LOKI97 的线性密码分析*

吴文玲 李宝 冯登国 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)

E-mail: wwl@ercist.iscas.ac.cn

摘要 该文利用线性密码分析对 LOKI97 进行了攻击,结果显示,LOKI97 的安全性并没有达到高级加密标准的要求;利用线性密码分析中的算法 1 和 2^{50} 个明密文对,以 0.977 的成功率预测 92 比特子密钥;利用线性密码分析中的算法 2 和 2^{45} 个明密文对,以 0.967 的成功率预测 LOKI97 的种子密钥.

关键词 线性密码分析,线性逼近,非线性度.

中图法分类号 TP309

LOKI97 是美国国家标准技术研究所(NIST)公布的 15 个 21 世纪高级加密标准(advanced encryption standard,简称 AES)的候选算法之一,它是 LOKI 系列密码的最新产品. Biham 和 Shamir 在文献[1]中对 LOKI89 进行了分析,结果显示,虽然 LOKI89 减少几轮变体后可能易受差分密码分析的攻击,但全部 16 轮的 LOKI89 却经得起差分密码分析的攻击. Tokita Sorimachi 和 Matsui 在文献[2]中对 LOKI91 对进行了线性密码分析,发现 12 轮以上的 LOKI91 对线性密码分析是安全的. LOKI97 选取的 S-盒的非线性性能非常好,S_1 的线性逼近的概率 p 满足: $\frac{1}{2}-2^{-7}\leqslant p\leqslant\frac{1}{2}+2^{-7}$, S_2 的线性逼近的概率 p 满足: $\frac{1}{2}-2^{-6}\leqslant p\leqslant\frac{1}{2}+2^{-6}$. 由此,文献[3]给出下列结果:

- 单轮的最佳线性逼近概率 p_{best} 满足: $\frac{1}{2}-2^{-11}\leqslant p_{best}\leqslant\frac{1}{2}+2^{-11}$;
- 14 轮 LOKI97 的最佳线性逼近概率 p_{best} 满足: $\frac{1}{2}-2^{-141}\leqslant p_{best}\leqslant\frac{1}{2}+2^{-141}$;
- 16 轮 LOKI97 的最佳线性逼近概率 p_{best} 满足: $\frac{1}{2}-2^{-161}\leqslant p_{best}\leqslant\frac{1}{2}+2^{-161}$.

利用文献[4]和上面的结果,可以估计出用线性密码分析攻击 LOKI97 所需的明密文对大约为 2^{282}. 这似乎反映了 LOKI97 对线性密码分析是免疫的,然而,事实却不然,在本文中,我们利用 LOKI97 轮函数的特点,对某些密钥构造出单轮的线性逼近,它们仅涉及输出和密钥,然后利用"+"运算对于最低比特位的线性性,把单轮的线性逼近结合起来,构造出 14 轮和 16 轮 LOKI97 的线性逼近,它们的概率 p 分别满足:

$$\frac{1}{2}-2^{-21}\leqslant p\leqslant\frac{1}{2}+2^{-21},$$

$$\frac{1}{2}-2^{-25}\leqslant p\leqslant\frac{1}{2}+2^{-25}.$$

利用这些线性逼近,我们对 LOKI97 进行线性密码分析.

1 LOKI97 算法描述

LOKI97 的分组长度为 128 比特,密钥长度为 128,192,256 比特. 它采用的是 16 轮的 Fesitel 结构.

* 本文研究得到国家自然科学基金(No. 69673016)和国家博士后基金资助. 作者吴文玲,女,1966 年生,博士后,主要研究领域为分组密码的设计与分析. 李宝,1962 年生,博士后,主要研究领域为椭圆曲线公钥密码体制的分析与实现. 冯登国,1965 年生,研究员,主要研究领域为信息安全. 卿斯汉,1939 年生,研究员,博士生导师,主要研究领域为信息安全技术.

本文通讯联系人:吴文玲,北京 100080,中国科学院信息安全技术工程研究中心

本文 1998-12-15 收到原稿,1999-03-17 收到修改稿

1.1 加密过程

1.1.1 加密算法的总体结构

$P=L_0|R_0$ 为 128 比特的明文输入，用下列方式计算密文，对于 $j=1,\ldots,16$，有

$$R_i=L_{i-1}\oplus F(R_{i-1}+K3_{i-2},K3_{i-1}),$$

$$L_i=R_{i-1}+K3_{i-2}+K3_i,$$

$$C=R_{16}|L_{16}\text{为密文}.$$

1.1.2 轮函数 F

轮函数 $F:F_2^{64}\times F_2^{64}\to F_2^{64}$，

$$F(A,B)=Sb(P(Sa(E(KP(A,B)))),B).$$

$KP(A,B)$是一个简单的密钥控制置换，它将 64 比特输入 A 分成两个 32 比特字，用输入 B 的较低(最右边) 32 比特确定是交换这些字中比特的相应位(如果密钥比特是 1)，还是不交换(如果密钥比特为 0).

E 是一个扩展函数，E 从 64 个输入比特中产生一个 96 比特输出值.

$$[4-0,63-56|58-48\ 52-40|42-32|34-24|28-16|18-8|12-0].$$

Sa 由盒 S_1 和盒 S_2 并置构成，$Sa=[S_1,S_2,S_1,S_2,S_2,S_2,S_2,S_1]$，$Sa$ 的输入是 E 的输出.

P 把输入比特[63—0]映射到输出比特：

$$[56,48,40,32,24,16,08,00,57,49,41,33,25,17,09,01,$$
$$58,50,42,34,26,18,10,02,59,51,43,35,27,19,11,03,$$
$$60,52,44,36,28,20,12,04,61,53,45,37,29,21,13,05,$$
$$62,54,46,38,30,22,14,06,63,55,47,39,31,23,15,07],$$

即输入比特 63 转入输出比特 56，输入比特 62 转入输出比特 48 等.

Sb 由盒 S_1 和盒 S_2 并置构成，$Sb=[S_2,S_2,S_1,S_1,S_2,S_2,S_1,S_1]$，$Sb$ 的输入是

$$B[63-61]|P[63-56],\ B[60-58]|P[55-48],\ B[57-53]|P[47-40],$$
$$B[52-48]|P[39-32],\ B[47-45]|P[31-24],\ B[44-42]|P[23-16],$$
$$B[41-37]|P[15-8],\ B[36-32]|P[7-0],$$

其中 $B[63-61]$表示由 B 的第 63 到 61 比特组成的比特串. Sb 的第 1 个 S 盒 S_2 的输入为 $B[63-61]|P[63-56]$.

1.2 解密过程

输入密文 $C=R_{16}|L_{16}$，然后反向对轮进行操作. 即对 $i=1,\ldots,16$，有

$$L_{i-1}=R_i\oplus F(L_i-K3_i,K3_{i-1}),$$

$$R_{i-1}=L_i-K3_i-K3_{i-2},$$

$P=L_0|R_0$，即为明文.

1.3 密钥方案

16 轮 LOKI97 需要 48 个 64 比特的密钥，我们用下述方法把种子密钥 K 扩展为子密钥. 首先，依据种子密钥的长度，预制 4 个 64 比特字$[K4_0|K3_0|K2_0|K1_0]$.

$K=[Ka|Kb|Kc|Kd]$为 256 比特，令$[K4_0|K3_0|K2_0|K1_0]=[Ka|Kb|Kc|Kd]$；

$K=[Ka|Kb|Kc]$为 192 比特，令$[K4_0|K3_0|K2_0|K1_0]=[Ka|Kb|Kc|f(Ka,Kb)]$；

$K=[Ka|Kb]$为 128 比特，令$[K4_0|K3_0|K2_0|K1_0]=[Ka|Kb|f(Kb,Ka)|f(Ka,Kb)]$，

然后对 $i=1,\ldots,48$ 作如下计算：

$$K_i=K1_i=K4_{i-1}\oplus g_i(K1_{i-1},K3_{i-1},K2_{i-1}),$$

$$K4_i=K3_{i-1},$$

$$K3_i=K2_{i-1},$$

$$K2_i=K1_{i-1},$$

其中 $g_i(K1,K3,K2)=F(K1+K3+(Delta*i),K2)$,

$$Delta=\lfloor(sqrt(5)-1)*2^{63}\rfloor=9E3779B97F4A7C15_{16}.$$

2　LOKI97 的线性逼近

令 $S_1(x_{12},\ldots,x_2,x_1,x_0)=(f_7,f_6,f_5,f_4,f_3,f_2,f_1,f_0)$:$F_2^{13}\to F_2^8$,通过计算,我们给出 S_1 的分支函数 f_0 的代数表达式为:

$$\begin{aligned}f_0=&x_{12}\oplus x_{12}x_{11}\oplus x_{10}\oplus x_9\oplus x_{12}x_9\oplus x_9x_8\oplus x_7\oplus x_{11}x_7\oplus x_{10}x_7\oplus x_6\oplus x_{12}x_6\oplus x_{11}x_6\oplus x_{10}x_6\oplus\\&x_9x_6\oplus x_7x_6\oplus x_{12}x_7\oplus x_9x_7\oplus x_6x_5\oplus x_{12}x_4\oplus x_{10}x_4\oplus x_9x_4\oplus x_8x_4\oplus x_{11}x_3\oplus x_8x_3\oplus x_6x_3\oplus\\&x_5x_3\oplus x_{12}x_2\oplus x_{11}x_2\oplus x_9x_2\oplus x_8x_2\oplus x_{11}x_1\oplus x_{10}x_1\oplus x_9x_1\oplus x_8x_1\oplus x_7x_1\oplus x_6x_1\oplus x_9x_0\oplus 1.\end{aligned}$$

令$(x_{12},x_{11},x_{10},x_9,x_8)=i$,$0\leqslant i\leqslant 31$,可得 32 个布尔函数 $g_i(x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0)$,它们的汉明重量归纳如下:

$W_H(g_0)=144$, $W_H(g_1)=128$, $W_H(g_2)=128$, $W_H(g_3)=128$, $W_H(g_4)=144$, $W_H(g_5)=128$,
$W_H(g_6)=128$, $W_H(g_7)=128$, $W_H(g_8)=128$, $W_H(g_9)=144$, $W_H(g_{10})=128$, $W_H(g_{11})=128$,
$W_H(g_{12})=128$, $W_H(g_{13})=112$, $W_H(g_{14})=128$, $W_H(g_{15})=128$, $W_H(g_{16})=128$, $W_H(g_{17})=112$,
$W_H(g_{18})=128$, $W_H(g_{19})=128$, $W_H(g_{20})=128$, $W_H(g_{21})=144$, $W_H(g_{22})=128$, $W_H(g_{23})=128$,
$W_H(g_{24})=112$, $W_H(g_{25})=128$, $W_H(g_{26})=128$, $W_H(g_{27})=128$, $W_H(g_{28})=112$, $W_H(g_{29})=128$,
$W_H(g_{30})=128$, $W_H(g_{31})=128$.

显然,$g_0,g_4,g_9,g_{13},g_{17},g_{21},g_{24},g_{28}$是非平衡的布尔函数,因此,它们的非线性度小于 16.又因为轮函数 F 的 S_5 层的每一个 S 盒的最高几比特输入是子密钥,所以对某些密钥,可以给出轮函数 $F(X,K)=Y$ 的一批概率为 $p=\frac{1}{2}+\frac{1}{2^4}$且仅涉及输出和密钥的线性逼近:

$$Y[0]=K[h(36-32)],\tag{1}$$

其中 $K[h(36-32)]=h(k_{36},k_{35},k_{34},k_{33},k_{32})$,$h$ 是线性布尔函数.

令(L_{i-1},R_{i-1})和(L_i,R_i)分别是第 i 轮的输入和输出,

$$L_i=R_{i-1}+K_i^1+K_i^3,\tag{2}$$

$$R_i=L_{i-1}\oplus F(R_{i-1},K_i^2).\tag{3}$$

对于式(2),有下列概率为 1 的线性逼近:

$$E_i:\ L_i[0]=R_{i-1}[0]\oplus K_i^1[0]\oplus K_i^3[0].$$

对于式(3),利用式(1),给出下列概率为$\frac{1}{2}+\frac{1}{2^4}$的线性逼近:

$$D_i:\ R_i[0]=L_{i-1}[0]\oplus K_i^2[h(36-32)].$$

对于 16 轮的 LOKI97,令(L_0,R_0)和(R_{16},L_{16})分别是它的输入和输出,我们构造轨迹为$(E_1,D_2,E_3,D_4,E_5,D_6,E_7,D_8,E_9,D_{10},E_{11},D_{12},E_{13},D_{14},E_{15},D_{16})$的线性逼近:

$$R_0[0]\oplus\Big(\bigoplus_{\substack{1\leqslant i\leqslant 16\\ i\ \text{odd}}}(K_i^1[0]\oplus K_i^3[0])\Big)\oplus\Big(\bigoplus_{\substack{1\leqslant i\leqslant 16\\ i\ \text{even}}}(K_i^2[h(36-32)])\Big)=R_{16}[0].\tag{4}$$

轨迹为$(D_1,E_2,D_3,E_4,D_5,E_6,D_7,E_8,D_9,E_{10},D_{11},E_{12},D_{13},E_{14},D_{15},E_{16})$的线性逼近:

$$L_0[0]\oplus\Big(\bigoplus_{\substack{1\leqslant i\leqslant 16\\ i\text{是偶数}}}(K_i^1[0]\oplus K_i^3[0])\Big)\oplus\Big(\bigoplus_{\substack{1\leqslant i\leqslant 15\\ i\text{是奇数}}}(K_i^2[h(36-32)])\Big)=L_{16}[0].\tag{5}$$

式(4)和式(5)的概率都满足:$\frac{1}{2}-2^{-25}\leqslant p\leqslant\frac{1}{2}+2^{-25}$.

从第 2 轮开始,以轨迹$(E_2,D_3,E_4,D_5,E_6,D_7,E_8,D_9,E_{10},D_{11},E_{12},D_{13},E_{14},D_{15},E_{16})$构造线性逼近:

$$L_0[0]\oplus F(R_0-K_1^1,K_1^2)[0]\oplus k=L_{16}[0],\tag{6}$$

其中 $k=\Big(\bigoplus_{\substack{2\leqslant i\leqslant 16\\ i\text{是偶数}}}(K_i^1[0]\oplus K_i^3[0])\Big)\oplus\Big(\bigoplus_{\substack{2\leqslant i\leqslant 15\\ i\text{是奇数}}}(K_i^2[h(36-32)])\Big)$,式(6)的概率满足:

$$\frac{1}{2}-2^{-21}\leqslant p\leqslant\frac{1}{2}+2^{-21}.$$

3 LOKI97 的线性密码分析

利用式(4)，我们以 0.977 的成功率预测 K_i^2 的第 36 到 32 比特，i 是偶数，$1\leqslant i\leqslant 16$；利用式(5)，我们以 0.977的成功率预测 K_i^2 的第 36 到 32 比特，i 是奇数，$1\leqslant i\leqslant 16$.

分析所需的明密文对数 $N=2^{50}$. 下面以式(4)为例，给出操作办法.

第 1 步. 对任意给定的偶数 $j(1\leqslant j\leqslant 16)$，固定式(4)中 $K_i^2[h(36-32)](i\neq j)$的 h.

第 2 步. 令 $K_j^2[h(36-32)]=K_j^2[32]$，用式(4)预测 $k_0=k'\oplus K_j^2[32]$. 其中 $k'=(\bigoplus_{\substack{1\leqslant i\leqslant 16\\ i\text{是奇数}}}(K_i^1[0]\ominus K_i^3[0]))\oplus(\bigoplus_{\substack{i\neq j\\ i\text{是偶数}}}(K_i^2[h(36-32)]))$.

第 3 步. 令 $K_j^2[h(36-32)]=K_j^2[33]$，用式(4)预测 $k_1=k'\oplus K_j^2[33]$.

第 4 步. 令 $K_j^2[h(36-32)]=K_j^2[32,33]$，用式(4)预测 $k_2=k'\oplus K_j^2[32,33]$.

第 5 步. 令 $K_j^2[h(36-32)]=K_j^2[32,33,34]$，用式(4)预测 $k_3=k'\oplus K_j^2[32,33,34]$.

第 6 步. 令 $K_j^2[h(36-32)]=K_j^2[32,33,34,35]$，用式(4)预测 $k_4=k'\oplus K_j^2[32,33,34,35]$.

第 7 步. 令 $K_j^2[h(36-32)]=K_j^2[32,33,34,35,36]$，用式(4)预测 $k_5=k'\oplus K_j^2[32,33,34,35,36]$.

第 8 步. 计算 $K_j^2[32]=k_0\oplus k_2$，$K_j^2[33]=k_1\oplus k_2$，$K_j^2[34]=k_3\oplus k_2$. $K_j^2[35]=k_3\oplus k_4$，$K_j^2[35]=k_5\oplus k_4$.

上面我们利用线性密码分析的算法 1，以 0.977 的成功率预测出子密钥的 92 比特，所需明密文对为 2^{50}. 下面，我们对密钥长度为 128 比特的 LOKI97，用线性密码分析的算法 2 进行分析. 令 $K=(K_1,K_2)$，由密钥方案可得下面的方程：

$$\begin{cases}K_1^1=K_1\oplus g(K_2,f(K_2,K_1),f(K_1,K_2))\\ K_1^2=K_2\oplus g(f(K_2,K_1),f(K_1,K_2),K_1^1)\end{cases}\tag{7}$$

我们假定已知 K_1^1 和 K_1^2，从此方程求解 K_1 和 K_2 比较容易.

因为 $F(R_0+K_1^1,K_1^2)[0]$与 K_1^2 的 37 到 63 比特无关，又因为 K_1^2 的 32 到 36 比特已知，所以，(K_1^1,K_1^2)的可能值有 2^{96}个. 首先，利用式(6)和文献[4]中的算法 2，预测 K_1^1 及 K_1^2 的低 32 比特，所需明密文对为 2^{45}，成功率是 0.967；然后，对 K_1^2 的任意可能值(共有 2^{27}个)，求解方程式(7)；最后，再用明密文对检测所得的结果是否为真正的密钥.

4 结束语

本文对 LOKI97 进行了线性密码分析，结果显示，LOKI97 的安全性并没有设计者所希望的那么强大，我们利用轮函数的仅涉及输出和密钥的线性逼近，再利用 Feistel 网络的结构特性，对某些密钥构造出 14 轮和 16 轮 LOKI97 线性逼近，并以此对 LOKI97 进行分析. 由此，我们指出：在设计体制时，轮函数应保证子密钥和输入的充分混合，使得攻击者构造不出仅涉及密钥和输出的有效线性逼近.

参考文献

1 Biham E, Shamir A. Differential cryptanalysis Snefru, Kharfe, REDOC-II, LOKI and Lucifer, Vol. 576. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1991. 156～171

2 Toshio Tokita, Tohru Sorimachi, Mitsuru Matsui. Linear cryptanalysis of LOKI and S2DES, Vol. 917. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1994. 363～366

3 Lawrie Brown. LOKI97, http://csrc.ncsl.nist.gov/encryption/aes/aes-home.htm

4 Mitsuru Matsui. Linear cryptanalysis method for DES cipher, Vol. 765. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1993. 368～397

Linear Cryptanalysis of LOKI97

WU Wen-ling LI Bao FENG Deng-guo QING Si-han

(*Engineering Research Center for Information Security Technology The Chinese Academy of Sciences Beijing* 100080)
(*State Key Laboratory of Information Security Institute of Software The Chinese Academy of Sciences Beijing* 100080)

Abstract In this paper, LOKI97 is analyzed using linear cryptanalysis. The results show that LOKI97 does not meet the needs of AES (advanced encryption standard). Using algorithm 1 of linear cryptanalysis, the authors can get the 92-bit subkey with 2^{50} known-plaintexts and the success rate is 0.977; using algorithm 2 of linear cryptanalysis, it is possible to break LOKI97 with 2^{45} known-plaintexts and the success rate is 0.967.

Key words Linear cryptanalysis, linear approximation, nonlinearity.