The Optimal MISTY-Type Tweakable Transformations

Fengtong Wen
School of Science, University of Jinan, inan, China · wftwq@163.com

Abstract—In order to improve the blockcipher's efficiency and debase its operating costs, we propose some optimal structures of tweakable blockciphers without using pre-existing block-cipher on the basis of MISTY-Type transformation. We optimize the 5-round structure by using the XOR-universal permutation to replace the first three random permutation. Finally, we give the concrete cryptanalysis for the CPA-secure 5 round Optimal MISTY-Type tweakable blockciphers.

Keywords—Cryptography; block cipher; tweakable blockcipher; MISTY-Type structure; XOR-universal permutation

1. INTRODUCTION

In cryptography, a blockcipher, regarded as of permutations on a message space indexed by a secret key, is a symmetric key cipher. When encrypting, the encryption algorithm $E$ takes two inputs—a secret key $K$ and a message block $M$ and outputs a corresponding length block of ciphertext. The decryption algorithm $D$ reverse the process. We call a blockcipher pseudorandom permutation if no attacker with polynomially many encryption queries can distinguish between the block cipher and a random permutation. A tweakable blockcipher is a blockcipher which takes an extra input, the tweak $T$, that is used only to provide variation and is easy to be changed without more cost. A tweakable blockcipher is secure if it is indistinguishable from a family of random permutation indexed by the tweak $T$. The notion of tweakable blockcipher was formalized by Liskov et al.[1], they describe two levels of security: a CPA-secure tweakable blockcipher is one that is indistinguishable from a random permutation family under chosen plaintext attack; a CCA-secure tweakable blockcipher is one that is indistinguishable from a random permutation family under chosen ciphertext attack.

Tweakable blockcipher has many practical application in the field of computer science. An important application is that of disk encryption as has been pointed out by Halevi and Rogaway in [2]. Here the disk sectors are separately encrypted and the sector addresses are taken to be the tweaks. Thus, if the plaintext block $P$ is encrypted twice under the same key, the output ciphertext blocks will not be the same.

MISTY-Type structure was firstly introduced by Matsui[3]. It was applied to the block cipher MISTY[4], so we call it as MISTY-Type structure. It has many good property. Matsui showed that MISTY-Type structure was faster and more robust than Feistel structure on linear cryptanalysis and differential cryptanalysis. It has been an actively studied class of construction. Ju-Sung Kang et al.[5] prove that the four round MISTY-Type transformations are pseudorandom permutation ensembles for non-adaptive distinguishers. Wen[6] proved that the four round tweakable MISTY-Type transformations were not pseudorandom permutation ensembles and some 5 round round tweakable MISTY-Type transformations were CPA-secure.

2. PRELIMINARIES

Let $I_n$ denote the set of $n$-bit strings and $Perm_n$ be the set of all permutations from $I_n$ to itself where $n$ is positive integer.
Definition 1. Permutation set is called a TPE if all permutations in $Perm_n$ are uniformly distributed.

Definition 2.[1] Tweakable blockcipher is a triple of algorithms $(G; E; D)$ for key generation, encryption and decryption, respectively. The algorithms, $G(\cdot)$, $E(\cdot)$, $D(\cdot)$, are all efficiently computable, and where the correctness property holds: that is, for all $M, T$ and $K \in G(\cdot)$, $DK(EK(M; T); T) = M$. Over all adversaries with access to an encryption oracle, the maximum advantage is defined as:

$$ADV_{\varepsilon}(E, q, t) = \max_{\varepsilon} \left[ |p(A^\varepsilon(1^n) = 1) - p(A^0(1^n) = 1)| \right]$$

where $1$ is a random permutation family indexed by $T$; $(2)\varepsilon$ is allowed to make at most $q$ oracle queries. A tweakable blockcipher is CPA-secure if for all $n$, for $q$ queries and time $t$, $ADV_{\varepsilon}(E, q, t)$ is negligible in $n$.

Definition 3.(MISTY-Type Structure). For some input $\text{tweak}\text{-}\text{able blockcipher}$ is CPA-secure if for all $n$, for $q$ queries and time $t$, $ADV_{\varepsilon}(E, q, t)$ is negligible in $n$.

Definition 4.(MISTY-Type Tweakable Blockcipher). It is a MISTY-Type structure with adding a tweak in some location. The concrete scheme is defined as: for some input $(L, R)$,

$$L_{\alpha} = R; R_{\alpha} = f_{\alpha}(L) \oplus R, 1 \leq i \leq n$$

where the input is $M = (L_n, R_n) = (L, R)$, the output after $n$ round is $(L_n, R_n)$, each $f_{\alpha} \in Perm_n$ is a random permutation.

Definition 5.[7] $\varepsilon - \text{XOR}$ universal permutation ensemble. Let $H$ be a permutation family over $L_\alpha$, $H$ is $\varepsilon - \text{XOR}$ universal permutation ensemble if the following condition satisfied: for any two distinct element $x \neq y \in L_\alpha$ and any element $z \in L_\alpha$,

$$P[h(x) \oplus h(y) = z] \leq \varepsilon$$

Lemma 1. Let $H$ be $\varepsilon - \text{XOR}$ universal permutation ensemble. $h_1, h_2$ are independently chosen from $H$. Then for any $a, b, c, d \in L_\alpha$, such that $a \neq b, c \neq d$

$$P[h_1(a) \oplus h_1(b) \oplus h_1(c) \oplus h_1(d) = y] \leq 2^s \varepsilon^2$$

Proof. Let $A$ be the event of $h_1(a) \oplus h_1(b) \oplus h_1(c) \oplus h_1(d) = y$ and $A_j$ be the event of $h_1(a) \oplus h_1(b) = w_j$ for $1 \leq j \leq 2^s$, where $L_{w} = \{w_1, \ldots, w_{2^s}\}$. Then by definition 5, we obtain that

$$P(A \cap A_j) = P(h_1(a) \oplus h_1(b) = w_j)P(h_2(c) \oplus h_2(d) = y \oplus w_j) \leq \varepsilon^2$$

Therefore, $P(A) = \sum_{j=1}^{2^s} P(A \cap A_j) \leq 2^s \varepsilon^2$.

Lemma 2. Let $H$ be $\varepsilon - \text{XOR}$ universal permutation ensemble. $h_1, h_2, h_3$ are independently chosen from $H$. Then for any $a \neq b, c \neq d, p \neq q, y \in L_\alpha$

$$P[h_1(a) \oplus h_1(b) \oplus h_1(c) \oplus h_1(d) \oplus h_1(p) \oplus h_1(q) = y] \leq 2^{s-1} \varepsilon^3$$

3. **OPTIMAL MISTY-TYPE TWEAKABLE BLOCKCIPHERS WITH CPA SECURITY**

In this section, we will discuss the CPA security of 5 round optimal tweakable MISTY-Type structure. In the optimal structure, in order to improve its efficiency and debase its running costs, we use the XOR-universal permutation to replace the first three random permutation of the 5 round MISTY-Type tweakable structure. A concrete scheme is defined as: for some input $(L, R, T)$,

$$R_1 = h_1(L_{\alpha}) \oplus R_{\alpha}, L_{\alpha} = R; R_2 = h_2(L_{\alpha} \oplus T) \oplus R_{\alpha}, L_{\alpha} = R$$

$$R_3 = h_3(L_{\alpha} \oplus T) \oplus R_{\alpha}, L_{\alpha} = R; R_4 = f_1(L_{\alpha}) \oplus R_{\alpha}, L_{\alpha} = R$$

where the input is $M = (L_n, R_n) = (L, R), f_1, f_2 \in Perm_n$, are random permutation. $h_1, h_2, h_3$ are XOR universal permutation.

Theorem 1. Let $H$ be $\varepsilon - \text{XOR}$ universal permutation ensemble, $h_1, h_2, h_3 \in H$, $f_1, f_2 \in Perm_n$, they are independent each other. Then the above 5 round optimal MISTY-Type tweakable transformation $T$ is indistinguishable(in a CPA attack) from a random $2n$-bit permutation $\Pi_{n}$ indexed by $T$. 

Proof. A can query an oracle $O$, $O$ chose a permutation from

For $\Pi_n$. We assume that the attacker $A$ makes $q$ different queries $(L^1, R^1, T^1), \ldots, (L^q, R^q, T^q)$ to the oracle $O$. Let $(L^i_j, R^i_j), i = 1, \ldots, q; j = 1, 2, 3, 4$ be the $j$-th round output in the $i$-th oracle query. Let $A_q$ denote the event that $L^i_1, L^i_2, \ldots, L^i_q$ are all distinct. $A_q$ denote the event that $R^i_1, R^i_2, \ldots, R^i_q$ are all distinct. If $A_q$ occurs, we then can see that $L^i_1, L^i_2, \ldots, L^i_q$ are completely random, since $L^i_1 = R^i_1 \oplus f(L^i_1), i = 1, \ldots, q$ and $f$ is a random permutation. Similarly, if $A_q$ occurs, then $r^i_1, r^i_2, \ldots, r^i_q$ are completely random. So $(L^i_1, R^i_1), (L^i_2, R^i_2), \ldots, (L^i_q, R^i_q)$ are completely random permutation. Therefore, if $A_q$ and $A_q$ occur, then $ADV_A$ is bounded above as follows:

$$ADV_A = |P(A \rightarrow 1|O \leftarrow \Gamma) - P(A \rightarrow 1|O \leftarrow \Pi_{2n}|)$$

$$= P((A \rightarrow 1|O \leftarrow \Gamma)A_L \cap A_R | P(A_L \cap A_R) + P((A \rightarrow 1|O \leftarrow \Gamma)A_L \cap A_R | P(A_L \cap A_R)$$

$$-P((A \rightarrow 1|O \leftarrow \Pi_{2n})A_L \cap A_R | P(A_L \cap A_R) - P((A \rightarrow 1|O \leftarrow \Pi_{2n})A_L \cap A_R | P(A_L \cap A_R)|$$

$$\leq P(A_L \cap A_R) \leq \sum_{1 \leq i, j \leq q} P(L^i_3 = L^j_3 \cap R^i_3 = R^j_3)$$

Now we estimate $P(L^i_3 = L^j_3, R^i_3 = R^j_3), 1 \leq i, j \leq q$. Let $(L_n, R_n, T) = (L, R, T)$. We have the following four cases.

Case 1. $L^i_0 = L^j_0, R^i_0 \neq R^j_0$. In this case it is easy to see that $P(L^i_3 = L^j_3) = P(h_2(R^i_0 \oplus T^i) \oplus R^j_0 = h_2(R^j_0 \oplus T^j) \oplus R^i_0) \leq \epsilon$ (by Definition 5), since $h_2$ is a $\epsilon - XOR$ universal permutation. We can obtain by lemma 1 and definition 5 that

$$P(R^i_3 = R^j_3) = P(h_3(R^i_0 \oplus h(L^i_0)) \oplus R^j_0 = h_2(R^j_0 \oplus T^j)) = \leq \max(2^\epsilon, \epsilon)$$

Case 2. $L^i_0 \neq L^j_0, R^i_0 \neq R^j_0$. Observe that

$$P(L^i_3 = L^j_3) = P(h_2(R^i_0 \oplus T^i) \oplus R^j_0 \oplus h(L^i_0) = h_2(R^j_0 \oplus T^j) \oplus R^i_0 \oplus h(L^i_0) \leq \epsilon$$

Then we obtain by definition 5 and lemma 1, we obtain that

$$P(L^i_3 = L^j_3) \leq \max(2^\epsilon, \epsilon)$$

$$P(R^i_3 = R^j_3) = P(h_3(R^i_0 \oplus h(L^i_0)) \oplus R^j_0 \oplus h_2(R^j_0 \oplus T^j)) \leq \max(2^\epsilon, \epsilon)$$

Then by definition 5, lemma 1.2, we obtain that

$$P(R^i_3 = R^j_3) \leq \max(2^\epsilon, \epsilon, 2^\epsilon)$$

Case 3. $L^i_0 \neq L^j_0, R^i_0 = R^j_0$. Then we obtain by definition

5, lemma 1 that

$$P(L^i_3 = L^j_3) = P(h_2(R^i_0 \oplus T^i) \oplus h(L^i_0) = h_2(R^j_0 \oplus T^j) \oplus h(L^j_0) \leq \epsilon$$

$$P(R^i_3 = R^j_3) = P(h_3(R^i_0 \oplus h(L^i_0)) \oplus h(L^j_0) \oplus h_2(R^j_0 \oplus T^j) \leq \max(2^\epsilon, \epsilon)$$

Case 4. $L^i_0 = L^j_0, R^i_0 = R^j_0$. Then $P(L^i_3 = L^j_3) = P(R^i_3 = R^j_3) = 0$

Hence, for any case,

$$P(L^i_3 = L^j_3) \leq \max(2^\epsilon, \epsilon)$$

$$P(R^i_3 = R^j_3) \leq \max(2^\epsilon, \epsilon, 2^\epsilon)$$

Therefore we obtain that
\[ \sum_{1 \leq i \leq j \leq q} P(L^I_3 = L^I_3) \leq C_q^2 \epsilon' = \frac{q(q-1)}{2} \epsilon' \]
\[ \sum_{1 \leq i \leq j \leq q} P(R^I_3 = R^I_3) \leq C_q^2 \epsilon'' = \frac{q(q-1)}{2} \epsilon'' \]
\[ ADV \leq \sum_{1 \leq i \leq j \leq q} P(L^I_3 = L^I_3) \oplus \sum_{1 \leq i \leq j \leq q} P(R^I_3 = R^I_3) \leq q(q-1) \max(\epsilon', \epsilon'') \]

which is negligible.

Using the same methods, we can prove that the following optimal schemes are CPA-secure.

Theorem 2. Let H be \( e \sim XOR \) universal permutation ensemble, \( h_i, h_j, h_k \in H \), \( f_i, f_j \) be chosen from TPE \( \text{Permn} \), they are independent each other. If (1) the tweak T is XORed with \( R_1 \) or (3) the tweak T is XORed with \( R_2 \) and \( L_2 = R_1 \oplus T, R_2 = R_2 \oplus T \oplus h_i(L_2) \), then the above 5 round optimal MISTY-Type tweakable transformation \( \Gamma \) is indistinguishable (in a CPA attack) from a random 2n-bit permutation \( \Pi_{2n} \) indexed by T.

4. CONCLUSION

In this paper, on the basis of MISTY-type transformations, we propose some optimal CPA-secure tweakable blockciphers directly and solve an open problem, that is, how to construct tweakable blockciphers without using a pre-existing blockcipher proposed by Liskov et al. We use less random permutation in the optimal structure. We prove that the 5 round optimal tweakable MISTY-type blockciphers are CPA-secure.

5. ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of shandong province (No.Y2008A29), the Science and Technique Foundation of shandong province (No.2008GG 30009008), graduate education innovation program of Shandong Educational Committee (No.SDYY08 0029).

6. REFERENCES