F-HASH: Securing Hash Functions Using Feistel Chaining

Duo Lei

Department of Science, National University of Defense Technology,
Changsha, China
Duoduolei@gmail.com

Abstract. The Feistel structure is well-known as a good structure for building block ciphers, due to its property of invertibility. It can be made non-invertible by fixing the left half of the input to 0, and by discarding the left half of the output bits. It then becomes suitable as a hash function construction. This paper uses the structure to build a hash function called F-Hash, which is immune to recent attack styles. The paper extends on this result by presenting two MACs and an encryption mode. Generally the security of such structures is discussed using Random Oracle Models. In this paper, a more precise evaluation method, based upon conditional probability, is given.

Keywords: Hash Function, Conditional probability, Feistel structure

1 Introduction

Most hash functions, including MD5[15] and SHA-1[14] are based upon compression functions iterated using the Merkle-Damgård structure [10, 22] with fixed IVs [35]. Since MD5 and SHA-1 were attacked by Wang et. al [6, 41, 42], more attention has been paid to the area of hash functions, with the intention of strengthening these hash functions or finding new, resilient hash functions.

The Wang attacks are based upon differential cryptanalysis, first known to academics in the early nineties [5]. Attacks against block ciphers and hash functions are very similar, as witnessed by the use of block cipher cryptanalysis techniques against hash functions [4, 26]. Increasing attention has been paid to designing hash functions using the same technology as block ciphers [4], as that technology is well-established.

One such technology is the Feistel structure, which is frequently used to build block ciphers using a $2n \rightarrow 2n$ invertible transformation. By fixing the leftmost n bits of the input to 0, and by outputting the rightmost n bits, the Feistel structure becomes a non-invertible n to n transformation that is suitable for building hash functions. We call this the FL-structure (Feistel-like structure). If the round function of the FL structure is chosen in the same way as the round function of the Feistel-based block cipher, then the new construction, when using more than two rounds, inherits many of the properties of the corresponding

block cipher, with the exception of invertibility. The benefit of the FL structure is that it leverages the extensive analysis conducted on the Feistel structure. Therefore we think that the non-invertibility of the FL structure qualifies it as a good component for building hash compression functions to resist pre-image and collision attacks.

This paper discusses building dedicated hash functions using Feistel structure, including a complete hash function based on the FL structure, which we name F-Hash. We give a proof of security of this hash function, and show that for robust underlying block ciphers, the hash function is immune against all known attacks. Using the same round function and key schedule, we build a MAC – F-MAC – and block encryption mode – FBC.

In this paper, we give a new evaluation model to quantify the security of structures based upon conditional probability. We discuss the influence of the compression function's conditional probability on the entire construction's conditional probability. This informs us that the outputs of F-Hash are uniformly distributed for any fixed IV and random message, or for any selected message and random IV, if only the compression function has the following properties: that the function is immune against adaptive chosen plaintext and adaptive chosen-key attacks and that the distribution of the function's inputs and outputs are uniform.

It is basic requirement upon the block cipher that the distribution of input and output are independent. Patarin [27–31] provided security proofs for the Feistel Structure, and Piret [32, 33] gave proofs of round functions with random permutations. Similar conclusions were also given by Vaudenay [39, 40]. Luby and Rackoff [21] introduced a method that permitted the assessment of security of some block cipher constructions. The limitations of these proofs are that although they discuss immunity against adaptive chosen plaintext attacks, they neglect adaptive chosen-key attacks. For F-Hash, we should consider security against chosen-key attacks. In this paper we give a proof that if the Feistel cipher is immune against adaptive chosen plaintext attacks and the key schedule algorithm is sufficiently non-linear, then we can build a secure F-hash.

In Section 2, we give Feistel constructions and define the new hash function, MACs and block cipher encryption modes. In Section 3, we provide security proofs. In Section 4, we provide a discussion and conclusion.

2 The Feistel Constructions

A Feistel structure is a general way of constructing block ciphers from simple functions. The original idea was invented by Horst Feistel [11] for use with block ciphers. The security of the Feistel structure is not obvious but comprehensive analysis of DES [13] has shown that it is a good way to construct ciphers. No weakness has been found in the Feistel structure itself. In this section, we present some constructions derived from the Feistel structure, but first introduce the structure itself.

2.1 The Feistel Compression Function

Let I_n be the set $\{0,1\}^n$ where $a, b \in I_n$, and $a\|b \in I_{2n}$ and $|a| = n$. The key schedule algorithm is $\psi(k)$ and $k^{(i)}$are the round keys, such that $k^{(0)} = k$, $k^{(i)} = \psi(k^{(i-1)})$, $i \geq 1$. The round function of the block cipher is $f : I_n \times I_n \rightarrow I_n$ [1]. The round output $y = f(k^{(i)}, x)$, also denoted by $f_{k^{(i)}}$. Then with $\circ$ denoting composition of a function, a Feistel block cipher is denoted by $E^{Fe} : I_n \times I_{2n} \rightarrow I_{2n}$, where:

$E^{Fe}(k, x'\|x) \stackrel{def}{=} \Psi^R(f)(x'\|x) = \Psi(f_{k^{(R)}}) \circ \Psi(f_{k^{(R-1)}}) \circ \ldots \circ \Psi(f_{k^{(1)}}(x'\|x))$,

$y'\|y \stackrel{def}{=} \Psi(f_k)(x'\|x) = \begin{cases} y' = x \\ y = x' \oplus f_k(x) \end{cases}$ such that $x', x, y', y \in I_n$; $(x'\|x)^L$ and $(x'\|x)^R$: and the leftmost and rightmost n bits of binary sequence $x'\|x$, respectively. Also $\tilde{0}$ is an n-bit string with all bits equal to 0.

Also define an SPN block cipher $E^{Sp} : I_n \times I_n \rightarrow I_n$, such that $E^{Sp}(k, x) = f_{(k^{R'})} \circ f_{k^{(R'-1)}} \circ \ldots \circ f_{k^{(1)}}(x)$. Let $F_c : I_n \times I_n \rightarrow I_n$ be Feistel-Like Structured Function with round function, $F_c(k, x) = (E^{Fe}(k, \tilde{0}\|x))^R$; F_{c-1} : Feistel-Structured function with one round fewer than F_c, and E^{-1} be the inverse of E, where E is a permutation.

Remark 1. Unless otherwise noted, E^{Fe}, E^{Sp}, F_c and F_{c-1} have same key schedule algorithm $\psi(k)$ and round function f. The round function f is a permutation.

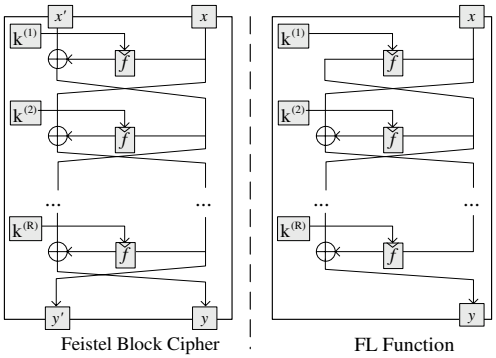

Fig. 1. Contrast Between Feistel Structure and FL-Structure

Definition 1 (FL Structure). *Let function $F_c : I_n \times I_n \rightarrow I_n$, if $F_c(k, x) = \Psi^R(f)(x'\|x) = \Psi(f_{k^{(R)}}) \circ \Psi(f_{k^{(R-1)}}) \circ \ldots \circ \Psi(f_{k^{(1)}}(\tilde{0}\|x))^R$, then we call function F_c the FL-Function (Feistel Like function) and the entire structure FL-Structure(Feistel Like Structure). This is shown in Figure 1.*

[1] We assume that the key length $\kappa = n$, with padding if required.

2.2 F-HASH Function

Let $z = H(m, x)$: the hash function, where m be message and x be initial value; message[2] $m \in I_{n\cdot *}$, $\mathtt{m}_i$ be message block with $\mathtt{m}_i \in I_n$, $m = \mathtt{m}_* \| \mathtt{m}_{*-1} \| \ldots \| \mathtt{m}_1$, $\mathtt{m}_* \subseteq m$; A selected m be denoted $m_i \in I_{n\cdot t}, t \geq 1$; $y = F(x_m, x_h)$: the hash compression function, where x_h be chaining value, x_m be message block; $z = H^M(m, x)$: iterated hash with M-D construction, if $m = \mathtt{m}_t \| \ldots \| \mathtt{m}_1$, then $z = F(\mathtt{m}_t, F(\mathtt{m}_{t-1}, \ldots F(\mathtt{m}_1, x) \ldots))$ with compression function $y = F(x_m, x_h)$; Message Padding: adding zero at the end of Message[3].

Definition 2 (Feistel Compression Function). *If the function $F_c : I_n \times I_n \to I_n$ is used as compression function of iterated hash with format $y = F_c(x_m, x_h)$, where x_h is the chaining value, we call this function the Feistel Compression Function.*

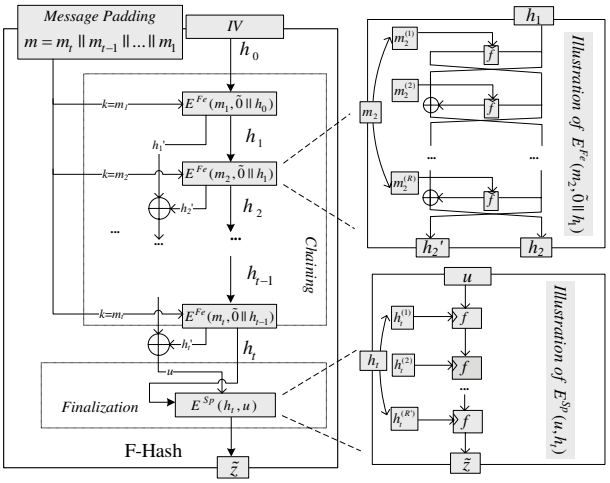

Fig. 2. F-HASH Function

Definition 3 (F-HASH). *Let F-HASH $H^F : I_{n\cdot *} \times I_n \to I_n$, $\tilde{z} = H^F(m, x)$, $m \in I_{n\cdot t}$ is defined as*

$$
\begin{aligned}
&h_0 = x \\
&h_i = F_c(\mathtt{m}_i, h_{i-1}), \qquad (i = 1, \ldots, t) \\
&h'_i = F_{c-1}(\mathtt{m}_i, h_{i-1}), \qquad (i = 1, \ldots, t) \\
&\tilde{z} = E^{Sp}(\bigoplus_{i=1}^{t} h'_i, h_t).
\end{aligned}
$$

[2] When message block is used as key, the message block length be κ.

[3] That is to make thing simple. In realized design, we should select a length related padding

Lemma 1. $y'\|y = E^{Fe}(x_m, \tilde{0}\|x_h) \Leftrightarrow y' = F_{c-1}(x_m, x_h), y = F_c(x_m, x_h)$

In fact, we have $h'_i\|h_i = E^{Fe}(\mathtt{m}_i, \tilde{0}\|h_{i-1}), (i = 1, \ldots, t)$. The figure illustration of F-HASH is given in Fig 2.

2.3 F1-MAC and F2-MAC

In this subsection two MAC structures are given which have a similar structure to F-HASH, figure illustration is Fig 3.

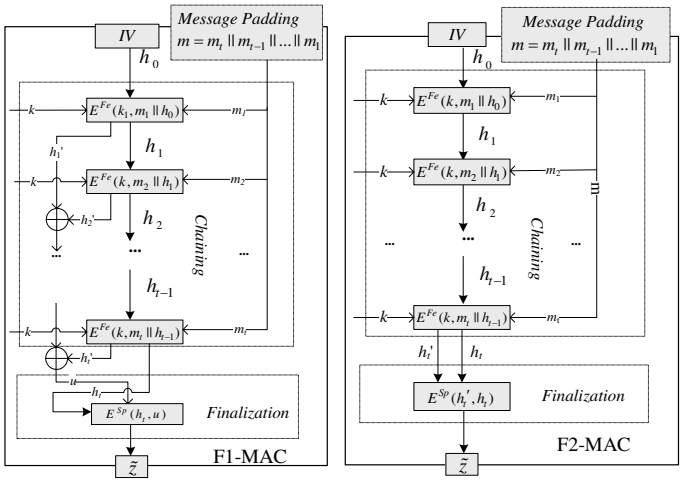

Fig. 3. F1-MAC and F2-MAC

Definition 4 (F1-MAC). *Let* $M^{F1} : I_n \times I_{n\cdot *} \times I_n \to I_n$*, F-MAC is defined as* $\tilde{z} = M^{F1}(k, m, x)$*,* $m \in I_{n\cdot t}$

$$
\begin{aligned}
&h_0 = x \\
&h'_i\|h_i = E^{Fe}(k, \mathtt{m}_i\|h_{i-1}), \qquad (i = 1, \ldots, t) \\
&\tilde{z} = E^{Sp}(\bigoplus_{i=1}^{t} h'_i, h_t).
\end{aligned}
$$

Definition 5 (F2-MAC). *Let* $M^{F2} : I_n \times I_{n\cdot *} \times I_n \to I_n$*, F-MAC is defined as* $\tilde{z} = M^{F2}(k, m, x)$*,* $m \in I_{n\cdot t}$

$$
\begin{aligned}
&h_0 = x \\
&h'_i\|h_i = E^{Fe}(k, \mathtt{m}_i\|h_{i-1}), \qquad (i = 1, \ldots, t) \\
&\tilde{z} = E^{Sp}(h'_t, h_t).
\end{aligned}
$$

The F1-MAC is a MAC similar to F-HASH. The F2-MAC is a MAC similar to FBC mode.

2.4 FBC Encrypt Mode

In this subsection we give a encrypt on mode based on the Feistel structure, called FBC(Feistel Block Chaining), figure illustration is Fig. 4.

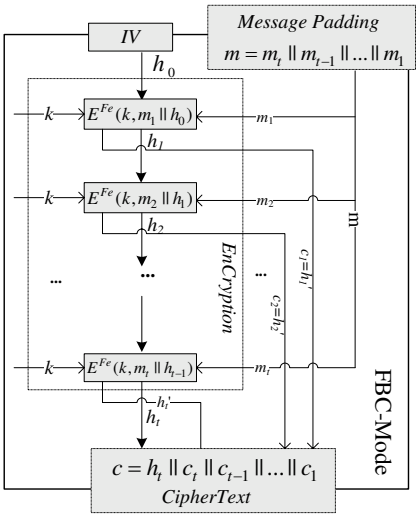

Fig. 4. FBC Encrypt Mode

Definition 6 (FBC Mode). *Let* $E^{FBC} : I_n \times I_{n \cdot t} \times I_n \rightarrow I_{n \cdot (t+1)}$, $c = E^{FBC}(k, m, x)$ *is defined as*

$$
\begin{aligned}
&h_0 = x \\
&c_i \| h_i = E^{Fe}(k, m_i \| h_{i-1}), \qquad (i = 1, \ldots, t) \\
&c = h_t \| c_t \| c_{t-1} \| \ldots \| c_1.
\end{aligned}
$$

In FBC mode the ciphertext of the previous encryption is added to the subsequent encryption, the mode is similar as CBC mode and inheriting all the advantage of CBC mode and improving upon it.

1. the CBC mode requires the communication sides hold the initialization vector, whereas FBC mode does not.
2. when the x is randomized, all the ciphertext be randomized.
3. the fixed initial value x can be used as authentication.
4. the encryption and decryption have the same structure with different key schedules.

Theorem 1. *Every key recovery attack on FBC mode can be converted to known plaintext key recovery attack on the Feistel block cipher.*

3 Security Proof of F-HASH

The securities of F-HASH, F-MAC are based on security of Feistel Block cipher and the security of the structure.

In this section, we give the security proofs of compression function and the structure, where the security of compression function is totally based upon security of the Feistel block cipher. Then we give the security proof of the structure.

Let X be a random variable which takes on a finite set S of values $x \in S$ with probability $P_X(x) \stackrel{def}{=} P(X = x)$. Also, let X', Y, Y', Z and $\tilde{Z}$ be random variables which take on finite sets of values.

Theorem 2 (Derived Probability). *Let function $y = G(m, x)$, $G : I_{n \cdot t} \times I_n \to I_n$, $t \in \mathbf{N}$, let the distributions of independent random variable M and X are $P_X(x)$ and $P_M(m)$, let function $\chi_{G(m,x)}(y)$ is defined as that*

$$\chi_{G(m,x)}(y) \stackrel{def}{=} \begin{cases} 1 & y = G(m, x) \\ 0 & y \neq G(m, x) \end{cases}$$

Then the distribution of random variable Y can be derived from X and M by

$$\begin{aligned} P_Y(y) &\stackrel{def}{=} P_Y(y = G(M, X)) \\ &= \sum_{x \in I_n} \sum_{m \in I_{n \cdot t}} P_{XM}(x, m) \chi_{G(m,x)}(y) \\ &= \sum_{x \in I_n} \sum_{m \in I_{n \cdot t}} P_X(x) P_M(m) \chi_{G(m,x)}(y) \end{aligned}$$

we call the probability of Y, the derived probability of M and X.

For any $y \in I_n$, if does not exist $P_Y(y)$, then we have $P_Y(y) \stackrel{def}{=} 0$.

Definition 7 (Conditional probability). *Directed followed Theorem 2, the conditional probability is defined as follows*

1. $P_{Y|M=m_0}(y_0) = \sum_{x \in I_n} P_X(x) \chi_G(y_0, m_0, x)$;
2. $P_{Y|X=x_0}(y_0) = \sum_{m \in I_{n \cdot t}} P_M(m) \chi_G(y_0, m, x_0)$;
3. $P_{Y|X=x_0, M=m_0}(y_0) = \chi_G(y_0, m_0, x_0)$.

Remark 2. If X and M are uniformly distributed, which means $P_M(m) = \frac{1}{2^{n \cdot t}}$, $P_X(x) = \frac{1}{2^n}$, we use notation of $P_{\dot{Y}}(y)$, that is also holds in the conditional probability.

3.1 Security of Feistel Compression Function

Since the proof of chosen plain-text attack on Feistel block cipher is known and chosen key attack on Feistel block cipher is uncertain. And the chosen-key attack on Feistel block cipher can be converted to a chosen chaining value attack on Feistel compression function. The motivation of this section is that, if there

exist a secure Feistel block cipher, immune against adaptive chosen plaintext , then there exist a secure Feistel compression function, immune against adaptive chosen message attack and adaptive chosen chaining attack.

We give following assumption for E^{Fe}, which is based upon the known results of Feistel structured block cipher.

Assumption 1 *For E^{Fe} and E^{Sp}*

1. *The ciphers are immune against chosen plaintext attack and chosen ciphertext attack, and the chosen plaintext and adaptive chosen plaintext attack have same complexity;*
2. *The distributions of plaintext and ciphertext of those ciphers are independent for each constant key,*
3. *The best way to find weak keys ($E^{Fe}(k, x'\|x) = E^{Fe}(k', x'\|x)$) of E^{Fe} and E^{Sp} is exhaustive key search attack based on birthday paradox;*
4. *No weakness are found in E^{Fe} and E^{Sp}.*

Remark 3. Let $y'\|y = E^{Fe}(k, x\|x')$, the item 2 of Assumption 1 can be written as follows

$$\begin{aligned} P_{Y'\|Y,M|K=k}(y'\|y, m) &= P_{Y'\|Y|K=k}(y'\|y)P_{M|K=k}(m) \\ &= P_{Y'|K=k}(y')P_{Y|K=k}(y)P_M(m) \end{aligned}$$

So we have

$$\begin{aligned} P_{Y,M|K=k}(y, m) &= P_{Y|K=k}(y)P_M(m) \\ P_{Y',M|K=k}(y', m) &= P_{Y'|K=k}(y')P_M(m). \end{aligned}$$

Remark 4. There exist Feistel block ciphers, which satisfy Assumption 1, or else we can build some attack on the cipher. Of cause no weakness just means immune against known attack.

Assumption 2 *If E^{Fe} satisfies Assumption 1, then replacing the key schedule algorithm with $k^{(i)} \stackrel{def}{=} \psi(k^{i-1}) \oplus k, k^{(0)} = k$, the new E^{Fe} still satisfies Assumption 1.*

Remark 5. In the proof of security of Feistel structure[27–30], the compression function is assumed as pseudo random function. If the $\psi(k)$ is pseudo random function, then $\psi(k) \oplus k$ is still a pseudo random function. The Assumption 2 implies the key schedule algorithm $\psi(k)$ has property of that does not exit i, j with $\psi(k^{(i)}_{\{j\}}) \equiv k_{\{j\}}$.

Theorem 3. *Let the round function f be the format of $f(k^{(i)}, x) = f(x \oplus k^{(i)})$, if E^{Fe} satisfies Assumption 1 and Assumption 2, then there exist FL-function $\tilde{y} = \tilde{F}_c(k, x)$ and $\tilde{y}' = \tilde{F}_{c-1}(k, x)$ satisfying following properties*

1. *$\tilde{F}_c$ is immune against adaptive chosen chaining value attack and adaptive chosen message block attack*[4]*;*
2. *the distributions of $\tilde{Y}$ and X_m are independent for each constant x_h and the distributions of $\tilde{Y}$ and X_h are independent for each constant x_m, that are also hold for $\tilde{Y}'$;*
3. *There are no weakness in $\tilde{F}_c$ and $\tilde{F}_{c-1}$*[5]*.*

Proof. Firstly, we give a conclusion of that. If E^{Fe} has rounds r, key schedule algorithm $\psi(k)$ and round function $f(k^{(i)}, x) = f(x) \oplus k^{(i)}$, then we have

$$E^{Fe}(k_0, \tilde{k} \| x \oplus \tilde{k})^R \oplus \tilde{k} = \tilde{F}_c(\tilde{k}, x) \tag{1}$$

where the key schedule algorithm of $\tilde{F}_c$ is $\tilde{k}^{(i)} = \psi(k_0^{(i)}) \oplus \tilde{k}$. The proof of Equation (1) is follows

When $r = 1$

$$\begin{aligned}(\Psi(f_{k_0^{(1)}})(\tilde{k} \| x \oplus \tilde{k}))^R &= \tilde{k} \oplus f(x \oplus \tilde{k} \oplus \psi(k_0^{(1)})) \\ &= \tilde{0} \oplus f(x \oplus (\psi(k_0^{(0)}) \oplus \tilde{k})) \oplus \tilde{k} \\ &= (\Psi(f_{k_0^{(1)} \oplus \tilde{k}})(\tilde{0} \| x \oplus))^R \oplus \tilde{k}\end{aligned}$$

Assume that for $r < k$, the equation is true then

$$\begin{aligned}&(\Psi(f_{k_0^{(r)}} \circ \ldots \circ f_{k_0^{(1)}})(\tilde{k} \| x \oplus \tilde{k}))^R \\ &= (\Psi(f_{k_0^{(r-2)} \oplus \tilde{k}} \circ \ldots \circ f_{k_0^{(1)} \oplus \tilde{k}})(\tilde{0} \| x))^R \oplus \tilde{k} \\ &\quad \oplus f((\Psi(f_{k_0^{(r-1)} \oplus \tilde{k}} \circ \ldots \circ f_{k_0^{(1)} \oplus \tilde{k}})(\tilde{0} \| x))^R \oplus \tilde{k} \oplus k_0^{(r)}) \\ &= (\Psi(f_{k_0^{(r-2)} \oplus \tilde{k}} \circ \ldots \circ f_{k_0^{(1)} \oplus \tilde{k}})(\tilde{0} \| x))^R \\ &\quad \oplus f((\Psi(f_{k_0^{(r-1)} \oplus \tilde{k}} \circ \ldots \circ f_{k_0^{(1)} \oplus \tilde{k}})(\tilde{0} \| x))^R \oplus (\tilde{k} \oplus k_0^{(r)})) \oplus \tilde{k} \\ &= (\Psi(f_{k_0^{(r)} \oplus \tilde{k}} \circ \ldots \circ f_{k_0^{(1)} \oplus \tilde{k}})(\tilde{0} \| x))^R \oplus \tilde{k}.\end{aligned}$$

Secondly, We give the proof of that, if E^{Fe} satisfy Assumption 1, then $\tilde{F}_c$ satisfy the item 1,2 and 3. Since $\tilde{F}_c$'s message block and chaining value equivalence to the left and right most n bits plaintext of E^{Fe} with a fixed key, respectively, output of $\tilde{F}_c$ equivalence to the right-most n bits ciphertext of E^{Fe} with the fixed key, then we can get the conclusion directly. □

We also can get following theorem.

[4] The definition of adaptive chosen chaining attack or message block attack is parallel to adaptive chosen plaintext attack or adaptive chosen key attack upon block cipher.

[5] No weakness means can not find the inner relation between output and chaining value or output and message block.

Theorem 4. *Let the round function f be the format of $f(k^{(i)}, x) = f(x \oplus k^{(i)})$, if F_c and F_{c-1} satisfies item 1,2 and 3 of Theorem 3, then there exist a Feistel block cipher satisfy item 1,2 and 4 of Assumption 1*

Proof. The proof is analog to the proof of Theorem 3. Since we have

$$F_c(k, x) = \tilde{E}^{Fe}(k, x_0' \| x \oplus x_0')^R \oplus x_0' \tag{2}$$

where the key schedule algorithm of $\tilde{E}^{Fe}$ is $x_0'^{(i)} = \psi(k^{(i)}) \oplus x_0'$. The proof can be given similar to equation (1), we omit it. □

3.2 The Output Distribution of F-HASH

This subsection gives the output distribution of F-hash for selected massage and selected initial value. The conclusions are that, the output distribution of F-Hash for selected message or selected initial value is near to that of compression function. So, if can build a secure Feistel compression function, then that can guaranteers the output distribution of the F-HASH.

Firstly, we give some basic notation and definition, which will be used in the output probability distribution of F-HASH. Let $G : I_\kappa \times I_m \to I_n$, $y = G(k, x)$ then:

$\{(y, k, x)\} \stackrel{def}{=} \{(y, k, x) | k \in I_\kappa, x \in I_m, y \in I_n\}$;

$\{(y, k, x)\}^G \stackrel{def}{=} \{(y, k, x) | (y, k, x) \in \{(y, k, x)\}, G(k, x) = y\}$;

$\{((y_0, k, x)\}^G \stackrel{def}{=} \{((y_0, k, x) | (y, k, x) \in \{(y, k, x)\}^G, y = y_0\}$;

$\{(y, k, x)\}^G_{x \in \Lambda} \stackrel{def}{=} \{(y, k, x) | (y, k, x) \in \{(y, k, x)\}^G, x \in \Lambda\}$;

$\{\{((y_0, k, x)\}^G\}_{y_0 \in \Lambda} \stackrel{def}{=} \bigcup_{y_0 \in \Lambda} \{\{((y_0, k, x)\}^G\}$.

$S_1 \stackrel{def}{=} \max_{x_{m_0}, y_0} \#\{(y_0, x_{m_0}, x_h)\}^{F_{c-1}}$; $S_2 \stackrel{def}{=} \max_{x_{h_0}, y_0} \#\{(y_0, x_m, x_{h_0})\}^{F_{c-1}}$;

$S_3 \stackrel{def}{=} \max_{y_0} \#\{(y_0' \| y_0, x_m, x_{h_0}' \| x_{h_0})\}^{E^{Fe}}$; $T_1 \stackrel{def}{=} \max_{x_{m_0}, y_0} \#\{(y_0, x_{m_0}, x_h)\}^{F_c}$;

$T_2 \stackrel{def}{=} \max_{x_{h_0}, y_0} \#\{(y_0, x_m, x_{h_0})\}^{F_c}$; $T_3 \stackrel{def}{=} \max_{y_0} \#\{(y_0, x_m, x_h)\}^{F_c}$.

Remark 6. Iterated hash function $H(m, x)$, we consider the x can be all value in I_n, because we can redefine a hash function $H(m \| x, IV) = H(m, F(x, IV)) \stackrel{def}{=} H'(m, x')$, the attack on H' may be an attack on H, in selected hash IV is constant.

Let $\tilde{z} = E^{Sp}(u, z)$, $z = H^M(m, x) = h_*$, $h_0 = x$, $u = O_h(m, x) \stackrel{def}{=} \bigoplus_{i=1}^{t} h_i'$, $h_i = F_c(\mathtt{m}_i, h_{i-1})$, $h_i' = F_{c-1}(\mathtt{m}_i, h_{i-1})$, $m = \mathtt{m}_* \| \ldots \| \mathtt{m}_0$, x and m are independent and uniformly distributed in I_n and $\bigcup_{i=1}^{t} I_{n \cdot i}$, respectively.

Lemma 2. *If the compression function $F_c(x_m, x_h)$ satisfy item 2 of Theorem 3 and $i \geq 2$, then u, z, h_i and h_i' are independent from each other, where $i \in [1, t-1]$ for h_i and $i \in [1, t]$ for h_i'.*

Proof. That is direct conclusion of Theorem 3. □

Theorem 5. *If the compression function $F_c(x_m, x_h)$ satisfy item 2 of Theorem 3, then F-HASH $\tilde{z} = H^F(m, x)$, $z = H^M(m, x)$ have*

1. $P_{\dot{Z}|M=m}(z) \leq 2^{-n} T_1^{\frac{|m|}{n}}$;
2. $P_{\dot{Z}|X=x}(z) \leq 2^{-n} T_2$;
3. $P_{\tilde{Z}|M=m}(\tilde{z}) \leq 2^{-n} S_1$;
4. $P_{\tilde{Z}|X=x}(\tilde{z}) \leq 2^{-n} S_2$.

The proof is given by deduction theory in Appendix 3.2.

3.3 Immunity Against Collision Attack and Preimage Attack

This section gives security of F-HASH against collision attack and preimage attack. The conclusion of this part is based on theorem of [24] that, if the compression function is immune against adaptive chosen message attack and adaptive chosen chaining value attack, and the output distribution of the iterated hash structure is given, then the hash is secure.

Definition 8. *The definitions about the advantage of A in finding Primage and Collision of function H are as follows, write $\widetilde{A}dv(A) \stackrel{def}{=} \max\{Adv(A)\}$ where the maximum is get the luckiest adversary's advantage, $Adv(q) \stackrel{def}{=} \max\{Adv(A)\}$, where the maximum is taken over adversaries that ask at most q queries. If F is invertible with F^{-1}, then A can ask queries of F and F^{-1}, the whole search space is whole space.*

- ***Fixed Start Preimage Attack***

$$\widetilde{A}dv_H^{FixP}(A) = \max_{y_0, x_0} Pr[y_0 \in I_n, x_0 \in I_n; \omega \leftarrow A^{F,H} : \omega \in \{(z_0, m, x_0)\}^H]$$

- ***Fixed Start Collision Attack***

$$\widetilde{A}dv_H^{FixC}(A) = \max_{y_0, x_0} Pr[x_0 \in I_n; \omega, \omega' \leftarrow A^{F,H} : \omega, \omega' \in \sigma, \sigma \in \{\{(z_0, m, x_0)\}^H\}_{z_0 \in I_n}]$$

Theorem 6. *Let F_c and F_{c-1} satisfy Theorem 3, then F-HASH $\tilde{z} = H^F(m, x)$ has*

- $\widetilde{A}dv_{H^F}^{FixP}(q) \leq \max\{2q\frac{S_2}{2^n}, q\frac{S_1}{2^n}\}$;
- $\widetilde{A}dv_{H^F}^{FixC}(q) \leq \max\{q(q-1)\frac{S_2}{2^n}, q\frac{S_1}{2^n}\}$.

Proof. F_c and F_{c-1} satisfy Item 2 of Theorem 3, the best way of finding collision or preimage attack is exhaustive search. F_c and F_{c-1} satisfy Item 2 of Theorem 3, then output distribution satisfy Theorem 5, we have the conclusion from Theorem18 of [24]. □

3.4 Other Attacks on F-HASH

The other attacks on F-HASH needs more discussion, there are some.

Multi Collision[18] Suppose that multi collision is possible, for each inner collision $H^M(m_{i+1}, H^M(m_i\| \dots \|m_1, x_0)) = H^M(m'_{i+1}, H^M(m'_i\| \dots \|m'_1, x_0))$, $i \in [1, t]$, if the inner collision can make true collision requires $O_h(m, IV) = O_h(m', IV)$. That does not always hold when the inner collision occurs. In fact it will happen with high probability when $|m_i| = n$.

Extension Attack[35] If the extension collision is possible, when there exists an inner collision $H^M(m, x_0) = H^M(m', x_0)$, the extension should be with $O_h(m''\|m, IV) = O_h(m''\|m', IV)$, as the complexity of finding $O_h(m''\|m, IV) = O_h(m''\|m', IV)$ is $\mathcal{O}(2^{\sqrt{n}})$. When the collision is final collision $H^F(m, x) = H^F(m', x)$, not a inner collision, the extension attack is impossible.

Fixed Point Attack The requirement of success of the fixed point attack is similar to that of a multi collision attack, which requires $O_h(m, IV) = O_h(m', IV)$ and the fixed block length should be $|m_i| = n$.

4 Discussions and Conclusions

Our security discussion of F-HASH is based on the security of Feistel Block cipher, and we assume the Fesitel block cipher is secure. This section we give more discussion on the realized design of Feistel compression function.

4.1 The Value of T_1,T_2,S_1 and S_2

This subsection, we discuss the upper bound of T_1,T_2,S_1 and S_2.

Let $g : I_{2n} \to I_{2n}, y\|y' = \mathtt{g}(x\|x')$ be a random permutation, then we have[3]

$$P_{Y'|X'=x_0}(y = \mathtt{g}(x_0)) = 2^{-2n}$$

then $y = (\mathtt{g}(x'_0\|x))^R$ is random function. Let $\mathtt{f}(x_0, x) \stackrel{def}{=} (\mathtt{g}(x'_0\|x))^R$

$$P_{Y^R|X=x_0}(y = \mathtt{f}(x'_0\|x_0)) = 2^{-n}$$

then we have[3]

$$P_{Y^R|X_1=x_1,X_2=x_2}(y = \mathtt{f}(x'_0\|x_1), y = \mathtt{f}(x'_0\|x_2)) = \begin{cases} 2^{-2n} & x_1 \neq x_2 \\ 2^{-n} & x_1 = x_2 \end{cases}$$

In block cipher E^{Fe}, for each fixed key, if we can not distinguish the E^{Fe} from a Pseudo-random permutation, then we have

$$P(T_1 = k) = 2^{-k\cdot n}2^n, \qquad P(S_1 = k) = 2^{-k\cdot n}2^n, \qquad k \in \mathbf{N}$$

If the F_c is selected as Equation 1, then we have

$$P(T_2 = k) = 2^{-k \cdot n} 2^n, \qquad P(S_2 = k) = 2^{-k \cdot n} 2^n, \qquad k \in \mathbf{N}$$

If for each $x_0' \| x_0$, we can not distinguish $E^{Fe}(k, x_0' \| x_0)$ from a random function then we have

$$P(T_2 = k) = 2^{-k \cdot n} 2^n, \qquad P(S_2 = k) = 2^{-k \cdot n} 2^n, \qquad k \in \mathbf{N}.$$

From above discussion, we known the upper bound of T_1,T_2,S_1 and S_2, but those values are only with maximum probability of equals 1, which is need more discussion. But the more discussion on those values are also required in block cipher design.

4.2 Round function and Key Schedule Algorithm

In the proof of Theorem 3, we find that x' can be moved into the key schedule algorithm and for the whole discussion we assume the round function f is permutation. The most common design of round function with permutation is SPN structure. The SP structure is used in Feistel structure can result in the linear part can be moved into the previous rotund or the posterior round[23], so we prefer the round function with SPS(SBox-Linear part-Sbox) structure.

The key schedule algorithm $\psi(k)$ is assumed not to be a linear transformation. We prefer the key schedule algorithm itself is pseudo random function, which has been discussed in PhD paper of Rijmen[36].

4.3 The Round Number of F_c Function

The block cipher of Feistel structure is require more round than that of SPN structured block cipher with same round function and key schedule algorithm. On that condition, the block cipher with Feistel structure has double size that of SPN Block cipher.

The Feistel Compression function and SPN block cipher with same round function and key schedule algorithm have same block size. In fact, the requirement of Feistel compression function to build F-HASH require same block size as SPN block cipher, but the F-MAC and FBC mode require more. The realized round number should depend on the key schedule algorithm and the round function.

4.4 The Motivation of $E^S P$ Cipher

The motivation of last compression of F-HASH is to randomize the output distribution of the hash. without that part, the F-HASH become a iterated hash with Merkle-Damagård structure.

4.5 Contrast with Other Structures

The output distribution of F-HASH is near to uniformly distribution. 3C also have such property, if we can select a good compression function. Those part of discussion can see the paper[24]. The most outstanding of this structure is that, the security of structure and realized hash relies on the security of basement of block cipher.

4.6 Securities about F-MAC and FBC Mode

The security of F1-MAC, F2-MAC and FBC mode can be discussed analogously to F-HASH, and since the conditional probability of F-HASH is given, we can give the security prove of the MACs and FBC mode. The security of F2-MAC can also be discussed similar as CBC-MAC[2] and the security of FBC mode is similar as that of CBC mode[3], and prohibits the attack based on fixed IV[3]. More precise discussion and true attacks should be based on the assumption of round function f and key schedule algorithm ψ. This paper only gives the proof of security of the structure.

4.7 Conclusion

In this paper we present a new way to construct hash function. Security of FL-Function relies on the security of Feistel structured block cipher's round function and key schedule algorithm. And the design of FL-function require higher design criteria than that of block cipher. All design principle of block cipher can be used in design of hash function. If we can design a secure hash function based on FL-structure then we can design a more secure block cipher. Due to page limitation, the page limitation, security discussion about F-MAC and FBC Mode is omitted.

Acknowledgement The previous two sections of this version are rewritten by Dr.Matt Henricksen. He also gives many suggestions on reordering the remaining sections. And also, more comments will be gotton from him. Since he think, his contribution not passed 25persent of this previous version, he is not a co-author of this paper. I want to give special thank to him.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima and T. Tokita.: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. SAC2000. LNCS 1281. Springer-Verlag, Berlin Heidelberg New York (2000) pp.39-56.
2. M. Bellare, K. Pietrzak, and P. Rogaway, Improved Security Analyses for CBC MACs, In Advances in Cryptology Crypto 2005, LNCS 3621, pp.527-545, 2005.
3. M. Bellare and P. Rogaway, Introduction to Modern Cryptography.

4. 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.
5. E. Biham and A. Shamir, Diffrential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, Vol.4, No.1, p..3-72, 1991.
6. E.Biham and R.Chen. Near-Collisions of SHA-0,In Advances in Cryptology CRYPTO'2004, LNCS 3152,p..290-305, 2004.
7. 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, LNCS 2442, Springer-Verlag, pp.320-335, 2002.
8. C.Chchin. Entropy Measures and Uncoditional Security in Cryptography, PHD thesis.
9. J.Daemen and V. Rijmen, "A new MAC Construction Alred and a Specific Instance Alpha-MAC,", Fast Software Encryption 2005, LNCS , Springer-Verlag.
10. I.Damgård. A design principle for hash functions. In G. Brassard, editor, Advances in Cryptology-CRYPTO'89, LNCS 435. Springer-Verlag, 1990.
11. H. Feistel. Cryptography and Computer Privacy. Scientific American.
12. D. Feng, W. Wu :Block Cipher Analysis and Design.
13. FIPS 46-3: Data Encryption Standard. In National Institute of Standards and Technology, Oct. 1999.
14. Helena Handschuh and David Naccache. SHACAL, 2001. Available at https://www.cosic.esat.kuleuven.ac.be/nessie/tweaks.html/shacal tweak.pdf.
15. Carlo Harpes, Gerhard Kramer, and James Massey. A generalization of linear cryptanalysis and the applicability of Matsui's Piling-up lemma. In Louis Guillou and Jean-Jacques Quisquater, editors, Advances in Cryp- tology - Proceedings of EUROCRYPT 95, volume 921 of Lecture Notes in Computer Science, pp. 24-38. Springer-Verlag, 1995.
16. P.Gauravaram, W.Millan, J. Gonzalez Neito and E. Dawson: 3C-A Provably Secure Pseudorandom Function and Message Authentication Code. A New mode of operation for Cryptographic Hash Function. The preliminary draft version of this work is available at eprint-2005/390 .
17. P.Junod and S. Vaudenay, FOX : a New Family of Block Ciphers, Selected Areas in Cryptography-SAC 2004,LNCS 2595, pp.131-146
18. A. Joux, Multicollisions in iterated Hash functions. Application to cascaded constructions. Proceedings Crypto 2004, Springer-Verlag LNCS 3152, pp.306-316, 2004.
19. A. Joux, P.Carribault, W. Jalby and C. Lemuet. Collisions in SHA-0. Presented at the rump session of CRYPTO 2004, 2004.
20. X. Lai and J. L. Massey: Hash functions based on block ciphers. In Advances in Cryptology Eurocrypt'92, LNCS 658. Springer-Verlag, Berlin Hei-delberg New York (1993) pp.55-70.
21. M. Luby and C. Rackoff, How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing, Vol. 17, No. 2 (1988) pp.373-386.
22. R.C.Merkle, One Way Hash Functions and DES, In G. Brassard, editor, Advances in Cryptology-CRYPTO' 89, LNCS 435 Springer-Verlag, pp.428-446, 1990.
23. D. Lei, L. Chao, F. Keqin. New Observation On Camellia. Selected Area in Cryptography, SAC 2005, LNCS 3897, pp.51-64, 2006.
24. D. Lei. New Integrated proof method On Iterated Hash Structure. http://eprint.iacr.org/2006/147.

25. Stefan Lucks: A Failure-Friendly Design Principle for Hash Functions, ASIACRYPT 2005, LNCS 3788, pp.474-494, 2005.
26. NESSIE Consortium. Ongoing Research Areas in Symmetric Cryptography, January 2005. Avalaible at URL https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/ D.STVL.3-2.1.pdf.
27. J. Patarin About Feistel Schemes with Six (or More) Rounds, in Fast Software Encryption 1998, pp.103-121.
28. J. Patarin. Luby-Rackoff 7 Rounds are Enough for $2n^{(1-\varepsilon)}$ Security. CRYPTO'03, Springer, LNCS 2729, pp.513-529,
29. J. Patarin, Security of Random Feistel Scemes with 5 or more rounds. CRYPTO'04, LNCS 3152, pp.106-122, Springer.
30. J.Patarin, Generic Attacks on Feistel Schemes, Available from the author.
31. J.Patarin, Security of Random Feistel Schemes with 5 or more rounds, Available from the author.
32. G.Piret, Luby-Rackoff Revisited: On the Use of Permutations as Inner Functions of a Feistel Scheme,Designs, Codes and Cryptography, 39, pp.233-245, 2006
33. G.Piret, Block Ciphers: Security Proofs, Cryptanalysis, Design, and Fault Attacks, PHD, 2005.
34. B.Preneel: The State of Cryptographic Hash Functions. In Lectures on Data Security, LNCS 1561. Springer-Verlag, Berlin Heidelberg New York (1999) pp.158-182.
35. 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. LNCS 1528. Springer-Verlag, Berlin Heidelberg New York(1998) pp.106-131.
36. V. Rijmen, Cryptanalysis and design of iterated block ciphers, Katholieke Universiteit Leuven, Belgium, 9 October 1997
37. C.E.Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal, Vol.27, pp.379-423,1948.
38. C.E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, Vol 28: pp.656-715, 1949.
39. S. Vaudenay. On the Lai-Massey scheme. In K. Lam, T. Okamoto, and C. Xing, editors, Advances in Cryptology - ASIACRYPT'99, LNCS 1716 pp.8-19. Springer-Verlag, 2000.
40. S. Vaudenay. Decorrelation: A Theory For Block Cipher security. Journal of Cryptology, 16(4):pp.249-286, 2003.
41. 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.
42. X. Wang, H. Yu, How to Break MD5 and Other Hash Functions, EUROCRYPT'2005, Springer-Verlag, LNCS 3494, pp.19-35, 2005.
43. A.F.Webster and S. E. Tavares. On the design of S-boxes. Advances in Cryptology-CRYPTO'85, LNCS 218, pp.523-534.

A Proof of Theorem 3.2

Let us restate the following theorem.

Theorem 7. *If the compression function $F_c(x_m, x_h)$ satisfy item 2 of Theorem 3, then F-HASH $\tilde{z} = H^F(m, x)$, $z = H^M(m, x)$ have*

1. $P_{\tilde{Z}|M=m}(z) \leq 2^{-n} T_1^{\frac{|m|}{n}}$;

2. $P_{\dot{Z}|X=x}(z) \leq 2^{-n}T_2$;
3. $P_{\tilde{\tilde{Z}}|M=m}(\tilde{z}) \leq 2^{-n}S_1$;
4. $P_{\tilde{\tilde{Z}}|X=x}(\tilde{z}) \leq 2^{-n}S_2$.

Proof. The proof of Theorem 5 is given by deduction theory.

1. When $t = 1$

$$\begin{aligned} P_{\dot{Z}|M=m}(z) &\leq \max_{m_0,z_0} \sum_{x\in I_n} P_X(x)\chi_{F_c(m_0,x)}(z_0) \\ &= \max_{m_0,z_0} \sum_{i\in[1,2^n]} 2^{-n}\#\{(m_0,x_i,z_0)\}^{F_c} \leq 2^{-n}T_1 \end{aligned}$$

Suppose $t < l$, the inequality is true. When $t = l$

$$\begin{aligned} P_{\dot{Z}|M=m}(z) &= P_{\dot{Z}|M=\mathtt{m}_l\|m'}(z) \\ &= \sum_{x\in I_n} P_X(x)\chi_{F_c(\mathtt{m}_l,H^M(m,x))}(z) \\ &= \sum_{x\in I_n}\sum_{u\in I_n} \frac{1}{2^n}\cdot\chi_{F_c(\mathtt{m}_l,u)}(z)\cdot\chi_{H^M(m',x)}(u) \\ &= \sum_{u\in I_n}\sum_{x\in I_n} \frac{1}{2^n}\cdot\chi_{F_c(\mathtt{m}_l,u)}(z)\cdot\chi_{H^M(m',x)}(u) \\ &= \sum_{u\in I_n} (\chi_{F_c(\mathtt{m}_l,u)}(z)\cdot\sum_{x\in I_n}\frac{1}{2^n}\chi_{H^M(m',x)}(u)) \\ &= \sum_{u\in I_n} \chi_{F_c(\mathtt{m}_l,u)}(z)\cdot P_{\dot{U}|M'=m'}(u) \\ &\leq 2^{-n}T_1^{l-1}\sum_{u\in I_n}\chi_{F_c(\mathtt{m}_l,u)}(z) \\ &\leq 2^{-n}T_1^{l-1}T_1 = 2^{-n}T_1^l \end{aligned}$$

2. When $t = 1$

$$\begin{aligned} P_{\dot{Z}|X=x}(z) &\leq \max_{x_0,z_0}\sum_m P_M(m)\chi_{F_c(m,x_0)}(z_0) \\ &= \max_{x_0,z_0}\sum_i 2^{-n}\#\{(\mathtt{m}_i,x_0,z_0)\}^{F_c} \leq 2^{-n}T_2 \end{aligned}$$

When $t > 1$

$$\begin{aligned} P_{\dot{Z}|X=x}(z) &= \sum_{m\in\cup_{i=1}^{l} I_{n\cdot i}} P_M(m)P_{\dot{Z}|M=m,X=x}(z) \\ &= \sum_{\mathtt{m}_l\in I_n}\sum_{m'\in\cup_{i=1}^{l-1} I_{n\cdot i}} P_{M'}(m')P_{M_l}(\mathtt{m}_l) \end{aligned}$$

$$
\begin{aligned}
& P_{\dot{Z}|M=m,X=x} P(z = F_c(\mathtt{m}_l, H^M(m', x))) \\
= & \sum_{\mathtt{m}_l \in I_n} \sum_{m' \in \cup_{i=1}^{l-1} I_{n\cdot i}} \sum_{u \in I_n} \\
& P_{M'}(m') P_{M_l}(\mathtt{m}_l) \cdot \chi_{F_c(\mathtt{m}_l,u)}(z) \cdot \chi_{H^M(m',x)}(u) \\
= & \sum_{u \in I_n} \sum_{\mathtt{m}_l \in I_n} P_{M_l}(\mathtt{m}_l) \cdot \chi_{F_c(\mathtt{m}_l,u)}(z) \\
& \sum_{m' \in \cup_{i=1}^{l-1} I_{n\cdot i}} P_{M'}(m') \cdot \chi_{H^M(m',x)}(u) \\
= & \sum_{u \in I_n} P_{\dot{Z}|U=u}(z) P_{\dot{U}|X=x}(u) \\
\leq & \, 2^{-n} T_2 \sum_{u \in I_n} P_{\dot{U}|X=x}(z) = 2^{-n} T_2
\end{aligned}
$$

3. $\forall\ t \geq 1$

$$
\begin{aligned}
P_{\tilde{\dot{Z}}|M=m}(\tilde{z}) &= P_{\tilde{\dot{Z}}|M=m}(\tilde{z} = E^{Sp}(u, z), u = O_h(m, x), z = H^M(m, x)) \\
&= \sum_{x,u,z \in I_n} P_X(x) \chi_{E^{Sp}(z,u)}(\tilde{z}) \chi_{H^M}(z, m, x) \chi_{O_h(m,x)}(u) \\
&= \sum_{u,z \in I_n} \chi_{E^{Sp}(z,u)}(\tilde{z}) \sum_{x \in I_n} P_X(x) \chi_{H^M}(z, m, x) \\
&\quad \sum_{x \in I_n} P_X(x) \chi_{O_h(m,x)}(u) \\
&= \sum_{u,z \in I_n} \chi_{E^{Sp}(z,u)}(\tilde{z}) P_{\dot{U}|M=m}(u) P_{\dot{Z}|M=m}(z) \\
&\leq \max_{u_0} P_{\dot{U}|M=m}(u_0) 2^n \sum_z P_{\dot{Z}|M=m}(z) \sum_u 2^{-n} \chi_{E^{Sp}(z,u)}(\tilde{z}) \\
&= \max_{u_0} P_{\dot{U}|M=m}(u_0) 2^n \sum_z P_{\dot{Z}|M=m}(z) P_{\tilde{Z}|Z=z}(\tilde{z}) \\
&\leq \max_{u_0} P_{\dot{U}|M=m}(u_0) \max_{z_0, \tilde{z_0}} 2^n P_{\tilde{Z}|Z=z_0}(\tilde{z_0}) \sum_z P_{\dot{Z}|M=m}(z) \\
&= \max_{u_0} P_{\dot{U}|M=m}(u_0)
\end{aligned}
$$

And also

$$
\begin{aligned}
P_{\dot{U}|M=m}(u) &= \sum_{x \in I_n} P_X(x) P_{U|M=m,X=x}(u = h'_1 \oplus \bigoplus_{i=2}^{t} h'_i) \\
&= \sum_{x \in I_n} P_X(x) P_{U|M=m'\|m_1,X=x}(u = v \oplus h'_1, v = \bigoplus_{i=2}^{t} h'_i) \\
&= \sum_{x \in I_n} \sum_{v \in I_n} P_X(x) P_{UV|M=m'\|m_1,X=x}(u = v \oplus h'_1, v = \bigoplus_{i=2}^{t} h'_i)
\end{aligned}
$$

$$= \sum_{x \in I_n} \sum_{v \in I_n} P_X(x) P_{U|M_1=\mathtt{m}_1, X=x}(u = h'_1 \oplus v)$$
$$P_{V|M'=m', X=x}(v = \bigoplus_{i=2}^{t} h'_i)$$
$$= \sum_{v \in I_n} P_{U|M_1=\mathtt{m}_1}(u = h'_t \oplus v) P_{V|M'=m'}(v = \bigoplus_{i=2}^{t} h'_i)$$
$$= \max P_{U|M_1=\mathtt{m}_1}(u) \sum_{v} P_{V|M'=m'}(v = \bigoplus_{i=2}^{t} h'_i) \leq \frac{S_1}{2^n}$$

4. $\forall\ t \geq 1$

$$P_{\tilde{\tilde{Z}}|X=x}(\tilde{z}) = P_{\tilde{\tilde{Z}}|X=x}(\tilde{z} = E^{Sp}(u,z), u = O_h(m,x), z = H^M(m,x))$$
$$= \sum_{u,z \in I_n} \sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} P_M(m) P_{\tilde{Z}|\dot{U}=u, Z=z}(\tilde{z})$$
$$P_{\dot{U},\dot{Z}|M=m,X=x}(u = O_h(m,x), z = H^M(m,x))$$
Since $P_M(x) = 2^{-\sum_i^t i \cdot n}$ and u, z are independent
$$= \sum_{u,z \in I_n} \chi_{E^{Sp}(z,u)}(\tilde{z})$$
$$\sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} P_M(m) P_{\dot{U}|M=m,X=x}(u = O_h(m,x))$$
$$\sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} P_M(m) P_{\dot{Z}|M=m,X=x}(z = H^M(m,x))$$
$$= \sum_{u,z \in I_n} \chi_{E^{Sp}(z,u)}(\tilde{z}) P_{\dot{U}|X=x}(u) P_{\dot{Z}|X=x}(z)$$
$$\leq \max_{u_0} P_{\dot{U}|X=x}(u_0) 2^n \sum_{z} P_{\dot{Z}|X=x}(z) \sum_{u} 2^{-n} P_{\tilde{\tilde{Z}}|U=u,Z=z}(\tilde{z})$$
$$= \max_{u_0} P_{\dot{U}|X=x}(u_0) 2^n \sum_{z} P_{\dot{Z}|X=x}(z) P_{\tilde{\tilde{Z}}|Z=z}(\tilde{z})$$
$$\leq \max_{u_0} P_{\dot{U}|X=x}(u_0) \max_{z_0, \tilde{z_0}} 2^n P_{\tilde{\tilde{Z}}|Z=z_0}(\tilde{z_0}) \sum_{z} P_{\dot{Z}|X=x}(z)$$
$$= \max_{u_0} P_{\dot{U}|X=x}(u_0)$$

And also

$$P_{\dot{U}|X=x}(u) = \sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} P_M(m) P_{U|M=m,X=x}(u = h'_1 \oplus \bigoplus_{i=2}^{t} h'_i)$$
$$= \sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} P_M(m) P_{U|M=m' \| m_1, X=x}(u = v \oplus h'_1, v = \bigoplus_{i=2}^{t} h'_i)$$

$$
\begin{aligned}
&= \sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} P_M(m) P_{UV|M=m' \| m_1, X=x}(u = v \oplus h'_1, V = \bigoplus_{i=2}^{t} h'_i) \\
&= \sum_{m \in \cup_{i=1}^{t} I_{n \cdot i}} \sum_{v \in I_n} P_M(m) P_{U|M_1=\mathtt{m}_1, X=x}(u = h'_1 \oplus v) \\
&\quad P_{V|M'=m', X=x}(v = \bigoplus_{i=2}^{t} h'_i) \\
&= \sum_{v \in I_n} \sum_{\mathtt{m}_t \in I_n} P_{M_t}(\mathtt{m}_t) P_{U|M_1=\mathtt{m}_1, X=x}(u = h'_1 \oplus v) \\
&\quad \sum_{m' \in \cup_{i=1}^{t-1} I_{n \cdot i}} P_{V|M'=m', X=x}(v = \bigoplus_{i=2}^{t} h'_i) \\
&= \sum_{v \in I_n} P_{U|X=x}(u = h'_1 \oplus v) P_{V|X=x}(v = \bigoplus_{i=2}^{t} h'_i) \\
&= \max_{u_0} P_{U|X=x}(u_0) \sum_{v} P_{V|X=x}(v = \bigoplus_{i=2}^{t} h'_i) \leq \frac{S_2}{2^n}
\end{aligned}
$$

□