# 对低轮 CLEFIA 分组密码的碰撞 - Square 攻击

韩 敬[1],张文英[1,2],徐小华[3]

(1. 山东师范大学信息科学与工程学院,山东济南 250014;
2. 中国科学院研究生院信息安全国家重点实验室,北京 100049;3. 济南 72241 部队,山东济南 250029)

**摘 要**: CLEFIA 是由 SONY 公司最近开发研制的一种高效率,高度安全的分组加密算法. 该算法采用广义 Feistel 结构,本文给出了 CLEFIA 的一个等价结构图,把碰撞攻击和 Square 攻击的思想相结合成功分析了 6 轮 CLEFIA,在普通 PC 机上两个小时之内即可完全恢复密钥.

**关键词**: CLEFIA; 分组密码; 碰撞攻击; Square 攻击

**中图分类号**: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2009) 10-2309-05

## Collision-Square Attacks on the Reduced-Round CLEFIA

HAN Jing[1], ZHANG Wen-ying[1,2], XU Xiao-hua[3]

(1. *School of Information Science and Engineering, Shandong Normal University, Jinan* 250014 *China*;
2. *State Key Lab of Information Security, Chinese Academy of Sciences, Beijing* 100080, *China*;
72241 *Troops, Jinan, Shandong* 250029, *China*)

Abstract: CLEFIA is an efficient, highly secure block cipher which is proposed by SONY corporation recently. CLEFIA employs a generalized Feistel structure which contains 4-branch data lines. This paper presents an equivalent structure of CLEFIA. By adopting Collision-Square attack, we recover the key of 6 round successfully within 2 hours in the ordinary PC.

Key words: CLEFIA, ; block cipher; collision attack; Square-attack

## 1 引言

CLEFIA[1]是由 SONY 公司最近研制开发的一种分组加密算法,旨在用来保护 SONY 公司的音乐和图像等数字内容的发行和进行“高级”版权保护与认证技术. 自 CLEFIA 被公布的一年多时间里,国内外学者用各种方法分析了 CLEFIA 的安全性,文献[2]对 CLEFIA 进行了不可能差分分析,其对 12 轮 128 比特 CLEFIA 攻击时间复杂度为 $2^{119}$;文献[3]对 CLEFIA 进行了诱导故障分析,提出了一种攻击模型;文献[4]对 CLEFIA 进行了不可能差分分析,其结果表明,可以用比 Sony 公司自己的评估报告所声称的复杂度小的时间和存储复杂度来分析 CLEFIA. 以上攻击方法都证明了算法并不像设计者所声称的那样安全. 我们也曾经提出了对 14 轮 CLEFIA 的一个分析思路[5].

本文将碰撞攻击方法[6,7]和 Square 攻击方法[8]相结合,成功的实现了对 6 轮 CLEFIA 的攻击. 整个攻击过程在普通 PC 机上不到两个小时即可完全恢复密钥.

## 2 CLEFIA 的简单描述

CLEFIA 的分组长度为 128 比特,支持 128,192,256 比特三种规模的密钥长度. 本文只研究 128 比特分组长度的 CLEFIA. 与传统的 Feistel 结构不同的是 CLEFIA 采用了 Feistel 结构的变种,它有四个分支(如图 1 左图),而传统的 Feistel 结构都有左右两组输入. 设 $T_0$, $T_1$, $T_2$, $T_3$ 为第 $r$ 轮的输入,则轮变换可以表示为:

$$T_1^{\,r},\ T_3^{\,r} \leftarrow T_2^{\,r-1},\ T_0^{\,r-1};$$

$$T_0^{\,r},\ T_2^{\,r} \leftarrow M_0[S(RK_{2i} \oplus T_0^{\,r-1})] \oplus T_1^{\,r-1},$$

$$M_1[S'(RK_{2i+1} \oplus T_2^{\,r-1})] \oplus T_3^{\,r-1}.$$

其中 $RK_{2i}$, $RK_{2i+1}$ 为第 $i$ 轮的子密钥,$M_0 S$, $M_1 S$ 为轮函数,$S$, $S$ 和 $M_0$, $M_1$ 如下定义:

$$S: F_2^{32} \leftarrow F_2^{32};$$

$$l_{1(8)} \mid l_{2(8)} \mid l_{3(8)} \mid l_{4(8)} \leftarrow S_0(l_{1(8)}) \mid S_1(l_{2(8)}) \mid S_0(l_{3(8)}) \mid S_1(l_{4(8)});$$

$$S': F_2^{32} \leftarrow F_2^{32};$$

$$l_{1(8)} \mid l_{2(8)} \mid l_{3(8)} \mid l_{4(8)} \leftarrow S_1(l_{1(8)}) \mid S_0(l_{2(8)}) \mid S_1(l_{3(8)}) \mid S_0(l_{4(8)}).$$

$$M_0 = \begin{pmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{pmatrix},\ M_1 = \begin{pmatrix} 01 & 08 & 02 & 0a \\ 08 & 01 & 0a & 02 \\ 02 & 0a & 01 & 08 \\ 0a & 02 & 08 & 01 \end{pmatrix}$$

收稿日期:2008-11-16;修回日期:2009-05-26
基金项目:国家自然科学基金(No.60673068);山东省自然科学基金(No.Y2008g01)

矩阵与向量的乘法是在模 $x^8+x^4+x^3+x^2+1$ 的有限域 $GF^8(2)$ 上进行的.

CLEFIA的密钥编排方法是首先由种子密钥生成128比特的 $L$,再由 $L$ 及原始密钥生成轮密钥 $RK_i$, $i=0,1,\cdots,35$,这里就不再详细描述,详见文献[1].

**定理1** 矩阵 $M_0$ 和 $M_1$ 都是自逆的,即

$$M_0^{-1}=M_0,\ M_1^{-1}=M_1.$$

**证明** 事实上有限域 $F_2^n$ 上所有形如

$$M=\begin{pmatrix}1 & a & b & a+b\\ a & 1 & a+b & b\\ b & a+b & 1 & a\\ a+b & b & a & 1\end{pmatrix}$$

的矩阵都是自逆的,这是因为

$$(1,a,b,a+b)(1,a,b,a+b)^{\mathrm{T}}$$
$$=1+a^2+b^2+(a+b)^2=1,$$
$$(1,a,b,a+b)(a,1,a+b,b)^{\mathrm{T}}$$
$$=a+a+b(a+b)+(a+b)b=0,$$
$$(1,a,b,a+b)(b,a+b,1,a)^{\mathrm{T}}$$
$$=b+a(a+b)+(a+b)a=0,$$
$$(1,a,b,a+b)(a+b,b,a,1)^{\mathrm{T}}$$
$$=a+b+ab+ba+a+b=0.$$

而这里的 $M_0$, $M_1$ 恰好全是形如 $M$ 的矩阵,所以都是自逆的.

## 3 CLEFIA的等价结构

为了应用对传统的Feistel结构分组密码的分析方法,我们给出CLEFIA的传统Feistel形式的等价结构(如图1右图).

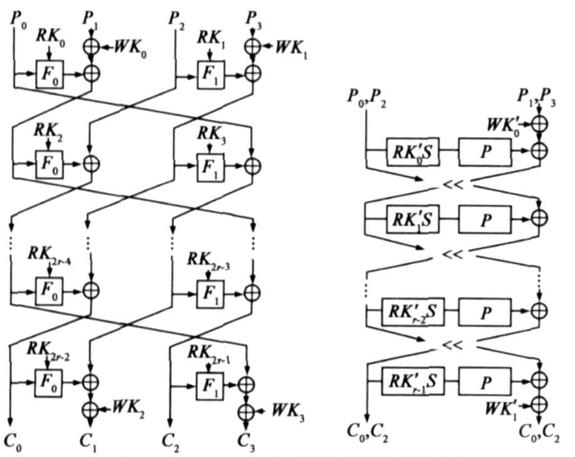


图1 CLEFIA加密流程及等价结构图

等价结构图中 $P=P_L\|P_R$ 表示明文, $P_L=P_0\|P_2$ 表示明文的左半输入,由原结构图中明文的下标为偶数的字级联而成, $P_R=P_1\|P_3$ 表示明文的右半输入由原结构图中明文的下标为奇数的字级联而成, $RK'_i=RK_{2i}\|RK_{2i+1}$, $0\le i\le r-1$ 是原算法中第 $i$ 轮中的64比特密钥, $WK'_i=WK_{2i}\|WK_{2i+1}$, $i=0,1$ 是原算法中第一轮之前和最后一轮之后的白化密钥.

## 4 四轮区分器

$L_{r-1}$, $R_{r-1}$ 为第 $r$ 轮的输入,选取

$$L_0=P_0\|P_2=(\alpha_1,\alpha_2,\cdots,\alpha_8),$$
$$R_0=P_1\|P_3=(x,\beta_2,\cdots,\beta_8),$$

其中 $x$ 取自 $F_2^8$, $a_i$, $\beta_i$ 均是常数,第一轮的输出为

$$L_1=[M_0(S_0(\alpha_1\oplus RK_0^1),S_1(\alpha_2\oplus RK_0^2),S_0(\alpha_3\oplus RK_0^3),S_1(\alpha_4\oplus RK_0^4))\|M_1(S_1(\alpha_5\oplus RK_1^1),S_0(\alpha_6\oplus RK_1^2),S_1(\alpha_7\oplus RK_1^3),S_0(\alpha_8\oplus RK_1^4))]\oplus(x,\beta_2,\cdots,\beta_8)\ @\ (x\oplus\gamma_1,\gamma_2,\cdots,\gamma_8)=T_1^0\|T_1^2,$$

$$R_1=(\alpha_5,\cdots,\alpha_8,\alpha_1,\cdots,\alpha_4)=T_1^1\|T_1^3 \quad (1)$$

在第二轮中, $L_1$ 经轮函数 $F$, $RK_2$, $RK_3$ 做如下变换:

$$L_1=(x\oplus\gamma_1,\gamma_2,\cdots,\gamma_8)\xrightarrow{F,RK_2,RK_3}(y\oplus\theta_1,02y\oplus\theta_2,04y\oplus\theta_3,06y\oplus\theta_4,\theta_5,\theta_6,\theta_7,\theta_8)$$

这里 $y=S_0(x\oplus\gamma_1\oplus RK_2^1)$,在子密钥取定的情况下, $\theta_1,\cdots,\theta_4$ 都是与 $RK_2$ 有关的常数, $\theta_5,\cdots,\theta_8$ 都是与 $RK_3$ 有关的常数,第二轮的输出为

$$L_2=(y\oplus w_1,02y\oplus w_2,04y\oplus w_3,06y\oplus w_4,w_5,w_6,w_7,w_8)=T_2^0\|T_2^2,$$

$$R_2=L_1<<32=(\gamma_5,\cdots,\gamma_8,x\oplus\gamma_1,\gamma_2,\gamma_3,\gamma_4)=T_2^1\|T_2^3 \quad (2)$$

其中 $w_i=\theta_i\oplus\alpha_{i+4}$. $i=1,\cdots,4$, $w_i=\theta_i\oplus\alpha_{i-4}$. $i=5,\cdots,8$ 均是常数.

在第三轮中, $L_2$ 经轮函数 $F$, $RK_4$, $RK_5$ 做如下变换:

$$L_2=(y\oplus w_1,02y\oplus w_2,04y_3\oplus,06y\oplus w_4,w_5,w_6,w_7,w_8)\xrightarrow{F,RK_4,RK_5}(f_1,\cdots,f_8).$$

第三轮的输出为:

$$L_3=[M_0(S_0(y\oplus w_1\oplus RK_4^1),S_1(02y\oplus w_2\oplus RK_4^2),S_0(04y\oplus w_3\oplus RK_4^3),S_1(06y\oplus w_4\oplus RK_4^4))\|M_1(S_1(w_5\oplus RK_5^1),S_0(w_6\oplus RK_5^2),S_1(w_7\oplus RK_5^3),S_0(w_8\oplus RK_5^4))]\oplus(\gamma_5,\cdots,\gamma_8,x\oplus\gamma_1,\gamma_2,\gamma_3,\gamma_4)$$
$$=(f_1\oplus\gamma_5,f_2\oplus\gamma_6,f_3\oplus\gamma_7,f_4\oplus\gamma_8,f_5\gamma_1,f_6\oplus\gamma_2,f_7\oplus\gamma_3,f_8\oplus\gamma_4)=T_3^0\|T_3^2,$$

$$R_3=L_2\ll32=(w_5,w_6,w_7,w_8,y\oplus w_1,02y\oplus w_2,04y\oplus w_3,06y\oplus w_4)=T_3^1\|T_3^3. \quad (3)$$

第四轮的输出的右半部分为:

$$R_4=L_3\ll32=[M_1(S_1(w_5\oplus RK_5^1),S_0(w_6\oplus RK_5^2),S_1(w_7\oplus RK_5^3),S_0(w_8\oplus RK_5^4))\|M_0(S_0(y\oplus w_1\oplus RK_4^1),S_1(02y\oplus w_2\oplus RK_4^2),$$

$$S_0(04y\oplus w_3\oplus RK_4^3),S_1(06y\oplus w_4\oplus RK_4^4))]$$
$$\oplus(x\oplus\gamma_1,\gamma_2,\gamma_3,\cdots,\gamma_8)$$
$$=(f_5\oplus x\oplus\gamma_1,f_6\oplus\gamma_2,f_7\oplus\gamma_3,f_8\oplus\gamma_4,f_1\oplus\gamma_5,f_2\oplus\gamma_6,f_3\oplus\gamma_7,f_4\oplus\gamma_8).\qquad(4)$$

## 5 具有 128 比特密钥的 6 轮 CLEFIA 的攻击

当我们在四轮区分器前后各加一轮,攻击 6 轮 CLEFIA 时,$R_5$ 就相当于四轮区分器中的 $R_4$,因此 $R_5$ 的各字节之间具有上述性质.在以下分析中,我们不考虑前期白化密钥加过程.在四轮区分器的前面再添加一轮,若取 $L_0=(\beta_5,\beta_6,\beta_7,\beta_8,i_0,\beta_2,\beta_3,\beta_4)$,则 $R_1=L_0\lll 32=(i_0,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$,这样 $R_1$ 满足了第一个字节活动其余字节固定的条件.此时,

$$R_0=L_1\oplus F(L_0,RK_0,RK_1)$$
$$=(\theta_1,\cdots,\theta_4,S_1(i_0\oplus RK_1^1),08S_1(i_0\oplus RK_1^1),$$
$$02S_1(i_0\oplus RK_1^1),0aS_1(i_0\oplus RK_1^1)).$$

设第 6 轮的输出 $(L_6,R_6)=(l_1,\cdots,l_8,r_1,\cdots,r_8)$,经过六轮加密后其值是已知的,则 $L_5=R_6\lll 32=(r_5,\cdots,r_8,r_1,\cdots,r_4)$,

$$R_5=F(L_5,RK_{10},RK_{11})\oplus L_6$$
$$=[M_0(S_0(r_5\oplus RK_{10}^1),S_1(r_6\oplus RK_{10}^2),$$
$$S_0(r_7\oplus RK_{10}^3),S_1(r_8\oplus RK_{10}^4))$$
$$|M_1(S_1(r_1\oplus RK_{11}^1),S_0(r_2\oplus RK_{11}^2),$$
$$S_1(r_3\oplus RK_{11}^3),S_0(r_4\oplus RK_{11}^4))]$$
$$\oplus(l_1,\cdots,l_8),$$

因为此时的 $R_5$ 相当于四轮区分器中的 $R_4$,所以 $R_5$ 的前四个字节满足如下关系:

$$M_0[S_0(r_5\oplus K_{10}^1),S_1(r_6\oplus RK_{10}^2)$$
$$S_0(r_7\oplus RK_{10}^3),S_1(r_8\oplus RK_{10}^4)]$$
$$\oplus l_1,l_2,l_3,l_4)$$
$$=(x\oplus f_5,\oplus\gamma_1,f_6\oplus\gamma_2,f_7\oplus\gamma_3,f_8\oplus\gamma_4),$$

由 $M_0$ 自逆,推得

$$S_0(r_5\oplus RK_{10}^1)=x\oplus f_5\oplus\gamma_1\oplus l_1\oplus 02(f_6\oplus\gamma_2\oplus l_1)\oplus 04(f_7\oplus\gamma_3\oplus l_3)\oplus 06(f_8\oplus\gamma_4\oplus l_4)\qquad(5)$$

由 $f_5,\cdots,f_8,\gamma_1,\cdots,\gamma_4$ 都是与 $x$ 无关的常数知:当输入只有 $x$ 变化时,第 6 轮两次输出 $(L_6,R_6)=(l_1,\cdots,l_8,r_1,\cdots,r_8)$,$(L_6',R_6')=(l_1',\cdots,l_8',r_1',\cdots,r_8')$ 应满足以下等式

$$S_0(r_5\oplus RK_{10}^1)\oplus S_0(r_5'\oplus RK_{10}^1)\oplus(l_1\oplus l_1')\oplus 02(l_2\oplus l_2')\oplus 04(l_3\oplus l_3')\oplus 06(l_4\oplus l_4')=x\oplus x'\qquad(6)$$

同理

$$S_1(r_6\oplus RK_{10}^2)\oplus S_1(r_6'\oplus RK_{10}^2)\oplus 02(l_1\oplus l_1')\oplus(l_2\oplus l_2')\oplus 06(l_3\oplus l_3')\oplus 04(l_4\oplus l_4')=02(x\oplus x')\qquad(7)$$

$$S_0(r_7\oplus RK_{10}^3)\oplus S_0(r_7'\oplus RK_{10}^3)\oplus 04(l_1\oplus l_1')\oplus 06(l_2\oplus l_2')\oplus(l_3\oplus l_3')\oplus 02(l_4\oplus l_4')=04(x\oplus x')\qquad(8)$$

$$S_1(r_8\oplus RK_{10}^4)\oplus S_1(r_8'\oplus RK_{10}^4)\oplus 06(l_1\oplus l_1')\oplus 04(l_2\oplus l_2')\oplus 02(l_3\oplus l_3')\oplus(l_4\oplus l_4')=06(x\oplus x')\qquad(9)$$

于是可得如下恢复 $(RK_1^1,RK_{10}^1)$ 的算法:

**算法 1.1**

第一步,猜测 $(RK_1^1,RK_{10}^1)$ 的值,用猜测的 $RK_1^1$ 计算出两个明文:

$$P_L=L_0=(\beta_5,\beta_6,\beta_7,\beta_8,i_0,\beta_2,\beta_3,\beta_4),$$
$$P_R=R_0=(\theta_1,\cdots,\theta_4,S_1(i_0\oplus RK_1^1),08S_1(i_0\oplus RK_1^1),$$
$$02S_1(i_0\oplus RK_1^1),0aS_1(i_0\oplus RK_1^1)),$$
$$P_L'=L_0'=(\beta_5,\beta_6,\beta_7,\beta_8,i_1,\beta_2,\beta_3,\beta_4),$$
$$P_R'=R_0'=(\theta_1,\cdots,\theta_4,S_1(i_1\oplus RK_1^1),08S_1(i_1\oplus RK_1^1),$$
$$02S_1(i_1\oplus RK_1^1),0aS_1(i_1\oplus RK_1^1)).$$

这里的 $\beta_i$,$\theta_i$ 均是任意取定的常数,加密得相应的密文 $(L_6,R_6)=(l_1,\cdots,l_8,r_1,\cdots,r_8)$,$(L_6',R_6')=(l_1',\cdots,l_8',r_1',\cdots,r_8')$.

第二步,用上述猜测的 $RK_{10}^1$ 计算

$$\Delta_0=S_0(r_5\oplus RK_{10}^1)\oplus l_1\oplus 02l_2\oplus 04l_3\oplus 06l_4,\Delta_1$$
$$=S_0(r_5'\oplus RK_{10}^1)\oplus l_1'\oplus 02l_2'\oplus 04l_3'\oplus 06l_4'.$$

由式(6)知道若猜测的 $(RK_1^1,RK_{10}^1)$ 正确,则对 $x$ 的两个不同取值 $i_0,i_1$,$S_0(r_5\oplus RK_{10}^1)\oplus S_0(r_5'\oplus RK_{10}^1)\oplus(l_1\oplus l_1')\oplus 02(l_2\oplus l_2')\oplus 04(l_3\oplus l_3')\oplus 06(l_4\oplus l_4')$ 应该等于 $i_0\oplus i_1$.

考察 $\Delta_0\oplus\Delta_1$ 是否等于 $i_0\oplus i_1$,若不等,则抛弃猜测的 $(RK_1^1,RK_{10}^1)$ 值;若相等,则输出猜测的 $(RK_1^1,RK_{10}^1)$ 值.

由于 $\Delta_0\oplus\Delta_1$ 等于 $i_0\oplus i_1$ 的概率为 $2^{-8}$,所以在 $(RK_1^1,RK_{10}^1)$ 的 $2^{16}$ 个侯选值中,通过第二步的 $(RK_1^1,RK_{10}^1)$ 的个数期望值为 $2^{16}\times 2^{-8}=2^8$.

第三步,对输出的每个 $(RK_1^1,RK_{10}^1)$ 的值,依第一步的方法再选取明文 $P_L''$,$P_R''$,计算 $\Delta_1''$,检查 $\Delta_0\oplus\Delta_1''$ 是否与 $i_0\oplus i_1$ 相等,如果不相等,则丢掉所猜测 $(RK_1^1,RK_{10}^1)$;如果相等,则输出 $(RK_1^1,RK_{10}^1)$ 的值,如果输出值仍然不唯一,重复第三步.

通过第三步 $(RK_1^1,RK_{10}^1)$ 的候选值个数的数学期望是 2 个,因为正确的 $(RK_1^1,RK_{10}^1)$ 一定要被输出;在进入第三步 $(RK_1^1,RK_{10}^1)$ 的 255 个非密钥值中,由于 $\Delta_0\oplus\Delta_1''$ 与 $i_0\oplus i_1$ 相等的概率为 $2^{-8}$,使得等式成立的个数为 $255\times\frac{1}{256}$,二者之和,接近 2.

攻击需要选择的明文数小于 $4\times 2^8$,攻击的时间复杂度主要是第二步的计算,计算每个 $\Delta$ 的计算量小于 1 轮加密,因此攻击的时间复杂度小于 $2^9$ 次 6 轮加密.

下面根据式(7),用与算法 1.1 类似的方法来恢复

$RK_{10}^2$.

**算法 1.2**

**第一步**,由于算法 1.1 中已经恢复 $RK_1^1$,可以根据算法 1.1 第一步的方法来计算明文.

由式(7)知道当输入中的 $i$ 发生变化时,$S_1(r_6 \oplus RK_{10}^2) \oplus S_1(r_6' \oplus RK_{10}^2) \oplus 02(l_1 \oplus l_1') \oplus (l_2 \oplus l_2') \oplus 06(l_3 \oplus l_3') \oplus 04(l_4 \oplus l_4')$ 应该等于 $02(i_0 \oplus i_1)$.

**第二步**,对 $RK_{10}^2$ 的每个候选值,计算

$$\Delta_0 = S_1(r_6 \oplus RK_{10}^2) \oplus 02\,l_1 \oplus l_2 \oplus 06\,l_3 \oplus 04\,l_4,$$

$$\Delta_1 = S_1(r_6' \oplus RK_{10}^2) \oplus 02\,l_1' \oplus l_2' \oplus 06\,l_3' \oplus 04\,l_4'.$$

考察 $\Delta_0 \oplus \Delta_1$ 是否与 $02(i_0 \oplus i_1)$ 相等,如果不相等,则丢掉相应的 $RK_{10}^2$ 的值;若相等,则输出.

**第三步**,对输出的每个 $RK_{10}^2$,依第一步的方法再选取明文 $P_L''$, $P_R''$,继续第二步.

攻击需要选择的明文数小于 $2 \times 2^8$,攻击的时间复杂度主要在第二步的计算,计算每个 $\Delta$ 的计算量小于 6 轮加密. 根据式(8)和式(9),用同样的方法便可分别恢复 $RK_{10}^3$ 和 $RK_{10}^4$. 因此攻击的时间复杂度小于 $4 \times 6 \times 2 \times 2^8$ 次加密.

以上就恢复了 $RK_{10}$ 的全部四个字节,下面考察如何恢复 $RK_{11}$.

由式(4)知道 $R_5$ 的后四个字节满足如下关系式:

$$\begin{aligned} & M_1(S_1(r_1 \oplus RK_{11}^1), S_0(r_2 \oplus RK_{11}^2), S_1(r_3 \oplus RK_{11}^3), \\ & \quad S_0(r_4 \oplus RK_{11}^4)) \oplus (l_5, \cdots, l_8) \\ & = M_0(S_0(y \oplus w_1 \oplus RK_6^1), S_1(02\,y \oplus w_2 \oplus RK_6^2), \\ & \quad S_0(04\,y \oplus w_3 \oplus RK_6^3), S_1(06\,y \oplus w_4 \oplus RK_6^4)) \\ & \quad \oplus (\gamma_5, \cdots, \gamma_8). \end{aligned}$$

对上式进行恒等变形,并注意到 $M_1$ 自逆,得

$$\begin{aligned} & (S_1(r_1 \oplus RK_{11}^1), S_0(r_2 \oplus RK_{11}^2), S_1(r_3 \oplus RK_{11}^3), \\ & \quad S_0(r_4 \oplus RK_{11}^4)) \oplus M_1[(\gamma_5, \cdots, \gamma_8) \oplus (l_5, \cdots, l_8)] \\ & = M_1 M_0(S_0(y \oplus w_1 \oplus RK_6^1), S(02 \oplus w_2 \oplus RK_6^2), \\ & \quad S_0(04\,y \oplus w_3 \oplus RK_6^3), S_1(06\,y \oplus w_4 \oplus RK_6^4)). \end{aligned} \tag{10}$$

由于 $S_0$, $S_1$ 是置换,式(10)右侧的四个分量 $S_0(y \oplus w_1 \oplus RK_6^1)$ 等都应该服从均匀分布,又 $M_0$, $M_1$ 可逆,故 $S_1(r_1^i \oplus RK_{11}^1) \oplus l_5^i \oplus 08\,l_6^i \oplus 02\,l_7^i \oplus 0a\,l_8^i$ 应该服从均匀分布. 若以 $l_1^i, \cdots, l_8^i, r_1^i, \cdots, r_8^i$ 表示当 $x$ 取为 $i$ 时第六轮的输出,则

$$\sum_{i=0}^{255} [S_1(r_1^i \oplus RK_{11}^1) \oplus l_5^i \oplus 08\,l_6^i \oplus 02\,l_7^i \oplus 0a\,l_8^i] = 0 \tag{11}$$

于是有以下的 Square 攻击算法:

**算法 2 恢复 RK₁₁**

**第一步**,设 $RK_{11}^1 = g^1$,对于 $i$ 的 256 个取值,分别选取相应的明文

$$P_L = L_0 = (\beta_5, \beta_6, \beta_7, \beta_8, i, \beta_2, \beta_3, \beta_4),$$

$$P_R = R_0 = (\theta_1, \cdots, \theta_4, S_1(i \oplus RK_1^1), 08\,S_1(i \oplus RK_1^1), 02\,S_1(i \oplus RK_1^1), 0a\,S_1(i \oplus RK_1^1)).$$

**第二步**,选取 $g^1 \in \{0, \cdots, 255\}$,对于 $i$, $i = 0, 1, \cdots, 255$ 相应的输出 $L_6^i = (l_1^i, \cdots, l_8^i)$, $R_6^i = (r_1^i, \cdots, r_8^i)$,计算

$$\sum_{i=0}^{255} [S_1(r_1^i \oplus g^1) \oplus l_5^i \oplus 08\,l_6^i \oplus 02\,l_7^i \oplus 0a\,l_8^i]$$

若等于 0,则输出 $g^1$ 的值,否则丢弃.

**第三步**,重复第二步,考察 $g^1$ 的所有 256 种取值,若只搜到一个数满足式(11),那么此数一定是要求的密钥,若搜索到多个数,那么正确的密钥一定是这些数中的某个,称这些数为准密钥,记准密钥作成的集合为 $S_{RK_{11}^1}$. 集合 $S_{RK_{11}^1}$ 所含准密钥个数的数学期望值为 2. 理由类似算法 1.

**第四步**,为了确定正确密钥,改变第一步中 $\beta_5$ 的取值,再选取明文

$$P_L' = L_0 = (\beta_5', \beta_6, \beta_7, \beta_8, i, \beta_2, \beta_3, \beta_4),$$

$$P_R' = R_0 = (\theta_1, \cdots, \theta_4, S_1(i \oplus RK_1^1), 08\,S_1(i \oplus RK_1^1), 02\,S_1(i \oplus RK_1^1), 0a\,S_1(i \oplus RK_1^1)).$$

得到另一个准密钥集合 $S'_{RK_{11}^1}$,则密钥一定属于 $S_{RK_{11}^1}$ 和 $S'_{RK_{11}^1}$ 的交集,若交集只含一个元素,则此元素就是要求的密钥;若有两个以上的元素,再选取 $\beta_5''$,得到 $S''_{RK_{11}^1}$,求三个集合的交集,如此反复,直到交集里只有一个元素为止.

攻击每个密钥字节需要选择的明文数等于 $2^8$,穷尽密钥个数为 $2^8$,计算每个 $\Sigma$ 的计算量等于 6 轮加密,若计算两个 $\beta_5$,则攻击的时间复杂度等于 $4 \times 6 \times 2 \times 2^8 \times 2^8$ 次加密. 所以,整个攻击过程的总运算量小于 $2^{22}$ 次加密.

至此第 6 轮的密钥全部恢复,图 2 是攻击过程示意图.

再利用 $RK_{10}$, $RK_{11}$ 解密得到第 5 轮的输出 $L_5$, $R_5$,

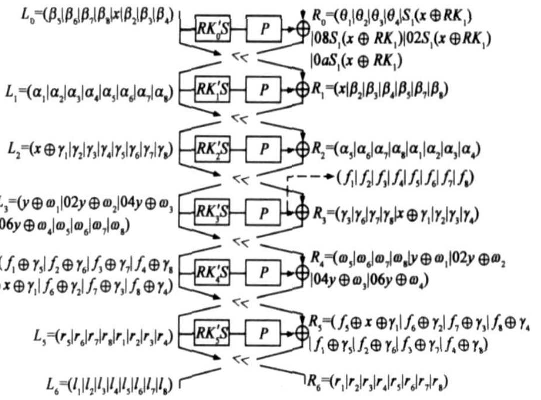


图2 6 轮CLEFIA攻击过程示意图

利用与恢复 $RK_{10}$ , $RK_{11}$ 类似的方法便可恢复 $RK_8$ , $RK_9$ , 根据密钥扩展算法

$$RK_8 | RK_9 | RK_{10} | RK_{11} \leftarrow \Sigma^2(L) \oplus CON_{32} | CON_{33} | CON_{34} | CON_{35}$$

可得到 $\Sigma^2(L)$ ,进而求得 $L$ ,再用 12 轮解密算法对 $L$ 解密便可得到种子密钥 $K$. 表 1 给出了各步攻击的复杂度.

表 1　6 轮 CLEFIA 的攻击复杂度

| 轮密钥 | 时间复杂度 | 存储复杂度 |
|---|---|---|
| $RK_1^1$ | $2^{16}$ | $3 \times 2^8$ |
| $RK_{10}$ | $2^{22}$ | $2 \times 2^8$ |
| $RK_{11}$ | $2^{22}$ | $2^{10}$ |

## 6　结论

本文给出了 CLEFIA 的一个的等价结构,在等价结构的基础上构造了一个四轮区分器,在四轮区分器前后各加一轮,将碰撞攻击与 Square 方法相结合成功分析了 6 轮的 CLEFIA. 我们的算法在普通 pc 机上经过验证都是正确的,在不到两个小时的时间内就可以完全恢复密钥.

**参考文献**:


[1] Taizo Shirai, Kyoji Shibutani, Toru Akishita, et al. The 128-bit Block cipher CLEFIA [A]. FSE 2007 [C]. LNCS 4593, Springer-Verlag, 2007. 181 - 195.

[2] Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki1, Hiroyasu Kubo, Impossible Differential Cryptanalysis of CLEFIA [A], FSE 2008 [C]. LNCS 5086, Springer-Verlag. 2008. 398 - 411.

[3] Hua Chen, Wenling Wu, Dengguo Feng. Differential Fault Analysis on CLEFIA [A]. ICICS, 2007 [C]. LNCS 4861, Springer-Verlag, 2008. 284 - 295.

[4] Wei Wang, Xiaoyun Wang. Improved Impossible Differential Cryptanalysis of CLEFIA [R]. IACR ePrint archive: Report 2007/466.

[5] Wenying Zhang, Jing Han, Impossible Differential Analysis of Reduced Round CLEFIA [A]. Inscrypt 2008 [C]. LNCS 5487, Springer-Verlag, 2009, 181 - 191.

[6] 吴文玲,冯登国. 低轮 Camellia 的碰撞攻击[J]. 中国科学 E 辑, 2004, 34(8): 857 - 868.

[7] 贺也平,吴文玲,卿斯汉. 对于 5 轮 Camellia 的 Square 攻击[J]. 中国科学院研究生院学报, 2001. 18(2): 177 - 180.

[8] Lei Duo. Square like attack on Camellia [A]. ICICS 2007 [C]. LNCS 4861, Springer-Verlag, 2008. 269 - 283.


**作者简介**:


**韩　敬**　女,1985 年 7 月出生于山东济南. 2007 年进入山东师范大学信息科学与工程学院. 现为硕士研究生在读,从事分组密码设计与分析,信息安全有关方面的研究.

E-mail: happyjerry2004@163.com

**张文英**　女,1970 年 6 月出生于山东鄄城. 副教授,信息安全国家重点实验室出站博士后. 研究方向为密码学和信息安全. 在国内外核心期刊发表学术论文 15 篇,其中多篇被 SCI、EI 检索. 主持过十一五科技预研项目、中国博士后基金、信息安全国家重点实验室开放课题和山东省自然基金.

**徐小华**　女,1975 年 5 月出生于山东昌邑,讲师. 2006 年于山东大学获理学硕士. 现研究方向为应用数学.