b),WCM}$. Let the adversary $\mathcal{A}$ will execute the $subGame^{coll}_{back(E^b),WCM}$, where backward query will be provided an output pair. A trigger $\left(tri^{coll}_{E^b,WCM}\right)$ will be defined, if collision occurs. According to this subgame and the previous explanation of the $subGame^{coll}_{forw(E^f),WCM}$, the collision probability will be:

$$= \sum_{l=2}^{q} \Pr[Tri^{coll}_{l,E^b,WCM}] = \sum_{l=2}^{q} \frac{2(l-1)}{(2^n - 2l)^2}$$

$$\leq \sum_{l=2}^{q} \frac{2(l-1)}{(2^n)^2} \leq \frac{q(q-1)}{2^{2n}} \tag{7}$$

$subGame^{coll}_{key(E^k),WCM}$. The explanation of probability of $subGame^{coll}_{key(E^k),WCM}$ is as that of the $subGame^{coll}_{forw(E^f),WCM}$. Therefore, the probability of collision will be:

$$= \sum_{l=2}^{q} \Pr[Tri^{coll}_{l,E^k,WCM}] = \sum_{l=2}^{q} \frac{2(l-1)}{(2^n - 2l)^2}$$

Table 4 Branches of $Game^{coll}_{WCM}$

Branch name	Condition
$subGame^{coll}_{forw(E^f),WCM}$	$E^f \rightarrow (x,y,m) \neq (x',y',m')$ $\wedge H^{NEW}(x,y,m) = H^{NEW}(x',y',m')$
$subGame^{coll}_{back(E^b),WCM}$	$E^b \rightarrow (x,y,m) \neq (x',y',m')$ $\wedge H^{NEW}(x,y,m) = H^{NEW}(x',y',m')$
$subGame^{coll}_{key(E^k),WCM}$	$E^k \rightarrow (x,y,m) \neq (x',y',m')$ $\wedge H^{NEW}(x,y,m) = H^{NEW}(x',y',m')$

$$\leq \sum_{l=2}^{q} \frac{2(l-1)}{(2^n)^2} \leq \frac{q(q-1)}{2^{2n}} \quad (8)$$

Adding the values of 6, 7 and 8, Theorem 2 will be proved.

Algorithm 2 $\left(Game^{coll}_{WCM}\right)$

1: Initailization : $l = 0$, $q = 2^n$, Q : Empty query database
2: **procedure** $Game^{coll}_{WCM}$
3: run: $subGame^{coll}_{forw,WCM}$, $subGame^{coll}_{back,WCM}$ and $subGame^{coll}_{key,WCM}$
4: **function** $subGame^{coll}_{forw(E^f),WCM}$
5: **for** $(l \leq q)$ **do**
6: run an oracle $\left(E^f\right)$ from WCM
7: reply:
8: $E^f \rightarrow x_l = \left(z^1_l \oplus m_l\right) = E^{upper}_{\tilde{x}_{l-1}\|\tilde{y}_{l-1}}(m_l) \oplus m_l$
9: $E^f \rightarrow y_l = \left(z^2_l \oplus \bar{m}_l\right) = E^{lower}_{\tilde{x}_{l-1}\|\tilde{y}_{l-1}}(\bar{m}_l) \oplus \bar{m}_l$
10: Check for collision hit event:
11: **if** $l' < l \leq q$ **then**
12: searching for $(x_{l'}, y_{l'})$ from Q
13: **if** $(x_l, y_l) = (x_{l'}, y_{l'}) \rightarrow$ Adversary wins **then**
14: introduce event $tri^{coll}_{E^f,WCM}$
15: terminate from $subGame^{coll}_{forw(E^f),WCM}$
16: **end if**
17: **else**
18: keep: $(x_l, y_l) \rightarrow Q$
19: **end if**
20: **end for**
21: **end function**
22: **function** $subGame^{coll}_{back(E^b),WCM}$
23: run an oracle $\left(E^b\right)$ from WCM
24: do same procedure as $subGame^{coll}_{forw(E^f),WCM}$ but use a different oracle
25: **end function**
26: **function** $subGame^{coll}_{key(E^k),WCM}$
27: run an oracle $\left(E^k\right)$ from WCM
28: do same procedure as $subGame^{coll}_{forw(E^f),WCM}$ but use a different oracle
29: **end function**
30: **end procedure**

6. Security Proof of Collision Resistance under ext.WCM

According to the definition of ext.WCM, the adversary $\mathcal{A}$ will make three types of query under a single instance non-adaptively (Table 2 and Fig. 1), where the adversary has no chance for repeated query. A $Game^{coll}_{(E^f,E^b,E^k),ext.WCM}$ (Algorithm 3) will be defined in this section for providing the security proof of the proposed scheme and it is categorized into three subgames with their task into Table 5.

Theorem 3: Let H^{NEW} be a two calls of $2n$ bit key blockcipher hash function, where it consists of blockcipher compression function F. The advantage of adversary $\mathcal{A}$ is to find collision through H^{NEW} (F) after q pairs of queries. Therefore, the adversarial advantage will be bounded by:

$$\mathrm{Adv}^{ext.WCM^{coll}}_{H^{NEW}}(q) = q^2 - q\Big/2N^2 + 3q/N$$

Table 5 Branches of $Game^{coll}_{(E^f,E^b,E^k),ext.WCM}$

Branch name	Condition
${}^{outer}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$	$E^{f,b,k} \rightarrow^{ext.} WCM^{k,m,c}(\cdot) \Rightarrow$ $(x_l, y_l, m_l) \neq (x_{l'}, y_{l'}, m_{l'}) \wedge$ $H^{NEW}(x_l, y_l, m_l)$ $= H^{NEW}(x_{l'}, y_{l'}, m_{l'})$
${}^{inner,IV}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$	$E^{f,b,k} \rightarrow^{ext.} WCM^{k,m,c}(\cdot) \Rightarrow$ $x_l = y_l$ when, $H^{NEW}(x_{l-1}, y_{l-1}, m_l) = (x_l, y_l)$ $\vee$ $(x_l, y_l) = (x_0, y_0)$ when, $H^{NEW}(x_{l-1}, y_{l-1}, m_l) = (x_l, y_l)$ and (x_0, y_0) = initial value

Proof: Let the adversary $\mathcal{A}$ will ask any relevant query and never makes any duplicate query through $E^f/E^b/E^k$. Under the ext.WCM model, the query will be asked non-adaptively at first. Therefore, the adversary looks for collision based on those executed queries.

${}^{outer}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$. The subgame of ${}^{outer}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$ will be assigned for finding collision under any iteration of the query process $l|\,(l \leq q)$. For an example, at the point of $l'\,(l' \leq q)$-th iteration, the resultant output are $x_{l'}, y_{l'}$. However, in the iteration of $l|\,(l' < l \leq q)$, the output are x_l, y_l. If the adversary $\mathcal{A}$ finds that there is a collision between $x_{l'}, y_{l'}$ and x_l, y_l then a trigger will be called. Hence, the conditions of collision are:

$$\left(\mathcal{A} \rightarrow^{make\ query} \left(E^f, E^b, E^k\right)\right) \wedge \text{(for two iterations of queries } (l, l')\,|(l' < l \leq q)) \quad (9)$$

Furthermore, (9) can be derived as:

$$z^1_l\left(E^{upper}_{\tilde{x}_{l-1},\tilde{y}_{l-1}}(m_l)\right) = z^1_{l'}\left(E^{upper}_{\tilde{x}_{l'-1},\tilde{y}_{l'-1}}(m_{l'})\right)$$
or,
$$z^1_l\left(E^{upper}_{\tilde{x}_{l-1},\tilde{y}_{l-1}}(m_l)\right) = z^2_{l'}\left(E^{lower}_{\tilde{x}_{l'-1},\tilde{y}_{l'-1}}(,\bar{m}_{l'})\right) \quad (10)$$

and

$$z^2_l\left(E^{lower}_{\tilde{x}_{l-1},\tilde{y}_{l-1}}(\bar{m}_l)\right) = z^2_{l'}\left(E^{lower}_{\tilde{x}_{l'-1},\tilde{y}_{l'-1}}(\bar{m}_{l'})\right)$$
or,
$$z^2_l\left(E^{lower}_{\tilde{x}_{l-1},\tilde{y}_{l-1}}(\bar{m}_l)\right) = z^1_{l'}\left(E^{upper}_{\tilde{x}_{l'-1},\tilde{y}_{l'-1}}(m_{l'})\right) \quad (11)$$

If, 10 and 11 occurs then ${}^{outer}tri^{coll}_{(E^f,E^b,E^k),ext.WCM}$ will be called. The probability of collision under the subgame of ${}^{outer}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$ will be:

$$\Pr\left[{}^{outer}Tri^{coll}_{(E^f,E^b,E^k),ext.WCM}\right] = \Pr\left[{}^{outer}tri^{coll}_{1,(E^f,E^b,E^k),ext.WCM}, \ldots, {}^{outer}tri^{coll}_{q,(E^f,E^b,E^k),ext.WCM}\right] \quad (12)$$

From 12,

$$\sum_{l=1}^{q} \Pr\left[{}^{outer}Tri^{coll}_{l,(E^f,E^b,E^k),ext.WCM}\right] = \sum_{l=1}^{q} \frac{(l-1)}{(2^{2n})} \leq \frac{q^2 - q}{2.2^{2n}} \quad (13)$$

${}^{inner}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$. Let, there is an iteration l, where $l \le q$. Under the l-th iteration, the output will be:

$$z_l^1 = E^{upper}_{\bar{x}_{l-1},\bar{y}_{l-1}}(m_l) \Rightarrow m_l \oplus z_l^1 = x_l \tag{14}$$

$$z_l^2 = E^{lower}_{\bar{x}_{l-1},\bar{y}_{l-1}}(\bar{m}_l) \Rightarrow \bar{m}_l \oplus z_l^2 = y_l \tag{15}$$

Algorithm 3 $\left(Game^{coll}_{(E^f,E^b,E^k),ext.WCM}\right)$

```
Initailization : l = 0, q = 2^n, Q : Empty query database
procedure (Game^{coll}_{(E^f,E^b,E^k),ext.WCM})
    for (l ≤ q) do
        Execution: E^f/E^b/E^k through ^{ext.}WCM^{k,m,c}(·)
        Answer from ext. WCM oracle
        E^f/E^b/E^k → x_l = (E^{upper}_{x_{l-1}||y_{l-1}}(m_l) ⊕ m_l)
        E^f/E^b/E^k → y_l = (E^{upper}_{x̄_{l-1}||ȳ_{l-1}}(m̄_l) ⊕ m̄_l)
        Store into Q
    end for
    (∗calling three subgames∗)
    CALL → ^{outer}subGame^{coll}_{(E^f,E^b,E^k),ext.WCM}
    searching for (x_l, y_l) and (x_{l'}, y_{l'}) from Q
    if {(x_l, y_l) = (x_{l'}, y_{l'})} → A wins then
        call collision event (^{outer}tri^{coll}_{(E^f,E^b,E^k),ext.WCM})
        break from ^{outer}subGame^{coll}_{(E^f,E^b,E^k),ext.WCM}
    end if
    CALL → ^{inner}subGame^{coll}_{(E^f,E^b,E^k),ext.WCM}
    searching for (x_l, y_l)
    if (x_l = y_l) → A wins then
        call collision event (^{inner}tri^{coll}_{(E^f,E^b,E^k),ext.WCM})
        break from ^{inner}subGame^{coll}_{(E^f,E^b,E^k),ext.WCM}
    end if
    CALL → ^{iv}Game^{coll}_{(E^f,E^b,E^k),ext.WCM}
    searching for (x_l, y_l)
    if {(x_l, y_l) = (x_0, y_0)} → A wins then
        call collision event (^{iv}tri^{coll}_{(E^f,E^b,E^k),ext.WCM})
        break from ^{iv}subGame^{coll}_{(E^f,E^b,E^k),ext.WCM}
    end if
end procedure
```

There is a chance to make collision between x_l and y_l. So, a trigger $\left({}^{inner}tri^{coll}_{(E^f,E^b,E^k),ext.WCM}\right)$ will be called when a collision occurs. Hence,

$$\Pr\left[{}^{inner}Tri^{coll}_{(E^f,E^b,E^k),ext.WCM}\right] = \Pr\left[{}^{inner}tri^{coll}_{1,(E^f,E^b,E^k),ext.WCM}, \cdots, {}^{inner}tri^{coll}_{q,(E^f,E^b,E^k),ext.WCM}\right] \tag{16}$$

From 16, the collision probability will be:

$$\sum_{l=1}^{q} \Pr\left[{}^{inner}Tri^{coll}_{l,(E^f,E^b,E^k),ext.WCM}\right] = \sum_{l=1}^{q} \frac{1}{2^n} \le \frac{q}{2^n} \tag{17}$$

${}^{iv}subGame^{coll}_{(E^f/E^b/E^k),ext.WCM}$. Under this subgame, there is a possibility for a collision such as $(x_l, y_l) = (x_0, y_0)$. Therefore, the probability of collision will be:

$$\sum_{l=1}^{q} \Pr\left[{}^{iv}Tri^{coll}_{l,(E^f,E^b,E^k),ext.WCM}\right] = \sum_{l=1}^{q} \frac{2}{2^n} \le \frac{2q}{2^n} \tag{18}$$

Theorem 3 will be proved after summing the values of 13, 17 and 18.

Table 6 Number of queries under ICM, WCM, ext. WCM model

Proposed Scheme	ICM	WCM	ext. WCM
	$q = 2^{125.31}$	$q = 2^{126.70}$	$q = 2^{125.42}$

7. Result Analysis

The proposed scheme satisfies the two calls of $2n$ bit blockcipher, where the number of cycle is two. The collision security bound of this scheme is $q = 2^{125.31}$ under the ICM (q = number of queries). The probability of adversarial advantage comes from Theorem 1, which is used for finding the number of queries.

Let $N = 2^n$ and $\mathrm{Adv}^{ICM^{coll}}_{H^{NEW}}(q) \le \frac{q^2+q}{(2^n-2q)^2} + \frac{2q}{(2^n-2q)}$ from Theorem 1. According to basic primitive, $n = 128$ (block-length/message) and $\mathrm{Adv}^{ICM^{coll}}_{H^{NEW}}(q) = \frac{1}{2}$ (due to birthday attack). Therefore, the value of q will be $2^{125.31}$ under the ICM. In similar way, the total number of queries under the WCM and ext.WCM will be evaluated and mentioned in Table 6.

8. Conclusion

There are many studies on the blockcipher cryptographic hash (compression function) where the security proof model plays an important role [17], [18], [20], [29], [30], [34]. Usually, the ICM is used as a model for the security proof, that depends on the ideal environment [3]–[5], [11], [12], [14], [16], [23], [24], [34]. However, the ICM is far away from the real world scenario [29], [34]. Therefore, it is obvious to use the security proof model, which is close to the real world such as the WCM [19], [20] and ext.WCM. Currently, none of the existing schemes are secure under more than one security proof model. In this article, the proposed $(n, 2n)$ blockcipher compression function is secure under three types of security proof model such as the ICM, WCM and ext.WCM (Table 6). The proposed scheme follows single key scheduling under the Matyas Meyer mode. The efficiency rate and number of calling blockcipher are respectively 1/2 and 2. However, the proposed scheme is not suitable for small message encryption and also it can not encrypt without padding. Additionally, this scheme is secure only under the Maytas Meyer Mode. Hence, there is a chance to provide a scheme which will be suitable for small domain encryption as well as padding free encrytion. Additionally, it will be secure under any mode of the PGV [17], [18].

References

[1] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, 5th ed, ISBN: 0-8493-8523-7, CRC Press, 1996.
[2] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, and Y. Seurin, "Hash functions and RFID tags: Mind the gap," LNCS, CHES, vol.5154, pp.283–299, 2008.
[3] E. Fleischmann, C. Forler, S. Lucks, and J. Wenzel, "Weimar-DM: A Highly Secure Double-Length Compression Function," LNCS, ACISP, vol.7372, pp.152–165, 2012.
[4] S. Hirose, "Some Plausible Constructions of Double-Block-Length Hash Functions," LNCS, FSE, vol.4047, pp.210–225, 2006.
[5] Y. Dodis, T. Ristenpart, and T. Shrimpton, "Salvaging Merkle-Damgard for Practical Applications," LNCS, EUROCRYPT, vol.5479, pp.371–388, 2009.
[6] J.-S. Coron, Y. Dodis, C. Malinaud, and P. Puniya, "Merkle-Damgard Revisited: How to Construct a Hash Function," LNCS, CRYPTO, vol.3621, pp.430–448, 2005.
[7] X. Wang, X. Lai, D. Feng, H. Chen, and X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD," LNCS, EUROCRYPT, vol.3494, pp.1–18, 2005.
[8] X. Wang, Y.L. Yin, and H. Yu, "Finding Collisions in the Full SHA-1," LNCS, CRYPTO, vol.3621, pp.17–36, 2005.
[9] J.-P. Kaps and B. Sunar, "Energy Comparison of AES and SHA-1 for Ubiquitous Computing," LNCS, Emerging Directions in Embedded and Ubiquitous Computing, vol.4097, pp.372–381, 2006.
[10] J. Lee, K. Kapitanova, and S.H. Son, "The price of security in wireless sensor networks," ELSEVIER, Computer Network, vol.54, no.17, pp.2967–2978, Dec. 2010.
[11] X. Lai and J.L. Massey, "Hash function based on block ciphers," LNCS, EUROCRYPT, vol.658, pp.55–70, 1992.
[12] J. Lee and M. Stam, "MJH: A Faster Alternative to MDC-2," LNCS, CT-RSA, vol.6558, pp.213–236, 2011.
[13] B. Mennink, "Optimal Collision Security in Double Block Length Hashing with Single Length Key," LNCS, ASIACRYPT, vol.7658, pp.526–543, 2012.
[14] A. Miyaji, M. Rashed, and T. Sawada, "A New (n, n) Blockcipher Hash Function: Apposite for Short Messages," IEEE, ASIAJCIS, 978-1-4799-5733, pp.56–63, 2014.
[15] J. Lee and D. Kwon, "The Security of Abreast-DM in the Ideal Cipher Model," IEICE Transactions, vol.E94-A, no.1, pp.104–109, 2011.
[16] J. Lee, M. Stam, and J. Steinberger, "The Collision Security of Tandem-DM in the Ideal Cipher Model," LNCS, CRYPTO, vol.6841, pp.561–577, 2011.
[17] J. Black, P. Rogaway, and T. Shrimpton, "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV," LNCS, CRYPTO, vol.2442, pp.320–335, 2002.
[18] J. Black, P. Rogaway, T. Shrimpton, and M. Stam, "An Analysis of the Blockcipher-Based Hash Functions from PGV," LNCS, J.CRYPTOL, vol.23, no.4, pp.519–545, 2010.
[19] M. Liscov, "Constructing an ideal hash function from weak ideal compression function," LNCS, selected areas in cryptography, vol.4356, pp.358–375, 2006.
[20] S. Hirose and H. Kuwakado., "Collision Resistance of Hash Functions in a Weak Ideal Cipher Model," IEICE Transactions, vol.E95-A, no.1, pp.252–255, 2012.
[21] O. Ozen and M. Stam, "Another Glance at Double-Length Hashing," LNCS, Cryptography and Coding, vol.5291, pp.176–201, 2009.
[22] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell Systems Technical Journal, vol.28, no.4, pp.656–715, 1949.
[23] M. Nandi, W. Lee, K. Sakurai, and S. Lee, "Security Analysis of a 2/3-Rate Double Length Compression Function in the Black-Box Model," LNCS, FSE, vol.3557, pp.243–254, 2005.
[24] J. Lee, S. Hong, J. Sung, and H. Park, "A New Double-Block-Length Hash Function Using Feistel Structure," LNCS, ISA, vol.5576, pp.11–20, 2009.
[25] F. Armknecht, E. Fleischmann, M. Krause, J. Lee, M. Stam, and J. Steinberger, "The Preimage Security of Double-Block-Length Compression Functions," LNCS, ASIACRYPT, vol.7073, pp.233–251, 2011.
[26] E. Fleischmann, C. Forler, and S. Lucks, "The Collision Security of MDC-4," LNCS, Africacrypt, vol.7374, pp.272–269, 2012.
[27] M. Stam, "Blockcipher-Based Hashing Revisited," LNCS, FSE, vol.5665, pp.67–83, 2009.
[28] J.P. Steinberger, "The Collision Intractability of MDC-2 in the Ideal-Cipher Model," LNCS, Eurocrypt, vol.4515, pp.34–51, 2007.
[29] J.S. Coron, J. Patarin, and Y. Seurin, "The Random Oracle Model and the Ideal Cipher Model are Equivalent," LNCS, CRYPTO, vol.5157, pp.1–20, 2008.
[30] J. Black, "The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function," LNCS, FSE, vol.4047, pp.328–340, 2006.
[31] A. Miyaji and M. Rashed, "A new (n, 2n) Double Block Length Hash Function based on Single Key Scheduling," IEEE explore, AINA, pp.564–570, 2015.
[32] D. Joan and R. Vincent, The Design of Rijndael, AES-The Advanced Encryption Standard, Information security and cryptography, Springer, ISBN: 3-540-42580-2, 2002.
[33] Report paper, "Study on cryptographic protocols," ENISA, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols, ISBN: 978-92-9204-103-8, 2014.
[34] J. Katz, S. Lucks, and A. Thiruvengadam, "Hash Functions from Defective Ideal Ciphers," CT-RSA, vol.9048, pp.273–290, 2015.

Rashed Mazumder received his Bachelor degree from University of Dhaka, Bangladesh in the field of Computer Science and Engineering. In 2010, he joined as a faculty in Mawlana Bhashani Science and Technology University, Bangladesh. He completed a Masters degree from the university of Japan Advanced Institute of Science and Technology (JAIST), Japan in 2014. Currently he is in Ph.D. program at JAIST.

Atsuko Miyaji received the B. Sc., the M. Sc., and the Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Panasonic Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She was an associate professor at the Japan Advanced Institute of Science and Technology (JAIST) in 1998. She joined the computer science department of the University of California, Davis from 2002 to 2003. She has been a professor at Japan Advanced Institute of Science and Technology (JAIST) since 2007 and the director of Library of JAIST from 2008 to 2012. She has been a professor at Graduate School of Engineering, Osaka University since 2015. Her research interests include the application of number theory into cryptography and information security. She received Young Paper Award of SCIS'93 in 1993, Notable Invention Award of the Science and Technology Agency in 1997, the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, Engineering Sciences Society: Certificate of Appreciation in 2005, the AWARD for the contribution to CULTURE of SECURITY in 2007, IPSJ/ITSCJ Project Editor Award in 2007, 2008, 2009, and 2010, the Director-General of Industrial Science and Technology Policy and Environment Bureau Award in 2007, Editorial Committee of Engineering Sciences Society: Certificate of Appreciation in 2007, DoCoMo Mobile Science Awards in 2008, Advanced Data Mining and Applications (ADMA 2010) Best Paper Award, and The chief of air staff: Letter of Appreciation Award, Engineering Sciences Society: Contribution Award in 2012, and Prizes for Science and Technology, The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and the Mathematical Society of Japan.