扩大故障注入范围的 SM4 差分故障攻击研究

朱仁杰
(海军工程大学信息安全系 武汉 430000)

摘 要 为了使 SM4 分组密码的差分故障攻击在现实条件下更容易实现,文中深入研究并分析了可用于 SM4 差分故障攻击的各种方法。在现有的故障攻击方法基础上,提出了一种将故障注入的范围扩大到加密算法第 26 轮的攻击方法,解除了以往攻击方法中故障必须注入到加密算法后 4 轮的限制,达到了扩大可故障注入范围的目的。

关键词 差分故障攻击,扩大故障范围,SM4 分组密码算法
中图法分类号 TP301 **文献标识码** A

Study on SM4 Differential Fault Attack Under Extended Fault Injection Range

ZHU Ren-jie
(Department of Information Security, Naval University of Engineering, Wuhan 430000, China)

Abstract In order to make the differential fault attack on SM4 block cipher easier to implement under real conditions, various methods were studied and analyzed in depth for SM4 differential fault attack in this paper. Among the existing fault attack methods, this paper proposed a new attack method, which allow the scope of fault injection to extend to the 26th round of encryption algorithm. The limitation is removed that the fault must be injected into the last four rounds of encryption algorithm in the previous attack methods, and the purpose is achieved than expanding the fault injection range.

Keywords Different fault attack, Extended fault injection range, SM4 block cipher

1 引言

分组密码算法是现代密码学中的一个重要研究方向,是保障信息机密性和完整性的重要技术手段。为配合我国 WAPI 无线局域网标准的推广应用,SM4 分组密码算法(原名 SMS4[1])于 2006 年公开发布。随着我国密码算法标准化的发展,SM4 算法于 2012 年 3 月发布成为国家密码行业标准(标准号 GM/T0002-2012),于 2016 年 8 月发布成为国家标准(标准号 GB/T32907-2016)。2016 年 10 月,ISO/IEC SC27 会议专家组一致同意将 SM4 算法纳入 ISO 标准学习期。

SM4 算法自发布以来,国内外众多的科研人员对其进行了攻击,攻击方法[2-4]包括差分密码分析、线性密码分析、多维线性密码分析等。这些攻击方法的时间复杂度和空间复杂度较高,仅存在理论上的价值,在实际中不能对 SM4 分组密码算法构成威胁。

在诸多攻击手段中,故障攻击[5-10]由于能够被攻击者主动策划,为成功猜测秘密信息提供了更多的选择和更高的可能性,对密码应用安全造成了严重威胁。很多专家学者对于 SM4 算法的差分故障攻击都进行了深入的研究。在文献[11]中,所需要的故障模型为单字节随机故障,这种故障模型在实现上有较大的困难。文献[12]提出的攻击方法放宽了对故障注入的要求,只需要注入随机故障,不局限为单字节,但该方法在故障注入方面可以做更近一步的改进,使其对故障模型的要求更低。

本文为提高 SM4 差分故障攻击方法的实际可行性,深入分析了 SM4 算法结构特点与故障攻击的适用条件,在现有的攻击方法之上做出了进一步的改进,使其对故障注入的需求变得更低。对 SM4 加密算法的后 7 轮进行随机故障注入,可成功地利用错误密文信息攻击出原密钥。

2 SM4 算法描述

SM4 分组密码算法是一个迭代分组密码算法,由加密算法和密钥扩展算法组成。SM4 分组密码算法采用 Feistel 结构,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均采用 32 轮非线性迭代结构。加密运算与解密运算的结构相同,解密运算的轮密钥的使用顺序与加密运算相反。

2.1 密钥及密钥参量

SM4 分组密码算法的加密密钥长度为 128 bit,表示为 $MK=(MK_0,MK_1,MK_2,MK_3)$,其中 $MK_i(i=0,1,2,3)$ 为 32 bit。

轮密钥表示为 $rk_i(i=0,1,2,\cdots,31)$,为 32 bit。轮密钥由加密密钥生成。

$FK_i(i=0,1,2,3)$ 和 $CK_i(i=0,1,\cdots,31)$ 分别为系统参数与固定参数,用于密钥扩展算法,均为 32 bit。

2.2 加密算法

SM4 加密算法由 32 次迭代运算和一次反序变换 R 组成。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 $rk_i\in(Z_2^{32})^4(i=0,1,\cdots,$

本文受保密通信国防科技重点实验室基金项目(614210301030117)资助。
朱仁杰(1995-),男,硕士,主要研究方向为密码芯片安全性评估,E-mail:1149518111@qq.com。

31)。加密算法的运算过程如下。

(1)首先执行 32 次迭代运算:

$$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)$$
$$=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)$$

其中 $i=0,1,\cdots,31$。

(2)对最后一轮输出数据进行反序变换并得到密文输出:

$$(Y_0,Y_1,Y_2,Y_3)=R(X_{32},X_{33},X_{34},X_{35})$$
$$=(X_{35},X_{34},X_{33},X_{32})$$

其中,$T:Z_2^{32}\rightarrow Z_2^{32}$ 是一个可逆变换,由非线性变换 S 和线性变换 L 复合而成,即 $T=L\circ S$。

非线性变换 S 由 4 个并行的 S 盒组成,设输入为 $A=(a_0,a_1,a_2,a_3)\in(Z_2^8)^4$,则输出为 $B=(Sbox(a_0),Sbox(a_1),Sbox(a_2),Sbox(a_3))$。

L 是线性变换,非线性变换 S 的输出是线性变换的输入。设输入为 $B\in Z_2^{32}$,输出为 $C\in Z_2^{32}$,则:

$$C=L(B)=B\oplus(B\ll2)\oplus(B\ll10)\oplus(B\ll18)\oplus(B\ll24)$$

其加密算法流程如图 1 所示。

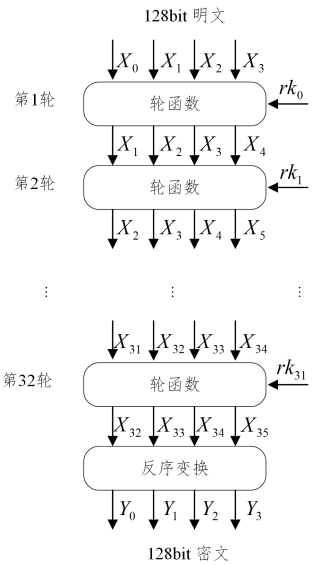

图 1 SM4 算法的加密流程

2.3 解密算法

解密变换与加密变换的结构相同,不同的仅是轮密钥的使用顺序。解密时轮密钥顺序与加密时顺序相反。

2.4 密钥扩展算法

轮密钥由加密密钥通过密钥扩展算法生成。设加密密钥为 $MK=(MK_0,MK_1,MK_2,MK_3)\in(Z_2^{32})^4$。轮密钥的生成方法为:

$$rk_i=K_{i+4}$$
$$=K_i\oplus T'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i)(i=0,1,\cdots,31)$$

其中,$K_0=MK_0\oplus FK_0$,$K_1=MK_1\oplus FK_1$,$K_2=MK_2\oplus FK_2$,$K_3=MK_3\oplus FK_3$。

(1)T'是将 2.2 节中的合成置换 T 的线性变换 L 替换为 L':

$$L'(B)=B\oplus(B\ll13)\oplus(B\ll23)$$

(2)系统参数 FK 的取值为 $FK_0=a3b1bac6$,$FK_1=56aa3350$,$FK_2=677d9197$,$FK_3=b27022dc$。

(3)固定参数 CK 的取值。设 $ck_{i,j}$ 为 CK_i 的第 j 个字节($i=0,1,\cdots,31;j=0,1,2,3$),即 $CK_i=(ck_{i,0},ck_{i,1},ck_{i,2},ck_{i,3})\in(Z_2^8)^4$,则 $ck_{i,j}=(4i+j)\times7(\mathrm{mod}\ 256)$。

3 SM4 差分故障分析

3.1 故障模型

如 2.2 节所述,SM4 算法是一种 32 轮迭代密码算法,每一轮都执行一次加密函数。对 SM4 算法进行故障攻击时,攻击者可以通过分析时钟周期等手段,来获取算法加密操作各轮开始的时间节点。

本文假设故障注入到加密算法的 26 轮至 31 轮的输出数据,以 29 轮为例,将轮函数输出的 32bit 数据变成一个随机值,即将 $X_{32}=F(X_{28},X_{29},X_{30},X_{31},rk_{28})\in Z_2^{32}$ 变成一个随机的 32bit 值。

攻击者可以利用电压毛刺、时钟毛刺等方法在特定轮注入故障。通过分析加密操作开始的时钟周期来控制故障注入的时间。

3.2 差分故障攻击第一步

注入的故障影响到轮函数的输出值,该输出值作为下一轮函数的输入,会影响下一轮函数的输出,最终产生加密错误的故障密文。

在攻击的第一步中,需要将随机故障注入到 SM4 加密算法 29 轮至 31 轮之间的任意位置。分析密码算法第 32 轮正确的加密操作与错误的加密操作可以分别得到式(1)、式(2):

$$X_{35}=X_{31}\oplus T(X_{32}\oplus X_{33}\oplus X_{34}\oplus rk_{31}) \quad (1)$$

$$X'_{35}=X_{31}\oplus T(X'_{32}\oplus X'_{33}\oplus X'_{34}\oplus rk_{31}) \quad (2)$$

其中,rk_{31} 是加密函数第 32 轮密钥,X'_{34} 和 X'_{35} 分别是加密函数第 31 轮与第 32 轮的故障输出。X'_{32} 和 X'_{33} 分别是加密函数第 29 轮与第 30 轮的输出,这两轮函数的输出可能是故障的,也可能是正确的,由故障的注入位置决定。无论这两轮函数的输出是正确的还是故障的,对式(2)的成立都没有任何影响,因此统一用 X'_{32} 和 X'_{33} 来表示加密函数第 29 轮与第 30 轮的输出。

将式(1)与式(2)进行异或运算,可以得到:

$$\Delta X_{35}=T(X_{32}\oplus X_{33}\oplus X_{34}\oplus rk_{31})\oplus T(X'_{32}\oplus X'_{33}\oplus X'_{34}\oplus rk_{31}) \quad (3)$$

式(3)两边同时进行线性变换 L 的逆运算,可以得到:

$$L^{-1}(\Delta X_{35})=S(X_{32}\oplus X_{33}\oplus X_{34}\oplus rk_{31})\oplus S(X'_{32}\oplus X'_{33}\oplus X'_{34}\oplus rk_{31}) \quad (4)$$

其中,L^{-1} 的具体运算过程为:

$$B=L^{-1}(C)=C\oplus(C\ll2)\oplus(C\ll4)\oplus(C\ll8)\oplus(C\ll12)\oplus(C\ll14)\oplus(C\ll16)\oplus(C\ll18)\oplus(C\ll22)\oplus(C\ll24)\oplus(C\ll30)$$

非线性变换 S 由 4 个独立的 S 盒组成,依此将式(4)分成 4 个独立的等式:

$$D_i=Sbox(X_{32,i}\oplus X_{33,i}\oplus X_{34,i}\oplus rk_{31,i})\oplus Sbox(X'_{32,i}\oplus X'_{33,i}\oplus X'_{34,i}\oplus rk_{31,i}),i=0,1,2,3 \quad (5)$$

D_i 表示为 $L^{-1}(\Delta X_{35})$ 的 8bit 数据,当 $i=0$ 时,代表前 8 位 bit,以此类推。

利用式(5)对所有可能的候选密钥进行筛选。将候选密钥代入到式(5)中,使等式成立的密钥可能为真正的密钥,没有使等式成立的密钥一定为不可能的密钥。4 个等式可以并行计算,计算的时间复杂度为 2^8。在攻击的过程中,需要利

用多对明密文对候选密钥进行筛选，利用一对明密文数据完成筛选之后，只将通过的密钥再次进行筛选，直到得到正确的密钥。这样做的目的是减小计算复杂度，提高攻击效率。

3.3　故障攻击第二步

由第一步的差分故障攻击可以得到第 32 轮密钥 rk_{31}。在接下来的攻击中，目标是依次恢复 rk_{30}，rk_{29}，rk_{28}。

攻击者在加密函数第 28 轮至第 30 轮之间注入随机故障，可以得到：

$$X'_{34}=X_{30}\oplus T(X'_{31}\oplus X'_{32}\oplus X'_{33}\oplus rk_{30}) \tag{6}$$

$$X_{34}=X_{30}\oplus T(X_{31}\oplus X_{32}\oplus X_{33}\oplus rk_{30}) \tag{7}$$

将式(6)、式(7)进行异或可以得到：

$$\Delta X_{34}=T(X_{31}\oplus X_{32}\oplus X_{33}\oplus rk_{30})\oplus T(X'_{31}\oplus X'_{32}\oplus X'_{33}\oplus rk_{30}) \tag{8}$$

利用在第一步中得到的 rk_{31}，可以分别计算出 X_{31} 与 X'_{31}。第 28 轮与第 29 轮函数输出的正确与否，不影响等式的成立，因此统一用 X'_{31} 和 X'_{32} 表示。运用与第一步中相同的密钥筛选方法，恢复出第 31 轮密钥 rk_{30}。

利用相同的方法恢复出第 30 轮密钥 rk_{29} 和第 29 轮密钥 rk_{28}，然后将 rk_{28}，rk_{29}，rk_{30}，rk_{31} 带入到密钥扩展算法中，恢复出原始密钥。

4　实验与分析

本文在 matlab 软件上进行模拟仿真实验，明文是 01234567 89ABCDEF FEDCBA98 76543210，仿真实验的主要过程包括故障注入、信息采集与故障分析。

4.1　攻击实验

在仿真实验中，需要分别在 29 至 31 轮、28 至 30 轮、27 至 29 轮、26 至 28 轮之间注入故障。生成若干个随机的 4 字节数据作为故障数据，随机选取注入故障范围内的加密操作，将故障数据加入到加密操作中，以此来模拟故障注入。

收集正确加密密文与故障加密密文，正确加密与错误加密的密文输出为：

```
correct_c:681EDF34 D206965E
          86B3E94F 536E4246
fault_c:6BF8202B 41A530E1
        E54DCC07 85A1D1CF
fault_c:EA6CBA46 274EFF36
        402EF995 DF81744D
fault_c:CACD4EAE 43AF8779
        C51C12C0 4B5EEB66
fault_c:F5A0560E 62C8A025
        FB97C350 2659DEB5
fault_c:A7DDF77A B9C30FB6
        268B7C64 B4E28FD6
fault_c:09245D67 2D4C1CBC
        B5EA2CCE 2B3A9347
fault_c:D95FB066 1EC936A6
        99624F23 90218F15
fault_c:EF193F5B A458C3A4
        7732A159 B832D741
```

图 2　输出密文数据

根据第 3 节所述的攻击原理开展故障攻击，对第 32 轮密钥的分析结果如图 3 所示。恢复得到 32 轮密钥为：91 24 A0 12。

对其他 3 轮的密钥分析与对 32 轮密钥分析过程类似，第 29 轮密钥分析结果与原始密钥分析结果如图 4 所示。

```
sub_roundkey0:91 E5
sub_roundkey1:24 B5
sub_roundkey2:34 A0
sub_roundkey3:12 86
sub_roundkey0:59 91
sub_roundkey1:24 EF
sub_roundkey2:41 A0
sub_roundkey3:12 88
roundkey32:91 24 A0 12
```

图 3　32 轮密钥分析结果

```
sub_roundkey0:2F 42
sub_roundkey1:8D FA
sub_roundkey2:36 71
sub_roundkey3:44 54
sub_roundkey0:42 88
sub_roundkey1:8D AB
sub_roundkey2:12 36
sub_roundkey3:54 BF
roundkey29:42 8D 36 54
SM4_KEY:01234567 89ABCDEF
        FEDCBA98 76543210
```

图 4　29 轮密钥与初始密钥的分析结果

利用攻击得到的密钥对相同明文进行加密，最终得到密文 681EDF34 D206965E 86B3E94F 536E4246，与攻击第一步中采集的正确密文信息一致，说明攻击成功地恢复了算法的初始密钥。

4.2　攻击过程分析

在 SM4 分组密码算法的第一步攻击中，攻击者在第 29 轮至第 31 轮之间注入随机故障，利用式(5)中的差分相等，恢复第 31 轮的轮密钥。

在对候选密钥进行筛选的过程中，加密函数中的非线性变换是由 4 个独立的 S 盒组成，因此，在对候选密钥进行筛选的过程中，将 32 bit 密钥拆分为独立的 4 组 8 bit，仿真实验结果表明，一组密文可将每组 8 bit 候选子密钥数量降为两个。一次成功的故障注入，可以把候选密钥数量降为 16 个，两次故障注入可恢复第 31 轮的轮密钥。

第二步攻击的目标是恢复 29、30、31 轮的轮密钥。在已恢复出后一轮密钥的基础上，可以恢复当前轮的轮密钥。

攻击者恢复 31 轮密钥 rk_{30}，需要在加密函数第 28 轮至第 30 轮之间注入随机故障，然后利用产生的故障差分进行密钥筛选，直到恢复出真正的密钥。

易知，攻击者在加密函数第 27 轮至第 29 轮之间注入随机故障，可恢复第 30 轮密钥。在第 26 轮至第 28 轮之间注入随机故障，可恢复第 29 轮密钥。

扩大故障注入范围的 SM4 分组密码算法差分故障攻击，在 8 次成功的故障注入的条件下，可恢复出最后 4 轮的轮密钥，从而恢复出算法密钥。其攻击的计算复杂度为 2^{10}。

结束语　为了使对 SM4 密码算法的差分故障攻击方法在实际中更容易实现，本文提出了一种将故障注入范围扩大到算法第 26 轮的攻击方法。分别在 29 至 31 轮、28 至 30 轮、27 至 29 轮、26 至 28 轮之间注入两个随机故障，可恢复出所有密钥信息。攻击者只需在 3 个加密周期之间的任意位置注入故障的能力，即可使用这种攻击方法，解除了以往攻击方法中故障必须注入到加密算法后 4 轮的限制，达到了扩大可故障注入范围的目的。

参 考 文 献

[1]　国家密码管理局. 国家密码管理局公告(7 号)[EB/OL]. [2016-11-04]. http://www.oscca.gov.cn/News/200709/News_1105.htm.

[2]　SU B Z, WU W L, ZHANG W T. Security of the SMS4 Block Cipher Against Differential Cryptanalysis[J]. Journal of Computer Science & Technology, 2011(1): 132-140.

(下转第 506 页)

表 4 密文图像的 NPCI 和 UACI

（单位：%）

NPCR	UACI
99.8977	33.4367

结束语 本文提出了一种基于分数阶超混沌的混沌细胞自动机图像加密算法，并且结合了明文图像，将置乱、代换、扩散 3 种操作有机地结合起来，使它们的优势互相补充。比一般加密或普遍使用的置乱-扩散结构更具安全性，并且加密效率更高。另外，本文使用高维超混沌系统，生成的伪随机序列不会因为计算机精度有限，而导致伪随机序列可能存在短周期，从而产生加密安全性不够高的问题。使用自适应加密，加密过程中不仅依赖于密钥，而且一定程度上依赖于明文和加密过程中产生的中间数据，使选择明文攻击将更难成功，算法的安全性更高。文中扩散算法使用混沌细胞自动机扩散，使扩散更复杂。本文算法不需要多轮迭代就可达到很高的安全级别，加密安全性与加密效率显著提高。

参 考 文 献

[1] 陈翼翔，汪小刚. 基于双随机相位编码的非线性双图像加密方法[J]. 光学学报，2014，34(7)：0710001.

[2] 陈翼翔，汪小刚. 一种基于迭代振幅-相位复算法和非线性双随机相位编码的图像加密方法[J]. 光学学报，2014，34(8)：0810003.

[3] GAO T G，CHEN Z Q. A new image encrypyion algorithm based on hyper-chaos[J]. Physics letter A，2008(372)：394-400.

[4] CHEN G，ZHAO X Y，LI J L. A Self-Adaptive Algoritthm on image Encryption[J]. Journal of Software，2005，16(11)：1975-1982.

[5] 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003，24(2)：51-57.

[6] ACHARYA B，PATRA S K，PANDA G. Image Encryption by Novel Cryptosystem Using Matrix Transformation[C]// First Internation Conference on Emerging Trends in Engineering and Technology，2008. Washington D C：IEEE Press，2008，77-81.

[7] 朱薇，杨庚，陈蕾，等. 基于混沌的改进双随机相位编码图像加密算法[J]. 光学学报，2014，34(6)：0607001.

[8] 潘泉，张磊，孟晋丽，等. 小波滤波方法及其应用[M]. 北京：清华大学出版社，2005.

[9] 刘钺. 一种小波变换域图像加密技术[J]. 计算工程与应用，2010，46(19)：157-159.

[10] 倪林. 小波变换与图像处理[M]. 合肥：中国科技技术大学出版社，2010.

[11] SCHNEIER B. Applied cryptography：protocols，algorithms，and source code in C[M]. John Wiley & Sons，2007.

[12] 绪其军，李德林，常琛亮，等. 基于 Q-plate 的双图像非对称偏振加密[J]. 物理学报：1-8.[2019-04-16].

[13] 曾健清，王君，吴超. 基于频谱融合和柱面衍射的双图像非对称加密[J]. 光子学报：1-11.[2019-04-16].

[14] 梁锡坤，陶利民，胡斌. 一类广义混沌映射和矩阵非线性变换的图像混合加密[J]. 中国图象图形学报，2019，24(3)：325-333.

[15] 钟艳如，刘华役，孙希延，等. 基于 2D Chebyshev-Sine 映射的图像加密算法[J]. 浙江大学学报(理学版)，2019(2)：131-141，160.

[16] 拜亚萌，张燕玲，邓小鸿. 自适应分块的医学图像混沌加解密算法[J]. 计算机应用研究：1-5.[2019-04-16].

[17] 韩啸，熊礼治，蒋鹏程，等. 一种密文图像安全性评价方案[J]. 计算机应用与软件，2019，36(3)：148-153.

[18] 傅彬. 一种混沌的图像加密算法的研究[J]. 科技通报，2019，35(2)：70-75.

[19] 袁源，和红杰，陈帆. 减少相邻位平面间冗余度的加密图像可逆信息隐藏[J]. 中国图象图形学报，219，24(1)：13-22.

[20] 程宁，王茜娟. 基于混沌 Gyrator 变换与矩阵分解的光学图像加密算法[J]. 电子测量与仪器学报，2019，33(1)：191-202.

(上接第 495 页)

[3] LIU M J，CHEN J Z. Improved Linear Attacks on the Chinese Block Cipher Standard[J]. Journal of Computer Science and Technology，2014：197-207.

[4] 马猛，赵亚群，刘庆聪，等. SMS4 算法的多维零相关线性分析[J]. 密码学报，2015，2(5)：458-466.

[5] PIRET G，QUISQUATER J J. A differential fault attack technique against SPN structure，with application to the AES and KHAZAD[C]// C. D. Walter，ÇK. Koçc，and C. Paar，editors，Cryptographic Hardware and Embedded Systems CHES 2003，volume 2779 of Lecture Notes in Computer Science. Springer Verlag，2003：77-88.

[6] TUNSTALL M，MUKHOPADHYAY D. Differential fault analysis of the Advanced Encryption Standard using a single fault[J]. Cryptology ePrint Archive，Report 2009/575，2009.

[7] BIHAM E，SHAMIR A. Differential Fault Analysis of Secret-Key Cryptosystems[C]// Proceedings of the 17th AnnualInternational Cryptology Conference. Berlin，Germany：Springer，1997：513-525.

[8] RIVAIN M. Differential fault analysis on DES middle rounds[C]// International Workshop on Cryptograhic Hardware and Embedded Systems. Berlin：Springer，2009：457-469.

[9] HEMME L. A differential fault attack against early rounds of (Triple-)DES. [C]// International Workshop on Cryptograhic Hardware and Embedded Systems. Berlin：Springer，2004：254-267.

[10] MATSUI M. On correlation between the order of S-boxes and the strength of DES[C]// DeSantis，A. (ed.) Advances in Cryptology—EUROCRYPT ’94，Lecture Notes in Computer-Science. Berlin：Springer，1995：366-375.

[11] 张蕾，吴文玲. SMS4 密码算法的差分故障攻击[J]. 计算机学报，2006(9)：86-92.

[12] 荣雪芳，吴震，王敏，等. 基于随机故障注入的 SM4 差分故障攻击方法[J]. 计算机工程，2016，42(7)：129-133.

[13] 王敏，吴震，饶金涛，等. 针对 SM4 算法的约减轮故障攻击[J]. 通信学报，2016，37(S1)：98-103.

[14] 李玮. 若干分组密码算法的故障攻击研究[D]. 上海：上海交通大学，2009.

[15] 陶智. 若干对称密码算法的安全性分析[D]. 上海：东华大学，2015.

[16] ABHISHEK C，BODHISATWA M，DEBDEEP M. Combined side-channel and fault analysis attack on protected grain family of stream ciphers[OL]. http://eprint. iacr. org/2015/602. pdf，2015.

[17] REN Y，WANG A，WU L. Transient-steady effect attack on block ciphers[C]// Cryptographic Hardware and Embedded Systems(CHES). Saint Malo，France，2015：433-450.

[18] SIKHAR P，ABHISHEK C，DEBDEEP M. Fault tolerant infective countermeasure for AES[J]. Security，Privacy and Applied Cryptography Engineering，2015，935(4)：190-209.