On High-Rate Cryptographic Compression Functions*

Richard Ostertág and Martin Stanek

Department of Computer Science
Faculty of Mathematics, Physics and Informatics
Comenius University
Mlynská dolina, 842 48 Bratislava, Slovak Republic
{ostertag, stanek}@dcs.fmph.uniba.sk

Abstract. The security of iterated hash functions relies on the properties of underlying compression functions. We study highly efficient compression functions based on block ciphers. We propose a model for high-rate compression functions, and give an upper bound for the rate of any collision resistant compression function in our model. In addition, we show that natural generalizations of constructions by Preneel, Govaerts, and Vandewalle to the case of rate-2 compression functions are not collision resistant.

Key words: Hash functions, compression functions, block ciphers, provable security.

1 Introduction

Cryptographic hash functions are basic building blocks in many security constructions – digital signatures, message authentication codes, etc. Almost all modern hash functions are built by iterating a compression function according the Merkle-Damgård paradigm [3, 5]. Moreover, these compression functions are often based on some underlying block cipher. Even dedicated hash function like SHA-1 is based on a block cipher called SHACAL-1 [4].

The first systematic study of 64 block cipher based hash functions was done by Preneel, Govaerts, and Vandewalle [6]. Subsequently, Black, Rogaway, and Shrimpton [2] analyzed these constructions in black box model and proved that 20 of them are collision resistant up to the birthday-attack bound.

An important property of a hash function is performance. Therefore, one would like to maximize the rate of hash function – the number of message blocks processed with one block cipher transformation. Another way to design fast hash functions is the usage of keys from a small fixed set of keys in all block cipher transformations, thus enabling a pre-scheduling of keys. Classical constructions [6] are rate-1 and require rekeying for every message block. Recently, Black,

* We appreciate any comments and suggestions.

Cochran, and Shrimpton [1] shown, that it is impossible to construct (block cipher based) provably secure rate-1 iterated hash function that use small fixed set of keys.

Our contribution. We analyze the existence of high-rate compression functions. Our contribution is twofold:

1. We propose a general model of (block cipher based) high-rate compression functions, and show an upper bound for rate of provably secure compression functions.
2. We show that generalizations of rate-1 constructions by Preneel, Govaerts, and Vandewalle [6] to the case of rate-2 compression functions are not collision resistant.

Remark 1. We focus solely on collision resistance as the "most problematic" property of cryptographic hash functions. Moreover, the results of our analysis are mostly negative, so there is no need to study other properties.

The paper is structured as follows. Section 2 contains notions and definitions used in the paper. In addition, we present our model of high-rate compression functions. In Section 3 we give an upper bound for rate of collision resistant compression functions in the model. The analysis of rate-2 compression functions is presented in Section 4.

2 Background and Definitions

The notation used in the paper follows closely the notation introduced in [1, 2]. Let V_m be a set of all m-ary binary vectors, i.e. $V_m = \{0,1\}^m$. Let k and n be positive integers. A block cipher is a function $E : V_k \times V_n \to V_n$, where for each key $K \in V_k$, the function $E_K(\cdot) = E(K, \cdot)$ is a permutation on V_n. Let $\mathrm{Bloc}(k, n)$ be the set of all block ciphers $E : V_k \times V_n \to V_n$. The inverse of block cipher E is denoted by E^{-1}.

A (block cipher based) compression function is a function $f : \mathrm{Bloc}(k, n) \times (V_a \times V_b) \to V_c$, where a, b, and c are positive integers such that $a + b \geq c$. An iterated hash of compression function $f : \mathrm{Bloc}(k, n) \times (V_a \times V_b) \to V_a$ is the hash function $H : \mathrm{Bloc}(k, n) \times V_b^* \to V_a$ defined by $H^E(m_1 \dots m_l) = h_l$, where $h_i = f^E(h_{i-1}, m_i)$ and h_0 is a fixed element from V_a. We set $H^E(\varepsilon) = h_0$ for empty string ε. We often omit superscripts E to f and H. If the computation of $f^E(h, m)$ uses e queries of E then f (and its iterated hash H) is rate-r, where $r = (b/n)/e$. Often $n \mid b$, and the rate represents the average number of message blocks processed by single E transformation. For example, for $b/n = 3$ and $e = 2$ we get compression function of rate-(3/2).

The experiment of choosing a random element x from the finite set S will be denoted by $x \xleftarrow{\$} S$.

Black-box model. An adversary A is given access to oracles E and E^{-1} where E is a block cipher. We write these oracles as superscripts, i.e. $A^{E,E^{-1}}$. We omit the superscripts when the oracles are clear from context. The adversary's task is attacking the collision resistance of a hash function H. We measure the adversary's effort of finding collision as a function of the number of E or E^{-1} queries it makes. Notice that we assume information-theoretic adversary, i.e. the computational power of the adversary is not limited in any way.

Attacks in this model treat the block cipher as a black box. The only structural property of the block cipher captured by the model is the invertibility. The model cannot guarantee the security of block cipher based hash functions instantiated with block ciphers having significant structural properties (e.g. weak keys). On the other hand, the black-box model is stronger that treating the block cipher as a random function, because the adversary's ability to compute E^{-1}.

We define the advantage of an adversary in finding collisions in a compression function $f : \mathrm{Bloc}(k,n) \times (V_a \times V_b) \to V_c$. Naturally (h,m) and (h',m') collide under f if they are distinct and $f^E(h,m) = f^E(h',m')$. We also take into account a collision with empty string, i.e. producing (h,m) such that $f^E(h,m) = h_0$. We look at the number of queries that the adversary makes compare this with the probability of finding a collision.

Definition 1 (Collision resistance of a compression function [2]). *Let f be a block cipher based compression function, $f : \mathrm{Bloc}(k,n) \times (V_a \times V_b) \to V_c$. Fix a constant $h_0 \in V_c$ and an adversary A. Then the advantage of finding collisions in f is the probability*

$$\mathbf{Adv}_f^{\mathrm{comp}}(A) = \Pr\Big[E \xleftarrow{\$} \mathrm{Bloc}(k,n);\ ((h,m),(h',m')) \leftarrow A^{E,E^{-1}} : \\ (h,m) \neq (h',m') \wedge f^E(h,m) = f^E(h',m') \vee f^E(h,m) = h_0\Big]$$

For $q \geq 0$ we write $\mathbf{Adv}_f^{\mathrm{comp}}(q) = \max_A\{\mathbf{Adv}_f^{\mathrm{comp}}(A)\}$ where the maximum is taken over all adversaries that ask at most q oracle (E or E^{-1}) queries.

Definition 2 (Collision resistance of a hash function [2]). *Let H be a block cipher based hash function, and let A be an adversary. Then the advantage of finding collisions in H is the probability*

$$\mathbf{Adv}_H^{\mathrm{coll}}(A) = \Pr\Big[E \xleftarrow{\$} \mathrm{Bloc}(k,n);\ (M,M') \leftarrow A^{E,E^{-1}} : \\ M \neq M' \wedge H^E(M) = H^E(M')\Big]$$

For $q \geq 0$ we write $\mathbf{Adv}_H^{\mathrm{coll}}(q) = \max_A\{\mathbf{Adv}_H^{\mathrm{coll}}(A)\}$ where the maximum is taken over all adversaries that ask at most q oracle (E or E^{-1}) queries.

The following theorem forms a basis for construction of iterated hash functions (Merkle-Damgård paradigm). It shows that the collision resistance of compression function is sufficient for the collision resistance of its iterated hash function.

Theorem 1 (Merkle-Damgård [3, 5]). *Let* $f : \mathrm{Bloc}(k, n) \times V_n \times V_n \to V_n$ *be a compression function and let* H *be an iterated hash of* f*. Then* $\mathbf{Adv}_H^{\mathrm{coll}}(q) \leq \mathbf{Adv}_f^{\mathrm{comp}}(q)$ *for any* $q \geq 1$*.*

Remark 2. Birthday attack is a generic collision-finding attack on a compression/hash function. The advantage of birthday attack is $\Theta(q^2/2^n)$, where q is number of evaluations of the function and n is the length of output. Usually, a compression function f (hash function H) is called collision resistant up to the birthday-attack bound, or simply collision resistant if $\mathbf{Adv}_f^{\mathrm{comp}}(q) = \Theta(q^2/2^n)$ ($\mathbf{Adv}_H^{\mathrm{coll}}(q)) = \Theta(q^2/2^n)$).

2.1 A Model of High-Rate Compression Function

We define a model of high-rate compression function $f : \mathrm{Bloc}(k, n) \times (V_a \times V_b) \to V_a$. The model assumes following:

- The evaluation of compression function f uses a single query E to compute $f(h, m)$.
- The length of m is an integer multiple of the E's block length n, i.e. $b = rn$ where $r \geq 1$.

According to the second condition the compression function is rate-r. Let $f_1 : V_a \times V_{rn} \to V_n$, $f_2 : V_a \times V_{rn} \to V_k$, and $f_3 : V_a \times V_{rn} \times V_n \to V_a$ be arbitrary functions. The computation of the compression function $f : \mathrm{Bloc}(k, n) \times (V_a \times V_{nr}) \to V_a$ is defined as:

$$
\begin{aligned}
&\textbf{function } f^E(h, m):\\
&X \leftarrow f_1(h, m)\\
&K \leftarrow f_2(h, m)\\
&Y \leftarrow E(K, X)\\
&\textbf{return } f_3(h, m, Y)
\end{aligned}
$$

When convenient we express m as a concatenation of n bit blocks. These r blocks are denoted by $m^{(1)}, \ldots, m^{(r)}$. Our model of high-rate compression function used in iterated hash is depicted in Fig. 1.

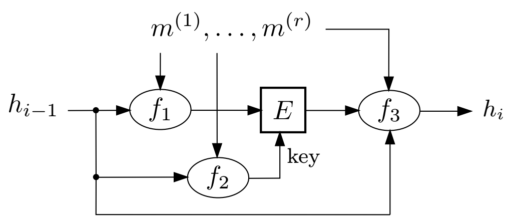

Fig. 1. Model of high-rate compression function

The model is quite general – it covers all compression functions that takes r blocks of a message and process them using exactly one encryption transformation E. Notice that all rate-1 schemes from [6] (we call them PGV) are special instances of the model.

3 An Upper Bound for the Rate of Compression Function

In the following theorem, we present an attack on collision resistance of compression function. This attack works on any compression function belonging to the model. As a by-product we obtain an upper bound for rate of any collision resistant compression function.

Theorem 2 (Upper bound for rate of a compression function). *Let* $E \in \mathrm{Bloc}(n,k)$. *Let* $f_1 : V_a \times V_{rn} \to V_n$, $f_2 : V_a \times V_{rn} \to V_k$, *and* $f_3 : V_a \times V_{rn} \times V_n \to V_a$ *be arbitrary functions. Let* $f : V_a \times V_{rn} \to V_a$ *be a compression function defined as* $f(h,m) = f_3(h,m,E_{f_2(h,m)}(f_1(h,m)))$. *Let* $r > 1 + k/n$. *Then* $\mathbf{Adv}_f^{\mathrm{comp}}(1) = 1$.

Proof. We describe an adversary A that asks exactly one oracle query. For any $X \in V_n$, and $K \in V_k$ we denote by $D_{X,K}$ the set of all pairs (h,m) such that $f_1(h,m) = X$, and $f_2(h,m) = K$, i.e. $D_{X,K} = f_1^{-1}(X) \cap f_2^{-1}(K)$. Adversary A proceeds as follows:

1. A finds such $X \in V_n$, and $K \in V_k$ that $|D_{X,K}|$ is maximal.
2. A computes $Y = E_K(X)$.
3. A finds a collision in the set $D_{X,K}$, i.e. $(h,m),(h',m') \in D_{X,K}$: $(h,m) \neq (h',m') \;\wedge\; f_3(h,m,Y) = f_3(h',m',Y)$.

One can easily check that (h,m) and (h',m') form a collision for compression function f:

$$\begin{aligned} f(h,m) &= f_3(h,m,E_{f_2(h,m)}(f_1(h,m))) = f_3(h,m,E_K(X)) = \\ &= f_3(h',m',E_K(X)) = f_3(h',m',E_{f_2(h',m')}(f_1(h',m'))) = f(h',m') \end{aligned}$$

Now, we argue that A succeeds in the third step of the attack. First, we show that $|D_{X,K}| \geq 2^{a+n(r-1)-k}$. Let us assume the opposite holds: $|D_{X,K}| < 2^{a+n(r-1)-k}$ for all $X \in V_n$, $K \in V_k$. Then

$$\sum_{X \in V_n,\, K \in V_k} |D_{X,K}| < 2^{n+k} \cdot 2^{a+n(r-1)-k} = 2^{a+nr}.$$

On the other hand

$$\sum_{X \in V_n,\, K \in V_k} |D_{X,K}| = \sum_{X \in V_n} \sum_{K \in V_k} |f_1^{-1}(X) \cap f_2^{-1}(K)| = \sum_{X \in V_n} |f_1^{-1}(X)| = 2^{a+nr},$$

a contradiction. Thus, the adversary selects X, K with $|D_{X,K}| \geq 2^{a+n(r-1)-k}$ in the first step of the attack. Since the range of compression function f has 2^a

elements (the range is the same as the range of f_3), the adversary succeeds in finding collision if $|D_{X,K}| > 2^a$. The inequality is satisfied if $2^{a+n(r-1)-k} > 2^a$, or equivalently $r > 1 + k/n$.

Adversary A produces a collision in compression function f with probability 1 (assuming $r > 1 + k/n$). Moreover, the adversary asks exactly one oracle (E) query during the attack. Thus, $\mathbf{Adv}_f^{\mathrm{comp}}(1) = 1$. □

Remark 3. Recall that the adversary was not computationally limited and the attack has exponential time complexity (more precisely, steps 1 and 3).

The theorem gives an upper bound $1 + k/n$ for the rate of collision resistant compression function. Compression functions with higher rate cannot be collision resistant (at least compression functions in our model). However, the theorem says nothing about collision resistance of compression functions with rate $r \leq 1 + k/n$. A natural question is whether this upper bound for collision resistant compression functions can be achieved. A negative answer for a class of compression functions is given in the following section.

4 PGV-like Rate-2 Compression Functions

The constructions of compression functions from block cipher often assume equal key and block lengths [6], i.e. $k = n$. Then the upper bound from Theorem 2 simplifies to $r \leq 2$. Similarly, the output of compression function has usually the same length as the block, i.e. $a = n$. Thus, we consider rate-2 compression functions of the form $f : V_n \times V_{2n} \to V_n$.

Preneel, Govaerts, and Vandewalle [6] studied rate-1 compression functions. They considered all 64 compression functions f of the form $f(h, m) = E_a(b) \oplus c$ where $a, b, c \in \{h, m, h \oplus m, v\}$ (v is a fixed constant). As showed in [2], 12 compression function are collision resistant, and additional 8, though not collision resistant, form collision resistant hash functions.

A natural extension of above constructions to the case of rate-2 compression functions is the following scheme:

$$f(h, (m^{(1)}, m^{(2)})) = E_a(b) \oplus c, \tag{1}$$

where $a, b, c \in \{h, m^{(1)}, m^{(2)}, h \oplus m^{(1)}, h \oplus m^{(2)}, m^{(1)} \oplus m^{(2)}, h \oplus m^{(1)} \oplus m^{(2)}, v\}$. This way we obtain 512 compression functions.

Remark 4. Notice that the compression functions instantiated in the scheme fall in our model – $f_1(h, m) = b$, $f_2(h, m) = a$, and $f_3(h, m, Y) = Y \oplus c$.

We show that no compression function of the form (1) is collision resistant (for any function there exists an adversary that finds a collision and asks at most two queries). We partition these functions into distinct classes according attacks that find (at least one) collision. Summary of the classes is given in Table 1. For each class the table shows the number of compression functions in the class, and the number of oracle queries needed in collision finding attack.

Table 1. Collision classes of rate-2 compression functions

class	functions	queries
1 – Superfluous Variables	169	0
2 – Balanced Combinations	133	0
3 – Compensations	150	2
4 – "Hard" Core	60	$2, 0$

Remark 5. There are compression functions that are vulnerable to multiple attacks using e.g. superfluous variables or balanced combinations. In such situation we assign particular function to the class with lowest number.

4.1 Class 1 – Superfluous Variables

First class contains all those compression functions that do not depend on all input vectors, i.e. at least one of h, $m^{(1)}$, $m^{(2)}$ is not required for computing the function. Examples of such compression functions are $E_h(h \oplus m^{(1)}) \oplus h$, $E_{m^{(2)}}(v) \oplus m^{(1)} \oplus m^{(2)}$, or $E_v(h \oplus m^{(2)}) \oplus h \oplus m^{(2)}$. Trivially, one can find many collisions in compression functions from this class. It suffices to vary the superfluous variable. Moreover, no oracle queries are needed to produce collisions.

4.2 Class 2 – Balanced Combinations

Our second class consists of those compression functions that are not in class 1, and have a balanced combination of two input vectors. Let $x_1, x_2 \in \{h, m^{(1)}, m^{(2)}\}$ be two distinct input vectors, i.e. $x_1 \neq x_2$. We call a combination $x_1 \oplus x_2$ balanced in compression function f, if every occurrence of x_1 in f's parameters a, b or c implies x_2 occurrence in the same parameters (and vice versa). Examples of compression functions in this class are:

$$E_{h \oplus m^{(1)} \oplus m^{(2)}}(m^{(1)} \oplus m^{(2)}) \oplus v,$$
$$E_{m^{(2)}}(h \oplus m^{(1)}) \oplus h \oplus m^{(1)},$$
$$E_{h \oplus m^{(2)}}(h \oplus m^{(1)} \oplus m^{(2)}) \oplus h \oplus m^{(1)} \oplus m^{(2)}.$$

It can be easily seen that collisions can be find without any oracle queries. Balanced combination $x_1 \oplus x_2$ allows choosing 2^n values pairs (x_1, x_2) without changing parameters a, b, and c. Hence, the value of f does not change either.

4.3 Class 3 – Compensations

Third class of compression functions contains those functions (not in classes 1 and 2) that have some input vector solely in either parameter b or parameter c.

Let $x \in \{h, m^{(1)}, m^{(2)}\}$ be such input vector. Let x appears only in f's parameter b, i.e. input of block cipher transformation. An adversary can find collision in the following way. He sets the output of f to some fixed value z. Similarly he sets the values of all input vectors except x randomly. Using a query to E^{-1} oracle the adversary can compute "suitable" x value. Repeating this procedure for different random choice of input vectors values and the same fixed z, the adversary obtains a collision for f. The situation for x appearing solely in parameter c is treated analogously.

Examples of compression functions in this class are:

$$E_{m^{(2)}}(m^{(1)}) \oplus h \oplus m^{(2)},$$
$$E_{m^{(1)}}(m^{(2)}) \oplus h \oplus m^{(1)} \oplus m^{(2)},$$
$$E_{h \oplus m^{(1)}}(m^{(1)} \oplus m^{(2)}) \oplus v.$$

4.4 Class 4 – "Hard" Core

There are 60 compression functions left after sorting the functions into classes 1, 2, and 3. Let us denote this set C. We call two functions f_1, f_2 permutation-equivalent, if f_1 can be obtained from f_2 by some permutation of its inputs. It can be easily observed that $\mathbf{Adv}^{\mathrm{comp}}_{f_1}(q) = \mathbf{Adv}^{\mathrm{comp}}_{f_2}(q)$ for any permutation-equivalent compression functions f_1, f_2, and any $q \geq 0$. Therefore the set C can be partitioned to equivalence classes. Since every equivalence class has 6 members, it suffices to analyze the collision resistance of any 10 permutation-nonequivalent compression functions (each one drawn from different equivalence class). One selection of these 10 functions is shown in Table 2.

Table 2. Permutation-nonequivalent compression functions of "hard" core class

i	a	b	c
1	$m^{(1)} \oplus m^{(2)}$	h	$h \oplus m^{(2)}$
2	$m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(2)}$	h
3	$m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(2)}$	$h \oplus m^{(2)}$
4	$m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(2)}$	$h \oplus m^{(1)}$
5	$m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(2)}$	$h \oplus m^{(1)} \oplus m^{(2)}$
6	$m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(2)}$
7	$h \oplus m^{(1)} \oplus m^{(2)}$	$m^{(2)}$	$m^{(1)}$
8	$h \oplus m^{(1)} \oplus m^{(2)}$	$m^{(2)}$	$m^{(1)} \oplus m^{(2)}$
9	$h \oplus m^{(1)} \oplus m^{(2)}$	$m^{(1)} \oplus m^{(2)}$	$m^{(2)}$
10	$h \oplus m^{(1)} \oplus m^{(2)}$	$m^{(1)} \oplus m^{(2)}$	$h \oplus m^{(2)}$

Now we show collisions in all 10 permutation-nonequivalent compression functions. Hence, all 60 functions from set C are not collision resistant. We refer compression functions from Table 2 as $f_1, \ldots, f_{10}$. For brevity, let 0 (1) be all-zero (all-one) vector in V_n, respectively. Let A be following collision finding adversary:

1. A sets $(h, m^{(1)}, m^{(2)}) = (0, 0, 0)$, i.e. $f_i(h, m^{(1)}, m^{(2)}) = E_0(0)$.
2. A asks two oracle queries and computes $x = E_0(0) \oplus E_1(0)$.
3. A solves following equations (a', b', c' denote corresponding linear combinations of h', $m'^{(1)}$, $m'^{(2)}$ for compression function f_i):

$$\begin{aligned} a' &= 1 \\ b' &= 0 \\ c' &= x \end{aligned}$$

   For any solution $(h', m'^{(1)}, m'^{(2)})$ we have $f_i(h', m'^{(1)}, m'^{(2)}) = E_{a'}(b') \oplus c' = E_1(0) \oplus E_0(0) \oplus E_1(0) = E_0(0)$. Hence any solution different from $(0, 0, 0)$ yields a collision.

Let us illustrate adversary's computation on f_1. Adversary A solves following equations in step 3:

$$\begin{aligned} m'^{(1)} \oplus m'^{(2)} &= 1 \\ h' &= 0 \\ h' \oplus m'^{(2)} &= x \end{aligned}$$

Solution is $(h', m'^{(1)}, m'^{(2)}) = (0, 1 \oplus x, x) \neq (0, 0, 0)$, and A obtains a collision.

Adversary A can successfully find collisions for all functions $f_1, \ldots, f_{10}$, see Table 3, except for f_3 and f_4 due to the linear dependence of a', b', and c'. We produce collisions for these functions separately (moreover, no oracle queries are needed). It can be easily verified that $f_3(0, 0, 0) = f_3(1, 1, 1)$, and $f_4(0, 0, 0) = f_4(1, 1, 1)$.

Summarizing attacks from this section we obtain following theorem:

Theorem 3. *Let $E \in \mathrm{Bloc}(n, k)$. Let $f : V_n \times V_{2n} \to V_n$ be a compression function defined as $f(h, (m^{(1)}, m^{(2)})) = E_a(b) \oplus c$, where $a, b, c \in \{h, m^{(1)}, m^{(2)}, h \oplus m^{(1)}, h \oplus m^{(2)}, m^{(1)} \oplus m^{(2)}, h \oplus m^{(1)} \oplus m^{(2)}, v\}$. Then $\mathbf{Adv}_f^{\mathrm{comp}}(2) = 1$.*

Remark 6. The attacks presented in this section do not use the full strength of black-box model – a computationally unbounded adversary. These attacks require just polynomially bounded adversary asking constant number oracle queries.

5 Conclusion

Many interesting questions arise from the results presented in the paper. We state two most prominent ones as open problems:

1. Are there any collision resistant compression functions with rate > 1?

Table 3. Collisions for $(0, 0, 0)$ produced by adversary A

i	h'	$m'^{(1)}$	$m'^{(2)}$
1	0	$1 \oplus x$	x
2	x	$1 \oplus x$	x
3	$-$	$-$	$-$
4	$-$	$-$	$-$
5	$1 \oplus x$	x	$1 \oplus x$
6	1	x	$1 \oplus x$
7	$1 \oplus x$	x	0
8	$1 \oplus x$	x	0
9	1	x	x
10	1	$1 \oplus x$	$1 \oplus x$

2. Collision resistance of compression function is sufficient, but not necessary condition for collision resistance of iterated hash [2]. Are there any PGV-like rate-2 compression functions that result in collision resistant iterated hash function?

References

1. Black, J., Cochran, M., Shrimpton, T.: On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions, In *Advances in Cryptology – Eurocrypt '05*, LNCS 3494, Springer-Verlag, 2005.
2. Black, J., Rogaway, P., Shrimpton, T.: Black-box analysis of the block-cipher-based hash-function constructions from PGV, In *Advances in Cryptology – CRYPTO '02*, LNCS 2442, Springer-Verlag, 2002.
3. Damgård, I.: A design principle for hash functions, In *Advances in Cryptology – CRYPTO '89*, LNCS 435, Springer-Verlag, 1990.
4. Handschuh, H., Knudsen, L., Robshaw, M.: Analysis of SHA-1 in encryption mode, In *Advances in Cryptology – CT-RSA '01*, LNCS 2020, Springer-Verlag, 2001.
5. Merkle, R.: One way hash functions and DES, In *Advances in Cryptology – CRYPTO '89*, LNCS 435, Springer-Verlag, 1990.
6. Preneel, B., Govaerts, R., Vandewalle, J.: Hash functions based on block ciphers: A synthetic approach, In *Advances in Cryptology – CRYPTO '93*, LNCS 773, Springer-Verlag, 1994.