计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210200138

持久故障攻击威胁性研究

王 舰[1,2] 陈 华[1] 匡晓云[3] 杨祎巍[3] 黄开天[3]
1 中国科学院软件研究所可信计算与信息保障实验室 北京 100190
2 中国科学院大学 北京 100049
3 南方电网科学研究院 广州 510663

摘 要 持久故障攻击是一种利用持久性故障及统计方法恢复密钥信息的强大攻击技术,可应用于分组密码查表实现的密钥恢复,其最大的优势在于仅需一次故障注入即可恢复密钥信息,并且持久故障攻击可以应用于检测技术、掩码技术等经典的分组密码防护实现。虽然如此,经典的故障攻击防护技术仍然提高了持久故障攻击难度,检测、感染技术都使得提取正确密钥所需的密文数量有了常数倍的提升,这对于实际场景中的攻击会造成阻碍。对S盒进行实时的健康性检测是一种防范持久故障攻击的有效手段,一旦检测到S盒被注入故障则不再进行后续加密。持久故障攻击充分利用了S盒的双射特性,故针对S盒的双射特性进行健康性检测是一种高效的防护方法,对于一个8比特的S盒,只需进行255次异或操作即可完成对S盒双射特性的检验,远高于SHA3等通用的校验方法。此外,激光传感器等非算法层面的防护也应受到重视。

关键词:持久故障攻击;分组密码;防护技术;健康性检验;双射
中图法分类号 TP309.7

Study on Threat of Persistent Fault Attack

WANG Jian[1,2],CHEN Hua[1],KUANG Xiao-yun[3],YANG Yi-wei[3] and HUANG Kai-tian[3]
1 TCA Laboratory,Institute of Software,Chinese Academy of Sciences,Beijing 100190,China
2 University of Chinese Academy of Sciences,Beijing 100049,China
3 Electric Power Research Institute,China Southern Power Grid,Guangzhou 510663,China

Abstract Persistent Fault Attack(PFA) is a powerful attack which relies on persistent fault and statistical analysis,it can be applied in extracting secret key of block cipher implementation based on lookup tables. The greatest advantage of PFA is that it can recover the secret key with only one fault injection,meanwhile,it can be applied in countermeasures on fault attack like detection,mask and so on. However,these countermeasures still can make the attack more difficult,key recovery on implementation with countermeasures based on detection and infection need several times cipher text,this will hinder actual attack. Built-in health test for S-box will be a good countermeasure for PFA,the cipher device will stop working once there is a fault injection. PFA relies on the bijective characteristic of the S-box in block cipher,therefore,testing the bijection characteristic of S-box is an effective method to get a health test result for S-box. Just 255 XOR operations will give a reliable health test result for S-box,it costs much less than a normal test method like SHA3. Furthermore,non-algorithmic countermeasures like laser sensor should attractive some attention.

Keywords Persistent fault attack,Block cipher,Countermeasures,Health test,Bijection

1 引言

Boneh等[1]在1996年基于模运算的代数性质使用故障注入技术实现了对RSA-CRT公钥密码系统的攻击,首次提出了故障攻击(FA)这一概念;随后,Biham等[2]在次年提出了差分故障攻击(DFA)技术,并利用该技术实现了对使用DES算法的密码系统的密钥提取;在此之后,出现了大量对差分故障攻击的相关研究,差分故障攻击被成功应用到使用ECC[3],AES[4]等加密算法的密码系统中。

经典的差分故障攻击技术往往需要对同一明文进行正确和故障两次加密,对攻击者的能力要求较高。2013年Fuhr等[5]提出的统计故障攻击是一种唯密文攻击方法,充分利用了故障注入导致的中间值的不均匀特性,通过统计手段恢复轮密钥的信息,解决了这一难题。2007年Clavier等[6]证明了对公开的密码算法进行不公开的修改并不能抵抗故障攻击,并且提出了无效故障攻击(IFA)概念,即利用某些故障注入时导致密文不发生变化的性质确定该处的中间值进而恢复密钥;无效故障攻击虽然思路新奇,但对于故障模型要求过高,而统计无效故障攻击(SIFA)[7]在无效故障攻击的基础上引入了统计思想,极大地弱化了攻击条件,是一种非常强大的攻击手段,统计无效故障攻击不仅能应用于传统的密码实现及防护,对掩码和故障防护的综合实现依然能够

基金项目:国家重点研发计划(2018YFB0904900,2018YFB0904901)
This work was supported by the National Key R&D Program of China(2018YFB0904900,2018YFB0904901).
通信作者:陈华(chenhua@iscas.ac.cn)

成功地进行攻击[8]。

2018 年 Zhang 等[9]提出的持久故障攻击（PFA）同样是一种基于统计手段的强大故障攻击方法，与之前的故障攻击手段不同的是，持久故障攻击利用的是持久性故障，只需一次故障注入即可恢复出完整密钥，并且可以应用在基于冗余检测的分组密码防护实现上。随后，2020 年 Zhang 等[10]利用激光注入技术在微控制器上实现了实际的持久故障攻击，进一步验证了其可行性。

持久故障攻击的威胁性较大，但是针对其威胁性以及实际的防护方法的研究目前还较少，本文从持久故障攻击的特性出发，以 AES 算法为例，深入研究了当前主流的分组密码防护实现对于持久故障攻击的抵抗能力，并依据其防护能力结合自身特性对各防护方法进行了新的归类，可为后续持久故障攻击防护方法的研究提供参考。此外，本文还提出了一种算法层面上的健康性检验方法，能够以较低成本防护持久故障攻击。

本文第 2 节介绍了本文所用到的背景知识；第 3 节评估了经典的防护方法对于持久故障攻击的抵抗能力；第 4 节提出了一种防护持久故障攻击的健康性检验方法；最后总结全文并展望未来。

2 背景

2.1 故障攻击防护方法

防护故障攻击通常从避免故障传播或消除故障注入产生的影响入手，传统的故障攻击防护方法主要有以下 3 类。

2.1.1 检测技术

冗余检测技术是一种经典的故障攻击防护方法，其基本思想是对一次加密操作多次执行，比较结果以检测是否发生故障注入。若检测到故障注入，则系统做出相应的反应，即不输出或输出全 0 等无意义的数据；若未检测到故障，则正常输出密文。本文主要涉及以下几种检测技术[11]。

Simpleduplication with Comparison（SDC）：如图 1 所示，SDC 的防护实现由两个加密模块构成，两个加密模块独立地对同一明文 P 执行加密操作，加密结束后对两个模块得到的密文 C 和 C' 进行比较，若 $C=C'$，则认为未发生故障注入；否则，认为有故障注入发生。

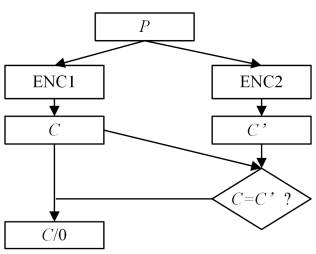


图 1 SDC 防护实现流程图

Fig. 1 Flowchart of SDC

Decryption Duplication with Comparison（DDC）：如图 2 所示，DDC 的防护实现由一个加密模块和一个解密模块构成，首先由加密模块对明文 P 进行正常加密得到密文 C，随后由解密模块对密文 C 进行解密得到解密后的结果 P'，若 $P=P'$，则认为未发生故障注入；否则，认为有故障注入发生。

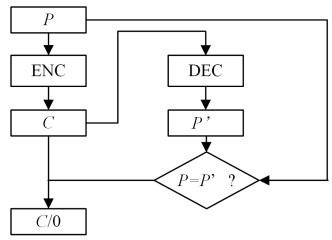


图 2 DDC 防护实现流程图

Fig. 2 Flowchart of DDC

Time Duplication with Comparison（TDC）：TDC 在原理上大致等同于 SDC，不同的是，SDC 采用空间冗余，而 TDC 采用时间冗余，即两次加密由一个加密模块先后完成，在一些研究中往往将二者等价，本文对二者进行区分的原因将在第 3 节进行说明。

2.1.2 随机化技术

随机化技术是本文根据对持久故障攻击的防护能力提出的故障攻击防护技术的新分类，包括感染技术以及 SDCR（SDC with randomness，即冗余计算检测到故障注入后输出随机数）技术，不同于检测技术致力于检测到故障注入后不再输出有意义的密文，随机化技术通过引入随机数的方式使得攻击者不能从注入故障后收集到的密文中获取任何有效信息。相较于检测技术，随机化技术的最大优势在于攻击者无法通过密文判断故障注入是否成功。

检测技术所依赖的条件判断有被攻击者跳过的可能，而感染技术则不存在该问题，因此感染技术是一种非常强大的故障攻击防护技术。但感染技术的实现多种多样，本文所使用的感染技术参考文献[12]中提出的防护方案，其描述见算法 1。

算法 1 感染技术[12]

输入：(P,K,R)

输出：C

1. C_0 = EN C_0(P,K)
2. C_1 = EN C_1(P,K)
3. temp = $C_0 \oplus C_1$
4. for each i∈[1,16] do
   temp[i] = temp[i]⊕R[i]
5. C = C_0⊕temp

对两路加密的结果进行异或，若未发生故障注入，则两路的输出结果相同，异或后得到临时值 $temp=0$；若发生故障注入，则 $temp\neq0$，随后利用随机数与 $temp$ 按字节乘进行感染后再与 $c[0]$异或，未发生故障的情况下，感染后的 $temp$ 依然是 0，不会改变 $c[0]$的值，而发生故障的情况下，$temp$ 中不为 0 的比特，即两路输出中不相同的比特，经过感染后会发生随机化和扩散，随后也会对 $c[0]$产生随机化的影响，使得攻击者无法获取与注入的故障有关的信息。

在检测技术中，当密码系统检测到故障注入后，除了不输出和输出全 0 这样的无意义数，还有一种策略是输出与密文等长的随机数，本文将该策略归类为随机化技术，并以 SDC 为例，研究该策略对于持久故障攻击的防护效果，下文中将这一防护方法简称为 SDCR。

2.1.3 掩码技术

掩码技术[13]最初用于防护能量、电磁等侧信道攻击，目

的是利用随机数消除中间值与密钥信息之间的相关性。掩码技术由于引入了随机性，也提高了故障攻击的难度。查表掩码是一种常见的掩码方式，常用于分组密码的软件防护实现。

一个基本的查表掩码的实现[14]大致如下：在每次加密开始前，首先使用随机数计算掩码版本的 S 盒，即 $S_m(x)=S(x\oplus m)$，相应地，轮函数也变为：

$$f(x)=(L(S_m(x\oplus m)\oplus m')\oplus k)\oplus L(m')$$

其中，S_m 表示掩码后的 S 盒，L 表示分组密码的线性层，m 表示随机的掩码值，在 d 阶掩码中 $m=m_0\oplus m_1\oplus\cdots\oplus m_{d-1}$。

2.2　持久故障攻击

持久故障攻击是 Zhang 等[9]于 2018 年提出的新型故障攻击方法，不同于传统的故障攻击技术多依赖于瞬时故障和永久性故障，利用差分性质恢复密钥信息，持久故障攻击依赖于只有在设备重启时才会消失的持久性故障，利用密文的统计特性恢复密钥信息。

持久故障攻击的基本思想是对分组密码的查表实现的 S 盒注入故障，使得其某一表项出现错误，进而导致密文中字节值的分布出现偏差。设 f 表示该分组密码的轮函数；L 表示其中的线性层；S 表示其中的非线性层，即 S 盒部分，S' 表示注入持久故障后的 S 盒；p 表示轮函数的输入；c 表示轮函数的输出，若该轮函数为末轮的轮函数，则 c 表示最终的密文输出。那么就有：

$$c=f(x)=L(S(x))\oplus k$$

AES 的非线性层为 8 比特 S 盒，且满足双射特性，若将 S 盒的某一表项 v 通过故障注入修改为 v^*，则对应的轮函数的输出也相应地变为 c^*，由于 S 盒的双射特性被修改，故 S 盒的输出中 v^* 出现的概率变为 $\frac{2}{256}$，而 v 出现的概率为 0。这样在密钥固定的情况下，加密足够多次数后，密文字节值分布会出现明显的统计偏差，如对于密文的第一字节 $c[0]$，由于该处对应的密钥第一字节 $k[0]$ 固定，相应地有 $c[0]=v\oplus k[0]$，$c^*[0]=v^*\oplus k[0]$，而由于前文提到的 v 和 v^* 存在统计偏差，则 $c[0]$ 和 $c^*[0]$ 也存在相应的统计偏差，即 $c[0]$ 出现的概率为 0，而 $c^*[0]$ 出现的概率为 $\frac{2}{256}$，这样在一定的加密次数后，就可以明显地从 256 个可能的字节值中区分出二者，又由于攻击者已知 S 盒的注入位置，即已知 v 值，故很容易根据出现概率为 0 的密文通过计算 $k[0]=c[0]\oplus v$ 求得单个字节的密钥值，重复这个过程即可逐字节恢复出末轮轮密钥，进而恢复出种子密钥。前文中为了便于理解忽略了分组密码中的线性层部分，实际上线性层不会影响该统计偏差，本文中所涉及的实验验证都是在完整的分组密码算法上进行的。

持久故障攻击共有 3 种密钥恢复策略[9]，本文中选用 $t_{\min}$ 策略，即 $c[0]$ 的可能值中仅存在一个出现频率为 0 的候选者时，我们即可确认该值即是目标 $c[0]$ 值。只有当 S' 中的 255 个值都被访问后才能确定该值，而需要多少次加密能够访问到全部 255 个值的问题可以归约到经典的概率问题——优惠券收集问题[15]，因此我们能够求得需要的加密次数 $N=255\times\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{255}\right)\approx 1561$。持久故障攻击能够应用于 SPN 结构的分组密码的查表实现，如 AES[9] 和 PRESENT[10]，在较为苛刻的场景下也可以应用于部分 Feistel 结构的分组密码，如 DES[9,16]；此外，持久故障攻击还可以应用于基于冗余检测[9]、掩码实现[14]等分组密码防护实现方案。

本文参考了持久故障攻击的经典故障模型，并结合当前实际的攻击能力，对攻击者的能力做出假设如下：

(1)对于一个查表实现的分组密码算法，攻击者能够利用激光注入技术在其 S 盒的某一表项注入故障，攻击者能够确定该表项的位置，但是不能确定故障注入导致的结果值，攻击者也不能对密码系统中的多处注入相同的故障；

(2)攻击者能够输入任意次数的明文，并收集相应得到的密文，其中输入的明文是随机分布的，攻击者不能有选择地输入明文。

2.3　激光注入技术

传统的故障注入技术包括电压扰动、外部时钟、温度、外部光源、电磁注入等。外部光源故障注入依赖于半导体对于光粒子的敏感性。由于光电效应，强光持续照射在开封装的芯片上，会在芯片内部产生电流，进而改变芯片内部存储介质(如 RAM)中存储的临时值，造成计算过程发生故障[11]。外部光源注入技术多种多样，包括普通强光、激光、x 光等，其中，激光注入技术有着能够准确地影响局部目标区域的优势，是当前最为强大的故障注入技术。

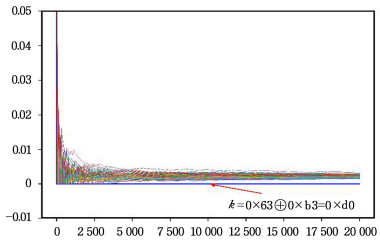
密码算法的故障攻击与防护一直是学界的研究热点，只有对当前的故障注入能力有一个准确的认识，才能确保密码系统防护设计的安全性。在 2015 年，Brummer 等[17]通过实验验证了激光注入能够成功改变 90nm 工艺和 45nm 工艺下的 FPGA 芯片中寄存器中的临时值。但有目的地准确注入多处故障实现起来是十分困难的，所以本文中将攻击者的能力限定在可以准确地对 S 盒中某一表项注入错误，但不具备对 S 盒的多个目标表项注入指定故障或者是对冗余轮的相同位置注入相同故障的能力。

3　经典防护方法对于持久故障攻击的抵抗能力分析

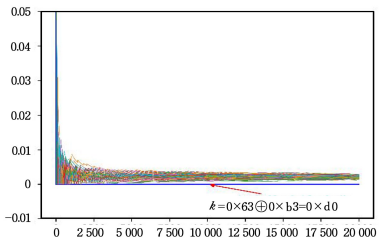
3.1　检测技术

持久故障攻击能够对基于检测技术的分组密码防护实现进行成功的密钥恢复[9]。当面对一个基于检测技术的分组密码防护实现时，攻击者能够轻易地区分每次加密的密文的正确与否(故障密文为全 0 或不输出)。一次加密过程若没有访问到故障表项，则两路加密结果相同，输出正确密文；若加密过程中访问到了故障表项，那么攻击者可以舍弃掉这次加密的结果。经过足够多次加密后，最终攻击者得到的密文中 $c[0]$ 的概率仍然是 0，攻击者仍然可以直接使用 $t_{\min}$ 策略恢复 k 值。

显然，该方法较于一般的持久故障攻击是需要付出额外代价的。以 SDC 策略为例，对于该防护实现的一次加密，只有当密钥拓展的 $10*4$ 以及轮函数中的 $16*10$ 共 200 次的 S 盒操作都没有访问到被修改的表项时，才能得到正确的密文输出，其概率为 $\left(1-\frac{1}{256}\right)^{200}\approx 0.45$。故对于基于 SDC 策略的实现而言，若攻击者试图获得与无防护实现相同的效果，需要 $\frac{1}{0.45}\approx 2.18$ 倍次数的加密，如图 3(a)所示。相似地，对于 DDC 策略的分组密码密码实现，只有当加密步骤的 200 次 S 盒操作都没有访问到故障表项时才能够正确输出密文，故 DDC 策略对于持久故障攻击的防护能力等同于 SDC，如图 3(b)所示。



(a)PFA oncountermeasure based on SDC



(b)PFA oncountermeasure based on DDC

图 3 检测技术对于持久故障攻击的防护能力

Fig. 3 Resistance of countermeasure basedon detection to PFA

与前两者不同的是，对于时间冗余(TDC)的检测技术来说，由于冗余加密使用的是同一个加密模块，而持久故障攻击的故障效果在时间上持续存在，故冗余加密得到的结果始终与正常加密得到的结果相同，因此时间冗余对于持久故障攻击不具备额外的防护效果，所以，在密码系统的实现时，若考虑到持久故障攻击的防护，那么时间冗余不应该在考虑范围内。

3.2 随机化技术

相较于检测技术，对于持久故障攻击而言，随机化技术有两点不同：1)攻击者无法区分当前输出的密文的有效性；2)如果一次加密过程中访问到了 S 盒的故障表项，导致密文会有随机的输出，即 $c[0]$不再有唯一出现概率为 0 的值，攻击者不能以该条件确定某一 $c[0]=v\oplus k[0]$，进而确定 $k[0]$值。

本文所提到的感染技术主要包括两类：SDCR 和感染技术(Infection)。前者是检测到故障注入后输出随机数作为本次加密的密文，后者是对故障对密文产生影响的部分使用随机数进行感染。由于雪崩效应的存在，中间值某一比特的改变在两轮加密后就会导致接近半数的比特发生变化[18]，所以对一次访问了 S 盒故障表项的加密，其最终密文的某一字节有非常大的概率是会发生变化的。如图 4 所示，在 100 次实验中，每次对 10000 条随机明文进行加密，每次访问到故障 S 盒后 $c[0]$未被感染的概率基本分布在 0.12～0.145，故对于一个字节而言，在当次加密访问到故障表项后该字节被感染的概率约为 0.87。因此，对于持久故障攻击而言，对感染技术成功攻击和对 SDCR 成功攻击需要增加的密文数量是相近的，可以视作同一强度的防护。

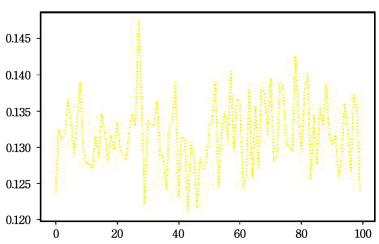
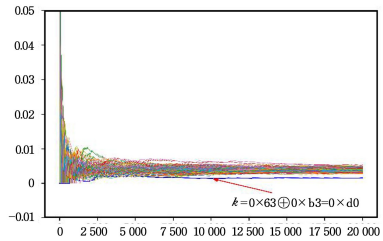


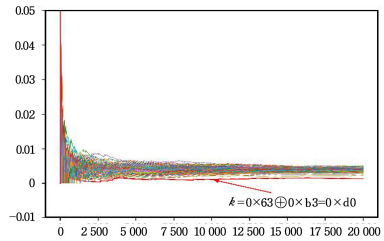
图 4 实验结果

Fig. 4 Experimental results

由于二者防护强度相近，本文只对基于 SDRC 的防护实现进行分析。这里依然以密文的第一字节 $c[0]$为例，当一次加密没有访问到故障项，即输出为正确密文时，$c[0]$中的密文是分布不均的，与前文中情况相同，约经过 1561 次没有访问到故障项的加密后，会出现唯一频率为 0 的值，可以与其他密文的字节值区分开来；而当访问到故障项时，$c[0]$的值为随机数，即在 0～255 之间均匀分布，每个值出现的概率均为 $\frac{1}{256}$。综上，两种情况下的密文的字节值分布叠加起来，偏差依然是存在的，如图 5 所示。不同的是，其不能像检测技术一样以唯一为 0 的值作为确定性的衡量标准，故需要引入阈值方法进行判断[9]，密钥值所需要的密文数量取决于阈值的选择。



(a)PFA on countermeasure based on Infection



(b)PFA on countermeasure based on SDCR

图 5 随机化技术对于持久故障攻击的防护能力

Fig. 5 Resistance of countermeasures based on randomness to PFA

3.3 掩码技术

持久故障攻击对于分组密码查表掩码实现的有效性已经得到了验证[14]。从 2.1 节可知，查表掩码实现通常会在加密开始前计算一个掩码版本的 S 盒 S_m 且 $S_m(x\oplus m)=S(x)$，若在掩码操作开始前，对 S 盒的 $S(x)=v$ 项注入一次持久故障，使得 $S'(x)=v^*$，那么相应地，$S_m(x\oplus m)=v^*$，如此，在掩码后的 S 盒中，v^* 作为 S 盒的输出值的概率翻倍，变为 $\frac{2}{256}$，原本的正确输出 v 在 S 盒的输出中出现的概率变为 0。此外，若 $S_m(x\oplus m)=S'(x)$，掩码实现的末轮轮函数可看作 $c=(L(S'(x)\oplus m')\oplus k)\oplus L(m')$，即 $c=L(S'(x))\oplus k$。这样一来，利用持久故障攻击恢复掩码实现的分组密码的密钥的难度就等同于恢复无防护的分组密码实现的密钥。此外，即便是高阶掩码，也可以看作一个 m 的各个分量，不会增加攻击难度。本文基于 Byte-Masked[19-20] 对该结论进行了验证，结果如图 6 所示。

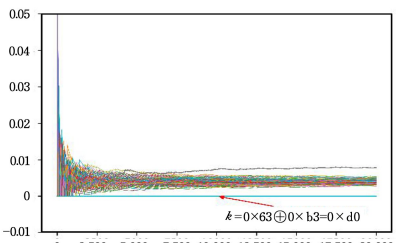


图 6 掩码技术对于持久故障攻击的防护能力

Fig. 6 Resistance of countermeasure based on mask to PFA

总而言之，在持久故障攻击的威胁下，对于一个分组密码的查表实现，传统的故障攻击防护方法并不能保证其绝对安全，但大多数都能够对持久故障攻击造成一定阻碍。就防护持久故障攻击而言，检测技术以空间冗余为优，时间冗余的检测技术不能给持久故障攻击带来新的困难，只是徒增成本；感染技术以及 SDCR 技术给持久故障攻击带来了相近的难度提升，故本文将这两者归为随机化技术；掩码技术虽然给一般的故障攻击造成了一定阻碍，但是查表掩码实现并没有给持久故障攻击带来难度上的提升。

表 1　经典防护方法对于持久故障攻击的抵抗能力

Table 1　Summary of resistance of classical countermeasures for PFA

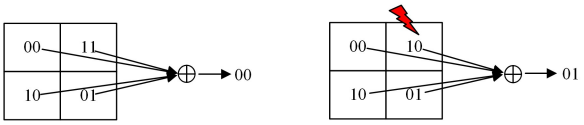
防护方法	防护效果
检测技术	攻击 SDC 和 DDC 技术的实现相较于无防护的实现需要 2.18 倍的密文数量，TDC 技术的实现未增加攻击难度
随机化技术	相较于无防护的实现需要多于 2.18 倍的密文数量，具体的密文数量由阈值选择决定
掩码技术	未增加攻击难度

4　持久故障攻击防护方法

当前持久故障攻击的强大能力已经得到了证实，防护该攻击主要应当从以下几个角度入手：1）避免攻击者获取正确或错误的密文，如直接在加密开始前对 S 盒进行校验，存在故障时不再进行加密；2）从实际攻击的角度，杜绝故障注入。本文基于以上认识，提出了一种高效的健康性校验方法，并从密码系统设计者的角度提出了一些防护建议。

持久故障攻击充分利用了分组密码 S 盒的双射特性，通过修改其双射特性造成密文的分布不均，进而通过统计手段恢复密钥信息。在加密开始前对 S 盒进行健康性检验是一种能够抵御持久故障攻击的方法[9]，但当前的健康性检验往往依赖于哈希函数等通用方法，对于分组密码系统而言耗时较大，得不偿失。本节提出一种针对持久故障攻击的专用健康性检验方法，能够以低成本高效地对分组密码的 S 盒进行健康性检验以抵御持久故障攻击。

该方法的主要思想如下，由于分组密码 S 盒的双射特性，S 盒中的2^n个元素从全 0 到全 1 均匀分布，故若将 S 盒的每个元素逐个异或后得到的最终结果会是 0。但若 S 盒中的某一表项被修改，则异或结果不再是 0。这里以一个 $n=2$ 的 S 盒为例，如图 7(a)所示，当未发生故障注入时，S 盒的各表项两两异或后计算结果为 0，若对 S 盒的某一表项注入故障，如图 7(b)所示，则计算结果不为 0，认为存在故障注入，不再进行加密操作。我们利用这一性质，在加密开始前对 S 盒进行校验，可以有效地避免由于持久故障注入带来的密文统计偏差，最重要的是，该方法只需要执行 255 次异或操作，其效率要远高于当前最新的标准哈希算法 SHA3[21]。



(a)无故障注入，通过检验　(b)故障注入，未通过检验

图 7　防护方法示意图

Fig. 7　Schematic diagram of our countermeasure

除了从算法层面对持久故障攻击进行方法，密码系统的设计人员还应当考虑其他层面的防护。首先，持久故障攻击对攻击者要求较高，目前实践中主要依靠激光注入故障实现，那么对于一个硬件密码系统而言，在芯片中加入激光传感器[22]会是一个有效的防护方法，在检测到激光注入之后便销毁系统中的私密信息不再进行计算或者直接重启系统；此外，持久故障攻击目前只能针对分组密码的查表实现，在可选的情况下选择分组密码的复合域实现也不失为一种备选方案；设计者还可以从器件材料等方面进行考虑，例如激光注入需要对芯片进行开封装，若提高开封装的难度和成本同样可以对攻击造成/阻碍。

结束语　本文在符合实际攻击能力的故障模型下，对持久故障攻击的攻击能力以及如何防护持久故障攻击进行了细致的研究，当前持久故障攻击能够在单故障注入的条件下实现对 SPN 结构的分组密码的密钥恢复，分组密码的检测、随机化、掩码等防护技术的实现虽然依然存在持久故障攻击风险，但也一定程度上提高了攻击难度，如对一个基于检测技术的分组密码防护实现的密钥恢复所需要的密文数量是一个无防护的分组密码实现的 2.18 倍。最后，本文针对持久故障攻击的特性，提出了一种利用分组密码 S 盒双射特性的持久故障攻击防护方法，能够以可接受的成本对分组密码的 S 盒进行健康性检验，有效防护持久故障攻击。

目前对持久故障攻击的攻击和防护的研究都还较少，尚未有使用持久故障攻击对 SM4 等 Feistel 结构的分组密码进行实际攻击的方法；此外，不会额外增加成本，能够适用于持久故障攻击和差分故障攻击两者的防护方法也有待提出。

参 考 文 献

[1] BONEH D, DEMILLO R A, LIPTON R J. On the importance of checking cryptographic protocols for faults[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 1997: 37-51.

[2] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[C]// Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 1997: 513-525.

[3] BIEHL I, MEYER B, MÜLLER V. Differential fault attacks on elliptic curve cryptosystems[C]// Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2000: 131-146.

[4] DUSART P, LETOURNEUX G, VIVOLO O. Differential fault analysis on AES[C]// International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2003: 293-306.

[5] FUHR T, JAULMES E, LOMNÉ V, et al. Fault attacks on AES with faulty ciphertexts only[C]// 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography. IEEE, 2013: 108-118.

[6] CLAVIER C. Secret external encodings do not prevent transient fault analysis[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2007: 181-194.

[7] CLAVIER D, EICHLSEDER M, KORAK T, et al. SIFA: exploiting ineffective fault inductions on symmetric cryptography[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018: 547-572.

（下转第 539 页）

[17] THAKKAR P, NATHAN S, VISHWANATHAN B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform [C]// 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). IEEE, 2018: 1-13.
[18] BENHAMOUDA F, HALEVI S, HALEVI T. Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation [C]// 2018 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2018: 1-7.
[19] AMPEL B, PATTON M, CHEN H. Performance Modeling of Hyperledger Sawtooth Blockchain[C]// 2019 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2019: 59-61.

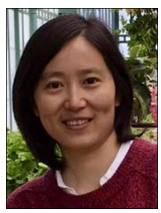
LING Fei, born in 1993, postgraduate. His main research interests include blockchian and big data.

CHEN Shi-ping, born in 1964, Ph. D, professor, Ph. D supervisor. His main research interests include cyber security and computer network communication.

（上接第 527 页）

[8] DOBRAUNIG C, EICHLSEDER M, GROβ H, et al. Statistical ineffective fault attacks on masked AES with fault countermeasures[C]// International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2018: 315-342.
[9] ZHANG F, LOU X, ZHAO X, et al. Persistent fault analysis on block ciphers[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3): 150-172.
[10] ZHANG F, ZHANG Y, JIANG H, et al. Persistent fault attack in practice[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(2): 172-195.
[11] BAR-EL H, CHOUKRI H, NACCACHE D, et al. The sorcerer's apprentice guide to fault attacks[J]. Proceedings of the IEEE, 2006, 94(2): 370-382.
[12] LOMNÉ V, ROCHE T, THILLARD A. On the need of randomness in fault attack countermeasures-application to AES[C]// 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography. IEEE, 2012: 85-94.
[13] MESSERGES T S. Securing the AES finalists against power analysis attacks[C]// International Workshop on Fast Software Encryption. Berlin, Heidelberg: Springer, 2000: 150-164.
[14] PAN J, ZHANG F, REN K, et al. One fault is all it needs: breaking higher-order masking with persistent fault analysis [C]// 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2019: 1-6.
[15] BLOM G, HOLST L, SANDELL D. Problems and Snapshots from the World of Probability[M]. Springer Science & Business Media, 1993.
[16] CAFORIO A, BANIK S. A study of persistent fault analysis [C]// International Conference on Security, Privacy, and Applied Cryptography Engineering. Cham: Springer, 2019: 13-33.
[17] SELMKE B, BRUMMER S, HEYSZL J, et al. Precise laser fault injections into 90 nm and 45 nm sram-cells[C]// International Conference on Smart Card Research and Advanced Applications. Cham: Springer, 2015: 193-205.
[18] STALLINGS W. Cryptography and Network Security: Principles and Practice[M]. Beijing: Publishing House of Electronics Industry, 2017: 153-179.
[19] MANGARD S, OSWALD E, POPP T. Power Analysis Attacks [M]. Beijing: Science Press, 2010: 181-185.
[20] YAO Y, YANG M, PATRICK C, et al. Fault-assisted side-channel analysis of masked implementations[C]// 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2018: 57-64.
[21] DWORKIN M J. SHA-3 standard: Permutation-based hash and extendable-output functions: Federal Inf. Process. Stds. (NIST FIPS) - 202 [S]. NIST: 2015.
[22] MATSUDA K, FUJII T, SHOJI N, et al. A 286 f 2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor[J]. IEEE Journal of Solid-State Circuits, 2018, 53(11): 3174-3182.

WANG Jian, born in 1998, postgraduate. His main research interests include side-channel analysis and countermeasures.



CHEN Hua, born in 1976, Ph.D, senior engineer, Ph.D supervisor. Her main research interests include side-channel analysis and countermeasures.