基于 MISTY 结构的可调分组密码的设计与分析

温凤桐 [1,2]

（1. 山东大学 计算机科学与技术学院，山东 济南 250101；2. 济南大学 理学院，山东 济南 250022）

摘 要：对如何不借助于现有的分组密码来直接设计可调分组密码进行了研究。通过在 MISTY 结构的不同位置添加一个标号，分析了在 4 轮和 5 轮 MISTY 结构上设计可调分组密码的可行性。对 4 轮结构提出了攻击的方法；对 5 轮结构提供了安全性理论证明。结果表明，在选择明文攻击下，5 轮 MISTY 结构才能提供安全的可调分组密码。

关键词：密码学；分组密码；伪随机置换；可调分组密码；MISTY 结构

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2010)07-0076-05

Design and analysis of the tweakable blockciphers based on the MISTY structure

WEN Feng-tong[1,2]

(1. School of Computer Science and Technology, Shandong University, Jinan 250101,China;

2. School of Science, University of Jinan, Jinan 250022, China)

Abstract: A problem that how to construct tweakable blockciphers without using preexisting blockcipher was researched by using MISTY-Type transformation. The feasibility to design tweakable blockciphers by XORing a tweak value into one place in the dataflow of the 4 round and 5 round MISTY-Type transformations was analyzed. The concrete cryptanalysis for the secure 5 round tweakable MISTY-Type blockciphers and the attack methods for 4 round structure were given. The result shows that a CPA-secure tweakable blockcipher need 5 round MISTY-Type structure.

Key words: cryptography; block cipher; pseudorandom permutation; tweakable blockcipher; MISTY structure

1 引言

分组密码是定义在消息空间上的由密钥引导的置换族，一个密钥决定一个置换。它的安全性是通过伪随机置换来衡量的，如果攻击者在多项式时间内通过加密询问而无法区分分组密码和真正随机的置换，则称分组密码是伪随机的。

可调分组密码是一种带有额外输入的分组密码，这一额外输入通常称之为“tweak”，它的作用是提高分组密码的灵活性，它不需要保密，比较容易改变。如果攻击者在多项式时间内通过加密询问而无法区分可调分组密码和由 tweak 引导的真正随机的置换，则称可调分组密码是安全的。可调分组密码有着很好的应用背景，如可以应用在磁盘分区加密中，应用这种分组密码可以保证同一消息在不同的磁盘分区中加密得到的密文是不同的。

收稿日期：2009-09-24；**修回日期**：2010-04-28

基金项目：山东省自然科学基金资助项目（Y2008A29）；山东省科技攻关基金资助项目（2008GG30009008）

Foundation Items: The Natural Science Foundation of Shandong Province (Y2008A29); The Science and Technique Foundation of Shandong Province (2008GG30009008)

可调分组密码的概念最早是由 Liskov、Rivest 和 Wagner 在文献[1]中提出来的，文中作者给出了 2 个如何利用现有的分组密码设计可调分组密码的实例，沿着这一思路人们开展了一系列的工作，设计了一系列的可调分组密码，如 Halevi 和 Rogaway 的 EMD，EME 模式[2,3]；中科院软件所王鹏博士、吴文玲研究员等基于 CTR 模式利用 Hash-CTR-Hash 结构设计了 HCTR[4]模式；Lopez 和 Kazuhiko 分别在文献[5]和文献[6]从实现和提高安全性的角度对此方案进行了研究；李学远等人在文献[7]又把此方案推广到了环上，使其性能得到进一步改善。上述方案都是建立在原有分组密码工作模式基础上，以原有分组密码为基本模块建立的。Liskov 等人在文献[1]中还提出了一个公开问题，即如何不借助于现有的分组密码而直接设计可调分组密码。目前人们针对这一公开问题研究取得的成果比较少，主要有 David Goldemberg[8]等人基于 Feistel 结构设计了 Tweaking Luby-Rackoff Blockcipher。MISTY 结构最早是由 Matsui 在文献[9]中提出的，并因在 MISTY 分组密码中被应用而得名，这一结构比 Feistel 结构速度更快，抵抗差分攻击和线性攻击的能力更强，因此在这一结构上研究此公开问题更有意义。温凤桐等在文献[10]中基于 Dual MISTY-Type 结构分析了解决这一公开问题的可行性，研究表明 3 轮 Dual MISTY-TYPE 结构不能保证方案的安全性，要想构造安全的方案至少需要 4 轮。论文其余部分组织如下：第 2 节介绍相关基础知识，第 3 节为主要研究结果，第 4 节为结束语。

2　基础知识

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

定义 1　分组密码 $E:\{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$ 是一个函数族，对 $\forall K\in\{0,1\}^k, E_K(\cdot)=E(K,\cdot)$ 是 I_n 上的置换。可调分组密码 $\overline{E}:\{0,1\}^k\times\{0,1\}^t\times\{0,1\}^n\to\{0,1\}^n$ 是一个函数族，对 $\forall K\in\{0,1\}^k, T\in\{0,1\}^t, \overline{E}_K^T(\cdot)=\overline{E}(K,T,\cdot)$ 是 I_n 上的置换。分组密码的安全性通过攻击者区分分组密码和随机置换的优势来衡量；可调分组密码的安全性是通过攻击者区分可调分组密码和可调随机置换的优势来衡量。具体的定义如下：

$$ADV_E^{\text{prp}}(A)=\left|P[A^{E_K(\cdot)}=1]-P[A^{\Pi(\cdot)}=1]\right|,$$

$$ADV_{\overline{E}}^{\text{tprp}}(A)=\left|P[A^{\overline{E}_K^T(\cdot)}=1]-P[A^{\Pi_T(\cdot)}=1]\right|$$

其中，Π 为 I_n 上的随机置换类，Π_T 为 I_n 上的可调随机置换类（由 T 引导的随机置换类）。若 $ADV_E(\cdot,q,t)=\max\limits_A\{ADV_E^{\text{prp}}(A)\}$ 是可忽略的，则称 E 在选择明文攻击下是安全的；若 $ADV_{\overline{E}}(\cdot,q,t)=\max\limits_A\{ADV_{\overline{E}}^{\text{tprp}}(A)\}$ 是可忽略的，则称 $\overline{E}$ 在选择明文攻击下是安全的，其中攻击者 A 被允许做 t 次操作和 q 次询问。

定义 2　MISTY 结构。具体算法如下：对输入 $(L,R)=(L_0,R_0)$

$$\begin{aligned}&L_{i+1}=R_i\\&R_{i+1}=f_{i+1}(L_i)\oplus R_i\end{aligned},\quad 1\leqslant i\leqslant n$$

定义 3　基于 MISTY 结构的可调分组密码。它是通过在 MISTY 结构中添加 tweak T 来构成。根据添加的位置不同可以把设计方案概括为以下形式：对输入 $(L,R,T)=(L_0,R_0,T)$

$$\begin{aligned}&L_{i+1}=R_i\\&R_{i+1}=f_{i+1}(L_i\oplus T)\oplus R_i\end{aligned},\quad 1\leqslant i\leqslant n$$

或

$$\begin{aligned}&L_{i+1}=R_i(\oplus T)\\&R_{i+1}=f_{i+1}(L_i)\oplus R_i\oplus T\end{aligned},\quad 1\leqslant i\leqslant n$$

其中，T 的长度为总长度的一半。

引理 1[11]　设 f 是 I_n 上的随机置换，则对 $\forall x_1\neq x_2, y\in I_n$ 有

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

引理 2[11]　设 f_1,f_2 是 I_n 上的 2 个相互独立的随机置换，则对 $\forall a\neq b, c\neq d, y\in I_n$ 有

$$P(f_1(a)\oplus f_1(b)\oplus f_2(c)\oplus f_2(d)=y)<\frac{1}{2^{n-1}}, n\geqslant 2$$

引理 3　设 f_1,f_2,f_3 是 I_n 上的 3 个相互独立的随机置换，则对 $\forall a\neq b, c\neq d, p\neq q, y\in I_n$ 有

$$\begin{aligned}&P(f_1(a)\oplus f_1(b)\oplus f_2(c)\oplus\\&f_2(d)\oplus f_3(p)\oplus f_3(q)=y)<\frac{2}{2^n-1}\end{aligned}$$

证明　设 A 表示事件 $f_1(a)\oplus f_1(b)\oplus f_2(c)\oplus f_2(d)\oplus f_3(p)\oplus f_3(q)=y$，$A_j$ 表示事件 $f_1(a)\oplus f_1(b)=w_j$, $1\leqslant j\leqslant 2^n$, 其中 $I_n=\{w_1,\cdots,w_{2^n}\}$。则由引理 1

和引理 2 得

$$\begin{aligned}&P(A\cap A_j)\\&=P(f_1(a)\oplus f_1(b)=w_j)P(f_2(c)\oplus\\&\quad f_2(d)\oplus f_3(p)\oplus f_3(q)=y\oplus w_j)\\&\leqslant\frac{1}{2^{n-1}}\cdot\frac{1}{2^n-1}\end{aligned}$$

因此 $P(A)=\sum_{j=1}^{2^n}P(A\cap A_j)\leqslant 2^n\cdot\frac{1}{2^{n-1}}\cdot\frac{1}{2^n-1}\leqslant\frac{2}{2^n-1}$。

3　可调分组密码的设计与分析

首先，我们讨论使用 4 轮 MISTY 结构设计的可调分组密码是不安全的，进一步指出如果 T 添加在不合适的位置，使用多少轮的 MISTY 结构都无法构造安全的分组密码。

定理 1　设 f_1,f_2,f_3,f_4 是 I_n 上相互独立的随机置换。如果把 tweak T 分别添加（采用加法⊕）到 $L_i,i=0,1,2,3$，则 4 轮 MISTY 型可调分组密码不是伪随机的。

证明　当 $i=0,2,3$ 时，攻击者做 2 次询问。

1) 当 $i=0$ 时，$L_1=R_0,R_1=R_0\oplus f_1(T\oplus L_0)$。询问 (L,R,T) 得到 (L_4^1,R_4^1)；询问 (L',R,T') 得到 (L_4^2,R_4^2)，2 次询问满足 $L\oplus T=L'\oplus T'=a$。因为 $L_1^1=L_1^2=R,\ L_1^1=L_1^2=R\oplus f_1(a)$，从而在输出中有 $L_4^1=L_4^2,\ R_4^1=R_4^2$

2) 当 $i=2$ 时，$L_3=R_2,R_3=R_2\oplus f_3(T\oplus L_2)$。询问（0，0，$T$）得到 (L_4^1,R_4^1)；询问 $(0,0,T')$ 得到 (L_4^2,R_4^2)，则有 $L_4^1\oplus L_4^2=R_4^1\oplus R_4^2=f_3(f_1(0)\oplus T)\oplus f_3(f_1(0)\oplus T')$，方案是不安全的。

3) 当 $i=3$ 时，$L_4=R_3,R_4=R_3\oplus f_4(T\oplus L_3)$。询问 (L,R,T) 得到 (L_4^1,L_4^1)；询问 (L,R,T') 得到 (L_4^2,R_4^2)，因为 L_4^1,L_4^2，只与 L，R 有关，而与 T，T' 无关，所以 $L_4^1=L_4^2$。

4) 当 $i=1$ 时，$L_2=R_1,R_2=R_1\oplus f_2(T\oplus L_1)$。攻击者做 4 次询问，分别询问 $(0,0,0),(0,0,1),(0,1,0),(0,1,1)$，对应的输出分别为 (L_4^1,R_4^1)，(L_4^2,R_4^2)，(L_4^3,R_4^3)，(L_4^4,R_4^4)，则有 $L_4^1\oplus L_4^2\oplus\ L_4^3\oplus L_4^4=0$。

定理 2　设 f_1,f_2,f_3,f_4 是 I_n 上相互独立的随机置换。如果把 tweak T 异或到 R_i, i=0,1,2,3，则 4 轮 MISTY 型可调分组密码不是伪随机的。

证明　攻击者做 2 次或 4 次询问。

1) 第一轮中 $L_1=T\oplus R_0$。询问 (L,R,T) 得到 (L_4^1,R_4^1)；询问 (L,T,R) 得到 (L_4^2,R_4^2)，$R\neq T$，则有 $L_4^1=L_4^2=T\oplus R\oplus f_1(L)\oplus f_2(R\oplus T)\oplus f_3(R\oplus T\oplus f_1(L))$。

2) 第二轮中 $L_2=R_1,R_2=T\oplus R_1\oplus f_2(L_1)$。询问 (L,R,T) 得到 (L_4^1,R_4^1)；询问 (L,R,T') 得到 (L_4^2,R_4^2)，则有 $L_4^1\oplus L_4^2=T\oplus T'$。如果 $L_2=R_1\oplus T,R_2=T\oplus R_1\oplus f_2(L_1)$，攻击者做 4 次询问 $(0,0,0),(0,0,1),(0,1,0),(0,1,1)$，对应的输出分别为 (L_4^1,R_4^1)，(L_4^2,R_4^2)，(L_4^3,R_4^3)，(L_4^4,R_4^4)，则 $L_4^1\oplus L_4^2\oplus L_4^3\oplus L_4^4=0$。

3) 在第三轮中，若 $L_3=R_2(\text{or}R_2\oplus T),\ R_3=T\oplus R_2\oplus f_3(L_2)$，或者在第四轮中，$L_4=R_3$ (或$R_3\oplus T$)，$R_4=T\oplus R_3\oplus f_4(L_3)$。攻击者采用与 2）相同的询问可进行攻击。

4) 第一轮输出为 $L_1=R_0,R_1=R_0\oplus T\oplus f_1(L_0)$，攻击者做 4 次询问 $(0,0,0),(0,0,1)\ (0,1,0),(0,1,1)$，对应的输出分别为 (L_4^1,R_4^1)，(L_4^2,R_4^2)，(L_4^3,R_4^3)，(L_4^4,R_4^4)，则 $L_4^1\oplus L_4^2\oplus L_4^3\oplus L_4^4=0$。

从定理 1 和定理 2 可以看出，对于基于 4 轮 MISTY 结构构造的可调分组密码，攻击者只需做 2 次或 4 次不同的询问，就可以以概率为 1 的可能性在输出的左半部分得到一个碰撞；但对于一个可调随机置换，在相同条件下出现这种可能性的概率是非常小的，这也就是说，攻击者几乎可以以概率为 1 的可能性区分一个基于 4 轮 MISTY 结构构造的可调分组密码和一个可调随机置换。这说明使用这样的结构是无法为我们提供安全保障的，在实际应用中要选用多轮的结构来设计自己需要的密码工具。

进一步还可以把 4 轮结构的一些结论推广到任意 n 轮。

定理 3　设 $f_1,\cdots,f_n,\forall n\geqslant 4$ 是 I_n 上相互独立的随机置换。如果把 tweak T 添加到 $L_0,L_{n-2},L_{n-1},R_{n-2},R_{n-1}$，则 n 轮 MISTY 型可调分组密码不是伪随机的。

证明　证明过程同 4 轮结构中的 L_0,L_2,L_3,R_2,R_3 情况。

从这个一般性结论中可以看出，无论选用的结构轮数有多大，当把标号“tweak”添加到第一轮左半部分和最后 2 轮时，MISTY 结构是无法提供安全的可调分组密码的。这也提醒我们在实际应用中，在利用 MISTY 结构来设计可调分组密码时，有些情况是无需考虑的。

下面讨论利用 5 轮 MISTY 结构能否提供安全

的可调分组密码，由上面的讨论知，在 L_0, L_3, L_4, R_3, R_4 这些位置添加 tweak 是无法保证安全的，下面来看其他情况。

定理 4　设 f_1, f_2, f_3, f_4, f_5 是 I_n 上相互独立的随机置换。如果把 tweak T 添加到 L_2，则此 5 轮 MISTY 型可调分组密码不是伪随机的。

证明　攻击者分别询问 $(0,0,0),(0,1,0),(0,0,1)$ $(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)$ 得到对应的输出分别为 (L_5^1, R_5^1)，(L_5^2, R_5^2)，(L_5^3, R_5^3)，(L_5^4, R_5^4)，(L_5^5, R_5^5)，(L_5^6, R_5^6)，(L_5^7, R_5^7)，(L_5^8, R_5^8)，则有

$$L_5^1 = f_1(0) \oplus f_2(0) \oplus f_3(f_1(0)) \oplus f_4(f_1(0) \oplus f_2(0))$$

$$L_5^2 = 1 \oplus f_1(0) \oplus f_2(1) \oplus f_3(1 \oplus f_1(0)) \oplus f_4(1 \oplus f_1(0) \oplus f_2(1))$$

$$L_5^3 = f_1(0) \oplus f_2(0) \oplus f_3(1 \oplus f_1(0)) \oplus f_4(f_1(0) \oplus f_2(0))$$

$$L_5^4 = 1 \oplus f_1(0) \oplus f_2(1) \oplus f_3(f_1(0)) \oplus f_4(1 \oplus f_1(0) \oplus f_2(1))$$

$$L_5^5 = f_1(1) \oplus f_2(0) \oplus f_3(f_1(1)) \oplus f_4(f_1(1) \oplus f_2(0))$$

$$L_5^6 = f_1(1) \oplus f_2(0) \oplus f_3(1 \oplus f_1(1)) \oplus f_4(f_1(1) \oplus f_2(0))$$

$$L_5^7 = 1 \oplus f_1(1) \oplus f_2(1) \oplus f_3(1 \oplus f_1(1)) \oplus f_4(1 \oplus f_1(1) \oplus f_2(1))$$

$$L_5^8 = 1 \oplus f_1(1) \oplus f_2(1) \oplus f_3(f_1(1)) \oplus f_4(1 \oplus f_1(1) \oplus f_2(1))$$

从而有 $L_5^1 \oplus L_5^2 \oplus L_5^3 \oplus L_5^4 \oplus L_5^5 \oplus L_5^6 \oplus L_5^7 \oplus L_5^8 = 0$。

从定理 4 可以看出，攻击者在 4 轮结构中询问 4 次达到的攻击效果在 5 轮结构中要询问 8 次才能达到，结构的轮数增加 1，攻击者要想达到相同的攻击效果，询问的次数要增加一倍。这说明增加轮数确实能增加攻击者的难度，增强结构的安全性能。

定理 5　设 f_1, f_2, f_3, f_4, f_5 是 I_n 上相互独立的随机置换。如果把 tweak T 添加到 R_2，且 L_3=R_2 $R_3 = R_2 \oplus T \oplus f_3(L_2)$，则此 5 轮 MISTY 型可调分组密码不是伪随机的。

证明　询问 (L,R,T) 和 (L,R,T')，分别得到 (L_5^1, R_5^1)，(L_5^2, R_5^2)，则有 $L_5^1 \oplus L_5^2 = T \oplus T'$。

定理 6　设 f_1, f_2, f_3, f_4, f_5 是 I_n 上相互独立的伪随机置换。如果把 tweak T 异或到 R_0，且 $L_1 = R_0, R_1 = R_0 \oplus T \oplus f_1(L_0)$，则此 5 轮 MISTY 型可调分组密码 ψ_{2n} 在选择明文攻击下是安全的。

证明　不失一般性，设 $f_i, i = 1,2,3,4,5$ 是随机的。攻击者 A 可以询问一个预言 O，O 为 ψ_{2n}、Π_T 中的一个。假设 A 对 O 做了 q 次不同询问 $(L^1, R^1, T^1), \cdots, (L^q, R^q, T^q)$。设 $(L_j^i, R_j^i), i = 1, \cdots, q$; $j = 1,2,3,4,5$ 为第 i 次询问的第 j 次输出结果。设 A_L 表示事件“$L_3^1, L_3^2, \cdots, L_3^q$ 互不相同”；A_R 表示事件“$R_3^1, R_3^2, \cdots, R_3^q$ 互不相同”。因为 $L_5^i = R_4^i = R_3^i \oplus f_4(L_3^i), i = 1, \cdots, q$ 且 f_4 是随机的，所以当事件 A_L 发生时，$L_5^1, L_5^2, \cdots, L_5^q$ 是完全随机的；同理因为 $R_5^i = R_4^i \oplus f_5(R_3^i), i = 1, \cdots, q$ 且 f_5 随机，所以当 A_R 发生时，$R_5^1, R_5^2, \cdots, R_5^q$ 是随机的。又因为 f_4、f_5 相互独立，所以 $(L_5^1, R_5^1), (L_5^2, R_5^2), \cdots, (L_5^q, R_5^q)$ 是随机的。从而

$$ADV_E^{\text{tprp}}(A) = \left| P[A \to 1 \middle| O \leftarrow \psi_{2n}] - P[A \to 1 \middle| O \leftarrow \Pi_T] \right|$$

$$= \left| P[(A \to 1 \middle| O \leftarrow \psi_{2n}) \middle| A_L \cap A_R] P(A_L \cap A_R) + \right.$$

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

$$P[(A \to 1 \middle| O \leftarrow \Pi_T) \middle| A_L \cap A_R] P(A_L \cap A_R) -$$

$$\left. P[(A \to 1 \middle| O \leftarrow \Pi_T) \middle| \overline{A_L \cap A_R}] P(\overline{A_L \cap A_R}) \right|$$

$$= \left| P[(A \to 1 \middle| O \leftarrow \psi_{2n}) \middle| \overline{A_L \cap A_R}] P(\overline{A_L \cap A_R}) - \right.$$

$$\left. P[(A \to 1 \middle| O \leftarrow \Pi_T) \middle| \overline{A_L \cap A_R}] P(\overline{A_L \cap A_R}) \right|$$

$$\leqslant P(\overline{A_L \cap A_R}) \leqslant \sum_{1 \leqslant i \leqslant j \leqslant q} P(L_3^i = L_3^j) \oplus \sum_{1 \leqslant i \leqslant j \leqslant q} P(R_3^i = R_3^j)$$

从上面的分析可以看出，5 轮结构的安全性主要取决于结构内部第三轮的输出中出现碰撞的概率大小，只要这一概率足够小，则攻击者获得的优势函数值就足够小，它就不足以把此结构与可调随机置换区分开来。所以在实际应用中要注意对结构关键部位的数据作重点分析。

下面来计算第三轮输出中出现碰撞的概率 $P(L_3^i = L_3^j), P(R_3^i = R_3^j), 1 \leqslant i \leqslant j \leqslant q$。分 4 种情况讨论：

1)　$L_0^i = L_0^j, R_0^i = R_0^j, T^i \neq T^j$，则 $P(L_3^i = L_3^j) = P(T^i = T^j) = 0$，

$$\begin{aligned} & P(R_3^i = R_3^j) \\ &= P(f_3(R_0^i \oplus T^i \oplus f_1(L_0^i)) \oplus T^i \\ &= f_3(R_0^j \oplus T^j \oplus f_1(L_0^j)) \oplus T^j) \\ &\leqslant \frac{1}{2^n - 1} \end{aligned}$$

因为 f_3 是随机的，$R_0^i \oplus T^i \oplus f_1(L_0^i) \neq R_0^j \oplus T^j \oplus f_1(L_0^j)$，由引理 1 知不等式成立。

2)　$L_0^i = L_0^j, R_0^i \neq R_0^j$，则由引理 1 得

$$P(L_3^i = L_3^j) = P(f_2(R_0^i) \oplus T^i \oplus R_0^i = f_2(R_0^j) \oplus T^j \oplus R_0^j) \leqslant \frac{1}{2^n - 1}$$

由 f_2, f_3 是相互独立的随机置换及引理 2 得

$$\begin{aligned}&P(R_3^i = R_3^j)\\&= P(f_3(R_0^i \oplus T^i \oplus f_1(L_0^i)) \oplus T^i \oplus R_0^i \oplus f_2(R_0^i)\\&= f_3(R_0^j \oplus T^j \oplus f_1(L_0^j)) \oplus T^j \oplus R_0^j \oplus f_2(R_0^j))\\&\leqslant \frac{1}{2^{n-1}}\end{aligned}$$

3) $L_0^i \neq L_0^j, R_0^i = R_0^j$，则由 f_1 是随机置换及引理 1 得

$$P(L_3^i = L_3^j) = P(f_1(L_0^i) \oplus T^i = f_1(L_0^j) \oplus T^j) \leqslant \frac{1}{2^n - 1}$$

由 f_1, f_3 是相互独立的随机置换及引理 2 得

$$\begin{aligned}P(R_3^i = R_3^j) &= P(f_3(R_0^i \oplus T^i \oplus f_1(L_0^i)) \oplus T^i \oplus f_2(L_0^i)\\&= f_3(R_0^j \oplus T^j \oplus f_1(L_0^j)) \oplus T^j \oplus f_2(L_0^j))\\&\leqslant \begin{cases}\dfrac{1}{2^n - 1}, & f_1(L_0^i) \oplus T^i = f_1(L_0^j) \oplus T^j\\ \dfrac{1}{2^{n-1}}, & f_1(L_0^i) \oplus T^i \neq f_1(L_0^j) \oplus T^j\end{cases}\end{aligned}$$

所以在此情况下 $P(R_3^i = R_3^j) \leqslant \frac{1}{2^{n-1}}$

4) $L_0^i \neq L_0^j, R_0^i = R_0^j$，由 f_1, f_2 是相互独立的随机置换及引理 2 得

$$\begin{aligned}&P(L_3^i = L_3^j)\\&= P(f_2(R_0^i) \oplus f_1(L_0^i) \oplus T^i \oplus R_0^i\\&= f_2(R_0^j) \oplus f_1(L_0^j) \oplus T^j \oplus R_0^j)\\&\leqslant \frac{1}{2^{n-1}}\end{aligned}$$

由 f_1, f_2, f_3 是相互独立的随机置换及引理 3 得

$$\begin{aligned}&P(R_3^i = R_3^j)\\&= P(f_3(R_0^i \oplus T^i \oplus f_1(L_0^i)) \oplus T^i \oplus f_1(L_0^i) \oplus f_2(R_0^i)\\&= f_3(R_0^j \oplus T^j \oplus f_1(L_0^j)) \oplus T^j \oplus f_1(L_0^j) \oplus f_2(R_0^j))\\&\leqslant \begin{cases}\dfrac{1}{2^{n-1}}, & f_1(L_0^i) \oplus T^i \oplus R_0^i = f_1(L_0^j) \oplus T^j \oplus R_0^j\\ \dfrac{2}{2^n - 1}, & f_1(L_0^i) \oplus T^i \oplus R_0^i \neq f_1(L_0^j) \oplus T^j \oplus R_0^j\end{cases}\end{aligned}$$

所以在此情况下 $P(R_3^i = R_3^j) \leqslant \frac{2}{2^n - 1}$

综上所述

$$\sum_{1 \leqslant i \leqslant j \leqslant q} P(L_3^i = L_3^j) \leqslant C_q^2 \frac{1}{2^{n-1}} = \frac{q(q-1)}{2^n}$$

$$\sum_{1 \leqslant i \leqslant j \leqslant q} P(R_3^i = R_3^j) \leqslant C_q^2 \frac{2}{2^n - 1} = \frac{q(q-1)}{2^n - 1}$$

所以就有

$$\begin{aligned}&ADV_{\bar{E}} = \max_A \{ADV_{\bar{E}}^{\text{tprp}}(A)\}\\&\leqslant P(\overline{A_L \cap A_R}) \leqslant \sum_{1 \leqslant i \leqslant j \leqslant q} P(L_3^i = L_3^j) \oplus \sum_{1 \leqslant i \leqslant j \leqslant q} P(R_3^i = R_3^j)\\&\leqslant \frac{q(q-1)}{2^n} + \frac{q(q-1)}{2^n - 1}\end{aligned}$$

是可忽略的。从而方案是安全的。

注：在此方案中，如果把 $L_1 = R_0, R_1 = R_0 \oplus T \oplus f_1(L_0)$ 换成 $L_1 = R_0 \oplus T, R_1 = R_0 \oplus T \oplus f_1(L_0)$，则方案是不安全的。只要询问 2 次即可攻破方案。询问 (L,R,T) 与 $(L,T,R), R \neq T$，则 2 次询问的输出是相同的。这种情况可以推广到任意 n 轮，即采用这种添加方式是无法保证安全的。用定理 6 的方法可以证明：

定理 7 设 f_1, f_2, f_3, f_4, f_5 是 I_n 上相互独立的伪随机置换。在下列 3 种情况下 5 轮 MISTY 型可调分组密码 ψ_{2n} 在选择明文攻击下是安全的。

1) 把 tweak T 添加到 L_1

2) 把 tweak T 添加到 R_1（$L_2 = R_1$ 或 $R_1 \oplus T$ 均可）

3) 把 tweak T 添加到 R_2，且

$L_3 = R_2 \oplus T, R_3 = R_2 \oplus T \oplus f_3(L_2)$

4 结束语

利用 MISTY 型结构对 Liskov 等人提出的公开问题，即如何不借助于现有的分组密码来直接设计可调分组密码进行了研究。通过在结构中的各轮添加 tweak 的方法，利用 4 轮和 5 轮 MISTY 结构设计了可调分组密码，并对各种方案的安全性进行了系统的分析。对 4 轮结构上的各种方案进行了攻击，指出 4 轮结构无法提供安全的可调分组密码。通过对 5 轮结构可调分组密码的分析，指出有些 5 轮结构可以提供安全的方案，在 MISTY 结构上设计安全的可调分组密码轮数不得少于 5。

参考文献：

[1] MOSES L, RONALD L R, DAVID W. Tweakable block ciphers[A]. CRTPTO 2002[C]. California, USA, Springer, Heidelberg, 2002. 31- 46.

[2] HALEVI S, ROGWAY P. A tweakable enciphering mode[A]. CRYPTO 2003[C]. California, USA, Springer, Heidelberg, 2002. 482-499.

（下转第 87 页）