# FL Construction Hash Functions From PGV

**Abstract.** Preneel,Govaerts, and Vandewalle[6] considered the 64 most basic ways to construct a hash function $H : \{0,1\}^* \to \{0,1\}^n$ from a block cipher $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. They regarded 12 of those 64 schemes as secure. Black, Rogaway and Shrimption[4] provided a formal and quantitative treatment of the 64 constructions considered by PGV and prove that, in black-box model, there are 20 of those schemes that are collision resistant. Here we consider those 64 schemes to construct a hash function from FL-Cipher $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$[2]. We prove that, in black-box model, 24 schemes of those 64 schemes are secure. Nonetheless, we prefer format1 schemes to other format to construct a hash function for given FL-Cipher.

keywords: Hash Function, Block Cipher, Feistel Structure

## 1 Introduction

Almost all known hash functions are based on a compression function with fixed size input and called an "iterated" hash function. The iterated hash functions have been divided into four classes[3]: hash function based on a block cipher, hash functions based on modular arithmetic, hash functions based on a knapsack and dedicated hash functions.

Constructing a hash function based on block cipher is turning a block cipher $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ in to a hash function $H : \{0,1\}^* \to \{0,1\}^n$ using a compression function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ derived from $E$. For $v$ a fixed $n$-bit constant, the compression function $f$ has the form of 64 schemes $f(h_{i-1}, m_i) = E_a(b) \oplus c$ where $a, b, c \in \{h_{i-1}, m_i, h_{i-1} \oplus m_i, v\}$. Preneel,Govaerts, and Vandewalle[6][6] discussed the probabilities of building a hash function using those 64 schemes and made a conclusion that 12 of 64 schemes are secure. Black, Rogaway and Shrimption[4] improved the result, where 20 of those 64 schemes are secure.

We presented a new type of iterated hash function in paper[2], its compression function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ has modified Feistel Structure and block cipher's round function, we called the compression function "FL-Cipher" and called the iterated hash function "FL-Construction hash function". We proved that FL-Cipher is a good compression function and FL-Construction is a OWHF and CRHF, in black-box model. Nonetheless, we only considered the condition that the compressing function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is in format of $f(h_{i-1}, m_i) = F(h_{i-1}, m_i)$.

Here we consider those 64 schemes to construct a hash function from FL-Cipher $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. We prove that, in black-box model, 24

schemes of those 64 schemes are secure and those 24 schemes are divided into 4 class. Nonetheless, we prefer format1 schemes to other format to construct a hash function for given FL-Cipher.

The paper is organized as follows. The mathematical preliminaries and notation employed are described in section2. Specification of FL-Cipher and FL-Construction are given in section3. The summary of our result is presented in section4 and section5 is our conclusion.

## 2 Definition

### 2.1 The Feistel Like Structure

A Feistel structure is a general way of constructing block ciphers from simple functions. The original idea was used in the block cipher, invented by Horst Feistel. Let Feistel structure be adopted in a block cipher with round function $f$. Let $x^L_{(r)}, x^R_{(r)}$ be the left and the right halves of the $r$ round inputs, The Feistel structure of block cipher is written as:

$$x^L_{(r+1)} = x^L_{(r)} \oplus f(x^R_{(r)}, k_{(r)}) \tag{1}$$

$$x^R_{(r+1)} = x^L_{(r)} \tag{2}$$

The security of the Feistel structure is not obvious, but analysis of DES[7] has shown that it is a good way to construct ciphers. And some new ciphers based on Feistel structure of SPN function have been discussed recently and no weakness is found in Feistel structure itself. In this section we give a modified structure of Feistel named Feistel like structure and call FL-structure.

**Definition 1.** *Let $f$ be round function, $x_{(r)}$ be the rth round inputs, $x_{(1)}$ be the input sequence, then the FL-Structure is defined as Eq.(3), Eq.(4).*

$$x_{(2)} = f(x_{(1)}, k_{(1)}) \tag{3}$$

$$x_{(r+1)} = x_{(r-1)} \oplus f(x_{(r)}, k_{(r)}) \tag{4}$$

Put simply, the standard Feistel network takes a function from $n$ bits to $n$ bits and produces an invertible function from $2n$ bits to $2n$ bits. FL-Structure takes a function from $n$ bites to $n$ bites and produces a one-way function from $n$ bits to $n$ bites. Figure illustration is given in Fig.1.

### 2.2 The FL-Construction

A block cipher is a map $E : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$ for each $k \in \{0,1\}^\kappa$, where the round function of $E$ is a map of $f : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, the functions $E_k(\cdot) = E(\cdot, k)$ is transformation on $\{0,1\}^n$. If $E$ is a permutation then $E^{-1}$ is its inverse, where $E^{-1}_k(y)$ is the string $x$ such that $E_k(x) = y$. We write $x \xleftarrow{\$} S$ for the experiment of choosing a random element from the finite set $S$ and calling it $x$. An adversary is an algorithm with access to one or more oracles.

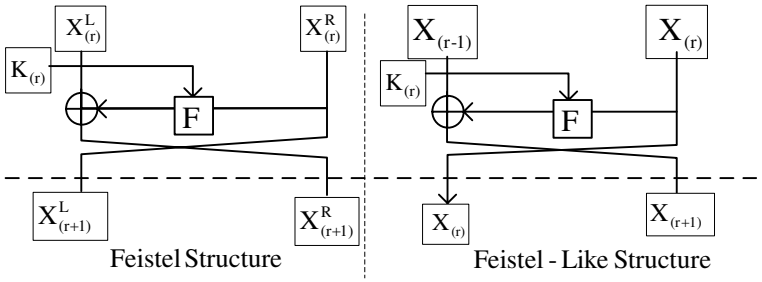


**Fig. 1.** Construct Between Feistel Structure and FL-Sreucture

**Definition 2** (*Block*$(n, \kappa)$)**.** *Let $E$ be block cipher $E : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, $f$ be round function, Block$(n, \kappa)$ is the set of all block cipher with form of $E$, where $E$ has form of Eq(5) and its round function $f$ is a permutation.*

$$x_{(r+1)} = f(x_{(r)}, k_{(r)}),\ r = 1, ..., R \tag{5}$$

**Definition 3 (FL-Cipher).** *Let $E \in Block(n, \kappa)$ be a $A$ block cipher, let $f$ be round function of $E$ and let $R$ be rounds of $E$. Then we called $F$ is FL-Cipher based on $E$, if $y = F(x, k)$ has the form of that:*

$$x_{(2)} = f(x_{(1)}, k_{(1)}) \tag{6}$$

$$x_{(r+1)} = x_{(r-1)} \oplus f(x_{(r)}, k_{(r)}), r = 1, ..., R' \tag{7}$$

**Definition 4 (Feistel Cipher and FL-Cipher).** *Let $F$ be FL-Cipher hash function with round function $f$ and rounds $R$, $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, $\widetilde{E} : \{0,1\}^{2n} \times \{0,1\}^\kappa \to \{0,1\}^{2n}$ be Feistel block cipher with round function $f$ and rounds $R$, then we call that $F$ is instance of $\widetilde{E}$.*

**Definition 5 (FL-Construction).** *Let $Feist(n, \kappa)$ be the set of all FL-Cipher $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$ with no weak hash key. We call the iterated hash function is a FL-Construction hash function, if the iterated hash function $H$'s compression function is a FL-Cipher and denoted $H_F$.*

### 2.3 Definition of Collision Resistant

There are many kinds of descriptions and notations about hash function, we use the descriptions given by John Black[4].

To quantify the collision resistance of a hash function $H_F$, we instantiate the compression function by a randomly chosen $F \in Feist(n, \kappa)$ with round function $f$. An adversary A is given oracles for $F(\cdot, \cdot)$ and wants to find a collision for $H_F$ that is, $M, M'$ where $M \neq M'$ but $H_F(M) = H_F(M')$. We look at the number of queries that the adversary makes and compare this with the probability of finding a collision.

**Definition 6 (Collision resistance[4]).** *Let $H_F$ be a FL-Construct hash function, $H_F : Feist(n,\kappa) \times \mathcal{D} \to \mathcal{R}$, and let $A$ be an adversary. Then the advantage of $A$ in finding collisions in $H_F$ is the real number*

$$Adv^{coll}_{H_F}(A) = Pr[F \xleftarrow{\$} Feist(n,\kappa); (M, M') \leftarrow A^F :$$

$$M \neq M' \wedge H_F(M) = H_F(M')].$$

For $q \geq 1$ we write $Adv^{coll}_{H_F}(q) = max_A\{Adv^{coll}_{H_F}(A)\}$ where the maximum is taken over all adversaries that ask at most $q$ oracle queries. Other advantage functions are silently extended in the same way.

**Definition 7 (Conventional definition of a OWF[4]).** *Let $H_F$ be hash function, $H_F : Feist(n,\kappa) \times \mathcal{D} \to \mathcal{R}$, and let $l$ be a number such that $\{0,1\}^l \subseteq \mathcal{D}$. Let $A$ be an adversary. Then the advantage of $A$ in inverting $H_F$ on the distribution induced by applying $H_F$ to a random $l$-bit string is the real number.*

$$Adv^{owf}_{H_F}(A) = Pr[F \xleftarrow{\$} Feist(n,\kappa); M \xleftarrow{\$} (\{0,1\}^n)^l; \sigma \xleftarrow{\$} H_F(M);$$

$$M' \leftarrow A^F(\sigma) : H_F(M') = \sigma].$$

We also define the advantage of an adversary in finding collisions in a FL-Cipher. Naturally $(k,m)$ and $(k',m')$ collide under $F$ if they are distinct and $F(k,m) = F(k',m')$.

**Definition 8 (Collision resistance of FL-Cipher).** *Let $F$ be a FL-Cipher $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, and let $A$ be an adversary. Then the advantage of $A$ in finding collisions in $F$ is the real number.*

$$Adv^{coll}_{F}(A) = Pr[F \xleftarrow{\$} Feist(n,\kappa); ((m,k),(m',k')) \leftarrow A^F :$$

$$(m \neq m' \vee k \neq k') \wedge F_k(m) = F_{k'}(m')].$$

**Definition 9 (One Way of FL-Cipher).** *Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, and let $A$ be an adversary. Then the advantage of $A$ in inverting $F$ on the distribution induced by applying $F$ is the real number.*

$$Adv^{owf}_{F}(A) = Pr[F \xleftarrow{\$} Feist(\kappa,n); k \xleftarrow{\$} \{0,1\}^\kappa; m \xleftarrow{\$} \{0,1\}^n; \sigma \xleftarrow{\$} F_k(m);$$

$$m' \leftarrow A^F(\sigma) \vee k' \leftarrow A^F(\sigma) : F_k(m) = F_k(m') \vee F_k(m) = F_{k'}(m)].$$

**Definition 10 (Inverting random points of FL-Cipher).** *Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, and let $A$ be an adversary. Then the advantage of $A$ in inverting $F$ is the real number.*

$$Adv^{inv}_{F}(A) = Pr[F \xleftarrow{\$} Feist(\kappa,n); \sigma \xleftarrow{\$} \{0,1\}^n;$$

$$(m,k) \leftarrow A^F(\sigma) : F_k(m) = \sigma].$$

## 3 Specification of FL-Cipher

### 3.1 Properties of Feistel Block Cipher and FL-Cipher

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a FL-Cipher, $\widetilde{E} : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^{2n}$ be a Feistel block cipher and $F$ is instance of $\widetilde{E}$. Let $Pr[k, m \xleftarrow{\$} \{0,1\}^n; y \leftarrow \{0,1\}^n : f_k(m) = y]$ means the probability of random selected $y$ satisfy equation $f_k(m) = y$ for a constant $m$ and $k$, $Pr[k, m \xleftarrow{\$} \{0,1\}^n; y \xleftarrow{\$} \{0,1\}^n : f_k(m) = y]$ means the probability of a selected $y$ satisfy equation $f_k(m) = y$ for a constant $m$ and $k$. There are some notations which will be used in following descriptions. Let $(m_1 \| m_2)$ be concatenate of $m_1$ and $m_2$, $Ri(m, n)$ is the right $n$ bits of sequence $m$ and $\Delta_k(m)$ be $\widetilde{E}_k(m \| f_k(m))$. Let $(3 \| y)$ be $(0_1 ... 0_{n-2} 11 \| y)$.

**Definition 11 (No Weak Hash Key).** *Let $F$ be FL-Cipher, $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, and $F$ is instance of $\widetilde{E} : \widetilde{E}_k(m \| m') = (y' \| y)$, if there are*

$$Pr[m, m', y, y' \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : \widetilde{E}_k(m \| m') = (y' \| y)] \cdot 2^n = O(1) \quad (8)$$

*we call the $\widetilde{E}$ has no weak hash key.*

**Definition 12 (No Weak Hash Key).** *Let $F$ be FL-Cipher, $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, and $F$ is instance of $\widetilde{E} : \widetilde{E}_k(m \| m') = (y' \| y)$, if there are*

$$\max(Pr[m, y \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m \| f_k(m)), n) = y]) \cdot 2^n = O(1) \quad (9)$$

*we call the FL-Cipher $F$ has no weak hash key.*

**Lemma 1.** *For a permutation $\widetilde{E}_k : \widetilde{E}_k(m \| m') = (y' \| y)$ and its inverse $\widetilde{E}_k^{-1} : \widetilde{E}_k(y \| y') = (m' \| m)$, we have*

1. $Pr[k, y, y' \xleftarrow{\$} \{0,1\}^n; (m, m') \leftarrow \{0,1\}^n : \widetilde{E}_k(m \| m') = (y' \| y)] = 2^{-2n}$;
2. $Pr[m, k, m' \xleftarrow{\$} \{0,1\}^n; (y, y') \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y' \| y) = (m \| m')] = 2^{-2n}$;

**Lemma 2.** *For block cipher $\widetilde{E} : \widetilde{E}_k(m \| m') = (y' \| y)$ and its inverse $\widetilde{E}_k^{-1} : \widetilde{E}_k(y \| y') = (m' \| m)$, if $\widetilde{E}$ has no weakness, we have*

1. $\max(Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m \| m'), n) = y] \cdot 2^n) = O(1)$;
2. $\max(Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; y', m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k^{-1}(y' \| y), n) = m \| m'] \cdot 2^n) = O(1)$;

*Proof.* Let $p \stackrel{\triangle}{=} \max_{k,y,m'} Pr[m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m \| m'), n) = y]$ and let when $m' = i', k = j, y = t$ we get the max probability, that means for block cipher $\widetilde{E}$ we can find two plaintext $(i_1 \| i')$ and $(i_2 \| i')$ that $\widetilde{E}_j(i_1 \| i')$ and $\widetilde{E}_j(i_2 \| i')$ has only $2^n - p$ bits different. From the design criteria of block cipher we know p should be satisfy $p = O(1)$. □

**Lemma 3.** *For block cipher* $\widetilde{E} : \widetilde{E}_k(m\|m') = (y'\|y)$ *and its inverse* $\widetilde{E}_k^{-1} : \widetilde{E}_k(y\|y') = (m'\|m)$*, if* $\widetilde{E}$ *has no weakness and has no weak hash key, we have*

1. $\max(Pr[m, y, m' \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) = y] \cdot 2^n) = O(1)$;
2. $\max(Pr[m, y, m' \xleftarrow{\$} \{0,1\}^n; y', k \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y'\|y) = (m\|m')] \cdot 2^n) = O(1)$;

**Lemma 4.** *For block cipher* $\widetilde{E} : \widetilde{E}_k(m\|m') = (y'\|y)$ *and its inverse* $\widetilde{E}_k^{-1} : \widetilde{E}_k(y\|y') = (m'\|m)$*, if* $\widetilde{E}$ *has no weakness,* $m$ *and* $Ri(\widetilde{E}_k(m\|f_k(m)))$ *are independent, then we have*

1. $max(Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) \oplus m = y] \cdot 2^n) = O(1)$;
2. $max(Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; y', m \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y'\|(y \oplus m)) = m\|m'] \cdot 2^n) = O(1)$;

*Proof.*

$$
\begin{aligned}
& Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) \oplus m = y] \\
= & \sum_{i=0}^{2^n-1} Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) = y \oplus i, m = i] \\
& \text{if } m \text{ and } Ri(\widetilde{E}_k(m\|f_k(m)) \text{ are independent then} \\
= & \sum_{i=0}^{2^n-1} Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) = y \oplus i] Pr[m = i] \\
= & \, Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) = y \oplus i] \sum_{i=0}^{2^n-1} Pr[m = i] \\
\Rightarrow & \max(Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) \oplus m = y] \cdot 2^n) \\
= & \max(Pr[k, y, m' \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) = y]). \square
\end{aligned}
$$

**Lemma 5.** *For block cipher* $\widetilde{E} : \widetilde{E}_k(m\|m') = (y'\|y)$ *and its inverse* $\widetilde{E}_k^{-1} : \widetilde{E}_k(y\|y') = (m'\|m)$*, if* $\widetilde{E}$ *has no weakness,* $k$ *and* $Ri(\widetilde{E}_k(m\|f_k(m)))$ *are independent, then we have*

1. $\max(Pr[m, y, m' \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) \oplus k = y] \cdot 2^n) = O(1)$;
2. $\max(Pr[m, y, m' \xleftarrow{\$} \{0,1\}^n; k, y' \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y'\|(y \oplus k)) = m\|m'] \cdot 2^n) = O(1)$;

**Lemma 6.** *For block cipher* $\widetilde{E} : \widetilde{E}_k(m\|m') = (y'\|y)$ *and its inverse* $\widetilde{E}_k^{-1} : \widetilde{E}_k(y\|y') = (m'\|m)$*, if* $\widetilde{E}$ *has no weakness,* $m, k$ *and* $Ri(\widetilde{E}_k(m\|f_k(m)))$ *are independent, then we have*

1. $\max(Pr[y, m' \xleftarrow{\$} \{0,1\}^n; m, k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) \oplus m \oplus k = y] \cdot 2^n) = O(1)$;
2. $\max(Pr[y, m' \xleftarrow{\$} \{0,1\}^n; m, k, y' \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y'\|(y \oplus k)) = m\|m'] \cdot 2^n) = O(1)$;

*Proof.*

$$
\begin{aligned}
& Pr[y, m' \xleftarrow{\$} \{0,1\}^n; m, k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) \oplus m \oplus k = y] \\
&= \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} Pr[y, m' \xleftarrow{\$} \{0,1\}^n; m, k : Ri(\widetilde{E}_k(m\|m'), n) = y \oplus i \oplus j, m = i, k = j] \\
& \text{if } m, k \text{ and } Ri(\widetilde{E}_k(m\|f_k(m)) \text{ are independent then} \\
&= \sum_{i=0}^{2^n-1} Pr[y, m' \xleftarrow{\$} \{0,1\}^n; m, k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|m'), n) = y \oplus i] Pr[m = i] \\
&= Pr[y, m'; m, k : Ri(\widetilde{E}_k(m\|m'), n) = y \oplus i \oplus j] \sum_{i=0}^{2^n-1} Pr[m = i] \sum_{j=0}^{2^n-1} Pr[k = j]. \square
\end{aligned}
$$

Let make definitions of that

$$
\begin{aligned}
p_{1m} &\triangleq \max_{k,y}(Pr[k, y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|f_k(m)), n) = y]) \\
p_{1y} &\triangleq \max_{k,m,y}(Pr[k, m, y \xleftarrow{\$} \{0,1\}^n; y' \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k^{-1}(y'\|y), n) = m\|m']) \\
p_{2m} &\triangleq \max_{m,y}(Pr[m, y \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : Ri(\widetilde{E}_k(m\|f_k(m)), n) = y]) \\
p_{2y} &\triangleq \max_{m,y}(Pr[m, y \xleftarrow{\$} \{0,1\}^n; y', k \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y'\|y) = (m\|f_k(m))]) \\
p &\triangleq (\max(p_{1m}, p_{1y}, p_{2m}, p_{2y})) \cdot 2^n.
\end{aligned}
$$

**Lemma 7.** *Let $F$ be FL-Cipher, $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, and let $F$ is instance of $\widetilde{E}$, if $F$ has no weak hash key and there is no weakness in block cipher $\widetilde{E}$, then we have*

$$Pr[\sigma \xleftarrow{\$} \{0,1\}^n; m, k \leftarrow \{0,1\}^n : Ri(\Delta_k(m), n) = \sigma] \leq p/2^n \tag{10}$$

$$Pr[\sigma \xleftarrow{\$} \{0,1\}^n; m, k, y \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y\|\sigma) = (m|f_k(m)] \leq p/2^n \tag{11}$$

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; m' \leftarrow \{0,1\}^n : Ri(\Delta_k(m), n) = Ri(\Delta', n)] \leq p_{1m}/2^n \tag{12}$$

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; y \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y\|Ri(\Delta_k(m), n)) = m'\|f_k(m')] \leq p_{1y}/2^n \tag{13}$$

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; k' \leftarrow \{0,1\}^n : Ri(\Delta_k(m), n) = Ri(\Delta_{k'}(m), n)] \leq p_{2m}/2^n \tag{14}$$

$$Pr[m,k \xleftarrow{\$} \{0,1\}^n; k', y \leftarrow \{0,1\}^n : \widetilde{E}_{k'}^{-1}(y \| Ri(\Delta_k(m),n)) = m \| f_{k'}(m)] \leq p_{2y}/2^n \tag{15}$$

$$Pr[m,k,m',k' \leftarrow \{0,1\}^n : Ri(\Delta_k(m),n) = Ri(\Delta_{k'}(m'),n)] \leq p^2/2^n \tag{16}$$

$$Pr[m,k,m',k',y \leftarrow \{0,1\}^n : E_{k'}^{-1}(y \| Ri(\Delta_k(m),n)) = m' \| f_{k'}(m')] \leq p^2/2^n \tag{17}$$

*Proof.* the proof of Eq(10)

$$\begin{aligned}
&Pr[\sigma \xleftarrow{\$} \{0,1\}^n; m,k \leftarrow \{0,1\}^n : Ri(\Delta_k(m),n) = \sigma] \\
&\leq \max(\max_{\sigma,m} Pr[k : Ri(\Delta_k(m),n) = \sigma]), \max_{\sigma,k} Pr[m : Ri(\Delta_k(m),n) = \sigma]) \\
&= \max(p_{1m}, p_{2m})/2^n \leq p/2^n.
\end{aligned}$$

the proof of Eq(11)

$$\begin{aligned}
&Pr[\sigma \xleftarrow{\$} \{0,1\}^n; m,k,y \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y\|\sigma) = (m|f_k(m))] = 1/2^n \\
&\leq \max(\max_{\sigma,m} Pr[k,y : \widetilde{E}_k^{-1}(y\|\sigma) = (m|f_k(m))]), \max_{\sigma,k} Pr[m,y : \widetilde{E}_k^{-1}(y\|\sigma) = (m|f_k(m))]) \\
&= \max(p_{1y}, p_{2y})/2^n \leq p/2^n.
\end{aligned}$$

the proof of Eq(12)

$$\begin{aligned}
&Pr[m,k \xleftarrow{\$} \{0,1\}^n; m' \leftarrow \{0,1\}^n : Ri(\Delta_k(m),n) = Ri(\Delta',n)] \\
&= Pr[y,k \xleftarrow{\$} \{0,1\}^n; m' \leftarrow \{0,1\}^n : Ri(\Delta',n) = y] \\
&\leq \max_{\sigma,k} Pr[m : Ri(\Delta_k(m),n) = \sigma]) \\
&= p_{1m}/2^n.
\end{aligned}$$

the proof of Eq(16)

$$\begin{aligned}
&Pr[m,k,m',k' \leftarrow \{0,1\}^n : Ri(\Delta_k(m),n) = Ri(\Delta_{k'}(m'),n)] \\
&\Leftrightarrow \sum_{i=0}^{2^n-1} Pr[m,k,m',k' \leftarrow \{0,1\}^n : Ri(\Delta_k(m),n) = i, Ri(\Delta_{k'}(m'),n) = i] \\
&\Leftrightarrow \sum_{i=0}^{2^n-1} Pr[m,k : Ri(\Delta_k(m),n) = i] Pr[m',k' : Ri(\Delta_{k'}(m'),n) = i] \\
&\leq \sum_{i=0}^{2^n-1} \max(Pr[m,k : Ri(\Delta_k(m),n) = i])^2 \\
&\leq p^2/2^n. \square
\end{aligned}$$

### 3.2 Collision Resistance of FL-Cipher

In this section we discuss the hash properties of FL-Cipher.

**Theorem 1 (Inverting random points of FL-Cipher).** *Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, and let $A$ be an adversary. Then the advantage of $A$ in inverting $F$ is $Adv_F^{inv}(q) \leq pq/2^{n-1}$.*

*Proof.* Let an adversary A for $F$, adversary A takes oracle $F$ and input $\sigma$ and, when successful, it outputs $k, m$ and have

$$F(m,k) = \sigma \Leftrightarrow Ri(\widetilde{E}_k(m \| f_k(m)), n) = \sigma$$

Since we have

$$Pr[\sigma \xleftarrow{\$} \{0,1\}^n; m, k \leftarrow \{0,1\}^n : Ri(\Delta_k(m), n) = \sigma] \leq p/2^n$$

$$Pr[\sigma \xleftarrow{\$} \{0,1\}^n; m, k, y \leftarrow \{0,1\}^n : \widetilde{E}_k^{-1}(y \| \sigma) = (m | f_k(m)] \leq q/2^n$$

So we have $Adv_{F(q)}^{owf} \leq pq/2^{n-1}$. □

**Theorem 2 (One Way Property of FL-Cipher).** *Let $F$ be FL-Cipher with round function $f$, $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, then $Adv_F^{owf}(q) \leq pq/2^{n-1}$.*

*Proof.* Let an adversary A for $F$: adversary A takes oracle $F$ and input $m, k, \sigma$ and, when successful, it outputs $m'$ or $k'$ such that $F(m,k) = F(m',k)$ or $F(m,k) = F(m,k')$. If adversary A find $m'$ such that $F(m,k) = F(m',k)$ then

$$F(m,k) = F(m',k) \Leftrightarrow Ri(\widetilde{E}_k(m \| f_k(m)), n) = Ri(\widetilde{E}_k(m' \| f_k(m')), n)$$

For block cipher $\widetilde{E}$,

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; m' \leftarrow \{0,1\}^n : Ri(\Delta_k(m), n) = Ri(\Delta', n)] \leq p/2^n \quad (18)$$

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; y : \widetilde{E}_k^{-1}(y \| Ri(\Delta_k(m), n)) = m' \| f_k(m')] \leq p/2^n \quad (19)$$

For any $i \in [1..q]$, let $C_i$ be the event that the randomly selected $m_i$ from $\{0,1\}^n$, where $m_i \neq m_j$ such that $F(m,k) = F(m_i,k)$. Since $Pr(C_i) \leq p/(2^n - i)$. we thus have $Pr(c_1 \vee ... \vee c_q) \leq pq/2^{(n-1)}$.

If adversary A find $k'$ such that $F(m,k') = F(m,k)$ then

$$F(m,k) = F(m,k') \Leftrightarrow Ri(\Delta_k(m), n) = Ri(\widetilde{E}_{k'}(m \| f_{k'}(m)), n)$$

For block cipher $\widetilde{E}$, since there is no weak key, then

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; k' \leftarrow \{0,1\}^n : Ri(\Delta_k(m), n) = Ri(\Delta_{k'}(m), n)] \leq p/2^n \quad (20)$$

$$Pr[m, k \xleftarrow{\$} \{0,1\}^n; k', y : \widetilde{E}_{k'}^{-1}(y \| Ri(\Delta_k(m), n)) = m \| f_{k'}(m)] \leq p/2^n \quad (21)$$

Similar as description of $F(m,k) = F(m',k)$, we get $Adv_F^{owf}(q) \leq pq/2^{n-1}$. □

**Theorem 3 (Collision resistance of FL-Cipher).** *Let $F$ be a FL-Cipher $F : \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$, then $Adv_F^{coll}(q) \leq p^2 q/2^{n-1}$*

*Proof.* Let an adversary A for $F$, adversary A takes oracle $F$ and , when successful, it outputs $k, m$ and $k', m'$ such that $F(m,k) = F(m',k')$

$$F(m,k) = F(m',k') \Leftrightarrow Ri(\Delta_k(m), n) = Ri(\widetilde{E}_{k'}(m' \| f_{k'}(m')), n)$$

For block cipher $\widetilde{E}$, since there is no week key, we have

$$Pr[m,k,m',k' \leftarrow \{0,1\}^n : Ri(\Delta_k(m),n)Ri(\Delta_{k'}(m'),n)] \leq p^2/2^n$$

$$Pr[m,k,m',k',y \leftarrow \{0,1\}^n : E_{k'}^{-1}(y \| Ri(\Delta_k(m),n)) = m' \| f_{k'}(m')] \leq p^2/2^n$$

So we have $Adv_{F(q)}^{coll} \leq p^2 q/2^{n-1}$ □

### 3.3 Collision Resistant of Compression Functions

**Theorem 4.** *(Hash Properties of format-1)Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \rightarrow \{0,1\}^n$, and let $h$ be compression function $h(m,k) = F(m,k)$, $A$ be an adversary. Then the adversary $A$ have $Adv_h^{inv}(q) = pq/2^{n-1}$, $Adv_h^{owf}(q) \leq pq/2^{n-1}$, $Adv_h^{coll}(q) \leq p^2 q/2^{n-1}$.*

**Theorem 5.** *(Hash Properties of format-2)Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \rightarrow \{0,1\}^n$, and let $h$ be compression function $h(m,k) = F(m,k) \oplus m$, $A$ be an adversary. If $m$ and $Ri(\widetilde{E}_k(m \| f_k(m)))$ are independent, then the adversary $A$ have $Adv_h^{owf}(q) \leq pq/2^{n-1}$, $Adv_h^{coll}(q) \leq p^2 q/2^{n-1}$.*

**Theorem 6.** *(Hash Properties of format-3)Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \rightarrow \{0,1\}^n$, and let $h$ be compression function $h(m,k) = F(m,k) \oplus k$, $A$ be an adversary. If $k$ and $Ri(\widetilde{E}_k(m \| f_k(m)))$ are independent, then the adversary $A$ have $Adv_h^{owf}(q) \leq pq/2^{n-1}$, $Adv_h^{coll}(q) \leq p^2 q/2^{n-1}$.*

**Theorem 7.** *(Hash Properties of format-4)Let $F$ be FL-Cipher hash function, $F : \{0,1\}^n \times \{0,1\}^\kappa \rightarrow \{0,1\}^n$, and let $h$ be compression function $h(m,k) = F(m,k) \oplus k \oplus m$, $A$ be an adversary. If $m, k$ and $Ri(\widetilde{E}_k(m \| f_k(m)))$ are independent, then the adversary $A$ have $Adv_h^{owf}(q) \leq pq/2^{n-1}$, $Adv_h^{coll}(q) \leq p^2 q/2^{n-1}$.*

### 3.4 Collision Resistance of FL-Construction

In this section we discuss the security of FL-Construction.

**Theorem 8.** *If $F : Feist(n,n) \times (\{0,1\}^n \times \{0,1\}^n) \rightarrow \{0,1\}^n$ is a FL-Cipher, $f : \{0,1\}^n \times \{0,1\}^n) \rightarrow \{0,1\}^n$ is a compression of FL-Construction hash function $H_f$, and $f$ has a form of format1∼4, if $f$ is one way and collision resistant then the FL-Construction hash function $H_f$ is OWHF and CRHF.*

**Lemma 8 (Instance of Damgård-Merkle[5]).** *Let $f$ be a compression function from FL-Cipher with form of format1∼4, and the compression function of FL-Construction hash function $H_f$ be $f$, Then $Adv_{H_f}^{coll}(q) \leq Adv_f^{coll}(q)$ for all $q$.*

**Lemma 9 (Instance of Lai-Massey[9]).** *Let $f$ be a compression function from FL-Cipher with form of format1∼4, and the compression function of FL-Construction hash function $H_f$ be $f$. Then $Adv_{H_F}^{owf}(q) \leq Adv_F^{owf}(q)$ for all $q$.*

## 4 Collision Resistance of PGV Schemes

There are 64 most basic ways to construct a hash function $H : \{0,1\}^* \to \{0,1\}^n$ from a block cipher $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Preneel,Govaerts, and Vandeawalle present that among those 64 schemes 12 are secure, and Joha Black, Rogaway, and Shrimpton prove that in a black-box model 20 scheme among those 64 are collision-resistant. There are also 64 basic ways to construct a hash function $H : \{0,1\}^* \to \{0,1\}^n$ from a FL-Cipher $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

The security of 64 PGV schemes is summarized in tables 1 , and the functions are numbered as Joha[4].

**Table 1.** Black-Box Analysis of FL-Cipher-Based Hash Function Constructions

| $Format$ | $j$ | $h_i =$ | $Fromat$ | $j$ | $h_i =$ |
|---|---|---|---|---|---|
| - | 1 | $F_{m_i}(m_i) \oplus v$ | 1 | 33 | $F_{m_i}(w_i) \oplus v$ |
| 1 | 2 | $F_{h_{i-1}}(m_i) \oplus v$ | 1 | 34 | $F_{h_{i-1}}(w_i) \oplus v$ |
| 1 | 3 | $F_{w_i}(m_i) \oplus v$ | - | 35 | $F_{w_i}(w_i) \oplus v$ |
| - | 4 | $F_v(m_i) \oplus v$ | - | 36 | $F_v(w_i) \oplus v$ |
| - | 5 | $F_{m_i}(m_i) \oplus m_i$ | 3 | 37 | $F_{m_i}(w_i) \oplus m_i$ |
| 2 | 6 | $F_{h_{i-1}}(m_i) \oplus m_i$ | 4 | 38 | $F_{h_{i-1}}(w_i) \oplus m_i$ |
| 2 | 7 | $F_{w_i}(m_i) \oplus m_i$ | - | 39 | $F_{w_i}(w_i) \oplus m_i$ |
| - | 8 | $F_v(m_i) \oplus m_i$ | - | 40 | $F_v(w_i) \oplus m_i$ |
| - | 9 | $F_{m_i}(m_i) \oplus h_{i-1}$ | 4 | 41 | $F_{m_i}(w_i) \oplus h_{i-1}$ |
| 3 | 10 | $F_{h_{i-1}}(m_i) \oplus h_{i-1}$ | 3 | 42 | $F_{h_{i-1}}(w_i) \oplus h_{i-1}$ |
| 4 | 11 | $F_{w_i}(m_i) \oplus h_{i-1}$ | - | 43 | $F_{w_i}(w_i) \oplus h_{i-1}$ |
| - | 12 | $F_v(m_i) \oplus h_{i-1}$ | - | 44 | $F_v(w_i) \oplus h_{i-1}$ |
| - | 13 | $F_{m_i}(m_i) \oplus w_i$ | 2 | 45 | $F_{m_i}(w_i) \oplus w_i$ |
| 4 | 14 | $F_{h_i}(m_i) \oplus w_i$ | 2 | 46 | $F_{h_i}(w_i) \oplus w_i$ |
| 3 | 15 | $F_{w_i}(m_i) \oplus w_i$ | - | 47 | $F_{w_i}(w_i) \oplus w_i$ |
| - | 16 | $F_v(m_i) \oplus w_i$ | - | 48 | $F_v(w_i) \oplus w_i$ |
| 2 | 17 | $F_{m_i}(h_{i-1}) \oplus v$ | - | 49 | $F_{w_i}(v) \oplus v$ |
| - | 18 | $F_{h_{i-1}}(h_{i-1}) \oplus v$ | - | 50 | $F_{h_{i-1}}(v) \oplus v$ |
| 2 | 19 | $F_{w_i}(h_{i-1}) \oplus v$ | - | 51 | $F_{w_i}(v) \oplus v$ |
| - | 20 | $F_v(h_{i-1}) \oplus v$ | - | 52 | $F_v(v) \oplus v$ |
| 3 | 21 | $F_{m_i}(h_{i-1}) \oplus m_i$ | - | 53 | $F_{m_i}(v) \oplus m_i$ |
| - | 22 | $F_{h_{i-1}}(h_{i-1}) \oplus m_i$ | - | 54 | $F_{h_{i-1}}(v) \oplus m_i$ |
| 4 | 23 | $F_{w_i}(h_{i-1}) \oplus m_i$ | - | 55 | $F_{w_i}(v) \oplus m_i$ |
| - | 24 | $F_v(h_{i-1}) \oplus m_i$ | - | 56 | $F_v(v) \oplus m_i$ |
| 2 | 25 | $F_{m_i}(h_{i-1}) \oplus h_{i-1}$ | - | 57 | $F_{m_i}(v) \oplus h_{i-1}$ |
| - | 26 | $F_{h_{i-1}}(h_{i-1}) \oplus h_{i-1}$ | - | 58 | $F_{h_{i-1}}(v) \oplus h_{i-1}$ |
| 2 | 27 | $F_{w_i}(h_{i-1}) \oplus h_{i-1}$ | - | 59 | $F_{w_i}(v) \oplus h_{i-1}$ |
| - | 28 | $F_v(h_{i-1}) \oplus h_{i-1}$ | - | 60 | $F_v(v) \oplus h_{i-1}$ |
| 4 | 29 | $F_{m_i}(h_{i-1}) \oplus w_i$ | - | 61 | $F_{m_i}(v) \oplus w_i$ |
| - | 30 | $F_{h_{i-1}}(h_{i-1}) \oplus w_i$ | - | 62 | $F_{h_{i-1}}(v) \oplus w_i$ |
| 3 | 31 | $F_{w_i}(h_{i-1}) \oplus w_i$ | - | 63 | $F_{w_i}(v) \oplus w_i$ |
| - | 32 | $F_v(h_{i-1}) \oplus w_i$ | - | 64 | $F_v(v) \oplus w_i$ |

## 5 Conclusion

We discussed the probability of building a FL-Construction hash function from FL-Cipher with PGV modes. We make a conclusion that format1 is the best way to build a FL-Construction hash function.

## References


1. B.Preneel, V. Rijmen, A.Bosselaers: Recent Developments in the Design of Conventional Cryptographic Algorithms. In State of the Art and Evolution of Computer Security and Industrial Cryptography. Lecture Notes in Computer Science, Vol 1528. Springer-Verlag, Berlin Heidelberg New York(1998) 106-131.
2. Duo Lei, Da Lin, LiChao: A New Hash Construction and a Specific Instance DOLLY."http://eprint.iacr.org/2005/430".
3. B.Preneel: The State of Cryptographic Hash Functions. In Lectures on Data Security, Lecture Notes in Computer Science, Vol. 1561. Springer-Verlag, Berlin Heidelberg New York (1999) 158-182.
4. J.Black, P.Rogaway, and T.Shrimpton, "Black-box analysis of the block-cipher-based hashfunction constructions from PGV". In Advances in Cryptology-CRYPTO'02, volume 2442 of Lecture Notes in Computer Science. Springer-Verlag, 2002.pp.320-335.
5. I.Damgård. A design principle for hash functions. In G. Brassard, editor, Advances in Cryptology-CRYPTO' 89, volume 435 of Lecture Notes in Computer Science. Springer-Verlag, 1990.
6. B. Preneel, R. Govaerts, and J. Vandewalle, " Hash functions based on block ciphers,", In Advances in Cryptology -CRYPTO'93, Lecture Notes in Computer Science,pages 368-378. Springer-Verlag, 1994.
7. FIPS 46-3: Data Encryption Standard. In National Institute of Standards and Technology, Oct. 1999.
8. C.E. Shannon. "Communication theory of secrecy systems,", Bell System Technical Journal, 28:656 C 715, 1949.
9. X. Lai and J. L. Massey: Hash functions based on block ciphers. In Advances in Cryptology Eurocrypt'92, Lecture Notes in Computer Science, Vol. 658. Springer-Verlag, Berlin Hei-delberg New York (1993) 55-70.