软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(9):2821−2828 [doi: 10.13328/j.cnki.jos.005271]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

对 SMS4 密码算法改进的差分攻击*

赵艳敏[1,2], 刘 瑜[1,3], 王美琴[1]

[1](山东大学 数学学院,山东 济南 250100)

[2](保密通信重点实验室,四川 成都 610041)

[3](潍坊学院 计算机工程学院,山东 潍坊 261041)

通讯作者: 王美琴, E-mail: mqwang@sdu.edu.cn

摘 要: 差分分析和线性分析是重要的密码算法分析工具.多年来,很多研究者致力于改善这两种攻击方法.Achiya Bar-On 等人提出了一种方法,能够使攻击者对部分状态参与非线性变换的 SPN 结构的密码算法进行更多轮数的差分分析和线性分析.这种方法使用了两个辅助矩阵,其目的就是更多地利用密码算法中线性层的约束,从而能攻击更多轮数.将这种方法应用到中国密码算法 SMS4 的多差分攻击中,获得了一个比现有攻击存储复杂度更低和数据复杂度更少的攻击结果.在成功概率为 0.9 时,实施 23 轮的 SMS4 密钥恢复攻击需要 $2^{113.5}$ 个明文,时间复杂度为 $2^{126.7}$ 轮等价的 23 轮加密.这是目前为止存储复杂度最低的攻击,存储复杂度为 2^{17} 个字节.

关键词: SMS4;分组密码;多差分攻击;矩阵;存储复杂度

中图法分类号: TP309

中文引用格式: 赵艳敏,刘瑜,王美琴.对 SMS4 密码算法改进的差分攻击.软件学报,2018,29(9):2821−2828. http://www.jos.org.cn/1000-9825/5271.htm

英文引用格式: Zhao YM, Liu Y, Wang MQ. Improved differential attack on 23-round SMS4. Ruan Jian Xue Bao/Journal of Software, 2018,29(9):2821−2828 (in Chinese). http://www.jos.org.cn/1000-9825/5271.htm

Improved Differential Attack on 23-Round SMS4

ZHAO Yan-Min[1,2], LIU Yu[1,3], WANG Mei-Qin[1]

[1](School of Mathematics, Shandong University, Ji'nan 250100, China)

[2](Science and Technology on Communication Security Laboratory, Chengdu 610041, China)

[3](School of Computer Engineering, Weifang University, Weifang 261041, China)

Abstract: For years, many cryptanalysts have been devoted to working on analyzing the security of block ciphers against differential attacks and linear attacks. Thus, there are copious methods to cryptanalyze a block cipher with differential and linear cryptanalyses. An original method proposed by Achiya Bar-On *et al*. enables attackers to analyze more rounds of a partial SPN network in differential and linear cryptanalyses. The method involves two auxiliary matrices, which makes it possible that more constraints on differences can be exploited to sieve the inappropriate pairs. In the paper, the method is implemented to SMS4 in the setting of a multiple differential cryptanalysis. By utilizing the 2^{14} existing 19-round differential characteristics, the paper carries out a 23-round key-recovery attack on SMS4, which leads to a lower data and memory complexities than previous multiple differential attack results on 23-round SMS4, namely,

* 基金项目: 国家重点基础研究发展计划(973)(2013CB834205); 国家自然科学基金(61133013, 61572293, 61602276); 教育部新世纪优秀人才项目(NCET-13-0350); 山东省自然科学基金(ZR2016FM22); 保密通信重点实验室基金项目(9140c110207150c11050)

Foundation item: National Grand Fundamental Research (973) Program of China (2013CB834205); National Natural Science Foundation of China (61133013, 61572293); Program for New Century Excellent Talents in University of China (NCET-13-0350); Shandong Natrural Science Foundation of China (ZR2016FM22); Science and Technology on Communication Security Laboratory Funded Projects (9140c110207150c11050)

收稿时间: 2016-12-19; 修改时间: 2017-02-05; 采用时间: 2017-02-28; jos 在线出版时间: 2017-03-31

CNKI 网络优先出版: 2017-03-31 21:54:41, http://kns.cnki.net/kcms/detail/11.2560.TP.20170331.2154.006.html

$2^{113.5}$ chosen plaintexts and 2^{17} bytes at a success possibility of 0.9. The attack presented in the paper can recover 128-bit key within $2^{126.7}$ equivalent 23-round encryptions

Key words: SMS4; block cipher; multiple differential attack; matrices; memory complexity

差分分析和线性分析是分组密码算法最基本和最重要的分析方法,同时,在设计分组密码算法时,密码算法抵抗差分分析和线性分析的能力也是密码设计者重点关注的因素之一.差分分析是由 Biham 和 Shamir 在 1990 年为了分析 DES 在文献[1]中首次提出.基于差分分析的思想衍生了很多其他的分析方法,如截断差分分析[2]、多差分分析[3].Blondeau 等人[3]提出了多差分攻击的概念,并且给出了多差分分析的时间和数据复杂度的计算方式.

Eurocrypt 2015 会议上,Achiya Bar-On 等人[4]提出了利用矩阵来恢复部分状态参与非线性变换的 SPN 结构的密码算法密钥的攻击方法.该方法利用密码算法非线性层提供的混淆效果差的弱点,采用矩阵这一代数概念充分体现线性层所提供的轮状态之间的关系,从而在攻击过程中可以尽可能早地筛减明密文对,达到降低时间复杂度的目的.

SMS4[5]是我国商用分组密码标准算法,是构建无线局域网安全的密码模块,其英语版本介绍可以在文献[6]中查看.正是由于 SMS4 密码算法的重要性,很多研究者给出了他们的密码分析结果.Liu 等人[7]给出了他们对 13 轮的 SMS4 的积分攻击.Ji 等人[8]使用代数攻击的方法评估了 SMS4 的安全性.Lu 在文献[9]中对 SMS4 实施了 14 轮的矩形攻击,并给出了一个 16 轮的不可能差分攻击的结果.之后, Lu 等人的结果被 Toz 和 Dunkleman 在文献[10]中改进.Zhang 等人[11]对 SMS4 进行了 21 轮的差分分析和 16 轮的矩形攻击.Etrog 等人在文献[12]中对 SMS4 进行了 22 轮的线性攻击分析.同年,Kim 等人[13]发表了他们对 SMS4 多个攻击的分析结果,包括 22 轮的差分和线性分析、18 轮的矩形攻击分析和 Boomerang 攻击分析.Zhang 等人[14]改进了 22 轮 SMS4 的差分分析的结果.Liu 等人[15]对 SMS4 进行了多线性攻击的分析.Su 等人[16]给出了 23 轮 SMS4 的差分攻击结果.Cho 和 Nyberg 给出了一个同样轮数的多维差分攻击结果[17].在文献[18]中,作者首次找到了一条偏差为 $2^{-62.27}$ 的 19 轮的线性近似,并对 SMS4 进行了改进的线性攻击分析.

本文将 Achiya Bar-On 等人[4]提出的密钥恢复攻击方法应用在 SMS4 上,利用该密码算法混淆性差的特点,改进了现有的对 SMS4 的 23 轮多差分攻击的结果,极大地降低了攻击过程中的存储复杂度.对 SMS4 主要攻击结果的汇总见表 1.

Table 1 Comparison between different attacks on SMS4

表 1 SMS4 不同攻击结果比较

轮数	攻击类型	数据复杂度	时间复杂度	存储复杂度	文献
18	矩阵攻击	2^{124}	$2^{112.83}$	2^{128} 字节	[13]
18	飞来去器攻击	2^{120}	$2^{116.83}$	2^{123} 字节	[13]
22	线性攻击	$2^{118.4}$	2^{117}	2^{112} 字节	[12]
22	线性攻击	2^{117}	$2^{109.68}$	2^{109} 字节	[13]
23	线性攻击	$2^{126.54}$	2^{122}	2^{116} 字节	[18]
23	多维线性攻击	$2^{126.6}$	$2^{127.4}$	$2^{120.7}$ 字节	[17]
23	差分攻击	2^{118}	$2^{126.7}$	2^{120} 字节	[16]
23	多差分攻击	$2^{113.5}$	$2^{126.7}$	2^{17} 字节	本文

本文第 1 节给出了符号定义和 SMS4 算法介绍.第 2 节介绍多差分分析的分析方法及如何获取攻击中所要用到的两个矩阵.第 3 节给出具体的攻击过程以及数据、时间、存储复杂度的分析.最后是总结.

1 初步认知

为了方便理解论文中的符号,我们首先给出符号含义的解释;其次,给出 SMS4 加密算法的描述.

1.1 符号描述

表 2 给出了符号含义的解释.

Table 2 Description of symbols

表 2 符号描述

F_2^{32}	二元域上 32 比特的向量集合
$S(\cdot)$	8 比特的非线性转换
$<<<i$	左循环 i 位
$>>>i$	右循环 i 位
$\|\|$	比特串的级联
ΔX	$X\oplus X'$,其中, $X, X'\in F_2^{32}$
RK_i	第 i 轮子密钥,其中,$0\leqslant i\leqslant 31$
$X^{[i,j]}$	X 中从 i 比特到 j 比特的比特串
$X_{[i,j]}$	X 中第 i 个和第 j 个 nibble
Δ_0,Δ_r	输入和输出的差分集合
δ_0,δ_r	具体的输入和输出差分值
$E_K(\cdot)$	密钥 K 下的加密
$E_K^{-i}(\cdot)$	密钥 K 下解密 i 轮
n_k	需要恢复密钥的比特数

1.2 SMS4的加密过程

SMS4 算法[5,6]的分组长度为 128 比特,密钥长度为 128 比特.它使用广义的 Feistel 结构,共有 32 轮迭代.加密和解密的不同之处在于子密钥的使用顺序不同.由于 SMS4 的 32 轮的轮函数是相同的结构,我们仅描述一轮轮函数.

将第 i 轮轮函数(如图表 1)使用子密钥 RK_i 定义为一个映射 Ψ_{RK_i},那么,

$$\Psi_{RK_i}:(X_{i+1},X_{i+2},X_{i+3},X_{i+4})\leftarrow(X_i,X_{i+1},X_{i+2},X_{i+3},),$$
$$X_{i+4}\leftarrow X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus RK_i,$$
$$X_{i+4}\leftarrow(S(X_{i+4}^{[0,7]}),S(X_{i+4}^{[8,15]}),S(X_{i+4}^{[16,23]}),S(X_{i+4}^{[24,31]})),$$
$$X_{i+4}\leftarrow X_{i+4}\oplus(X_{i+4}<<<2)\oplus(X_{i+4}<<<10)\oplus(X_{i+4}<<<18)\oplus(X_{i+4}<<<24).$$

S 盒和线性转换 L 在图 1 中统一在 T 转换中.因为我们的攻击并没有利用密钥的生成算法,所以不再描述这一内容.关于 SMS4 密钥生成算法的详细描述见文献[5].

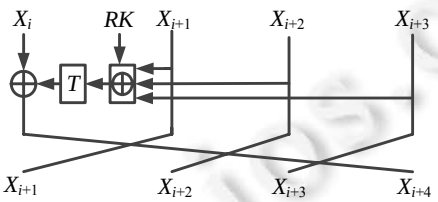

Fig.1 Round function for SMS4

图 1 SMS4 轮函数

2 主要方法

2.1 多差分攻击介绍

多差分分析是 Blondeau 等人[3]首次提出的一种攻击方法,该攻击方法是统计攻击的一种,一般包括 3 个阶段的分析过程.

(1) 过滤阶段:利用一定数量的明文和密文对获取候选密钥信息;

(2) 分析阶段:计算相应候选密钥的可能性并且获取可能性最大的一些候选密钥;

(3) 搜索阶段:由候选密钥推算主密钥,并测试每一个对应的主密钥的正确性.

接下来,我们将对多差分分析的过程进行描述.

输入:N 个选择明文和密文对(x_i,y_i),其中,$y_i=E_K(x_i)$;

输出:加密算法使用的密钥.

初始化 2^{n_k} 个计数器为 0
对于任意的$\delta_0\in\Delta_0$,执行:
    对于任意的明文对$(x,x\oplus\delta_0)$,执行:
        如果 $E_K(x)\oplus E_K(x\oplus\Delta_{r+\Delta r}$,那么,
            对任意的候选密钥 k,执行:
                计算 $\delta\leftarrow E_k^{-\Delta r}(E_K(x))\oplus E_k^{-\Delta r}(E_K(x\oplus\delta_0))$
                如果$\delta\in\Delta_r$,那么 $D[k]\leftarrow D[k]+1$
根据 $D[k]$取值大小排序,选取前 m 个可能性最大的候选密钥
对于列表中的每一个 k,执行:
    对于每一个对应于 k 的主密钥 CK,执行:
        如果 $E_{CK}(x_1)=y_1$,那么返回主密钥 CK

在本文中,多差分路径有不同的输入差分值,但是对应相同的输出差分值.更加详细的多差分攻击方法的介绍见文献[3].

2.2 矩阵法恢复密钥攻击

在本节中,我们描述攻击中所用矩阵构造的过程,该构造方法由 Bar-On 等人在文献[4]中提出.为了使本文结构完整和清晰,我们将矩阵构造整个过程进行了描述,并且描述方式更加适应本文攻击的环境.

- 首先对矩阵 A 的构造进行详细的描述.
  (1) 假设第 20 轮的输入差分为$(\Delta X_{20},\Delta X_{21},\Delta X_{22},\Delta X_{23})$,则第 20 轮的输出差分为$(\Delta X_{21},\Delta X_{22},\Delta X_{23},\Delta X_{20}\oplus L(Y_{20}))$,其中,$Y_{20}$ 为差分经过 S 盒之后引入的新变量;
  (2) 紧接上步,第 21 轮的输入差分为$(\Delta X_{21},\Delta X_{22},\Delta X_{23},\Delta X_{20}\oplus L(Y_{20}))$,则第 21 轮的输出差分为$(\Delta X_{22},\Delta X_{23},\Delta X_{20}\oplus L(Y_{20}),\Delta X_{21}\oplus L(Y_{21}))$,其中,$Y_{21}$ 为差分经过 S 盒之后引入的新变量;
  (3) 紧接上步,第 22 轮的输入差分为$(\Delta X_{22},\Delta X_{23},\Delta X_{20}\oplus L(Y_{20}),\Delta X_{21}\oplus L(Y_{21}))$,则第 22 轮的输出差分为$(\Delta X_{23},\Delta X_{20}\oplus L(Y_{20}),\Delta X_{21}\oplus L(Y_{21}),\Delta X_{22}\oplus L(Y_{22}))$,其中,$Y_{22}$ 为差分经过 S 盒之后引入的新变量;
  (4) 紧接上步,第 23 轮的输入差分为$(\Delta X_{23},\Delta X_{20}\oplus L(Y_{20}),\Delta X_{21}\oplus L(Y_{21}),\Delta X_{22}\oplus L(Y_{22}))$,则第 23 轮的输出差分为$(\Delta X_{20}\oplus L(Y_{20}),\Delta X_{21}\oplus L(Y_{21}),\Delta X_{22}\oplus L(Y_{22}),\Delta X_{23}\oplus L(Y_{23}))$,其中,$Y_{23}$ 为差分经过 S 盒之后引入的新变量.

第 23 轮的输出差分$(\Delta X_{20}\oplus L(Y_{20}),\Delta X_{21}\oplus L(Y_{21}),\Delta X_{22}\oplus L(Y_{22}),\Delta X_{23}\oplus L(Y_{23}))$即为密文差分$(\Delta C_1,\Delta C_2,\Delta C_3,\Delta C_4)$.上述的符号变量均为 32 比特,那么共引进 128 个新的比特变量;将 128 比特的密文差分看做 128 个比特变量,那么代表密文差分的 128 个比特变量与新引进的 128 个比特变量存在线性关系,这种关系可以使用矩阵概念进行描述.本文将此矩阵称为矩阵 A.

需要说明的一点是,矩阵 A 的构造与算法本身的设计有关.所以在分析某个具体密码算法时,矩阵 A 是可以预获取的.其实,可以简单地理解为:只要知道密文的差分值和矩阵 A,那么添加在区分器之外的轮函数的输入和输出差分值就可以通过一次矩阵乘法运算获取.

- 其次,矩阵 B 的构造是与矩阵 A 相类似的.

如果对于每轮轮函数的 S 盒的输入和输出的值分别引进新的变量,那么因为每轮需要引进 64 个新的变量,区分器之外添加 4 轮,因此共有 256 个新的变量产生.另外,涉及 128 比特的密钥和 128 的密文,我们同样引进新的变量符号.因为在进 S 盒之前总会有 32 个比特的线性限制条件,所以共有 128 个线性限制条件.它们实际上刻画了 128 比特的密钥与密文值、S 盒的输入输出值之间的线性关系.因此,这种关系可以使用矩阵进行描述.我们记为矩阵 B.

3 23 轮 SMS4 的密钥恢复攻击

3.1 SMS4的19轮差分特征

在本文的攻击中,我们使用 Su 等人在文献[19]中给出的 19 轮的差分路径:

$$(a_0,a_1,a_1,a_2)\xrightarrow[p=2^{-126}]{19-round}(a_6,a_7,a_1,a_1).$$

其中,a_1=0x*f*3*f*30033,a_2=0x*f*3000030,a_6=0x3*f*0000*cf*,a_7=0x*ccf*3*f*300*fc*.

接下来定义两个集合: $DT=\{x\in Z_2^{32}\mid Prob_T(a_2\to x)\neq 0\}$,$\Omega=\{y\in Z_2^{32}\mid y=x\oplus 0x00f30003,x\in DT\}$,$a_0\in\Omega$. 其中,$DT$ 是 a_2 经过 T 操作之后所有可能的差分值的集合.根据 SMS4 算法中 S 盒的性质,对于一个固定的输入差分,存在一个可能性为 2^{-6} 的输出差分值、126 个可能性为 2^{-7} 的输出差分值,因此,Ω集合的大小为$(2^7-1)^2\approx 2^{14}$.

3.2 SMS4的23轮攻击描述

本节对于 SMS4 进行的 23 轮差分攻击使用第 3.1 节中的差分路径,并且采用 Bar-On 等人在文献[4]中提出的密钥恢复攻击的新方法.该攻击成功的原因在于:SMS4 的非线性层的混淆效果并不是很强,利用矩阵这一代数工具可以充分利用线性层约束进行明密文对的筛减,从而降低时间复杂度.此外,SMS4 的轮密钥之间不直接共享密钥比特,使得恢复的轮密钥比特可以全部用来验证主密钥.对于现有的 19 轮差分路径,要想攻击多于 23 轮的攻击是不可能的,因为这会出现 128 个线性方程含有多于 128 个变量的情况,即,中间状态值对于某个明密文对是多种可能的,从而提高时间复杂度.

定义集合 $SET=\{x\in Z_2^{32}\mid Prob_T(a_7\to x)\neq 0\}$,是所有 a_7 经过 T 操作之后可能的差分取值.

定义 $\Lambda=\{y\in Z_2^{32}\mid y=x\oplus a_6,x\in SET\}$.根据 SMS4 中 S 盒的性质,Λ集合的大小为$(2^7-1)^3\approx 2^{21}$.

攻击 23 轮 SMS4 时,我们构建 structure,在 structure 中存在许多明文对(s_1,s_2),$s_1=(x,const_1,const_2,const_3)$,$s_2=(x\oplus a_0,const_1\oplus a_1,const_2\oplus a_1,const_3\oplus a_2)$,其中,$a_0\in\Omega$,且 x 为所有的 32bit 的可能取值.则一个 structure 包含 $2^{32}\times 2^{14}=2^{46}$ 个明文对.

假设需要 m 个 structure,那么一共可以构建 $m\times 2^{46}$ 个明文对,明文个数为 $m\times 2^{32}\times 2=m\times 2^{33}$.这些明文对的差分值为$(\Omega,a_1,a_1,a_2)$.具体的攻击过程如下(如图 2 所示).

1. 利用第 2.2 节中描述的办法预获取辅助矩阵 A 与辅助矩阵 B;
2. 对于每一个明文对(P_1,P_2)和对应的密文对(C_1,C_2),计算相应的密文差分,并判断密文差分值得第 1 个分支是否属于Λ集合:若否,舍弃这个明文对.这一步骤完成之后,剩余 $m\times 2^{46}\times\frac{2^{21}}{2^{32}}=m\times 2^{35}$ 个明文对;
3. 对于每一个剩余的明密文对(P,C)和(P',C'):
   - 密文的差分值异或(a_6,a_7,a_1,a_1)之后乘以矩阵 A,获取第 20 轮~第 23 轮 15 个活性 S 盒的输入和输出差分值;
   - 判断上步中输入和输出差分值是否符合 S 盒差分分布表:若否,则舍弃这一对明文,返回第 2 步继续进行计算.假设利用 S 盒删掉不符合差分分布表的密文对的概率为 0.5,那么在整个过程结束后,大约剩余 $m\times 2^{35}\times 2^{-12}=m\times 2^{23}$;
   - 对于符合差分分布表的输入和输出差分值,可以获取 S 盒相应的输入和输出值.并将这些值存储在一个表中,记为 list.
4. 对于 list 中的每一项ω:
   - 由ω和密文组成的向量乘以矩阵 B 获取密钥;
   - 猜测非活跃 S 盒对应的子密钥,并根据密钥生成算法计算主密钥.验证密钥的正确性,若通过验证,则返回正确候选密钥.

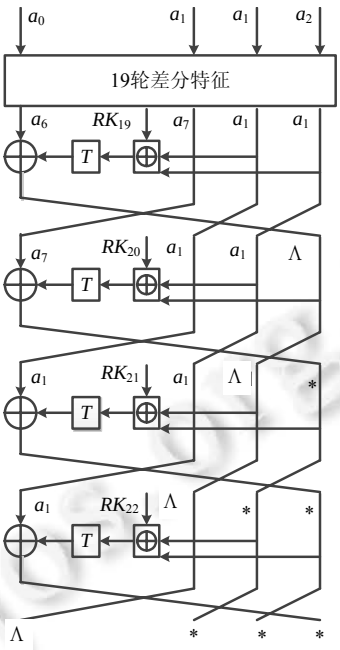

Fig.2 Diagram for differential cryptanalysis on 23-round SMS4

图 2 23 轮 SMS4 差分分析图示

3.3 复杂度分析

- 数据复杂度

文献[3]引用了 Blondeau 等人在文献[20]中得到的公式 $N=(-2)\times c\times\frac{\ln(2\sqrt{\pi}l2^{-n_k})}{|\Delta_0|D(p_*\|p)}$ 来计算多差分攻击数据复杂度的计算,并指出:如果要想获得的 0.8 的攻击成功率,那么 c 应该取值为 1.5;如果成功率为 0.9,那么 c 取值为 2.$D(p_*\|p)$是 p_*和 p 的 Kullback-Leibler 离散值,计算规则为

$$D(p_*\|p)=p_*\ln\left(\frac{p_*}{p}\right)+(1-p_*)\ln\left(\frac{1-p_*}{1-p}\right).$$

p_*是在正确密钥下多条差分路径的等价概率, $p_*=\frac{\sum_{i,j}p_*^{(i,j)}}{|\Delta_0|}\approx 2^{-126}$.$p$ 是错误密钥下多条差分路径的等价概率, $p=\frac{\sum_{i,j}p^{(i,j)}}{|\Delta_0|}\approx\frac{|\Delta|\times 2^{-m}}{|\Delta_0|}\approx\frac{2^{-14}\times 2^{-m}}{2^{-14}}\approx 2^{-128}$.我们恢复的密钥比特数 n_k 是 120(之所以不是 128 比特,是因为在 20 轮存在一个非活性的 S 盒),我们选取优势为 $l=2^{118}$.在成功率为 0.9 时,这样计算 $N=2^{113.5}$.从而,一共需要 $m=2^{80.5}$ 个 structure,有 $2^{80.5}\times 2^{46}=2^{126.5}$ 个明文对可以用于多差分攻击.

- 时间复杂度

我们对攻击的每一步进行时间复杂度分析:

由于第 1 步可以预计算,所以我们只分析后面步骤的时间复杂度.

在第 2 步中会对明密文对进行筛选,经此之后,剩余明文对数为 $2^{126.5}\times\frac{2^{21}}{2^{32}}=2^{115.5}$.

第 3 步中,如果将一次矩阵 A 的乘法视为 1 轮的加密,那么需要 $2^{115.5}\times\frac{1}{23}=2^{111}$ 次的 23 轮加密.经过第 2 步之后,剩余的明文对数为 $2^{115.5}\times 2^{-12}=2^{103.5}$.

第 4 步中,如果将一次矩阵 B 的乘法视为 4 轮的加密,那么需要 $2^{103.5}\times(2^{1.01})^{15}\times\frac{4}{23}=2^{116.1}$ 次 23 轮的加密.在验证阶段,需要猜测 8 比特子密钥,所以需要 $2^{103.5}\times(2^{1.01})^{15}\times2^8=2^{126.7}$ 次 23 轮加密.

综上所述,所需的时间复杂度为 $2^{111}+2^{116.1}+2^{126.7}\approx2^{126.7}$.若想攻击的成功率为 0.8,则数据复杂度和时间复杂度都会增加一个 0.75 的因子.

- 存储复杂度

本文中的攻击采用 Bar-On 等人[4]提出的密钥恢复攻击方法,不需要为候选密钥提供计数器,从而可以极大地降低存储复杂度.在攻击过程中,只有矩阵 A 和 B 需要存储.矩阵 A 大小为 120×128,矩阵 B 大小为 120×(120×2+128).所以存储大小不会超过 2^{17} 个字节.

4 总 结

利用 SMS4 非线性层混淆效果差的弱点,采用矩阵这一代数工具充分提取密码算法线性层的约束信息,进行 SMS4 的多差分攻击改进.攻击使用 $2^{113.5}$ 个明文,在 $2^{126.7}$ 次等价的 23 轮攻击下,以概率 0.9 可以恢复密钥.攻击的优势在于极大降低存储复杂度——不超过 128KB 的存储空间存储两个辅助矩阵.其次,攻击所用的明文量也是目前对 SMS4 所有 23 轮攻击中最少的一个.

References:

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

[2] Knudsen LR. Truncated and higher order differentials. In: Proc. of the Int'l Workshop on Fast Software Encryption. Berlin, Heidelberg: Springer-Verlag, 1994. 196−211.

[3] Blondeau C, Gérard B. Multiple differential cryptanalysis: Theory and practice. In: Proc. of the Int'l Workshop on Fast Software Encryption. Berlin, Heidelberg: Springer-Verlag, 2011. 35−54.

[4] Bar-On A, Dinur I, Dunkelman O, *et al*. Cryptanalysis of SP networks with partial non-linear layers. In: Proc. of the Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2015. 315−342.

[5] http://www.oscca.gov.cn/UpFile/200621016423197990.pdf

[6] Diffie W, Ledin G. SMS4 encryption algorithm for wireless networks. IACR Cryptology ePrint Archive, 2008. 329.

[7] Liu F, Ji W, Hu L, *et al*. Analysis of the SMS4 block cipher. In: Proc. of the Australasian Conf. on Information Security and Privacy. Berlin, Heidelberg: Springer-Verlag, 2007. 158−170.

[8] Ji W, Hu L. New description of SMS4 by an embedding over GF (28). In: Proc. of the Int'l Conf. on Cryptology in India. Berlin, Heidelberg: Springer-Verlag, 2007. 238−251.

[9] Lu J. Attacking reduced-round versions of the SMS4 block cipher in the Chinese WAPI standard. In: Proc. of the Int'l Conf. on Information and Communications Security. Berlin, Heidelberg: Springer-Verlag, 2007. 306−318.

[10] Toz D, Dunkelman O. Analysis of two attacks on reduced-round versions of the SMS4. In: Proc. of the Int'l Conf. on Information and Communications Security. Berlin, Heidelberg: Springer-Verlag, 2008. 141−156.

[11] Zhang L, Zhang W, Wu W. Cryptanalysis of reduced-round SMS4 block cipher. In: Proc. of the Australasian Conf. on Information Security and Privacy. Berlin, Heidelberg: Springer-Verlag, 2008. 216−229.

[12] Etrog J, Robshaw MJ. The cryptanalysis of reduced-round SMS4. In: Proc. of the 15th Int'l Workshop on Selected Areas in Cryptography (SAC 2008). Revised Selected Papers. Sackville, 2009.

[13] Kim TH, Kim J, Hong S, *et al*. Linear and differential cryptanalysis of reduced SMS4 block cipher. IACR Cryptology ePrint Archive, 2008,2008:281

[14] Zhang W, Wu W, Feng D, *et al*. Some new observations on the SMS4 block cipher in the Chinese WAPI standard. In: Proc. of the Int'l Conf. on Information Security Practice and Experience. Berlin, Heidelberg: Springer-Verlag, 2009. 324−335.

[15] Liu Z, Gu D, Zhang J. Multiple linear cryptanalysis of reduced-round SMS4 block cipher. Chinese Journal of Electronics, 2010, 19(3):389−393.

[16] Su BZ, Wu WL, Zhang WT. Security of the SMS4 block cipher against differential cryptanalysis. Journal of Computer Science and Technology, 2011,26(1):130−138.

[17] Cho JY, Nyberg K. Improved linear cryptanalysis of SMS4 block cipher. In: Proc. of the Symmetric Key Encryption Workshop. 2011. 1−14.

[18] Liu MJ, Chen JZ. Improved linear attacks on the Chinese block cipher standard. Journal of Computer Science and Technology, 2014,29(6):1123−1133.

[19] Su B, Wu W, Zhang W. Differential cryptanalysis of SMS4 block cipher. IACR Cryptology ePrint Archive, 2010,2010:62.

[20] Blondeau C, Gérard B, Tillich JP. Accurate estimates of the data complexity and success probability for various cryptanalyses. Designs, Codes and Cryptography, 2011,59(1-3):3−34.

赵艳敏(1991－),女,山东潍坊人,硕士生,主要研究领域为密码学.

王美琴(1974－),女,博士,教授,博士生导师,主要研究领域为密码学.

刘瑜(1981－),女,博士,主要研究领域为密码学.