针对MIBS的宽度差分故障分析

王素贞[1] 赵新杰[2] 王 韬[2] 吴 杨[2]
(河北经贸大学经济管理学院 石家庄 050091)[1] (军械工程学院计算机工程系 石家庄 050003)[2]

摘 要 MIBS分组密码主要用于RFID轻量级密码设备实现,对其安全性研究尚无公开结果发表。首先给出了MIBS算法及故障分析原理,提出了一种针对MIBS的宽度差分故障分析方法,并通过仿真实验进行了验证。实验结果表明,由于其Feistel结构和S盒特性,MIBS易遭受宽度故障攻击,通过在第32轮和第31轮分别导入1次32位故障即可将64位主密钥降低到21.70位,经1秒钟暴力破解恢复完整密钥。该故障分析方法也可为其它分组密码差分故障分析提供一定思路。

关键词 分组密码,MIBS密码,Feistel结构,差分故障分析,宽度故障

中图法分类号 TP309 **文献标识码** A

Wide Differential Fault Analysis on MIBS

WANG Su-zhen[1] ZHAO Xin-jie[2] WANG Tao[2] WU Yang[2]
(Dept. of Economy and Management, Hebei University of Economics & Business, Shijiazhuang 050091, China)[1]
(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)[2]

Abstract MIBS is a block cipher used in the implementation of lightweight cryptographic equipment such as RFID tag, and there has been no published paper on its security at present. This paper presented the MIBS algorithm and differential fault analysis principle, proposed a wide fault analysis method on MIBS, and verified it through simulation. Experiment results demonstrate: due to its Feistel structure and S-box feature, MIBS is vulnerable to wide fault attack, after injecting 32-bit fault to the 32th and 31th round left register, 64-bit MIBS master key search space can be reduced to 21.70-bit, the full key can be recovered after 1 second brute-force-search, and the fault analysis method in this paper can provide some ideas on other block ciphers using S-box.

Keywords Block cipher, MIBS cipher, Feistel structure, Differential fault analysis, Wide fault

1 引言

密码算法实现的故障信息可作为密码破解的思想,最早由Boneh等人[1,2]在1996年提出,即利用随机硬件故障来攻击公钥密码体制,最终成功攻破RSA签名算法。E. Biham和A. Shamir将这种攻击思想进行改进,在1997年提出差分故障分析方法[2],从而成功攻破了DES算法。后来,研究者利用差分故障分析又分别提出了对AES, Camellia, CLEFIA, RC4等密码算法的攻击手段及相应对策。显然,不论公钥密码、分组密码还是流密码算法,都面临着故障攻击的严重威胁。在分组密码方面,特别是最近文献[3]对ISO/IEC 18033-3中大量分组密码进行了多字节硬件故障攻击实验,验证了多字节故障攻击(又称宽度故障攻击)的可行性和威胁性。

MIBS算法是文献[4]在CANS 2009会议中提出的轻量级分组密码,主要用于RFID卡等设备的加解密实现。RFID设备是物联网的基本组件单元,由于其门电路数量有限,对密码算法设计与实现提出了严格的要求。MIBS算法以1400个门电路的精密设计,完全胜任在RFID卡中的快速安全实现。目前在对MIBS分组密码的安全性分析方面,国内外尚无先例。本文研究了MIBS分组密码的抗差分故障分析安全性,基于宽度故障模型,提出了一种针对MIBS的差分故障分析方法,对攻击复杂度进行了分析,并通过仿真实验加以验证。

本文第2节介绍了MIBS算法;第3节给出了差分故障分析原理;第4节提出了针对MIBS密码的差分故障分析方法;第5节对攻击复杂度及实验结果进行了分析;最后为结束语。

2 MIBS算法

MIBS算法采用Feistel结构,分组长度为64位,支持64位、80位两种密钥长度,整个加密过程由32轮组成,其加密过程与Camellia分组密码[5]类似。

到稿日期:2010-05-03 返修日期:2010-08-19 本文受国家自然科学基金资助项目(60772082),河北省自然科学基金数学研究专项(08M010)资助。

王素贞(1964—),女,博士,教授,硕士生导师,主要研究方向为网络安全、移动Agent系统、密码安全性分析;**赵新杰**(1986—),男,博士生,主要研究方向为分组密码旁路分析和故障分析;**王 韬**(1964—),男,博士,教授,博士生导师,主要研究方向为信息安全和密码旁路分析;**吴 杨**(1985—),男,硕士生,主要研究方向为对称密码故障分析。

加密过程：加密轮函数为

$$\begin{cases} L_r = R_r \oplus F(L_{r-1}, k_r) \\ R_r = L_{r-1} \end{cases} \tag{1}$$

L_r 和 R_r 分别为第 r 轮 64 位分组的左 32 位和右 32 位，k_r 为第 r 轮轮密钥，F 轮函数由轮密钥加、S 查表函数、M 混淆函数、P 置换函数组成，具体描述如下。

1)轮密钥加：F 函数的左半部分 32 位输入同轮密钥按位进行异或；

2)S 盒查表函数：将轮密钥加 32 位结果，每 4 位作为查表索引，查找一个 4×4 的 S 盒；

$$\begin{aligned} y_0' &= y_0 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_7 \\ y_1' &= y_0 \oplus y_1 \oplus y_4 \oplus y_5 \oplus y_6 \\ y_2' &= y_1 \oplus y_2 \oplus y_5 \oplus y_6 \oplus y_7 \\ y_3' &= y_2 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \\ y_4' &= y_0 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_7 \\ y_5' &= y_0 \oplus y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \\ y_6' &= y_0 \oplus y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \\ y_7' &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \end{aligned} \tag{2}$$

3)M 混淆函数：将 S 盒查表函数结果乘以一个矩阵，进行 $(GF(2)^4)^8 \rightarrow (GF(2)^4)^8$ 混淆变换，$(y_0, y_1, \cdots, y_7) \rightarrow (y_0', y_1', \cdots, y_7')$；

4)P 置换函数：将 M 混淆函数结果分为 8 块(0,1,…,7)，置换后的 8 个索引(0,1,2,3,4,5,6,7)分别对应原索引(6,2,3,0,1,4,7,5)。

密钥扩展算法：MIBS 密钥扩展算法与 PRESENT 密钥扩展算法类似。对于 64 位密钥的 MIBS，其 32 轮扩展密钥通过主密钥 $K(k_0, k_1, \cdots, k_{63})$ 经下面迭代函数产生。

S^0 = user-key

for(i=0;i<32;i++)

{

$S^i = S^i >>> 15$;

$S^i = S\text{-}box(S^i[63:60]) || S^i[59:0]$;

$S^i = S^i[63:16] || S^i[15:11] \oplus (i+1) || S^i[10:0]$;

$rk^i = S^i[63:32]$;

}

不失一般性，本文仅研究 64 位 MIBS 故障分析。

3 差分故障分析原理

为增强分组密码抗线性和差分分析能力，现代分组密码大都使用 S 盒查表操作来提高密码非线性度，同时使用 S 盒查找表访问 Cache 又可提高软件实现算法的执行效率。但是恰恰是由于差分 S 盒的不完美分布特性，导致其面临严重的故障攻击威胁。假如在分组密码查表时，对未知查表输入值 a 导入随机故障 f，一般来说，攻击者可得到密文差分 f'，且满足：

$$S[a] \oplus S[a \oplus f] = f' \tag{3}$$

查表输入值 a 常与扩展密钥直接相关。对于 MIBS 密码来说，其轮函数中的查表索引即为某个已知状态值和扩展密钥的异或值，恢复 a 后，该扩展密钥值即可推断出来，然后在前一轮导入故障，利用恢复扩展密钥值计算前一轮查找 S 盒的输入和输出差分，继续推断前一轮扩展密钥，直至得到恢复初始密钥所需的扩展密钥集合，经分析推断出初始密钥。

4 针对 MIBS 的宽度差分故障分析

4.1 第 32 轮故障分析

在 MIBS 加密过程中，在第 32 轮导入多个故障，每个故障长度为 4 位。在第 32 轮左寄存器 L_{31} 中随机导入 $m(m=5)$个故障，故障传播如图 1 所示，分析过程如下：

(1)导入故障个数及位置

在 MIBS 第 32 轮随机导入 m 个故障后，故障差分无变化地传播到密文右半部分。在导入随机个数故障的情况下，通过正确和故障密文差分值 ΔC_R，可确定故障个数及导入故障位置。

(2)求解第 32 轮 S 盒输入差分 ΔIL_{31} 和输出差分 ΔS_{32}

由图 1 易知，第 32 轮 S 盒输入差分 ΔIL_{31} 等于 ΔC_R，S 盒的输出差分为

$$\Delta S_{32} = M^{-1}(P^{-1}(\Delta C_L)) \tag{4}$$

(3)求解第 32 轮扩展密钥

根据第 3 节差分故障分析原理，可得到第 32 轮查找 S 盒的索引值，若该索引值等于 $C_R \oplus rk_{32}$，若 C_R 已知，则可推断出 rk_{32}。

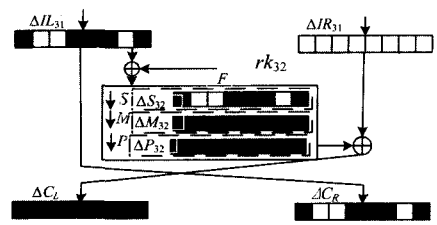

图 1 第 32 轮故障传播图

4.2 第 31 轮故障分析

在第 31 轮左寄存器 L_{30} 中随机导入 $m(m=5)$个故障，故障传播图如图 2 所示。

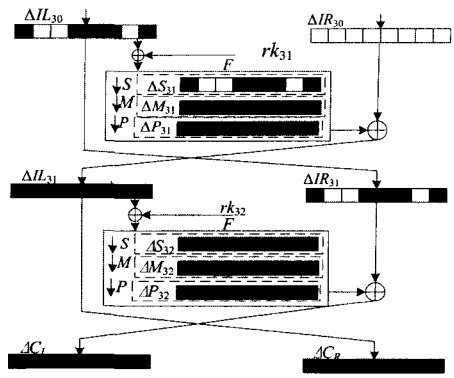

图 2 第 31 轮故障传播图

分析过程如下：

(1)计算第 31 轮输出差分 ΔIL_{31} 和 ΔIR_{31}

易知，第 31 轮左半部分输出差分 ΔIL_{31} 等于 ΔC_R，右半部分输出差分为

$$\Delta IR_{31} = \Delta C_L \oplus P(M(S(\Delta IL_{31} \oplus rk_{32}))) \tag{5}$$

(2)导入故障个数及位置

根据 ΔIR_{31} 中非 0 的 4 位值个数及其位置，即可确定第 31 轮导入故障的个数及位置。

(3)求解第 31 轮 S 盒输入差分 ΔIL_{30} 和输出差分 ΔS_{31}

由图 2 易知，第 31 轮 S 盒输入差分 ΔIL_{30} 等于 ΔIR_{31}，S

盒的输出差分为

$$\Delta S_{31}=M^{-1}(P^{-1}(\Delta IL_{31})) \tag{6}$$

(4)求解第 31 轮扩展密钥

根据第 3 节差分故障分析原理，可得到第 31 轮查找 S 盒的索引值 Y_{31} 为

$$Y_{31}=rk_{31}\oplus C_L\oplus P(M(S(C_R\oplus rk_{32}))) \tag{7}$$

Y_{31}，C_L，C_R，rk_{32} 均已知，则根据式(7)可推断出 rk_{31}。

4.3 密钥推断

根据 MIBS 密钥扩展算法，在获取 rk_{31} 和 rk_{32} 后，可将主密钥搜索空间降低到 2^{17}，密钥恢复过程如图 3 所示，算法如下：

1)在获取到 rk_{32} 后，可获得 S^{31} 的左32位值；

2)根据密钥扩展过程的逆过程进行 $S^{31}=S^{31}[63:16]||S^{31}[15:11]\oplus 32||^{31}[10:0]$ 运算；

3)取 S^{31} 的前 4 位作为查找 S^{-1} 索引值，查找逆 S 盒，并将查找结果与剩余 60 位组成新的 64 位值 S^{31}；

4)将 S^{31} 左移 15 位，并用移位后的值取代 S^{31}；

5)此时 S^{31} 的左半部分的 32 位值应与 rk_{31} 相同，易见 rk_{31} 前 17 位与 rk_{32} 后 17 位相等；

6)在一组 rk_{31} 和 rk_{32} 共同作用下，主密钥搜索空间可降低到 2^{17}，此时可利用暴力破解方式恢复主密钥。

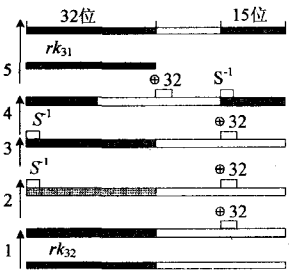

图 3 MIBS 初始密钥推导过程

5 实验结果

5.1 攻击复杂度分析

假设在 MIBS 第 32 轮注入 4 位随机值故障，满足下式

$$S[c\oplus k]\oplus S[c\oplus k\oplus f]=f' \tag{8}$$

c 为故障相关 4 位密文值，将 $c\oplus k$，$f(f\neq 0x00)$，f' 所有候选值代入式(8)，可得满足上式 k 值的统计分析表，见表 1。

表 1 MIBS S 盒故障分析效率统计

k 数目	出现次数	出现概率	均值
2	2880	0.75	1.5
4	960	0.25	1
总数	3840	1	$2.5=2^{1.322}$

由表 1 可知，在第 32 轮导入一次 32 位故障后，4 位密钥搜索空间可由原来的 2^4 降低到 $2^{1.322}$，据此可预测在 32 轮随机导入 32 位故障后，rk_{32} 将由 2^{32} 降到 $1526(2^{10.576})$ 左右，下面通过仿真实验验证攻击复杂度分析理论的正确性。

5.2 实验结果

在普通 PC 机(CPU 为 Intel(R) Celeron(TM) 1.3GHz，内存为 512MB)上使用 C++语言编程实现了本文 MIBS 多字节故障攻击，其中故障诱导过程通过计算机软件模拟。

在 MIBS 第 32 轮一次导入故障宽度为 32 位时，采集了 10 组攻击数据，每组对 rk_{32} 进行了 10000 次攻击，并对每组数据 rk_{32} 候选值个数求均值，将其作为纵坐标来绘制图 4。易见第 32 轮单次导入 32 位故障，可将 rk_{32} 搜索空间由 2^{32} 降到 $1544(2^{10.593})$。10 组实验测试数据的均值 1544 与 5.1 节中攻击复杂度分析的 1526 基本相符，证明了 5.1 节理论的正确性。

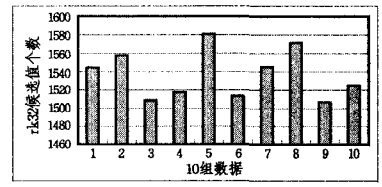

图 4 10 组 rk_{32} 密钥候选值数目统计

在分析获取 rk_{32} 候选值后，通过对第 31 轮导入一次 32 位故障，我们对 rk_{31} 候选值进行了进一步的分析。由 4.3 节可知 rk_{31} 前 17 位与 rk_{32} 后 17 位相等。根据该特性可进一步筛选 rk_{32} 和 rk_{31} 组合值，通过在 rk_{32} 和 rk_{31} 分别注入 1 次 32 位故障，10 组攻击数据(每组对 rk_{32}，rk_{31} 进行了 10000 次故障攻击) 经筛选后，其结果如图 5 所示。rk_{32}，rk_{31} 组合平均个数为 $25.89(2^{4.70})$，结合 4.3 节密钥推断算法，MIBS 64 位密钥搜索空间平均可降低到 $2^{21.70}$，经 1 秒钟暴力破解获取初始密钥，这也说明了实验方案的可行性以及 MIBS 算法对于差分故障分析的脆弱性。

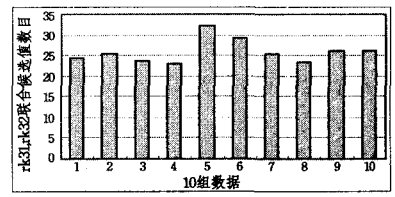

图 5 10 组 rk_{31}，rk_{32} 联合候选值数目统计

结束语 本文介绍了 MIBS 算法，并分析了 MIBS 的差分故障攻击原理及方法。实验及分析结果表明 MIBS 对于差分故障攻击是脆弱的。通过在第 32 轮和第 31 轮分别导入 1 次 32 位故障，即可将 64 位主密钥降低到 21.70 位，经 1 秒钟暴力破解恢复完整密钥。为了避免此类攻击，研究和改进 MIBS 算法抗差分故障攻击的方法，显得十分必要。

参 考 文 献

[1] Boneh D, DeMillo R, Lipton R. On the Importance of Checking Cryptographic Protocols for Faults[C]// Fumy W, ed. Advances in Cryptology—Eurocrypt'97. Konstanz, Germany, 1997, 1233: 37-51

[2] Biham E, Shamir A. Differential Fault Analysis of Secret Key Cryptosystems[C]// Advances in Cryptology-Crypto'97. Santa Barbara, California, USA, 1997, 1294: 513-525

[3] Fukunaga T, Takahashi J. Practical Fault Attack on a Cryptographic LSI with ISO/IEC 18033-3 Block Ciphers[C]// Proc. of 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography-FDTC2009. IEEE Computer Society, 2009: 84-92

[4] Izadi M, Sadeghiyan B, Sadeghian S S, et al. MIBS: A New Lightweight Block Cipher[C]// Garay J A, Miyaji A, Otsuka A, eds. CANS 2009. LNCS 5888. 2009: 334-348

[5] Aoki K, Ichikawa T, Kanda M, et al. Camellia: a 128-bit block cipher suitable for multiple platforms design and analysis[C]// Proc. of Selected Areas in Cryptography-SAC2000. volume 2012 of Lecture Notes in Computer Science. Springer, 2001: 39-56