一类非平衡 Feistel 网络的差分可证明安全性分析

王念平　　金晨辉　　李云强
（解放军信息工程大学电子技术学院　郑州　450004）

摘　要：该文深入研究了一类非平衡 Feistel 网络的差分可证明安全性。给出了其圈函数的具有非零差分概率的差分对应的结构形式。给出了连续 m 个非平凡差分对应的一个分布规律。证明了 $s(s\geqslant 2m)$圈非平凡差分对应概率的上界为其轮函数非平凡差分对应概率最大值 ($p_{\max}$) 的平方的 2 倍；当相应的轮函数为双射时，此上界可进一步改进为其轮函数非平凡差分对应概率的最大值的平方。最后对非平衡 Feistel 网络进行了讨论。

关键词：非平衡 Feistel 网络，差分可证明安全性，差分对应，差分概率，上界
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2005)06-0870-04

The Differential Provable Security Analysis of a Kind of Unbalanced Feistel Networks

Wang Nian-ping　　Jin Chen-hui　　Li Yun-qiang
(*Institute of Electron. Tech., The PLA Info. Eng. Univ., Zhengzhou* 450004, *China*)

Abstract　The differential provable security of a kind of unbalanced Feistel networks is investigated deeply. The structure of the differential correspondence between round functions whose differential probability is nonzero is given. A distribution of m sequential differential correspondences is given. If $p_{\max}$ is the maximum of the probability of round function $f(x)$, the upperbounds of the differential probability over at least $2m$ rounds is proven to be two times of the square of $p_{\max}$ and is proven to be the square of $p_{\max}$ when $f(k, x_m)$ is bijective. In conclusion, the unbalanced Feistel networks is discussed.

Key words　Unbalanced Feistel networks, The differential provable security, Differential correspondence, Differential probability,　Upperbounds

1　引言

差分密码分析[1]是目前已知的最好攻击方法之一，因此，每个分组密码设计者都要想办法估计新算法抵抗差分密码分析的能力。现有的做法要么是从实际的角度给出最大差分特征的概率（或是差分特征概率的上界），要么是从理论的角度对密码模型进行差分可证明安全性分析。这是两种不尽相同的分析方法，但后者更能反映密码抵抗差分密码分析的能力[2]。针对传统的 Feistel 密码，对前者有如下结论。

结论 1[3]　对于具有独立均匀随机子密钥的 r 圈 Feistel 密码，令 $p_{\max}$ 表示轮函数的最大差分概率，则有

(1) 当 $r=2m,\ 2m+1$ 时，r 圈最大差分特征概率 $\leqslant p_{\max}^{m}$。

(2) 当 $r=3m,3m+1$ 且轮函数是双射时，r 圈最大差分特征概率 $\leqslant p_{\max}^{2m}$。

(3) 当 $r=3m+2$ 且轮函数是双射时，r 圈最大差分特征概率 $\leqslant p_{\max}^{2m+1}$。

对后者有

结论 2[4]　条件同结论 1，有

(1) 当 $r\geqslant 4$ 时，r 圈最大差分概率 $\leqslant 2p_{\max}^{m}$。

(2) 当 $r\geqslant 3$ 且轮函数是双射时，r 圈最大差分概率 $\leqslant p_{\max}^{m}$。

Schneier 和 Kelsey[5]把 Feistel 网络推广到非平衡 Feistel 网络。Admas 在文献[6]中将如图 1 所示的非平衡 Feistel 网络应用于众所周知的 AES 候选算法 CAST-256。非平衡 Feistel 网络的最大优点是能够直接重用过去的轮函数。众所周知，过去的分组密码都是 64bit 分组长度，而随着计算能力的提高，现在设计分组密码都要求至少是 128bit 分组长度；对于传统的 Feistel 网络，分组长度的增加意味着轮函数 f 规模的增加，而构造大规模的轮函数又是比较困难的。如图 1 所示

2003-11-18 收到，2004-10-21 改回
国家部级基金(5143603ZDS0601)资助课题

的非平衡 Feistel 网络为我们设计密码创造了一条捷径。文献[7]对图 1 中的四分组非平衡 Feistel 网络的差分特征概率的上界进行了研究。但对非平衡 Feistel 网络的差分可证明安全性的研究却无人涉及。本文针对一类 m 分组非平衡 Feistel 网络的差分可证明安全性进行了分析，从而为其进一步应用提供了理论依据和支持，对密码方案的设计和分析也有一定的指导意义。

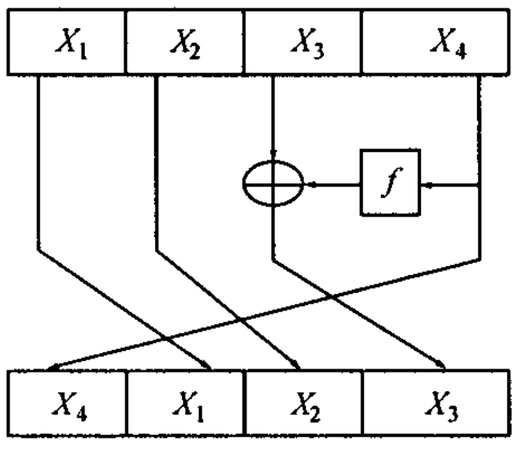

图 1　一圈四分组非平衡 Feistel 网络结构框图

2　预备知识

定义 1　设 $(X,\oplus)$ 是有限交换群，$X=Z_2^n$，$x_i\in Z_2^n$，$1\le i\le m$，则称

$$Q_k(x_1,\cdots,x_{m-1},x_m)=(x_m,x_1,\cdots,x_{m-2},f(k,x_m)\oplus x_{m-1})$$

为圈函数的结构为 m 分组非平衡 Feistel 网络。其中 k 表示密钥，$\oplus$ 表示逐位模 2 加运算，并称 $f(k,x_m)$ 为轮函数（下同）。

本定义中的 m 分组非平衡 Feistel 网络的初始定义始于文献[5]。

定义 2　设 $(X,+)$ 和 $(Y,+)$ 都是有限交换群，$f:X\to Y$，$\alpha\in X$，$\beta\in Y$，令

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

则称 $p_f(\alpha\to\beta)$ 为 f 的在输入差为 α 条件下，输出差为 β 的差分概率。此外，也称 $\alpha\to\beta$ 为 f 的一个差分对应，称 $p_f(\alpha\to\beta)$ 为该差分对应的概率。

由定义 1，对 m 分组非平衡 Feistel 网络恒有 $p_{Q_k}((0,0,\cdots,0)\to(0,0,\cdots,0))=1$，故称差分对应 $(0,0,\cdots,0)\to(0,0,\cdots,0)$ 为平凡的，以下只考虑圈函数的输入差分 $(\alpha_1,\alpha_2,\cdots,\alpha_m)\ne(0,0,\cdots,0)$ 即非平凡的情形。

引理 1[2]　若一个 r 圈迭代密码是马尔可夫密码，且 r 圈子密钥是独立均匀随机的，则差分序列 $\Delta x(0),\Delta x(1),\cdots,\Delta x(r)$ 是一条齐次马尔可夫链。其中，对 $\forall i,0\le i\le r,\Delta x(i)$ 表示第 $i+1$ 圈输入差（下同）。

引理 2[2]　设一个 r 圈迭代密码满足引理 1 中的条件，则 r 圈差分对应的概率由下式给出：

$$p(\Delta x(r)=\beta_r|\Delta x(0)=\beta_0)=\sum_{\beta_1}\sum_{\beta_2}\cdots\sum_{\beta_{r-1}}\prod_{i=1}^{r}p(\Delta x(1)=\beta_i|\Delta x(0)=\beta_{i-1})$$

3　主要结论

定理 1　对 m 分组非平衡 Feistel 网络 $Q_k(x_1,\cdots,x_{m-1},x_m)=(x_m,x_1,\cdots,x_{m-2},f(k,x_m)\oplus x_{m-1})$ 而言，其圈函数的具有非零差分概率的差分对应都具有形式：

$$(\alpha_1,\cdots,\alpha_{m-1},\alpha_m)\to(\alpha_m,\alpha_1,\cdots,\alpha_{m-2},\beta\oplus\alpha_{m-1})$$

且　$p_{Q_k}((\alpha_1,\cdots,\alpha_{m-1},\alpha_m)\to(\alpha_m,\alpha_1,\cdots,\alpha_{m-2},\beta\oplus\alpha_{m-1}))=p_{f_k}(\alpha_m\to\beta)$

这里 f_k 表示轮函数 $f(k,x_m)$（下同）。

定理 2　对 m 分组非平衡 Feistel 网络 $Q_k(x_1,\cdots,x_{m-1},x_m)=(x_m,x_1,\cdots,x_{m-2},f(k,x_m)\oplus x_{m-1})$ 而言，不可能有连续 m 个非平凡差分对应使相应的 f_k 函数的输入差都是 0。

为以下证明方便，用 $\Delta x_j(i)$ 表示第 $i+1$ 圈输入差的第 j 分块，并设 m 分组非平衡 Feistel 网络的连续 m 圈差分对应依次为

$$(\Delta x_1(0),\Delta x_2(0),\cdots,\Delta x_m(0))\to\cdots\to(\Delta x_1(m),\Delta x_2(m),\cdots,\Delta x_m(m))=(\beta_1,\beta_2,\cdots,\beta_m)$$

其中对 $\forall i,j,0\le i\le m-1,\ 1\le j\le m-2,\ \Delta x_m(i)=\Delta x_1(i+1),\ \Delta x_j(i)=\Delta x_{j+1}(i+1)$，从而相应的 f 函数（即 f_k 函数，下同）的差分对应依次为

$$\begin{aligned}\Delta x_m(0)&\to\Delta x_{m-1}(0)\oplus\beta_{m-1},\beta_{m-1}\\&\to\Delta x_{m-2}(0)\oplus\beta_{m-2},\cdots,\beta_{m-k}\\&\to\Delta x_{m-k-1}(0)\oplus\beta_{m-k-1},\cdots,\beta_2\\&\to\Delta x_1(0)\oplus\beta_1,\beta_1\to\Delta x_m(0)\oplus\beta_m\end{aligned}\tag{1}$$

其中 $2\le k\le m-3$。

定理 3　设 m 分组非平衡 Feistel 网络 $Q_k(x_1,\cdots,x_{m-1},x_m)=(x_m,x_1,\cdots,x_{m-2},f(k,x_m)\oplus x_{m-1})$ 满足引理 1 中的条件，则 $s(s\ge m)$ 圈非平凡差分对应的概率不大于 $p_{\max}$。其中 $p_{\max}=\max_{\gamma\ne0}p_{f_k}(\gamma\to\delta)$（下同）。

证明　(1)先证对 $\forall\alpha\ne0$ 及 β 有 $p(\Delta x(m)=\beta|\Delta x(0)=\alpha)\le p_{\max}$。

对 $\forall k,2\le k\le m-3$，由定理 2 及式(1)知 $\beta_1,\beta_2,\cdots,\beta_{m-k},\cdots,\beta_{m-1},\Delta x_m(0)$ 不全为零，从而由式(1)得

$$\begin{aligned}p(\Delta x(m)=\beta|\Delta x(0)=\alpha)&=p(\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\beta_{m-1})\\&\cdot p(\beta_{m-1}\to\Delta x_{m-2}(0)\oplus\beta_{m-2})\cdots\\&\cdot p(\beta_{m-k}\to\Delta x_{m-k-1}(0)\oplus\beta_{m-k-1})\cdots\\&p(\beta_2\to\Delta x_1(0)\oplus\beta_1)\cdot p(\beta_1\to\Delta x_m(0)\oplus\beta_m)\le p_{\max}\end{aligned}$$

(2) 当迭代圈数 $s>m$ 时，对 $\forall \alpha\neq 0$ 及 β 有

$$\begin{aligned}
&p(\Delta x(s)=\beta\,|\,\Delta x(0)=\alpha)\\
&\quad=\sum_{\Delta x(s-m)} p(\Delta x(s)=\beta,\Delta x(s-m)\,|\,\Delta x(0)=\alpha)\\
&\quad=\sum_{\Delta x(s-m)} p(\Delta x(s)=\beta\,|\,\Delta x(s-m),\Delta x(0)=\alpha)\\
&\qquad\cdot p(\Delta x(s-m)\,|\,\Delta x(0)=\alpha)\\
&\quad=\sum_{\Delta x(s-m)} p(\Delta x(s)=\beta\,|\,\Delta x(s-m))\cdot p(\Delta x(s-m)\,|\,\Delta x(0)=\alpha)\\
&\quad\le p_{\max}\cdot\sum_{\Delta x(s-m)} p(\Delta x(s-m)\,|\,\Delta x(0)=\alpha)=p_{\max}
\end{aligned}$$

其中倒数第 3 步用到了引理 1。 证毕

为以下证明方便，设 m 分组非平衡 Feistel 网络的连续 $2m$ 圈差分对应依次为 $(\Delta x_1(0),\Delta x_2(0),\cdots,\Delta x_m(0))\to\cdots\to(\Delta x_1(2m),\Delta x_2(2m),\cdots,\Delta x_m(2m))=(\beta_1,\beta_2,\cdots,\beta_m)$ 其中对 $\forall i$, j, $0\le i\le 2m-1$，$1\le j\le m-2$，$\Delta x_m(i)=\Delta x_1(i+1)$，$\Delta x_j(i)=\Delta x_{j+1}(i+1)$，从而相应的 f 函数的差分对应依次为

$$\begin{aligned}
&\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1),\ \Delta x_m(1)\to\Delta x_{m-2}(0)\oplus\Delta x_m(2),\\
&\cdots,\ \Delta x_m(k)\to\Delta x_{m-k-1}(0)\oplus\Delta x_m(k+1),\cdots,\Delta x_m(m-1)\to\\
&\Delta x_m(0)\oplus\Delta x_m(m),\ \Delta x_m(m)\to\Delta x_m(1)\oplus\beta_{m-1},\cdots,\beta_l\to\\
&\Delta x_m(m-l+1)\oplus\beta_{l-1},\cdots,\ \beta_1\to\Delta x_m(m)\oplus\beta_m \qquad (2)
\end{aligned}$$

其中 $2\le k\le m-2$，$2\le l\le m-1$。

定理 4 设 m 分组非平衡 Feistel 网络 $Q_k(x_1,\cdots,x_{m-1},x_m)=(x_m,x_1,\cdots,x_{m-2},f(k,x_m)\oplus x_{m-1})$ 满足引理 1 中的条件，则 $s(s\ge 2m)$ 圈非平凡差分对应的概率不大于 $2p_{\max}^2$。

证明 (1)先证对 $\forall\alpha\neq 0$ 及 β 有 $p(\Delta x(2m)=\beta\,|\,\Delta x(0)=\alpha)\le 2p_{\max}^2$。

为方便起见，在本定理证明过程中约定 $\Delta x_0(0)=\Delta x_m(0)$。由定理 2 及式（2）知 $\Delta x_m(1),\cdots,\Delta x_m(m)$ 中至少有一个非零，记

$$\begin{aligned}
B_1=\{&(\Delta x_m(1),\cdots,\Delta x_m(m))\,|\,\Delta x_m(1),\cdots,\Delta x_m(m)\\
&\text{中至少有两个非零}\}\\
B_2=\{&(\Delta x_m(1),\cdots,\Delta x_m(m))\,|\,\Delta x_m(1),\cdots,\Delta x_m(m)\\
&\text{中仅有一个非零}\}
\end{aligned}$$

(a) $(\Delta x_m(1),\cdots,\Delta x_m(m))\in B_1$ 时，显然有

$$\prod_{n=1}^{m-1} p(\Delta x_m(n)\to\Delta x_{m-n-1}(0)\oplus\Delta x_m(n+1))\cdot p(\Delta x_m(m)\to\Delta x_m(1)\oplus\beta_{m-1})\le p_{\max}^2$$

从而由式(2)得

$$\begin{aligned}
p_1&=p(\Delta x(2m)=\beta,(\Delta x_m(1),\cdots,\Delta x_m(m))\in B_1\,|\,\Delta x(0)=\alpha)\\
&=\sum_{\Delta x_m(m)}\sum_{\Delta x_m(m-1)}\cdots\sum_{\Delta x_m(1)} p(\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1))\\
&\quad\cdot\prod_{n=1}^{m-1} p(\Delta x_m(n)\to\Delta x_{m-n-1}(0)\oplus\Delta x_m(n+1))\\
&\quad\cdot p(\Delta x_m(m)\to\Delta x_m(1)\oplus\beta_{m-1})
\end{aligned}$$

$$\begin{aligned}
&\cdot\prod_{l=2}^{m-1} p(\beta_l\to\Delta x_m(m-l+1)\oplus\beta_{l-1})\cdot p(\beta_1\to\Delta x_m(m)\oplus\beta_m)\\
&\le p_{\max}^2\cdot\sum_{\Delta x_m(m)} p(\beta_1\to\Delta x_m(m)\oplus\beta_m)\cdots\\
&\sum_{\Delta x_m(m-l+1)} p(\beta_l\to\Delta x_m(m-l+1)\oplus\beta_{l-1})\cdots\\
&\sum_{\Delta x_m(1)} p(\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1))=p_{\max}^2
\end{aligned}$$

(b) $(\Delta x_m(1),\cdots,\Delta x_m(m))\in B_2$ 时，不妨设对某个 p, $1\le p\le m$, $\Delta x_m(p)\neq 0$，而对 $\forall k$, $1\le k\le m$, $k\neq p$, $\Delta x_m(k)$ 均为零。$p>1$ 时，由 $\Delta x_m(p-1)\to\Delta x_{m-p}(0)\oplus\Delta x_m(p)$ 及 $\Delta x_m(p-1)=0$ 知 $\Delta x_m(p)=\Delta x_{m-p}(0)$；$p=1$ 时，由 $\Delta x_m(m)\to\Delta x_m(1)\oplus\beta_{m-1}$ 及 $\Delta x_m(m)=0$ 知 $\Delta x_m(1)=\Delta x_m(p)=\beta_{m-1}$。故不论 p 为何值，$\Delta x_m(1),\cdots,\Delta x_m(m)$ 均为定值。再由定理 2 及式(2)知 $\Delta x_m(0),\Delta x_m(1),\cdots,\Delta x_m(m-1)$ 中至少有一个非零，$\Delta x_m(m),\cdots,\beta_l,\cdots,\beta_1$ 中至少有一个非零，从而对 $\forall\alpha\neq 0$ 及 β 有

$$\begin{aligned}
p_2&=p(\Delta x(2m)=\beta,(\Delta x_m(1),\cdots,\Delta x_m(m))\in B_2\,|\,\Delta x(0)=\alpha)\\
&=p(\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1))\\
&\quad\cdot p(\Delta x_m(1)\to\Delta x_{m-2}(0)\oplus\Delta x_m(2))\cdots\\
&\quad\cdot p(\Delta x_m(k)\to\Delta x_{m-k-1}(0)\oplus\Delta x_m(k+1))\cdots\\
&\quad\cdot p(\Delta x_m(m-1)\to\Delta x_m(0)\oplus\Delta x_m(m))\\
&\quad\cdot p(\Delta x_m(m)\to\Delta x_m(1)\oplus\beta_{m-1})\cdots\\
&\quad\cdot p(\beta_l\to\Delta x_m(m-l+1)\oplus\beta_{l-1})\cdots\\
&\quad\cdot p(\beta_1\to\Delta x_m(m)\oplus\beta_m)\le p_{\max}\cdot p_{\max}=p_{\max}^2
\end{aligned}$$

故 $p(\Delta x(2m)=\beta\,|\,\Delta x(0)=\alpha)=p_1+p_2\le p_{\max}^2+p_{\max}^2=2p_{\max}^2$。

(2) 当迭代圈数 $s>2m$ 时，仿定理 3 中 $s>m$ 时的情形即证。 证毕

定理 5 设 m 分组非平衡 Feistel 网络 $Q_k(x_1,\cdots,x_{m-1},x_m)=(x_m,x_1,\cdots,x_{m-2},f(k,x_m)\oplus x_{m-1})$ 满足引理 1 中的条件且轮函数 $f(k,x_m)$ 是双射，则 $s(s\ge 2m)$ 圈非平凡差分对应的概率不大于 $p_{\max}^2$。

证明 (1)先证对 $\forall\alpha\neq 0$ 及 β 有 $p(\Delta x(2m)=\beta\,|\,\Delta x(0)=\alpha)\le p_{\max}^2$。这一步分 4 种情形进行证明：（a）$\beta_1=0,\beta_2\neq 0$，（b）$\beta_1\neq 0,\beta_2=0$，（c）$\beta_1=\beta_2=0$，（d）$\beta_1\neq 0,\beta_2\neq 0$。因篇幅所限，只对第 1 种情形进行证明，其它情形同理可证。

当 $\beta_1=0,\beta_2\neq 0$ 时，由式(2)知此时 f 函数的差分对应依次为

$$\begin{aligned}
&\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1),\ \Delta x_m(1)\to\Delta x_{m-2}(0)\oplus\Delta x_m(2),\cdots,\\
&\Delta x_m(k)\to\Delta x_{m-k-1}(0)\oplus\Delta x_m(k+1),\cdots,\\
&\Delta x_m(m-1)\to\Delta x_m(0)\oplus\beta_m,\ \beta_m\to\Delta x_m(1)\oplus\beta_{m-1},\cdots,\\
&\beta_l\to\Delta x_m(m-l+1)\oplus\beta_{l-1},\cdots,\beta_2\to\Delta x_m(m-1),\ 0\to 0
\end{aligned}$$

因函数 $f(k,x_m)$ 是双射，故由 $\beta_2\to\Delta x_m(m-1)$ 及 $\beta_2\neq 0$

知 $\Delta x_m(m-1)\neq 0$。显然由 $\beta_2\neq 0$ 和 $\Delta x_m(m-1)\neq 0$ 知

$$p(\Delta x_m(m-1)\to\Delta x_m(0)\oplus\beta_m)\cdot p(\beta_m\to\Delta x_m(1)\oplus\beta_{m-1})$$
$$\cdot\prod_{l=3}^{m-1}p(\beta_l\to\Delta x_m(m-l+1)\oplus\beta_{l-1})\cdot p(\beta_2\to\Delta x_m(m-1))\le p_{\max}^2$$

从而由以上差分对应知

$$\begin{aligned}&p(\Delta x(2m)=\beta\,|\,\Delta x(0)=\alpha)\\&=\sum_{\Delta x_m(m-1)}\sum_{\Delta x_m(m-2)}\cdots\sum_{\Delta x_m(1)}p(\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1))\\&\cdot\prod_{n=1}^{m-3}p(\Delta x_m(n)\to\Delta x_{m-n-1}(0)\oplus\Delta x_m(n+1))\\&\cdot p(\Delta x_m(m-2)\to\Delta x_1(0)\oplus\Delta x_m(m-1))\\&\cdot p(\Delta x_m(m-1)\to\Delta x_m(0)\oplus\beta_m)\cdot p(\beta_m\to\Delta x_m(1)\oplus\beta_{m-1})\\&\cdot\prod_{l=3}^{m-1}p(\beta_l\to\Delta x_m(m-l+1)\oplus\beta_{l-1})\cdot p(\beta_2\to\Delta x_m(m-1))\\&\le p_{\max}^2\sum_{\Delta x_m(1)}p(\Delta x_m(0)\to\Delta x_{m-1}(0)\oplus\Delta x_m(1))\cdots\\&\sum_{\Delta x_m(n+1)}p(\Delta x_m(n)\to\Delta x_{m-n-1}(0)\oplus\Delta x_m(n+1))\cdots\\&\sum_{\Delta x_m(m-1)}p(\Delta x_m(m-2)\to\Delta x_1(0)\oplus\Delta x_m(m-1))=p_{\max}^2\end{aligned}$$

(2) 当迭代圈数 $s>2m$ 时，仿定理 3 中 $s>m$ 时的情形即证。　　证毕

4　对 m 分组非平衡 Feistel 网络的几点讨论

(1) 定理 4 和定理 5 在分组密码的抗差分攻击设计方面有重要的意义和应用。例如我们以 m 分组非平衡 Feistel 网络迭代 8 次的结果构成一个“大型”密码变换，并将函数 $f(k,x_m)$ 设计为双射，则由定理 5 知，该密码变换八圈非平凡差分对应的概率不超过 $p_{\max}^2$。

(2) 由定理 5 知，当函数 $f(k,x_m)$ 设计为双射时，差分概率的上界大大降低(去掉了因子 2)，从这个意义上讲，将 m 分组非平衡Feistel网络中的轮函数 $f(k,x_m)$ 设计为双射是合适的。

(3) 上述 m 分组非平衡Feistel网络可看作传统的Feistel网络的一个推广，从而也有人称其为广义 Feistel 网络。定理 4 的结论可看作对本文引言所述结论 2 (1)的推广。但对 m 分组非平衡 Feistel 网络而言，却没有得到与本文引言所述结论 2 (2)相应的推广后的结论。

(4) 文献[8,9]对一类广义 Feistel 网络进行了差分可证明安全性分析，但该文所指的广义 Feistel 网络与本文中的非平衡 Feistel 网络有本质的不同。文献[10]从随机性的角度对一类与本文中的 m 分组非平衡 Feistel 网络相似的密码模型进行了分析。但有关本文差分可证明安全性的结果却从未在公开文献中出现过。

5　结束语

本文对一类 m 分组非平衡 Feistel 网络的差分可证明安全性进行了研究和分析，对于更一般情形的非平衡 Feistel 网络安全性的研究与分析，还有待进一步解决。

参 考 文 献

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptsystems. *Journal of Cryptology*, 1991, 4(1): 3 – 72.

[2] Lai X, ,Massey J, Murphy S. Markov ciphers and differential cryptanalysis. Advances in Cryptology——EUROCRYPT'91, LNCS 547, Springer-Verlag, 1991: 17 – 38.

[3] Knudsen L R. Practically secure Feistel ciphers: Fast Software Encryption. LNSC 809, Berlin, Heidelberg, New York, Springer-Verlag, 1994: 211 – 221.

[4] Nyberg K, Knudsen L R. Provable security against a differential attack. *Journal of Cryptology*, 1995, 8(1): 27 – 38.

[5] Schneier B, Kelsey J. Unbalanced Feistel networks and block cipher design: Fast Software Encryption (Ed. D. Gollmann), LNCS 1039, Springer-Verlag, 1996: 121 – 144.

[6] Adams C. CAST-256, http:// www.nist.gov / aes.

[7] 吴文玲，贺也平. 一类广义 Feistel 密码的安全性评估. 电子与信息学报，2002, 24(9): 1177 – 1184.

[8] Kaneko Y, *et al*.. On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions. http://citeseer.nk.nec.com/ kaneko97provable, html.

[9] Nyberg K. Generalized Feistel networks. Advances in Cryptology-ASIACRYPT'96, Kyongju, Korea, Proceedings, Springer-Verlag, 1996: 91 – 104.

[10] Zheng Y, Matsumoto T, Imai H. On the construction of block ciphers provable secure and not relying on any unproven hypotheses. Advances in Cryptology——CRYPTO'89, LNCS 435, Springer-verlag, 1990: 461 – 480.

王念平：　男，1973 年生，博士生，主要研究领域为密码理论、应用数学.

金晨辉：　男，1965 年生，教授，博士生导师，主要研究领域为密码理论、信息安全.

李云强：　男，1968 年生，博士，副教授，主要研究领域为遗传算法、密码理论.