

CLEFIA 密码的 Square 攻击

唐学海^① 李超^{①②} 谢端强^①

^①(国防科技大学数学与系统科学系 长沙 410073)

^②(东南大学移动通信国家重点实验室 南京 210096)

摘要: 该文根据 CLEFIA 密码的结构特性, 得到了 Square 攻击的新的 8 轮区分器, 并指出了设计者提出的错误 8 轮区分器。利用新的 8 轮区分器对 CLEFIA 密码进行了 10 到 12 轮的 Square 攻击, 攻击结果如下: 攻击 10 轮 CLEFIA-128\192\256 的数据复杂度和时间复杂度分别为 2^{97} 和 $2^{92.7}$; 攻击 11 轮 CLEFIA-192\256 的数据复杂度和时间复杂度分别为 2^{98} 和 $2^{157.6}$; 攻击 12 轮 CLEFIA-256 的数据复杂度和时间复杂度分别为 $2^{98.6}$ 和 2^{222} 。攻击结果表明: 在攻击 10 轮 CLEFIA 时, 新的 Square 攻击在数据复杂度和时间复杂度都优于设计者给出的 Square 攻击。

关键词: 密码; CLEFIA; 区分器; Square 攻击

中图分类号: TN918.1

文献标识码: A

文章编号: 1009-5896(2009)09-2260-04

Square Bttack on CLEFIA

Tang Xue-hai^① Li Chao^{①②} Xie Duan-qiang^①

^①(Department of Mathematics and System Science, National University of Defense Technology, Changsha 410073, China)

^②(National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

Abstract: According to the structure properties of CLEFIA, new 8-round distinguishers for Square attack are presented, and the wrong 8-round distinguishers originally found by the designers are pointed out. Based on the new distinguisher, the square attack on CLEFIA can be improved as follows: 10-round CLEFIA-128\192\256 is attacked with data complexity 2^{97} and time complexity $2^{92.7}$, 11-round CLEFIA-192/256 is attacked with data complexity 2^{98} and time complexity $2^{157.6}$, and 12-round CLEFIA-256 is breakable with data complexity $2^{98.6}$ and time complexity 2^{222} . These results demonstrate that under the case of 10-round CLEFIA, both data and time complexity of our attack are better than those given by the designers.

Key words: Cryptograph; CLEFIA; Distinguisher; Square attack

1 引言

CLEFIA 密码^[1,2]是 SONY 公司在 FSE2007 上提出的一种新的分组密码算法, 它的数据分组长度为 128 bit, 密钥长度可以是 128 bit, 192 bit 和 256 bit, 对应的轮数分别是 18, 22 和 26 轮。文献[1, 2]指出 CLEFIA 密码在安全性, 加密速度和执行成本等三方面达到了很好的平衡。在文献[1, 3]中, 密码设计者用各种已知的密码分析方法对其进行了安全评估, 包括差分分析^[4], 线性分析^[5], 差分-线性分析^[6], 截断差分分析^[7], 不可能差分分析^[8], Square 攻击^[9], 相关密钥分析^[10]和其它的一些分析方法。CLEFIA 密码提出以后, 国际上许多密码研究者也对其安全性进行了分析和评估^[11-14]。在所有的攻击方法中, 对 CLEFIA 密码比较有效的攻击是差分故障攻击和不可能差分攻击。

密码设计者在文献[3]中分析了 CLEFIA 密码的 10 轮 Square 攻击, 攻击的数据复杂度为 $2^{97.6}$, 时间复杂度为 $2^{123.7}$ 。本文根据 CLEFIA 密码的结构特性, 指出了文献[3]中的错误 8 轮区分器并给出了正确的 8 轮区分器, 进一步对原来的 Square 攻击方法进行了改进, 利用新的 8 轮区分器, 可以攻击 10 轮的 CLEFIA-128/192/256、11 轮的 CLEFIA-192/256 和 12 轮的 CLEFIA-256。攻击结果如下: 攻击 10 轮 CLEFIA-128\192\256 的数据复杂度和时间复杂度分别为 2^{97} 和 $2^{92.7}$; 攻击 11 轮 CLEFIA-192\256 的数据复杂度和时间复杂度分别为 2^{98} 和 $2^{157.6}$; 攻击 12 轮 CLEFIA-256 的数据复杂度和时间复杂度分别为 $2^{98.6}$ 和 2^{222} 。攻击结果表明: 新的 Square 攻击在攻击 10 轮 CLEFIA 时, 数据复杂度和时间复杂度都优于设计者所做的 Square 攻击, 如表 1 所示。

文章结构如下: 第 2 节对 CLEFIA 密码进行了简单的描述, 只介绍了对本文分析有用的相关部分; 第 3 节描述了 CLEFIA 密码的新的 8 轮 Square 区

2008-09-19 收到, 2009-04-28 改回

国家自然科学基金(60803156, 60573028)和东南大学移动通信国家重点实验室开放基金(w200805)资助课题

表 1 CLEFIA 密码的 Square 攻击结果

攻击方法	攻击轮数	密钥长度	数据复杂度 (选择明文数)	时间复杂度 (加密次数)
文献[3]	10	128/192/256	$2^{97.6}$	$2^{123.7}$
本文	10	128/192/256	2^{97}	$2^{92.7}$
本文	11	192/256	2^{98}	$2^{157.6}$
本文	12	256	$2^{98.6}$	2^{222}

分器, 指出了设计者提出的错误 8 轮区分器; 第 4 节详细描述了改进 Square 攻击方法对 CLEFIA 密码 10~12 轮的攻击; 第 5 节是结论。

2 CLEFIA 密码简介

CLEFIA 密码采用 4 条数据线路的广义 Feistel 结构, 它的数据分组长度是 128 bit, 密钥长度可以为 128 bit, 192 bit, 256 bit, 对应的加密轮数分别是 18, 22, 26。由于密钥扩展算法与本文攻击算法无关, 所以下面只介绍数据加密过程。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 128 bit 的明文和密文, 其中 $P_i, C_i \in \{0,1\}^{32}$ ($0 \leq i < 4$); $RK_i \in \{0,1\}^{32}$ ($0 \leq i < 2r$) 为轮密钥, $WK_0, WK_1, WK_2, WK_3 \in \{0,1\}^{32}$ 为白化密钥。 r 轮数据加密流程(具体轮变换和加密流程见图 1)如下:

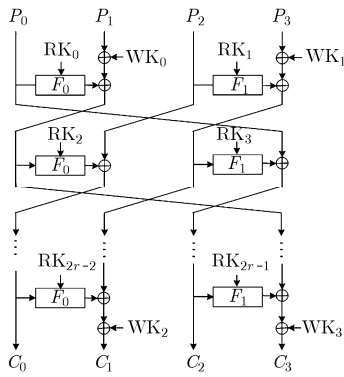


图 1 r 轮 CLEFIA 数据加密流程

步骤 1 计算 $T_0 | T_1 | T_2 | T_3 = P_0 | (P_1 \oplus WK_0) | P_2 | (P_3 \oplus WK_1)$;

步骤 2 对 $T_0 | T_1 | T_2 | T_3$ 进行 r 轮轮变换得到 $T'_0 | T'_1 | T'_2 | T'_3$;

步骤 3 计算 $C_0 | C_1 | C_2 | C_3 = T'_0 | (T'_1 \oplus WK_2) | T'_2 | (T'_3 \oplus WK_3)$ 。

图 1 中 F_0, F_1 是两个非线性可逆函数, 其具体实现与本文所述攻击无关, 本文不再赘述。

3 CLEFIA 密码的 8 轮 Square 区分器

Square 攻击是 Daemen 等针对 Square 密码^[9]提出的一种选择明文攻击方法。文献[3]利用这种方

法对 10 轮以及 10 轮以下的 CLEFIA 密码进行了分析, 其攻击均比穷尽密钥攻击快。下面介绍 Square 攻击的原理。

设 $X = \{X_i \in \{0,1\}^{32} | 0 \leq i < N\}$ 是 32 bit 数组, 则按如下方式, 可将 X 分成 4 类:

- (1) Const(C): if $\forall i, j X_i = X_j$;
- (2) All(A): if $\forall i, j i \neq j \Leftrightarrow X_i \neq X_j$;
- (3) Balance(B): if $\bigoplus_i X_i = 0$;
- (4) Unknown(U): 不是(1), (2), (3)。

现在考虑有 2^{32} 个明文的明文组, 它的其中一个 32 bit 的字遍历所有 2^{32} 种取值, 其余 3 个字都为常值, 比如它可以表示为 $(C C C A)$ 和 $(C A C C)$ 等形式。将这样的明文组作为输入, 文献[3]得到了下面的区分器。

- (1) $(C C C A) \xrightarrow{6r} (U U B U)$;
- (2) $(C A C C) \xrightarrow{6r} (B U U U)$;
- (3) $(A_{0(64)} A_{1(64)} C C) \xrightarrow{7r} (U U B U)$;
- (4) $(C C A_{0(64)} A_{1(64)}) \xrightarrow{7r} (B U U U)$;
- (5) $(A_{0(96)} A_{1(96)} A_{2(96)} C) \xrightarrow{8r} (U U B U)$;
- (6) $(A_{0(96)} C A_{1(96)} A_{2(96)}) \xrightarrow{8r} (B U U U)$ 。

其中 $A_{(64)} = A_{0(64)} | A_{1(64)}$ 表示 2^{64} 个 64 bit 的 A 状态集, $A_{(96)} = A_{0(96)} | A_{1(96)} | A_{2(96)}$ 表示 2^{96} 个 96 bit 的 A 状态集, nr 表示经过 n 轮变换。下面证明区分器(1)~(4)是正确的, 区分器(5)和(6)是错误的, 并给出正确的 8 轮区分器。

6 轮的区分器(2)详细流程见图 2, 易知其正确性, 区分器(1)类似。注意这里没有考虑白化密钥, 这是因为其为常值, 对上述区分器没有影响。对于区分器(3), 设第 1 轮的输入为 $(A_{0(64)} A_{1(64)} C C)$, 则经过一轮加密得到 $(B C C A_{0(64)})$, 由于加密运算是 1-1 映射, 故 $B | A_{0(64)}$ 遍历 2^{64} 种取值, 从而 $(B C C A_{0(64)})$ 可看作 2^{32} 个 $(C C C A)$, 再由 6 轮区分器(1)知区分器(3)是正确的, 类似可验证区分器(4)的正确性。对于区分器(5), 假设第 1 轮的输入为 $(A_{0(96)} A_{1(96)} A_{2(96)} C)$, 则经过第 1 轮加密得到 $(B A_{2(96)} A_{2(96)} A_{0(96)})$, 第 1 个字是平衡的, 再往下无法判断其性质, 也无法利用 7 轮区分器的结果, 不能确保第 8 轮输出的平衡性, 故区分器(5)是错误的, 类似可证区分器(6)也是错误的。

根据 CLEFIA 的加密结构特性, 我们可以得到下面的 8 轮 Square 区分器:

- (7) $(C A_{0(96)} A_{1(96)} A_{2(96)}) \xrightarrow{8r} (U U B U)$;
- (8) $(A_{0(96)} A_{1(96)} C A_{2(96)}) \xrightarrow{8r} (B U U U)$ 。

对与区分器(7), 易知经过第 1 轮加密有 $(C A_{0(96)} A_{1(96)} A_{2(96)}) \xrightarrow{1r} (U_0 U_1 U_2 C)$, 因为加密过程是 1-1 映射, $C | A_{0(96)} | A_{1(96)} | A_{2(96)}$ 共有 2^{96} 种取值, 所以 $U_0 |$

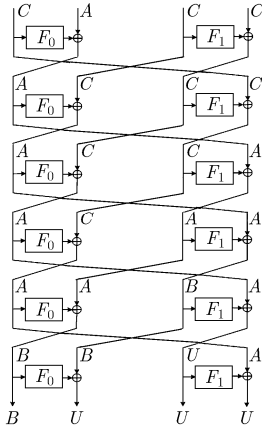


图2 6轮区分器

$U_1 | U_2 | C$ 也有 2^{96} 种取值, 即 $U_0 | U_1 | U_2$ 遍历 2^{96} 种取值, 即 $(U_0 U_1 U_2 C) = (A_{0(96)} A_{1(96)} A_{2(96)} C)$, 从而可将 $(A_{0(96)} A_{1(96)} A_{2(96)} C)$ 看作 2^{32} 个 $(A_{0(64)} A_{1(64)} C C)$, 再利用 7 轮区分器(3)知 8 轮区分器(7)是正确的, 区分器(8)类似可证。

4 CLEFIA 密码的 10~12 轮 Square 攻击

4.1 CLEFIA 密码的 10 轮 Square 攻击

对 CLEFIA 密码进行 10 轮 Square 攻击的基本思想是: 在上节中正确的 8 轮区分器后面再加两轮, 选择满足区分器输入状态的明文组进行 10 轮加密, 通过猜测最后两轮的部分密钥解密两轮, 验证第 8 轮的平衡性, 淘汰错误密钥。

对 CLEFIA 密码 10 轮的攻击见图 3(这里我们利用区分器(7))。由 F_0 的定义及加密结构, 令 $Y = F_1(RK_{19}, C_2) \oplus C_3 \oplus WK_3$, $Z = F_1(RK_{19}, C_2) \oplus C_3$, $RK'_{16} = RK_{16} \oplus WK_3$, 有下列关系式成立:

$$F_0(RK_{16}, Y) = F_0(RK_{16} \oplus WK_3, Z) = F_0(RK'_{16}, Z)$$

攻击过程需要恢复的密钥是 RK'_{16} 和 RK_{19} , 具体攻击步骤如下:

步骤 1 取 $RK'_{16\text{guess}}, RK_{19\text{guess}} \in \{0,1\}^{32}$ 分别作为 RK'_{16} 和 RK_{19} 的假设值;

步骤 2 任取一组形如 $(A_{0(96)} A_{1(96)} A_{2(96)} C)$ 含 2^{96} 个明文的明文组加密, 对任意的密文 $C_{(i)} = C_0 | C_1 | C_2 | C_3$, 计算 $Z_i = F_1(RK_{19\text{guess}}, C_2) \oplus C_3$ 和 $Y_i = F_0(RK'_{16\text{guess}}, Z_i) \oplus C_0$;

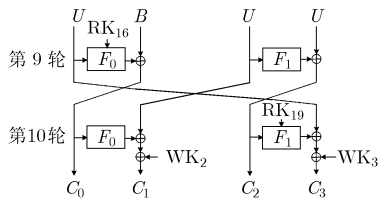


图3 10轮攻击图

步骤 3 计算 $Y = \oplus_i Y_i$, 由 8 轮区分器知, 若 $Y = 0$, 则对应的 $RK'_{16\text{guess}}, RK_{19\text{guess}}$ 分别作为 RK'_{16} 和 RK_{19} 的候选值, 反之则舍弃。

攻击复杂度分析如下: 任意一组假定的密钥(64 bit)能够被留下作为候选值的概率是 2^{-32} , 因此最多选两组含有 2^{96} 个明文的明文组便可唯一确定正确的密钥, 所以数据复杂度为 $2 \times 2^{96} = 2^{97}$ 。对于每一组假设的密钥, 计算 2^{32} 次 F_1 和最多 2^{32} 次 F_0 , 这是因为在密钥固定的情况下计算 F_1 只依赖于变量 C_2 , 而 C_2 的取值最多只有 2^{32} 种(有相同的不再重复计算), F_0 类似。由此可知, 处理第 1 组密文需要计算 $2^{64} \times 2 \times 2^{32}$ 次 F 函数, 留下的密钥数是 $2^{64} \times 2^{-32}$, 处理第 2 组密文需要计算 $2^{64} \times 2^{-32} \times 2 \times 2^{32}$ 次 F 函数。由于 10 轮算法加密一个数据需要计算 $2 \times 10 = 20$ 次 F 函数, 所以该攻击的时间复杂度是 $(2^{64} \times 2 \times 2^{32} + 2^{64} \times 2^{-32} \times 2 \times 2^{32}) / 20 \approx 2^{92.7}$ 。由上面的分析可知, 这种方法适用于所有长度密钥的 10 轮 CLEFIA 算法。

4.2 CLEFIA 密码的 11 轮和 12 轮 Square 攻击

在上述 10 轮攻击的基础上, 如果在末尾再加一轮, 类似地可以得到 CLEFIA 密码的 11 轮 Square 攻击(见图 4)。令 $RK'_{19} = RK_{19} \oplus WK_2$, 具体的攻击步骤如下:

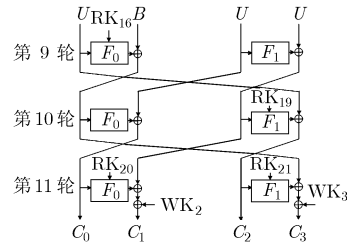


图4 11轮攻击图

步骤 1 $(RK_{16\text{guess}}, RK'_{19\text{guess}}, RK_{20\text{guess}}, RK_{21\text{guess}}) \in \{0,1\}^{128}$;

步骤 2 任取一组形如 $(A_{0(96)} A_{1(96)} A_{2(96)} C)$ 含 2^{96} 个明文的明文组加密, 对任意的密文 $C_{(i)} = C_0 | C_1 | C_2 | C_3$, 依次计算:

$$X_i = F_0(RK_{20\text{guess}}, C_0) \oplus C_1, Y_i = F_1(RK'_{19\text{guess}}, X_i) \oplus C_2, Z_i = F_1(RK_{21\text{guess}}, C_2) \oplus C_3 \text{ 和 } W_i = F_0(RK_{16\text{guess}}, Y_i) \oplus Z_i;$$

步骤 3 计算 $V = \oplus_i W_i$, 若 $V=0$ 则将 $(RK_{16\text{guess}}, RK'_{19\text{guess}}, RK_{20\text{guess}}, RK_{21\text{guess}})$ 作为 $(RK_{16}, RK'_{19}, RK_{20}, RK_{21})$ 的候选值, 反之舍弃, 然后重复上述步骤。

类似 10 轮攻击的分析知, 选取 4 组个数为 2^{96} 的明文组即可找到正确的密钥。数据复杂度为 4×2^{96}

$= 2^{98}$, 时间复杂度为 $[2^{128}(1 + 2^{-32} + 2^{-64} + 2^{-96}) \times 4 \times 2^{32}] / 22 \approx 2^{157.6}$, 故这种方法只适用于长度为 192 bit 和 256 bit 的密钥。

在 11 轮的基础上再加一轮, 就可以得到 CLEFIA 密码的 12 轮 Square 攻击, 类似 11 轮的攻击, 需要恢复的密钥是 $RK_{16} \oplus WK_2, RK_{19}, RK_{20} \oplus WK_3, RK_{21} \oplus WK_2, RK_{22}, RK_{23}$ 。数据复杂度是 $2^{96} \times 6 \approx 2^{98.6}$, 时间复杂度是 $[2^{192}(1 + 2^{-32} + 2^{-64} + 2^{-96} + 2^{-128} + 2^{-160}) \times 6 \times 2^{32}] / 24 \approx 2^{222}$, 故只适用于 256 bit 的密钥。

5 结论

本文给出了 CLEFIA 密码新的正确的 8 轮 Square 区分器及 10 轮, 11 轮和 12 轮的 Square 攻击原理和过程。攻击结果表明: 10 轮 Square 攻击的数据复杂度和时间复杂度分别为 2^{97} 和 $2^{92.7}$, 均优于设计者给出的分析结果; 11 轮攻击的数据复杂度是 2^{98} , 时间复杂度是 $2^{157.6}$, 适用于长度为 192 bit 和 256 bit 的密钥; 12 轮攻击的数据复杂度是 $2^{98.6}$, 时间复杂度是 2^{222} , 只适用于 256 bit 的密钥。密钥扩展算法对 Square 攻击复杂度的影响正在研究中。

参考文献

- [1] Shirai T, Shibutani K, Akishita T, Moriai S, and Iwata T. The 128-bit block cipher CLEFIA [C]. Fast Software Encryption 2007, Springer, Heidelberg, 2007, Vol. 4593: 181-195.
 - [2] Sony Corporation. The 128-bit Blockcipher CLEFIA: Algorithm Specification. Revision 1.0 June 1, 2007.
 - [3] Sony Corporation. The 128-bit Blockcipher CLEFIA: Security and Performance Evaluation. Revision 1.0 June 1, 2007.
 - [4] Biham E and Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. *Journal of Cryptology*, 1991, 4(1): 3-72.
 - [5] Matsui M. Linear cryptanalysis of the data encryption standard[C]. Proceedings of Eurocrypt' 93, Springer-Verlag, 1994, LNCS 765: 386-397.
 - [6] Langford S K and Hellman M E. Differential-linear cryptanalysis[C]. Proceedings of Crypto' 94, Springer-Verlag, 1994, LNCS 839: 17-25.
 - [7] Knudsen L R. Truncated and higher order differentials[C]. Fast Software Encryption: Second International Workshop, Springer-Verlag, 1994, LNCS1008: 196-211.
 - [8] Biham E, Biryukov A, and Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]. Proceedings of Eurocrypt' 99, Springer-Verlag, 1999, LNCS 1592: 12-23.
 - [9] Daemen J, Knudsen L, and Rijmen V. The block cipher square[C]. Fast Software Encryption 1997, Springer-Verlag, 1997, LNCS 1267: 149-165.
 - [10] Biham E. New types of cryptanalytic attacks using related keys[J]. *Journal of Cryptology*, 1994, 7(4): 229-246.
 - [11] Chen Hua, Wu Wen-ling, and Feng Deng-guo. Differential fault analysis on CLEFIA[C]. International Conference on Information and Communications Security, Birmingham, UK, 2008, LNCS 4861: 284-295.
 - [12] Takahashi J and Fukunaga T. Improved differential fault analysis on CLEFIA[C]. Fault Diagnosis and Tolerance in Cryptography 2008, Washington, DC, USA, 2008: 25-34.
 - [13] Wang Wei and Wang Xiao-yun. Improved impossible differential cryptanalysis of CLEFIA[R]. IACR ePrint archive: Report 2007/466.
 - [14] Tsunoo Y, Tsujihara E, Shigeri M, Saito T, Suzaki T, and Kubo H. Impossible differential cryptanalysis of CLEFIA[C]. Fast Software Encryption 2008, Lausanne, Switzerland, 2008: 398-411.
- 唐学海: 男, 1984 年生, 硕士生, 研究方向为编码密码理论及其应用。
李超: 男, 1966 年生, 教授, 博士生导师, 研究方向为编码密码理论及其应用。
谢端强: 男, 1963 年生, 教授, 硕士生导师, 研究方向为编码密码理论及其应用。