软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(2)):207−215

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

Lai-Massey 模型的差分和线性可证明安全性*

付立仕, 金晨辉

(解放军信息工程大学,河南 郑州 450001)

通讯作者: 付立仕, E-mail: 15036018167@163.com

摘 要: 1991 年,Lai 和 Massey 设计了 IDEA 算法.该算法首次用到了 Lai-Massey 模型.1999 年,Vaudenay 在 Lai-Massey 模型中引入正形置换或几乎非正形置换,证明了该 Lai-Massey 模型满足 Luby-Rackoff 定理.主要对 Lai-Massey 模型的差分和线性可证明安全性进行研究.首先,给出了 Lai-Massey 模型中差分活动 F 函数个数的下确界.其次,证明了当 F 函数是正形置换时,Lai-Massey 模型的差分活动 F 函数个数下确界与 Feistel 模型中活动 F 函数个数的下确界一样.最后,通过引入对偶模型,证明了 Lai-Massey 模型的差分传递链和组合传递链在结构上的对偶性,并基于该对偶性直接给出了 Lai-Massey 模型的线性可证明安全性.

关键词: Lai-Massey 模型;差分分析;线性分析;活动 F-函数;对偶性;正形置换

中文引用格式: 付立仕,金晨辉.Lai-Massey 模型的差分和线性可证明安全性.软件学报,2013,24(Suppl.(2)):207−215. http://www.jos.org.cn/1000-9825/13038.htm

英文引用格式: Fu LS, Jin CH. Differential and linear provable security of Lai-Massey scheme. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(2)):207−215 (in Chinese). http://www.jos.org.cn/1000-9825/13038.htm

Differential and Linear Provable Security of Lai-Massey Scheme

FU Li-Shi, JIN Chen-Hui

(The PLA Information Engineering University, Zhengzhou 450001, China)

Corresponding author: FU Li-Shi, E-mail: 15036018167@163.com

Abstract: Lai and Massey designed IDEA in 1991 when Lai-Massey scheme was first used in the algorithm. Vaudenay in 1999 added a function σ which has the orthomorphic or α-almost orthomorphic property in Lai-Massey scheme, and proved that this construction could make Lai-Massey scheme satisfy the Luby-Rackoff theorem. In this paper, the provable security of Lai-Massey scheme against differential and linear cryptanalysis is investigated. Firstly, the infimum of the number of differentially active F-functions in Lai-Massey scheme is given no matter if F is an orthomorphism or not. Secondly, the results in this paper indicate that when F is an orthomorphism, the infimum of the number of differentially active F-functions is the same as that of Feistel scheme. Finally, a dual model is introduced to study the duality between the differential characteristic chains and linear approximation chains in Lai-Massey scheme, which can be used to obtain similar results of linear cryptanalysis for Lai-Massey scheme directly.

Key words: Lai-Massey scheme; differential cryptanalysis; linear cryptanalysis; active F-function; duality; orthomorphism

Lai-Massey 模型是 1991 年由 Lai 和 Massey 提出来的.该模型首先在 IDEA[1]算法中得到了应用.在 1999 年的 Asiacrypt 上,Vaudenay [2]证明了,如果双射σ是正形置换(即双射σ使$\sigma(x)-x$仍是双射)或α几乎正形置换(使$\sigma(x)-x$最多只有α个元素没有原象),则该结构 3 圈具备伪随机特性、4 圈具有超伪随机特性,因而建议将 Lai-Massey 结构双射σ设计为正形置换或几乎正形置换.在本文中,我们主要针对 Vaudenay 提出的改进 Lai-Massey 模型进行研究.进而,Luo[3]等人证明了 3 轮是 Lai-Massey 模型达到伪随机性的必要条件,4 轮是 Lai-Massey 模型达到强伪随机性的必要条件.2004 年,Junod 和 Vaudenay 设计了 FOX 算法[4],指出 FOX 在各种平台上的性能良

* 基金项目: 国家自然科学基金(61272488)
收稿时间: 2013-07-17; 定稿时间: 2013-10-16

好,且连续两轮的非平凡的差分传递链和组合传递链中至少有 1 个活动的 F 函数.

自从 FOX 算法提出以来,学者们已经对 FOX 做了积分攻击[5]、不可能差分攻击[6,7]、积分碰撞攻击[8]和差错攻击[9].但是,这些攻击都没有影响到 FOX 算法的安全性,从反面说明了 FOX 算法设计的实用性.2011 年,Yun 等人扩展了 Feistel 模型,提出了类 Feistel 模型[10]的概念,并证明了 Lai-Massey 模型也是类 Feistel 模型的一个实例,进而从另一个方面证明了 Lai-Massey 模型与 Feistel 模型具有相同的 Luby-Rackoff 安全性特性[11].对于 Feistel 模型已经有大量的安全性结论,但对于 Lai-Massey 模型,其安全性结论却较少.本文主要对 Lai-Massey 模型的可证明安全性结论进行研究.

目前,对分组密码算法最为有效的攻击方法是差分分析[12]和线性分析[13].因此,对于一种新分组密码算法,设计者需要评估该算法抵抗差分分析和线性分析的能力.由于 Lai-Massey 模型仅含有 F 函数和 σ 函数,对于 σ 为仿射变换的 Lai-Massey 模型,其 n 轮差分特征(线性逼近)的概率仅与活动 F 函数的个数有关.因此,本文主要利用活动 F 函数的个数来研究含仿射变换 σ 的 Lai-Massey 模型的可证明安全性.在本文中,我们给出了差分和线性活动 F 函数个数的下确界,作为衡量 Lai-Massey 模型最大差分转移概率和线性逼近优势的指标.其次,在考察 Lai-Massey 模型的线性可证明安全性时,本文通过引入对偶模型,证明了在 Lai-Massey 模型中,其差分传递链和组合传递链在结构上是对偶的,并根据该对偶性直接得到了 Lai-Massey 模型的线性可证明安全性.

本文第 1 节给出本文常见符号的定义.第 2 节给出 Lai-Massey 模型的差分传递链中活动 F 函数个数的下确界,并得出在 F 函数是正形置换时,该下确界与 Feistel 模型的下确界相同.第 3 节给出 Lai-Massey 模型中存在的对偶定理,进而直接得到 Lai-Massey 模型组合传递链中活动 F 函数个数的下确界.第 4 节对本文进行总结.

1 基础知识

本节主要给出 Lai-Massey 模型的差分(线性)分析的相关概念,对偶模型也在本节中引入,用以证明 Lai-Massey 模型中的对偶定理.

定义 1[2]. 设 F_k 和 σ 是 $\{0,1\}^n$ 到 $\{0,1\}^n$ 的映射且 σ 是双射, $(\{0,1\}^n,+)$ 为交换群, k 是圈密钥,则称以

$$Q_k(x,y)=(\sigma(x+F_k(x-y)),y+F_k(x-y))$$

为圈函数的分组密码为 Lai-Massey 模型,并称 F_k 是圈函数 Q_k 的 F 函数,称 σ 是圈函数 Q_k 的 σ 函数.

为保证 Lai-Massey 模型加解密的相似性,最后一圈的圈函数一般设置为

$$Q_k(x,y)=(x+F_k(x-y),y+F_k(x-y)).$$

本文主要研究定义在群 $(\{0,1\}^n,\oplus)$ 上的 Lai-Massey 模型.为使描述更加简单,本文中我们将忽略最后一圈的圈函数与前几圈的差异,并将 $F_1,F_2,...,F_r$ 都记为 F, 则 $Q_k(x,y)=(\sigma(x\oplus F(x\oplus y)),y\oplus F(x\oplus y))$, 该处理并不影响本文结果的适用性.

定义 2[14]. 设 $(G,+)$ 是交换群, $f:G\to G,\alpha\in G,\beta\in G$, 则称

$$p_f(\alpha\to\beta)=\frac{1}{|G|}\#\{x\in G:f(x+\alpha)-f(x)=\beta\}$$

为 f 的差分对应 $\alpha\to\beta$ 的概率.这里 $|G|$ 是集合 G 中点的个数.

定义 3[14]. 设 $f:\{0,1\}^n\to\{0,1\}^m,\alpha\in\{0,1\}^n,\beta\in\{0,1\}^m$, 则称

$$W_{(f)}(\alpha\to\beta)=\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{\beta\cdot f(x)\oplus\alpha\cdot x}$$

为 f 的线性逼近 $\alpha\to\beta$ 的相关系数,这里 $\alpha\cdot x$ 是向量 α 与向量 x 的点积.

定义 4[2]. 设 δ 是交换群 $(G,+)$ 到自身的同态, $c\in G$, 则称函数 $\sigma(x)=\delta(x)+c$ 为群 $(G,+)$ 上的一个仿射函数.

由于 $\sigma(x+\alpha)-\sigma(x)=\sigma(\alpha)-\sigma(0)$, 因而仿射函数的差分对应的概率只能是 0 或 1.

定义 5[2]. 设 $(G,+)$ 是交换群, $f:G\to G$, 令 $g(x)=f(x)-x$, 如果 f 和 g 都是双射,则称 f 为群 $(G,+)$ 上的正形置换.

定义 6[14]. 设 $\alpha_i \to \alpha_{i+1}$ 是第 i 圈圈函数的差分对应,则称 $\alpha_1 \to \alpha_2 \to \alpha_3 \to ... \to \alpha_{m+1}$ 是一条 m 轮差分传递链.又设 $A_i \to \gamma_i$ 是第 i 圈圈函数中 F 函数的差分对应,如果 $A_i \neq 0$, 则称该 F 函数是活动的,并称 $A_1, A_2, ..., A_m$ 中非零元的个数为该差分传递链中活动 F 函数的个数.如果 $\alpha_1 = ... = \alpha_{m+1} = 0$, 则称该链是一条平凡差分传递链,否则称为非平凡差分传递链.

定义 7[14]. 设 $\alpha_i \to \alpha_{i+1}$ 是第 i 圈圈函数的线性逼近,则称 $\alpha_1 \to \alpha_2 \to \alpha_3 \to ... \to \alpha_{m+1}$ 是一条 m 轮组合传递链.又设 $A_i \to \gamma_i$ 是第 i 圈圈函数中 F 函数的线性逼近,如果 $\gamma_i \neq 0$, 则称该 F 函数是活动的,并称 $\gamma_1, \gamma_2, ..., \gamma_m$ 中非零元的个数为该组合传递链中活动 F 函数的个数.如果 $\gamma_1 = ... = \gamma_{m+1} = 0$, 则称该链是一条平凡组合传递链,否则称为非平凡组合传递链.

由于平凡的差分对应(线性逼近)的研究意义不大,故在本文中,我们研究的都是非平凡的差分对应(线性逼近).

定义 8. 设仿射变换 $\sigma(x) = Mx \oplus C$ 是双射,则称将 Lai-Massey 模型中的 σ 函数替换为 $\sigma_D(x) = (M^{-1})^T x \oplus C$ 所得的模型为该 Lai-Massey 模型的对偶模型.

2 Lai-Massey 模型 *n* 轮差分传递链中活动 *F* 函数的下确界

我们首先给出 Lai-Massey 模型圈函数的差分对应与其 F 函数和 σ 函数的差分对应之间的关系.

定理 1. Lai-Massey 模型圈函数 Q 的差分对应 $(\alpha, \beta) \to (A, B)$ 的概率非零的充要条件是 F 函数和 σ 函数的差分对应分别为 $\alpha \oplus \beta \to \beta \oplus B$ 和 $\alpha \oplus \beta \oplus B \to A$, 且这两个差分对应的概率均非零,且

$$p_Q((\alpha, \beta) \to (A, B)) = p_F(\alpha \oplus \beta \to \beta \oplus B) p_\sigma(\alpha \oplus \beta \oplus B \to A).$$

特别地,若 $\sigma(x) = \delta(x) \oplus \sigma(0)$ 是仿射函数,则 F 函数的输出差为 $\beta \oplus B = \alpha \oplus \delta^{-1}(A)$.

证明:设 Lai-Massey 模型的两个输入分别为 (x, y) 和 $(x \oplus \alpha, y \oplus \beta)$, 则 F 函数对应的输出分别为 $b_1 = F(x \oplus y)$ 和 $b_2 = F(x \oplus y \oplus \alpha \oplus \beta)$. 由于圈函数 Q 的输出差为

$$\begin{aligned}
&Q(x \oplus \alpha, y \oplus \beta) \oplus Q(x, y)\\
&= (\sigma(x \oplus \alpha \oplus F(x \oplus y \oplus \alpha \oplus \beta)), y \oplus \beta \oplus F(x \oplus y \oplus \alpha \oplus \beta)) \oplus (\sigma(x \oplus F(x \oplus y)), y \oplus F(x \oplus y))\\
&= (\sigma(x \oplus \alpha \oplus b_2), y \oplus \beta \oplus b_2) \oplus (\sigma(x \oplus b_1), y \oplus b_1)\\
&= (\sigma(x \oplus \alpha \oplus b_2) \oplus \sigma(x \oplus b_1), \beta \oplus b_1 \oplus b_2).
\end{aligned}$$

因而圈函数 Q 的输出差为 (A, B) 等价于

$$\begin{cases} \sigma(x \oplus \alpha \oplus b_2) \oplus \sigma(x \oplus b_1) = A \\ F(x \oplus y) \oplus F(x \oplus y \oplus \alpha \oplus \beta) = \beta \oplus B \end{cases},$$

即 F 和 σ 的差分对应分别为 $\alpha \oplus \beta \to \beta \oplus B$ 和 $\alpha \oplus \beta \oplus B \to A$.

记 $z = x \oplus y$. 显然,使得 Q 的输出差为 (A, B) 的输入的总数为

$$\begin{aligned}
&\#\{(x, y) : F(x \oplus y) \oplus F(x \oplus y \oplus \alpha \oplus \beta) = \beta \oplus B, \sigma(x \oplus \alpha \oplus b_2) \oplus \sigma(x \oplus b_1) = A\}\\
&= \#\{(x, z) : F(z) \oplus F(z \oplus \alpha \oplus \beta) = \beta \oplus B, \sigma(x \oplus \alpha \oplus b_2) \oplus \sigma(x \oplus b_1) = A\}\\
&= \sum_z \#\{x : F(z) \oplus F(z \oplus \alpha \oplus \beta) = \beta \oplus B, \sigma(x \oplus \alpha \oplus b_2) \oplus \sigma(x \oplus b_1) = A\}\\
&= \sum_{z : F(z) \oplus F(z \oplus \alpha \oplus \beta) = \beta \oplus B} \#\{x : \sigma(x \oplus \alpha \oplus b_2) \oplus \sigma(x \oplus b_1) = A\}.
\end{aligned}$$

再将 $b_2 = b_1 \oplus \beta \oplus B$ 代入上式,即得

$$\begin{aligned}
&\sum_{z : F(z) \oplus F(z \oplus \alpha \oplus \beta) = \beta \oplus B} \#\{x : \sigma(x \oplus \alpha \oplus b_1 \oplus \beta \oplus B) \oplus \sigma(x \oplus b_1) = A\}\\
&= \sum_{z : F(z) \oplus F(z \oplus \alpha \oplus \beta) = \beta \oplus B} \#\{t : \sigma(t \oplus \alpha \oplus \beta \oplus B) \oplus \sigma(t) = A\}\\
&= \#\{z : F(z) \oplus F(z \oplus \alpha \oplus \beta) = \beta \oplus B\} \times \#\{t : \sigma(t \oplus \alpha \oplus \beta \oplus B) \oplus \sigma(t) = A\}.
\end{aligned}$$

这说明圈函数 Q 的差分对应 $(\alpha, \beta) \to (A, B)$ 的概率为

$$p_Q((\alpha,\beta)\to(A,B))=p_F(\alpha\oplus\beta\to\beta\oplus B)p_\sigma(\alpha\oplus\beta\oplus B\to A).$$

因而 $p_Q((\alpha,\beta)\to(A,B))\neq 0$ 等价于 $p_F(\alpha\oplus\beta\to\beta\oplus B)\neq 0$ 且 $p_\sigma(\alpha\oplus\beta\oplus B\to A)\neq 0$.

特别地,如果 σ 是仿射函数,则在给定输入差时,其输出差是确定的.故由 $p_\sigma(\alpha\oplus B\oplus\beta\to A)=1$ 可知, $\delta(\alpha\oplus\beta\oplus B)=A$, 因而有 $\sigma(\alpha\oplus B\oplus\beta)=A$, 故 F 函数的输出差 $\beta\oplus B=\alpha\oplus\delta^{-1}(A)$. □

引理 1. 设 $f:\{0,1\}^n\to\{0,1\}^n$ 是双射,则以下 3 个条件等价:

(1) f 是正形置换;

(2) $\forall\alpha\neq 0, p_f(\alpha\to\alpha)=0$;

(3) $\forall\alpha\neq 0, W_{(f)}(\alpha\to\alpha)=0$.

证明:记 $g(x)=f(x)\oplus x$,则 f 是群 $(G,+)$ 上的正形置换等价于 g 是双射,即对 $\forall\alpha\neq 0$, 都有 $g(x\oplus\alpha)\oplus g(x)\neq g(x)\neq 0$, 这等价于 $\forall\alpha\neq 0$, 均有 $p_g(\alpha\to 0)=0$, 又由 $p_g(\alpha\to 0)=p_f(\alpha\to\alpha)$ 可知,(1)与(2)等价.另一方面,由 Walsh 谱的性质可知, g 是双射等价于 $\forall\alpha\neq 0$, 均有 $W_g(0\to\alpha)=0$, 即 $W_{(f)}(\alpha\to\alpha)=0$, 即(1)与(3)等价.本定理得证. □

在以下的讨论中,我们均假设 σ 是仿射函数.显然,如果仿射函数 $\sigma(x)=\delta(x)+\sigma(0)$ 是正形置换,则线性函数 $\delta(x)$ 也是正形置换.

引理 2. 设仿射函数 σ 是正形置换,则 σ^2 也是正形置换;又若正形置换 σ 是线性函数,则 $\sigma(x)=x$ 当且仅当 $x=0$.

证明:后一结论显然,现证前一结论.设 $\lambda(x)=\sigma(x)\oplus x$, 则

$$\sigma^2(x)\oplus x=[\sigma^2(x)\oplus\sigma(x)]\oplus\sigma(x)\oplus x=[\sigma(\sigma(x)\oplus x)\oplus\sigma(0)]\oplus\sigma(x)\oplus x=\lambda^2(x)\oplus\sigma(0).$$

又 λ 是双射,因而 λ^2 也是双射,故 $\sigma^2(x)\oplus x$ 为双射,再由 $\sigma^2(x)$ 是双射即知 $\sigma^2(x)$ 是正形置换. □

结合定理 1,我们直接给出 4 轮 Lai-Massey 模型的差分传递链的结构,如下引理 3 所示.

引理 3. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 是仿射变换,Lai-Massey 模型的输入差为 (α,β), 其第 1 圈~第 4 圈 F 函数的输出差依次为 c,d,e,f,则 Lai-Massey 模型 4 轮差分传递链的结构为

$$\begin{aligned}(\alpha,\beta)&\to(\delta(\alpha)\oplus\delta(c),\beta\oplus c)\to(\delta^2(\alpha)\oplus\delta^2(c)\oplus\delta(d),\beta\oplus c\oplus d)\\&\to(\delta^3(\alpha)\oplus\delta^3(c)\oplus\delta^2(d)\oplus\delta(e),\beta\oplus c\oplus d\oplus e)\\&\to(\delta^4(\alpha)\oplus\delta^4(c)\oplus\delta^3(d)\oplus\delta^2(e)\oplus\delta(f),\beta\oplus c\oplus d\oplus e\oplus f),\end{aligned}$$

且相应的 F 函数的差分对应依次为

$$\alpha\oplus\beta\to c,\delta(\alpha)\oplus\delta(c)\oplus\beta\oplus c\to d,\delta^2(\alpha)\oplus\delta^2(c)\oplus\delta(d)\oplus\beta\oplus c\oplus d\to e,$$
$$\delta^3(\alpha)\oplus\delta^3(c)\oplus\delta^2(d)\oplus\delta(e)\oplus\beta\oplus c\oplus d\oplus e\to f.$$

定理 2. 设 σ 是正形置换,则 Lai-Massey 模型概率非零的两轮非平凡差分传递链中至少有 1 个活动的 F 函数.

证明:由定理 1 可知,Lai-Massey 模型中第 1 圈的圈函数的差分对应为 $(\alpha,\beta)\to(A,B)$ 等价于其 F 函数和 σ 函数的差分对应分别为 $\alpha\oplus\beta\to\beta\oplus B$ 和 $\alpha\oplus\beta\oplus B\to A$; 第 2 圈的圈函数的差分对应为 $(A,B)\xrightarrow{Q}(u,v)$ 等价于其 F 函数和 σ 函数的差分对应分别为 $A\oplus B\to B\oplus v$ 和 $A\oplus B\oplus v\to u$.

如果第 1 圈的 F 函数不活动,则有 $\alpha=\beta$, 故有 $\alpha=\beta=B$; 另外,若第 2 圈的 F 函数也不活动,则有 $A=B$, 故有 $A=B=v$, 故第 1 圈 σ 函数的差分对应为 $A\to A$. 由 $(A,B)\neq(0,0)$ 和 $A=B$ 可知 $A\neq 0$, 从而由引理 1 可知,当 σ 是正形置换时, $p_\sigma(A\to A)=0$, 进而由定理 1 可知, $p_Q((\alpha,\beta)\to(A,B))=0$, 这与题设矛盾.该矛盾说明第 1 圈和第 2 圈的 F 函数至少有 1 个是活动的. □

结合定理 2,我们可直接得到 Lai-Massey 模型的概率非零的 t 轮非平凡差分传递链中活动 F 函数的个数的下界,如推论 1 所示.

推论 1. 设 σ 是正形置换,则 Lai-Massey 模型的概率非零的 t 轮非平凡差分传递链中活动 F 函数的个数 $\geqslant\lfloor t/2\rfloor$.

定理 2 拓展了文献[4]中给出的在 FOX 算法中,连续两轮的非平凡差分传递链中至少有 1 个活动 F 函数的结论,并将该结论拓展至一般的 Lai-Massey 模型.下面的定理 3 给出了 Lai-Massey 模型中的一条活动 F 函数个数为 n 的 $2n$ 轮差分传递链,即该下界是不可改进的.

定理 3. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 为仿射正形置换, $\alpha\neq 0$, 则下述概率非零的 $2n$ 轮差分传递链是 Lai-Massey 模型的一条活动 F 函数个数为 n 的非平凡差分传递链:

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\alpha),\delta(\alpha))\to\ldots\to(\delta^{n-1}(\alpha),\delta^{n-1}(\alpha))$$
$$\to(\delta^{n}(\alpha),\delta^{n-1}(\alpha))\to(\delta^{n}(\alpha),\delta^{n}(\alpha)),$$

且其奇数轮 F 函数的差分对应为 $0\to 0$, $2t$ 轮 F 函数的差分对应为 $\delta^{t}(\alpha)\oplus\delta^{t-1}(\alpha)\to\delta^{t}(\alpha)\oplus\delta^{t-1}(\alpha)$.

证明:由定理 1 可以直接验证,当圈函数的差分对应为 $(\delta^{t}(\alpha),\delta^{t}(\alpha))\to(\delta^{t+1}(\alpha),\delta^{t}(\alpha))$ 时,其 F 函数的差分对应必为 $0\to 0$. 当圈函数的差分对应为 $(\delta^{t}(\alpha),\delta^{t-1}(\alpha))\to(\delta^{t}(\alpha),\delta^{t}(\alpha))$ 时,其 F 函数的差分对应必为 $\delta^{t}(\alpha)\oplus\delta^{t-1}(\alpha)\to\delta^{t}(\alpha)\oplus\delta^{t-1}(\alpha)$.

又 $\alpha\neq 0$, 由 σ 为正形置换得 $\delta(\alpha)\oplus\alpha\neq 0$, 进而可得 $\delta^{t-1}(\delta(\alpha)\oplus\alpha)\neq 0$, 即 $\delta^{t}(\alpha)\oplus\delta^{t-1}(\alpha)\neq 0$, 即偶数轮的 F 函数是活动的.故本定理构造的 $2n$ 轮差分传递链的活动 F 函数的个数为 n ,这说明本定理成立. □

由引理 1 可知,当 F 函数是正形置换时,定理 3 中所示的差分传递链的概率为 0,这是由于 F 函数不存在形如 $\alpha\to\alpha$ 的差分对应.定理 4 及其推论说明了当 F 函数是正形置换时,定理 2 和它的推论可以得到改进.

引理 4. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 为仿射正形置换,则 Lai-Massey 模型的概率非零且活动 F 函数个数为 1 的 3 轮差分传递链的结构为

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\alpha),\delta(\alpha))\to(\delta^{2}(\alpha),\delta(\alpha)),$$

且 F 函数相应的差分对应为 $0\to 0,\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha,0\to 0$, 这里 $\alpha\neq 0$.

证明:略. □

由引理 4 我们可直接给出在 Lai-Massey 模型中 3 轮差分传递链中活动 F 函数的个数下界,如定理 4 所示.

定理 4. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 为仿射正形置换,若 Lai-Massey 模型的 F 函数是正形置换,则其概率非零的 3 轮非平凡差分传递链中至少有 2 个活动 F 函数.

证明:如果 Lai-Massey 模型 3 轮差分传递链中只有 1 个活动 F 函数,则由引理 4 可知,其连续 3 轮的 F 函数的差分对应一定是 $0\to 0$, $\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha$ 和 $0\to 0$. 由于 F 函数是正形置换,故由引理 1 可知,当 F 函数是正形置换时,差分对应 $\delta(\alpha)\oplus\alpha\to\delta(\alpha)\oplus\alpha$ 的概率非零等价于 $\delta(\alpha)\oplus\alpha=0$. 又因为 δ 为线性正形置换,故由引理 2 知 $\delta(\alpha)\oplus\alpha=0$ 等价于 $\alpha=0$,这说明此时引理 4 给出的 3 轮差分传递链是平凡的差分传递链,故 3 轮非平凡差分传递链中至少有 2 个活动 F 函数. □

引理 5. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 为仿射正形置换,则当 F 函数为正形置换时,Lai-Massey 模型的概率非零且活动 F 函数个数为 2 的 4 轮差分传递链的结构为

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\delta(\alpha)\oplus d),\alpha\oplus d)$$
$$\to\left(\alpha\oplus d\oplus e,\alpha\oplus d\oplus e\right)\to(\delta(\alpha\oplus d\oplus e),\alpha\oplus d\oplus e),$$

且相应的 F 函数的差分对应依次为 $0\to 0,\delta(\alpha)\oplus\alpha\to d,\delta^{2}(\alpha)\oplus\delta(d)\oplus\alpha\oplus d\to e,0\to 0$. 其中, e 由方程 $\delta(e)\oplus e=\delta^{3}(\alpha)\oplus\alpha\oplus\delta^{2}(d)\oplus d$ 被 α 和 d 唯一确定,这里 $\alpha\neq 0$.

证明:略. □

定理 5. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 为仿射正形置换, $r\geqslant 3$, 如果 F 函数是正形置换,则 Lai-Massey 模型概率非零的 r 轮差分传递链中活动 F 函数的个数至少为 $D^{(r)}$, 其中,

$$D^{(r)}=\begin{cases}2n, & \text{若 } r=3n,3n+1\\ 2n+1, & \text{若 } r=3n+2\end{cases}.$$

证明:由定理 4 可知,对于 $0\leqslant i\leqslant n-1$, 第 $3i+1,3i+2,3i+3$ 轮圈函数中均至少有两个活动 F 函数,因而 $3n$ 轮差分传递链中至少有 $2n$ 个活动 F 函数,故 $3n+1$ 轮差分传递链中也至少有 $2n$ 个活动 F 函数.又因 2 轮差分传递

链中至少有 1 个活动 F 函数,且 $3n+2$ 轮差分传递链可写成一条 $3n$ 轮差分传递链与一条 2 轮差分传递链的链接,因而至少由 $2n+1$ 个活动 F 函数. □

定理 5 说明在 F 函数是正形置换时,Lai-Massey 模型的活动 F 函数个数的下界与 Feistel 模型的下界相同. 下面证明定理 5 的下界是可达的.

定理 6. 设 $\sigma(x)=\delta(x)\oplus\sigma(0)$ 为仿射正形置换, $\alpha_1=\alpha$, 且对任意的 $n\geqslant 1$ 有 $\alpha_{n+1}=\alpha_n\oplus d_n\oplus e_n$, 这里, e_n 被 α_n 和 d_n 由 $\delta(e_n)\oplus e_n=\delta^3(\alpha_n)\oplus\delta^2(d_n)\oplus d_n$ 唯一确定.如果 $\forall n\geqslant 1$, 均有 $\delta(d_n)\oplus d_n\neq\delta^2(\alpha_n)\oplus\alpha_n$, 则下述概率非零的 Lai-Massey 模型差分传递链

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\delta(\alpha)\oplus d_1),\alpha\oplus d_1)\to(\alpha\oplus d_1\oplus e_1,\alpha\oplus d_1\oplus e_1)\to\ldots$$
$$\to(\alpha_k,\alpha_k)\to(\delta(\alpha_k),\alpha_k)\to(\delta(\delta(\alpha_k)\oplus d_k),\alpha_k\oplus d_k)\to(\alpha_{k+1},\alpha_{k+1})\to\ldots$$

的前 $3n$ 轮和前 $3n+1$ 轮中活动 F 函数的个数均为 $2n$, 前 $3n+2$ 轮中活动 F 函数的个数为 $2n+1$, 且该链的第 $3n-2,3n-1,3n$ 圈 F 函数的差分对应依次为 $0\to 0,\delta(\alpha_n)\oplus\alpha_n\to d_n,\delta(\delta(\alpha_n)\oplus d_n)\oplus\alpha_n\oplus d_n\to e_n$.

证明:当 $\delta(d_n)\oplus d_n\neq\delta^2(\alpha_n)\oplus\alpha_n$ 时,即定理中的差分传递链中第 $3n$ 圈 F 函数是活动的.下面考察第 $3n-1$ 圈 F 函数是否活动,假设第 $3n-1$ 圈 F 函数不活动,即 $\delta(\alpha_n)\oplus\alpha_n=d_n=0$. 由 σ 为正形置换可得 $\alpha_n=d_n=0$, 这与 $\delta(d_n)\oplus d_n\neq\delta^2(\alpha_n)\oplus\alpha_n$ 矛盾,故 $\alpha_n\neq 0$, 第 $3n-1$ 圈 F 函数活动.由此可得,在 $\delta(d_n)\oplus d_n\neq\delta^2(\alpha_n)\oplus\alpha_n$ 时,定理中的差分传递链的第 $3n,3n-1$ 圈的 F 函数均是活动的.

下面利用归纳法证明本结论.当 $n=1$ 时,由引理 4 可知,该链的前 3 轮的活动 F 函数个数为 2,且第 3 轮圈函数的输出差为 (α_2,α_2). 假设该定理在 $n=m$ 时成立,则其第 $3m$ 轮圈函数的输出差为 $(\alpha_{m+1},\alpha_{m+1})$, 且其前 $3m$ 轮中共有 $2m$ 个活动 F 函数.由引理 4 可知,3 轮差分传递链

$$(\alpha_m,\alpha_m)\to(\delta(\alpha_m),\alpha_m)\to(\delta(\delta(\alpha_m)\oplus d_m),\alpha_m\oplus d_m)\to(\alpha_{m+1},\alpha_{m+1})$$

对应的 F 函数的差分对应依次为 $0\to 0,\delta(\alpha_m)\oplus\alpha_m\to d_m,\delta(\delta(\alpha_m)\oplus d_m)\oplus\alpha_m\oplus d_m\to e_m$. 其中,

$$\alpha_{m+1}=\alpha_m\oplus d_m\oplus e_m \text{ 且 } \delta(e_m)\oplus e_m=\delta^3(\alpha_m)\oplus\delta^2(d_m)\oplus d_m,$$

将该 3 轮差分传递链与归纳假设的 $3m$ 轮差分传递链链接,则可得其前 $3m+1$ 轮、$3m+2$ 轮和 $3m+3$ 轮中活动 F 函数的个数分别为 $2m,2m$ 和 $2m+1$, 这说明当 $n=m+1$ 时本定理成立,故由归纳法知该定理成立. □

特别地,若 $\forall n\geqslant 1,\delta(d_n)\oplus d_n=\delta^2(\alpha_n)$, 那么定理 6 中所给出的概率非零的差分传递链是一条周期为 3 的链,且其结构为

$$(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\delta(\alpha)\oplus d),\alpha\oplus d)\to(\alpha,\alpha)\to\ldots$$
$$\to(\alpha,\alpha)\to(\delta(\alpha),\alpha)\to(\delta(\delta(\alpha)\oplus d),\alpha\oplus d)\to(\alpha,\alpha)\to\ldots$$

3 Lai-Massey 模型 *n* 轮组合传递链中活动 *F* 函数的下确界

我们首先给出 Lai-Massey 模型圈函数 Q_k 的线性逼近与其 F 函数和 σ 函数的线性逼近之间的关系.

定理 7. 设 $\sigma(x)=Mx\oplus C$ 是仿射变换,则 Lai-Massey 模型圈函数 Q_k 的线性逼近 $(\alpha,\beta)\to(A,B)$ 的相关系数是非零 ρ 的充要条件是 $\alpha\oplus\beta\oplus B\oplus M^TA=0$, 且对应的 F 函数的线性逼近 $\beta\oplus B\to\alpha\oplus\beta$ 的相关系数是 $\rho\times(-1)^{A\cdot C}$, 其中, M^T 是矩阵 M 的转置.

证明:设 $(\alpha,\beta)\to(A,B)$ 是 Lai-Massey 模型圈函数 Q_k 的一个相关系数为 ρ 的线性逼近,且 $\rho\neq 0$. 再设 (x_1,x_2) 为 Lai-Massey 模型的输入,令 $x=x_1,y=x_1\oplus x_2$, 则有

$$\begin{aligned}&(A,B)\cdot Q_k(x_1,x_2)\oplus(\alpha,\beta)\cdot(x_1,x_2)\\&=A\cdot\sigma(F(x_1\oplus x_2)\oplus x_1)\oplus B\cdot(F(x_1\oplus x_2)\oplus x_2)\oplus\alpha\cdot x_1\oplus\beta\cdot x_2\\&=\alpha\cdot x\oplus A\cdot\sigma(x)\oplus(\beta\oplus B)\cdot(x\oplus y)\oplus A\cdot\sigma(F(y))\oplus B\cdot F(y)\oplus A\cdot C\\&=(\alpha\oplus\beta\oplus B)\cdot x\oplus A\cdot\sigma(x)\oplus(\beta\oplus B)\cdot y\oplus A\cdot\sigma(F(y))\oplus B\cdot F(y)\oplus A\cdot C.\end{aligned}$$

将上式中所有变量均看作列向量,则将 $\sigma(x)=Mx\oplus C$ 代入,可将上式等价地表示为

$$
\begin{aligned}
&(\alpha\oplus\beta\oplus B)\cdot x\oplus A\cdot Mx\oplus A\cdot C\oplus(\beta\oplus B)\cdot y\oplus A\cdot MF(y)\oplus B\cdot F(y)\oplus A\cdot C\oplus A\cdot C\\
&=(\alpha\oplus\beta\oplus B)^T x\oplus A^T Mx\oplus(\beta\oplus B)^T y\oplus A^T MF(y)\oplus B^T F(y)\oplus A\cdot C\\
&=[(\alpha\oplus\beta\oplus B)^T\oplus A^T M]x\oplus(A^T M\oplus B^T)F(y)\oplus(\beta\oplus B)^T y\oplus A\cdot C\\
&=(\alpha\oplus\beta\oplus B\oplus M^T A)\cdot x\oplus(M^T A\oplus B)\cdot F(y)\oplus(\beta\oplus B)\cdot y\oplus A\cdot C.
\end{aligned}
$$

于是,有

$$
\begin{aligned}
&\sum_{x_1,x_2}(-1)^{(A,B)\cdot Q_k(x_1,x_2)\oplus(\alpha,\beta)\cdot(x_1,x_2)}=\sum_{x,y}(-1)^{(\alpha\oplus\beta\oplus B\oplus M^T A)\cdot x\oplus(M^T A\oplus B)\cdot F(y)\oplus(\beta\oplus B)\cdot y\oplus A\cdot C}\\
&=\left[\sum_x(-1)^{(\alpha\oplus\beta\oplus B\oplus M^T A)\cdot x}\right]\left[\sum_y(-1)^{(M^T A\oplus B)\cdot F(y)\oplus(\beta\oplus B)\cdot y\oplus A\cdot C}\right].
\end{aligned}
$$

因此,若 $\alpha\oplus\beta\oplus B\oplus M^T A\neq 0$, 则有 $\sum_x(-1)^{(\alpha\oplus\beta\oplus B\oplus M^T A)\cdot x}=0$. 由于 x,y 是两个独立的变量,因而

$$\sum_{x_1,x_2}(-1)^{(A,B)\cdot Q_k(x_1,x_2)\oplus(\alpha,\beta)\cdot(x_1,x_2)}=0,$$

这与 $\rho\neq 0$ 矛盾.该矛盾说明 $\alpha\oplus\beta\oplus B\oplus M^T A\neq 0$. 此时,

$$
\begin{aligned}
W_{(Q_k)}((\alpha,\beta)\to(A,B))&=W_{(F)}(\beta\oplus B\to M^T A\oplus B)\times(-1)^{A\cdot C}\\
&=W_{(F)}(\beta\oplus B\to\alpha\oplus\beta)\times(-1)^{A\cdot C}.
\end{aligned}
$$

□

引理 6. 设 $\sigma(x)=Mx\oplus C$, 则有:

(1) σ 是正形置换的充要条件是 σ_D 是正形置换;

(2) 如果 $M^k=E$ 的充要条件是 $((M^{-1})^T)^k=E$, 这里 E 是单位矩阵.

证明:(1) 由 σ 是正形置换知 $M\oplus E$ 是可逆矩阵,因而 $Mx=x$ 只有零解,从而 $M^{-1}x=x$ 只有零解,故 $y(M^{-1})^T=y$ 只有零解,这说明 $(M^{-1})^T\oplus E$ 是可逆矩阵,因而 σ_D 是正形置换.

(2) 由 $((M^{-1})^T)^k=((M^{-1})^k)^T=((M^k)^{-1})^T=(E^{-1})^T=E$ 即可得知.

由引理 6 可知,当 σ 是仿射正形置换时, σ_D 也为正形置换,且这两个置换的周期相等.

引理 7. 设仿射变换 σ 是双射,则 Lai-Massey 模型圈函数的概率非零的差分对应 $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ 中 F 函数的差分对应为 $\alpha_0\oplus\alpha_1\to c$ 的充要条件是其对偶模型的相关系数非零的线性逼近 $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ 中 F 函数的线性逼近为 $c\to\alpha_0\oplus\alpha_1$.

证明:由定理 1 可知,圈函数的概率非零的差分对应为 $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ 等价于其 F 函数的差分对应为 $\alpha_0\oplus\alpha_1\to\alpha_1\oplus\beta_1$ 且 $\alpha_0\oplus\alpha_1\oplus\beta_1=M^{-1}\beta_0$.

再由定理 7 可知,相关系数非零的线性逼近 $(\alpha_0,\alpha_1)\to(\beta_0,\beta_1)$ 是其对偶 Lai-Massey 模型的圈函数的线性逼近等价于 F 函数的线性逼近为 $\alpha_1\oplus\beta_1\to\alpha_0\oplus\alpha_1$ 且 $\alpha_0\oplus\alpha_1\oplus\beta_1\oplus((M^{-1})^T)^T\beta_0=0$, 即 $\alpha_0\oplus\alpha_1\oplus\beta_1=M^{-1}\beta_0$, 这说明本定理成立. □

在 Feistel 模型中,它的差分传递链和组合传递链的结构之间存在对偶关系,故其线性可证明安全性可由差分可证明安全性直接得到.基于引理 7,我们考察在 Lai-Massey 模型中,其差分传递链和组合传递链之间是否也存在类似的对偶关系.

定理 8(Lai-Massey 模型中组合传递链与差分传递链的对偶定理).设仿射变换 σ 是双射,则 Lai-Massey 模型的概率非 0 的 n 轮差分传递链 $(a_{0,1},a_{0,2})\to(a_{1,1},a_{1,2})\to\ldots\to(a_{n,1},a_{n,2})$ 中 F 函数的差分对应依次为 $a_{0,1}\oplus a_{0,2}\to c_0, a_{1,1}\oplus a_{1,2}\to c_1,\ldots,a_{n-1,1}\oplus a_{n-1,2}\to c_{n-1}$ 的充要条件是相关系数非 0 的 n 轮传递链

$$(a_{0,1},a_{0,2})\to(a_{1,1},a_{1,2})\to\ldots\to(a_{n,1},a_{n,2})$$

是其对偶模型的 n 圈组合传递链,且相应 F 函数的线性逼近依次为

$$c_0\to a_{0,1}\oplus a_{0,2}, c_1\to a_{1,1}\oplus a_{1,2},\ldots,c_{n-1}\to a_{n-1,1}\oplus a_{n-1,2}.$$

证明:利用引理 7 结合归纳假设法可直接证明该定理. □

定理 8 说明 Lai-Massey 模型的差分传递链和它的对偶模型的组合传递链在结构上是对偶的,该对偶性是一个模型到另一个模型的对偶,故可以保持活动 F 函数的个数不变.基于该对偶定理,可由差分传递链的相关结论直接得到有关组合传递链的结论,如定理 9 所示.

定理 9. 设 σ 是仿射正形置换,则 Lai-Massey 模型相关系数非 0 的 t 轮非平凡组合传递链中活动 F 函数的个数 $\geqslant \lfloor t/2 \rfloor$.

定理 10. 设 $\sigma(x)=Mx\oplus C$ 为仿射正形置换, $W=(M^{-1})^T, \alpha\neq 0$, 则下述相关系数非 0 的 $2n$ 轮组合传递链是 Lai-Massey 模型的一条活动 F 函数个数为 n 的非平凡组合传递链:

$$(\alpha,\alpha)\to(W\alpha,\alpha)\to(W\alpha,W\alpha)\to(W^2\alpha,W\alpha)\to(W^2\alpha,W^2\alpha)$$
$$\to\ldots\to(W^{n-1}\alpha,W^{n-1}\alpha)\to(W^n(\alpha),W^{n-1}\alpha)\to(W^n(\alpha),W^n(\alpha)),$$

且奇数轮 F 函数的线性逼近为 $0\to 0, 2t$ 轮 F 函数的线性逼近为 $W^t\alpha\oplus W^{t-1}\alpha\to W^t\alpha\oplus W^{t-1}\alpha$.

定理 11. 设 $\sigma(x)=Mx\oplus C$ 为仿射正形置换, $W=(M^{-1})^T, r\geqslant 3$. 如果 F 函数是正形置换,则 Lai-Massey 模型相关系数非 0 的 r 轮组合传递链中活动 F 函数的个数至少为 $L^{(r)}$, 其中 $L^{(r)}$ 为

$$L^{(r)}=\begin{cases}2n, & \text{若 } r=3n,3n+1\\ 2n+1, & \text{若 } r=3n+2\end{cases}.$$

定理 12. 设 $\sigma(x)=Mx\oplus C$ 为仿射正形置换, $W=(M^{-1})^T$. 又设 $\alpha_1=\alpha$, 且对于任意 $n\geqslant 1$, 都有 $\alpha_{n+1}=\alpha_n\oplus d_n\oplus e_n$, 这里 e_n 被 α_n 和 d_n 由 $We_n\oplus e_n=W^3\alpha_n\oplus W^2d_n\oplus d_n$ 唯一确定.如果 $\forall n\geqslant 1$, 均有 $Wd_n\oplus d_n\neq W^2\alpha_n\oplus\alpha_n$, 则下述 Lai-Massey 模型相关系数非 0 的组合传递链

$$(\alpha,\alpha)\to(W\alpha,\alpha)\to(W^2\alpha\oplus Wd_1,\alpha\oplus d_1)\to(\alpha\oplus d_1\oplus e_1,\alpha\oplus d_1\oplus e_1)\to\ldots$$
$$\to(\alpha_k,\alpha_k)\to(W\alpha_k,\alpha_k)\to(W^2\alpha_k\oplus Wd_k,\alpha_k\oplus d_k)\to(\alpha_{k+1},\alpha_{k+1})\to\ldots$$

的前 $3n$ 轮和前 $3n+1$ 轮中活动 F 函数的个数为 $2n$, 前 $3n+2$ 轮中活动 F 函数的个数为 $2n+1$, 且该组合传递链中第 $3n-2, 3n-1, 3n$ 圈 F 函数的线性逼近依次为 $0\to 0, d_n\to W\alpha_n\oplus\alpha_n, e_n\to W^2\alpha_n\oplus Wd_n\oplus\alpha_n\oplus d_n$.

4 结束语

自从 Lai-Massey 模型和 FOX 算法提出以来,学者们已经对它们做了多种攻击.但是在其差分(组合)传递链中活动 F 函数个数的下界方面,除了设计者给出的 FOX 算法两轮中至少有 1 个活动的 F 函数之外,则没有其他的结论,而活动 F 函数个数的下界则是影响差分特征(线性逼近)概率上界的重要工具.本文给出了 Lai-Massey 模型的差分(线性)活动 F 函数个数的下界,并通过引入对偶模型得到了在 Lai-Massey 模型中,其差分传递链和组合传递链在结构上是对偶的.该对偶性可以简化 Lai-Massey 模型线性可证明安全性的证明过程.此外,本文指出,在 F 函数是正形置换时,其活动 F 函数个数的下确界与 Feistel 模型的下确界相同.本文的结果进一步丰富了 Lai-Massey 模型的分析理论,从而为基于该模型设计的密码算法的安全性提供了理论支撑.

References:

[1] Lai X, Massey J. A p6roposal for a new block encryption standard. In: Advances in Cryptology—EUROCRYPT'90. LNCS 473, 1990. 389−404.

[2] Vaudenay S. On the Lai-Massey scheme. In: Advances in Cryptology-ASIACRYPT'99. LNCS 1716, 1999. 8−19.

[3] Luo YY, Lai XJ, Gong Z. Pseudorandomness analysis of the (extended) Lai-Massey scheme. Information Processing Letters, 2010, 111(2):90−96.

[4] Junod P, Vaudenay S. FOX: A new family of block ciphers. In: Selected Areas in Cryptography—SAC. LNCS 259, 2004. 131−146.

[5] Wu WL, Zhang WT, Feng DG. Improved integral cryptanalysis of reduced FOX block cipher. In: Information Security and Cryptology—ICISC. LNCS 3935, 2005. 229−241.

[6] Wu ZM, Lai XJ, Zhu B, Luo YY. Impossible differential cryptanalysis of FOX. 2009. http://eprint.iacr.org/2009/357

[7] Wei YC, Sun B, Li C. Impossible differential attacks on FOX. Journal on Communications, 2010,31(9):24−29 (in Chinese with English abstract).

[8] Wu WL, Wei HR. Collision-Integral attack of reduced-round FOX. Journal of Electronics & Information Technology, 2005,33(7): 1307−1310 (in Chinese with English abstract).

[9] Li RL, You JX, Sun B, Li C. Fault analysis study of the block cipher FOX64. Multimedia Tools and Applications, 2013,63(3): 691−708.

[10] Yun A, Park JH, Lee J. On Lai-Massey and quasi-Feistel ciphers. Design Codes and Cryptography, 2011,58:45−72.

[11] Luby M, Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing, 1988,17(2),373−386.

[12] Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991,14(1):3−72.

[13] Matsui M. Linear cryptanalysis method for DES cipher. In: Advances in Cryptology—Eurocrypt'93. LNCS 3788, 1993. 386−397.

[14] Jin CH, Zheng HR, Zhang SW, Hu B, Shi JH. Cryptology. Beijing: Higher Education Press, 2009. 11 (in Chinese).

附中文参考文献:

[7] 魏悦川,孙兵,李超.FOX 密码的不可能差分分析.通信学报,2010,31(9):24−29.

[8] 吴文玲,卫宏儒.低圈 FOX 分组密码的碰撞-积分攻击.电子与信息学报,2005,33(7):1307−1310.

[14] 金晨辉,郑浩然,张少武,胡斌,史建红.密码学.北京:高等教育出版社,2009. 11.

付立仕(1989－),女,河南南阳人,硕士,主要研究领域为分组密码算法设计与分析.
E-mail: 15036018167@163.com

金晨辉(1965－),男,博士,教授,博士生导师,主要研究领域为密码算法设计与分析.
E-mail: jinchenhui@126.com