优化 MISTY 型结构的伪随机性

温凤桐[①③]　吴文玲[②]　温巧燕[①]
[①](北京邮电大学理学院　北京　100876)
[②](中国科学院软件研究所信息安全国家重点实验室　北京　100080)
[③](济南大学理学院　济南　250022)

摘　要：该文对 4 轮 MISTY 和 3 轮双重 MISTY 两种结构进行了优化。在保持其安全性不变的情况下，把 4 轮 MISTY 结构中第 1 轮的伪随机置换，用一个 XOR-泛置换代替，第 2，第 3 轮采用相同的伪随机置换，3 轮结构中第 1 轮的伪随机置换用 XOR-泛置换代替，其它轮相同。伪随机置换的数量分别由原来的 4 个变为 2 个，3 个变为 1 个，从而缩短了运行时间，节省了密钥量，大大降低了结构的实现成本。

关键词：分组密码；伪随机置换类；MISTY 结构；双重 MISTY 结构
中图分类号：TN918.2　　**文献标识码**：A　　**文章编号**：1009-5896(2007)05-1173-04

Pseudorandomness of Optimal MISTY-Type Structure

Wen Feng-tong[①③]　Wu Wen-ling[②]　Wen Qiao-yan[①]
[①](*Shool of Science*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
[②](*State Key Lab. of Info. Security*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100080, *China*)
[③](*School of Science*, *Jinan University*, *Jinan* 250022, *China*)

Abstract: The four round MISTY-type and the three round dual MISTY-type transformation are optimized by replacing the first round pseudorandom permutation with XOR-universal permutation and employing identical pseudorandom permutation in the second and the third round. Thus the running time is shortened and the number of keys are saved by reducing the number of pseudorandom permutation. Hence the running cost is debased greatly. At the same time, the security remains.

Key words: Block cipher; Pseudorandom permutation ensemble; MISTY structure; Dual-MISTY structure

1　引言

分组密码的安全性主要依赖于其结构和轮函数。常用的分组密码结构有：Feistel 结构；MISTY 结构；IDEA 结构等等。伪随机性是衡量分组密码安全性的重要标准，这种方法通过假设分组密码的轮函数是伪随机的来研究其伪随机性。Luby 和 Rackoff 在文献[1]中使用伪随机置换和超伪随机置换介绍了这种方法的理论模型：如果攻击者经过多项式次加密询问而无法区分一个分组密码和一个真正随机的置换类，就称此分组密码是伪随机的；如果攻击者经过多项式次加密、解密询问而无法区分一个分组密码和一个真正随机的置换类，就称此分组密码是超伪随机的。

在文献[1]中，Luby和Rackoff证明了 3 轮Feistel结构是伪随机的，4 轮Feistel结构是超伪随机的。Naor和Reingold在文献[2]中对上述结构进行了优化，指出 3 轮结构中的第 1 轮，4 轮结构中的第 1，第 4 轮轮函数可使用不同的XOR-泛杂凑函数代替，其伪随机性和超伪随机性不变。对于MISTY结构Sakurai和zheng[3]证明了 3 轮结构不是伪随机的；Ju-sung kang等[4]证明了在非适应模型下 4 轮MISTY结构，3 轮双重MISTY结构是伪随机的。因为伪随机置换的运行时间长，实现成本非常高，为缩短运行时间，节省密钥量，降低结构的实现成本，本文对 4 轮MISTY结构，3 轮双重MISTY结构进行了优化，利用一个XOR-泛置换代替结构中的第 1 轮的伪随机置换，第 2、第 3 轮函数取相同的伪随机置换，这样 4 轮MISTY结构的 4 个不同的伪随机置换减为 2 个，3 轮双重MISTY结构的 3 个不同的伪随机置换减为 1 个。在非适应性模型下证明了这两个结构是伪随机的。

2005-09-30 收到，2006-03-13 改回
国家自然科学基金(90604036，60373059)，国家 973 项目(2004CB318004)，教育部博士点基金(20040013007)，济南大学博士基金项目(B0631)和济南大学科技基金项目(Y0609)资助课题

2　基本知识

设 I_n 表示集合 $\{0,1\}^n$，Perm_n 表示 I_n 上所有置换的集合。

定义 1[4]　如果对 $\forall \pi \in \mathrm{Perm}_n$ 有 $P(\pi)=1/2^n!$，则称 Perm_n 为真正随机的置换类(TPE)。

定义 2[2]　如果对 $\forall c>0$，对充分大的 $m \in N$ 有 $h(m)<1/m^c$，则称函数 $h: N \to R$ 是可忽略的。

定义 3[5]　如果对所有的 $x \neq y \in I_n, z \in I_n$ 有

$P[h \xleftarrow{R} H : h(x) \oplus h(y) = z] \le \varepsilon$，则称$H$是$\varepsilon$-XOR泛置换。例如有限域$\mathrm{GF}(2^n)$上的$f_{a,b}(x) = a \cdot x + b \ \ (a \ne 0)$就是一个$\dfrac{1}{2^n - 1}$-XOR泛置换。

下面考虑一个安全模型：设 D 是一个带有一个预言(oracle) O的分类器，ψ_n 是一个分组密码，预言 O可以从 ψ_n 或Perm_n中随机选择一个置换π。D 的目的就是来区分 O 是从 ψ_n 中选择的π，还是从Perm_n中选择的π。实际攻击中 O的作用相当于一个置换，D可以询问 O，通过 O的输出结果作出判断，如果判定$\pi \in \mathrm{Perm}_n$，则 D输出 0；如果判定$\pi \in \psi_n$，则 D输出 1。

定义下面的优势函数：

定义 4[4] 设D是一个上述描述的分类器，Perm_n是TPE，ψ_n是一个置换类。分类器D的优势Adv_D定义为

$$\mathrm{Adv}_D = \left|\Pr(D \text{ output } 1 \middle| O \leftarrow \mathrm{Perm}_n) - \Pr(D \text{ output } 1 \middle| O \leftarrow \psi_n)\right|$$

假定询问 O的次数最多为$\mathrm{poly}(n)$。如果询问的是x，预言回答的是$y = \pi(x)$，π是由 O随机选取的，则称 D是伪随机分类器。

定义 5[4] 设ψ_n是一个有效的可计算的置换类，如果对任意的伪随机分类器D有Adv_D是可忽略的，则称ψ_n是伪随机置换类PPE。

定义 6[6] 对$\forall f \in \mathrm{Perm}_n$，$2n$比特的MISTY型置换$M_f \in \mathrm{Perm}_{2n}$定义为

$$M_f(L,R) = (R, f(L) \oplus R) \quad L,R \in I_n$$

定义 7[6] 对$\forall g \in \mathrm{Perm}_n$，$2n$比特的双重MISTY型置换$\mathrm{DM}_g \in \mathrm{Perm}_{2n}$定义为

$$\mathrm{DM}_g(L,R) = (g(L \oplus R), L) \quad L,R \in I_n$$

引理 1 设π是I_n上的随机置换，则对$\forall x_1 \ne x_2, y \in I_n$有

$$P(\pi(x_1) \oplus \pi(x_2) = y) = \begin{cases} \dfrac{1}{2^n - 1}, & y \ne 0 \\ 0, & y = 0 \end{cases}$$

证明 设Γ表示事件“$\pi(x_1) \oplus \pi(x_2) = y$”，$A_i$表示事件$\pi(x_1) = w_i \quad 1 \le i \le 2^n$。$I_n = \{w_1, w_2, \cdots, w_{2^n}\}$。如果$y = 0$，因为$x_1 \ne x_2$，所以 $P(\pi(x_1) \oplus \pi(x_2) = 0) = 0$。如果$y \ne 0$，

$$P(\Gamma \cap A_i) = P(\pi(x_1) \oplus \pi(x_2) = y, \pi(x_1) = w_i) = P(\pi(x_2) = y \oplus w_i, \pi(x_1) = w_i) = \frac{(2^n - 2)!}{2^n!} = \frac{1}{2^n(2^n - 1)}$$

所以如果$y \ne 0$，则

$$P(\Gamma) = \sum_{i=1}^{2^n} P(\Gamma \cap A_i) = 2^n \cdot \frac{1}{2^n(2^n - 1)} = \frac{1}{2^n - 1}$$

4 轮的 MISTY 结构用$M_{f_4} \cdot M_{f_3} \cdot M_{f_2} \cdot M_{f_1}$表示，3 轮双重MISTY 结构用$\mathrm{DM}_{g_3} \cdot \mathrm{DM}_{g_2} \cdot \mathrm{DM}_{g_1}$表示。

3 主要结果

定理 1 设F是I_n上的伪随机置换类，$f_1, f_2 \in F$，h是I_n上的ε-XOR 泛置换，f_1, f_2, h是相互独立的，ψ_{2n}是由$M_{f_2} \cdot M_{f_1} \cdot M_{f_1} \cdot M_h$所确定的置换类。则$\psi_{2n}$是 $2n$ 比特的伪随机置换类。

证明 设Perm_n，Perm_{2n}是 TPE，D是区分Perm_{2n}与ψ_{2n}的分类器。不失一般性，不妨设 $f_1, f_2 \in \mathrm{Perm}_n$。设$(L,R)$为$2n$比特输入，则$\psi_{2n}(L,R)$的第$i$轮输出$(L_i, R_i)$为

$$(L_1, R_1) = M_h(L,R), \ (L_2, R_2) = M_{f_1} \cdot M_h(L,R),$$
$$(L_3, R_3) = M_{f_1} M_{f_1} M_h(L,R), \ (L_4, R_4) = M_{f_2} M_{f_1} M_{f_1} M_h(L,R)$$

设 D对预言 O作q次询问$(L^1, R^1), \cdots, (L^q, R^q)$，每次询问各不相同，$(L^i, R^i)$为第$i$次询问，$(L^i_j, R^i_j), i = 1, \cdots, q$为第$i$次询问的第$j$轮输出。设$A_L$表示事件“$L^1_2, L^2_2, \cdots, L^q_2$互不相同”，$A_R$表示事件“$R^1_2, R^2_2, \cdots, R^q_2$互不相同”。因为$L^i_4 = R^i_3 = R^i_2 \oplus f_1(L^i_2)$，$i = 1, \cdots, q$，$f_1$是随机置换，所以如果$A_L$发生，则$L^1_4, L^2_4, \cdots, L^q_4$是完全随机的。同理如果$A_R$发生，因为$R^i_4 = R^i_2 \oplus f_2(R^i_2) \ \ i = 1, \cdots, q$，$f_2$是随机置换，所以$R^1_4, R^2_4, \cdots, R^q_4$是完全随机的。又因为$f_1, f_2$相互独立，所以输出$(L^1_4, R^1_4), \cdots, (L^q_4, R^q_4)$是完全随机的。从而

$$\begin{aligned}
\mathrm{Adv}_D &= \left|\Pr(D \text{ output } 1 \middle| O \leftarrow \mathrm{Perm}_{2n}) - \Pr(D \text{ output } 1 \middle| O \leftarrow \psi_{2n})\right| \\
&= \Big|\Pr((D \text{ output } 1 \big| O \leftarrow \mathrm{Perm}_{2n}) \big| A_L \cap A_R) P(A_L \cap A_R) \\
&\quad + \Pr((D \text{ output } 1 \big| O \leftarrow \mathrm{Perm}_{2n}) \big| \overline{A_L \cap A_R}) P(\overline{A_L \cap A_R}) \\
&\quad - \Pr((D \text{ output } 1 \big| O \leftarrow \psi_{2n}) \big| A_L \cap A_R) P(A_L \cap A_R) \\
&\quad - \Pr((D \text{ output } 1 \big| O \leftarrow \psi_{2n}) \big| \overline{A_L \cap A_R}) P(\overline{A_L \cap A_R})\Big|
\end{aligned}$$

因为当A_L，A_R同时发生时，ψ_{2n}输出是完全随机的，所以有

$$\begin{aligned}
&\Pr((D \text{ output } 1 \big| O \leftarrow \mathrm{Perm}_{2n}) \big| A_L \cap A_R) P(A_L \cap A_R) \\
&\quad = \Pr((D \text{ output } 1 \big| O \leftarrow \psi_{2n}) \big| A_L \cap A_R) P(A_L \cap A_R)
\end{aligned}$$

所以

$$\begin{aligned}
\mathrm{Adv}_D &= \Big|\Pr((D \text{ output } 1 \big| O \leftarrow \mathrm{Perm}_{2n}) \big| \overline{A_L \cap A_R}) \cdot P(\overline{A_L \cap A_R}) \\
&\quad - \Pr((D \text{ output } 1 \big| O \leftarrow \psi_{2n}) \big| \overline{A_L \cap A_R}) \, P(\overline{A_L \cap A_R})\Big| \\
&= \Big|\Pr((D \text{ output } 1 \big| O \leftarrow \mathrm{Perm}_{2n}) \big| \overline{A_L \cap A_R}) \\
&\quad - \Pr((D \text{ output } 1 \big| O \leftarrow \psi_{2n}) \big| \overline{A_L \cap A_R}) \Big| P(\overline{A_L \cap A_R}) \\
&\le P(\overline{A_L \cap A_R}) \le \sum_{1 \le i < j \le q} P(L^i_2 = L^j_2) \\
&\quad + \sum_{1 \le i < j \le q} P(R^i_2 = R^j_2)
\end{aligned}$$

下面计算概率$P(L^i_2 = L^j_2)$和$P(R^i_2 = R^j_2)$，分 3 种情况讨论，令$(L_0, R_0) = (L, R)$。

(1) $L^i_0 \ne L^j_0, R^i_0 = R^j_0$，则

$$P(L_2^i = L_2^j) = P(R_1^i = R_1^j) = P(R_0^i \oplus h(L_0^i) = R_0^j \oplus h(L_0^j))$$
$$= P(h(L_0^i) = h(L_0^j)) = 0$$
$$P(R_2^i = R_2^j) = P[f_1(R_0^i) \oplus h(L_0^i) \oplus R_0^i$$
$$= f_1(R_0^j) \oplus h(L_0^j) \oplus R_0^j] = 0$$

(2) $L_0^i = L_0^j, R_0^i \neq R_0^j$，则

$$P(L_2^i = L_2^j) = P(R_1^i = R_1^j) = P(R_0^i \oplus h(L_0^i) = R_0^j \oplus h(L_0^j))$$
$$= P(R_0^i = R_0^j) = 0$$
$$P(R_2^i = R_2^j) = P[f_1(R_0^i) \oplus h(L_0^i) \oplus R_0^i = f_1(R_0^j) \oplus h(L_0^j) \oplus R_0^j]$$
$$= P[f_1(R_0^i) \oplus R_0^i = f_1(R_0^j) \oplus R_0^j]$$
$$\leq 1/(2^n - 1)\text{(由引理1得)}$$

(3) $L_0^i \neq L_0^j, R_0^i \neq R_0^j$，则

$$P(L_2^i = L_2^j) = P(R_1^i = R_1^j) = P(R_0^i \oplus h(L_0^i) = R_0^j \oplus h(L_0^j))$$
$$= P(h(L_0^i) \oplus h(L_0^j) = R_0^i \oplus R_0^j)$$

由 h 是 ε - XOR 泛置换知 $P(L_2^i = L_2^j) \leq \varepsilon$。

$$P(R_2^i = R_2^j) = P[f_1(R_0^i) \oplus h(L_0^i) \oplus R_0^i = f_1(R_0^j) \oplus h(L_0^j) \oplus R_0^j]$$
$$= P[h(L_0^i) \oplus h(L_0^j) = f_1(R_0^i) \oplus f_1(R_0^j) \oplus R_0^i \oplus R_0^j]$$
$$\leq \varepsilon$$

这样就有

$$\sum_{1\leq i<j\leq q} P(L_2^i = L_2^j) \leq C_q^2 \varepsilon = \frac{q(q-1)\varepsilon}{2}$$
$$\sum_{1\leq i<j\leq q} P(R_2^i = R_2^j) \leq C_q^2 \cdot \max\left\{\varepsilon, \frac{1}{2^n - 1}\right\} = \frac{q(q-1)\varepsilon'}{2}$$

其中 $\varepsilon' = \max\left\{\varepsilon, \frac{1}{2^n - 1}\right\}$。从而

$$\mathrm{Adv}_D \leq \sum_{1\leq i<j\leq q} P(L_2^i = L_2^j) + \sum_{1\leq i<j\leq q} P(R_2^i = R_2^j) \leq q(q-1)\varepsilon'$$

定理 2　设 F 是 I_n 上的伪随机置换类，$g \in F$，h 是 I_n 上的 ε - XOR 泛置换，g,h 是相互独立的，ψ_{2n} 是由 $\mathrm{DM}_g \cdot \mathrm{DM}_g \cdot \mathrm{DM}_h$ 所确定的置换类。则 ψ_{2n} 是 $2n$ 比特的伪随机置换类。

证明　设 $\mathrm{Perm}_n, \mathrm{Perm}_{2n}$ 是 TPE，D 是区分 Perm_{2n} 与 ψ_{2n} 的分类器。不失一般性，不妨设 $g \in \mathrm{Perm}_n$。

设分类器 D 作 q 次询问 $(L^1,R^1),\cdots,(L^q,R^q)$，每次询问各不相同，$(L^i,R^i)$ 为第 i 次询问，$(L_j^i,R_j^i), i = 1,\cdots,q$ 为第 i 次询问的第 j 轮输出。

设 A 表示事件“$L_1^1 \oplus R_1^1,\cdots,L_1^q \oplus R_1^q$ 互不相同”。如果 A 发生，则 $L_3^1,\cdots,L_3^q$ 是完全随机的，因为 $L_3^i = g(L_1^i \oplus g(L_1^i \oplus R_1^i))$，而 g 的输出是随机的；$R_3^1,\cdots,R_3^q$ 也是完全随机的，因为 $R_3^i = g(L_1^i \oplus R_1^i))$，$g$ 的输出是随机的。而 $L_1^i = h(L^i \oplus R^i)$，$h,g$ 相互独立，从而 L_3^i, R_3^i 是随机的且相互独立，这样输出 $(L_3^1,R_3^1),\cdots,(L_3^q,R_3^q)$ 是随机的。从而类似于定理 1 的分析有

$$\mathrm{Adv}_D = \left|\Pr(D \text{ output } 1 | O \leftarrow \mathrm{Perm}_{2n}) - \Pr(D \text{ output } 1 | O \leftarrow \psi_{2n})\right| \leq P(\overline{A})$$
$$= \sum_{1\leq i<j\leq q} P(L_1^i \oplus R_1^i = L_1^j \oplus R_1^j)$$

下面分情况讨论：

(1) $L^i \neq L^j, R^i = R^j$，则 $L_1^i = h(L^i \oplus R^i), L_1^j = h(L^j \oplus R^j)$，从而有

$$P(L_1^i \oplus R_1^i = L_1^j \oplus R_1^j)$$
$$= P(h(L^i \oplus R^i) \oplus L^i = h(L^j \oplus R^j) \oplus L^j)$$
$$= P(h(L^i \oplus R^i) \oplus h(L^j \oplus R^j) = L^i \oplus L^j) \leq \varepsilon$$

(2) $L^i = L^j, R^i \neq R^j$，则

$$P(L_1^i \oplus R_1^i = L_1^j \oplus R_1^j) = P(h(L^i \oplus R^i) = h(L^j \oplus R^j)) = 0$$

(3) $L^i \neq L^j, R^i \neq R^j$，则

$$P(L_1^i \oplus R_1^i = L_1^j \oplus R_1^j) = P(h(L^i \oplus R^i) \oplus L^i$$
$$= h(L^j \oplus R^j) \oplus L^j)$$
$$= P(h(L^i \oplus R^i) \oplus h(L^j \oplus R^j) = L^i \oplus L^j)$$

(a) 如果 $L^i \oplus R^i = L^j \oplus R^j$ $h(L^i \oplus R^i) \oplus h(L^j \oplus R^j) = 0$，而 $L^i \oplus L^j \neq 0$，所以

$$P(h(L^i \oplus R^i) \oplus h(L^j \oplus R^j) = L^i \oplus L^j) = 0$$

(b) 如果 $L^i \oplus R^i \neq L^j \oplus R^j$，则由 h 的定义知 $P(h(L^i \oplus R^i) \oplus h(L^j \oplus R^j) = L^i \oplus L^j) \leq \varepsilon$。综上所述有

$P(\overline{A}) \leq C_q^2 \cdot \varepsilon = \frac{q(q-1)\varepsilon}{2}$，从而有

$$\mathrm{Adv}_D \leq \frac{q(q-1)\varepsilon}{2}$$

4　结束语

本文从节约运行成本，缩短运行时间的角度对 4 轮 MISTY 结构、3 轮双重 MISTY 结构进行优化，4 轮结构中，利用一个 XOR-泛置换代替结构中的第 1 轮的伪随机置换，第 2，第 3 轮取相同的伪随机置换，这样原来的 4 个不同的伪随机置换减为 2 个，3 轮结构中利用一个 XOR-泛置换代替结构中的第 1 轮的伪随机置换，第 2，第 3 轮取相同的置换。这样既缩短了运行时间，又节省了密钥材料，从而大大降低了结构的实现成本，使结构得到很好的优化。优化后的安全性没有降低，在非适应性模型下证明了其伪随机性。

参 考 文 献

[1] Luby M and Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 1988，17(2): 373–386.

[2] Naor M and Reingold O. On the construction of pseudorandom permutations: Luby-Rackoff revisited. *Journal of Cryptology*, 1999, 12(1): 29–66.

[3] Sakurai K and Zheng Y. On non-pseudorandomness from

block ciphers with provable immunity against linear cryptanalysis. *IEICE Trans. Fundamentals*, 1997, E80-A(1): 19–24.

[4] Kang J S, Yi O, and Hong D, *et al.*. Pseudorandomness of MISTY-TYPE transformations and the block cipher KASUMI. Information Security and Privacy, 6th Australasian Conference，Sydney 2001, LNCS 2119, Berlin Heidelberg Springer- Verlag 2001: 60–73.

[5] Carter L and Wegman M. Universal hash functions. *Journal of Computer and System Sciences*, 1979, 18: 143–152.

[6] Matsui M. New permutation of block ciphers with provable security against differential and linear cryptanalysis, Fast software encryption, 1996, LNCS 1039, Cambridge, UK: Springer-Verlag, 205–218.

温凤桐： 男，1970 年生，博士生，研究方向为密码学.

吴文玲： 女，1966 年生，研究员，博士生导师，研究方向为密码学、信息安全.

温巧燕： 女，1959 年生，教授，博士生导师，研究方向为密码学、应用数学.