分组加密算法 SMS4 的 14 轮 Square 攻击

钟名富，胡予濮，陈 杰
(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘要：为了对分组加密算法 SMS4 进行新的安全性分析，基于 SMS4 的轮结构中的活跃字变化的特点，选择 1 个特定的明文形式来构造 1 个含 3 个活跃字的 Λ 集，通过观察平衡字的传播路径，在第 9 轮找到了 1 个平衡字，由此构建出 1 个新型的 12 轮区分器并对 14 轮 SMS4 进行 Square 攻击. 研究结果表明：攻击所需的明文数据量为 2^{32}，计算复杂度为 $2^{96.5}$，这说明 14 轮 SMS4 对 Square 攻击是不免疫的.

关键词：SMS4 算法；平方攻击；计算复杂度；分组加密
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2008)01-0105-05

Square attack on the 14-round block cipher SMS4

ZHONG Ming-fu, *HU Yu-pu*, *CHEN Jie*
(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi′an 710071, China)

Abstract: In order to make a new security evaluation for the block cipher SMS4, a certain plaintext is chosen to built a gamma set that contains three active words. Based on the character of the diversification of the active words in the round structure of SMS4, a balance word is found in the ninth round by observing the spread path of the balance words, and therefore a new 12-round distinguisher is constructed, by use of which a 14-round square attack is made on SMS4. In the attack 2^{32} chosen plaintexts are needed and the time complexity is about $2^{96.5}$. Thus the 14-round SMS4 is not immune to the Square attack.

Key Words: SMS4; square attack; time complexity; block cipher

SMS4 是用于 WAPI 的分组密码算法，也是国内官方公布的第 1 个商用密码算法[1]. 由于其公布时间的不长，目前对于它的攻击仍仅限于边信道攻击方面的结果[2]. 如何对 SMS4 加密算法做出新的安全性评价，是当前的研究热点之一.

1997 年 Joan Daemen 等人针对类 Square 密码算法首次提出了 Square 攻击[3]. Square 攻击是一种选择明文攻击，利用的是扩散层及活跃字节变化的特点进行分析；这种分析技术在 AES 等标准算法分析中发挥着重要的作用. 笔者基于 SMS4 的轮结构特点，构建出了 1 个新型的 12 轮区分器；并由此对 14 轮 SMS4 进行 Square 攻击. 研究结果表明：利用 Square 攻击对 14 轮 SMS4 进行攻击所需的明文数据量为 2^{32}，计算复杂度为 $2^{96.5}$.

1 SMS4 算法简介

SMS4 算法是一个分组密码算法，该算法的分组长度为 128 bit，密钥长度为 128 bit. 加密算法与密钥扩展算法都采用 32 轮非线性迭代结果. 解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序.

1.1 轮 函 数

算法采用非线性迭代结构，以字为单位进行加密运算，称一次迭代运算为一轮变换.

收稿日期：2007-03-29
基金项目：国家自然科学基金资助(60673072)；国家密码发展基金资助
作者简介：钟名富(1983-)，男，西安电子科技大学硕士研究生，E-mail：mfzh023@163.com.

设输入为 $(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$,轮密钥为 $rk\in Z_2^{32}$,则轮函数 F 为:$F(X_0,X_1,X_2,X_3,rk)=X_0\oplus T(X_1\oplus X_2\oplus X_3\oplus rk)$,其中 T 为 $Z_2^{32}\to Z_2^{32}$ 的一个可逆变换,由非线性变换 τ 和线性变化 L 复合而成,即 $T(\cdot)=L(\tau(\cdot))$. 其中:非线性变换 τ 是由 4 个并行的 S 盒构成. 设输入为 $A=(a_1,a_2,a_3,a_4)\in(Z_2^8)^4$,输出为 $B=(b_1,b_2,b_3,b_4)\in(Z_2^8)^4$,则有:$((b_1,b_2,b_3,b_4)=\tau(A)=(S_{box}(a_1),S_{box}(a_2),S_{box}(a_3),S_{box}(a_4))$.

线性变换 L:非线性变换 τ 的输出即为线性变换 L 的输入. 设输入为 $B\in Z_2^{32}$,则有 $C=L(B)=B\oplus(B\lll 2)\oplus(B\lll 10)\oplus(B\lll 18)\oplus(B\lll 24)$,其中 $\lll i$ 为32 bit循环左移 i 位.

1.2 加/解密算法

定义反序变换 R 为:$R(A_0,A_1,A_2,A_3)=(A_3,A_2,A_1,A_0)$,$A_i\in Z_2^{32}$,$i=0,1,2,3$. 设明文输入为 $(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$,密文输出为 $(Y_0,Y_1,Y_2,Y_3)\in(Z_2^{32})^4$,轮密钥为 $rk_i\in Z_2^{32}$,$i=0,1,\cdots,31$. 则本算法的加密变换为:$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)$,$i=0,1,\cdots,31$. $(Y_0,Y_1,Y_2,Y_3)=R(X_{32},X_{33},X_{34},X_{35})=(X_{35},X_{34},X_{33},X_{32})$. 具体的加密算法结构如图 1 和图 2 所示.

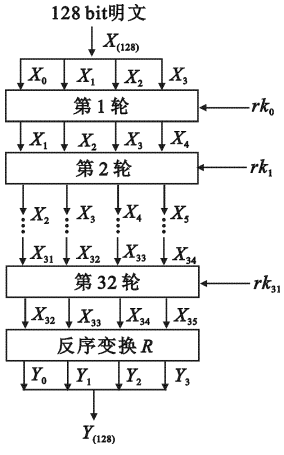

图 1 SMS4 加密算法整体结构

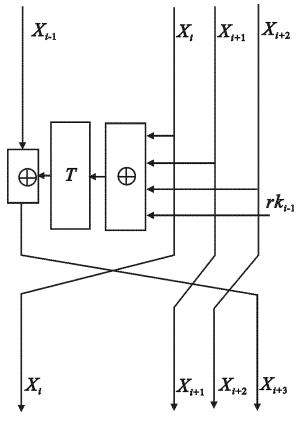

图 2 第 i 轮 SMS4 加密算法结构

算法的解密变换与加密变换结构相同,不同的仅是轮密钥的使用顺序.

加密时轮密钥的使用顺序为 $(rk_0,rk_1,\cdots,rk_{31})$.

解密时轮密钥的使用顺序为 $(rk_{31},rk_{30},\cdots,rk_0)$.

1.3 密钥扩展算法

算法中加密算法的轮密钥由加密密钥通过密钥扩展算法生成.

加密密钥 $M_K=(M_{K_0},M_{K_1},M_{K_2},M_{K_3})$,$M_{K_i}\in Z_2^{32}$,$i=0,1,2,3$.

令 $K_i\in Z_2^{32}$,$i=0,1,\cdots,35$,轮密钥为 $rk_i\in Z_2^{32}$,$i=0,1,\cdots,31$,则密钥生成方法为:$(K_0,K_1,K_2,K_3)=(M_{K_0}\oplus F_{K_0},M_{K_1}\oplus F_{K_1},M_{K_2}\oplus F_{K_2},M_{K_3}\oplus F_{K_3})$,对 $i=0,1,2,\cdots,31$ 有 $rk_i=K_{i+4}=K_i\oplus T'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus C_{K_i})$,其中 T' 变换与轮函数中的 T 变换基本相同,只将其中的线性变换 L 修改为以下 L':$L'(B)=B\oplus(B\lll 13)\oplus(B\lll 23)$.

系统参数 F_K 的取值,采用 16 进制表示为:$F_K=(F_{K_0},F_{K_1},F_{K_2},F_{K_3})$,其中 $F_{K0}=(A3B1BAC6)$,$F_{K_1}=(56AA3350)$,$F_{K_2}=(677D9197)$,$F_{K_3}=(B27022DC)$.

固定参数 $C_K=(C_{K_0},C_{K_1},\cdots,C_{K_{31}})$ 为 32 个固定参数,其值参看相关标准[1].

2 平方攻击的核心思想

2.1 平方攻击介绍

1997 年 Joan Daemen 等人针对类 Square 密码算法首次提出了 Square 攻击,这种攻击主要利用了 Square 密码的块操作特性和 SPN 结构密码中每一变换的可逆性提出的一种攻击方法. 它对于攻击低轮数类似 Square 密码是十分有效的[3~5]. 随后 N. Ferguson 和 H. Gilbert 等人分别利用动态规划和生日悖论的

技巧推广了 Square 攻击并都取得了很好的效果[6,7].

2.2 平方攻击基本思想

Square 攻击主要建立在以下两个重要概念——Λ 集平衡性之上的一种选择明文攻击[8,9].

① Λ 集是一个包含 2^{32} 个状态的集合,这些状态在某些字(称为活动字)上两两互异(因而遍历字的所有的可能值),而在其他字(称为非活动字)上则完全相同,即对任意状态 $A,B\in\Lambda$ 有:

$$\begin{cases} A_{i,j}\neq B_{i,j}, & \text{若}(i,j)\text{位置上是活动字},\\ A_{i,j}=B_{i,j}, & \text{若}(i,j)\text{位置上是非活动字}. \end{cases}$$

② 对包含 2^{32} 个状态的集合 P,某个位置(i,j)上的字是平衡的当且仅当所有状态在该位置上的字的异或结果为 0,即字(i,j)是平衡的 $\Leftrightarrow \bigoplus_{A\in P} A(i,j)=0$.

基本的攻击过程是:

Step1　选择一个 Λ 集.

Step2　对此 Λ 集加密并观察加密过程中平衡字的传播路径(此过程包含密钥猜测).

Step3　对路径末端平衡字的所有可能取值求和,由此来决定保留或删除所猜测的密钥,可以选择多个 Λ 集重复上述过程来验证所保留密钥的正确性.

Step4　输出正确的密钥.

3　14 轮 SMS4 平方攻击密码分析

3.1 SMS4 的 12 轮 Square 攻击区分器的构造

选择具有形式为$(\alpha,\alpha,\alpha,0)$的一个明文加密,其中$\alpha\in Z_2^{32}$,由 SMS4 的轮结构特点,则得到具体的明文加密时转移的情况如表 1 所示.

表 1　12 轮明密文编排表

轮数	明文			
1	α	α	α	0
2	α	α	0	$\alpha\oplus T(r_0)$
3	α	0	$\alpha\oplus T(r_0)$	$\alpha\oplus T(T(r_0)\oplus r_1)$
4	0	$\alpha\oplus T(r_0)$	$\alpha\oplus T(T(r_0)\oplus r_1)$	$\alpha\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)$
5	$\alpha\oplus T(r_0)$	$\alpha\oplus T(T(r_0)\oplus r_1)$	$\alpha\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)$	β_1
6	$\alpha\oplus T(T(r_0)\oplus r_1)$	$\alpha\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)$	β_1	β_2
7	$\alpha\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)$	β_1	β_2	*
8	β_1	β_2	*	*
9	β_2	*	*	*
10	*	y	*	*
11	*	*	y	*
12	*	*	*	y

表 1 中 $0,\alpha,\beta_1,\beta_2$ 均取于 Z_2^{32},* 为任意数,$\beta_1=T(\alpha\oplus T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)\oplus r_3)$,$\beta_2=\alpha\oplus T(r_0)\oplus T(T(T(r_0)\oplus r_1)\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)\oplus T(\alpha\oplus T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)\oplus r_3)\oplus r_4)$,又因密钥 r_0,r_1,r_2,r_4 都是固定的,所以经过变换 T 之后仍然是个定值,则令$T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus T(T(r_0)\oplus T(T(r_0)\oplus r_1)\oplus r_2)\oplus r_3=A$,则$\beta_1=T(\alpha\oplus A)$,同理令$T(r_0)=B_1$,$T(T(r_0)\oplus r_1)\oplus T(T(r_0)\oplus T(T(r_0)\oplus$

$r_1) \oplus r_2) = B_2$,则$\beta_2 = \alpha \oplus B_1 \oplus T(B_2 \oplus T(\alpha \oplus A))$,其中 A, B_1, B_2 都是定值.

而通过对线性层 L 的分析以及对 S 盒的测试能得到如下结论:

(1) 对于任意的 $a \in Z_2^{32}$,$b \in Z_2^{32}$,若 $a \neq b$,则有 $L(a) \neq L(b)$.

证明 设 $a,b,c \in Z_2^{32}$,因$(a \oplus b) \oplus c = a \oplus (b \oplus c)$,$a \oplus b = b \oplus a$,且若$a \oplus b = a \oplus c$,则有$b = c$,设 $a = a_0 a_1 \cdots a_{31}$, $b = b_0 b_1 \cdots b_{31}$, 则令 $N = L(a) = a \oplus (a \ll 2) \oplus (a \ll 10) \oplus (a \ll 18) \oplus (a \ll 24) = n_1 n_2 \cdots n_{31}$, $M = L(b) = b \oplus (b \ll 2) \oplus (b \ll 10) \oplus (b \ll 18) \oplus (b \ll 24) = m_1 m_2 \cdots m_{31}$,若$N = M$,则有$n_{31} = m_{31}$,而$n_{31} = a_{31} \oplus 0 \oplus 0 \oplus 0 \oplus 0 = a_{31}$,$m_{31} = b_{31} \oplus 0 \oplus 0 \oplus 0 \oplus 0 = b_{31}$,所以有$a_{31} = b_{31}$, 同理得$a_{30} = b_{30}$. 又因$n_{29} = a_{29} \oplus a_{31} \oplus 0 \oplus 0 \oplus 0$,$m_{29} = b_{29} \oplus b_{31} \oplus 0 \oplus 0 \oplus 0$,而$a_{31} = b_{31}$,所以$a_{29} = b_{29}$,同理得$a_i = b_i$,$i = 0,1,\cdots,28$. 也即若$N = M$,则$a = b$.

(2) 因为 S 盒是双射的,则对于任意的 $a \in Z_2^{32}$,$b \in Z_2^{32}$,若$a \neq b$,则有$S(a) \neq S(b)$. 因此$T(a) \neq T(b)$,也即若 x 跑遍 0 到$(2^{32}-1)$ 则 $T(x)$ 也跑遍 0 到$(2^{32}-1)$,$T(x \oplus A)$ 也跑遍 0 到$(2^{32}-1)$,再进一步则得 $T(T(x))$ 也跑遍 0 到$(2^{32}-1)$. 同理得$T(B_2 \oplus T(\alpha \oplus A))$ 也跑遍 0 到$(2^{32}-1)$。

由以上结论可证明 $\sum_{\alpha} \beta_2 = 0$,因当 a 跑遍 0 到$(2^{32}-1)$ 时,显然有 $\sum_{a} \alpha = 0$, $\sum_{\alpha} T(B_2 \oplus T(\alpha \oplus A)) = 0$,则 $\sum_{\alpha} \beta_2 = 0 + 0 = 0$ 得证.

12 轮区分器为: $\sum_{y} y = 0$,输入特征为$(\alpha,\alpha,\alpha,0)$,其中$\alpha \in Z_2^{32}$. 输出特征为$\left(*,*,*,\sum_{y} y = 0\right)$,其中 y 为第 12 轮输出块,且$y \in Z_2^{32}$.

3.2 14 轮平方攻击过程详述

具体攻击过程如下:

Step1 选择一个明文为 $(\alpha,\alpha,\alpha,0)$,通过加密得到一个明文编排表(表 1)并得到经过 14 轮加密后的密文.

Step2 全猜测第 14 轮的子密钥 rk_{13} 并解密第 14 轮的密文,也即得到了第 13 轮的明文.

Step3 全猜测第 13 轮的子密钥 rk_{12} 并解密上一步所得到的第 13 轮的明文,也即得到了第 12 轮的明文.

Step4 让 α 跑遍 0 到$(2^{32}-1)$,并重复 Step 2 和 Step 3,把得到的 12 轮的明文的最后一个字 y 相加. 而因最后一个字 y 的和为 0 的概率是 2^{-32},则一共有$2^{32} \times 2^{32} \times 2^{-32} = 2^{32}$个密钥使得 $\sum_{y} y = 0$, 也即能保留下来的可能的正确的密钥量为 2^{32} 个.

Step5 对这 2^{32} 个可能的密钥进行全测试,直至得到惟一的正确的子密钥.

Step6 对余下的 128−64=64 bit 进行全搜索得到正确的子密钥,从而完全恢复出所有密钥.

3.3 复杂度分析

(1) 在 Step 4 中需要对每一个 α 都分别猜测第 13 轮和第 12 轮的子密钥,每猜测一轮子密钥的计算复杂度为 2^{32},而一共有 2^{32} 个 α, 所以这一步所需的计算复杂度为$2^{32} \times 2^{32} \times 2^{32} = 2^{96}$.

(2) 在 Step 5 中需要对 2^{32} 个可能的密钥每一个都进行测试,所以这步的计算复杂度为 2^{32}.

(3) 在 Step 6 中还需对剩下的 64 bit 子密钥进行全搜索,也即必须进行 2^{64} 次 14 轮加密,因此这一步的计算复杂度为 2^{64}.

所以单轮计算复杂度为$(2^{96} + 2^{32})/14 \approx 2^{93}$,而此攻击方法总共所需的计算复杂度为$2^{96} + 2^{32} + 2^{64} \approx 2^{96.5}$. 故攻击 14 轮 SMS4 所需的复杂度为:明文数据量为 2^{32},计算复杂度为 $2^{96.5}$.

4 结 束 语

通过对 SMS4 加密算法中的线性变换 L 的特点以及平衡字节的变化情况进行了分析,并首次利用平方攻击方法对其进行攻击. 结果表明:攻击所需的明文数据量为 2^{32},计算复杂度为 $2^{96.5}$,这说明 14 轮 SMS4 对 Square 攻击是不免疫的. 但目前为止还没有证据显示 32 轮的 SMS4 算法是否能足以抵抗文中算法的平方攻击.

参考文献:

[1] Office of State Commercial Cipher Administration. Block Cipher for WLAN Products—SMS4[EB/OL]. [2006-12-23]. http://www.oscca.gov.cn/UpFile/2006021016423197990.

[2] 张蕾, 吴文玲. SMS4 密码算法的差分故障攻击[J]. 计算机学报, 2006, 29(9):1594-1600.

[3] Daemen J, Knudsen R L, Rijmen V. The Block Cipher Square[C]//Fast Software Encryption. Berlin: Springer-Verlag, 1997: 149-165.

[4] Daemen J, RijmenV. AES Proposal: Rijndael Version 2[EB/OL]. [2006-11-10]. http://www.east.kuleuven.ac.be/~rijmen/rijndael.

[5] Barreto P, Rijmen V. The ANUBIS Block Cipher[EB/OL]. [2005-08-23]. http://www.cryptonessie.org.

[6] Ferguson N, Kelsey J, Schneier B, et al. Improved Cryptanalysis of Rijndael[C]//Proceedings of Fast Software Encryption Workshop: Vol 1978. Berlin: Springer-Verlag, 2000: 213-230.

[7] Gilbert H, Minier M. A Collision Attack on 7 Rounds of Rijndael[EB/OL]. [2006-10-15]. http://csrc.nist.gov/eccryption/aes/round2/conf3/aes3papers.html.

[8] 韦宝典, 刘东苏, 王新梅. 一种新的 Square 攻击[J]. 西安电子科技大学学报, 2003, 30 (4):473-476.
Wei Baodian, Liu Dongsu, Wang Xinmei. A New Type of Square Attack[J]. Journal of Xidian University, 2003, 30 (4): 473-476.

[9] 李清玲, 李超. 变种 Camellia 对 Square 攻击的安全性[J]. 应用科学学报, 2006, 24 (5): 485-490.

(编辑: 齐淑娟)

(上接第 104 页)

[8] Wandell B A. Foundations of Vision. Sinauer Associates [M]. First Edition. Sunderland: Sinauer Associates, Inc,1995.

[9] Imgeun L, Jongsik K. Wavelet Transform Image Coding Using Human Visual System [C]//IEEE Asia-Pacific Conference on Circuits and Systems. Taipei: IEEE, 1994: 619-623,

[10] Miloslavski M, Ho Y S. Zerotree Wavelet Image Coding Based on the Human Visual System Model [C]//IEEE Asia-Pacific Conference on Circuits and Systems. Chiangmai: IEEE, 1998: 57-60.

[11] Nadenau M J, Julien R, Murat K. Wavelet-Based Color Image Compression: Exploiting the Contrast Sensitivity [J]. IEEE Trans on Image Processing, 2003, 1, 12(1): 58 - 70.

[12] Sheikh H R, Wang Z, Bovik A C, et al. Image and Video Quality Assessment Research at LIVE [DB/OL]. [2003- 10-12]. http://live.ece.utexas.edu/rese-arch/quality/.

[13] VQEG. Final Report from the Video Quality Experts Group on the Validation of Objective Models of Video Quality Assessment [DB/OL]. [2003-03 -12]. http://www.vqeg.org/.

(编辑: 齐淑娟)