旁路攻击与故障攻击的关联性研究综述

吴童, 周大伟, 欧庆于, 褚潍禹

引用本文

吴童, 周大伟, 欧庆于, 褚潍禹. 旁路攻击与故障攻击的关联性研究综述[J]. 计算机科学, 2023, 50(11A): 220700223-7.

WU Tong, ZHOU Dawei, OU Qingyu, CHU Weiyu. Review of Relationship Between Side-channel Attacks and Fault Attacks [J]. Computer Science, 2023, 50(11A): 220700223-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220700223

旁路攻击与故障攻击的关联性研究综述

吴 童 周大伟 欧庆于 褚潍禹
海军工程大学信息安全系 武汉 430000

摘 要 旁路攻击与故障攻击是当前应用较广泛的攻击方式。文中分析比对了其泄漏模型,并从算法层面和物理层面阐述了二者本质上的一致性。最后,从如何构建统一的物理泄漏函数模型,提出统一的物理安全测评标准,设计通用防御策略等角度分析了当前研究热点,这对从二者的关联性角度出发继续做好深入研究具有重要意义。

关键词:旁路攻击;故障攻击;泄漏模型;安全测评;防御策略
中图法分类号 TP309.1

Review of Relationship Between Side-channel Attacks and Fault Attacks

WU Tong,ZHOU Dawei,OU Qingyu and CHU Weiyu
Department of Information Security,Naval University of Engineering,Wuhan 430000,China

Abstract Side-channel attacks and fault attacks are widely used at present. This paper analyzes and compares the leakage models of the above two attack methods,and expounds the inherent consistency from algorithm level and physical level. Finally,the current research hotspots such as how to build a unified physical leakage function model,propose a unified physical security evaluation standard,and design a general protection strategy are analyzed,which are of great significance for further research from the perspective of the relationship between the two.

Keywords Side-channel attacks,Fault attacks,Leakage model,Safety evaluation,Defense strategy

1 引言

对安全嵌入式系统的物理攻击主要分为旁路攻击(Side-Channel Attacks,SCA)和故障攻击(Fault Attacks,FA)两大类,前者通过测量目标设备运行过程中泄漏的信息量恢复密钥等敏感信息,后者注入故障以干扰系统正常运行并通过统计分析等方法获取密钥等敏感信息。上述两类物理攻击易于实施且成本较低,应用广泛,因此除了关注算法本身的安全性外,系统抗旁路攻击和故障攻击的能力也应得到提高。

本文主要从旁路攻击与故障攻击的原理、泄漏模型、二者的关联性、当前研究前沿热点等几个方面进行综述。研究结果对理解旁路攻击与故障攻击的内在联系以及构建统一的物理泄漏模型、统一的物理安全测评标准和设计通用的防御策略具有重要意义。

2 旁路攻击与故障攻击的原理

现场可编辑逻辑门阵列(Field Programmable Gate Array,FPGA)具有低成本、高性能且可快速实现的优点,在数字和混合逻辑中被广泛应用;高级加密标准(Advanced Encryption Standard,AES)是当前使用较广的加密标准,本文基于FPGA平台对AES算法进行旁路攻击和故障攻击分析。

2.1 旁路攻击的原理

旁路攻击收集目标设备运行时侧信道泄漏的相关信息,如功耗[1]、运行时间[2]、电磁泄漏[3]等。不同侧信道的数据测量方式存在差异,但统计分析的方式相似,同时由于功耗攻击方法多样且应用广泛,因此本文选择功耗侧信道作为示例开展研究,探索旁路攻击与故障攻击的关联。

功耗攻击通过寻找功耗或信号的其他电磁泄漏信息与目标设备正在进行的操作、正在处理的数据之间的关系,分析并恢复密钥等信息。其攻击方法种类多样,有简单功耗分析[2](Simple Power Analysis,SPA)、差分功耗分析[1](Differential Power Analysis,DPA)、相关功耗分析[4](Correlation Power Analysis,CPA)、互信息分析[5](Mutual Information Analysis,MIA)和模板攻击[6](Template Attack,TA)等。

在目标设备中,执行加解密操作在硬件层面为晶体管的通断电切换,即为高低电平的转换。目前大部分的微处理器、微控制器及其他数字电路都使用CMOS技术,可通过CMOS电路的功耗分析相应密码设备的功耗。CMOS电路的功耗由静态功耗和动态功耗组成:静态功耗由晶体管的漏电流引起,取决于电路的设计;动态功耗由晶体管状态的切换引起,取决于正在进行的操作和正在处理的数据。

CMOS反相器在状态0和状态1的翻转过程中会出现一个组合MOS管同时导通的瞬间,产生瞬时短路电流。处理不同汉明重量的数据时,CMOS电路中电容的放电情况不同,产生的功耗不同,可通过功耗判断出CMOS电路状态,分析算法中相应操作及处理的数据的特征。

静态功耗基本恒定,而动态功耗随着操作和处理的数据变化,因此总功耗的变化仅由动态功耗引起,取决于加密协议

基金项目:国家自然科学基金(11202239)
This work was supported by the National Natural Science Foundation of China(11202239).
通信作者:吴童(2795237341@qq.com)

和具体算法的实现。

2.2 故障攻击的原理

故障攻击通常在目标环境中引入故障，通过电磁攻击[7]、光注入攻击[8]、电压和时钟毛刺[9]及温度变化[10]等手段，改变目标设备的运行状态，使其产生可控的故障。分析故障信息，以减少未知密钥的熵。

Yang 等[11]提出故障敏感度分析(Fault Sensitivity Analysis，FSA)，不断改变注入故障的强度以观察产生错误输出的阈值，即故障敏感度，通过分析故障敏感度和处理的相关数据之间的关系恢复密钥。Biham 等[12]提出差分故障分析(Differential Fault Analysis，DFA)，逐块对密钥进行破解，通过分析错误密文缩小密钥空间，再对明密文对穷举搜索以定位正确的密钥。Moradi 等[13]提出基于碰撞的故障敏感度分析(Collision FSA，CFSA)，通过提取错误密文字节的分布或组合电路的定时特性，尝试找到碰撞，以恢复相应密钥。Nahid 等[14]提出差分故障强度分析(Differential Fault Intensity Analysis，DFIA)，故障强度的微小变化只会在正确的密钥假设下导致输出密文错误的微小变化，将故障强度和故障值作为统计分析的观察值，计算错误密文的“错误值”的变化，从而恢复出密钥。Nahid 等[14]提出盲故障分析(Blind Fault Analysis，BFA)，计算连续两轮中间值的汉明权重以恢复密钥。该方法无需获得密文甚至明文。Christoph 等[15-16]提出统计无效故障分析(Statistical Ineffective Fault Analysis，SIFA)，攻击者统计分析注入后对加密操作无影响的“无效故障”。Keyvan 等[17-18]提出故障强度图分析(Fault Intensity Map Analysis，FIMA)，并使用神经网络密钥识别器(FIMA-NN)对密钥排序，将正确密文的偏差分布与数据分布随故障强度的变化相结合，以减少恢复密钥所需的故障数量。Sayandeep 等[19]提出故障模板攻击(Fault Template Attacks，FTA)，构建故障注入后的模板并与目标设备的测量值进行比较以恢复密钥。Zhang 等[20]提出了持续故障攻击(Persistent Fault Analysis，PFA)，其故障模型假设故障是持久性的，可能持续到设备重新启动。该攻击可在注入单字节故障情况下恢复密钥，并能够抵御经典 FA 对策及高阶屏蔽 S 盒[21]。Liu 等[22]提出了差分错误率攻击(Differential Error Rate Analysis，DERA)，将不同信号间误码率的固有偏差作为密钥识别器设计的基础，时间和空间攻击复杂度更低。Wang 等[23]提出了相关故障攻击(Correlation Fault Attack，CFA)，免去了耗时的故障模板和训练的过程，仅需少量正确、故障密文对即可成功恢复密钥。

故障攻击使密码设备内部元件在操作期间的特定时钟周期内失效，在硬件实现中即为电路运行过程中破坏寄存器或触发器的数据。攻击者通常通过监测电路的功耗变化情况来确定故障注入时机或控制系统的输入以触发时钟。攻击者可根据系统中已知的加密算法推断出故障传播路径，并对其进行跟踪，以恢复密钥。

基于 FPGA 平台对 AES 算法进行故障攻击时，通常在 FPGA 板和电源之间串联一个小电阻，通过示波器对功率轨迹进行采样和记录。结合算法特性，在特定时钟周期改变电路频率再恢复正常以执行故障注入，使得数据发生误读，操作结果产生逻辑错误。例如，在 AES 第 8 轮加密开始时注入 1 个字节的故障，结合正确与故障输出的差分 $C\oplus C'=\Delta C$，穷举搜索第 10 轮密钥 K_{10} 的 4 个字节，计算目标状态(第 9 轮加密列混合之前的状态)下的 4 个字节的差分。同时，由注入态(第 8 轮加密开始前的状态)的差分 $I\oplus I'=\Delta I$ 也可计算出目标态的差分。将 K_{10} 的 16 个字节分为 4 组，通过 DFA 分别搜索，其密钥空间为 $2^{32}\times 4=2^{34}$。

3 泄漏模型

泄漏模型(Leakage Model)描述了密码算法运行过程中状态变化与泄漏信息之间的关系，用于模拟真实的泄漏，预评估芯片的安全性等。按泄漏函数，可划分为单比特泄漏模型、部分比特泄漏模型、汉明重量模型、汉明距离模型、碰撞泄漏模型、故障泄漏模型等。

3.1 功耗攻击的泄漏模型

功耗攻击主要分为非刻画攻击(Non-profiled Attacks)和刻画攻击(Profiled Attacks)。非刻画攻击主要有比特模型、汉明重量模型、汉明距离模型和转换距离模型等泄漏模型，刻画攻击有高斯模型等泄漏模型。例如，DPA 使用了比特模型，CPA 使用了汉明模型，而高斯模型采用了均值和方差，描述更为准确。

密码芯片在执行加解密相关操作时，其功耗与处理的数据类型及数据量直接相关，在逻辑门电路中表现为 CMOS 门电路的充放电次数，在寄存器中表现为状态 0 与 1 的翻转次数，在操作数据中表现为原始数据与结果数据的汉明距离。

功耗攻击的模型主要有汉明重量模型和汉明距离模型。

(1)汉明重量模型

汉明重量模型(Hamming Weight，HW)，计算寄存器中某时刻所存储数据的 1 的个数。一个 k 位二进制数据 $V=(v_{k-1}\cdots v_1 v_0)$ 的汉明重量可表示为：

$$HW(V)=\sum_{0}^{k-1} v_i \tag{1}$$

该模型只能考虑电路当前状态，较适合静态功耗分析，可假设当前电路静态漏电流与此时数据比特的个数成正比。

2)汉明距离模型

汉明距离模型(Hamming Distance，HD)，计算寄存器在某特定时间段内 0 到 1 转换和 1 到 0 转换的总数。该模型需遵守以下假设：0 到 1 的转换和 1 到 0 的转换具有相同的功耗，0 到 0 的转换和 1 到 1 的转换对功耗有相同的影响。V_0 表示寄存器在初始时刻的值，V_1 表示变化之后的值，则两者之间的汉明距离可表示为：

$$HD(V_0,V_1)=HW(V_0\oplus V_1) \tag{2}$$

该模型较适合动态功耗分析，尤其是攻击时序电路中的寄存器或微控制器的总线时，用电平转换的总数描述电路动态功耗的均值。寄存器由时钟信号驱动，且每个时钟周期内数据仅能改变一次，因此可用连续时钟周期内寄存器存储数据的汉明距离来评估寄存器的功耗；数据总线的负载电容通常很大，且总线一般由时序元件直接驱动，不会产生毛刺，因此可认为其动态功耗正比于 $HD(V_0,V_1)$。

实际上，0 到 1 的转换和 1 到 0 的转换的功耗差别微小，因此一般优先选用 HD 模型。

汉明重量模型实现较简单，假设中间状态的原始值为零字符串来预测功率；而汉明距离模型消除了零串假设，并通过基于先前状态预测功率生成更准确的功率估计。在实际操作中，汉明距离模型较汉明重量模型功能更为强大，可在给定

数量的功率轨迹中检索到更多的子密钥[24]。

3.2　故障攻击的泄漏模型

(1)故障泄漏模型

攻击者通过干扰密码设备的正常运行使之产生故障输出，在此基础上利用故障的传播特性，结合相关算法进行密钥恢复。通常从信息论角度出发，以信息量、互信息量、信息熵等构建泄漏函数。

第一类是比特翻转模型。假设可以控制单个比特的值，如将密钥中特定位置为0，若密文正确则该位值为0，否则为1。该模型执行难度大，需要对时间和电路精准控制。第二类是字节翻转模型。在单个字节中(随机)更改一个或多个比特。该模型更为灵活，对手完全控制时间，但仅部分控制位置，因此无法准确预测新的错误值。

Piret 等[25]提出 Piret 故障模型，关注故障注入态下 ΔI 的信息量，$\Delta I=I\oplus I'$，其中 I 表示正常运算下的计算中间值，I'表示故障注入后的计算中间值。在 AES-128 算法中，两个128比特数据的差值有 255×16 种可能性，255 表示 255 个可能的值，16 表示可能的故障位置。故障注入态下的 ΔI 可提供的密钥相关的信息量为 $-\log_2\frac{1}{2^{128}}-\left(-\log_2\frac{1}{255\times16}\right)=116$ bits。基于正确密文和故障密文对(C,C')，AES-128 的密钥空间可被缩小至 2^{40}，可获得 $128-40=88$ bits 密钥相关的信息量，在缩小后的密钥空间中进行穷举搜索即可。

文献[26]分析 AES S 盒中连续两个时钟周期内信号转换引起的信息量变化以恢复密钥。$I_p\in[0,\cdots,255]$表示前一个时钟周期的 S 盒输入，$I_c\in[0,\cdots,255]$ 表示当前时钟周期的 S 盒输入，$I_c\oplus I_p$ 表示两个周期输入的差值。测量故障敏感度(Fault Sensitivity，FS)时，单独测量每个 S 盒的泄漏值，以 AES 第 9 轮和第 10 轮的输入 I_9，I_{10} 分别对应 I_p，I_c 构造 FS 泄漏曲线。该研究在两个不同的 FPGA 平台上测量分析并对比 I_c，I_p，$I_c\oplus I_p$ 这 3 个维度泄漏的信息量，选取泄漏量最大的维度作为泄漏函数。

文献[5]中假设泄漏函数为 $\hat{L}$，由寄存器状态的转换决定，计算泄漏量的假设值和测量值之间的互信息量 $\tilde{I}(L_{\hat{k}}^{\wedge},O(t))$。其中 $L_{\hat{k}}^{\wedge}$ 为在猜测密钥 $\hat{k}$ 下通过泄漏函数计算出的假设值，$O(t)$为 t 时刻的测量值。泄漏模型使用 HD 或 HW 模型，互信息量最大值对应的猜测密钥 $\hat{k}$ 即为正确的密钥。

(2)故障敏感信息泄漏模型

Yang 等[11]提出基于故障信息的泄漏模型，泄漏函数为：

$$f_{F_g^C}=HW(InvSbox(CT[i]\oplus K_g)) \tag{3}$$

并通过遍历密文 $CT[i]$和猜测密钥 K_g 恢复故障注入强度：

$$F_g^C[i]=f_{F_g^C}(CT[i],K_g) \tag{4}$$

计算相应的故障注入强度与实际故障注入强度的相关性：

$$Cor[K_g]=\rho(F^C,F_g^C) \tag{5}$$

相关性最大时对应的猜测密钥即为正确的密钥。

Ghalaty 等[14]用被影响的故障位的数量构建泄漏函数，攻击者可通过控制故障强度来增加或减少故障位数量。

(3)故障概率泄漏模型

Spruty 等[27]提出故障关联性分析(Fault Correlation Analysis，FCA)，将功耗曲线转换成故障概率曲线，并提出两种泄漏模型。通过在与操作相关的同一时间点重复注入故障并观察各类型结果的概率，得到给定时间点各类型的故障概率；在不同的时间点重复此过程，得到整个操作过程的故障概率曲线。故障结果分为成功、静音、重启、损坏、其他 5 类，并据此提出两种泄漏模型：基于成功的模型(成功输出与其他)和基于静音的模型(故障、成功输出与其他)，二者本质上都是基于 HW 的 CPA。

4　功耗攻击与故障攻击的关联性

4.1　基于算法的关联性分析

Yang 等[26]以 AES 的 S 盒为目标，从算法层面研究了故障攻击和功耗攻击之间的关联。该研究基于 FPGA 实验，构建了故障敏感度和功耗的泄漏函数，并证明两者存在高度相关性，使用 FS 的配置文件作为功耗攻击的泄漏模型成功实现了密钥恢复。这两个侧信道在不同维度上泄漏的信息量分布不同，在某些维度二者可以共享泄漏模型，但攻击效率不同。同时，由于 FS 测量易于精确到字节级或比特级，且零值攻击和碰撞攻击在 FSA 中效果更为明显，FSA 可作为一种评估工具，以较低的数据复杂度发现一阶泄漏。

故障敏感度分析(FSA)是一种基于故障注入的主动攻击，但与功耗攻击更为相似。Yang 等[11]指出，FS 提供了与关键路径延迟(Critical Path Delay，CPD)的相关信息，CPD 与被处理的数据相关，因此 FS 泄漏了故障发生时正在处理的数据的信息。FSA 中使用的泄漏模型取决于加密组件的具体实现，如 AES 中的 S 盒与旁路攻击的建模方式类似，而非 DFA 等故障攻击方式更注重底层算法的分析攻击。

Jean-Luc 等[28]提出了基于相关性的二阶定时攻击(2O-TA)，并将其与二阶功耗攻击(2O-CPA)进行了比较。实验[28]表明，与 2O-CPA 相比，2O-TA 的侵入性较小，成本较低，速度更快。

Roche 等[29]提出将一阶旁路攻击与故障攻击相结合，以击败抗故障注入和屏蔽 AES 实现。此方法大大减少了对故障注入位置的约束，且即使攻击者能够获得旁路泄漏的错误密文，故障注入攻击仍能很好地工作，此攻击可以扩展到任何 SPN 结构。

文献[11，26]从算法层面说明了泄漏函数实际上和算法的结构紧密相关，甚至和攻击的方法也是紧密相关的。

4.2　基于反馈的关联性分析

Albert 等[27]提出的 FCA，更加宏观地阐述了故障攻击与功耗攻击之间的关联。向目标设备注入故障后，将功耗曲线转化为故障概率曲线，并对故障概率曲线实施 CPA。该方法无需掌握明文或密文的具体数据以及算法的具体实现形式，只需观察目标设备的反馈情况。文中提出两种分组方法：一种是基于成功概率，观察加密操作是否成功；另一种是基于静音概率，观察设备是否发生故障且不再响应。该研究在 3 个不同的目标硬件设备上进行了成功的攻击。实验结果表明故障注入和旁路攻击关联性极强，可认为故障概率与特定的操作及正在处理数据的功耗有关。

文献[27]不关注具体的算法，而是从物理层面切入，从本质上说明了故障攻击和旁路攻击是高度重合的。实验结果表明二者的泄漏函数是高度吻合的，否则故障攻击条件下得到的概率曲线与旁路攻击下的功耗曲线将不相符。

功耗攻击通过分析功率的变化情况恢复密钥，而功率的

变化与正在执行的指令以及与正在处理的数据有关。电路开关网络的状态发生变化，本质是晶体管的通断状态发生变化。被导通的晶体管极易受到脉冲信号的干扰，在故障攻击中，被导通的晶体管的数量越多，目标设备的正常加解密操作受到干扰的概率就越大，消耗的能量就越多，其对应的能量曲线就越高。

功耗攻击和故障攻击本质都是电路中晶体管通断状态随执行的指令及处理的数据发生了变化，因此，二者的泄漏函数、故障概率都是高度一致的。

5 前沿研究热点

功耗攻击效果较好，故障攻击操作简单、成本较低，二者均受到广泛关注，其关联性研究也取得了一定的进展。当前仍有一些热点问题值得做进一步深入研究。

由于二者本质一致，可通过构建统一的物理泄漏函数模型，减少所需数据量且降低噪声干扰，以准确评估攻击的能力；提出统一的物理安全测评标准，以准确评估抗攻击的能力；设计通用防御策略，以抵御组合攻击等更强有力的攻击方法。

5.1 构建统一的物理泄漏模型

泄漏模型是侧信道攻击评估的重要工具，其准确性会影响评估的可靠性。当前，大多数泄漏模型仅分析了低阶信息，无法规避假设误差和估计误差。

已有泄漏模型的对比如表 1 所列。功耗模型攻击效果较好，但需要的数据量过大，效率不高；故障模型需要的数据量较少，但对数据的要求较高，且易受噪声干扰；故障敏感度模型不受噪声干扰，但所需数据量较大，攻击效率不高；故障概率模型对数据无特殊要求，不受噪声干扰，攻击效果较好，但所需数据量较大。已有泄漏模型大都存在一定的局限性，无法同时兼顾对数据的要求、数据量、容错能力以及攻击效率。

表 1 泄漏模型对比

Table 1 Comparison of leakage models

泄漏模型	分析方法	泄漏源	密钥恢复方法	数据要求	数据量	容错能力
功耗模型	SPA[2]、DPA[1]、CPA[4]	侧信道(功耗)	模型测试	噪声较小	较大	较差
	TA[6]	侧信道(功耗)	模板测试	无特殊要求	较大	较强
故障模型	MIA[5]	故障互信息量	模型测试	猜测值和观测值对	较大	一般
	DFIA[14]	有偏故障	模型测试	故障有偏分布	较少	较强
	DFA[12]	故障	精确计算	无特殊要求	最少	差
故障敏感度模型	FSA[11-26]	故障敏感度	模型测试	故障发生的时序信息	较多	不受噪声干扰
故障概率模型	FCA[27]	输出状态	模型测试	无特殊要求	较大	不受噪声干扰

在高阶泄漏的测量中，噪声干扰更为严重，上述模型评估效果大打折扣。文献[30]提出以最大熵分布构建泄漏模型。所有概率值都相等时熵最大，故该模型没有引入任何模型的主观假设，可以利用任意高阶矩的信息拟合达到高精度，减小模型假设误差和估计误差，无限逼近泄漏分布。

基于当前的泄漏模型，不能通过 FS 泄漏证明功耗泄漏的存在性，同时，也不能通过功耗泄漏证明 FS 泄漏的存在性。Moradi 等[13]指出，SASEBO-R 上的所有 AES 实现都具有一阶 FS 泄漏，但对于 SASEBO-R 上的随机开关逻辑(RSL)实现[31]，使用一阶功耗分析无法成功恢复密钥。

从物理层面分析，功耗攻击和故障攻击信息泄漏的本质是一致的，其存在性也是一致的。将功耗模型与故障模型相结合，构建统一的物理泄漏模型，降低对数据量的要求，同时也可减少噪声的干扰。

5.2 提出统一的物理安全测评标准

在密码系统抗旁路攻击能力评估中，通常以成功率、猜测熵等指标度量密钥恢复能力，即侧信道泄漏的信息多大程度上能够应用到密码恢复上。评估旁路信息泄漏时，大多使用泄漏检测(如 Welch's t-test[32-33]、相关 ρ-test[34] 和 χ^2-test[35])以 CMI[36-37](Continuous Mutual Information)、DMI[38-39](Discrete Mutual Information)等数据为指标量化系统安全性。目前应用最广泛且相对简单的泄漏评估方法为 TVLA[40]：在使用相同加密算法和密钥的前提下，对目标密码系统分别采集随机输入和固定输入下的加密曲线，并对两组功耗曲线进行 Welch's t-test。当总体的样本量和方差都不等时，Welch's t-test是一种易于实现且成本较低的测试方法，其统计量为：

$$t_{\text{obs}}=\frac{\overline{X}_A-\overline{X}_B}{\sqrt{\frac{S_A^2}{N_A}+\frac{S_B^2}{N_B}}} \tag{6}$$

$$H_0:\mu_A=\mu_B,H_1:\mu_A\neq\mu_B$$

其中，$\overline{X}_A$，$\overline{X}_B$ 为总体 A，B 的均值，S_A，S_B 为总体 A，B 的标准差，N_A，N_B 为总体 A，B 的样本总数，μ_A，μ_B 为总体 A，B 的期望。拒绝域的临界值由显著性水平 α 和自由度 v 计算出。

T 分布样本数量 $n>100$ 时，收敛于正态分布。Goodwill 等[41]建议使用 $t_{\text{obs}}=\pm4.5$ 的置信区间。$n=100$ 时，观测值有 99.5% 的概率落入置信区间；$n=5\,000$ 时，观测值有 99.999% 的概率落入置信区间。

Durvaux 等[34]对比了基于 Welch's t-test 的泄漏检测方案和基于相关 ρ-test 的泄漏检测方案，表明 t-test 采样复杂度更低，并基于信噪比对其进行改进，数据量减少约 80%，检测速度明显更快。

文献[35]表明在噪声较小或泄漏在不同阶分布不同的情况下，χ^2-test 效果优于 t-test。t-test 适用于较高阶数的泄漏评估，χ^2-test 适用于噪声较小的泄漏评估，将二者结合可提高评估效果。

为解决采集 Welch's t-test 数据需要物理访问目标设备且需要专门的设备测量功耗等问题，GLAMOCČANIN 等[42]提出了一种适用于 FPGA 的功率侧信道泄漏自评估内置测试方法，自评估对一阶功率 SCA 的防御能力，被触发后，FPGA 可自测内部电源电压，并实时进行 t-test 计算。

文献[43]提出构建统一的物理安全评估方法，将信息论和安全指标结合，量化实际的泄漏函数，用信息论指标(条件熵)评估实现效果，用安全指标(成功率或猜测熵)评估攻击和

对手,衡量泄漏的信息如何被转化为成功的攻击。

文献[44]以累积部分猜测熵为指标判断密钥搜索是否完成。部分猜测熵表示猜测单个子密钥字节的正确值所需的平均次数,其值为零表示子密钥完全已知。若 AES 子密钥字节的所有 PGE 之和为零,表示无需猜测,可通过 CPA 恢复出完整的密钥。

当前针对物理安全的测评方法不尽统一,效果差异较大,需要进一步优化评估检测方法,选择合适的评估指标,构建统一的物理安全测评标准。

5.3　设计通用防御策略

功耗攻击防御策略主要分为两类:一是降低功耗曲线的波动,减少泄漏的信息量,即采用幅度噪声,降低信噪比;二是消除功耗与密钥之间的数据相关性,使功耗曲线模糊,即增加冗余功耗或随机噪声。算法层的防御策略包括随机插入空指令或者等待状态[45-46]、数据隐藏[47]和消除计算中的条件分支[14]。逻辑层的防御策略主要平衡芯片的功耗,普适性更强,如 SDDL 电路[48]和 WDDL 电路[49-50]等。

掩码防御技术包括布尔掩码和乘法掩码,实现简单,成本低廉。在 AES 算法的所有步骤中,只有字节替换中的 S 盒为非线性函数,在掩码算法的操作过程中需要利用修正函数进行修正,使之修正为与掩码值相符的线性函数,因此每次运算都要重新计算 S 盒,运算效率将大幅降低,资源消耗较高。

故障攻击防御策略主要分为两类:一是算法层面,引入时间冗余或在编码中加入检验位;二是电路层面,引入面积冗余,输入使能信号或在电路中加入可配置延时模块(Configurable Delay Blocks,CDB)等等。随着研究的深入,CFSA 等方法已具备对掩码电路的攻击能力。而引入时间冗余、面积冗余、CDB 等增加了电路的面积开销和时间开销。

当前针对 SCA 和 FA 的防御研究广泛开展,通常使用单独的对策分别防御,难以抵御另一种攻击或组合攻击,且针对特定攻击的对策可能会对另一种攻击产生一定影响。文献[51]中专用电路Ⅱ是基于专用电路Ⅰ构建的,且带有抗 FA 的编码工具,但无法保证在故障环境下的安全性。文献[44]表明在基于 FPGA 平台的 AES 完整实现中,不同故障检测(Fault Detection,FD)方法对 CPA 的密钥检索速度影响差异较大。文献[24]基于 FPGA 平台研究 FA 对策是否以及如何影响 CPA 的效率,提出了结合动态掩蔽和错误偏置的新对策,以抵御 CPA 和 FA 的组合攻击。当前,有针对组合攻击的单一防御对策被提出,如文献[52]中提出编码技术抵抗组合攻击,文献[53]中提出基于多项式的多方计算(Multi-party Computation,MPC)使 SCA 失效并同时进行故障注入检测。以上方法具有高安全性,但资源消耗过高。

随着芯片尺寸的缩小,静态功耗比重日益增加,而现有的防御技术中主要是针对目标设备运行过程中的动态功耗。

通用的防御策略可解决上述问题,设计时可考虑将算法层面的掩码和逻辑层面的延时电路相结合,提高组合攻击的防御能力。

结束语　本文综述了旁路攻击与故障攻击的原理和泄漏模型,并阐述了其关联性,分析了当前的研究热点。对二者关联性进行了分析,表明二者不论在本质上还是算法层面都具有较高的一致性,并指出现有泄漏模型、检测方法存在的问题。构建统一的物理泄漏函数模型,提出统一的物理安全测评标准,设计通用防御策略,作为当前热点,可作进一步研究。

参 考 文 献

[1] KOCHER P,JAFFEJ,JUN B. Differential Power Analysis[C]// Advances in Cryptology— CRYPTO'99. Lecture Notes in Computer Science,1999:388-397.

[2] KOCHER P. Timing Attacks on Implementations of Diffie-Hellman,RSA,DSS,and Other Systems[J]. Lecture Notes in Computer Science,1996,1109(1):104-113.

[3] GANDOLFI K,MOURTEL C,OLIVIER F. Electromagnetic Analysis:Concrete Results[M]. Berlin,Heidelberg:Springer,2001:251-261.

[4] BRIER E,CLAVIER C,OLIVIER F. Correlation Power Analysis with a Leakage Model[C]// Cryptographic Hardware and Embedded Systems— CHES 2004. Lecture Notes in Computer Science,2004:16-29.

[5] GIERLICHS B,BATINA L,TUYLS P,et al. Mutual Information Analysis[C]// Cryptographic Hardware and Embedded Systems(CHES 2008). 10th International Workshop,Washington,2008.

[6] CHARI S,RAO J R,ROHATGI P. Template Attacks[C]// International Workshop on Cryptographic Hardware & Embedded Systems. 2002.

[7] QUISQUATER J J,SAMYDE D. Eddy Current for Magnetic Analysis with Active Sensor[C]// Proceedings of eSMART-2002. 2018:1-20.

[8] CAI F,BAI G,LIU H. Optical Fault Injection Attacks for Flash Memory of Smartcards[C]// 2016 6th International Conference on Electronics Information and Emergency Communication. IEEE,2016:46-50.

[9] AGOYAN M,DUTERTRE J,NACCACHE D,et al. When Clocks Fail:On Critical Paths and Clock Faults[M]. Berlin,Heidelberg:Springer,2010:182-193.

[10] CHONG H K,QUISQUATER J J. Faults,Injection Methods,and Fault Attacks[J]. IEEE Design & Test of Computers,2007,24(6):544-545.

[11] YANG L,SAKIYAMA K,GOMISAWA S,et al. Fault Sensitivity Analysis[C]// Cryptographic Hardware & Embedded Systems. International Workshop,Santa Barbara,2010.

[12] BIHA M,SHAMIR A. Real-time detection of anomalous taxi trajectories from GPS traces[C]// Advances in Cryptology— CRYPTO '97. Lecture Notes in Computer Science,1997:513-525.

[13] MORADI A,MISCHKE O,PAAR C,et al. On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting[M]. Berlin,Heidelberg:Springer:2011:292-311.

[14] GHALATY N F,YUCE B,TAHA M,et al. Differential Fault Intensity Analysis[C]// Workshop on Fault Diagnosis & Tolerance in Cryptography. 2014.

[15] DOBRAUNIG C,EICHLSEDER M,KORAK T,et al. SIFA:Exploiting Ineffective Fault Inductions on Symmetric Cryptography[J]. IACR Transactions on Cryptographic Hardware and

Embedded Systems, 2018, 20(3): 547-572.
[16] DOBRAUNIG C, MANGARD S, MENDEL F, et al. Fault Attacks on Nonce-Based Authenticated Encryption: Application to Keyak and Ketje[C]// International Conference on Selected Areas in Cryptography. 2018.
[17] RAMEZANPOUR K, AMPADU P, DIEHL W. Fault intensity map analysis with neural network key distinguisher[J]. Journal of Cryptographic Engineering, 2021, 11(3): 273-288.
[18] RAMEZANPOUR K, AMPADU P, DIEHL W. Fault intensity map analysis with neural network key distinguisher[C]// Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop. 2019: 33-42.
[19] SAHA S, BAG A, BASU ROY D, et al. Fault Template Attacks on Block Ciphers Exploiting Fault Propagation[M]. Cham: Springer International Publishing, 2020: 612-643.
[20] Fan ZHANG X L X Z. Persistent Fault Analysis on Block Ciphers[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 3: 150-172.
[21] CHENG Y, ZHENG M, HUANG F, et al. A Fast-Detection and Fault-Correction Algorithm against Persistent Fault Attack [C]// 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2021: 557-568.
[22] LIU Y, ZHANG J, WEI L, et al. DERA: Yet another differential fault attack on cryptographic devices based on error rate analysis [C]// Proceedings of the 52nd Annual Design Automation Conference. 2015: 1-6.
[23] WANG Q, WANG A, QU G, et al. New Methods of Template Attack Based on Fault Sensitivity Analysis[J]. IEEE Transactions on Multi-Scale Computing Systems, 2017, 3(2): 113-123.
[24] DOFE J, PAHLEVANZADEH H, YU Q. A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack[J]. Journal of Electronic Testing, 2016, 32(5): 611-624.
[25] PIRET G, QUISQUATER J J. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD[C]// Cryptographic Hardware and Embedded Systems—CHES 2003. Springer Berlin Heidelberg, 2003: 77-88.
[26] YANG L, ENDO S, DEBANDE N, et al. Exploring the Relations between Fault Sensitivity and Power Consumption[C]// International Conference on Constructive Side-channel Analysis & Secure Design. 2013.
[27] SPRUYT A, MILBURN A, CHMIELEWSKI ?. Fault injection as an oscilloscope: fault correlation analysis[C]// Cryptographic Hardware and Embedded Systems. 2021: 192-216.
[28] CARLET C, DANGER J, GUILLEY S, et al. Achieving side-channel high-order correlation immunity with leakage squeezing [J]. Journal of Cryptographic Engineering, 2014, 4(2): 107-121.
[29] ROCHE T, LOMNÉ V, KHALFALLAH K. Combined fault and side-channel attack on protected implementations of AES [C]// Smart Card Research and Advanced Applications: 10th IFIP WG 8.8/11.2 International Conference (CARDIS 2011). Springer Berlin Heidelberg, 2011: 65-83.
[30] OU C, ZHOU X, LAM S, et al. Information Entropy-Based Leakage Profiling[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40(6): 1052-1062.
[31] OTT R L, LONGNECKER M T. An introduction to statistical methods and data analysis[M]. Cengage Learning, 2015: 198-199.
[32] DING A A, CHEN C, EISENBARTH T. Simpler, faster, and more robust t-test based leakage detection[C]// Constructive Side-Channel Analysis and Secure Design: 7th International Workshop (COSADE 2016). Springer International Publishing, 2016: 163-183.
[33] STANDAERT F. How (Not) to Use Welch's T-Test in Side-Channel Security Evaluations[M]. Cham: Springer International Publishing, 2019: 65-79.
[34] DURVAUX F, STANDAERT F. From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces [M]. Berlin, Heidelberg: Springer, 2016: 240-262.
[35] MORADI A, RICHTER B, SCHNEIDER T, et al. Leakage Detection with the χ^2-Test[C]// Cryptographic Hardware and Embedded Systems. 2018: 209-237.
[36] CHOTHIA T, GUHA A. A Statistical Test for Information Leaks Using Continuous Mutual Information[C]// IEEE Computer Security Foundations Symposium. 2011.
[37] HETTWER B, GEHRER S, G? NEYSU T. Applications of machine learning techniques in side-channel attacks: a survey[J]. Journal of Cryptographic Engineering, 2020, 10: 135-162.
[38] CHATZIKOKOLAKIS K, CHOTHIA T, GUHA A. Statistical Measurement of Information Leakage[C]// DBLP. 2010: 390-404.
[39] BISWAS A, BANERJI A, CHANDRAVANSHI P, et al. Experimental Side Channel Analysis of BB84 QKD Source[J]. IEEE Journal of Quantum Electronics, 2021, 57(6): 1-7.
[40] LEV-AMI T, SAGIV M. TVLA: A system for implementing static analyses[C]// International Static Analysis Symposium. Berlin, Heidelberg: Springer, 2000: 280-301.
[41] AIGNER M, OSWALD E, AIGNER@IAIK M, et al. Power analysis tutoriall[C]// Institute for Applied Information Processing and Communication University of Technology Graz. 2000.
[42] GLAMOANIN O, COULON L, REGAZZONI F, et al. Built-in Self-Evaluation of First-Order Power Side-Channel Leakage for FPGAs[C]// The 2020 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA '20). ACM, 2020.
[43] STANDAERT F, MALKIN T G, YUNG M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks [M]. Berlin, Heidelberg: Springer, 2009: 443-461.
[44] PAHLEVANZADEH H, DOFE J, YU Q. Assessing CPA resistance of AES with different fault tolerance mechanisms[C]// 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC). IEEE, 2016: 661-666.
[45] YANG S, WOLF W, VIJAYKRISHNAN N, et al. Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach[C]//2005 Design, Automation and Test in Europe Conference and Exposition (DATE 2005). IEEE, 2005.
[46] BUCCI M, LUZZI R, GUGLIELMO M, et al. A countermeasure against differential power analysis based on random delay inser-

tion[C]// 2005 IEEE International Symposium on Circuits and Systems(ISCAS). IEEE,2005:3547-3550.

[47] CHONG K,NG J,CHEN J,et al. Dual-Hiding Side-Channel-Attack Resistant FPGA-Based Asynchronous-Logic AES:Design, Countermeasures and Evaluation[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems,2021,11(2):343-356.

[48] TIRI K,VERBAUWHEDE I. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation [C]// Design,Automation & Test in Europe Conference & Exhibition. 2004.

[49] TIRI K. A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs[C]// DBLP. 2005:1530-1591.

[50] NIKNIA F,DANGER J,GUILLEY S,et al. Aging Effects on Template Attacks Launched on Dual-Rail Protected Chips[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2022,41(5):1276-1289.

[51] ISHAI Y,PRABHAKARAN M,SAHAI A,et al. Private Circuits II:Keeping Secrets in Tamperable Circuits[C]// International Conference on the Theory & Applications of Cryptographic Techniques. 2006.

[52] JAKUB B,HOU X. Feeding Two Cats with One Bowl:On Designing a Fault and Side-Channel Resistant Software Encoding Scheme[C]// Cryptographers Track at the Rsa Conference. 2017.

[53] SEKER O,FERNANDEZ-RUBIO A,EISENBARTH T,et al. Extending Glitch-Free Multiparty Protocols to Resist Fault Injection Attacks[C]// Cryptographic Hardware and Embedded Systems. 2018.

WU Tong, born in 1996, postgraduate. Her main research interests include cryptographic chip security assessment and so on.