对 8 轮 CLEFIA 算法的一种现实攻击

唐学海,孙 兵,李 超
(国防科技大学数学与系统科学系,湖南长沙 410073)

摘 要: CLEFIA 算法是 SONY 公司在 2007 年的快速软件加密大会上提出的一个分组密码算法.研究了 CLEFIA 算法的等价结构,并找到了它的一个 5 轮区分器.基于 5 轮区分器,利用中间相遇攻击方法对 6/7/8 轮的 CLEFIA 算法进行了攻击.攻击复杂度都比较小,其中对于 6 轮和 7 轮的攻击在普通 PC 机上不到 1 秒钟就可恢复密钥,8 轮的攻击在高性能计算机上也是可以实现的.

关键词: 分组密码; CLEFIA; 中间相遇攻击; 现实攻击
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 07-1608-05

A Real-World Attack of 8-Round CLEFIA

TANG Xue-hai, SUN Bing, LI Chao
(*Department of Mathematics and System Science, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

Abstract: CLEFIA is a block cipher proposed in FSE (Fast Software Encryption) 2007 by SONY Corporation. Some 5-round distinguishers of CLEFIA are presented according to study an equivalent structure of CLEFIA. Based on the 5-round distinguishers, some meet-in-the-middle attacks can be made on 6/7/8-round CLEFIA. The attack complexities are low enough and the key of 6/7-round CLEFIA can be recovered within one second in the ordinary PC. Moreover, the 8-round attack can be also implemented in the high-performance computer.

Key words: block cipher; CLEFIA; meet-in-the-middle attack; real-world attack

1 引言

SONY 公司为了在其发行的音乐和图像等数字内容中加入版权保护和认证技术,在 2007 年的快速软件加密大会(FSE)上提出了一种新的迭代分组密码算法 CLEFIA[1,2].CLEFIA 算法的数据分组长度为 128bit,密钥长度可以是 128bit,192bit 和 256bit,对应的加密轮数分别是 18,22 和 26 轮,它具有安全、高效和低成本等特点.自 CLEFIA 算法被公布以来,国内外许多密码分析学者都对其安全性进行了研究,包括差分分析[3],线性分析[3],不可能差分分析[3~6],积分攻击[7,8]和碰撞-Square 攻击[9]等.

上述对 CLEFIA 算法的分析几乎都只是理论上的结果,攻击复杂度都相当高,在现有计算机水平下是不可能实现的,只有在文献[9]中韩敬等利用碰撞攻击和 Square 攻击相结合的方法成功分析了 6 轮 CLEFIA 算法,在普通 PC 机上不到两小时可以恢复密钥.中间相遇攻击的思想最早由 Diffie 和 Hellman 在分析 Two-DES 的时候提出[10],后来被扩展到一般的情形下,如对 AES[11,12]的分析.本文利用 CLEFIA 算法的等价结构和中间相遇攻击方法相结合分析了 6-8 轮 CLEFIA 算法,攻击复杂度都比较低,其中对于 6 轮和 7 轮的 CLEFIA 算法用我们的方法在普通 PC 机上不到一秒钟就可恢复密钥,对 8 轮的攻击在高性能计算机上也是可以实现的,这是目前对低轮 CLEFIA 算法现实破译最好的结果.

2 CLEFIA 算法简介

CLEFIA 算法的数据分组长度为 128bit,支持长度为 128/192/256 bit 的密钥,它采用了具有 4 个分支的广义 Feistel 结构.设 $P=(P_0,P_1,P_2,P_3)$和 $C=(C_0,C_1,C_2,C_3)\in\{0,1\}^{128}$分别为 128bit 的明文和密文,其中 $P_i,C_i\in\{0,1\}^{32}(0\leqslant i<4)$为 32bit 的分支;$K_i\in\{0,1\}^{32}(0\leqslant i<2r)$为轮密钥,$WK_0,WK_1,WK_2,WK_3\in\{0,1\}^{32}$为白化密钥.$r$ 轮 CLEFIA 算法加密过程如下(如图 1 左图所示):

(1)初始白化层 $T=(T_0,T_1,T_2,T_3)=(P_0,P_1\oplus WK_0,P_2,P_3\oplus WK_1)$为第一轮的输入.

(2) r 轮轮变换 设 $T^{(i-1)}=(T_0^{(i-1)},T_1^{(i-1)},T_2^{(i-1)},T_3^{(i-1)})$为第 i 轮的输入,则第 i 轮的输出为

收稿日期:2010-04-16;修回日期:2011-02-23
基金项目:国家自然科学基金(No.60803156,No.61070215)

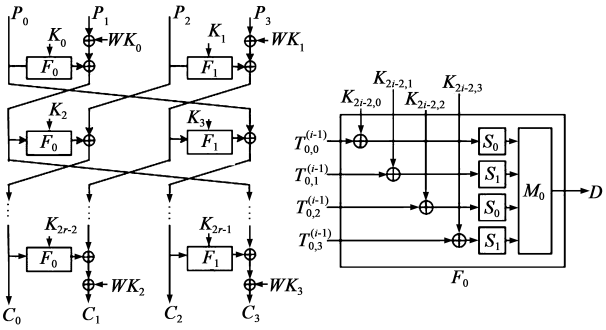

图1　r轮CLEFIA数据加密流程和轮函数F_0

$T^{(i)}=(T_0^{(i)},T_1^{(i)},T_2^{(i)},T_3^{(i)})$

$=(F_0(T_0^{(i-1)},K_{2i-2})\oplus T_1^{(i-1)},T_2^{(i-1)},F_1(T_2^{(i-1)},K_{2i-1})\oplus T_3^{(i-1)},T_0^{(i-1)})$.

(3)末尾白化层　密文 $C=(C_0,C_1,C_2,C_3)=(T_3^{(r)},T_0^{(r)}\oplus WK_2,T_1^{(r)},T_2^{(r)}\oplus WK_3)$.

上述 F_0,F_1 是两个非线性可逆函数,F_0 定义如下(如图 1 右图所示):

(*a*)轮密钥加　计算 $A=T_0^{(i-1)}\oplus K_{2i-2}$.

(*b*)非线性变换　令 $A=(A_0,A_1,A_2,A_3)$,其中 $A_i\in\{0,1\}^8(0\leqslant i\leqslant 3)$,计算 $B_0=S_0(A_0),B_1=S_1(A_1),B_2=S_0(A_2),B_3=S_1(A_3)$.

(*c*)线性变换　计算 $D=\boldsymbol{M}_0(B_0,B_1,B_2,B_3)^{\mathrm{T}}$.

其中 S_0 和 S_1 是两个非线性 S 盒,$\boldsymbol{M}_0$ 为一个 4×4 的矩阵.非线性函数 F_1 的定义类似,只需将其中的 S_0 和 S_1 的位置互换,将 $\boldsymbol{M}_0$ 变为 $\boldsymbol{M}_1$ 即可.$\boldsymbol{M}_0$ 和 $\boldsymbol{M}_1$ 的十六进制表示如下:

$$\boldsymbol{M}_0=\begin{pmatrix}0x01&0x02&0x04&0x06\\0x02&0x01&0x06&0x04\\0x04&0x06&0x01&0x02\\0x06&0x04&0x02&0x01\end{pmatrix},$$

$$\boldsymbol{M}_1=\begin{pmatrix}0x01&0x08&0x02&0x0a\\0x08&0x01&0x0a&0x02\\0x02&0x0a&0x01&0x08\\0x0a&0x02&0x08&0x01\end{pmatrix}.$$

矩阵与向量的乘法定义在有限域 $GF(2^8)$ 上,其本原多项式为 $z^8+z^4+z^3+z^2+1$.容易验证矩阵 $\boldsymbol{M}_0$ 和 $\boldsymbol{M}_1$ 都是自逆的,即 $\boldsymbol{M}_0=\boldsymbol{M}_0^{-1},\boldsymbol{M}_1=\boldsymbol{M}_1^{-1}$.

3　CLEFIA 算法的一种等价结构

在文献[13]中,多磊等学者利用线性变换的性质给出了 Camellia 算法的几种等价结构,从而改进了 Camellia 算法的 Square 攻击结果.同样,我们也可以利用 CLEFIA 算法中线性变换的性质给出 CLEFIA 算法的一种等价结构.记 F 函数中的轮密钥加为 K,非线性变换为 S,线性变换为 $\boldsymbol{M}_0$ 或 $\boldsymbol{M}_1$,则两轮的 CLEFIA 算法可描述为图 2 中第一个加密结构.另外,我们利用这几个基础变换和异或运算可以构造图 2 中的第 2 个加密结构,称之为 CLEFIA(Ⅰ).下面的定理将证明这两个结构是等价的.

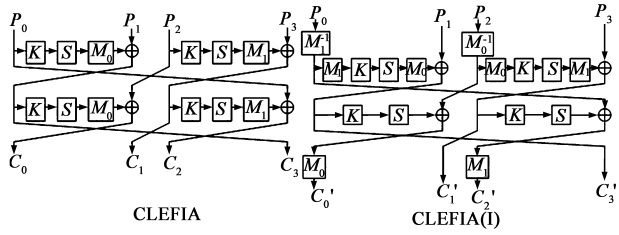

图2　两轮CLEFIA及其等价结构CLEFIA(Ⅰ)

定理 1　两轮 CLEFIA 算法与 CLEFIA(Ⅰ)等价.

证明　如图 2 所示,设两轮 CLEFIA 的输入和输出分别为(P_0,P_1,P_2,P_3)和(C_0,C_1,C_2,C_3),轮密钥依次是 K_0,K_1,K_2,K_3,则第一轮的输出为

$(\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1,P_2,\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3,P_0)$,从而第 2 轮的输出为

$(C_0,C_1,C_2,C_3)=(\boldsymbol{M}_0(S(\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1\oplus K_2))\oplus P_2,\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3,\boldsymbol{M}_1(S(\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3\oplus K_3))\oplus P_0,\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1)$.

下面考虑 CLEFIA(Ⅰ):设其输入和输出分别为(P_0,P_1,P_2,P_3)和(C_0',C_1',C_2',C_3'),轮密钥同样依次是 K_0,K_1,K_2,K_3,则第一轮的输出为

$(\boldsymbol{M}_0(S(\boldsymbol{M}_1(\boldsymbol{M}_1^{-1}(P_0))\oplus K_0))\oplus P_1,\boldsymbol{M}_0^{-1}(P_2),\boldsymbol{M}_1(S(\boldsymbol{M}_0(\boldsymbol{M}_0^{-1}(P_2))\oplus K_1))\oplus P_3,\boldsymbol{M}_1^{-1}(P_0))$

$=(\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1,\boldsymbol{M}_0^{-1}(P_2),\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3,\boldsymbol{M}_1^{-1}(P_0))$.

进而第 2 轮的输出为

$(\boldsymbol{M}_0(S(\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1\oplus K_2)\oplus\boldsymbol{M}_0^{-1}(P_2)),\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3,\boldsymbol{M}_1(S(\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3\oplus K_3)\oplus\boldsymbol{M}_1^{-1}(P_0)),\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1)$

由 $\boldsymbol{M}_0$ 和 $\boldsymbol{M}_1$ 都是线性变换知,可将上式化简得

$(C_0',C_1',C_2',C_3')=(\boldsymbol{M}_0(S(\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1\oplus K_2))\oplus P_2,\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3,\boldsymbol{M}_1(S(\boldsymbol{M}_1(S(P_2\oplus K_1))\oplus P_3\oplus K_3))\oplus P_0,\boldsymbol{M}_0(S(P_0\oplus K_0))\oplus P_1)$

$=(C_0,C_1,C_2,C_3)$

即对于相同的明文和密钥,采用图 2 中两轮 CLEFIA 与 CLEFIA(Ⅰ)加密结果一样,从而它们等价.证毕!

4　CLEFIA 算法的 5 轮区分器

本节利用上述等价结构构造 CLEFIA 算法的一个 5 轮区分器.考虑 6 轮 CLEFIA 算法(不考虑始末的白化层),其由 3 个 CLEFIA(Ⅰ)相连接构成(如图 3 所示),

称这个加密结构为 CLEFIA(Ⅱ).

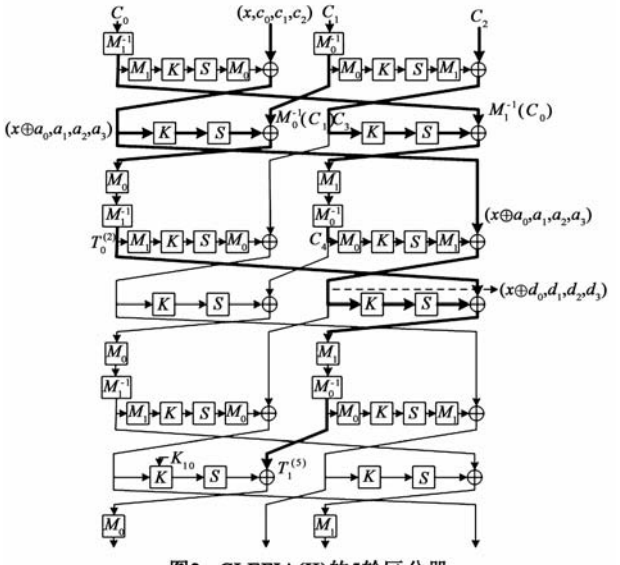

图3 CLEFIA(II)的5轮区分器

设一组包含 256 个明文的明文组形如 $(C_0,(x,c_0,c_1,c_2),C_1,C_2)$,其中 C_i 和 c_i 分别代表此位置取固定的 32bit 常值和 8bit 常值(不同位置处的常值不一定相等),x 代表此位置取 256 个不同的值.也就是说,这组明文除在 x 处取值不同外,别的地方取值都相同.对于图 3 中的加密结构,在密钥给定的情况下,将上述明文组作为输入,则经过 5 轮加密后的输出可以看作是关于变量为 x 的函数,而常值 C_i 和 c_i 以及密钥都是这个函数的参数.设第 i 轮的输入和输出分别为 $T^{(i-1)}=(T_0^{(i-1)},T_1^{(i-1)},T_2^{(i-1)},T_3^{(i-1)})$ 和 $T^{(i)}=(T_0^{(i)},T_1^{(i)},T_2^{(i)},T_3^{(i)})$,下面我们沿着图 3 中粗线所示路径来详细计算第 5 轮输出的第二个分支 $T_1^{(5)}$.

第一轮的输入为 $T^{(0)}=(C_0,(x,c_0,c_1,c_2),C_1,C_2)$,即 $T_{1,0}^{(0)}=x$ 作为变量,由加密结构可知,第一轮的输出 $T^{(1)}=((x\oplus a_0,a_1,a_2,a_3),\boldsymbol{M}_0^{-1}(C_1),C_3,\boldsymbol{M}_1^{-1}(C_0))$,其中 $a_i(0\leqslant i\leqslant 3)$为一些由轮密钥 K_0 和常值 C_0,c_0,c_1,c_2 决定的常值,C_3 也为常值,其由轮密钥 K_1 和常值 C_1,C_2 决定.

令 $K_{i,j}$为轮密钥 K_i 的第 $j+1$ 个字节,$b_0=K_{2,0}\oplus a_0$,$b_1=S_1(a_1\oplus K_{2,1})$,$b_2=S_0(a_2\oplus K_{2,2})$,$b_3=S_1(a_3\oplus K_{2,3})$,则第 2 轮输出的第一个分支

$$\begin{aligned}T_0^{(2)}&=\boldsymbol{M}_1^{-1}(\boldsymbol{M}_0((S_0(x\oplus b_0),b_1,b_2,b_3)\oplus\boldsymbol{M}_0^{-1}(C_1)))\\&=\boldsymbol{M}_1^{-1}(\boldsymbol{M}_0(S_0(x\oplus b_0),b_1,b_2,b_3))\oplus\boldsymbol{M}_1^{-1}(C_1),\end{aligned}$$

第 2 轮输出的第 3 和第 4 两个分支分别为 $T_2^{(2)}=C_4$ 和 $T_3^{(2)}=(x\oplus a_0,a_1,a_2,a_3)$,其中 C_4 为常值,它由轮密钥 K_3 和常值 $C_3,\boldsymbol{M}_1^{-1}(C_0)$决定.易知第 3 轮输出的第 3 和第 4 两个分支分别为 $T_2^{(3)}=(x\oplus d_0,d_1,d_2,d_3)$和 $T_3^{(3)}=T_0^{(2)}$,其中 $d_i(0\leqslant i\leqslant 3)$为一些常值,由轮密钥 K_5 和常值 C_4 决定.

令 $e_0=K_{7,0}\oplus d_0$,$e_1=S_0(d_1\oplus K_{7,1})$,$e_2=S_1(d_2\oplus K_{7,2})$,$e_3=S_0(d_3\oplus K_{7,3})$,则可得第 4 轮输出的第 3 个分支

$$\begin{aligned}T_2^{(4)}&=\boldsymbol{M}_0^{-1}(\boldsymbol{M}_1((S_1(x\oplus e_0),e_1,e_2,e_3)\oplus T_3^{(3)}))\\&=\boldsymbol{M}_0^{-1}(\boldsymbol{M}_1(S_1(x\oplus e_0),e_1,e_2,e_3))\\&\quad\oplus\boldsymbol{M}_0^{-1}(\boldsymbol{M}_1(T_0^{(2)}))\\&=\boldsymbol{M}_0^{-1}(\boldsymbol{M}_1(S_1(x\oplus e_0),e_1,e_2,e_3))\oplus\\&\quad\boldsymbol{M}_0^{-1}(\boldsymbol{M}_1(\boldsymbol{M}_1^{-1}(\boldsymbol{M}_0(S_0(x\oplus b_0),\\&\quad b_1,b_2,b_3))\oplus\boldsymbol{M}_1^{-1}(C_1)))\\&=\boldsymbol{M}_0^{-1}(\boldsymbol{M}_1(S_1(x\oplus e_0),e_1,e_2,e_3))\oplus(S_0(x\oplus b_0),\\&\quad b_1,b_2,b_3)\oplus\boldsymbol{M}_0^{-1}(C_1)\end{aligned}$$

通过有限域上的乘法可计算得

$$\boldsymbol{M}_0^{-1}\boldsymbol{M}_1=\begin{pmatrix}0\text{x}37&0\text{x}46&0\text{x}34&0\text{x}40\\0\text{x}46&0\text{x}37&0\text{x}40&0\text{x}34\\0\text{x}34&0\text{x}40&0\text{x}37&0\text{x}46\\0\text{x}40&0\text{x}34&0\text{x}46&0\text{x}37\end{pmatrix},$$

于是可得

$$T_1^{(5)}=T_2^{(4)}=\begin{cases}0\text{x}37\,S_1(x\oplus e_0)\oplus S_0(x\oplus b_0)\oplus f_0\\0\text{x}46\,S_1(x\oplus e_0)\oplus f_1\\0\text{x}34\,S_1(x\oplus e_0)\oplus f_2\\0\text{x}40\,S_1(x\oplus e_0)\oplus f_3\end{cases}\tag{1}$$

其中 $f_i(0\leqslant i\leqslant 3)$为一些常值,由常值 e_1,e_2,e_3,b_1,b_2,b_3 和 $\boldsymbol{M}_0^{-1}(C_1)$决定.由此可得下面的定理:

定理 2(CLEFIA 算法的 5 轮区分器) 对于 CLEFIA(Ⅱ)加密结构,设第 i 轮的输入和输出分别为 $T^{(i-1)}=(T_0^{(i-1)},T_1^{(i-1)},T_2^{(i-1)},T_3^{(i-1)})$和 $T^{(i)}=(T_0^{(i)},T_1^{(i)},T_2^{(i)},T_3^{(i)})$,$T_{j,k}^{(i)}$表示 $T_j^{(i)}$ 的第 $k+1$ 个字节.一组包含 256 个明文的明文组满足 $T_{1,0}^{(0)}$取值不同,而其余位置都取常值,将这组明文加密 5 轮,则映射 $T_{1,0}^{(0)}\mapsto T_{1,0}^{(5)}$由 3 个 8bit 参数完全决定;映射 $T_{1,0}^{(0)}\mapsto T_{1,k}^{(5)}(1\leqslant k\leqslant 3)$由 2 个 8bit 参数完全决定.

证明 由式(1)知 $T_{1,0}^{(5)}=0\text{x}37\,S_1(x\oplus e_0)\oplus S_0(x\oplus b_0)\oplus f_0$,故映射 $T_{1,0}^{(0)}\mapsto T_{1,0}^{(5)}$由参数 e_0,b_0,f_0 完全决定,同理可证其余部分.证毕!

5 对低轮 CLEFIA 算法的中间相遇攻击

利用上节中的 5 轮区分器可以对低轮 CLEFIA 算法进行中间相遇攻击.以映射 $T_{1,0}^{(0)}\mapsto T_{1,0}^{(5)}$为例,对 6 轮 CLEFIA 算法的中间相遇攻击的基本步骤是:

步骤 1 对于(e_0,b_0,f_0)的每一个值,由 $T_{1,0}^{(5)}=0\text{x}37\,S_1(x\oplus e_0)\oplus S_0(x\oplus b_0)\oplus f_0\triangleq f_{(e_0,b_0,f_0)}(x)$,计算并存储 $f_{(e_0,b_0,f_0)}(i)$,其中$(0\leqslant i\leqslant n-1)$.

步骤 2 选择 n 个形如$(C_0,(x,c_0,c_1,c_2),C_1,C_2)$

的明文,其中 $0 \leqslant x \leqslant n-1$.将这组明文加密 6 轮,对于 $x=i$,记相应的明文和密文分别为 $P^{(i)}$和 $C^{(i)}$.

步骤 3　猜测 $K_{10,0}$的一个值 gk,由密文 $C^{(i)}$经部分解密可计算得 $T_{1,0}^{(5)}$的一个值,记为 $f_{gk}(i)$.现在如果在步骤 1 中的存储表中能找到一个(e_0, b_0, f_0)使得 $f_{(e_0,b_0,f_0)}(i)=f_{gk}(i)$对所有 $0 \leqslant i \leqslant n-1$ 都成立,称找到一个"匹配".因为前 5 轮中与 $T_{1,0}^{(5)}$相关的正确的密钥必包含在某一个(e_0, b_0, f_0)中,从而若所猜密钥 gk 是 $K_{10,0}$的正确值,那么必定可以找到一个"匹配",这就是"中间相遇"的思想.一共有 2^{24}个可能的(e_0, b_0, f_0),所以错误的 gk 能够得到一个"匹配"的概率是 $2^{24} \times (2^{-8})^n$,错误的密钥共有 2^8-1 个,所以只要$(2^8-1) \times 2^{24} \times (2^{-8})^n < 1$ 即可得到唯一正确的密钥,从而只须取 $n=5$.

复杂度分析　步骤 1 称为预计算,其复杂度为 $2^{24} \times 5 \times 2$ 个 S 盒计算,1 轮 CLEFIA 加密有 8 个 S 盒计算,故预计算复杂度为 $2^{24} \times 5 \times 2/(6 \times 8) \approx 2^{21.7}$次 6 轮加密;数据复杂度显然为 5;时间复杂度为 $5 \times 2^8/(6 \times 8) \approx 2^{4.7}$次 6 轮加密.类似地,利用映射 $T_{1,0}^{(0)} \mapsto T_{1,k}^{(5)}(1 \leqslant k \leqslant 3)$可恢复 K_{10}的其余几个字节,因为这几个映射中只有 2 个参数,所以预计算复杂度均为 $2^{8\times 2} \times 5/(6 \times 8) \approx 2^{12.7}$,数据选择可以和前面一样,且只要 4 个就可以了,时间复杂度几乎也和前面一样.故恢复轮密钥 K_{10}的总的预计算复杂度为 $2^{21.7}+3 \times 2^{12.7} \approx 2^{21.7}$,数据复杂度为 5,时间复杂度为 $2^{4.7} \times 4 = 2^{6.7}$.若将 5 轮区分器的输入换为$(C_0, C_1, C_2, (x, c_0, c_1, c_2))$,可得类似的区分器,按照上述方法可恢复轮密钥 K_{11}.恢复出轮密钥 K_{10}和 K_{11}后,对于轮密钥 K_8 和 K_9,可以按上述方法找到适当的 4 轮区分器来恢复,复杂度相比 6 轮的可以忽略,这样由密钥扩展算法[2]就可得到种子密钥.

上述方法还可以进一步改进以降低预计算复杂度,具体如下:步骤 1 中我们可以计算并且存储

$$f_{(e_0,b_0,f_0)}(i) \oplus f_{(e_0,b_0,f_0)}(0)$$
$$= 0\text{x}37 S_1(i \oplus e_0) \oplus S_0(i \oplus b_0) \oplus 0\text{x}37 S_1(0 \oplus e_0) \oplus S_0(0 \oplus b_0) \triangleq \Delta f_{e_0,b_0}(i),$$

其中 $1 \leqslant i \leqslant n$,步骤 3 中找"匹配"时就用相应的"$\Delta f_{e_0,b_0}(i)=f_{gk}(i) \oplus f_{gk}(0)$",所以参数 f_0 就可以忽略,预计算复杂度降为 $2^{13.7}$,数据复杂度和时间复杂度刚好不变.下面利用这种方法给出对 8 轮 CLEFIA 算法的中间相遇攻击,它是基于 6 轮的 CLEFIA(Ⅱ),再在首尾各加一轮(如图 4 所示).

步骤 1　对于(e_0, b_0)的每一个可能的值计算并且存储

$$f_{(e_0,b_0,f_0)}(i) \oplus f_{(e_0,b_0,f_0)}(0)$$
$$= 0\text{x}37 S_1(i \oplus e_0) \oplus S_0(i \oplus b_0) \oplus 0\text{x}37 S_1(0 \oplus e_0) \oplus S_0(0 \oplus b_0) \triangleq \Delta f_{e_0,b_0}(i)$$

其中 $1 \leqslant i \leqslant n$.

步骤 2　猜测 $K_{1,0}$的一个值,选择 $n+1$ 个形如

$$(C_2, C_0', (x, c_0, c_1, c_2), \boldsymbol{M}_1(S_1(x \oplus K_{1,0}), c_0', c_1', c_2'))$$

的明文组加密 8 轮,其中 $0 \leqslant x \leqslant n$, C_i, C_i', c_i, c_i' 均为常值,对于 $x=i$,记相应的明文和密文分别为 $P^{(i)}$和 $C^{(i)}$.

步骤 3　猜测$(K_{12,0}, K_{15}) \triangleq gk$,对于每一个密文 $C^{(i)}$,按图 4 中粗线所示的路径部分解密可得 $T_{1,0}^{(6)}$的一个值,记为 $f_{gk}(i)$.现在对于步骤 1 中的每一个(e_0, b_0),判断是否有 $\Delta f_{e_0,b_0}(i)=f_{gk}(i) \oplus f_{gk}(0)(1 \leqslant i \leqslant n)$成立,若存在$(e_0, b_0)$使得上式成立,则上述所猜密钥可能是正确的,否则重新猜测$(K_{12,0}, K_{15})$再次判断.

步骤 4　若猜测完$(K_{12,0}, K_{15})$的所有值都找不到一个"匹配",则重复步骤 2 和 3,直到找到一个"匹配",输出相应所猜的密钥值.所猜的密钥一共有 6 字节,要使错误的密钥全部淘汰需要$(2^{8\times 6}-1) \times 2^{16} \times (2^{-8})^n < 1$,故 $n=9$ 即可.

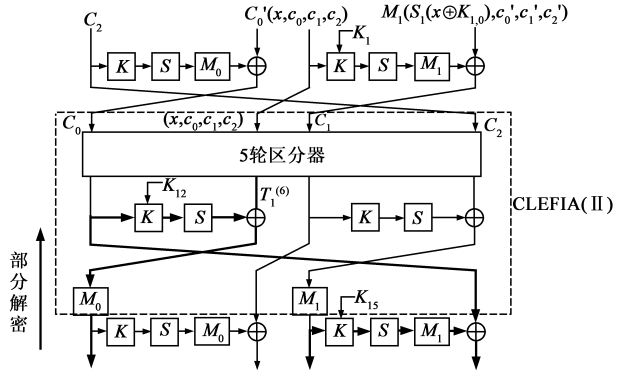

图4　对8轮CLEFIA算法的攻击

复杂度分析　步骤 1 的预计算复杂度为 $2^{16} \times (9+1) \times 4/(8 \times 8) \approx 2^{15.3}$次 8 轮加密;数据复杂度显然为$(9+1) \times 2^8 \approx 2^{11.3}$;一轮部分解密包含 5 个 S 盒的计算,故时间复杂度为 $2^{11.3} \times 2^{5\times 8} \times 5/(8 \times 8) \approx 2^{47.6}$次 8 轮加密.同理,若将 5 轮区分器的输入换为$(C_0, C_1, C_2, (x, c_0, c_1, c_2))$,可得类似的区分器,按照上述方法可恢复轮密钥 K_{14}.

7 轮 CLEFIA 算法的攻击与上述 8 轮的攻击相似,只是在末尾少加一轮.恢复 $K_{12,0}$的预计算复杂度是 2^{14},数据复杂度为 6×2^8,时间复杂度为 2^{13}次 7 轮加密.完全恢复 K_1 和 K_{12}的预计算复杂度为 2^{14},数据复杂度为 $6 \times 2^8 \times 4 \approx 2^{12.6}$,时间复杂度为 $2^{13} \times 4 = 2^{15}$.

上述 6 轮和 7 轮的攻击我们在普通 PC 机上做过实验,不到 1 秒就可恢复出密钥.而对于 8 轮的攻击在普通 PC 机上还实现不了,但对于现在的高性能计算机来

说还是能够实现的.

6 总结

本文研究了 CLEFIA 算法的一种等价结构,基于此等价结构建立了 CLEFIA 算法的一类 5 轮区分器,利用"中间相遇"思想和 5 轮区分器对低轮 CLEFIA 算法进行了中间相遇攻击,表 1 列出了本文的攻击结果和以往文献关于低轮 CLEFIA 算法的一些攻击结果.其中的复杂度都以恢复一个 32bit 的轮密钥来进行衡量.经比较可以发现本文的结果在数据复杂度和时间复杂度方面都非常低,其中对于 6 轮和 7 轮的攻击都可以很容易地在普通 PC 机上实现.当然,利用本文的方法还可以寻找到更高轮数的区分器,实现对更高轮数的 CLEFIA 算法的攻击,只要保证映射中的参数个数不是特别大,因为参数的个数足够大的时候就会使步骤 1 中的预计算复杂度超过穷尽搜索,这样就没有意义了.对于更高轮数的 CLEFIA 算法我们也研究过,只是效果没有别的攻击方法的好,但是对于低轮 CLEFIA 算法其优势很明显.

表 1 对低轮 CLEFIA 算法的一些攻击结果

文献	攻击方法	攻击轮数	数据复杂度	时间复杂度	预计算复杂度
[9]	碰撞-Square	6	2^{10}	2^{22}	–
本文	中间相遇	6	5	$2^{6.7}$	$2^{13.7}$
[3]	饱和度分析	7	$2^{9.6}$	2^{76}	–
本文	中间相遇	7	$2^{12.6}$	2^{15}	2^{14}
本文	中间相遇	8	$2^{11.3}$	$2^{47.6}$	$2^{15.3}$

一个很显然的问题是为什么本文要利用 CLEFIA 算法的等价结构?它究竟有什么优点?事实上,如果直接利用 CLEFIA 算法的原始结构,一方面,按照上述寻找区分器的方法也可以得到类似的区分器,但是相应的映射中常量参数的个数会多一些,这样步骤 1 中预计算复杂度会增加;另一方面,在猜测密钥阶段,以 6 轮的攻击为例,需要猜测的不止 $K_{10,0}$一个字节的值,而是整个 K_{10}的值,这样数据复杂度和时间复杂度都会增加很多.另外,本文给出的等价结构同样可以改进以往的积分攻击的结果,但由于积分攻击的选择明文必须要一个字节遍历,这样数据复杂度就比本文的高,从而时间复杂度也会比本文的高.

参考文献

[1] T Shirai, K Shibutani, T Akishita, et a1. The 128-bit Block cipher CLEHA [A]. FSE 2007 [C]. Berlin: LNCS 4593, Springer-Verlag, 2007. 181 – 195.

[2] Sony Corporation. The 128-bit Blockcipher CLEFIA: Algorithm Specification [R/OL]. http://www.sony.net/products/cryptography/clefia/index.html, 2007 – 06 – 01.

[3] Sony Corporation. The 128-bit Blockcipher CLEFIA: Security and Performance Evaluation [R/OL]. http://www.sony.net//products/cryptography/clefia/index.html, 2007 – 06 – 01.

[4] Y Tsunoo, E Tsujihara, M Shigeri, et a1. Impossible differential cryptanalysis of CLEFIA [A]. FSE 2008 [C]. Berlin: LNCS 5086, Springer-Verlag, 2008. 398 – 411.

[5] Zhang Wenying, Han Jing. Impossible differential analysis of reduced round CLEFIA [A]. Inscrypt 2008 [C]. Berlin: LNCS5487, Springer-Verlag, 2009. 181 – 191.

[6] Wang Wei, Wang Xiao-yun. Impossible differential cryptanalysis of CLEFIA-128/192/256 [J]. Journal of Software, 2009, 20(9): 2587 – 2596.

[7] 王薇,王小云.对 CLEFIA 算法的饱和度分析[J].通信学报,2008,29(10):88 – 92.
Wang Wei, Wang Xiao-yun. Saturation cryptanalysis of CLEFIA [J]. Journal of Communication, 2008, 29(10): 88 – 92. (in Chinese)

[8] 唐学海,李超,谢端强.CLEFIA 密码的 Square 攻击 [J].电子与信息学报,2009,31(9):2260 – 2263.
Tang Xue-hai, Li Chao, Xie Duan-qiang. Square bttack on CLEFIA [J]. Journal of Electronics and Information Technology, 2009, 31(9): 2260 – 2263. (in Chinese)

[9] 韩敬,张文英,徐小华.对低轮 CLEFIA 分组密码的碰撞-Square 攻击 [J].电子学报,2009,37(10):2309 – 2313.
Han Jing, Zhang Wen-ying, Xu Xiao-hua. Collision-square attacks on the reduced-round CLEFIA [J]. Acta Electronica Sinica, 2009, 37(10): 2309 – 2313. (in Chinese)

[10] W Diffie, M Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard [J]. Computer, 1977, 10(6): 74 – 84.

[11] H Demirci, A A Selcuk. A meet-in-the-middle attack on 8-round AES [A]. FSE 2008 [C]. Berlin: LNCS 5086, Springer-Verlag, 2008. 116 – 126.

[12] H Demirci, I Taskin, M Coban, A Baysal. Improved meet-in-the-middle attacks on AES [A]. Indocrypt 2009 [C], Berlin: LNCS 5922, Springer-Verlag, 2009. 144 – 156.

[13] Duo Lei, Li Chao, Feng Ke-qing. New observation on camellia [A]. SAC 2005 [C], Berlin: LNCS 3897, Springer-Verlag, 2006. 51 – 64.

作者简介

唐学海 男,1984 年 2 月出生于四川三台.2009 年 3 月进入国防科技大学理学院数学与系统科学系学习.现为博士研究生在读,从事编码密码理论及其应用方面的研究.
E-mail: txh0203@163.com

孙 兵 男,1981 年 8 月出生于江苏南通.2009 年 12 月于国防科技大学理学院获理学博士学位.现为国防科技大学理学院讲师,研究方向为编码密码理论及其应用. E-mail: happy_come@163.com