Lai-Massey结构平均差分概率和平均线性链概率的上界估计

凡如亚* 金晨辉 崔 霆

(解放军战略支援部队信息工程大学 郑州 450001)

摘 要：Lai-Massey结构是由IDEA算法发展而来的一个分组密码结构，FOX系列密码算法是该密码结构的代表。该文从差分概率关于独立等概轮密钥的平均概率上界和给定起点和终点的线性链的平均概率上界两个角度出发，研究Lai-Massey 结构的差分和线性可证明安全性。该文证明了2轮Lai-Massey结构的非平凡差分对应关于独立等概的轮密钥的平均概率$\leq p_{\max}$；证明了当Lai-Massey 结构的F函数是正型置换时，轮数$r\geq 3$的非平凡差分对应关于独立等概的轮密钥的平均概率$\leq p_{\max}^2$。针对给定起点和终点的线性链的平均概率上界，该文也获得了类似的结论。

关键词：密码学；Lai-Massey 结构；差分分析；线性分析；可证明安全；正型置换

中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2018)12-2986-06

DOI: 10.11999/JEIT180196

Upper Bound Estimation of Average Differential Probability and Average Linear Chains Probability of Lai-Massey Structure

FAN Ruya JIN Chenhui CUI Ting

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

Abstract: Lai-Massey structure is a block cipher structure developed from IDEA algorithm. FOX is the representative of this cipher structure. In this paper, the keys are assumed to be generated independently and uniform randomly, and then the provable security against differential and linear cryptanalysis of Lai-Massey structure is studied from two aspects: the upper bound of the average differential probability and the upper bound of the average linear chains probability with the given starting and ending points. This paper proves that when r=2, the average differential probability $\leq p_{\max}$. With the F function of the Lai-Massey structure is orthomorphism, this paper proves that when $r\geq 3$, the average differential probability $\leq p_{\max}^2$. A similar conclusion is obtained for the linear chains with a given starting and ending point.

Key words: Cryptography; Lai-Massey structure; Differentially cryptanalysis; Linearly cryptanalysis; Provable security; Orthomorphism

1 引言

IDEA算法[1]的整体结构是很有特色的密码结构，它不同于Feistel结构，其中$G_k(x,y)\rightarrow(x\oplus f_k(x\oplus y), y\oplus f_k(x\oplus y))$是其核心模块。IDEA算法通过在函数$G_k$之前增加一个异于$\oplus$的群运算，在函数$G_k$之后增加一个块移位的方法，克服函数$G_k$左右块模2和不变的内在缺陷。1999年，Vaudenay等人[2]通过引入线性的正型置换σ，采用在函数G_k之后对左块实施σ变换的方法，克服了函数G_k左右块模2和不变的缺陷，并将该结构定义为Lai-Massey结构。2004年，以Lai-Massey结构为基础，Junod等人[3]提出了FOX系列密码算法，并指出该算法在各个平台上都有很好的性能，并在欧洲有线电视等领域拥有广泛应用。目前，针对FOX密码算法，已有多篇论文[3–9]进行分析。针对Lai-Massey结构与伪随机置换和强伪随机置换的不可区分性，也有多篇论文研究[10–12]。

差分分析和线性分析是对分组密码的重要攻击方法，评估一个分组密码算法抵抗最基本的差分攻击和线性攻击的能力主要有两个方法。一个是考察差分链概率的上界和线性链的线性概率的上界，另一个是考察差分概率关于密钥的平均值[13, 14]的上界，以及给定起点和终点的线性链的线性概率的平均值[13, 14]的上界。

目前，针对SPN结构和Feistel结构，学者们利用上述两种方法获得了相应的结论[13, 14]。针对Lai-

收稿日期：2018-02-28；改回日期：2018-07-20；网络出版：2018-08-06
*通信作者： 凡如亚 fanruya@126.com
基金项目：国家自然科学基金(61402523, 61572516, 61502532)
Foundation Items: The National Natural Science Foundation of China (61402523, 61572516, 61502532)

Massey结构，差分链概率的上界和线性链的线性概率的上界也已获得[15,16]。但是，该结构的差分概率关于密钥的平均值的上界，以及给定起点和终点的线性链的线性概率的平均值的上界的研究还没有展开。本文将研究这个问题。

2　基础知识

定义 1[17]　设$(G,+)$为交换群，$f:G\to G$, $\alpha\in G$, $\beta\in G$，则称

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

为f的差分对应$\alpha\to\beta$的差分概率，其中$|G|$是集合中点的个数。

定义 2[17]　设$f:\{0,1\}^n\to\{0,1\}^m$, $\alpha\in\{0,1\}^n$, $\beta\in\{0,1\}^m$，则称

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

为f的线性逼近$\alpha\to\beta$的相关系数，称$[\rho_f(\alpha\to\beta)]^2$为线性逼近$\alpha\to\beta$的线性概率，其中$\alpha\cdot x$表示$\alpha$与$x$的点积。

当$\alpha\neq 0$时，称差分对应$\alpha\to\beta$为非平凡差分对应，称线性逼近$\beta\to\alpha$为非平凡线性逼近。

定义 3[15]　设$(G,+)$为交换群，$f:G\to G$，令$g(x)=f(x)-x$，如果f和g都是双射，则称f为$(G,+)$上的正型置换。

定义 4[17]　设$\Omega(\alpha,\beta,x)=\#\{k: Q_k(x+\alpha)-Q_k(x)=\beta\}$。如果对任意$\alpha$, β和x, y，都有$\Omega(\alpha,\beta,x)=\Omega(\alpha,\beta,y)$，则称以$Q_k(x)$为轮函数的密码为Markov密码。

定义 5[17]　设$Q:\{0,1\}^n\to\{0,1\}^m$, $\alpha\in\{0,1\}^n$, $\beta\in\{0,1\}^m$, $k\in K$，则称

$$p_Q(\alpha\to\beta)=\frac{1}{|K|}\sum_{k\in K}p_{Q_k}(\alpha\to\beta) \quad (3)$$

为Q_k的差分对应$\alpha\to\beta$关于密钥的平均差分概率。

引理 1[16]　设$f:\{0,1\}^n\to\{0,1\}^n$, $\alpha\in\{0,1\}^n$, $\beta\in\{0,1\}^n$, $g(x)=f(x)\oplus x$，则有

(1)$p_f(\alpha\to\beta)=p_g(\alpha\to\alpha\oplus\beta)$；

(2)$\rho_f(\alpha\to\beta)=\rho_g(\alpha\oplus\beta\to\beta)$。

引理 2[16]　设$f:\{0,1\}^n\to\{0,1\}^n$为双射，则以下3个条件等价：

(1)f是正型置换；

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

(3)$\forall\alpha\neq 0$，有$\rho_f(\alpha\to\alpha)=0$。

定理 1[17]　设以Q_k为轮函数的密码为Markov密码，则$E_{(k_1,\cdots,k_n)}(x)=Q_{k_n}\circ Q_{k_{n-1}}\circ\cdots\circ Q_{k_1}(x)$关于独立等概的轮密钥$k_1,k_2,\cdots,k_n$的平均差分概率为

$$p_E(\alpha_1\to\alpha_{n+1})=\sum_{\alpha_2,\cdots,\alpha_n}\prod_{i=1}^{n}p_Q(\alpha_i\to\alpha_{i+1}) \quad (4)$$

其中，$f\circ g(x)$表示复合函数$f(g(x))$。

定义 6[2]　设$Q_k(x,y)=(\sigma(x\oplus F_k(x\oplus y)),\ y\oplus F_k(x\oplus y))$，$\sigma$为线性函数且是正型置换，则称以$Q_k$为轮函数的密码为Lai-Massey结构。

定理 2[16]　设$Q_k(x,y)=(\sigma(x\oplus f_k(x\oplus y)),\ y\oplus f_k(x\oplus y))$为Lai-Massey结构的轮函数，$(\alpha,\beta)\to(u,v)$为$Q_k$的概率非零的差分对应，则有$u=\sigma(\alpha\oplus\beta\oplus v)$和

$$p_{Q_k}((\alpha,\beta)\to(u,v))=p_{f_k}(\alpha\oplus\beta\to v\oplus\beta) \quad (5)$$

定理 3　设$Q_k(x,y)=(\sigma(x\oplus F_k(x\oplus y)),y\oplus F_k(x\oplus y))$为Lai-Massey结构的轮函数，则以$Q_k$为轮函数的密码构成Markov密码的充要条件是以$F_k$为轮函数的密码构成Markov密码。

证明　由定理2知，$Q_k(x\oplus\alpha,y\oplus\beta)\oplus Q_k(x,y)=(u,v)$等价于$u=\sigma(\alpha\oplus\beta\oplus v)$和$F_k(x\oplus y\oplus\alpha\oplus\beta)\oplus F_k(x\oplus y)=v\oplus\beta$同时成立。当$u\neq\sigma(\alpha\oplus\beta\oplus v)$时，有

$$\begin{aligned}&\Omega_Q((\alpha,\beta),(u,v),(x,y))\\&=\#\{k: Q_k((x,y)\oplus(\alpha,\beta))\oplus Q_k(x,y)\\&=(u,v)\}=0\end{aligned} \quad (6)$$

故此时$\Omega_Q((\alpha,\beta),(u,v),(x,y))$与$(x,y)$的取值无关；当$u=\sigma(\alpha\oplus\beta\oplus v)$时，有

$$\begin{aligned}&\Omega_Q((\alpha,\beta),(u,v),(x,y))\\&=\#\{k: Q_k((x,y)\oplus(\alpha,\beta))\\&\quad\oplus Q_k(x,y)=(u,v)\}\\&=\#\{k: F_k(x\oplus y\oplus\alpha\oplus\beta)\\&\quad\oplus F_k(x\oplus y)=v\oplus\beta\}\\&=\Omega_F(\alpha\oplus\beta,v\oplus\beta,x\oplus y)\end{aligned} \quad (7)$$

即$\Omega_Q((\alpha,\beta),(u,v),(x,y))=\Omega_F(\alpha\oplus\beta,\ v\oplus\beta,x\oplus y)$，故$\Omega_Q((\alpha,\beta),(u,v),(x,y))$与$(x,y)$的取值无关等价于$\Omega_F(\alpha\oplus\beta,v\oplus\beta,x\oplus y)$与$x\oplus y$的取值无关。　证毕

定理 4　设$(G,+)$为交换群，$f_k:G\to G$，令$F_{(k_1,k_2)}(x)=f_{k_2}(x+k_1)$且$k_1$与$k_2$独立，则以$F_{k_1,k_2}(x)$为轮函数的密码为Markov密码。

证明　(1)对于给定的α,β,x，有

$$\begin{aligned}\Omega(\alpha,\beta,x)&=\#\{(k_1,k_2): g_{k_2}(x+k_1+\alpha)\\&\quad-g_{k_2}(x+k_1)=\beta\}\\&\overset{y=x+k_1}{=}\#\{(y-x,k_2): g_{k_2}(y+\alpha)\\&\quad-g_{k_2}(y)=\beta\}\\&=\#\{(y,k_2): g_{k_2}(y+\alpha)-g_{k_2}(y)=\beta\}\\&=\Omega(\alpha,\beta,0)\end{aligned} \quad (8)$$

因而以$F_{k_1,k_2}(x)$为轮函数的密码为Markov密码。证毕

定理3和定理4说明，使得Lai-Massey结构构成Markov密码是很容易的。特别地，FOX系列算法都是Markov密码。

3 Lai-Massey结构的平均差分概率的上界

文献[15]证明了，当线性函数σ不是正型置换时，任意轮的Lai-Massey结构都具有概率为1的非平凡差分对应和概率为1的线性逼近，因而当将σ设计为线性函数时，必须将它设计为正型置换。因此，本文仅针对σ是线性函数且是正型置换的情形进行研究。

定理 5 设Lai-Massey结构的F函数的非平凡差分对应关于密钥的平均差分概率$\le p_{\max}$，则2轮的Lai-Massey结构的非平凡差分对应关于独立等概的轮密钥的平均概率$\le p_{\max}$。

证明 设第1轮的输入差为(α,β)且$(\alpha,\beta)\neq(0,0)$，第2轮的输出差为(u,v)，则由定理1知，2轮Lai-Massey结构的差分对应$(\alpha,\beta)\to(u,v)$关于独立等概的轮密钥的平均差分概率为

$$p=\sum_{x,y}p_Q((\alpha,\beta)\to(x,y))p_Q((x,y)\to(u,v)) \quad (9)$$

设$p_Q((\alpha,\beta)\to(x,y))p_Q((x,y)\to(u,v))\neq 0$，则由定理2知$\left.\begin{array}{l}x=\sigma(\alpha\oplus\beta\oplus y)\\ u=\sigma(x\oplus y\oplus v)\end{array}\right\}$，即

$$\left.\begin{array}{l}x\oplus\sigma(x)=\sigma(\alpha\oplus\beta)\oplus u\oplus\sigma(v)\\ y\oplus\sigma(y)=\sigma(\alpha\oplus\beta)\oplus\sigma^{-1}(u)\oplus v\end{array}\right\} \quad (10)$$

由σ是正型置换知$\sigma(z)\oplus z$是双射，故(x,y)由(α,β)和(u,v)唯一确定。再由定理2知

$$\left.\begin{array}{l}p_Q((\alpha,\beta)\to(x,y))=p_F(\alpha\oplus\beta\to y\oplus\beta),\\ p_Q((x,y)\to(u,v))=p_F(x\oplus y\to v\oplus y)\end{array}\right\} \quad (11)$$

(1)如果$\alpha\oplus\beta=0$，则有$y\oplus\beta=0$。再由$x=\sigma(\alpha\oplus\beta\oplus y)$知$x=\sigma(\alpha)$，因而$x\oplus y=\sigma(\alpha)\oplus\beta=\sigma(\alpha)\oplus\alpha$。由$(\alpha,\beta)\neq(0,0)$知$\alpha=0$，再由$\sigma$是正型置换知$\sigma(\alpha)\oplus\alpha\neq 0$，因而有

$$\begin{aligned}p&=\sum_{x,y}p_Q((\alpha,\beta)\to(x,y))p_Q((x,y)\to(u,v))\\ &=p_F(0\to 0)p_F(\sigma(\alpha)\oplus\alpha\to v\oplus\beta)\\ &=p_F(\sigma(\alpha)\oplus\alpha\to v\oplus y)\le p_{\max}\end{aligned} \quad (12)$$

(2)如果$\alpha\oplus\beta\neq 0$，则有

$$\begin{aligned}p&=\sum_{x,y}p_Q((\alpha,\beta)\to(x,y))\\ &\quad\cdot p_Q((x,y)\to(u,v))\\ &=p_F(\alpha\oplus\beta\to y'\oplus\beta)p_F(x'\oplus y'\to v\oplus y')\\ &\le p_{\max}\times 1=p_{\max}\end{aligned} \quad (13)$$

这里

$$\left.\begin{array}{l}x'\oplus\sigma(x')=\sigma(\alpha\oplus\beta)\oplus u\oplus\sigma(v)\\ y'\oplus\sigma(y')=\sigma(\alpha\oplus\beta)\oplus\sigma^{-1}(u)\oplus v\end{array}\right\} \quad (14)$$

故总有$p\le p_{\max}$。证毕

定理 6 存在2轮Lai-Massey结构的密码算法，使得定理5中的上界可达。

证明 设Lai-Massey结构的F函数为$F_k(x)=f(x\oplus k)$，且存在$\alpha\neq 0$，使得

$$p_f(\sigma(\alpha)\oplus\alpha\to\sigma(\alpha)\oplus\alpha)=\max_{a,b\text{且}a\neq 0}p_f(a\to b) \quad (15)$$

则F_k的平均差分概率的最大值$p_{\max}=p_f(\sigma(\alpha)\oplus\alpha\to\sigma(\alpha)\oplus\alpha)$。根据定理5的证明，2轮Lai-Massey结构的差分对应$(\alpha,\alpha)\to(\sigma(\alpha),\sigma(\alpha))$的平均概率为

$$p=p_F(0\to 0)p_F(\sigma(\alpha)\oplus\alpha\to\sigma(\alpha)\oplus\alpha)=p_{\max} \quad (16)$$

这说明定理5的上界可达。证毕

以定理6中2轮Lai-Massey结构证明为基础，直接在后面添加1轮，此时定理5的上界仍可达。说明轮数变为3轮时，如果不加上其他的限制条件，其差分概率上界也可能没有任何改善。因此，我们将尝试对F函数作限制，以期改善3轮的差分概率上界。下面证明，当Lai-Massey结构的F函数是正型置换时，上述结论还可加强。

定理7 设Lai-Massey结构的F函数是正型置换，且F函数的非平凡差分对应关于密钥的平均概率$\le p_{\max}$，则当轮数$r\ge 3$时，r轮Lai-Massey结构的非平凡差分对应关于独立等概的轮密钥的平均概率$\le p_{\max}^2$。

证明 设第1轮的输入差为(α,β)且$(\alpha,\beta)\neq(0,0)$，第3轮的输出差为(u,v)，则由定理1知，3轮复合的Lai-Massey结构的差分对应$(\alpha,\beta)\to(u,v)$关于独立等概的轮密钥的平均差分概率为

$$\begin{aligned}p&=\sum_{x,y,s,t}p_Q((\alpha,\beta)\to(x,y))\\ &\quad\cdot p_Q((x,y)\to(s,t))p_Q((s,t)\to(u,v))\end{aligned} \quad (17)$$

设$p_Q((\alpha,\beta)\to(x,y))p_Q((x,y)\to(s,t))p_Q((s,t)\to(u,v))\neq 0$，则根据定理2知

$$\left.\begin{aligned} &p_Q((\alpha,\beta)\to(x,y))=p_F(\alpha\oplus\beta\to y\oplus\beta)\\ &p_Q((x,y)\to(s,t))=p_F(x\oplus y\to t\oplus y)\\ &p_Q((s,t)\to(u,v))=p_F(s\oplus t\to v\oplus t)\end{aligned}\right\}$$

$$\text{和}\left.\begin{aligned} &x=\sigma(\alpha\oplus\beta\oplus y)\\ &s=\sigma(x\oplus y\oplus t)\\ &u=\sigma(s\oplus t\oplus v)\end{aligned}\right\},\ \text{即}$$

$$\left.\begin{aligned} &x=\sigma(\alpha\oplus\beta\oplus y)\\ &s\oplus\sigma(s)=\sigma(x\oplus y\oplus v)\oplus u\\ &t\oplus\sigma(t)=\sigma(x\oplus y)\oplus v\oplus\sigma^{-1}(u)\end{aligned}\right\}\tag{18}$$

由σ是正型置换知$\sigma(z)\oplus z$是双射，因而x, s, t由 y唯一确定。

(1)如果$\alpha\oplus\beta=0$，则有$y=\beta\neq 0$，从而$x\oplus y=\sigma(\alpha\oplus\beta\oplus y)\oplus y=\sigma(y)\oplus y\neq 0$。

假设$s\oplus t=0$，则有$u=\sigma(s\oplus t\oplus v)=\sigma(v)$, 进而有$t\oplus\sigma(t)=\sigma(x\oplus y)$。又因

$$\begin{aligned}x\oplus\sigma(x)&=\sigma(\alpha\oplus\beta\oplus y)\oplus\sigma(x)=\sigma(x\oplus y)\\&=t\oplus\sigma(t)\end{aligned}\tag{19}$$

再由σ是正型置换知$x=t$，因而有$t\oplus y=x\oplus y$。但由σ是正型置换知$p_F(x\oplus y\to t\oplus y)=p_F(x\oplus y\to x\oplus y)=0$，矛盾。该矛盾说明$s\oplus t\neq 0$，这说明

$$\begin{aligned}p&=\sum_{x,y,s,t}p_F(\alpha\oplus\beta\to y\oplus\beta)\\&\quad\cdot p_F(x\oplus y\to t\oplus y)p_F(s\oplus t\to v\oplus t)\\&=p_F(0\to 0)p_F(x'\oplus y'\to t'\oplus y')\\&\quad\cdot p_F(s'\oplus t'\to v\oplus t')\le p_{\max}^2\end{aligned}\tag{20}$$

其中，s',t',x',y'由$y'=\beta$和式(18)唯一确定。

(2)如果$\alpha\oplus\beta\neq 0$，则有$p_F(\alpha\oplus\beta\to y\oplus\beta)\le p_{\max}$。

如果$u=\sigma(v)$，则$s\oplus t=\sigma^{-1}(u)\oplus v=0$，因而$t=v$被唯一确定。再由$t\oplus\sigma(t)=\sigma(x\oplus y)\oplus v\oplus\sigma^{-1}(u)$知$x\oplus y$被唯一确定，进而由$x\oplus y=\sigma(\alpha\oplus\beta\oplus y)\oplus y$知$\sigma(y)\oplus y$被唯一确定，故$y$被唯一确定，因而$x,y,s,t$都是唯一的。

假设$x\oplus y=0$，则有$t\oplus\sigma(t)=\sigma(x\oplus y)\oplus v\oplus\sigma^{-1}(u)=0$，因而$t=0$，于是有$v=t=0$和$u=\sigma(v)=0$，故$(u,v)=(0,0)$，进而有$(\alpha,\beta)=(0,0)$，矛盾。该矛盾说明$x\oplus y\neq 0$。因而有

$$\begin{aligned}p&=\sum_{x,y,s,t}p_F(\alpha\oplus\beta\to y\oplus\beta)\\&\quad\cdot p_F(x\oplus y\to t\oplus y)p_F(s\oplus t\to v\oplus t)\\&=p_F(\alpha\oplus\beta\to y'\oplus\beta)\\&\quad\cdot p_F(x'\oplus y'\to t'\oplus y')p_F(s'\oplus t'\to v\oplus t')\\&\le p_{\max}\times p_{\max}\times 1=p_{\max}^2\end{aligned}\tag{21}$$

其中，s',t',x',y'由$t'=v$和式(18)唯一确定。

如果$u\neq\sigma(v)$，则有$s\oplus t\neq 0$，因而有

$$\left.\begin{aligned} &p_F(\alpha\oplus\beta\to y\oplus\beta)\le p_{\max}\\ &p_F(s\oplus t\to v\oplus t)\le p_{\max}\end{aligned}\right\}\tag{22}$$

进而有

$$\begin{aligned}p&=\sum_{x,y,s,t}p_F(\alpha\oplus\beta\to y\oplus\beta)\\&\quad\cdot p_F(x\oplus y\to t\oplus y)p_F(s\oplus t\to v\oplus t)\\&\le p_{\max}^2\sum_y p_F(x\oplus y\to t\oplus y)\end{aligned}\tag{23}$$

由于$x\oplus y=\sigma(\alpha\oplus\beta)\oplus\sigma(y)\oplus y$和

$$\begin{aligned}(1\oplus\sigma)(t\oplus x)&=(\sigma(x\oplus y)\oplus v\oplus\sigma^{-1}(u))\\&\quad\oplus(1\oplus\sigma)(x)\\&=x\oplus\sigma(y)\oplus v\oplus\sigma^{-1}(u)\\&=\sigma(\alpha\oplus\beta)\oplus v\oplus\sigma^{-1}(u)\end{aligned}\tag{24}$$

因而有：$t\oplus x=(1\oplus\sigma)^{-1}(\sigma(\alpha\oplus\beta)\oplus v\oplus\sigma^{-1}(u))\overset{\text{def}}{=}A$。

令$G_k(x)=F_k(x)\oplus x$，则由F_k是正型置换知G_k是双射，因而有

$$\begin{aligned}p_{F_k}(x\oplus y\to t\oplus y)&=p_{G_k}(x\oplus y\to x\oplus t)\\&=p_{G_k}(\sigma(\alpha\oplus\beta)\\&\quad\oplus\sigma(y)\oplus y\to A)\end{aligned}\tag{25}$$

于是，有

$$\begin{aligned}&\sum_y p_F(x\oplus y\to t\oplus y)\\&\quad=\sum_y p_G(\sigma(\alpha\oplus\beta)\oplus\sigma(y)\oplus y\to A)\\&\quad=\sum_z p_G(\sigma(\alpha\oplus\beta)\oplus z\to A)=1\end{aligned}$$

这说明

$$p\le p_{\max}^2\sum_y p_F(x\oplus y\to t\oplus y)=p_{\max}^2\tag{26}$$

因此，对于3轮Lai-Massey结构，总有$p\le p_{\max}^2$。再利用归纳法，证明该结论对轮数≥ 4也成立。

假设本定理对r轮Lai-Massey成立，现证明当轮数为r+1时本定理仍成立。

事实上，设第1轮的输入差为a且$a\neq 0$，第r+1轮的输出差为c，则由归纳假设知，对任意b，有$p(a\xrightarrow{r\text{轮}}b)\le p_{\max}^2$，从而由定理1知

$$\begin{aligned}p(a\xrightarrow{r+1\text{轮}}c)&=\sum_b p(a\xrightarrow{r\text{轮}}b)p(b\xrightarrow{1\text{轮}}c)\\&\le p_{\max}^2\sum_b p(b\xrightarrow{1\text{轮}}c)\\&=p_{\max}^2\end{aligned}\tag{27}$$

故此时本定理对r+1成立，故由归纳法和本定理对$r=3$成立知本定理成立。 证毕

4 Lai-Massey结构的平均线性链概率的上界

下面证明类似的结论对线性链的平均概率也成立。

定理 8[16] 设$\sigma(x)=Mx$是线性变换，令$\delta(x)=(M^T)^{-1}x$，则Lai-Massey结构轮函数的线性逼近$(\alpha,\beta)\to(A,B)$的相关系数$\rho\neq 0$的充要条件是$A=\delta(\alpha\oplus\beta\oplus B)$且对应的F函数的线性逼近$\beta\oplus B\to\alpha\oplus\beta$的相关系数为$\rho$。

定义 7[13, 14] 设k为给定的密钥，则称

$$\omega_{E_k}(\alpha_1\to\alpha_{n+1})=\sum_{\alpha_2,\cdots,\alpha_n}\prod_{i=1}^{n}[\rho_{Q_k}(\alpha_i\to\alpha_{i+1})]^2$$

为以α_1为起点，以α_{n+1}为终点的线性链的平均概率。当$\alpha_1\neq 0$时，称以α_1为起点的线性链为非平凡链。

定理 9 设Lai-Massey结构的F函数的非平凡线性逼近的相关系数的平方$\le p_{\max}$，则当r=2时，r轮Lai-Massey结构的非平凡线性链的平均概率$\le p_{\max}$。

证明 根据定义7和定理8，当$r=2$时，有

$$\begin{aligned}\omega&=\sum_{x,y}\rho^2_{Q_{k_1}}((\alpha,\beta)\to(x,y))\rho^2_{Q_{k_2}}((x,y)\to(u,v))\\&=\sum_{x,y}\rho^2_{F_{k_1}}(\beta\oplus y\to\alpha\oplus\beta)\rho^2_{F_{k_2}}(y\oplus v\to x\oplus y)\end{aligned}\tag{28}$$

且$x=\delta(\alpha\oplus\beta\oplus y)$和$u=\delta(x\oplus y\oplus v)$。以下只需将$p_F(0\to b)\neq 0$蕴含$b=0$的依据修改为$\rho_{F_k}(a\to 0)\neq 0$蕴含$a=0$，将$\sum_b p_f(a\to b)=1$的依据修改为$\sum_a\rho_f^2(a\to b)=1$，就可将定理5的证明修改为本定理的证明，具体证明略。

定理 10 设Lai-Massey结构的F函数是正型置换，且F函数的非平凡线性逼近的概率$\le p_{\max}$，则当轮数$r\ge 3$时，r轮Lai-Massey结构的非平凡线性逼近的总概率$\le p^2_{\max}$。

证明 根据定义7和定理8，当$r\ge 3$时，有

$$\begin{aligned}\omega&=\sum_{x,y,s,t}\rho^2_{Q_{k_1}}((\alpha,\beta)\to(x,y))\\&\quad\cdot\rho^2_{Q_{k_2}}((x,y)\to(s,t))\rho^2_{Q_{k_3}}((s,t)\to(u,v))\\&=\sum_{x,y,s,t}\rho^2_{F_{k_1}}(\beta\oplus y\to\alpha\oplus\beta)\\&\quad\cdot\rho^2_{F_{k_2}}(y\oplus t\to x\oplus y)\rho^2_{F_{k_3}}(s\oplus v\to s\oplus t)\end{aligned}\tag{29}$$

$$\left.\begin{aligned}x&=\sigma(\alpha\oplus\beta\oplus y)\\\text{和}\quad s&=\sigma(x\oplus y\oplus t)\\u&=\sigma(s\oplus t\oplus v)\end{aligned}\right\}\text{，即}$$

$$\left.\begin{aligned}&x=\sigma(\alpha\oplus\beta\oplus y)\\&s\oplus\sigma(s)=\sigma(x\oplus y\oplus v)\oplus u\\&t\oplus\sigma(t)=\sigma(x\oplus y)\oplus v\oplus\sigma^{-1}(u)\end{aligned}\right\}\tag{30}$$

同样，只需将$p_F(0\to b)\neq 0$蕴含$b=0$的依据修改为$\rho_{F_k}(a\to 0)\neq 0$蕴含$a=0$，将$\sum_b p_f(a\to b)=1$的依据修改为$\sum_a\rho_f^2(a\to b)=1$，就可将定理7的证明修改为本定理的证明，具体证明略。

5 结束语

自从 Lai-Massey 结构和 FOX 算法提出以来，学者们已经对它们进行了很多的分析。本文主要从差分概率关于独立等概轮密钥的平均概率上界和给定起点和终点的线性链的平均概率上界两个角度出发，对Lai-Massey 结构的差分和线性可证明安全性进行了研究。本文的结果进一步丰富了Lai-Massey 结构的分析结果，对于认识基于该结构设计的密码算法有实际的意义。

参 考 文 献

[1] LAI Xuejia and MASSEY J. A proposal for a new block encryption standard. In: Advances in Cryptology[J]. *LNCS*, 1990, 473: 389–404. doi: 10.1007/3-540-46877-3_35.

[2] VAUDENAY S. On the Lai-Massey scheme[J]. *LNCS*, 1999, 1716: 8–19. doi: 10.1007/978-3-540-48000-6_2.

[3] JUNOD P and VAUDENAY S. FOX: A new family of block ciphers[C]. LNCS, 2004, 259: 131–146. doi: 10.1007/978-3-540-30564-4_8.

[4] WU Wenling, ZHANG Wentao, and FENG Dengguo. Improved integral cryptanalysis of reduced FOX block cipher[C]. LNCS, 2005, 3935: 229–241. doi: 10.1007/11734727_20.

[5] WU Zhongming, LAI Xuejia, ZHU Bo, *et al*. Impossible differential cryptanalysis of FOX[J]. *LNCS*, 2010, 6163: 236–249. doi: 10.1007/978-3-642-14597-1_15.

[6] 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 Yuechuan, SUN Bing, and LI Chao. Impossible differential attacks on FOX[J]. *Journal on Communications*, 2010, 31(9): 24–29.

[7] 吴文玲, 卫宏儒. 低轮 FOX 分组密码的碰撞-积分攻击[J]. 电子学报, 2005, 33(7): 1307–1310.
WU Wenling and WEI Hongru. Collision-integral attack of reduced-round FOX[J]. *Acta Electronica Sinica*, 2005, 33(7): 1307–1310.

[8] 郭瑞, 金晨辉. 低轮FOX64算法的零相关-积分分析[J]. 电子与信息学报, 2015, 37(2): 418–422. doi: 10.11999/JEIT140373.
GUO Rui and JIN Chenhui. Zero correlation-Integral attack of reduced-round FOX[J]. *Journal of Electronics & Information Technology*, 2015, 37(2): 418–422. doi: 10.11999/JEIT140373.

[9] LI Ruilin, YOU Jianxiong, SUN Bing, *et al*. Fault analysis study of the block cipher FOX64[J]. *Multimedia Tools and Applications*, 2013, 63(3): 691–708. doi: 10.1007/s11042-011-0895-x.

[10] LUO Yiyuan, LAI Xuejia, and GONG Zheng. Pseudorandomness analysis of the (extended) Lai-Massey scheme[J]. *Information Processing Letters*, 2010, 111(2): 90–96. doi: 10.1016/j.ipl.2010.10.012.

[11] YUN A, PARK J H, and LEE J. On Lai-Massey and quasi-Feistel ciphers[J]. *Design Codes and Cryptography*, 2011, 58: 45–72. doi: 10.1007/s10623-010-9386-8.

[12] 郭瑞, 金晨辉. Lai-Massey结构伪随机特性研究[J]. 电子与信息学报, 2014, 36(4): 828–833. doi: 10.3724/SP.J.1146.2013.00870.
GUO Rui and JIN Chenhui. On the pseudorandomness of the Lai-Massey scheme[J]. *Journal of Electronics & Information Technology*, 2014, 36(4): 828–833. doi: 10.3724/SP.J.1146.2013.00870.

[13] AOKI K and OHTA K. Strict evaluation of the maximum average of differential probability and the maximum average of linear probability[J]. *IEICE Transactions Fundamentals*, 1997, E80-A(1): 2–8.

[14] NYBERG L and KNUDSEN L R. Provable security against a differential attack[J]. *Journal of Cryptology*, 1995, 8: 27–37. doi: 10.1007/BF00204800.

[15] 付立仕, 金晨辉. 基于仿射非正型σ变换的Lai-Massey模型的密码学缺陷[J]. 电子与信息学报, 2013, 35(10): 2536–2540. doi: 10.3724/SP.J.1146.2012.01574.
FU Lishi and JIN Chenhui. The cryptographic weakness of Lai-Massey scheme with an affine but not orthomorphic bijection σ[J]. *Journal of Electronics & Information Technology*, 2013, 35(10): 2536–2540. doi: 10.3724/SP.J.1146.2012.01574.

[16] 付立仕, 金晨辉. Lai-Massey 模型的差分和线性可证明安全性[J]. 软件学报, 2013, 24(Suppl.2): 207–215.
FU Lishi and JIN Chenhui. Differential and linear provable security of Lai-Massey scheme[J]. *Journal of Software*, 2013, 24(Suppl.2): 207–215.

[17] 金晨辉, 郑浩然, 张少武, 等. 密码学[M]. 北京: 高等教育出版社, 2009: 175–198.
JIN Chenhui, ZHENG Haoran, ZHANG Shaowu, *et al*. Cryptology[M]. Beijing: Higher Education Press, 2009: 175–198.

凡如亚：男，1989年生，博士生，研究方向为分组密码算法的设计与分析.

金晨辉：男，1965年生，教授，博士生导师，主要研究方向为密码算法的设计与分析.

崔　霆：男，1985年生，副教授，主要研究方向为密码算法的设计与分析.