CS-CIPHER 两个变体的线性密码分析

吴文玲, 卿斯汉
(中国科学院信息安全技术工程研究中心, 北京 100080; 中国科学院软件研究所信息安全国家重点实验室, 北京 100080)

摘 要: CS-CIPHER 是 NESSIE 公布的 17 个候选算法之一, 它的分组长度为 64 比特. 本文对 CS-CIPHER 的两个变体进行了线性密码分析. 对第一个变体的攻击成功率约为 78.5%, 数据复杂度为 2^{52}, 处理复杂度为 2^{32}. 对第二个变体的攻击成功率约为 78.5%, 数据复杂度为 2^{52}, 处理复杂度为 2^{112}.

关键词: 分组密码; 线性密码分析; S 盒
中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2002) 02-0283-03

Linear Cryptanalysis on Two Variants of CS-CIPHER

WU Wen-ling, QING Si-han
(1. *Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing* 100080, *China*;
2. *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: CS-CIPHER is a block cipher as a candidate for NESSIE, whose block length is 64 bits. In this paper two variants of CS-CIPHER by linear cryptanalysis. The attack to the first variant needs 2^{32} counters and 2^{52} known plaintexts. The success rate of attack is about 78.5%. The attack to the second variant needs 2^{52} known plaintexts and 2^{112} counters. The success rate is about 78.5%.

Key words: block cipher; linear cryptanalysis; S-box

1 引言

CS-CIPHER[1] 最早发表于 1998 年, 2000 年又作为 NESSIE 的候选算法公布, 它的分组长度为 64 比特, 密钥长度是可变的, 可达 128 比特. 文献[1]称 CS-CIPHER 是一个 8 轮迭代密码, 它的轮函数基于快速傅立叶变换和 F_2^{16} 上的函数 M, 轮函数中实际包含了 3 层"混淆层"; 因此, CS-CIPHER 的结构本质上类似 SHARK[2]、Square[3]和 SAFER[4], 采用的是 SP 结构, 由前期白化, 24 轮运算和后期白化组成. 限于篇幅, 这里不详列 CS-CIPHER 的加密算法和密钥编排算法. 鉴于密码体制的关键不在于前期白化和后期白化, 所以本文不考虑 CS-CIPHER 的前期白化和后期白化. CS-CIPHER 的轮函数 F_i 定义如下:

$$F_i = P(S^8(X \oplus c^i))$$

S^8 由 8 个 S 盒并置而成;

$$c^i = \begin{cases} K^j, & i = 3j \\ c, & i = 3j+1, \\ c', & i = 3j+2 \end{cases}$$

K^j 是子密钥, c 和 c' 是给定的常数; P 如图 1 所示, 其中 R_l 表示左循环 1 位,

$\psi: F_2^8 \to F_2^8 \qquad X \to (R_l(X) \wedge 0x55) \oplus X.$

2 CS-CIPHER 的线性逼近

S^8 是 CS-CIPHER 的非线性层, 令 $Y = S(X)$, 通过测试, S 有如下线性逼近:

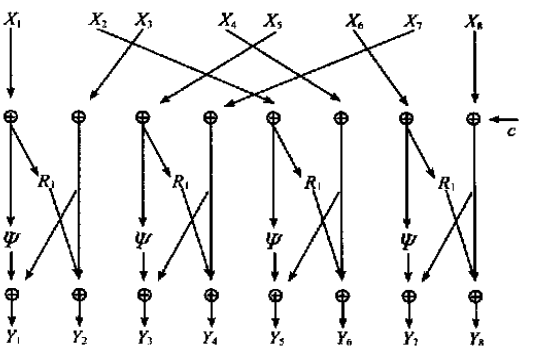

图 1 P 变换

$$Y[7] = X[7], \quad \left| p - \frac{1}{2} \right| = 2^{-3} \tag{1}$$

$$Y[7,6] = X[7], \quad \left| p - \frac{1}{2} \right| = 2^{-5} \tag{2}$$

利用式(1)、(2)和 p 的特点, 构造两轮 CS-CIPHER 的线性逼近. 如图 2 所示可得两轮线性逼近:

$$X[63,27] \oplus Y[63,27] = c^i[63,62,27,26] \oplus c^{i+1}[63,55,48,39] \tag{3}$$

式(3)的概率满足: $\left| p - \frac{1}{2} \right| = 2^{-17}$.

如图 3 所示可得两轮线性逼近:

收稿日期: 2000-06-22; 修回日期: 2001-10-22
基金项目: 国家自然科学基金(No. 60103023)

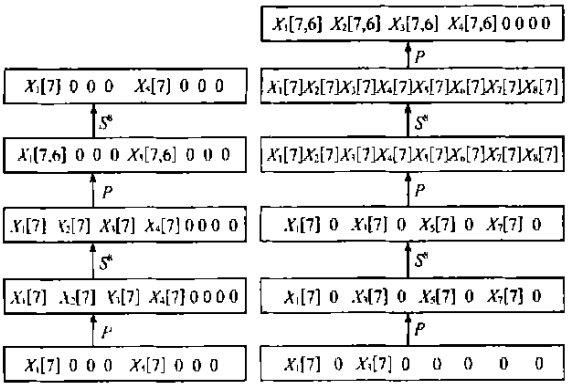

图 2 2 轮线性逼近(3) 图 3 2 轮线性逼近(4)

$$X[63, 62, 55, 54, 47, 46, 39, 38] \oplus Y[63, 47] = c^i[63, 62, 55, 54, 47, 46, 39, 38] \oplus c^{i+1}[63, 55, 47, 39, 31, 23, 15, 7] \oplus c^{i+2}[63, 55, 47, 39] \quad (4)$$

式(4)的概率满足: $\left| p - \frac{1}{2} \right| = 2^{-25}$.

3 CS1 的线性密码分析

CS-CIPHER 的主体是 24 轮 SP 网络, 但是只有 8 轮有密钥嵌入, 因此, 这里讨论 CS-CIPHER 的一个变体—CS1, 它的子密钥是 $K^0, K^1, K^2, K^3, K^4, K^5$.

令 X^0 是明文, $X^i (1 \le i \le 6)$ 是第 i 轮的输出, 则 CS1 的加密过程为:

$$X^6 = P(S^8(P(S^8(P(S^8(P(S^8(P(S^8(X^0), K^0)), K^1)), K^2)), K^3)), K^4)), K^5)$$

利用方程(3), 我们构造如下线性逼近:

$$X^1[63, 55, 47, 39] \oplus X^4[63, 31] = K^1[63, 55, 31, 23] \oplus K^2[63, 62, 31, 30] \oplus K^3[63, 55, 31, 23] \quad (5)$$

方程(5)的概率满足: $|p - 1/2| = 2^{-25}$.

令 X_j^i 是 X^i 的第 j 字节(从右到左), 利用 P 的特点, 我们得到如下方程:

$$X^1[63] = S(X_1^0)[7] \oplus S(X_3^0)[7] \oplus K^0[63, 55]$$
$$X^1[55] = S(X_1^0)[0] \oplus S(X_3^0)[7] \oplus K^0[56, 55]$$
$$X^1[47] = S(X_5^0)[7] \oplus S(X_7^0)[7] \oplus K^0[47, 39]$$
$$X^1[39] = S(X_5^0)[0] \oplus S(X_7^0)[7] \oplus K^0[40, 39]$$

因此, 有

$$X^1[63, 55, 47, 39] = S^8(X^0)[63, 56, 31, 24] \oplus K^0[63, 56, 47, 40] \quad (6)$$

如果已知 $X_1^5, X_2^5, X_3^5, X_4^5$, 则有

$$X^4[63] = (X_1^5 \oplus X_2^5)[7, 6] \oplus K^4[63]$$
$$X^4[31] = (X_3^5 \oplus X_4^5)[7, 6] \oplus K^4[47]$$

因此

$$X^4[63, 31] = (X_1^5 \oplus X_2^5)[7, 6] \oplus (X_3^5 \oplus X_4^5)[7, 6] \oplus K^4[63, 47] \quad (7)$$

由 P 的特点可知: $(X_1^5, X_2^5, X_3^5, X_4^5)$ 仅和 K^5 的第 1、2、5 和 6 字节有关. 令 $K' = (X_1^5, X_2^5, X_5^5, X_6^5)$, $F = PS^8$, 则

$$(X_1^5 \oplus X_2^5)[7, 6] \oplus (X_3^5 \oplus X_4^5)[7, 6] = (F^{-1}(X^5, K')_1 \oplus F^{-1}(X^5, K')_2)[7, 6] \oplus (F^{-1}(X^5, K')_3 \oplus F^{-1}(X^5, K')_4)[7, 6] \quad (8)$$

利用方程(5)、(6)、(7)和(8), 可得

$$S^8(X^0)[63, 56, 31, 24] \oplus (F^{-1}(X^5, K')_1 \oplus F^{-1}(X^5, K')_2)[7, 6] \oplus (F^{-1}(X^5, K')_3 \oplus F^{-1}(X^5, K')_4)[7, 6] = K^0[63, 56, 47, 40] \oplus K^1[63, 55, 31, 23] \oplus K^2[63, 62, 31, 30] \oplus K^3[63, 55, 31, 23] \oplus K^4[63, 47] \quad (9)$$

利用线性逼近(9)攻击 CS1, 攻击的数据复杂度为 2^{52}, 处理复杂度为 2^{32}, 成功率约为 78.5%.

4 CS2 的线性密码分析

CS2 是 4-轮 CS-Cipher, 且没有最后一轮的子密钥加; 它的加密过程如下:

$$S^8P(\cdots S^8P(X, K^0), c), c'), \cdots K^2), c), c')K^3), c), c')$$

令 X 和 Y 分别表示输入和输出, 攻击如下操作:

第一步, 对给定的 $K^3(2^{64})$, 解密密文得

$$S^8P(\cdots(S^8P(S^8P(X, K^0), c), c'), K^1), c), c'), K^2) = S^{-8}(P^{-1}S^{-8}\cdots(P^{-1}S^{-8}(Y, c'), c), K^3), c'), c)$$

第二步, 对给定的 $(K_1^3, K_3^3, K_5^3, K_7^3)$, 解密第一步的结果可得

$$P(S^8P\cdots(S^8P(X, K^0), c), c'), K^1) = F'(Y, K^3, K_1^2, K_3^2, K_5^2, K_7^2)$$ 的第一和第三字节.

第三步, 对给定的 $(K_1^0, K_2^0, K_3^0, K_4^0)$, 可得 $P(S^8P(X, K^0))$ 的第 1、2、3 和 4 字节.

第四步, 利用方程(4), 构造如下线性逼近:

$$P(S^8P(X, K_1^0, K_2^0, K_3^0, K_4^0))[63, 62, 55, 54, 47, 46, 39, 38] \oplus [63, 47] = c[63, 62, 55, 54, 47, 46, 39, 38] \oplus c'[63, 55, 47, 39, 31, 23, 15, 7] \oplus K^1[63, 55, 47, 39] \quad (10)$$

方程(10)的概率满足 $|p - 1/2| = 2^{-25}$.

第五步, 利用方程(10)和文献[5]中的算法 2 攻击 CS2.

如果已知 $(K_1^0, K_2^0, K_3^0, K_4^0)$ 和 K^3, 可以由密钥编排算法计算 K_1^2 和 K_3^2; 因此, 攻击的数据复杂度为 2^{52}, 处理复杂度为 2^{32}, 成功率约为 78.5%.

5 结束语

CS-CIPHER 的整体结构看似复杂, 但本质上类似 SHARK, 采用的是 SP 结构, 且基础模块的密码特性没有 SHARK 的好; 因此, 对 CS-CIPHER 存在概率满足 $|p - 1/2| = 2^{-17}$ 和 $|p - 1/2| = 2^{-25}$ 的两轮线性逼近. 利用这两个线性逼近, 分析 CS-CIPHER 的两个变体, 对第一个变体的攻击成功率约为 78.5%, 数据复杂度为 2^{52}, 处理复杂度为 2^{32}; 对第二个变体的攻击成功率约为 78.5%, 数据复杂度为 2^{52}, 处理复杂度为 2^{112}.

参考文献:

[1] Jacques Stern, Serge Vaudenay. CS-CIPHER [A]. In Fast Software En-

cryption, Paris, France, Lectures Notes in Computer Science 1372 [C], Springer-Verlag, 1998: 189- 205.

[2] J Daemen, L Kundsen, V Rijmen. The cipher SHARK [A]. In Fast Software Encryption, Cambridge, England, Lectures Notes in Computer Science 1372 [C], Springer- Verlag, 1996: 99- 111.

[3] V Rijmen, J Daemen. The block cipher SQUARE [A]. In Fast Software Encryption, Haifa, Israel, Lectures Notes in Computer Science 1267 [C], Springer-Verlag, 1997: 149- 165.

[4] J L Massey. Safer K- 64: a byte-oriented block-ciphering algorithm [A]. In Fast Software Encryption, Cambridge, England, Lectures Notes in Computer Science 1372 [C], Springer-Verlag, 1993: 1- 7.

[5] M Matsui. Linear cryptanalysis method for DES cipher [A]. Advances in Cryptology-EUROCRYPT' 93 [C], Springer-Verlag, 1995: 386- 397.

[6] S Vaudenay. On the security of CS-cipher [A]. In Fast Software Encryption, Rome, Italy, Lectures Notes in Computer Science 1636 [C], Springer-Verlag, 1999: 260- 274.

作者简介:

吴文玲　女. 1966 年生于陕西省蒲城县. 1990 年 7 月于西北大学获硕士学位, 1997 年 9 月于西安电子科技大学获密码学专业博士学位, 1997 年 12 月至 1999 年 12 月在中国科学院信息安全技术工程研究中心做博士后, 现为中国科学院软件研究所副研究员. 近几年一直从事分组密码的研究, 研制了一系列实用的分组密码算法, 发表 50 余篇论文, 合作出版著作一部.

卿斯汉　男. 1939 年生. 中国科学院软件研究所研究员, 博士生导师, 中国科学院信息安全技术工程研究中心主任, 研究兴趣包括密码学、信息及网络安全等.