韩国加密标准的安全性分析

吴文玲,马恒太,冯登国
(1. 中国科学院软件研究所信息安全国家重点实验室,北京 100080;2. 中国科学院信息安全技术工程研究中心,北京 100080)

摘 要: SEED 是韩国的数据加密标准,设计者称用线性密码分析攻击 SEED 的复杂度为 $2^{335.4}$,而用本文构造的 15 轮线性逼近攻击 SEED 的复杂度为 2^{328}. 为了说明 SEED 抵抗差分密码分析的能力,设计者首先对 SEED 的变体 SEED* 做差分密码分析,指出 9 轮 SEED * 对差分密码分析是安全的;利用 SEED* 的扩散置换和盒子的特性,本文构造 SEED* 的 9 轮截断差分,因此 10 轮 SEED* 对截断差分密码分析是不免疫的. 本文的结果虽然对 SEED 的实际应用构成不了威胁,但是显示了 SEED 的安全性并没有设计者所称的那样安全.

关键词: 分组密码; 安全性; 差分密码分析; 线性密码分析; 截断差分密码分析
中图分类号: TP391 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0585-04

Security on Korean Encryption Standard

WU Wen-ling, MA Heng-tai, FENG Deng-guo
(1. *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080, *China*;
2. *Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: SEED is the Korean encryption standard. It was pointed by designers that the complexity for the linear cryptanalysis of SEED is $2^{335.4}$. Using the linear approximations in this paper, the complexity for the linear cryptanalysis of SEED is 2^{328}. To analyze the differential cryptanalysis of SEED, the modified SEED was considered. It was pointed out that 9-round modified SEED was secure against the differential cryptanalysis. There are 9-round truncated differentials available to the truncated differential cryptanalysis in the modified SEED. Hence, 10-round modified SEED is not immune to truncated differential cryptanalysis. Although the results can not threaten the application of SEED, they show the security of SEED is not as strong as that designers predicted.

Key words: block cipher; security; differential cryptanalysis; linear cryptanalysis; truncated differential cryptanalysis.

1 引言

1.1 概述

SEED 是一个分组长度和密钥长度均为 128 比特的分组密码,它是由韩国信息安全代理处(KISA —Korea Information Security Agency)于 1998 年研制的,1999 年被指定为韩国工业联合会的标准(TTA KO-12.0004,1999),2000 年被韩国信息和通信部指定为国家标准 —KICS(Korean Information Communication Standard),SEED 现已用于韩国的许多安全系统中. 文献[1]对 SEED 的安全性做了全面的分析,它首先讨论 SEED 的变体(SEED *)对差分密码分析[2~4]的安全性,然后推断 SEED 对差分密码分析是安全的;对于线性密码分析[5],设计者指出攻击的复杂度为 $2^{335.4}$. 本文首先对 SEED 的基础模块进行了深入研究,然后构造轮函数的差分特征及线性逼近,进一步构造多轮 SEED 的差分特征和线性逼近,并以此分析 SEED 的安全性,结果显示 SEED 的安全性并没有设计者所称的安全. 为了方便,下面详细描述 SEED 的加密算法,因为本文不涉及 SEED 的密钥编排算法,所以这里不列出.

1.2 SEED 分组加密算法

1.2.1 整体结构 SEED 的整体结构是 16 轮的 *Feistel* 网络,首先,128 比特明文被分成左右两半,记为 $P = (L_0, R_0)$;然后,对 $1 \le i \le 15$,做如下操作:

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

对 $i = 16$,

$$L_{16} = L_{15} \oplus F(R_{15}, K_{16})$$
$$R_{16} = R_{15}$$

最后,输出 128 比特密文 $C = (L_{16}, R_{16})$.

其中 F 为轮函数,K_i 为轮子密钥.

1.2.2 轮函数 F 轮函数的输入是 64 比特,首先将 64 比特输入分成左右两个 32 比特子块 (X_0, X_1);然后嵌入轮子密钥 $K_i = (K_{i,0}, K_{i,1})$;其次进行三层函数和模 2^{32} 加组成的变换;最后,输出两个 32 比特子块 (Y_0, Y_1). 轮函数 F 的流程图见图 1,它的表达式如下:

收稿日期:2001-11-09;修回日期:2002-04-03
基金项目:国家自然科学基金(No. 60103023);973 项目(No. G1999035802)

$$Y_0 = G[\,G[\,G[\,(X_0 \oplus K_{i,0}) \oplus (X_1 \oplus K_{i,1})\,] + (X_1 \oplus K_{i,1})\,] + G[\,(X_0 \oplus K_{i,0}) \oplus (X_1 \oplus K_{i,1})\,]\,]$$

$$Y_1 = Y_0 + G[\,G[\,X_0 \oplus K_{i,0} \oplus X_1 \oplus K_{i,1}\,] + (X_1 \oplus K_{i,1})\,]$$

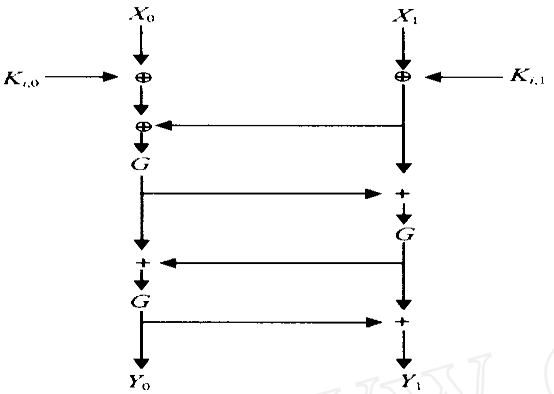

图 1 F 的流程图

1.2.3 G 函数

$$G:(F_2^8)^4 \to (F_2^8)^4$$

$$(A_3, A_2, A_1, A_0) \to (B_3, B_2, B_1, B_0)$$

$$B_0 = (S_1(A_0) \,\&\, m_0) \oplus (S_2(A_1) \,\&\, m_1) \oplus (S_1(A_2) \,\&\, m_2) \oplus (S_2(A_3) \,\&\, m_3)$$

$$B_1 = (S_1(A_0) \,\&\, m_1) \oplus (S_2(A_1) \,\&\, m_2) \oplus (S_1(A_2) \,\&\, m_3) \oplus (S_2(A_3) \,\&\, m_0)$$

$$B_2 = (S_1(A_0) \,\&\, m_2) \oplus (S_2(A_1) \,\&\, m_3) \oplus (S_1(A_2) \,\&\, m_0) \oplus (S_2(A_3) \,\&\, m_1)$$

$$B_3 = (S_1(A_0) \,\&\, m_3) \oplus (S_2(A_1) \,\&\, m_0) \oplus (S_1(A_2) \,\&\, m_1) \oplus (S_2(A_3) \,\&\, m_2)$$

其中：$m_0 = 0xfc$，$m_1 = 0xf3$，$m_2 = 0xcf$，$m_3 = 0x3f$.

1.2.4 S-盒

G 函数中的两个盒子 S_1 和 S_2 定义如下：

$$S_i : F_2^8 \to F_2^8,\ S_i(x) = C^{(i)} \cdot x^{n_i} \oplus d_i$$

其中 $n_1 = 247$，$n_2 = 251$，$d_1 = 169$，$d_2 = 56$，

$$c^{(1)} = \begin{bmatrix} 1&0&0&0&1&0&1&0 \\ 1&1&1&1&1&1&1&0 \\ 1&0&0&0&0&1&0&1 \\ 0&1&0&0&0&0&1&0 \\ 0&1&0&0&0&1&0&1 \\ 0&0&1&0&0&0&0&1 \\ 1&0&0&0&1&0&0&0 \\ 0&0&0&1&0&1&0&0 \end{bmatrix},\quad C^{(2)} = \begin{bmatrix} 0&1&0&0&0&1&0&1 \\ 1&0&0&0&0&1&0&1 \\ 1&1&1&1&1&1&1&0 \\ 0&0&1&0&0&0&0&1 \\ 1&0&0&0&1&0&1&0 \\ 1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&1&0 \\ 0&0&0&1&0&1&0&0 \end{bmatrix}$$

注意有限域 F_2^8 上的乘法运算对应的本原多项式为

$$p(x) = x^8 + x^6 + x^5 + x + 1$$

2 基础模块的密码特性

2.1 S-盒的差分和线性特性

$S_1 : X \to S_1(X) = Y$ 存在如下线性逼近：

$$X[0] = Y[0] \tag{1}$$

式(1)的线性概率为

$$\left\{\frac{2\#\{X \in F_2^8 \mid X[0] = S(X)[0]\}}{2^8} - 1\right\}^2 = \left\{\frac{2 \times 140 - 256}{256}\right\}^2 = \frac{9}{2^{10}}$$

令 $H = \{\alpha = 0a_20a_1 \in (F_2^2)^4 \setminus \{0\}\}$，也就是把 8 比特看成 4 个 2 比特，从左到右排序. 寻找满足下列 4 个等式的 $(\alpha, \alpha^*) \in H \times H$，

$$\begin{cases} \#\{X \in F_2^8 \mid S_2(X) \oplus S_2(X \oplus \alpha) = \alpha^*\} \neq 0 \\ \#\{X \in F_2^8 \mid S_2(X) \oplus S_2(X \oplus \alpha) = \alpha^*\} \neq 0 \\ \#\{X \in F_2^8 \mid S_2(X) \oplus S_2(X \oplus \alpha \oplus \alpha^*) = \alpha^*\} \neq 0 \\ \#\{X \in F_2^8 \mid S_2(X) \oplus S_2(X \oplus \alpha \oplus \alpha^*) = \alpha\} \neq 0 \end{cases} \tag{2}$$

测试显示 S_2 有 14 个满足式(2)的 (α, α^*) 对，它们分别是：(1,31)；(1,2)；(31,1)；(31,2)；(31,3)；(2,1)；(2,31)；(12,13)；(12,33)；(3,31)；(3,13)；(13,12)；(13,3)；(33,12).

2.2 G 函数

G 函数可以看成两个函数 S 和 P 的复合，

$$S:(F_2^8)^4 \to (F_2^8)^4$$

$$(A_3, A_2, A_1, A_0) \to (E_3, E_2, E_1, E_0)$$

$$E_0 = S_1(A_0),\ E_1 = S_2(A_1)$$

$$E_2 = S_1(A_2),\ E_3 = S_2(A_3).$$

为了直观，这里把 1 字节数据看成 4 个 2 比特或十六进制表示，例 $E_i = (e_{i3}e_{i2}e_{i1}e_{i0})$，$e_{ij} \in F_2^2$.

$$P:(F_2^8)^4 \to (F_2^8)^4$$

$$(E_3, E_2, E_1, E_0) \to (B_3, B_2, B_1, B_0)$$

可以表示为：

$$\begin{pmatrix} E_0 \\ E_1 \\ E_2 \\ E_3 \end{pmatrix} = \begin{pmatrix} e_{03}e_{02}e_{01}e_{00} \\ e_{13}e_{12}e_{11}e_{10} \\ e_{23}e_{22}e_{21}e_{20} \\ e_{33}e_{32}e_{31}e_{30} \end{pmatrix} \xrightarrow{P} \begin{pmatrix} e_{33}e_{22}e_{11}e_{00} \\ e_{03}e_{32}e_{21}e_{10} \\ e_{13}e_{02}e_{31}e_{20} \\ e_{23}e_{12}e_{01}e_{30} \end{pmatrix} \oplus \begin{pmatrix} T \\ T \\ T \\ T \end{pmatrix} = \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix}$$

其中 $T = E_3 \oplus E_2 \oplus E_1 \oplus E_0$.

如果 $\alpha \in H$，可以看出形如 $(0, \alpha, 0, \alpha)$ 和 $(\alpha, 0, \alpha, 0)$ 的 32 比特块在变换下保持不变. 因此，利用式(1)可以构造 G 函数的线性逼近：

$$A_0[0] \oplus A_2[0] = B_0[0] \oplus B_2[0] \tag{3}$$

式(3)的线性概率为 $9^2/2^{20}$.

令 (α, α^*) 满足式(2)，$\alpha = 0a_20a_1$，$\alpha^* = 0b_20b_1$，$\beta = 0a_20a_10000a_20a_10000 \in (F_2^2)^{16}$，$\beta^* = 0b_20b_10000b_20b_10000 \in (F_2^2)^{16}$，则可以构造 G 函数的如下差分特征：

$$\beta \xrightarrow{G} \beta^* \tag{4}$$

$$\beta^* \xrightarrow{G} \beta \tag{5}$$

$$\beta \oplus \beta^* \xrightarrow{G} \beta \tag{6}$$

$$\beta \oplus \beta^* \xrightarrow{G} \beta^* \tag{7}$$

式(4)、(5)、(6)和式(7)的差分特征仅有两个活动 S_2 盒子，因此，它们的概率均为 2^{-14}.

对 $\beta = 0a_20a_10000a_20a_10000 \in (F_2^2)^{16}$，则有概率为 1 的截断差分：

$$\beta = 0a_20a_10000a_20a_10000 \xrightarrow{G} 0?0??0?00?0??0?0 = \gamma \tag{8}$$

直观表示为：

$$\beta=\begin{pmatrix}0&0&0&0\\0&a_2&0&a_1\\0&0&0&0\\0&a_2&0&a_1\end{pmatrix}\xrightarrow{S}\begin{pmatrix}0&0&0&0\\?&?&?&?\\0&0&0&0\\?&?&?&?\end{pmatrix}\xrightarrow{P}\begin{pmatrix}?&0&?&0\\0&?&0&?\\?&0&?&0\\0&?&0&?\end{pmatrix}=\gamma$$

“?”表示相应的 2 比特差分不考虑.

3　轮函数的线性和差分特性

3.1　轮函数的线性逼近

$$F:(F_2^8)^8\to(F_2^8)^8$$

$$(X_7X_6X_5X_4X_3X_2X_1X_0)\to(Y_7Y_6Y_5Y_4Y_3Y_2Y_1Y_0)$$

因为模 2^{32} 加运算 $(X+Y=Z)$,存在概率为 1 的线性逼近:

$$X[0]\oplus Y[0]=Z[0]$$

所以利用式(3)可以构造轮函数的如下线性逼近:

$$X_0[0]\oplus X_2[0]=Y_0[0]\oplus Y_2[0]\oplus Y_4[0]\oplus Y_6[0] \quad (9)$$

$$X_0[0]\oplus X_2[0]\oplus X_4[0]\oplus X_6[0]=Y_4[0]\oplus Y_6[0] \quad (10)$$

$$X_4[0]\oplus X_6[0]=Y_0[0]\oplus Y_2[0] \quad (11)$$

式(9)、(10)和式(11)线性逼近都仅有两个活动 G 函数,因此,它们的线性概率均为 $9^4/2^{40}$.

3.2　轮函数变体的差分特性

轮函数的变体指的是把 3 个模 2^{32} 加$(+)$全改变为 $\oplus$,把改变后的轮函数记为 F^*,以 F^* 为轮函数的密码记为 SEED*. 利用式(4)、(5)、(6)及式(7),可以构造 F^* 的如下差分特征:

$$(0,\beta)\xrightarrow{F^*}(0,\beta^*) \quad (12)$$

$$(0,\beta^*)\xrightarrow{F^*}(0,\beta) \quad (13)$$

式(12)和(13)的概率均为 $(2^{-7})^4=2^{-28}$. 其中 $\beta=(\alpha,0,\alpha,0)\in(F_2^8)^4$,$\beta^*=(\alpha^*,0,\alpha^*,0)$,$(\alpha,\alpha^*)\in H\times H$,满足式(2). 由 2.1 节知:满足式(2)的(α,α^*)对有 14 对,我们举例说明 F^* 的一个截断差分,令 $\alpha=13$,$\beta=(\alpha,0,\alpha,0)=(13,0,13,0)$.

$$(0,\beta)=(0000000000000000,0103000001030000)\xrightarrow{F^*}(0\,?\,0\,??\;0\,?\,00\,?\,0\,??\;0\,?\,0,0\,?\,0\,??\;0\,?\,00\,?\,0\,??\;0\,?\,0)=(\gamma,\gamma) \quad (14)$$

F^* 由 4 个 $\oplus$ 和 3 个 G 函数组成,用下列形式描述式(14)差分的形成过程:

$$(0,\beta)\xrightarrow{\oplus}(\beta,\beta)\xrightarrow{G}(\beta,\beta)\xrightarrow{\oplus}(\beta,0)\xrightarrow{G}(\beta,0)\xrightarrow{\oplus}(\beta,0)\xrightarrow{G}(\gamma,0)\xrightarrow{\oplus}(\gamma,\gamma)$$

这里 β、β_1 和 β_2 都具有形式$(\alpha,0,\alpha,0)$,$\alpha\in H$.

对 S_2 的差分特性测试知,对 $\alpha=13$,$\#\{X\in F_2^8\mid S_2(X)\oplus S_2(X\oplus\alpha)=\alpha_1\}=2$,因此第一个“$\xrightarrow{G}$”的概率为 2^{-14},第二个“$\xrightarrow{G}$”的概率为 1,第三个“$\xrightarrow{G}$”的概率由式(8)知也为 1,第四个“$\xrightarrow{\oplus}$”的概率均为 1;所以式(14)的概率为 2^{-14}.

4　SEED* 的截断差分密码分析

令 $\alpha=13$,$\beta=(\alpha,0,\alpha,0)=(13,0,13,0)\in(F_2^8)^4$,$(0,\beta,0,0)\in(F_2^{32})^4$;利用式(12)和(13)可以构造 SEED* 的 7 轮差分

$$(0,\beta,0,0)\xrightarrow{}(0,0,0,\beta)\xrightarrow{}(0,\beta,0,\beta^*)\xrightarrow{}(0,\beta^*,0,0)\xrightarrow{}(0,0,0,\beta^*)\xrightarrow{}(0,\beta^*,0,\beta)\xrightarrow{}(0,\beta,0,0)\xrightarrow{}(0,0,0,\beta) \quad (15)$$

因为对 $\alpha=13$,满足式(2)的 α^* 有两个,所以式(15)的概率大于 $2\times(2^{-28})^4=2^{-111}$.

结合式(14)和式(15)可以构造 SEED* 的 9 轮截断差分:

$$(0,\beta,0,0)\xrightarrow{7\ round}(0,0,0,\beta)\xrightarrow{}(0,\beta,\gamma,\gamma)\xrightarrow{}(\gamma,\gamma,?,?) \quad (16)$$

式(16)的概率为 $2^{-111}\times2^{-14}=2^{-125}$.

利用式(16)攻击 10 轮 SEED* 的步骤如下:

第一步,选取明文对$(P_i,P_i^*)1\le i\le2^{125}$,使得 $P_i\oplus P_i^*=(0,\beta,0,0)$,$(C_i,C_i^*)$是相应的密文对.

第二步,对子密钥 K_{10} 的每一种候选值,解密密文得 $D_i=C_{iL}\oplus F(C_{iR},K_{10})$ 和 $D_i^*=C_{iL}^*\oplus F(C_{iR}^*,K_{10})$.

第三步,检验 $D_i\oplus D_i^*=(\gamma,\gamma)$ 是否成立.

此攻击的数据复杂度为 2^{125},所以此攻击比强力攻击有效. 文献[1]指出对 SEED* 最多存在 8 轮的有用差分,也就是差分密码分析最多可攻击 9 轮 SEED*,这里利用截断差分密码分析可攻击 10 轮 SEED*.

5　SEED 的线性密码分析

我们把(L_i,R_i)看成字节串$(L_{i,7}L_{i,6},\cdots,L_{i,1}L_{i,0},R_{i,7},R_{i,6},\cdots,R_{i,1}R_{i,0})$. 利用式(9)、(10)和式(11),可以构造如下 5 轮循环线性逼近:

$$R_{5,0}[0]\oplus R_{5,2}[0]=R_{0,0}[0]\oplus R_{0,2}[0] \quad (17)$$

式(17)的轨迹为:

$$R_{5,0}[0]\oplus R_{5,2}[0]\xrightarrow{}R_{4,0}[0]\oplus R_{4,2}[0]\oplus L_{4,0}[0]\oplus L_{4,2}[0]\oplus L_{4,4}[0]\oplus L_{4,6}[0]\xrightarrow{}R_{3,0}[0]\oplus R_{3,2}[0]\oplus R_{3,4}[0]\oplus R_{3,6}[0]\oplus L_{3,0}[0]\oplus L_{3,2}[0]\oplus L_{3,4}[0]\oplus L_{3,6}[0]\xrightarrow{}R_{2,0}[0]\oplus R_{2,2}[0]\oplus L_{2,0}[0]\oplus L_{2,2}[0]\oplus L_{2,4}[0]\oplus L_{2,6}[0]\xrightarrow{}L_{1,0}[0]\oplus L_{1,2}[0]=R_{0,0}[0]\oplus R_{0,2}[0]$$

因为式(9)、(10)和式(11)的线性概率均为 $9^4/2^{40}$,所以式(17)的线性概率为 $9^{16}/2^{160}$.

利用式(17),可以构造 15 轮 SEED 的线性逼近:

$$R_{15,0}[0]\oplus R_{15,2}[0]=R_{0,0}[0]\oplus R_{0,2}[0] \quad (18)$$

因为式(17)的线性概率为 $9^{16}/2^{160}$,所以式(18)的线性概率为 $(9^{16}/2^{160})^3>2^{-328}$.

利用式(18)和文献[5]中的算法 2 攻击 SEED,复杂度为 2^{328},小于文献[1]所称的用线性密码分析攻击 SEED 的复杂度.

6　结束语

SEED 是韩国的数据加密标准,它的设计有自己的特点,

尤其是扩散置换的设计,有它的独到之处.作为国家标准,SEED 经受了韩国密码专家的深入分析.为了解 SEED 的设计思想,我们对 SEED 进行了研究,研究结果显示 SEED 的安全性并没有设计者所称的那样安全.设计者称用线性密码分析攻击 SEED 的复杂度不会小于 $2^{335.4}$,而用我们构造的 15 轮线性逼近攻击 SEED 的复杂度为 2^{328}.为了说明 SEED 抵抗差分密码分析的能力,设计者首先对 SEED 的变体 SEED* 做差分密码分析,指出 9 轮 SEED* 对差分密码分析是安全的;利用 SEED* 的扩散置换和盒子的特性,可以构造 SEED* 的 9 轮截断差分,因此 10 轮 SEED* 对截断差分密码分析是不免疫的.

参考文献:

[1] KISA, A Design and Analysis of SEED (S), 1998. (http://www.kisa.or.kr/technology/sub1/128-seed.pdf)

[2] E Biham, A Shamir. Differential cryptanalysis of DES-like cryptosystems [J]. Journal of Cryptology, 1991, 4(1): 3 - 72.

[3] L R Knudsen. Truncated and Higher Order Differentials [A]. Fast Software Encryption, 2nd International Workshop Proceedings [C]. Berlin, Springer-Verlag, 1995, 196 - 211.

[4] L R Kundsen, T A Berson. Truncated Differentials of SAFER [A]. Fast Software Encryption, 3nd International Workshop Proceedings [C]. Berlin, Springer-Verlag, 1996, 15 - 26.

[5] M Matsui. Linear Cryptanalysis Method for DES Cipher [A]. Advances in Cryptology-EUROCRYPT '93 Proceedings [C]. Berlin, Springer-Verlag, 1994, 386 - 397.

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.目前的研究兴趣为分组密码的设计与分析.

马恒太 男,1970 年生于山东省临朐县,2001 年 3 月于中国科学院软件研究所获博士学位,现在中国科学院软件研究所从事网络安全产品的研发工作.

冯登国 男,1965 年生于陕西省靖边县,现为中国科学院软件所研究员,信息安全国家重点实验室主任,目前主要从事信息与网络安全的研究.