Camellia 的差分和线性迭代特征

李 超[1,2,3], 沈 静[1]
(1. 国防科技大学理学院数学与系统科学系, 湖南长沙 410073; 2. 国防科技大学计算机学院网络与信息安全研究所, 湖南长沙 410073;
3. 中国科学院计算机科学重点实验室, 北京 100080)

摘 要: Camellia 是 NESSIE 计划 2003 年公布的分组密码标准算法之一. 本文对 Camellia 的差分迭代特征和线性迭代特征进行分析, 发现了 P 置换及其逆置换对 3 轮和 4 轮迭代特征的影响, 找到了到目前为止最优的 3 轮和 4 轮差分和线性迭代特征, 并利用 4 轮最优差分和线性迭代特征, 给出了 r ($6 \leqslant r \leqslant 18$) 轮 Camellia 变体的差分特征概率和线性偏差概率, 其中 18 轮的差分特征概率为 2^{-296}, 线性偏差概率为 $2^{-141.32}$, 这些结果优于 Eli Biham 等人 2001 所得的结果.

关键词: 分组密码; Camellia; 差分迭代特征; 线性迭代特征; 置换
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2005) 08-1345-04

Differential and Linear Iterative Characteristics of Camellia

LI Chao[1,2,3], SHEN Jing[1]
(1. *Department of Mathematics and System Science, School of Science, NUDT, Changsha, Hunan* 410073, *China*;
2. *Institute of Network and Information Security, School of Compute, NUDT, Changsha, Hunan* 410073, *China*;
3. *Laboratory of Computer Science, Institute of Software, Chinese Academic of Science, Beijing* 100080, *China*)

Abstract: Camellia is one of standard block ciphers algorithms published in 2003 by the NESSIE project. We analyze differential iterative characteristics and linear iterative characteristics, and find how the permutation and its inverse permutation affect 3-round and 4-round iterative characteristics, and the best 3-round and 4-round differential and linear iterative characteristics are found by us. Usingthe best 4-round iterative characteristics, we construct r-round differential and linear characteristics of Camellia variant. The differential probability of the 18th round is 2^{-296}, and the linear bias is $2^{-141.32}$. These results are better than the results given by Eli Biham in 2001.

Key words: block cipher; Camellia; differential iterative characteristics; linear iterative characteristics; permutation

1 引言

继美国推出 AES(Advanced Encryption Standard) 计划以后, 欧洲于 2000 年 1 月启动了新欧洲签名、完整性和加密计划–NESSIE(New European Schemes for Signatures, Integrity, and Encryption) 计划, 以适应 21 世纪信息安全发展的全面需求. 该计划为期三年, 投资 33 亿欧元, 主要目的就是通过公开征集和进行公开的、透明的测试、评估提出一套高效的密码标准, 以保持欧洲工业界在密码学研究领域的领先地位. 和 AES 相比, NESSIE 涉及的范围更广, 这套标准不但有分组密码, 还包括序列密码、认证码、杂凑函数和数字签名等标准. 2001 年底, NESSIE 工作组在十七种候选的分组密码算法中, 选定了 IDEA、Khazad、MISTY1、Camellia、SHACAL、RC6、SAFER++ 等七种分组密码算法为分组密码的决赛算法, 在六种候选的序列密码算法中, 选定了 BMGL, SNOW, SOBER-t16, SOBER-t32 等四种序列密码算法作为序列密码的决赛算法. 2003 年 2 月 27 日, NESSIE 工作组公布了包括分组密码、认证码、杂凑函数和数字签名等在内的十七个标准算法, 其中 MISTY1、Camellia、SHACAL 三个分组密码算法连同 AES 算法一起作为欧洲新世纪的分组密码标准算法.

Camellia 是一个明文分组 128 比特的 Feistel 型分组密码, 其密钥长度是可变的, 可为 128, 192 和 256 比特. 它由 18 轮 Feistel 结构的轮函数 $F[K^i]$, 初始及末尾白化和中间每隔 6 轮插入的逻辑函数 FL 和 FL^{-1} 组成的密码算法. 由于 FL 和 FL^{-1} 是与密钥有关的线性函数, 它们对差分密码分析[2] 和线性密码分析[3] 的影响不大[4], 故人们只考虑去掉 FL 和 FL^{-1} 后的 Camellia 变体的差分特征和线性特征. 文献[1] 构造了 Camellia 变体的 3 轮差分迭代特征, 利用 3 轮差分迭代特征, 给出了 5, 6, 7, 8 轮的差分特征概率分别为: 2^{-72}, 2^{-104}, 2^{-104} 和 2^{-130}, 进一步可以得到 18 轮 Camellia 变体的差分特征概率

收稿日期: 2003-11-26; 修回日期: 2005-05-23
基金项目: 中国科学院计算机科学重点实验室开放基金(No. SYSKF0402); 国防科技大学基础研究基金

为 2^{-308}; 文献[5]给出了 16 轮 Camellia 变体的差分特征概率的上界为 2^{-128}, 线性偏差概率的上界为 2^{-65}; 文献[6]给出了 10 轮 Camellia 变体的差分特征概率的上界为 2^{-128}, 线性偏差概率的上界为 2^{-65}. 本文得到了 Camellia 变体到目前为止最优的3 轮和 4 轮差分迭代特征和线性迭代特征, 并利用 3 轮和4 轮差分和线性迭代特征, 构造了任意轮的差分特征概率和线性偏差概率, 结果表明: 利用 4 轮差分和线性迭代特征得到的结果优于利用 3 轮差分和线性迭代特征得到的结果[1].

2 Camellia 的轮函数

Camellia 的轮函数是 SPN 型的, 它由与密钥异或, S 盒替换和 P 置换三部分组成, 且采用了宽轨迹策略, 变换 都是作用在字节上的.

Camellia 的轮函数表示为: $F[K]=P\circ S\circ\sigma[K]$(下面的带有下标的字母表示一个字节). 这里:

• $\sigma[K]$是密钥异或映射

$$\sigma[K](Y)=Y'\Leftrightarrow y'_i=y_i\oplus k_i \qquad i=1,2,3,4,5,6,7,8$$

• S 盒替换是由 8 个 S 盒组成的映射. 这 8 个 S 盒来自 4 个不同的 S 盒(S_1, S_2, S_3, S_4). S_i 是 8×8 的 S 盒. 每个 S 盒最大的差分概率是 2^{-6}, 最大线性偏差是 2^{-4}.

$$S: GF(2^8)^8\rightarrow GF(2^8)^8$$

$$(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)\rightarrow(S_1(x_1),S_2(x_2),S_3(x_3),S_4(x_4),S_2(x_5),S_3(x_6),S_4(x_7),S_1(x_8))$$

• $\boldsymbol{P}$ 置换是线性映射

$$\boldsymbol{P}: GF(2^8)^8\rightarrow GF(2^8)^8$$

$$\begin{pmatrix}z'_8\\z'_7\\\vdots\\z'_1\end{pmatrix}=\boldsymbol{P}\begin{pmatrix}z_8\\z_7\\\vdots\\z_1\end{pmatrix}$$

$\boldsymbol{P}$ 置换及其逆置换如下:

$$\boldsymbol{P}=\begin{bmatrix}0&1&1&1&1&0&0&1\\1&0&1&1&1&1&0&0\\1&1&0&1&0&1&1&0\\1&1&1&0&0&0&1&1\\0&1&1&1&1&1&1&0\\1&0&1&1&0&1&1&1\\1&1&0&1&1&0&1&1\\1&1&1&0&1&1&0&1\end{bmatrix}\quad \boldsymbol{P}^{-1}=\begin{bmatrix}1&1&1&0&1&0&0&1\\0&1&1&1&1&1&0&0\\1&0&1&1&0&1&1&0\\1&1&0&1&0&0&1&1\\0&1&1&1&0&1&1&1\\1&0&1&1&1&0&1&1\\1&1&0&1&1&1&0&1\\1&1&1&0&1&1&1&0\end{bmatrix}$$

3 差分迭代特征

为研究 Camellia 变体的差分和线性迭代特征, 我们引进如下记号:

(1)"–"表示概率为 1 的平凡特征; A, B 等大写字母表示某一轮的轮特征.

(2)ΔX^A, ΔY^A 表示 A 轮的输入差分和输出差分, ΔZ^A 表示 A 轮 S 盒的输出差分. 三者之间的关系为 $\Delta Z^A=S(\Delta X^A)$, $\Delta Y^A=P(\Delta Z^A)$. 这里 $\Delta X=(\Delta x_1,\cdots,\Delta x_8)$, Δx_i 表示第 i 个 S 盒的差分.

(3)ΓX^A, ΓY^A 表示 A 轮的输入选择模式和输出选择模式. ΓZ^A 表示 A 轮 S 盒的输出选择模式. 三者之间的关系为 $\Gamma Z^A=S(\Gamma X^A)$, $\Gamma Z^A=\boldsymbol{P}^T(\Gamma Y^A)$, $\boldsymbol{P}^T$ 是 $\boldsymbol{P}$ 的转置. 这里 $\Gamma X=(\Gamma x_1,\cdots,\Gamma x_8)$, Γx_i 表示第 i 个 S 盒的选择模式.

(4)[Φ] 表示全 0 字节, [I] 表示 8 个字节取值情况. 如 [12, 0, 0, 0, 0, 0, 0, 0]. $X[I]$ 表示 I 中的每个字节转换成二进制后, 非 0 比特对应的位置异或之和.

定义 **1** 输入差分不为 0 的 S 盒称为差分活跃 S 盒; 输出选择模式不为 0 的 S 盒称为线性活跃 S 盒.

定义 **2** 在 SPN 型轮函数中, 差分分支数定义如下:

$$B_d=\min_{\Delta X\neq 0}(H_w(\Delta X)+H_W(P(\Delta X)))$$

其中 ΔX 是输入差分, P 是扩散层.

定义 **3** 在 SPN 型轮函数中, 线性分支数定义如下:

$$B_l=\min_{\Gamma Y\neq 0}(H_w(\Gamma Y)+H_W(P^*(\Gamma Y)))$$

其中 ΓY 是输出选择模式, $P^*(\Gamma Y)$ 是扩散层的输入选择模式.

文献[5]表明: Camellia 的 P 置换的差分分支数和线性分支数均为 5.

定义 **4** 如果有差分列:

$$\Delta Y_m,\Delta Y_{m+1},\cdots,\Delta Y_{m'} \qquad (1)$$

ΔY_m 经过 $\Delta Y_i(m<i<m')$得到 $\Delta Y_{m'}$的概率 p, 称式(1)为 $m'-m+1$ 轮特征.

定义 **5** 如果特征式(1)满足如下条件:

$$([\Phi],[I]),\Delta Y_m,\Delta Y_{m+1},\cdots,\Delta Y_{m'},([J],[\Phi]) \qquad (2)$$

且中间不包含概率为 0 的特征, 称式(2)为 $m'-m+1$ 轮差分迭代特征.

引理 **1**[5] 设 $\boldsymbol{P}$ 是 $GF(2)^m$ 上的 $n\times n$ 可逆矩阵. 当置换 $\boldsymbol{P}$ 满足: $[y_i]^t=[P_{ij}][z_j]^t$, 那么下列关系成立:

$$[\Delta y_i]^t=[P_{ij}][\Delta z_j]^t,[\Gamma z_i]^t=[P_{ji}][\Gamma y_i]^t$$

由定义 4 和定义 5 知, 没有一轮差分迭代特征, 从引理 1 可以看出, 差分和线性特征都与 P 置换有关.

定理 **1** 轮函数是 SPN 型的 Feistel 型密码没有两轮差分迭代特征.

证明: 假如存在两轮迭代特征, 那么两轮差分迭代特征的形式如下:

$$([\Phi],[\Delta X])$$
$$A:[\Phi]\leftarrow[\Delta X]$$
$$([\Delta X],[\Phi])$$

其中 ΔX 是输入差分, 不能为全 0 比特, ΔY 是输出差分, 为全 0 比特, 用[Φ] 表示. 令 $\Delta Z=S(\Delta X)$, 则 $\Delta Y=P(\Delta Z)=P(S(\Delta X))$. 由引理 1 知 $[\Delta z_i]^t=[P_{ij}^{-1}][\Delta y_j]^t$, 故 ΔZ 为全 0 比特, 又由于 S 盒是双射, 要使 A 的概率不为 0, 则 ΔX 必为全 0 比特, 矛盾. 从而轮函数为 SPN 型的 Feistel 型密码不存在两轮迭代特征.

这一点与 DES 密码是不同的, 由于 DES 的 S 盒不是双射, 故存在这样 $A:[\Phi]\leftarrow[\Delta X]$概率不为 0 的特征.

3 轮差分迭代特征要满足如下形式:

$$([\Phi],[\Delta X])$$
$$A:[\Delta Y]\leftarrow[\Delta X]$$

$$B:[\Delta X]\leftarrow[\Delta Y]$$
$$([\Delta Y],[\Phi])$$

定理 **2**　在构造 3 轮差分迭代特征时, 轮特征 A 中不可能恰有一个差分活跃 S 盒.

证明: 令 $sign((x_1,\cdots,x_8))=(a_1,\cdots,a_8)$,

$$a_i=\begin{cases}0, & x_i=0\\ x, & x_i\neq 0\end{cases}$$

用 ΔX^A, ΔY^A 表示轮特征 A 的输入输出差分, 用 ΔX^B, ΔY^B 表示轮特征 B 的输入输出差分. 根据 3 轮差分迭代特征的要求有: $\Delta X^A=\Delta Y^B=\Delta X$, $\Delta Y^A=\Delta X^B=\Delta Y$.

假如 $A:[\Delta Y^A]\leftarrow[\Delta X^A]$ 中只有一个差分活跃 S 盒. 不妨设第 i 个 S 盒的输入差分不为 0, 其余 S 盒的输入差分全为 0, 即 ΔX^A 的第 i 个字节不为 0, 其余均为 0. 经过 S 替换后, ΔZ^A 的第 i 个字节不为 0, 其余都为 0. 经过 P 置换后, $sign(\Delta Y^A)$ 与矩阵 $\boldsymbol{P}$ 的第 9– i 列相等, 又 $\Delta Y^B=\Delta X^A$, $\Delta Z^B=\boldsymbol{P}^{-1}(\Delta Y^B)$, 故 $sign(\Delta Z^B)$ 与矩阵 $\boldsymbol{P}^{-1}$ 的第 9– i 列相等. 而 S 盒是双射, 故 $sign(\Delta Z^B)=sign(\Delta X^B)$, 又 $\Delta X^B=\Delta Y^A$, $sign(\Delta X^B)=sign(\Delta Y^A)$, 所以有 $sign(\Delta Z^B)=sign(\Delta Y^A)$, 即矩阵 $\boldsymbol{P}$ 的第 9 – i 列要与矩阵 $\boldsymbol{P}^{-1}$ 的第 9– i 列相等. 经过观察, 我们发现矩阵 $\boldsymbol{P}$ 和矩阵 $\boldsymbol{P}^{-1}$ 对应的列没有相等的, 矛盾! 故轮特征 A 中不可能只有一个活跃 S 盒.

定理 **3**　3 轮差分迭代特征中的活跃 S 盒超过 5 个.

证明: 用 (a,b) 表示 A, B 中有活跃 S 盒的数目. 假如 3 轮差分迭代特征中有 5 个活跃 S 盒, (a,b) 的取值只有 $(1,4)$, $(4,1)$, $(2,3)$, $(3,2)$.

由于 A, B 的对称性, 我们只需考虑 $(1,4)$, $(2,3)$ 两种情况. 而 $(1,4)$ 这种情况通过定理 2 就排除了. 而满足 3 轮迭代特征的必要条件是 $sign(\Delta Z^B)=sign(\Delta Y^A)$.

当特征 A 中有两个差分活跃 S 盒时, 不妨设第 i_1, i_2 个 S 盒为活跃 S 盒, 有下列四种情况:

(1) $\Delta X^A_{i1}=\Delta X^A_{i2}$, $\Delta Z^A_{i1}=\Delta Z^A_{i2}$.

(2) $\Delta X^A_{i1}=\Delta X^A_{i2}$, $\Delta Z^A_{i1}\neq\Delta Z^A_{i2}$.

(3) $\Delta X^A_{i1}\neq\Delta X^A_{i2}$, $\Delta Z^A_{i1}=\Delta Z^A_{i2}$.

(4) $\Delta X^A_{i1}\neq\Delta X^A_{i2}$, $\Delta Z^A_{i1}\neq\Delta Z^A_{i2}$.

因为, $\Delta X^A_{i1}=\Delta X^A_{i2}$, $sign(\Delta Z^B)$ 的值等于矩阵 $\boldsymbol{P}^{-1}$ 第 9– i_1 列和第 9– i_2 列的异或, $\Delta Z^A_{i1}=\Delta Z^A_{i2}$, $sign(\Delta Y^A)$ 的值等于矩阵 $\boldsymbol{P}$ 的第 9– i_1 列和第 9– i_2 列的异或. 而矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{P}^{-1}$ 矩阵任意两个互相对应的列异或都没有相等的, 情形 (1) 被排除掉.

当 $\Delta Z^A_{i1}\neq\Delta Z^A_{i2}$ 时, $sign(\Delta Y^A)$ 的值等于矩阵 $\boldsymbol{P}$ 的第 9– i_1 列和第 9– i_2 列的取并后的值. 我们发现要满足 $sign(\Delta Z^B)=sign(\Delta Y^A)$ 条件, B 中至少有 7 个活跃 S 盒.

同样地, 当 $\Delta X^A_{i1}\neq\Delta X^A_{i2}$, $sign(\Delta Z^B)$ 的值等于矩阵 $\boldsymbol{P}^{-1}$ 的第 9– i_1 列和第 9– i_2 列的取并后的值, 故满足条件的 B 中至少有 7 个活跃 S 盒.

文献[5] 在估计特征列“ – AB – ”的差分特征概率上界时, 要求活跃 S 盒的个数达到分支数. 由于 $sign(\Delta Z^B)=sign(\Delta Y^A)$ 的限制, 选取好的 P 置换, 差分概率特征就达不到上界, 因此文献[5] 中差分概率特征的上界在 Camellia 变体中是达不到的.

经过分析, 我们发现 3 轮差分迭代特征含有最少活跃 S 盒的情况为: A 中含有 4 个活跃 S 盒, B 中含有 4 个活跃 S 盒. 由于 Camellia 的 S 盒的最大差分概率是 2^{-6}, 活跃 S 盒的数目起决定性的作用. 我们首先找到满足 $sign(\Delta Z^B)=sign(\Delta Y^A)$ 条件的 S 盒的位置, 然后再用穷尽的方法搜索 3 轮最优迭代特征, 大大减少了寻找 3 轮迭代特征的计算量. 按照我们的方法, 我们找到了到目前为止 3 轮最优差分迭代特征, 其概率为 2^{-52} (此结果和文献[1] 的结果一样). 特征如下:

$A:[204,0,39,0,39,0,204,0]\leftarrow[204,0,39,0,39,0,204,0]$

$B:[204,0,39,0,39,0,204,0]\leftarrow[204,0,39,0,39,0,204,0]$

4 轮差分迭代特征的形式如下:

$$([\Phi],[\Delta X])$$
$$A:[\Delta Y]\leftarrow[\Delta X]$$
$$B:[\Delta X\ominus\Delta X']\leftarrow[\Delta Y]$$
$$C:[\Delta Y]\leftarrow[\Delta X']$$
$$([\Delta X'],[\Phi])$$

从特征 A, C 可以看出, $sign(\Delta X)=sign(\Delta X')$, 且 $\Delta X\ominus\Delta X'\neq 0$, 否则 B 的概率为 0. 类似 3 轮迭代特征的分析方法, 我们发现 4 轮迭代特征中轮特征 A 中不可能只有一个活跃 S 盒, 当 $sign(\Delta X,\Delta X')=sign(\Delta X)=sign(\Delta X')$, 与 3 轮差分迭代特征的情况一样考虑. 找到满足 3 轮差分迭代特征的 S 盒的位置, 在此基础上就能构造 4 轮差分迭代特征. 4 轮差分迭代特征至少有 11 个差分活跃 S 盒. 同样, 我们找到了到目前为止 4 轮最优差分迭代特征, 其概率为 2^{-71}, 特征如下:

$A:[3,148,148,151,148,151,0,3]\leftarrow[11,1,0,0,0,0,0,0]$

$B:[150,210,0,0,0,0,0,0]\leftarrow[3,148,148,151,148,151,0,3]$

$C:[3,148,148,151,148,151,0,3]\leftarrow[157,211,0,0,0,0,0,0]$

我们利用 4 轮差分迭代特征构造了 18 轮差分特征, 结果如下:

$$-ABC-CBA-ABC-CBA-D$$

其中 $D:[218,57,57,227,57,227,0,218]\leftarrow[11,1,0,0,0,0,0,0]$, 概率为 2^{-12}. 故用 4 轮差分迭代特征构造 18 轮差分特征的概率为 2^{-296}, 优于利用 3 轮迭代特征构造的 18 轮差分特征概率 2^{-308}[1]. 表 1 是 r 轮差分特征的概率分布的情况 (** 表示轮特征是最优的特征, * 表示轮特征是用 4 轮最优差分迭代特征构造的, 是局部最优).

表 **1**　r 轮差分特征的概率分布

r	概率	r	概率	r	概率
3	2^{-12}**	8	2^{113}*	13	2^{-202}*
4	2^{-42}**	9	2^{131}*	14	2^{-225}*
5	2^{-60}**	10	2^{154}*	15	2^{-237}*
6	2^{-83}*	11	2^{-166}*	16	2^{-255}*
7	2^{-95}*	12	2^{-184}*	17	2^{-273}*

4　线性迭代特征

定义 **6**　如果下列等式:

$$X_m(I)\ominus X_{m+1}[I']\ominus X_{m'}[J]\ominus X_{m'+1}[J']=\bigoplus_{t=m+1}^{m'}K_t[I_{K_t}] \tag{3}$$

成立的概率 $p\neq 1/2$, 称式 (3) 为 $m'-m+1$ 轮线性特征. 如果

式(3)能简化为:

$$X_m[I] \oplus X_{m'+1}[J'] = \bigoplus_{t=m+1}^{m'} K_t[I_{K_t}] \quad (4)$$

称式(4)为 $m'-m+1$ 轮线性迭代特征.

由引理 1 以及差分特征和线性特征的对偶性[3]知,只要对 $\boldsymbol{P}$ 矩阵和 $\boldsymbol{P}^{-1}$ 矩阵的行进行考虑即可. 我们发现矩阵 $\boldsymbol{P}$ 和矩阵 $\boldsymbol{P}^{-1}$ 有这样的关系: $(p_{ij})^{-1}=(p_{9-j,9-i})$,故考虑行的情况与考虑列的情况是一致的,于是我们得到与差分迭代特征类似的结果.

定理 **4** 轮函数是 SPN 型的 Feistel 型密码没有两轮线性迭代特征.

定理 **5** 3 轮线性迭代特征 A 中不可能恰有一个线性活跃 S 盒.

定理 **6** 3 轮线性迭代特征中的线性活跃 S 盒超过 5 个.

找到了到目前为止 3 轮最优线性迭代特征,其概率为 $2^{-26.77}$. 特征如下:

$A:[0,110,0,186,0,186,0,110] \leftarrow [0,110,0,186,0,186,0,110]$

$B:[0,110,0,186,0,186,0,110] \leftarrow [0,110,0,186,0,186,0,110]$

我们找到了到目前为止 4 轮最优线性迭代特征,其概率为 $2^{-34.58}$. 特征如下:

$A:[18,85,0,71,85,71,18,18] \leftarrow [0,0,0,0,122,0,0,200]$

$B:[0,0,0,0,122,0,0,200] \leftarrow [91,176,0,235,176,235,91,91]$

$C:[73,229,0,172,229,172,73,73] \leftarrow [0,0,0,0,122,0,0,200]$

用 4 轮线性迭代特征构造了 18 轮线性特征,结果如下:

$$D-ABC-CBA-ABC-CBA-$$

其中 $D:[18,85,0,71,85,71,18,18] \leftarrow [0,0,0,0,77,0,0,103]$,概率为 2^{-7}. 故用 4 轮线性迭代特征构造 18 轮线性偏差概率为 $2^{-141.32}$,优于利用 3 轮迭代特征构造的 18 轮线性偏差概率为 $2^{-152.85}$. 表 2 是 r 轮线性特征的线性偏差概率分布的情况(** 表示轮特征是最优的特征,* 表示轮特征是用 4 轮最优线性迭代特征构造的,是局部最优).

表 **2** r 轮线性特征的线性偏差概率分布

r	线性偏差	r	线性偏差	r	线性偏差
3	2^{-7}**	8	$2^{-55.58}$*	13	$2^{-98.16}$*
4	2^{-21}**	9	$2^{-64.58}$*	14	$2^{-107.4}$*
5	2^{-31}**	10	$2^{-74.16}$*	15	$2^{-113.74}$*
6	$2^{-40.58}$**	11	$2^{-80.16}$*	16	$2^{-121.74}$*
7	$2^{-46.58}$**	12	$2^{-89.16}$*	17	$2^{-130.74}$*

5 结论

本文研究了 Camellia 变体的差分迭代特征和线性迭代特征,并用我们找到的 4 轮差分和线性迭代特征构造任意 r 轮的局部最优特征. 我们可以在局部最优特征的基础上,采用文献[7]中的方法继续寻找全局最优的特征. 同时我们也注意到轮函数是 SPN 型的 Feistel 型密码的 P 置换对迭代特征有很大的影响.

参考文献:

[1] Eli Biham, Orr Dunkelman, Vladimir Furman, Tal Mor. Preliminary Report on the Nessie Submissions: Anubis, Camellia, Khazad, IDEA, Misty1, NIMBUS, and Q* [R]. https://www.cosic.esat.kuleuven.ac.be/nessie/reports/, 2000.

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

[3] M Matsui. Linear cryptanalysis method for DES cipher[A]. Advances in Cryptology-EUROCRYT'93 Proceedings[C]. Berlin: Springer-verlag, 1994. 386-397.

[4] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita. Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms[S]. Copyright NTT and Mitsubishi Electric Corporation 2000-2002.

[5] Masayuki Kanda. Practical security evaluation against differential and linear cryptanalyses for feistel ciphers with SPN round function[A]. D R Stinson, S Tavares(Eds.): SAC 2000[C]. Berlin: Springer-verlag, 2001. 324-338.

[6] Taizo Shirai, Shoji Kamamaru, George Abe. Improved upper bounds of differential and linear characteristic probability for camellia [A]. J Daemen, V Rijmen(Eds.): FSE 2002[C]. Berlin: Springer-verlag, 2002. 128-142.

[7] Mitsuru Matsui. On correlation between the order of S-boxes and the strength of DES[A]. Advances in Cryptology-EUROCRYPT'94[C]. Berlin: Springer-verlag, 1995. 366-375.

作者简介:

李 超 男,1966 年生于湖南省汨罗市,国防科技大学数学与系统科学系教授,博士生导师,目前主要从事编码与密码方面的研究. E-mail: lichao.nudt@sina.com.

沈 静 女,1980 年生于湖北省随州市,硕士研究生,目前的研究方向为分组密码的设计与分析.