# Can Feistel Structure be Used to Construct Hash Function

Duo Lei[1], Da Lin[2], and Li Chao[1]

[1] Department of Science, National University of Defense Technology,
Changsha, China
Duoduolei@163.com
[2] College of Mechanical and Electronic Control Engineering, Beijing Jiaotong
University, BeiJing, China

**Abstract.** The possibility of building dedicate hash function based on Feistel structure is discussed in this paper. Feistel Structure is known as a good structure for building block cipher. Replacing the right half bits input with round function transformation of the left half bits input in the first round, and outputting only right half byte of last round bits, the Feistel structure become a n-bit to n-bit transformation instead of a 2n-bit to 2n-bit transformation, and is not invertible, the new structure is called "FL-Structure", a function with FL-structure is called "FL-function". A block cipher $E$ with round function $F$ has Feistel structure, satisfy avalanche effect and has no related key, then the FL-function $C$ with round function $F$ is preimage resistance, second premiage resistance and collision resistant. The conclusions are that FL-structure is good structure for build dedicate hash function and more stronger design criteria are required for key schedule algorithm than block cipher design.

Keywords: Block cipher, Hash Function, Feistel structure

## 1 Introduction

A hash function is a function $H : \{0,1\}^* \rightarrow \{0,1\}^n$ for a fixed positive integer $n$ and with the property that $H(x)$ is easy to compute for all $x \in \{0,1\}^*$ for any person. A cryptographic hash function is a hash function with collision resistant. A hash function uses a secret parameter (the key) then called a Message Authentication Code or MAC.

The main ideas of the recent attacks[12][3][6] on hash functions are differential attack and were known in block ciphers years ago, which let us think the attacks against block ciphers and hash functions are similar. The design criteria of block ciphers, as strong avalanche criterion and strong diffusion ensure that neutral bits cannot exist. Block ciphers received much attention and had an interesting framework and also Block cipher cryptanalysis techniques were partially used against hash functions. Related-key attacks were initially viewed as a secondary kind of attack, and their merge with differential cryptanalysis was late and slow[7]. More and more attentions have been paid on much attention of Hash functions to be designed by the same technology as block ciphers with same principles and design criteria were receive .

The possibility of building dedicate hash function based on Feistel structure is discussed in this paper. Feistel Structure is known as a good structure for building block cipher. Replacing the right half bits input with round function transformation of the left half bits input in the first round, and outputting only right half byte of last round bits, the Feistel structure become a n-bit to n-bit transformation instead of a 2n-bit to 2n-bit transformation, and is not invertible, the new structure is called "FL-Structure", a function with FL-structure is called "FL-function". A block cipher $E$ with round function $F$ has Feistel structure, satisfy avalanche effect and has no related key, then the FL-function $C$ with round function $F$ is preimage resistance, second premiage resistance and collision resistant. The conclusions are that FL-structure is good structure for build dedicate hash function and more stronger design criteria are required for key schedule algorithm than block cipher design.

The paper is organized as follows. Specification of FL-Function and FL-Structure are given in section2. The collision resistant properties of FL-function are given in section3. The security of against block cipher attack are described in section4 and section6 is our conclusions.

## 2 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.The security of the Feistel structure is not obvious, but analysis of DES[9] 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.

Let Feistel structure be adopted in a block cipher $E(X^L_{(0)} \| X^R_{(0)}, K)$ with the round function $F$ and the round number $R$, $X^L_{(r)}, X^R_{(r)}$ be the left and the right halves of the $rth$ round outputs, $x^L_{(0)}, x^R_{(0)}$ are input plaintext, $X^L_{(R)}, X^R_{(R)}$ be output ciphertexts and $K_{(r)}$ is round key. Let function $C$ with round function $F$ input 'plaintext' $X_{(0)}$ and $rth$ round output be $X_{(r)}$ and get 'ciphertext' $X_{(R+1)}$, if $Y = C(X_0, K)$ satisfy Eq.(1), Eq.(2)Eq.(3) then we call that the structure is $R+1$ round FL-Structure and the function $C$ is FL-function. The contrast between Feistel structure and FL-Structure is given in Fig.1.

$$X_{(1)} = f(X_{(0)}, K_{(1)}) \tag{1}$$

$$X_{(r+1)} = X_{(r-1)} \oplus f(X_{(r)}, K_{(r+1)}), r = 1, ..., R \tag{2}$$

$$Y = X_{(R+1)} \tag{3}$$

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

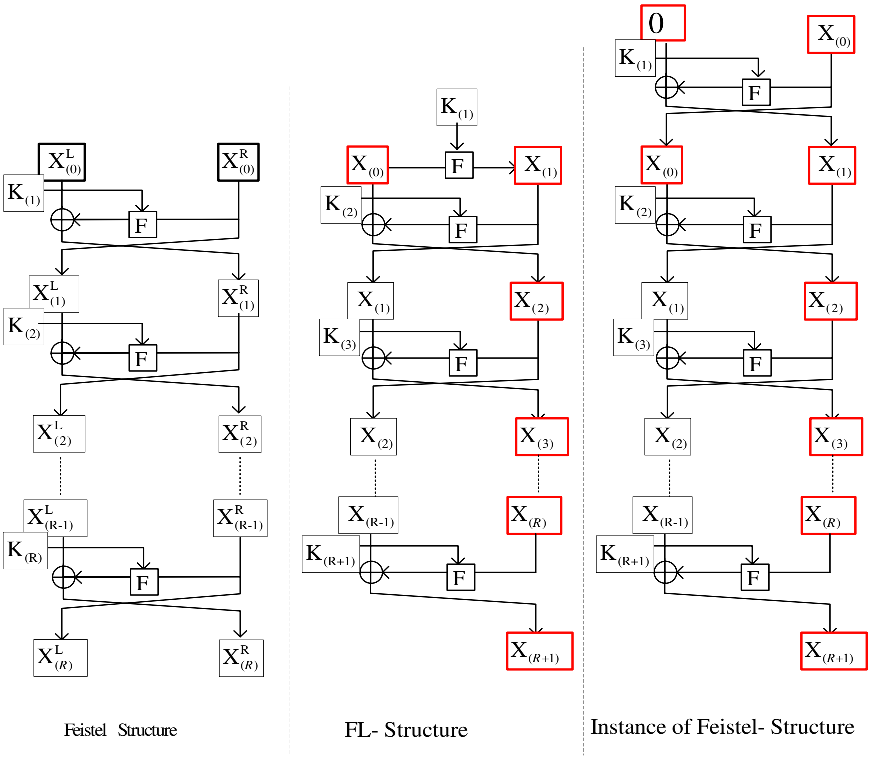


**Fig. 1.** Contrast Between Feistel Structure and FL-Sreucture

takes a function from $n$ bites to $n$ bites and produces an one-way function from $n$ bits to $n$ bites. Or the FL-structure is a Feistel structure with left half bits of input is all zero and output the only right half of output.

## 3 Collision Resistance of FL-Function

The notations of the paper are described as follows:

- $E : \{0,1\}^{2n} \times \{0,1\}^{\kappa} \rightarrow \{0,1\}^{2n}$ is Feistel structured block cipher with round function $F$, rounds $R+1$ and round key $K_{(1)}, ..., K_{(R+1)}$;
- $C : \{0,1\}^{n} \times \{0,1\}^{\kappa} \rightarrow \{0,1\}^{n}$ is FL-Function with round function $F$ and rounds $R+1$, and round key $K_{(1)}, ..., K_{(R+1)}$;
- $(m_1 \| m_2)$:Concatenate of $m_1$ and $m_2$;
- $R(m,n)$: the right $n$ bits of sequence $m$;
- $L(m,n)$: the left $n$ bits of sequence $m$;
- $x \overset{\$}{\leftarrow} S$: The experiment of choosing a random element from the finite set $S$;
- $E^{-1}$: The inverse of $E$, where $E$ is a permutation;
- $x = E_k^{-1}(y)$: The string $x$ such that $E_k(x) = y$;

- $\#[y \overset{\$}{\leftarrow} S; k, m \leftarrow S : y = E_k(m)]$: The number of $m, k$ in $S$ satisfy $y = E_k(m)$ for given $y$;
- $P[y \overset{\$}{\leftarrow} S; k, m \leftarrow S : y = E_k(m)]$: For given $y$, for all $x$ and $k$ in $S$ and do the encryption $y = E_k(m)$ and the probability of find the value satisfying the equation;
- $P_M[y \overset{\$}{\leftarrow} S; k, m \leftarrow S : y = E_k(m)] \overset{\triangle}{=} \max_{y \in S} P[y \overset{\$}{\leftarrow} S; k, m \leftarrow S : y = E_k(m)]$;
- $\tilde{0}$:n-bit binary, all bits are 0;
- $S : S \overset{\triangle}{=} \{0,1\}^n$;
- $T_1 \overset{\triangle}{=} \max \#[m, y \overset{\$}{\leftarrow} \{0,1\}^n; k \leftarrow \{0,1\}^n : R(E_k(\tilde{0} \| m), n) = y]$;
- $T_2 \overset{\triangle}{=} \max \#[k, y \overset{\$}{\leftarrow} \{0,1\}^n; m \leftarrow \{0,1\}^n : R(E_k(\tilde{0} \| m), n) = y]$;
- $T_3 \overset{\triangle}{=} \max \#[k, y \overset{\$}{\leftarrow} \{0,1\}^n; y' \leftarrow \{0,1\}^n : E_k^{-1}(y' \| y) = (\tilde{0} \| m)]$.

**Definition 1 (Strict avalanche effect of plaintext).** *[1] Each Ciphertext bit should change with a probability of one half whenever a single ciphertext bit is complemented.*

**Definition 2 (Strict avalanche effect of key).** *Each ciphertext bit should change with a probability of one half whenever a single key bit is complemented.*

**Definition 3 (No Similar Key).** *Block cipher $E : \{0,1\}^{2n} \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$*

$$max\#[m, m', y, y' \overset{\$}{\leftarrow} \{0,1\}^n; k \leftarrow \{0,1\}^n : E_k(m \| m') = (y' \| y)] = 2 \qquad (4)$$

*Call the Feistel block cipher $E$ has no similar key.*

**Lemma 1.** *In block cipher $E$: $T_2 \equiv T_3$.*

*Proof.* Let $k, y$ and different $m_1, ..., m_{T_2}$ satisfy $R(E_k(\tilde{0} \| m_i), n) = y, i \leq T_2$, we get values $L(E_k(\tilde{0} \| m_1), n), ..., L(E_k(\tilde{0} \| m_{T_2}), n)$, $E$ is permutation that means $L(E_k(\tilde{0} \| m_i), n) \neq L(E_k(\tilde{0} \| m_j), n)$, $i \neq j$ which implies $T_2 \geq T_3$. On the contrary $T_3 \geq T_2$. □

**Lemma 2.** *In black box model, for Feistel Cipher $E$:*

$$P[k, y \overset{\$}{\leftarrow} \{0,1\}^n; y' \leftarrow \{0,1\}^n : E_k^{-1}(y' \| y) = (\tilde{0} \| m)] = 1/2^n \qquad (5)$$

*Proof.* $\#[k \overset{\$}{\leftarrow} \{0,1\}^n; y, y' \leftarrow \{0,1\}^n : L(E_k^{-1}(y' \| y), n) = (\tilde{0} \| m)] = 2^n$.
$\#[y, y' \leftarrow \{0,1\}^n] = 2^{2n}$,$\#[m \leftarrow \{0,1\}^n] = 2^n$,
for a constant $k$ and $y$, $\forall y' \in \{0,1\}^n, P[L(E_k^{-1}(y' \| y), n) = 0] = 1/2^n$. □

**Lemma 3.** *If block cipher $E$ has no similar key, and in black box model:*

$$P[m, y \overset{\$}{\leftarrow} \{0,1\}^n; k \leftarrow \{0,1\}^n : R(E_k(\tilde{0} \| m), n) = y] = 1/2^{n-1} \qquad (6)$$

*Proof.* $\#P[m,y,y' \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m),n) = y'\|y] = 2$.
$\#[m \leftarrow \{0,1\}^n] = 2^n$, for constant $k$ and $y$, $\forall k \in \{0,1\}^n$
$P[R(E_k(\tilde{0}\|m),n) = y] = 2/2^n$. □

A compression function of collision-resistant hash function is a function $H(M,V)$ that satisfies the following conditions where $M$ is Message block and $V$ is initial vector or output of previous round iteration:

- The input $M$ can be of fixed length and the result $H$ has a fixed length.
- Given $H$ and an input $M$, the computation of $H(M)$ must be 'easy'.
- preimage-resistance: Given a Y in the image of H, it is 'hard' to find a message $M$ such that $H(M) = Y$(one-way).
- second preimage-resistance: Given $M$ and $H(M)$ it is 'hard' to find a message $M' \neq M$ such that $H(M') = H(M)$.
- collision-resistance: It is 'hard' to find two distinct messages $M$ and $M'$ such that $H(M) = H(M'))$.

If FL-function $C(m,k)$ or $C(k,m)$ is a hash compression function, the properties of preimage-resistance, second preimage-resistance, and collision are written in following modes:

- preimage-resistance:
  $P_M[k,y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : y = C(m,k)] < \varepsilon$
  $P_M[m,y \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : y = C(m,k)] < \varepsilon$
  $P_M[y \xleftarrow{\$} \{0,1\}^n; k,m \leftarrow \{0,1\}^n : y = C(m,k)] < \varepsilon$
- second preimage-resistance:
  $P_M[k_1,m_1 \xleftarrow{\$} \{0,1\}^n; m_2 \leftarrow \{0,1\}^n : C(m_2,k_1) = C(m_1,k_1)] < \varepsilon$
  $P_M[k_1,m_1 \xleftarrow{\$} \{0,1\}^n; k_2 \leftarrow \{0,1\}^n : C(m_1,k_1) = C(m_1,k_2)] < \varepsilon$
  $P_M[k_1,m_1 \xleftarrow{\$} \{0,1\}^n; m_2,k_2 \leftarrow \{0,1\}^n : C(m_1,k_1) = C(m_2,k_2)] < \varepsilon$
- collision-resistance:
  $P_M[m_1,k_1,k_2 \leftarrow \{0,1\}^n : C(m_1,k_1) = C(m_1,k_2)] < \varepsilon$
  $P_M[m_2,k_1,k_2 \leftarrow \{0,1\}^n : C(m_1,k_1) = C(m_2,k_1)] < \varepsilon$
  $P_M[m_1,m_2,k_1,k_2 \leftarrow \{0,1\}^n : C(m_1,k_1) = C(m_2,k_2)] < \varepsilon$.

**Lemma 4.** *For block cipher $E$ we have:*

- $P_M[k,y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m),n) = y] \leq 2^{-n}T_2$;
- $P_M[m,y \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m),n) = y] \leq 2^{-n}T_1$;
- $P_M[y \xleftarrow{\$} \{0,1\}^n; m,k \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m),n) = y] \leq 2^{-n}\max\{T_1,T_2\}$.

*Proof.*

- There are two ways to get the correct value $m$ for given $k$,$y$, first way is for all $m \in \{0,1\}^n$, check equation $R(E_k(\tilde{0}\|m),n) = y$ being hold or not, another way is for all $y' \in \{0,1\}^n$, check the left half output of $E_k^{-1}(y'\|y)$ is zero or not. Since

$\max \#[k, y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] = T_2;$
$\max \#[k, y \xleftarrow{\$} \{0,1\}^n; y' \leftarrow \{0,1\}^n : E_k^{-1}(y'\|y) = (\tilde{0}\|m)] = T_3;$
the maximum success probability of first way is $2^{-n}T_3$, that of second way is $2^{-n}T_2$. We have:
$P_M[k, y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] \leq 2^{-n}T_2.$

- There are two ways to get the correct value $k$ for given $m$,$y$, first way is that for each $k \in \{0,1\}^n$, check $R(E_k(\tilde{0}\|m), n)$ equals $y$ or not, another way is that for each $y' \in \{0,1\}^n$ and a random $k \in \{0,1\}^n$, check the left half output of $E_k^{-1}(y'\|y)$ is zero or not.
  $\max \#[m, y \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] \leq T_1;$
  $\max \#[m, y, k \xleftarrow{\$} \{0,1\}^n; y' \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] \leq T_1;$
  the maximum success probability of that is $2^{-n}T_1$
- To get the correct value $k$ and $m$, we should suppose one of $k$ and $m$ is constant, first way is for a random $m \in \{0,1\}^n$, check all $k \in \{0,1\}^n$, another way is for a random selected $k \in \{0,1\}^n$, check all $m \in \{0,1\}^n$. we have:
  $P_M[y \xleftarrow{\$} \{0,1\}^n; m, k \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] \leq 2^{-n} \max\{T_1, T_2\}.$

□

**Lemma 5.** *If block cipher $E$ satisfy the strict avalanche effect:*

- $P_M[m_1, k \xleftarrow{\$} \{0,1\}^n; m_2 \leftarrow \{0,1\}^n :$
  $R(E_k(\tilde{0}\|m_1), n) = R(E_k(\tilde{0}\|m_2)), n)] \leq 2^{-n}(T_2 - 1)$*;*
- $P_M[m, k_1 \xleftarrow{\$} \{0,1\}^n; k_2 \leftarrow \{0,1\}^n :$
  $R(E_{k_1}(\tilde{0}\|m), n) = R(E_{k_2}(\tilde{0}\|m), n)] \leq 2^{-n}(T_1 - 1)$*;*
- $P_M[m_1, k_1 \xleftarrow{\$} \{0,1\}^n; m_2, k_2 \leftarrow \{0,1\}^n :$
  $R(E_{k_1}(\tilde{0}\|m_1), n) = R(E_{k_1}(\tilde{0}\|m_1), n)] \leq 2^{-n}(\max\{T_1, T_2\} - 1)$*;*

*Proof.*

- There are two ways to get the correct value $m_2$, first way is checking the equation $R(E_k(\tilde{0}\|m_1), n) = R(E_k(\tilde{0}\|m_2), n)$ being hold or not, for all $m_2 \in \{0,1\}^n$. Another way is that for all $y' \in \{0,1\}^n$, checking the output of $E_k^{-1}(y'\|R(E_k(\tilde{0}\|m_1), n))$ satisfying the relation $m' = F_k(m)$ or not where if the block cipher $E$ is designed in strict avalanche effect then the value $E_k(\tilde{0}\|m_1)$ gives no information about correct $y'$.
  $\max \#[k, y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] = T_2;$
  $\max \#[k, y \xleftarrow{\$} \{0,1\}^n; y' \leftarrow \{0,1\}^n : E_k^{-1}(y'\|y) = (\tilde{0}\|m)] = T_3;$
  The probability of getting the correct value $m_2$ is $2^{-n}(T_2 - 1)$.
- There are two ways to get the correct value $k_2$, first way is checking the equation $R(E_{k_1}(\tilde{0}\|(m_1)), n) = R(E_{k_2}(\tilde{0}\|m_2), n)$ being hold or not, for each $k_2 \in \{0,1\}^n$. Another way is for each $y' \in \{0,1\}^n$ and a random select $k_2$ checking the equation $E_{k_2}^{-1}(y'\|R(E_{k_1}(\tilde{0}\|m_1), n))$ being satisfied or not. If Block cipher $E$ satisfying strict avalanche effect of key, the select of $k_2$ are not influenced by $k_1$. Since

$\max \#[m, y \xleftarrow{\$} \{0,1\}^n; k \leftarrow \{0,1\}^n : Re(E_k(\tilde{0}\|m), n) = y] \leq T_1;$
$\max \#[m, y, k \xleftarrow{\$} \{0,1\}^n; y' \leftarrow \{0,1\}^n : Re(E_k(\tilde{0}\|m), n) = y] \leq T_1;$
the probability of getting the correct value $m_2$ is $2^{-n}(T_1 - 1)$;

- To get the correct value $k_2$ or $m_2$, we should suppose one of $k_2$ and $m_2$ is unchanged, first way is for a random $m \in \{0,1\}^n$, check all $k \in \{0,1\}^n$, another way is for a constant $k \in \{0,1\}^n$, check all $k \in \{0,1\}^n$. The maximum complexity of the checking is $2^{-n}(\max\{T_1, T_2\} - 1)$.

□

**Lemma 6.** *If block cipher $E$ satisfy the strict avalanche effect:*

- $P_M[m_1, k, m_2 \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m_1), n) = R(E_k(\tilde{0}\|m_2)), n)]$
  $\leq 2^{-n}T_2(T_2 - 1)/2$*;*
- $P_M[m, k_1, k_2 \leftarrow \{0,1\}^n : R(E_{k_1}(\tilde{0}\|m), n) = R(E_{k_2}(\tilde{0}\|m), n)]$
  $\leq 2^{-n}T_1(T_1 - 1)/2$*;*
- $P_M[m_1, k_1, m_2, k_2 \leftarrow \{0,1\}^n : R(E_{k_1}(\tilde{0}\|m_1), n) = R(E_{k_2}(\tilde{0}\|m_2), n)]$
  $\leq 2^{-n}(\max\{T_1(T_1 - 1), T_2(T_2 - 1)\} - 1)/2$*;*

*Proof.*

- To get the correct value $k$,$m_1$ and $m_2$, one way is checking the equation $R(E_k(\tilde{0}\|m_1), n) = R(E_k(\tilde{0}\|m_2), n)$ being hold or not, second way is checking $L(E_k^{-1}(y'\|R(E_k(\tilde{0}\|m_1), n))$ being satisfied or not.
  $\max \#[k, y \xleftarrow{\$} \{0,1\}^n; m \leftarrow \{0,1\}^n : R(E_k(\tilde{0}\|m), n) = y] = T_2;$
  $\max \#[k, y \xleftarrow{\$} \{0,1\}^n; y' \leftarrow \{0,1\}^n : E_k^{-1}(y'\|y) = (\tilde{0}\|m)] = T_3$; the maximum probability of the result is $2^{-n}\{T_2(T_2 - 1)/2$.
- similarly the maximum probability is $\max 2^{-n}\{T_1(T_1 - 1)/2$.
- similarly the maximum probability is $2^{-n} \max\{T_1(T_1 - 1)/2, T_2(T_2 - 2)/2$.

□

**Theorem 1 (Preimage-resistance).** *In black box model, Block cipher $E$ satisfy avalanche effect, then the FL-function is Preimage-resistant.*

**Theorem 2 (Second Preimage-resistance).** *In black box model, Block cipher $E$ satisfy avalanche effect, then the FL-function is second Preimage-resistant.*

**Theorem 3 (Collision resistance).** *In black box model, Block cipher $E$ satisfy avalanche effect, then the FL-function is collision resistant.*

## 4 Design Principle of FL-Function

The hash function is far more sensitive to defects on designing than that of block cipher, for finding a weak key in block cipher does not result in failure of the block cipher, but finding a weak key in hash function always means finding a collision that results in the failure of the hash function. In some point of view, the FL-function is a special instance of block cipher, so the attacks against block cipher should be considered.

**Attacks on block cipher** The FL-function is a Feistel cipher of left half bits of input with zero. If the Feistel cipher is designed to be immune against attacks on block cipher, then the FL-function be immune against those attacks.

**Key Schedule** In block cipher design, the key schedule algorithm is design with strict avalanche in itself, where influences of each key on plaintext are considered, influences of different key on same plaintext is ignored. But in hash function design, the influences of different keys on same plaintext is as important as the influences of one key on different plaintext.

**Input Modes** The compression function of hash function $H(V, M)$ needs two input value, one of which is output of previous round output and one of which is the expansion of plaintext. FL-function $F(m, k)$ also has two input value plaintext and key. From the discussion given in previous section, the security of two ways are same. If we select the key in $F$ as plaintext, then in hashing procedure we can compute the compression and key schedule at the same time.

## 5 FL-Construction Hash Function

In the previous sections we discussed the possibility of build a compression function using a Feistel structure. If we concatenate the FL-function and Feistel Cipher, we build a new hash function that has many advantage contrast with MD-construction[11].

**Definition 4.** *Let $E$ is a feistel cipher,expanded message are $M_1, ..., M_q$ :*

$$H_1 = R(E_{M_1}(0, IV), n)$$
$$H_i = E_(M_i), i = 1, ..., q$$
$$h(x) = R(H_q, n)$$

*we call the hash function Feistel Hash function.*

Figure illustration is given in Fig.2.

**Theorem 4 (Preimage-resistance).** *In black box model, Feistel $E$ satisfy avalanche effect, then Feistel hash function is preimage-resistance.*

**Theorem 5 (Second Preimage-resistance).** *In black box model, Feistel $E$ satisfy avalanche effect, then Feistel hash function is second Preimage-resistance.*

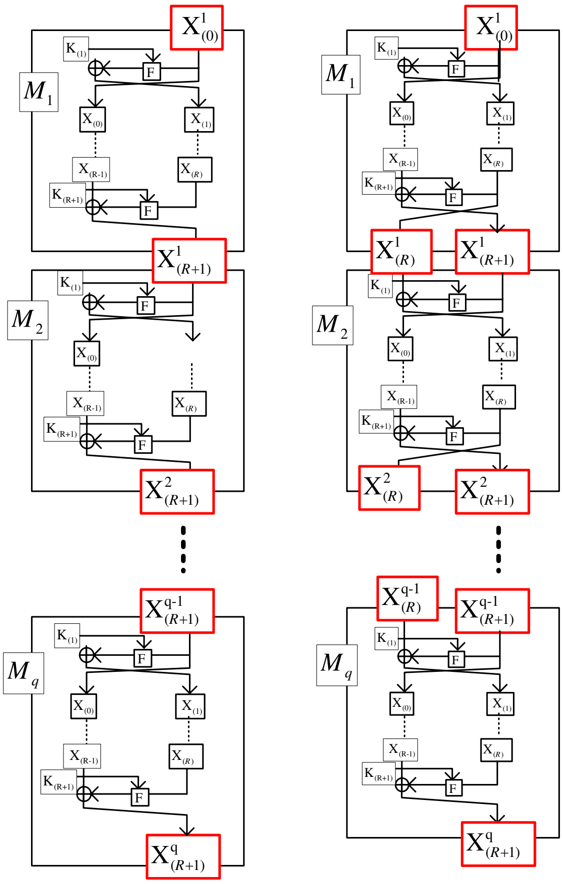
**Theorem 6 (Collision resistance).** *In black box model, Feistel $E$ satisfy avalanche effect, then Feistel hash function is collision resistant.*

*Proof.* Since the Feistel itself is a FL-function, so we have the conclusion. □

**Theorem 7.** *Feistel hash function is immune against Multi collision[2]*

**Theorem 8.** *Feistel hash function is immune against extension attack.*

It is clear that the FL-Hash function is not immune against fix point attack, that should be considered in design principle of $E$ function.



MD-Construction

FL-Construction

**Fig. 2.** Contrast Between MD-Construction and FL-Construction

## 6 Conclusion

In this paper we present a new way to construct hash function. Security of FL-Function relies on the security of Feistel structure, round function and key schedule algorithm. And the design of FL-function require more considers than block cipher design, but the criteria of design block cipher all can be used in design. If we can design a secure hash function based on FL-structure then we design a more secure block cipher.

## References

1. A. F.: Webster and S. E. Tavares. On the design of S-boxes. Advances in Cryptology-CRYPTO'85 Lecture Notes in Computer Science 218, P 523-534.

2. A. Joux, Multicollisions in iterated Hash functions. Application to cascaded constructions. Proceedings Crypto 2004, Springer-Verlag LNCS 3152 (2004) 306-316.
3. A. Joux, P.Carribault, W. Jalby and C. Lemuet. Collisions in SHA-0. Presented at the rump session of CRYPTO 2004, August 2004.
4. A. Webster and S. Tavares.: On the design of S-boxes. In Advances in Cryptology-CRYPTO'85, vol.219, Lecture Notes in Computer Science, pp.423.
5. 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.
6. E.Biham. Recent advances in hash functions-the way to go. Presented at ECRYPT Conference on Hash Functions (Cracow, June 2005), see http://www.ecrypt.eu.org/stvl/hfw/Biham.ps.
7. E.Biham and R.Chen. Near-Collisions of SHA-0. In Advances in Cryptology CRYPTO 2004, LNCS 3152P.290-305. [24] E.Biham and R.Chen. Near-Collisions of SHA-0 and SHA-1. In Selected Areas in Cryptography-SAC 2004.
8. 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.
9. FIPS 46-3: Data Encryption Standard. In National Institute of Standards and Technology, Oct. 1999.
10. H. Feistel. Cryptography and Computer Privacy. Scientific American,
11. 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.
12. X. Wang, X.Lai, D.Feng and H.Yu., Cryptanalysis of the Hash Functions MD4 and RIPEMD, EUROCRYPT 2005, LNCS 3494, pp.1-18, Springer-Verlag, 2005. [18] X. Wang, H. Yu, How to Break MD5 and Other Hash Functions, EUROCRYPT 2005, LNCS 3494, pp.19-35, Springer-Verlag, 2005.
13. 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. 228(5):15-23.