2010 2nd International Conference on Information and Multimedia Technology (ICIMT 2010)
IPCSIT vol. 42 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V42.2

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 transform -ation. We optimize the 5-round structure by using the XOR-universal permuta- tion to replace the first three random permuta- tion. Finally, we give the concrete cryptanalysis for the CPA-secure 5 round Optimal MISTY-Type tweakable blockciphers.

Keywords-Cryptography; block cipher; tweak-able blockcipher; MISTY-Type structure; XOR-universal per- mutation

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 tweak-able blockcipher is one that is indistinguishable from a random permutation family under chosen plaintext attack; a CCA-secure tweakable blockcipher is one that is indisting- uishable 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. $Perm_n$ 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* (.), *E* (.,.), *D*(., .), are all efficiently computable, and where the correctness property holds: that is, for all M,T and $K \in G(1^n)$,*D*K(*EK*(*M*; *T*); *T*) = *M*. Over all adversaries with access to an encryption oracle, the maximum advantage is defined as:

$$ADV_K(E,q,t) = \max_K : \left| p(A^{E_K}(1^n) = 1 \right| - \left| p(A^{\Pi}(1^n) = 1 \right|$$

where (1) Π is a random permutation family indexed by T ; (2)*A* is allowed to make at most *q* oracle queries. A tweak-able blockcipher is CPA-secure if for all *n*, for *q* queries and time *t*, *ADV*K(*E* ,*q*, *t*) is negligible in *n*.

Definition 3.(MISTY-Type Structure). For some input(*L*,*R*),

$$L_{i+1} = R_i; R_{i+1} = f_{i+1}(L_i) \oplus R_i, 1 \le i \le n$$

where the input is $M = (L_0, R_0) = (L, R)$), the output after *n* round is (Ln,*Rn*), each $f_i \in Perm_n$ is a random permutation.

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*, *T*)

$$L_{i+1} = R_i; R_{i+1} = f_{i+1}(L_i \oplus T) \oplus R_i$$

or

$$L_{i+1} = R_i; R_{i+1} = f_{i+1}(L_i) \oplus R_i \oplus T$$

for some i($1 \le i \le n$). where the tweak is a half-block in length; that is, on input $M=(L_0,R_0)=(L,R)$ of size 2n, the tweak is of size *n*.

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

$$P[h \xleftarrow{R} H : h(x) \oplus h(y) = z] \le \varepsilon$$

Lemma 1. Let H be $\varepsilon - XOR$ universal permutation ensemble. h_1, h_2 are independently chosen from H. Then for any $a,b,c,d,y \in I_n$, such that $a \ne b, c \ne d$

$$P[h_1(a) \oplus h_1(b) \oplus h_2(c) \oplus h_2(d) = y] \le 2^n \varepsilon^2$$

Proof. Let *A* be the event of $h_1(a) \oplus h_1(b) \oplus h_2(c) \oplus h_2(d) = y$ and *Aj* be the event of $h_1(a) \oplus h_1(b) = w_j$ for $1 \le j \le 2^n$,where $I_n = \{w_1, \cdots, w_{2^n}\}$. Then by definition 5, we obtain that

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

Therefore, $P(A) = \sum_{j=1}^{2^n} P(A \cap A_j) \le 2^n \varepsilon^2$

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

$$P[h_1(a) \oplus h_1(b) \oplus h_2(c) \oplus h_2(d) \oplus h_3(p) \oplus h_3(q) = y] \le 2^{2n} \varepsilon^3$$

3. OPTIMAL MISTY-TYPE TWEAKABLEBLOCKCIPHERS WITHCPA 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*),

$$R_1 = h_1(L_0) \oplus R_0, L_1 = R_0; R_2 = h_2(L_1 \oplus T) \oplus R_1, L_2 = R_1$$
$$R_3 = h_3(L_2) \oplus R_2, L_3 = R_2; R_4 = f_4(L_3) \oplus R_3, L_4 = R_3$$
$$R_5 = f_5(L_4) \oplus R_4, L_5 = R_4$$

where the input is $M = (L_0, R_0) = (L, R), f_4, f_5 \in Perm_n$, are random permutation. h_1, h_2, h_3 are XOR universal permutation

Theorem 1.Let H be $\varepsilon - XOR$ universal permuta-tion ensemble, $h_1, h_2, h_3 \in H$, f_4, f_5 be chosen from TPE *Perm*$_n$, they are independent each other. Then the obove 5 round optimal MISTY-Type tweakable transformation Γ is indistinguishable(in a CPA attack) from a random 2n-bit permutation Π_{2n} indexed by *T*.

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

Γ or Π_{2n}. 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 $(L^i_j,R^i_j), i=1,\ldots,q;\ j=1,2,3,4,5$ be the j-th round output in the i-th oracle query. Let A_L denote the event that $L^1_3,L^2_3,\ldots,L^q_3$ are all distinct. A_R denote the event that $R^1_3,R^2_3,\ldots,R^q_3$ are all distinct. If A_L occurs, then we can see that $L^1_5,L^2_5,\ldots,L^q_5$ are completely random, since $L^i_5=R^i_4=R^i_3\oplus f_4(L^i_3), i=1,\ldots,q$ and f_4 is a random permutation. Similarly, if A_R occurs, then $R^1_5,R^2_5,\ldots,R^q_5$ are completely random. So (L^1_5,R^1_5), $(L^2_5,R^2_5)\ldots,(L^q_5,R^q_5)$ are completely random since f_4 and f_5 are independently random permutation. Therefore, if A_L and A_R occur, then $ADVA$ is bounded above as follows:

$$ADV_A=\left|P[A\to 1|O\leftarrow\Gamma]-P[A\to 1|O\leftarrow\Pi_{2n}]\right|$$

$$=\Big|P[(A\to 1|O\leftarrow\Gamma)|A_L\cap A_R]P(A_L\cap A_R)+P[(A\to 1|O\leftarrow\Gamma)|\overline{A_L\cap A_R}]P(\overline{A_L\cap A_R})$$

$$-P[(A\to 1|O\leftarrow\Pi_{2n})|A_L\cap A_R]P(A_L\cap A_R)\quad -P[(A\to 1|O\leftarrow\Pi_{2n})|\overline{A_L\cap A_R}]P(\overline{A_L\cap A_R})\Big|$$

$$=\Big|P[(A\to 1|O\leftarrow\Gamma)|\overline{A_L\cap A_R}]P(\overline{A_L\cap A_R})\quad -P[(A\to 1|O\leftarrow\Pi_{2n})|\overline{A_L\cap A_R}]P(\overline{A_L\cap A_R})\Big|$$

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

Now we estimate $P(L^i_3=L^j_3), P(R^i_3=R^j_3), 1\le i\le j\le q$. Let

$(L_0,R_0,T)=(L,R,T)$. .We have the following four cases.

Case1. $L^i_0=L^j_0, R^i_0\ne R^j_0$. In this case it is easy to see that $P(L^i_3=L^j_3)=P(h_2(R^i_0\oplus T^i)\oplus R^i_0=h_2(R^j_0\oplus T^j)\oplus R^j_0)\le\varepsilon$ (by Definition5), since $h2$ is a $\varepsilon-XOR$ universal permutation. We can obtain by lemma 1and definition5 that

$$P(R^i_3=R^j_3)=P(h_3(R^i_0\oplus h_1(L^i_0))\oplus R^i_0\oplus h_2(R^i_0\oplus T^i)$$
$$=h_3(R^j_0\oplus h_1(L^j_0))\oplus R^j_0\oplus h_2(R^j_0\oplus T^j))\le\max(2^n\varepsilon^2,\varepsilon)$$

Case2 $L^i_0\ne L^j_0, R^i_0\ne R^j_0$. Observe that

$$P(L^i_3=L^j_3)$$
$$=P(h_2(R^i_0\oplus T^i)\oplus R^i_0\oplus h_1(L^i_0)=h_2(R^j_0\oplus T^j)\oplus R^j_0\oplus h_1(L^j_0))\le\varepsilon$$

then we obtain by defition 5 and lemma 1, we obtain that

$$P(L^i_3=L^j_3)\le\max(2^n\varepsilon^2,\varepsilon)$$

$$P(R^i_3=R^j_3)=P(h_3(R^i_0\oplus h_1(L^i_0))\oplus h_1(L^i_0)\oplus R^i_0\oplus h_2(R^i_0\oplus T^i)$$
$$=h_3(R^j_0\oplus h_1(L^j_0))\oplus h_1(L^j_0)\oplus R^j_0\oplus h_2(R^j_0\oplus T^j))$$

Then by defition 5,lemma 1,2 ,we obtain that

$$P(R^i_3=R^j_3)\le\max(2^n\varepsilon^2,\varepsilon,2^{2n}\varepsilon^3)$$

Case3. $L^i_0\ne L^j_0, R^i_0=R^j_0$. Then we obtain by definition 5,lemma 1 that

$$P(L^i_3=L^j_3)=P(h_2(R^i_0\oplus T^i)\oplus h_1(L^i_0)=h_2(R^j_0\oplus T^j)\oplus h_1(L^j_0))$$
$$\le\max(\varepsilon,2^n\varepsilon^2)$$
$$P(R^i_3=R^j_3)=P(h_3(R^i_0\oplus h_1(L^i_0))\oplus h_1(L^i_0)\oplus h_2(R^i_0\oplus T^i)$$
$$=h_3(R^j_0\oplus h_1(L^j_0))\oplus h_1(L^j_0)\oplus h_2(R^j_0\oplus T^j))\le\max(2^n\varepsilon^2,\varepsilon,2^{2n}\varepsilon^3)$$

Case4. $L^i_0=L^j_0, R^i_0=R^j_0$. Then $P(L^i_3=L^j_3)=P(R^i_3=R^j_3)=0$

Hence, for any case,

$$P(L^i_3=L^j_3)\le\max(2^n\varepsilon^2,\varepsilon)=\varepsilon'$$

$$P(R^i_3=R^j_3)\le\max(2^n\varepsilon^2,\varepsilon,2^{2n}\varepsilon^3)=\varepsilon''$$

Therefore we obtain that

$$\sum_{1\le i\le j\le q} P(L_3^i = L_3^j) \le C_q^2 \varepsilon' = \frac{q(q-1)}{2}\varepsilon'$$

$$\sum_{1\le i\le j\le q} P(R_3^i = R_3^j) \le C_q^2 \varepsilon'' = \frac{q(q-1)}{2}\varepsilon''$$

$$ADV_A \le \sum_{1\le i\le j\le q} P(L_3^i = L_3^j) \oplus \sum_{1\le i\le j\le q} P(R_3^i = R_3^j)$$

$$\le q(q-1)\max(\varepsilon', \varepsilon'')$$

which is negligible.

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

Theorem 2.Let H be $\varepsilon - XOR$ universal permutation ensem-ble, $h_1, h_2, h_3 \in H$, f_4, f_5 be chosen from TPE $Perm_n$, they are independent each other. If (1)the tweak T is XORed with $R1$ or (3)the tweak T is XORed with $R2$ and $L_3 = R_2 \oplus T, R_3 = R_2 \oplus T \oplus h_3(L_2)$,Then the obove 5 round optimal MISTY-Type tweakable transformation Γ is indistingui- shable(in a CPA attack) from a random 2n-bit permutation Π_{2n} indexed by T.

4. CONCLUSION

In this paper, on the basis of MISTY-type transfor-mations, we propose some optimal CPA-secure tweakable blockciph-ers 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 blockci-phers 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.SDYY0 8029).

6. REFERENCES

[1] Moses Liskov, Ronald L.Rivest, and David Wagner. Tweak-bale block ciphers. In Advances in Cryptology-CRYPTO’ 02, California, USA, 2002, pp.31-46.

[2] Halevi, S., Rogway,P.A Tweakable Enciphering Mode. In Advances in Cryptology-CRYPTO’03, California, USA, 2003, pp.482-499.

[3] M.Matsui. New struture of block ciphers with provable security against differential and linear cryptanalysis. In Fast Software Encryption, Cambridge, UK, 1996, pp.206-218.

[4] M.Matsui.New block encryption algorithm MISTY. In FSE97, Haifa, Israel, 1997, pp. 54-68.

[5] Ju-Sung Kang, Okyeon Yi, Dowon Hong at el. Pseudorandom- ness of MISTY-Type Transformations and the Block Cipher KASUMI. In Proceedings of the 6th Australasian Conference on Information Security and Privacy,Sydney, Australia, 2001, pp.60-73.

[6] Fengtong Wen.Design and analysis of the tweakable block- ciphers based on the MISTY structure.Journal on communica- tions, 31(7),2010,pp.76-80.

[7] Carter L, Wegman M. Universal hash functions. Journal of computer and system sciences, 1979,18: 143-152.