基于仿射非正型σ变换的 Lai-Massey 模型的密码学缺陷

付立仕* 金晨辉
(解放军信息工程大学 郑州 450004)

摘 要：Vaudenay(1999)从伪随机性的角度出发，证明了 Lai-Massey 模型中的σ 变换应设计为正型置换或几乎正型置换。该文从抗差分攻击和线性攻击的角度重新考察了 Lai-Massey 模型双射σ 的设计问题。证明了基于任意有限交换群设计的 Lai-Massey 模型，如果σ 变换设计为该群上的仿射变换，则必须为正型置换，否则该算法将分别存在概率为 1 的差分对应和线性逼近，结论表明仿射的几乎正型置换并不适用于 Lai-Massey 模型的设计。此外，该文借助有限群的特征标引入了一种新的线性逼近方式，收集和刻画了一般有限交换群上 Lai-Massey 模型输入和输出的线性逼近关系。

关键词：密码学；有限交换群；差分分析；线性分析；Lai-Massey 模型；正型置换
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2013)10-2536-05
DOI: 10.3724/SP.J.1146.2012.01574

The Cryptographic Weakness of Lai-Massey Scheme with an Affine but not Orthomorphic Bijection σ

Fu Li-shi Jin Chen-hui
(*The Information Engineering University of PLA*, *Zhengzhou* 450004, *China*)

Abstract: Vaudenay (1999) proved that the permutation σ in Lai-Massey scheme should be an orthomorphism or almost orthomorphism. This paper mainly focuses on the principle of the function σ in Lai-Massey scheme, which is described by its resistance to differential and linear attack. It shows that no matter how the group G is defined, if σ is an affine function on G, then it should be defined as an orthomorphism, or else there exists a differentially characteristic with probability 1 and a linearly approximation with correlation coefficient 1, therefore it has potential security risk. Moreover, by the characteristic spectrum in finite group, a new linear relationship between the input and output of Lai-Massey scheme is introduced, which is used to describe the linear relationship lying between the input and the output of Lai-Massey scheme.

Key words: Cryptography; Finite a-bel group; Differentially cryptanalysis; Linearly cryptanalysis; Lai-Massey scheme; Orthomorphism

1 引言

IDEA算法[1]采用了与Feistel模型、广义Feistel模型、SP网络以及它们的各种组合变型都不相同的模型。在IDEA算法中，对合变换$G_k:(x,y)\rightarrow(x\oplus f_k(x\oplus y),y\oplus f_k(x\oplus y))$是其核心模块，但是该模块最大的信息泄漏是输入和输出的左右块的模2和保持不变。为克服该缺点，IDEA算法在G_k变换之前增加了一层群运算。1999年，Vaudenay等人[2]研究了IDEA算法模型的一般化问题，提出了Lai-Massey模型，其圈函数是$Q_k:(x,y)\rightarrow(\sigma(x+F_k(x-y)),y+F_k(x-y))$，这里+是某个群运算，该模型具有扩散速度快等优势[3,4]，且自从该整体结构提出至今，人们尚未发现该结构的明显的漏洞。此外，利用Lai-Massey结构，文献[5,6]设计了FOX系列分组密码算法(即IDEA-NXT)。在对FOX算法的安全性分析方面，国内外的学者们给出了很多精彩的结果：吴文玲等人分析了4-7轮FOX算法抗积分攻击[7]和碰撞-积分攻击[8]的能力、文献[9]利用FOX算法的4轮不可能差分给出了对5-7轮FOX64以及5轮FOX128的攻击、文献[10]给出了改进的不可能差分分析，文献[11]则分析了FOX算法抗差错攻击的能力。最近，文献[12]给出了对5-7轮FOX64以及5轮FOX128的差分碰撞攻击。上述的结果表明，在传统分析方法下，FOX系列算法展现了充分的安全性冗余。由此可得Lai-Massey模型是一类安全性较高的密码模型，值得进一步深入研究。

Lai-Massey 结构最大的设计亮点在于其中的σ

2012-12-04 收到，2013-02-22 改回
国家自然科学基金(61272488)资助课题
*通信作者：付立仕 fulishil123@sohu.com

变换，该变换的引入大大降低了该结构的设计难度和分析难度。文献[4]指出双射 σ 的使用能够有效增强 Lai-Massey 结构抵抗区分攻击的能力。Vaudenay 等人[2]则证明了，如果双射 σ 是正型置换(即双射 σ 使 $\sigma(x)-x$ 仍是双射)或 α 几乎正型置换(使 $\sigma(x)-x$ 至多只有 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 设计为正型置换或几乎正型置换。特别地，由于不是任意群上都存在正型置换，Vaudenay 指出，此时可以利用几乎正型置换设计双射 σ，从而推广了 Lai-Massey 模型的应用范围。

Vaudenay 是从伪随机性的角度出发，得出应将 σ 设计成为正型置换或几乎正型置换的结论，但并没有从其它方面对该结论进行分析。本文将从抗差分攻击和抗线性逼近攻击的角度出发，研究 Lai-Massey 模型的双射 σ 的设计。本文证明了无论 Lai-Massey 结构上的群运算如何定义，如果将 σ 变换设计为该群上的仿射变换，则必须将其设计为该群上的正型置换，否则加密算法将存在概率为 1 的差分对应和概率为 1 的线性逼近，因而具有安全缺陷，从而说明仿射的几乎正型置换不适用于 σ 变换的设计。其中，在考察线性逼近时，我们借助了有限群的特征标 $\chi_\alpha(x)$ 和 $\chi_\beta(g(x))$ 之间的关系来收集和刻画输入 x 的“ α 组合 ”和输出 $g(x)$ 的“ β 组合 ”之间的关系，给出了 Lai-Massey 模型在一般有限交换群上时其输入和输出的线性逼近关系。

2　基于仿射非正型 σ 变换的 Lai-Massey 模型的差分信息泄漏分析

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 模型的加解密的相似性，最后一圈的圈函数一般设置为 $Q_k(x,y)=(x+F_k(x-y),y+F_k(x-y))$。但是，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，并将最后一圈的圈函数也按 $Q_k(x,y)=(\sigma(x+F_k(x-y)),y+F_k(x-y))$ 对待。这种处理并不影响本文结果的适用性。

定义 2　设 $(G,+)$ 是交换群，$f:G\to G$，$\alpha\in G$，$\beta\in G$，则称 $p_f(\alpha\to\beta)=(1/|G|)\#\{x\in G:f(x+\alpha)-f(x)=\beta\}$ 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。

我们首先分析 Lai-Massey 模型圈函数的形如 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的差分对应的概率。

定理 1　Lai-Massey 模型圈函数 Q_k 的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的差分转移概率为 $p_\sigma(\alpha\to\alpha)$。

证明　设 Lai-Massey 模型的两个输入分别为 $(x+\alpha,y+\alpha)$ 和 (x,y)，其中 $F:G\to G$，$\sigma:G\to G$，$Q_k:G^2\to G^2$，则 F 函数对应的两个输出均为 $F_k(x-y)$，因而圈函数 Q_k 的两个输出的差为

$$\begin{aligned}&Q_k(x+\alpha,y+\alpha)-Q_k(x,y)\\&=(\sigma(x+\alpha+F_k(x-y)),y+\alpha+F_k(x-y))\\&\quad-(\sigma(x+F_k(x-y)),y+F_k(x-y))\\&=(\sigma(x+\alpha+F_k(x-y))-\sigma(x+F_k(x-y)),\alpha)\end{aligned}$$

从而由定义知 Lai-Massey 模型圈函数 Q_k 的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的差分转移概率为

$$\begin{aligned}&\frac{1}{|G|^2}\#\left\{(x,y):Q_k(x+\alpha,y+\alpha)-Q_k(x,y)=(\alpha,\alpha)\right\}\\&=\frac{1}{|G|^2}\#\{(x,y):(\sigma(x+\alpha+F_k(x-y))\\&\quad-\sigma(x+F_k(x-y)),\alpha)=(\alpha,\alpha)\}\\&=\frac{1}{|G|^2}\#\{(x,y):\sigma(x+\alpha+F_k(x-y))\\&\quad-\sigma(x+F_k(x-y))=\alpha\}\end{aligned}$$

记 $x-y\triangleq z$，则有

$$\begin{aligned}&\frac{1}{|G|^2}\#\{(x,y):\sigma(x+\alpha+F_k(x-y))\\&\qquad-\sigma(x+F_k(x-y))=\alpha\}\\&=\frac{1}{|G|^2}\#\left\{(x,z):\sigma(x+\alpha+F_k(z))-\sigma(x+F_k(z))=\alpha\right\}\\&=\frac{1}{|G|^2}\sum_z\#\left\{x:\sigma(x+\alpha+F_k(z))-\sigma(x+F_k(z))=\alpha\right\}\end{aligned}$$

记 $x+F_k(z)\triangleq t$，则有

$$\begin{aligned}&\frac{1}{|G|^2}\sum_z\#\{x:\sigma(x+\alpha+F_k(z))-\sigma(x+F_k(z))=\alpha\}\\&=\frac{1}{|G|^2}\sum_z\#\{t:\sigma(t+\alpha)-\sigma(t)=\alpha\}\\&=\frac{1}{|G|^2}\times|G|\#\{t:\sigma(t+\alpha)-\sigma(t)=\alpha\}\\&=\frac{1}{|G|}\#\{t:\sigma(t+\alpha)-\sigma(t)=\alpha\}\end{aligned}$$

由于 $(1/|G|)\#\{t:\sigma(t+\alpha)-\sigma(t)=\alpha\}$ 为 σ 的差分对应 $\alpha\to\alpha$ 的差分转移概率，即 $p_\sigma(\alpha\to\alpha)$。故 Lai-Massey 模型的圈函数 Q_k 的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的差分转移概率为 $p_\sigma(\alpha\to\alpha)$。　　证毕

定义 3　设 $(\alpha_i,\beta_i)\to(\alpha_{i+1},\beta_{i+1})$ 是第 i 圈圈函数的差分对应，则称 $(\alpha_1,\beta_1)\to(\alpha_2,\beta_2)\to\cdots\to(\alpha_{r+1},$

$\beta_{r+1})$ 为 r 圈 Lai-Massey 模型的一条起点为 (α_1,β_1) 终点为 $(\alpha_{r+1},\beta_{r+1})$ 的差分路径，并称 $\prod_{i=1}^{r} p_{Q_{k_i}}\cdot((\alpha_i,\beta_i)\to(\alpha_{i+1},\beta_{i+1}))$ 为该差分路径的概率。

由定理 1 和定义 3 即得：

定理 2 r 圈 Lai-Massey 模型的差分路径 $(\alpha,\alpha)\to(\alpha,\alpha)\to\cdots\to(\alpha,\alpha)$ 的概率为 $[p_\sigma(\alpha\to\alpha)]^r$。

备注 1 当 Lai-Massey 模型构成 Markov 密码时，r 圈 Lai-Massey 模型的差分对应 $(\alpha_1,\beta_1)\to(\alpha_{r+1},\beta_{r+1})$ 的概率就是所有起点为 (α_1,β_1)、终点为 $(\alpha_{r+1},\beta_{r+1})$ 的差分路径的概率之和。由于我们无法计算出所有差分路径的概率，因而在实际分析中，我们通常设法构造出一条高概率的差分路径，再用该差分路径的概率近似为 r 圈 Lai-Massey 模型的差分概率。因此，定理 2 说明，如果 Lai-Massey 模型构成 Markov 密码，则 r 圈 Lai-Massey 模型的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的概率 $\geq[p_\sigma(\alpha\to\alpha)]^r$。当 $[p_\sigma(\alpha\to\alpha)]^r$ 较大时，就会造成严重的差分信息泄漏。

下面证明，当 σ 是群 $(\{0,1\}^n,+)$ 上的仿射函数但不是正型置换时，一定存在非零的 α，使得 r 圈 Lai-Massey 模型的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的概率是 1。因此，如果将 σ 设计为群 $(\{0,1\}^n,+)$ 上的仿射函数，则必须将之设计为正型置换，而不能被设计为几乎正型置换。

定义 4 设 δ 是交换群 $(\{0,1\}^n,+)$ 到自身的同态，$c\in\{0,1\}^n$，则称函数 $\sigma(x)=\delta(x)+c$ 为群 $(\{0,1\}^n,+)$ 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 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 $(G,+)$ 上的正型置换。

引理 1 设 $f:G\to G$ 是双射，则 f 是群 $(G,+)$ 上的正型置换等价于 $\forall\alpha\neq0$，都有 $p_f(\alpha\to\alpha)=0$。

证明 记 $g(x)=f(x)-x$，则 f 是群 $(G,+)$ 上的正型置换等价于 g 是双射，即对 $\forall\alpha\neq0$ 和 $\forall x\in G$，都有 $g(x+\alpha)-g(x)=0$，这等价于 $\forall\alpha\neq0$，均有 $p_g(\alpha\to0)=0$，从而由 $p_g(\alpha\to0)=p_f(\alpha\to\alpha)$ 知引理 1 成立。

定理 3 设 σ 是交换群 $(G,+)$ 上的仿射函数且不是正型置换，则存在 $\alpha\neq0$，使得 r 圈 Lai-Massey 模型的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的概率为 1。

证明 设 σ 是仿射函数但不是正型置换，则由引理 1 知，存在 $\alpha\neq0$，使得 $p_\sigma(\alpha\to\alpha)\neq0$，故由 σ 为仿射函数知 $p_\sigma(\alpha\to\alpha)=1$。再设 $(x_L^{(i)},x_R^{(i)})$ 和 $(x_L^{(i+1)},x_R^{(i+1)})$ 分别是第 i 圈圈函数的输入和输出，则由定理 1 和 $p_\sigma(\alpha\to\alpha)=1$ 知，第 i 圈圈函数的输入 $(x_L^{(i)}+\alpha,x_R^{(i)}+\alpha)$ 对应的输出一定是 $(x_L^{(i+1)}+\alpha,x_R^{(i+1)}+\alpha)$，从而由归纳法可证，当第 1 圈的输入差是 (α,α) 时，第 r 圈 Lai-Massey 模型的输出差也一定是 (α,α)，这说明 r 圈 Lai-Massey 模型的差分对应 $(\alpha,\alpha)\to(\alpha,\alpha)$ 的概率为 1。 证毕

3 基于仿射非正型 $\boldsymbol{\sigma}$ 变换的 Lai-Massey 模型的线性信息泄漏分析

为适应 Lai-Massey 模型中的群 $(\{0,1\}^n,+)$ 的加法未必是逐位模 2 加 $\oplus$ 这一情形，我们需要针对群运算 $+$ 发展一种新的线性逼近，并证明当 σ 是仿射函数但不是正型置换时，该线性逼近对 Lai-Massey 模型非常有效。为此，我们记 $(\{0,1\}^n,+)=(G^m,+)$，从而将 Lai-Massey 模型看作 $G^m\times G^m$ 到自身的双射。特别地，如果 $G=\{0,1\}$ 是二元域，则群 $(G^m,+)$ 上的加法就是逐位模 2 加；如果 $n=mt$ 且 $G=Z/(2^t)$ 是模 2^t 剩余类群，则群 $(G^m,+)$ 上的加法就是逐块模 2^t 加。因此，Lai-Massey 模型中的群运算以常见的逐位模 2 加和逐块模 2^t 加为特例。

下面以有限交换群 $(G^m,+)$ 至复数域的乘法群 C^* 上的同态为工具，收集群 $(G^m,+)$ 的线性信息。

由文献[13]知，有限交换群 $(G,+)$ 至复数域的乘法群 C^* 上的所有同态构成的集合为 $\{\chi_\alpha(x):\alpha\in G\}$，且有 $\chi_{-\alpha}(x)=\chi_\alpha(-x)$。在群论中，$\chi_\alpha(x)$ 称为群 $(G,+)$ 的一个特征标。

当 $\boldsymbol{\alpha}=(\alpha_1,\cdots,\alpha_m)\in G^m$ 和 $\boldsymbol{x}=(x_1,\cdots,x_m)\in G^m$，有 $\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})=\prod_{i=1}^{m}\chi_{\alpha_i}(x_i)$，其中 χ_{α_i} 是有限交换群 $(G,+)$ 至复数域的乘法群 C^* 上的同态。

特别地，当 $(G^m,+)$ 是 $(\{0,1\}^n,\oplus)$ 时，$\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})=(-1)^{\boldsymbol{\alpha}\cdot\boldsymbol{x}}=(-1)^{\overset{n}{\underset{i=1}{\oplus}}\alpha_i x_i}$；当 $n=mt$ 且 $G=Z/(2^t)$ 是模 2^t 剩余类群时，$\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})=e^{\frac{2\pi\sqrt{-1}}{2^t}\boldsymbol{\alpha}\cdot\boldsymbol{x}}=e^{\frac{2\pi\sqrt{-1}}{2^t}\sum_{i=1}^{m}\alpha_i x_i \bmod 2^t}$。一般地，根据有限生成交换群的结构定理，存在 $m_1,m_2,\cdots,m_n$，使得群 G 同构于群 $\prod_{i=1}^{n}Z/(m_i)$ [12]，因而有 $\chi_\alpha(\boldsymbol{x})=e^{\sum_{j=1}^{n}\frac{2\pi\sqrt{-1}}{m_j}[\alpha_j x_j \bmod mj]}$，这里 $(\alpha_1,\cdots,\alpha_n)$ 和 $(x_1,\cdots,x_n)$ 分别是 $\boldsymbol{\alpha}$ 和 $\boldsymbol{x}$ 在 G 至 $\prod_{i=1}^{n}Z/(m_i)$ 的同构映射下的像。

以下用 $\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})$ 表示输入 $\boldsymbol{x}$ 的“$\boldsymbol{\alpha}$ 组合信息”，用 $\chi_{\boldsymbol{\beta}}(g(\boldsymbol{x}))$ 表示输出 $\boldsymbol{g}(\boldsymbol{x})$ 的“$\boldsymbol{\beta}$ 组合信息”，此时 $\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})$ 与 $\chi_{\boldsymbol{\beta}}(g(\boldsymbol{x}))$ 之间的关系反映了利用 $g(\boldsymbol{x})$ 的线性组合 $\chi_{\boldsymbol{\beta}}(g(\boldsymbol{x}))$ 获得的 $\boldsymbol{x}$ 的线性组合 $\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})$ 的信息泄露。接下来我们将证明，当 σ 是群 $(G^m,+)$ 上的仿射函数但不是正型置换时，对于 Lai-Massey 模型的加密算法

$E_k(x)$，存在非零的 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$，使得 $\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})$ 与 $\chi_{\boldsymbol{\beta}}(E_k(\boldsymbol{x}))$ 之间存在概率为 1 的等式关系。

定理 4　设 Lai-Massey 模型中的群是 $(G^m,+)$，$\sigma(\boldsymbol{x})=\delta(\boldsymbol{x})+\boldsymbol{c}$ 是群 $(G^m,+)$ 上的仿射变换。又设 $\boldsymbol{\alpha}\in G^m$ 使得 $\forall \boldsymbol{x}\in G^m$，都有 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})=1$，则有 $\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(Q_k(\boldsymbol{x},\boldsymbol{y}))=\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\boldsymbol{x},\boldsymbol{y})\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})$。

证明　由于 $\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})$ 是定义在复数域的乘法群 C^* 上，则 $\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(Q_k(\boldsymbol{x},\boldsymbol{y}))\div\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\boldsymbol{x},\boldsymbol{y})$ 代表了 $Q_k(\boldsymbol{x},\boldsymbol{y})$ 的输出组合 $(\boldsymbol{\alpha},-\boldsymbol{\alpha})$ 与 $(\boldsymbol{x},\boldsymbol{y})$ 的输入组合 $(\boldsymbol{\alpha},-\boldsymbol{\alpha})$ 之间的线性关系，再结合 Lai-Massey 模型圈函数的定义可得：

$$\begin{aligned}
&\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(Q_k(\boldsymbol{x},\boldsymbol{y}))\div\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\boldsymbol{x},\boldsymbol{y})\\
&\quad=\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\sigma(F_k(\boldsymbol{x}-\boldsymbol{y})+\boldsymbol{x}),F_k(\boldsymbol{x}-\boldsymbol{y})+\boldsymbol{y})\\
&\qquad\div\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\boldsymbol{x},\boldsymbol{y})\\
&\quad=\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\delta(F_k(\boldsymbol{x}-\boldsymbol{y}))+\delta(\boldsymbol{x})+\boldsymbol{c},\\
&\qquad F_k(\boldsymbol{x}-\boldsymbol{y})+\boldsymbol{y})\div[\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})\chi_{-\boldsymbol{\alpha}}(\boldsymbol{y})]\\
&\quad=\chi_{\boldsymbol{\alpha}}(\delta(F(\boldsymbol{x}-\boldsymbol{y}))+\delta(\boldsymbol{x})+\boldsymbol{c})\chi_{-\boldsymbol{\alpha}}\\
&\qquad\cdot(F(\boldsymbol{x}-\boldsymbol{y})+\boldsymbol{y})\div[\chi_{\boldsymbol{\alpha}}(\boldsymbol{x})\chi_{\boldsymbol{\alpha}}(-\boldsymbol{y})]\\
&\quad=\chi_{\boldsymbol{\alpha}}(\delta(F(\boldsymbol{x}-\boldsymbol{y}))+\delta(\boldsymbol{x}))\chi_{\boldsymbol{\alpha}}(-F(\boldsymbol{x}-\boldsymbol{y})-\boldsymbol{y})\\
&\qquad\cdot\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})[\chi_{\boldsymbol{\alpha}}(-\boldsymbol{x})\chi_{\boldsymbol{\alpha}}(\boldsymbol{y})]\\
&\quad=\chi_{\boldsymbol{\alpha}}(\delta(F(\boldsymbol{x}-\boldsymbol{y}))-F(\boldsymbol{x}-\boldsymbol{y})+\delta(\boldsymbol{x})-\boldsymbol{x})\\
&\qquad\cdot\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})\\
&\quad=\chi_{\boldsymbol{\alpha}}(\delta(F(\boldsymbol{x}-\boldsymbol{y}))-F(\boldsymbol{x}-\boldsymbol{y}))\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})\\
&\qquad\cdot\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})=\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})
\end{aligned}$$

证毕

由定理 4 利用归纳法即得定理 5 如下。

定理 5　设 Lai-Massey 模型中的群是 $(G^m,+)$，$\sigma(x)=\delta(\boldsymbol{x})+\boldsymbol{c}$ 是群 $(G^m,+)$ 上的仿射变换。又设 $\boldsymbol{\alpha}\in G^m$ 使得 $\forall \boldsymbol{x}\in G^m$，都有 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})=1$，则对于 r 圈迭代的加密算法 $E_k(\boldsymbol{x},\boldsymbol{y})$，有 $\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(E_k(\boldsymbol{x},\boldsymbol{y}))=\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\boldsymbol{x},\boldsymbol{y})[\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})]^r$。

备注 2　当 $G=Z/(2^t)$ 时，由 $\chi_{\boldsymbol{\alpha}}$ 的结构知 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})=1$ 等价于 $\boldsymbol{\alpha}\cdot\delta(\boldsymbol{x})=\boldsymbol{\alpha}\cdot\boldsymbol{x}\bmod 2^t$。由于群 $([Z/(2^t)]^m,+)$ 到自身的同态 δ 都具有形式 $\delta(\boldsymbol{x})=\boldsymbol{M}\boldsymbol{x}$，这里 $\boldsymbol{M}$ 是 $Z/(2^t)$ 上的 m 级方阵。因此，如果记 $\boldsymbol{\alpha}$ 是 m 维列向量，则由 $\boldsymbol{\alpha}\cdot\delta(\boldsymbol{x})=\boldsymbol{\alpha}\cdot\boldsymbol{M}\boldsymbol{x}=\boldsymbol{\alpha}^{\mathrm{T}}\cdot\boldsymbol{M}\boldsymbol{x}=(\boldsymbol{M}^{\mathrm{T}}\boldsymbol{\alpha})\cdot\boldsymbol{x}$ 知，$\boldsymbol{\alpha}\cdot\delta(\boldsymbol{x})=\boldsymbol{\alpha}\cdot\boldsymbol{x}\bmod 2^t$ 等价于 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{\alpha}=\boldsymbol{\alpha}$，即 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})=1$ 等价于 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{\alpha}=\boldsymbol{\alpha}$。

由于当 $\boldsymbol{\alpha}=\boldsymbol{0}$ 时，定理 5 的结论是平凡的。因此，下面需要解决的问题是，是否存在非零的 $\boldsymbol{\alpha}$，使得 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})\equiv 1$。我们将证明，当 σ 是群 $(G^m,+)$ 上的仿射变换但不是正型置换时，G^m 中一定存在非零的 $\boldsymbol{\alpha}$，使得 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})\equiv 1$。因此，如果将 σ 设计为群 $(G^m,+)$ 上的仿射变换，则必须将之设计为群 $(G^m,+)$ 上的正型置换，而不能设计为几乎正型置换。

引理 2　设 G 是有限交换群，H 是 G 的子群，则 H 是 G 的真子群的充要条件是存在 $\boldsymbol{\alpha}\in G^n\setminus\{0\}$，使得 $\chi_{\boldsymbol{\alpha}}(H)$ 是单点集。

证明　略。

定理 6　设 δ 是 G^m 至 G^m 的群同构，则仿射变换 $\sigma(\boldsymbol{x})=\delta(\boldsymbol{x})+\boldsymbol{c}$ 是群 $(G^m,+)$ 上的正型置换的充要条件是 $\forall\boldsymbol{\alpha}\in G^m\setminus\{0\}$，$\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})\equiv 1$ 都不成立。

证明　由正型置换的定义知，$\sigma(\boldsymbol{x})=\delta(\boldsymbol{x})+\boldsymbol{c}$ 是正型置换等价于 $\xi(\boldsymbol{x})=\delta(\boldsymbol{x})-\boldsymbol{x}$ 是双射。

设 $\boldsymbol{\alpha}\in G^n\setminus\{0\}$。由于 $\xi(\boldsymbol{x})=\delta(\boldsymbol{x})-\boldsymbol{x}$ 是 G^n 至 G^n 的群同态，且 $\chi_{\boldsymbol{\alpha}}$ 是 G^n 至 C^* 的群同态，因而 $\chi_{\boldsymbol{\alpha}}(\xi(\boldsymbol{x}))$ 是 G^n 至 C^* 的群同态。记 $H=\xi(G^n)=\{\xi(\boldsymbol{x}):\boldsymbol{x}\in G^n\}$ 是 ξ 的像集，则由 ξ 是群同态知 ξ 是 G^n 至 H 的满射，因而 $\chi_{\boldsymbol{\alpha}}(\xi(\boldsymbol{x}))$ 的像集 $\chi_{\boldsymbol{\alpha}}(\xi(G^n))=\{\chi_{\boldsymbol{\alpha}}(\xi(\boldsymbol{x})):\boldsymbol{x}\in G^n\}=\{\chi_{\boldsymbol{\alpha}}(\boldsymbol{u}):\boldsymbol{u}\in H\}=\chi_{\boldsymbol{\alpha}}(H)$。

(1)设 ξ 是双射，则有 $H=G^n$，从而由引理 2 知 $\forall\boldsymbol{\alpha}\in G^n\setminus\{0\}$，$\chi_{\boldsymbol{\alpha}}(H)$ 都不是单点集，即 $\chi_{\boldsymbol{\alpha}}(\xi(\boldsymbol{x}))$ 的像集 $\chi_{\boldsymbol{\alpha}}(\xi(G^n))$ 不是单点集，这说明 $\chi_{\boldsymbol{\alpha}}(\xi(\boldsymbol{x}))$ 不是常值函数，故 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})\equiv 1$ 不成立，这说明必要性成立。

(2)设 $\xi(\boldsymbol{x})=\delta(\boldsymbol{x})-\boldsymbol{x}$ 不是双射，则 $\xi(\boldsymbol{x})$ 的像集 $H=\xi(G^n)$ 构成 G^n 的真子群，从而由引理 2 知，存在 $\alpha\in G^n\setminus\{0\}$ 使得 $\chi_{\boldsymbol{\alpha}}(H)$ 是单点集，因而 $\chi_{\boldsymbol{\alpha}}(\xi(\boldsymbol{x}))$ 的像集 $\chi_{\boldsymbol{\alpha}}(\xi(G^n))=\chi_{\boldsymbol{\alpha}}(H)$ 是单点集，故 $\chi_{\boldsymbol{\alpha}}(\delta(\boldsymbol{x})-\boldsymbol{x})\equiv 1$，这说明充分性成立。　证毕

由定理 6 结合备注 2 可得如下推论。

推论 1　有限交换群上的仿射变换 $\sigma(\boldsymbol{x})=\boldsymbol{M}\boldsymbol{x}+\boldsymbol{c}$ 是正型置换的充要条件是 $\forall\boldsymbol{\alpha}\neq\boldsymbol{0}$，均有 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{\alpha}\neq\boldsymbol{\alpha}$。

由推论 1，则定理 4 可演化为定理 7。

定理 7　设 Lai-Massey 模型中的群是 $(G^m,+)$，$\sigma(\boldsymbol{x})=\delta(\boldsymbol{x})+\boldsymbol{c}$ 是群 $(G^m,+)$ 上的仿射变换但不是正型置换，则存在 $\boldsymbol{\alpha}\in G^m\setminus\{0\}$，使得对于 r 圈迭代的加密算法 $E_k(\boldsymbol{x},\boldsymbol{y})$，有 $\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(E_k(\boldsymbol{x},\boldsymbol{y}))=\chi_{(\boldsymbol{\alpha},-\boldsymbol{\alpha})}(\boldsymbol{x},\boldsymbol{y})\cdot[\chi_{\boldsymbol{\alpha}}(\boldsymbol{c})]^r$。

定理 7 阐述了当 $\sigma(\boldsymbol{x})=\delta(\boldsymbol{x})+\boldsymbol{c}$ 是群 $(G^m,+)$ 上的仿射变换但不是正型置换时，一定存在 $\boldsymbol{\alpha}\in G^m\setminus\{0\}$，使得 r 圈迭代的加密算法 $E_k(\boldsymbol{x},\boldsymbol{y})$ 的输入组合 $(\boldsymbol{\alpha},-\boldsymbol{\alpha})$ 与输出组合 $(\boldsymbol{\alpha},-\boldsymbol{\alpha})$ 之间存在概率为 1 的线性逼近关系。特别地，有以下两个推论成立。

推论 2　设 Lai-Massey 模型中的群是 $([Z/(2^t)]^m,+)$，$\sigma(\boldsymbol{x})=\boldsymbol{M}\boldsymbol{x}+\boldsymbol{c}$ 是群 $([Z/(2^t)]^m,+)$ 上的

仿射变换但不是正型置换，这里 $\boldsymbol{M}$ 是 $Z/(2^t)$ 上的 m 级方阵，$\boldsymbol{c}$ 是 $Z/(2^t)$ 上的 m 维列向量，则存在 $\boldsymbol{\alpha}\in[Z/(2^t)]^m\setminus\{0\}$，使得对于 r 圈迭代的加密算法 $E_k(\boldsymbol{x},\boldsymbol{y})$，有

$$(\boldsymbol{\alpha},-\boldsymbol{\alpha})\cdot E_k(\boldsymbol{x},\boldsymbol{y})=[(\boldsymbol{\alpha},-\boldsymbol{\alpha})\cdot(\boldsymbol{x},\boldsymbol{y})+r(\boldsymbol{\alpha}\cdot\boldsymbol{c})]\bmod 2^t$$

推论 3 设 Lai-Massey 模型中的群是 $(\{0,1\}^n,\oplus)$，$\sigma(\boldsymbol{x})=\boldsymbol{M}\boldsymbol{x}+\boldsymbol{c}$ 是群 $(\{0,1\}^n,\oplus)$ 上的仿射变换但不是正型置换，这里 $\boldsymbol{M}$ 是 $\{0,1\}^n$ 上的 m 级二元方阵，$\boldsymbol{c}$ 是 m 维二元列向量，则存在 $\boldsymbol{\alpha}\in\{0,1\}^n\setminus\{0\}$，使得对于 r 圈迭代的加密算法 $E_k(\boldsymbol{x},\boldsymbol{y})$，有 $(\boldsymbol{\alpha},-\boldsymbol{\alpha})\cdot E_k(\boldsymbol{x},\boldsymbol{y})=(\boldsymbol{\alpha},-\boldsymbol{\alpha})\cdot(\boldsymbol{x},\boldsymbol{y})\oplus(\boldsymbol{\alpha}\cdot\boldsymbol{c})(r\bmod 2)$。

上述推论表明当 Lai-Massey 模型是定义在 $(\{0,1\}^n,\oplus)$ 或 $([Z/(2^t)]^m,+)$ 上的仿射非正型置换时，一定存在非零的 $\boldsymbol{\alpha}$ 使得 Lai-Massey 模型的输入和输出之间存在概率为 1 的线性制约关系。因此，当 σ 为仿射变换时，它应该被设计成为正型置换而不能是几乎正型置换。但当 σ 是非线性函数时，则存在任意轮概率为 1(相关优势为 1)的差分对应(线性逼近)，因此，仍可将 σ 设计成为非线性几乎正型置换。

4 结束语

本文针对有限交换群上定义的 Lai-Massey 模型，研究了其 σ 变换的设计问题。我们从抗差分攻击和抗线性逼近攻击的角度出发，证明了当 σ 是群上的仿射变换时，σ 必须被设计为正型置换，而不能被设计为几乎正型置换，对 Vaudenay 等人给出的 σ 变换的设计要求做了更进一步的限制。此外，本文在研究过程中还针对一般的有限交换群引入了一种新的线性逼近方式，如何利用该线性逼近分析密码算法，还有待进一步研究。

参 考 文 献

[1] Lai X and Massey J. A proposal for a new block encryption standard[C]. Advances in Cryptology-EUROCRYPT' 90, LNCS, 1990, 473: 389-404.

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

[3] Aumasson J P. Exponential attacks on 6-round Luby-Rackoff and on 5-round Lai-Massey[EB/OL]. http://eprint.iacr.org/2011/015. 2011.

[4] Aaram Yun, Je Hong Park, and Jooyoung Lee. On Lai-Massey and quasi-Feistel ciphers[J]. *Design Codes and Cryptography*, 2011, 58(1): 45-72.

[5] Junod P and Vaudenay S. FOX: a new family of block ciphers[C]. Selected Areas in Cryptography -SAC, LNCS, 2004, 259: 131-146.

[6] Nakahara J. An analysis of FOX[C]. Proceedings of the First International Conference on Trusted Systems, Springer-Verlag Berlin, Heidelberg, LNCS, 2010: 236-249.

[7] Wu Wen-ling, Zhang Wen-tao, and Feng Deng-guo. Integral cryptanalysis of reduced FOX block cipher[C]. Information Security and Cryptology -ICISC, LNCS, 2005, 3935: 229-241.

[8] 吴文玲, 卫宏儒. 低圈 FOX 分组密码的碰撞-积分攻击[J]. 电子学报, 2005, 33(7): 1307-1310.
Wu Wen-ling and Wei Hong-ru. Collision-integral attack of reduced-round FOX[J]. *Acta Electcnica Sinica*, 2005, 33(7): 1307-1310.

[9] Wu Zhong-ming, Lai Xue-jia, Zhu Bo, *et al*.. Impossible differential cryptanalysis of FOX[EB/OL]. http://eprint.iacr.org/2009/357. 2009.

[10] 魏悦川, 孙兵, 李超. FOX 密码的不可能差分分析[J]. 通信学报, 2010, 31(9): 24-29.
Wei Yue-chuan, Sun Bing, and Li Chao. Impossible differential attacks on FOX[J]. *Journal on Communications*, 2010, 31(9): 24-29.

[11] Li Rui-lin, You Jian-xiong, Sun Bing, *et al*.. Fault analysis study of the block cipher FOX64[EB/OL]. http://eprint.iacr.org/2010/166, 2010.

[12] Chen Jie, Hu Yupu, Zhang Yueyu, *et al*.. Differential collision attack on reduced FOX block cipher[J]. *Communications Software*, 2012, 7(9): 71-76.

[13] 金晨辉. 多值密码函数的理论和方法研究[D]. [博士论文], 解放军信息工程大学, 2000.
Jin Chen-hui. Researches in theory and methods for multivalued cryptographic functions[D]. [Ph.D. dissertation], The Information Engineering University of PLA, 2000.

付立仕： 女，1989 年生，硕士生，研究方向为密码学.

金晨辉： 男，1965 年生，教授，博士生导师，主要研究方向为密码学.