MIBS 深度差分故障分析研究

赵新杰[1]，王韬[1]，王素贞[2]，吴杨[1]

(1. 军械工程学院 计算机工程系，河北 石家庄 050003；2. 河北经贸大学 经济管理学院，河北 石家庄 050091)

摘 要：给出了 MIBS 算法及故障分析原理，基于不同深度的故障模型，提出了 3 种针对 MIBS 差分故障分析方法，并进行实验验证。实验结果表明，由于其 Feistel 结构和 *S* 盒差分特性，MIBS 易遭受深度差分故障攻击，最好的结果为在第 30 轮左寄存器导入 1 次 4bit 故障，故障位置和故障差分值未知，可将 64bit 主密钥搜索空间降低到 2^{24}，经 1min 暴力破解恢复完整主密钥。此外，该故障分析方法也可为其他使用 *S* 盒的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；*S* 盒；差分故障分析；深度故障

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2010)12-0082-08

Research on deep differential fault analysis against MIBS

ZHAO Xin-jie[1], WANG Tao [1], WANG Su-zhen[2], WU Yang[1]

(1. Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;

2. Dept.of Economy and Management, Hebei University of Economics & Business, Shijiazhuang 050091, China)

Abstract: The MIBS algorithm and its differential fault analysis principle were presented, then three differential fault analysis methods against MIBS were proposed based on different depth of fault model and verified through experiments. Experiment results demonstrate that due to its Feistel structure and *S*-box differential feature, MIBS is vulnerable to deep differential fault attack. The best result is that after injecting one 4-bit fault into the 30th round left register, both the fault location and fault differential are unknown, the 64-bit MIBS master key searching space can be reduced to 2^{24} and be recovered after one minute brute-force-search. Moreover, the fault analysis method can provide some ideas on differential fault analysis against other block ciphers using *S*-box.

Key words: block cipher; MIBS cipher; Feistel structure; *S*-box; differential fault analysis; deep fault

1 引言

密码算法实现的故障信息可能作为密码破解的思想，最早由 Boneh 等人[1,2]在 1996 年提出，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]，通过分析正确密文和错误密文输出的差分值，成功攻破 DES 算法。后来，研究者利用差分故障分析又分别提出了对 ECC[3]、3DES[4]、AES[5~7]、Camellia[8~10]、ARIA[11]、SMS4[12,13]、RC4[14]等密码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 CHES 2010 会议上，有研究者[15]提出利用故障注入时物理效应输出的灵敏度进行密钥破解的方法，结果表明仅通过检测故障输出防御密码故

收稿日期：2010-06-28；修回日期：2010-09-27

基金项目：国家自然科学基金资助项目(60772082)；河北省自然科学基金资助项目(08M010)

Foundation Items: The National Natural Science Foundation of China (60772082); The Natural Science Foundation of Hebei Province (08M010)

障攻击是不够的，通过分析故障注入时的脉冲时延同加密中间状态的数据依赖性，使用相关性分析方法，仍可恢复 AES 密钥。由于故障的精确注入需要精密的设备（精度越高，代价越大），常常很难获取大量的理想故障样本，因此，对于攻击者来说，最有效的攻击应具备故障位置、宽度等限制条件相对宽松或攻击所需故障样本较小的特点。

随着信息技术和电子元器件的发展，密码设备发展呈现出轻型化的趋势，如何在 RFID 标签等轻型的密码设备上实现密码算法已成为分组密码研究的新热点。由于轻型密码设备门电路数量有限（一般在 200~2 000 个左右），因此对密码算法设计与实现提出了严格的要求。相继出现了 WISA 2005 会议提出的 mCrypton[16]、CHES 2006 会议提出的 HIGHT[17]、CARDIS 2006 会议上提出的 SEA[18]、CHES 2007 会议上提出的 PRESENT[19]、EUROMICRO 2008 会议上提出的 PUFFIN[20]、CANS 2009 会议上提出的 MIBS[21]算法。MIBS 算法以 1 400 个门电路的精密设计，完全胜任在 RFID 卡中的快速安全实现，其设计者从理论角度对 MIBS 密码进行了线性分析、差分分析、代数分析以及相关密钥分析，但并没有对其实现安全性（如抗故障攻击能力）进行分析。

非接触式 IC 卡（RFID）的出现是智能卡发展中的重要里程碑，它通过磁耦合或微波的方式来实现能量与信号的非接触传输，可有效解决接触式智能卡使用机械电气触点产生的静电击穿、机械磨损、易受外界环境影响等问题，并且已被成功应用到身份识别、公交票据、物联网等领域中。在 RFID 标签与读卡器通信过程中，需要运行数据加解密操作，由于 RFID 标签的时钟和电源都是使用天线的交流信号整形得到的，因此通过改变交流信号谐波的幅度、对称性、频率，很容易实施电压故障攻击，而且通过对 RFID 标签工作的环境进行电磁干扰和激光干扰，很容易实施电磁和激光故障攻击。文献[22,23]对被动式高频和超高频 RFID 标签的电磁和激光故障攻击进行了物理实验，结果表明 RFID 标签易遭受故障攻击。

本文对 MIBS 分组密码的抗故障攻击安全性进行了研究，基于 3 种深度的故障模型，分别提出了针对 MIBS 的差分故障分析方法，并通过仿真实验进行验证。最好的实验结果表明，通过在第 30 轮左寄存器导入 1 次 4bit 故障，故障位置和值未知，经分析可将 MIBS 64bit 主密钥降低到 24bit，1min 暴力破解可恢复完整密钥。

本文的创新点如下。

1) 将 MIBS 分组密码差分故障分析归结于求解 S 盒输入和输出故障差分问题，基于 3 种不同深度的故障模型，在故障位置和故障差分值未知的前提条件下，分别提出故障分析方法，分析获取故障位置和故障差分值，然后经进一步分析在有限时间内破解密钥，并对攻击复杂度进行了详细的分析，通过仿真实验进行了理论验证。

2) 3.3 节基于 MIBS 第 30 轮一个 4bit 的故障模型，故障位置和故障值未知，1 次故障注入经分析可获取故障位置和故障值，进一步分析可将 64bit 主密钥搜索空间降低到 2^{24}，经 1min 暴力破解恢复完整主密钥。在实际故障攻击中，故障注入次数越少[7,10,13]，攻击代价越小，攻击威胁力越大，因此 3.3 节分析方法可大大提高 MIBS 故障攻击的可行性。此外，3.3 节利用差分 S 盒的不完全覆盖特性求解 S 盒输入差分方法可适用于 AES、ARIA、Camellia[10]等分组密码的差分故障分析。

本文结构如下：第 2 节介绍了 MIBS 算法及差分故障攻击相关知识；第 3 节给出了 3 种 MIBS 差分故障分析方法；第 4 节对攻击复杂度及实验结果进行了分析；第 5 节为结束语。

2　相关知识

2.1　MIBS 算法

MIBS 算法采用 Feistel 结构，分组长度为 64bit，支持 64bit 和 80bit 2 种密钥长度，加密过程由 32 轮组成。

加密过程：加密轮函数为

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

1) 轮密钥加：F 函数的左半部分 32bit 输入同轮密钥按位进行异或；

2) S 盒查表函数：将轮密钥加 32bit 结果每 4bit 作为查表索引，查找一个 4 进 4 出的 S 盒；

3) M 混淆函数：将 S 盒查表函数结果乘以一个矩阵，进行$(\mathrm{GF}(2)^4)^8 \rightarrow (\mathrm{GF}(2)^4)^8$ 混淆变换，$(y_0, y_1, \cdots, y_7) \rightarrow (y'_0, y'_1, \cdots, y'_7)$，定义 M 函数的扩散度 τ 为一个 4bit 输入所影响的 4bit 输出值个数，由式(2)易见 y_0, y_1, y_2, y_3 对应 τ 值为 5，y_4, y_5, y_6, y_7 对应 τ 值为 6，

则 MIBS 的 M 混淆函数的平均扩散度为 5.5，该值在 4.1 节故障攻击复杂度分析时还将用到；

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

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 密钥扩展算法同 PRESENT[19] 密钥扩展算法类似，对于 64bit 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++){

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

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

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

$rk_{i+1} = S^i$[63:32];

}

不失一般性，本文仅对 64bit MIBS 差分故障分析进行研究。

2.2 故障攻击

故障攻击一般由故障诱导和故障分析2部分组成。

故障诱导主要是在某个合适的时间将故障注入密码运行中的某中间状态位置，其技术实施和实际效果严重依赖于攻击者的工作环境与所使用的设备，常用的故障诱导条件包括电压、时钟、温度、辐射、强光、涡流等因素的突然变化。

故障分析主要是利用错误的结果，使用特定分析方法恢复出全部或部分密钥。故障分析依赖于密码系统设计与实现、密码算法规范、所诱导的故障类型，并且在大多数条件下，故障分析都会同传统的密码分析方法相结合。在分组密码故障分析方面常用的分析方法为差分故障分析[2]，分析的对象主要为 S 盒查表操作。本文主要对针对 S 盒的分组密码差分故障分析进行研究，故障诱导问题在很多文献（如文献[24]）中都有讨论，本文在此不再赘述。

2.3 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 盒查表提高非线性度，同时 S 盒查表访问 Cache 又可提高算法软件实现效率，但是正是由于差分 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'，且满足下式

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

查表输入值 a 往往与扩展密钥直接相关，对于 MIBS 密码来说，其轮函数中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，利用恢复扩展密钥计算前一轮查找 S 盒输入和输出差分，继续推断前一轮扩展密钥，直至得到恢复主密钥所需扩展密钥集合，经分析推断出主密钥。

3 MIBS 深度差分故障分析

3.1 故障深度为 1

第 32 轮故障分析：在第 32 轮左寄存器 L_{31} 导入 1 个宽度为 4bit 的故障，故障位置和故障值未知（下文故障均属本类型），故障传播如图 1 所示，具体分析过程如下。

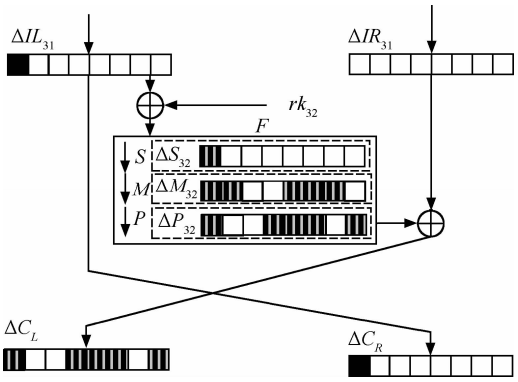

图 1 第 32 轮注入故障传播

1) 确定导入故障位置。

通过观察密文右半部分差分ΔC_R非 0 的 4bit 值位置，可确定所导入故障的位置。

2) 求解第32轮S盒输入差分ΔIL_{31}和输出差分ΔS_{32}。

第 32 轮 S 盒输入差分ΔIL_{31}等于ΔC_R，S 盒输出差分ΔS_{32}为

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

3) 求解第 32 轮扩展密钥 rk_{32}。

根据 2.3 节差分故障分析原理，可得到第 32 轮某次查找 S 盒索引值 $C_L \oplus rk_{32}$，并推断出一个 rk_{32} 中 4bit 密钥的 2~4 个候选值。多次执行步骤 1)~步骤 3)，可恢复完整的 rk_{32}，然后进行第 31 轮故障注入及分析。

第 31 轮故障分析：在第 31 轮左寄存器 L_{30} 导入 1 个宽度为 4bit 的故障，rk_{31} 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ΔIR_{31} 等于

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

2) 确定导入故障的位置。

根据ΔIR_{31} 中非 0 的 4bit 值位置，即可确定第 31 轮导入故障的位置。

3) 求解第31轮S盒输入差分ΔIL_{30}和输出差分ΔS_{31}。

第 31 轮 S 盒输入差分ΔIL_{30} 等于ΔIR_{31}，S 盒的输出差分ΔS_{31} 等于

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

4) 求解第 31 轮扩展密钥 rk_{31}。

根据第 2.3 节原理推导第 31 轮查找 S 盒索引值 Y_{31}

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

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

3.2　故障深度为 2

第 32 轮故障分析：在第 31 轮导入 1 个 4bit 宽度故障，如图 2 所示，分析过程如下。

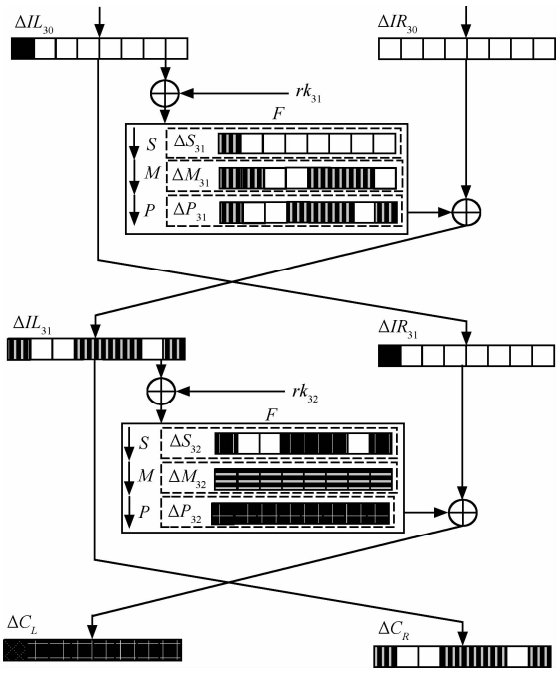

图 2　第 31 轮注入故障传播

1) 确定第 32 轮导入故障个数及位置。

通过观察ΔC_R 非 0 的 4bit 值位置，可确定第 32 轮所导入故障个数及位置，如表 1 所示，表 1 也验证了 2.1 节关于 MIBS 中平均 M 函数扩散度值为 5.5 的说明。

表 1　　**故障位置判断**

IL_{30} 故障位置	C_R 故障位置	IL_{30} 故障位置	C_R 故障位置
0	0,3,4,5,7	4	0,2,3,4,6,7
1	0,1,4,6,7	5	0,1,3,4,5,6
2	0,1,2,5,6	6	1,2,4,5,6,7
3	2,3,5,6,7	7	0,1,2,3,5,7

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

易知，ΔIL_{31} 等于ΔC_R，ΔS_{32} 中 5 或 6 个非 0 的 4bit 值同ΔIR_{31} 中的 1 个非 0 的 4bit 值进行作用，得到ΔC_L，这样可得到 8 个方程，8 个方程中变量只有 6 或 7 个，易知这 6 或 7 个变量可被求解出来，即可求解ΔS_{32} 和ΔIR_{31}。

$$\Delta C_L = \Delta IR_{31} \oplus P(M(\Delta S_{32})) \tag{8}$$

3) 求解第 32 轮扩展密钥 rk_{32}。

根据 2.3 节原理，可一次得到 rk_{32} 中的 5 或 6 个 4bit 密钥(20~24bit)的候选值。多次执行步骤 1)~步骤 3)，可恢复唯一的 rk_{32} 值。

第 31 轮故障分析：在第 30 轮注入 1 个 4bit 故障，结合上面恢复的 rk_{32} 值分析 rk_{31} 值。

3.3　故障深度为 3

在第 30 轮左寄存器 L_{29} 中导入 1 个 4bit 故障，故障传播如图 3 所示。该故障可 1 次恢复最后 2 轮的扩展密钥，具体分析过程如下。

1）确定故障位置，计算第 32 轮 S 盒输入差分ΔIL_{31} 和第 31 轮 S 盒输出差分ΔS_{31}。

易知，ΔIL_{31} 等于ΔC_R，ΔS_{31} 中的 5 或 6 个非 0 的 4bit 值同ΔIR_{30} 中的 1 个非 0 的 4bit 值进行作用得到ΔIL_{31}，这样可得到 8 个方程，8 个方程中变量只有 6 或 7 个，易知这 6 或 7 个变量可被求解出来，即可求解ΔS_{31} 和ΔIR_{30}。

$$\Delta IL_{31} = \Delta IR_{30} \oplus P(M(\Delta S_{31})) \tag{9}$$

式(9)可被转化为

$$\Delta S_{31} = M^{-1}(P^{-1}(\Delta IL_{31} \oplus \Delta IR_{30})) \tag{10}$$

ΔS_{31} 和ΔIR_{30} 的具体求解方法如下。

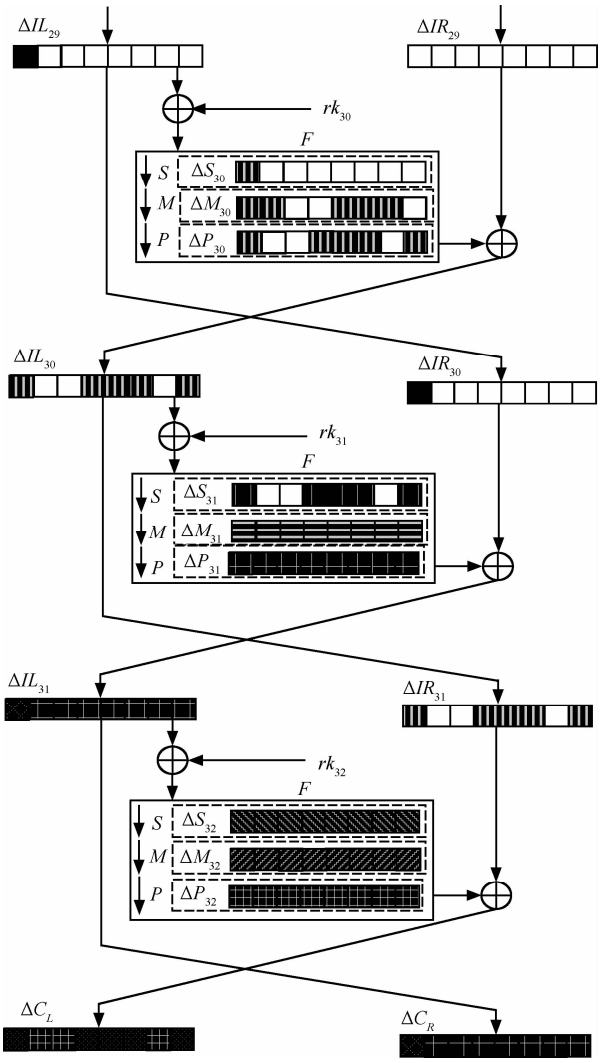

图 3 第 30 轮注入故障传播

① 假设故障位置为ΔIL_{29}第 i 个位置（$0 \leqslant i \leqslant 7$），如 i=0，此时ΔIR_{31}中第 1、2、6 这 3 个 4bit 值为 0，其余 5 个位置值非 0，ΔIR_{30}第 0 个 4bit 值为 0，其余 7 个位置值非 0。

② 将ΔIR_{30}的 16 个候选值代入式(10)，可分别得到一个ΔS_{31}值，然后判断ΔS_{31}的第 1、2、6 这 3 个 4bit 值是否为 0，其余 5 个位置值是否非 0，满足该条件的为ΔS_{31}和ΔIR_{30}候选值。

③ 分别假设故障位置为 1~7 其他 7 种可能，应用上面方法进行排除筛选。

实际仿真实验发现，对于正确的故障位置 i，ΔIR_{30}的 16 个候选值经式(10)排除分析后可得到唯一的ΔS_{31}值，对于错误的故障位置 i，经式(10)排除分析后会得到 0 个ΔS_{31}值，这样就得到了一种利用式(9)和式(10)求解故障位置、ΔS_{31}和ΔIR_{30}的一种方法。

2) 计算第 31 轮 S 盒输入差分ΔIL_{30}。

根据步骤 1 可得到ΔS_{31}，其中有 5 或 6 个非 0 的 4bit S 盒输出差分。由图 3 可知，ΔIL_{30}的 5 或 6 个非 0 的 4bit S 盒输入差分均相等，设为 δ，δ 共有 15 个候选值，为每个候选值构建一个差分 S 盒（每个盒 16 个元素），逐一检查ΔS_{31}中的 5 或 6 个非 0 的 4bit S 盒输出差分是否位于这 15 个差分 S 盒中，如果有任何一个输出差分不在某差分 S 盒中，则可排除该ΔIL_{30}候选值。

0	1	2	3
4	5	6	7
8	9	a	b
c	d	e	f

(a) S盒

0	1	2	3
4	5	6	7
8	9	a	b
c	d	e	f

(b) 差分S盒(δ=1)

0	1	2	3
4	5	6	7
8	9	a	b
c	d	e	f

(c) 差分S盒(δ=2)

图 4 MIBS S 盒和差分 S 盒元素(δ=1,2)按大小值递增分布

图 4 是 MIBS 的 S 盒和差分 S 盒（δ=1,2）按照大小值递增的分布，灰色方块表示覆盖到的值，白色方块表示没有覆盖到的值。易见图 4(a)中 MIBS 原始 S 盒取到了 0~f 16 个候选值，而差分 S 盒没有完全覆盖，仅有 7 个左右，如果ΔS_{31}中的 5 或 6 个非 0 的 4bit S 盒输出差分都在同一个差分 S 盒的灰色区域，则该差分 S 盒对应的 δ 值可能是正确的；而如果ΔS_{31}中的 5 或 6 个非 0 的 4bit S 盒输出差分中至少有一个在同一个差分 S 盒的白色区域，即可排除掉 δ 值，将 δ 的 16 个候选值经排除分析后，大部分情况下可得到唯一的 δ 值，具体可参考 4.2 节实验结果统计分析部分。

事实上，对于 SPN 结构分组密码，如 AES、ARIA，在加密第 $r-1$ 轮混淆函数前注入单个字节故障（r 为加密轮数），利用差分 S 盒取值的不完全覆盖特性，可求解第 r 轮的相关密钥；对于 Feistel 结构分组密码，如 Camellia，在加密第 $r-2$ 轮混淆函数前注入单字节故障，利用差分 S 盒取值的不完全覆盖特性，可求解第 $r-1$ 轮、r 轮相关密钥[10]。

3) 计算第 32 轮 S 盒输出差分ΔS_{32}。

根据步骤 2 推导的ΔIL_{30}，结合ΔC_L和 MIBS 轮函数，可推导出ΔS_{32}：

$$\Delta S_{32} = M^{-1}(P^{-1}(\Delta C_L \oplus \Delta IL_{30})) \tag{11}$$

4) 求解第 32 轮扩展密钥 rk_{32}。

根据 2.3 节原理，可推断出 rk_{32} 的候选值。

5) 求解第 31 轮扩展密钥 rk_{31}。

第 31 轮 S 盒输入差分ΔIL_{30}和输出差分ΔS_{31}的候选值已知，根据 2.3 节原理，可推断出 rk_{31}。

3.4 主密钥恢复

根据 2.1 节 MIBS 密钥扩展算法，获取 rk_{31} 和 rk_{32} 可将主密钥空间降低到 2^{17}，主密钥恢复算法如下：

1) 在获取到 rk_{32} 后，可获得 S^{31} 的左 32bit 值；

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

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

4) 将 S^{31} 左移 15bit，并用移位后的值取代 S^{31}；

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

6) 在一组 rk_{31} 和 rk_{32} 共同作用下，主密钥空间可降低到 2^{17}，暴力破解可恢复其值。

4 实验结果

4.1 攻击复杂度分析

假设在 MIBS 第 32 轮注入 4bit 随机值故障，满足式(12)：

$$S[c\oplus k]\oplus S[c\oplus k\oplus f]=f' \tag{12}$$

其中，c 为故障相关 4bit 密文值，将 $c\oplus k, f(f\neq 0x00)$, f'所有候选值代入式(12)，可得满足式(12)的 k 值统计分析表，如表 2 所示。

表 2　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	2 880	0.75	1.5
4	960	0.25	1
总数	3 840	1	$2.5=2^{1.322}$

3.1 节故障攻击复杂度分析：由表 2 可知，在 MIBS 某轮左寄存器同一个 4bit 的位置连续 2 次导入单字节随机故障可恢复对应的 4bit 密钥值，理想情况下恢复某轮扩展密钥需 16 次故障导入，恢复 rk_{31} 和 rk_{32} 共需深度为 1 的 32 次 4bit 故障注入。

表 3　故障次数与扩展密钥搜索空间的关系

故障次数 N	扩展密钥搜索空间（出现概率）（N 次故障位置均不重复）	扩展密钥搜索空间（故障位置可重复）
1	231 250.00	231 250.00
2	236.19 (87.5%)	478.67
3	20.21(98.44%)	53.90
4	5.65(99.80%)	9.89
5	2.31(99.98%)	2.85
6	1.43(99.997%)	1.50

3.2 节故障攻击复杂度分析：由于 M 函数扩散度为 5.5，经统计分析，在导入深度为 2 的故障模型下，故障注入次数和某轮扩展密钥平均搜索空间关系见表 3，易见 32 轮和 31 轮分别 3 或 4 次随机故障注入即可将 rk_{32} 和 rk_{31} 搜索空间均降低到 20 个以内，结合 rk_{31} 和 rk_{32} 之间关系即可恢复唯一的 rk_{31} 和 rk_{32}。

3.3 节故障攻击复杂度分析：在 MIBS 第 30 轮导入 1 个 4bit 故障，即可将故障扩散至 31 轮 L_{30} 的 5 或 6 个 4bit 故障，32 轮 L_{31} 全部 32bit 故障，由于第 32 轮 S 盒输入差分已知，每个第 32 轮 S 盒输出差分可将 rk_{32} 密钥空间降低到 $2^{10.576}=2.5^8=1\ 526$，由于第 32 轮 S 盒输出差分个数等于第 31 轮 S 盒输入差分 ΔIL_{30} 的个数，假设为 m，则 30 轮导入 1 个 4bit 故障可将 rk_{32} 密钥搜索空间降低到 1 526 m 个，同时由于第 31 轮 S 盒输出差分已知，结合每个第 31 轮 S 盒输入差分可将 rk_{31} 密钥空间降低到 $2^{17.82}=(2.5^5\times4\times16\times16\times16+2.5^6\times4\times16\times16)/8$。由于 MIBS 第 30 轮导入 1 个 4bit 故障的位置共有 8 种，则整个 rk_{32} 和 rk_{31} 的初步联合密钥搜索空间为 $m\times 2^{17.82+10.576+3}=m\times 2^{31.396}$，然后可进一步结合 3.4 节 rk_{31} 前 17bit 同 rk_{32} 后 17bit 相等特性进一步降低。

4.2 实验结果与分析

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，其中故障诱导过程是通过计算机软件模拟的，攻击结果如表 4 所示。

表 4　MIBS 深度故障分析结果

攻击	故障类型	故障位置	样本量	主密钥空间	时间
3.1 节	4bit 随机故障	L_{30},L_{31}	32	2^{17}	1s
3.2 节	4bit 随机故障	L_{29},L_{30}	6~8	2^{17}	1s
3.3 节	4bit 随机故障	L_{29}	1	2^{24}	1min

篇幅限制，下面仅给出故障深度为 3 时的具体实验数据统计分析。

在通过对第 30 轮导入一次 4bit 故障，为便于统计分析，故障位置假设已知为 L_{29} 第 0~3bit。通过采集 10 组数据，每组进行 100 万次故障攻击实验，得出第 31 轮 S 盒输入差分 ΔIL_{30} 个数 m 的统计图，如图 5 所示，可见 m 的值只有 1 和 3 这 2 种情况，m 平均值为 1.25 左右，根据 4.1 节分析 rk_{32} 密钥搜索空间降低到 1907=1526×1.25 个。通过对 rk_{32} 进行 100 万次攻击，得到 rk_{32} 候选值数量的频率统计

图，如图 6 所示，rk_{32} 候选值数量最小为 256，当其小于等于 8 192 时(概率为 80%)，rk_{32} 平均候选值个数为 2 433，该值也基本接近于理论值 1 907。

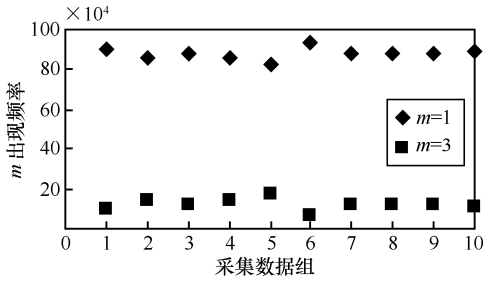

图 5 10 组 100 万次 m 值出现频率统计

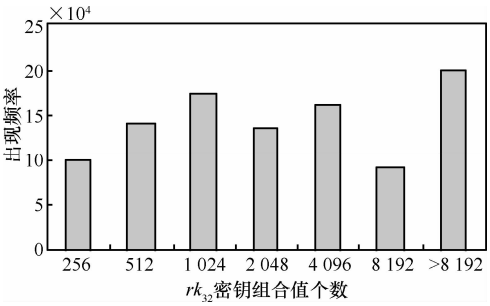

图 6 100 万次 rk_{32} 密钥候选值数目频率统计

在分析获取 rk_{32} 候选值后，对 rk_{31} 候选值进行了进一步分析，并结合 rk_{31} 前 17bit 同 rk_{32} 后 17bit 相等特性进一步筛选 rk_{31} 和 rk_{32} 组合值，1 万次攻击的 rk_{31} 和 rk_{32} 组合值数量的频率统计如图 7 所示。可见 MIBS 64bit 密钥搜索空间最小可被降低到 2^{25}，经 2min 暴力破解获取主密钥，证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。实际上，如果 L_{29} 注入故障的 4bit 索引值为 4~7，恢复 rk_{31} 和 rk_{32} 组合值数会更小，一般为 128~1 024 左右，MIBS 64bit 密钥搜索空间最小可被降低到 2^{24}，1min 内即可恢复主密钥。

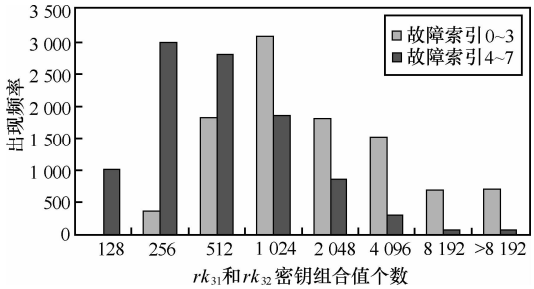

图 7 1 万次 rk_{31},rk_{32} 联合候选值数目频率统计

5 结束语

在故障攻击方面大体有 3 个研究方向：故障注入、故障分析、故障攻击检测与防护，本文主要对 MIBS 分组密码故障分析进行了研究，并通过软件仿真进行了验证。理论分析和仿真实验结果表明 MIBS 易遭受深度差分故障攻击，最好实验结果为在第 30 轮导入 1 次 4bit 故障，故障值和位置未知，可将 64bit 主密钥搜索空间降低到 2^{24}，经 1min 暴力破解恢复完整主密钥。

以下几个方面值得将来研究和关注：第一，研究 RFID 标签故障注入方法，利用本文故障分析方法，对实现了 MIBS 算法的 RFID 标签开展故障攻击物理实验；第二，研究 MIBS 密码故障攻击检测与防护措施；第三，开展密码故障灵敏度分析研究，研究故障注入时泄漏的物理效应同加密中间状态的相关性及密钥分析方法。

参考文献：

[1] BONEH D, DEMILLO R, LIPTON R. On the importance of checking cryptographic protocols for faults[A]. Eurocrypt 1997[C]. Konstanz, Germany, 1997. 37-51.

[2] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[A]. CRYPTO 1997[C]. Santa Barbara, California, USA, 1997. 513-525.

[3] BIEHL I, MEYER B, MULLER V. Differential fault analysis on elliptic curve cryptosystems[A]. CRYPTO 2000[C]. Santa Barbara, California, USA, 2000. 131-146.

[4] HEMME L. A differential fault attack against early rounds of (triple-) DES[A]. CHES 2004[C]. Cambridge (Boston), USA, 2004. 254-267.

[5] PIRET G, QUISQUATER J J. A differential fault attack technique against SPN structures, with application to the AES and khazad[A]. CHES 2003[C]. Cologne, German, 2003. 77-88.

[6] DEBDEEP M. An improved fault based attack of the advanced encryption standard[A]. AFRICACRYPT 2009[C]. Gammarth, Tunisia, 2009. 421-434.

[7] MICHAEL T, DEBDEEP M. Differential fault analysis of the advanced encryption standard using a single fault[EB/OL]. http://eprint.iacr.org/2009/575.pdf, 2009.

[8] ZHOU Y B, WU W L, XU N N, *et al*. Differential fault attack on camellia[J]. Chinese Journal of Electronics, 2009, 18(1):13-19.

[9] ZHAO X J, WANG T. An improved differential fault analysis on camellia[EB/OL]. http://eprint.iacr.org/2009/585.pdf, 2009.

[10] ZHAO X J, WANG T. Further improved differential fault analysis on camellia by exploring fault width and depth[EB/OL]. http://eprint.iacr.org/2010/026.pdf, 2010.

[11] LI W, GU D W, LI J R . Differential fault analysis on the ARIA algorithm[J]. Information Sciences, 2008, 178(19):3727-3737.

[12] 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): 2596-2602.
ZHANG L, WU W L. Differential fault analysis on SMS4[J]. Chinese Journal of Computers, 2006, 29(9): 2596-2602.

[13] LI R L, SUN B, LI C, *et al*. Differential fault analysis on sms4 using a single fault[EB/OL]. http://eprint.iacr.org/2010/063, 2010.

[14] HOCH J J, SHAMIR A. Fault analysis of stream ciphers[A]. CHES 2004[C]. Cambridge (Boston), USA, 2004. 240-253.

[15] LI Y, SAKIYAMA K, *et al*. Fault sensitivity analysis[A]. CHES 2010[C]. Santa Barbara, California, USA, 2010. 320-334.

[16] LIM C H, KORKISHKO T. A lightweight block cipher for security of low-cost RFID tags and sensors[A]. WISA 2005[C]. Jeju Island, Korea, 2006. 243-258.

[17] HONG D, SUNG J, HONG S, *et al*. HIGHT: a new block cipher suitable for low-resource device[A]. CHES 2006[C]. Yokohama, Japan, 2006. 46-59.

[18] STANDAERT F X, PIRET G, GERSHENFELD N, *et al*. SEA: a scalable encryption algorithm for small embedded applications[A]. CARDIS 2006[C]. Tarragona, Spain, 2006. 222-236.

[19] BOGDANOV A, KNUDSEN L R, LEANDER, *et al*. PRESENT: an ultra-lightweight block cipher[A]. CHES 2007[C]. Vienna, Austria, 2007. 450-466.

[20] CHENG H, HEYS H, WANG C. PUFFIN: a novel compact block cipher targeted to embedded digital systems[A]. The 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools[C]. University of Parma, Parma (Italy), 2008. 383-390.

[21] IZADI M, SADEGHIYAN B, SADEGHIAN S S, *et al*. MIBS: a new lightweight block cipher[A]. CANS 2009[C]. Kanazawa, Ishikawa, Japan, 2009. 334-348.

[22] MICHAEL H, JORN-MARC S, THOMAS P. RFID and its vulnerability to faults[A]. CHES 2008[C]. Washington, DC, USA, 2008. 363-379.

[23] MICHAEL H, THOMAS P MARTIN F. On the security of RFID devices against implementation attacks[J]. International Journal of Security and Networks, 2010, 5(2/3):106-118.

[24] GIRAUD C, THIEBEAULD H. A survey on fault attacks[A]. CARDIS 2004[C]. Toulouse, France, 2004. 22-27.

作者简介：

赵新杰（1986-），男，河南开封人，军械工程学院博士生，主要研究方向为分组密码旁路分析和故障分析。

王韬（1964-），男，河北石家庄人，博士，军械工程学院教授、博士生导师，主要研究方向为信息安全和密码旁路分析。

王素贞（1964-），女，河北石家庄人，博士，河北经贸大学教授、硕士生导师，主要研究方向为网络安全、移动 Agent 系统和密码安全性分析。

吴杨（1985-），男，四川成都人，军械工程学院硕士生，主要研究方向为对称密码故障分析和卫星网络认证安全性分析。