侧信道攻击与防御技术研究进展

王永娟[1)] 樊昊鹏[1)] 代政一[2),3)] 袁庆军[1)] 王相宾[1)]

[1)](战略支援部队信息工程大学 郑州 450001)

[2)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

[3)](中国科学院大学网络空间安全学院 北京 100049)

摘 要 侧信道攻击利用密码实现的物理泄露而不是理论弱点来恢复密钥,对密码系统的安全实现有严重的现实威胁. 密码设备运行时所产生的能量、电磁、缓存和故障输出等侧信息均可能导致密钥信息泄漏，攻击者通过分析侧信息中与密钥相关的特征点来获取密钥信息. 为了应对侧信道攻击，侧信道防御技术和抗泄漏密码学也成为研究的热点问题. 前者的总体思路在于消除侧信息泄漏或者消除秘密信息与所泄漏侧信息之间的相关性，而后者旨在准确量化密码系统执行过程中的侧信息泄漏，进而构造具有抗泄漏安全性的密码方案. 本文系统地介绍了侧信道攻击与防御技术发展：首先，剖析了时序攻击、能量分析攻击、缓存攻击和故障攻击的基本原理、攻击方法、应用场景和发展现状，并提炼出每一类攻击的通用模型；其次，概括出侧信道防御技术的本质特征，并分析了侧信道防御技术的基本原理、安全模型和应用场景；之后总结了抗泄漏密码学的基本原理与发展现状，梳理了典型的抗泄漏密码方案；最后分析了现有研究工作中存在的问题，并对未来的研究方向进行了展望.

关键词 侧信道攻击；侧信道防御；抗泄漏密码学；能量分析攻击；缓存攻击；故障攻击

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2023.00202

Advances in Side Channel Attacks and Countermeasures

WANG Yong-Juan[1)] FAN Hao-Peng[1)] DAI Zheng-Yi[2),3)] YUAN Qing-Jun[1)] WANG Xiang-Bin[1)]

[1)](PLA Strategic Support Force Information Engineering University, Zhengzhou 450001)

[2)](State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)

[3)](School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049)

Abstract Side-channel attacks recover keys from the physical implementation leakage of the cryptosystem rather than the theoretical weaknesses. Side-channel attacks seriously affect the security implementation of the cryptosystem. The power, electromagnetic, cache, and fault output generated by the cryptographic devices can lead to the leakage of the key. The adversary can recover the key by analyzing the key-related points in the side-channel information. To counter side-channel attacks, side-channel countermeasures, and leakage-resilient cryptography have also become hot research issues. The general idea of the former is to eliminate side-channel information leakage or to remove the correlation between secret information and the side-channel information, while the latter aims at accurately quantify the side message leakage during the execution of a cryptosystem and thus construct a cryptographic scheme with leakage-resilient security. This paper systematically introduces the development of side-channel attacks and countermeasures. Firstly, it analyses the basic principles, attack methods, application scenarios, and development status of timing attacks, energy analysis attacks, cache attacks, and fault attacks, and distills a general model for each type

收稿日期：2021-09-23；在线发布日期：2022-07-04. 本课题得到国家自然基金（61602512）资助. **王永娟**，博士，研究员，主要研究领域为信息安全、人工智能、侧信道分析等. E-mail: pinkywyj@163.com. **樊昊鹏**（通信作者），硕士研究生，主要研究领域为密码学、侧信道分析. E-mail: fanhaopeng15gc@sina.com. **代政一**，硕士研究生，主要研究领域为密码学、侧信道分析. **袁庆军**，博士研究生，讲师，主要研究领域为侧信道分析、网络流量分析. **王相宾**，硕士研究生，主要研究领域为侧信道分析.

of attack; secondly, it outlines the essential features of side-channel countermeasures, and analyses the basic principles, security models, and application scenarios of side-channel countermeasures; after that, it summarizes the basic principles and development status of leakage-resilient cryptography; finally, this paper points out the problems in the current research and look forward to the future research directions.

Keywords　side-channel attack; side-channel countermeasures; leakage-resilient cryptography; power analysis attack; cache attack; fault attack

1　引　言

自二十世纪九十年代 Kocher 提出侧信道攻击技术[1]以来，其一直被认为是密码系统实现的安全威胁. 侧信道攻击利用系统在执行过程中的行为信息恢复秘密数据，即使是在可证明安全模型下密码系统也易受侧信道攻击的威胁. 当设备处理的数据与其侧信道泄漏（运行时间，能量曲线，电磁辐射等）之间存在数据依赖性时，攻击者可以利用这些泄漏信息恢复密钥等秘密数据.

侧信道攻击为攻击者提供了额外的信息，降低了恢复未知密钥的难度. 与传统的密码分析不同，侧信道攻击的破解技术与密钥长度无关或线性相关. 当泄漏的信息足够多时，侧信道攻击仅需要很小的代价就可以恢复密钥. 根据不同类别的侧信息，侧信道攻击可分为：时序攻击、能量分析攻击、电磁攻击、缓存攻击、故障攻击和其他侧信道攻击方法.

在时序攻击中，攻击者将密码设备视为一个黑盒，加密一个或多个消息，获取每个消息的加密时间，利用时间的差异恢复密钥的部分信息，再利用排除法或优势叠加法恢复完整密钥.

在能量分析攻击中，攻击者记录密码系统设备的电压值变化，以确定可用于破坏密码系统和检索密钥的特征. 常见的能量分析攻击方法有：简单能量分析、差分能量分析、相关能量分析和模板攻击等.

电磁攻击的原理在于电荷的运动伴随着电磁场的产生，攻击者可无接触地采集密码系统设备的电磁泄露. 常见的电磁分析攻击方法有：简单电磁分析、差分电磁分析和相关电磁分析.

缓存攻击以攻击者与受害者共享部分缓存资源为前提，根据受害者进程的从内存与缓存取数据时间的差异获得其缓存争用情况，进而获取受害者的秘密信息. 现代云计算方案通过资源共享的方式提升了系统资源的利用率，但资源共享为缓存攻击提供了条件，同时带来了潜在的漏洞.

故障攻击通过激光、时钟毛刺和高强度电磁波等手段使密码芯片发生故障，从而达到篡改设备并使其执行一些错误操作以泄漏秘密信息. 故障分为永久性故障，持久性故障和暂时性故障，永久性故障（如将存储单元冻结到一个恒定值、切断数据总线等）会永久性地损坏密码装置，使其在以后的所有计算中都会产生错误的结果；暂时性故障（放射性爆炸、时钟频率异常和电源电压异常等）使设备在计算过程中受到干扰，在特定运算过程中产生故障. 持久性故障持续的时间介于两者之间，通常在注入持久性故障后，该故障会存在一段时间，直至内存刷新或设备重置. 一旦存在这种类型的故障，在加密过程中可能产生错误密文. 常用的技术有 Rowhammer 注入技术，通常应用于改变加密过程中存储的常量、S 盒中元素的值等.

其他侧信道攻击方法如光侧信道攻击、声侧信道攻击、热成像攻击和流量分析攻击分别利用密码设备在执行加密操作时液晶显示器所产生的光强度、计算部件的声发射、热成像和网络中关键节点的流量来分析密码设备的密钥信息.

侧信道攻击往往给用户或系统带来灾难性的后果，因此需要通过在硬件和软件中增加侧信道防护机制以提高密码算法实现的健壮性. 侧信道防御的难度要远远大于攻击的难度，攻击可以只攻其一点，但是防御要兼顾方方面面. 侧信道防御的核心是消除或减少攻击者能够利用的具有数据依赖性的侧信息，主要有三类总体思路：其一是在密码算法的具体实现上去除侧信息的数据依赖性，如在进行与秘密信息有关的计算时使用恒定时间实现的算法，或是利用掩码方案随机化重要的中间变量，使得物理设备执行密码算法时产生的能量/电磁泄漏难以利用；其二是通过掩盖侧信息，弱化其某些特征，使得攻击者难以分辨和利用，如对于声、光、热等侧信息的泄漏，可使用吸收材料消除这些特征，或是引入频率接近的随机干扰源，与加密设备同时释放声、光、热信息，从而达到侧信道防御的目的；其

三是从系统级层面综合考虑去除侧信息的数据依赖性，即需要考虑多个侧信道防御措技术之间的相互影响，相对来说，系统防御技术具有较高的灵活性和可扩展性，实现成本较低.

为了抵抗侧信道攻击，量化密码算法执行过程中的侧信道泄漏以及合理评估密码系统的安全性，密码学家提出了一个重要的研究方向——抗泄漏密码学. 在其考虑的场景中，攻击者可以获得有关内部状态的物理泄漏，密码学家需要在此条件下构造出抗泄漏的密码方案.

下面本文将从侧信道攻击、侧信道防御和抗泄漏密码学三个方面介绍基本原理、攻击/防御模型、应用场景以及发展现状.

2 侧信道攻击

侧信道攻击为攻击者提供了额外的信息，降低了恢复未知密钥的难度. 与传统的密码分析不同，侧信道攻击的破解技术与密钥长度无关或线性相关. 当泄漏的信息足够多时，侧信道攻击仅需要很小的代价就可以恢复密钥. 本章主要介绍时序攻击、能量分析攻击、缓存攻击和故障攻击的基本原理、攻击方法、应用场景和发展现状.

2.1 时序攻击

时序攻击最早由 Kocher 等人[1]提出. 该攻击利用加密所需的时间信息以破解密钥. 通过检查模幂运算的时间变化，证明了该攻击对非对称系统的适用性. 考虑从右到左的平方乘算法(如算法 1 所示)，如果指数位为 1，则算法先执行乘法操作，然后执行平方操作. 如果指数位为 0，算法仅执行平方操作. 要发起时序攻击，攻击者的任务是查找区分前一种情况和后一种情况的输入. 指数位为 1 会导致可测量的执行时间增加，而指数位为 0 则不会. 因此，从最低有效位开始，攻击者可以观察执行时间差异来跟踪平方乘求幂算法的状态，之后通过迭代的方法恢复密钥. 这项工作主要涉及具有静态密钥的公钥密码系统，如静态 Diffie-Hellman，RSA 和 DSS 等.

算法 1. 平方乘算法

输入: 基数 b ，模数 m ，指数 $e=(e_{n-1}\cdots e_0)_2$

输出： $b^e \bmod m$

1. $r=1$
2. for $i=n-1$ downto 0 do
3. if $e_i=1$ then
4. $r=r\cdot b \bmod m$
5. end if
6. $r=r^2 \bmod m$
7. end for
8. return r

Brumley 等人[2]提出了开创性的结果，证明时序攻击适用于通用软件系统. 他们根据 Montgomery 模简化算法引入的时间依赖性和 OpenSSL 实现使用的乘法操作，对 OpenSSL 的 RSA 解密实现实施了时序攻击. 该攻击利用了两个重要的事实：其一是 Montgomery 模简化算法根据输入不同，可能需要额外的模简化步骤；其二是多精度整数乘法操作（在 RSA 计算中大量使用）根据两个操作数的长度使用两种性能不同的算法（Karatsuba 或 Schoolbook）中的一种. 根据这两个事实，Brumley 等人攻击了滑动窗口模幂算法，并设计了一种能够检索密钥的完全因子分解攻击.

Billy 等人[3]通过一个客户端发起了一次现实攻击，该客户端测量 OpenSSL 服务器在 SSL 握手期间响应 RSA 解密查询所需的时间. 在本地网络环境和服务器负载较轻的情况下，在同一台计算机上运行的两个进程和同一台计算机上的两个虚拟机之间，攻击都是有效的. 此外，Billy 等人还分析了 WAN 和无线链路上的实验，以评估噪声对攻击的影响. 最后，他们设计了三种可能的防御措施，这些措施被 OpenSSL 在内的几个加密库所采用.

非恒定时间的 RSA、（EC）DSA 和（EC）DH 算法很容易被攻击，因为攻击者可以直接通过观察算法执行时间差异获取用户的秘密信息[4-8]，因此涉及用户秘密（密钥，随机数等）的计算必须以恒定时间实现. 目前常用的实现方法是 Montgomery 阶梯标量乘法，其具有抵抗时序攻击的能力. 该算法非常规则，无论密钥为何值，其总是执行相同的操作序列，因而是恒定时间实现的. Montgomery 阶梯标量乘法如算法 2 所示：

算法 2. Montgomery 阶梯标量乘法

输入: 基数 b ，模数 m ，指数 $e=(e_{n-1}\cdots e_0)_2$

输出： $b^e \bmod m$

1. $(r_0,r_1)=(b,b^2)$
2. for $i=n-1$ downto 0 do
3. if $e_i=0$ then
4. $(r_0,r_1)=(r_0^2,r_0\cdot r_1)$
5. else
6. $(r_0,r_1)=(r_0\cdot r_1,r_0^2)$
7. end if
8. end for
9. return R_0

从理论上看，Montgomery 阶梯标量乘法可以抵抗时序攻击. 但在实践中，Montgomery 阶梯标量乘法实现真的是“恒定时间”吗？Aranha 等人[9]指出，在 OpenSSL 1.0.2u 版本中，二进制曲线（如 SECG① 曲线 sect163r1 和 NIST 曲线 B-283、K-283 等）在第一次迭代时因乘数不同而决定是否需要调用取模函数，进而产生时间差异，素数曲线（如 SECG 曲线 secp192k1 和 NIST 曲线 P-192、P-224 等）在第二个 MSB 值为 0 时会调用 BN_copy 函数进行加速，会产生缓存攻击可以检测到的时间差. 两类曲线都会在循环第一次迭代的时候泄漏第二个 MSB 的值. Genkin 等人[10]则利用了 Curve25519 曲线中四阶元素所生成的群（设为 G_4）破解完整密钥. 虽然 Libgcrypt 算法库使用 Montgomery 阶梯标量乘法实现，但其中调用的取模函数并不是恒定时间的. 在进行倍乘操作时，Montgomery 阶梯标量乘法设置了辅助点 Q_0 与点 Q_1，以存储每一步的运算结果. 取模函数会根据 Q_0 是否属于 G_4 的二阶子群（设为 G_2）判断是否提前跳出函数. 若相邻的两个密钥比特 α_i 和 α_{i+1} 满足 $\alpha_i=\alpha_{i+1}$，则有 $Q_0\in G_2$，取模函数的运行时间短；若 $\alpha_i\neq\alpha_{i+1}$，则有 $Q_0\notin G_2$，取模函数的运行时间长，这产生了时间差异. 攻击者可以从猜测密钥最后一比特值开始，根据取模函数的运行时间逐步还原前一比特的密钥值，最终还原大部分密钥比特的值.

从上述攻击可以看出，Montgomery 阶梯标量乘法完全的恒定时间实现必须满足三个基本前提：

（1）内存操作不能依赖密钥（或随机数）的每一比特，以避免通过内存层次结构泄漏.

（2）必须以相同顺序、相同数量和相同类型的字段操作来进行群运算，而与密钥（或随机数）的每一比特无关.

（3）Montgomery Ladder 标量乘法实现调用的子函数（如取模函数）也必须满足上述条件.

2.2　能量分析攻击

2.2.1　泄漏模型

能量是指密码设备在执行操作时所产生的电压值，将一段时间内电压值构成的曲线称为能量迹. 能量分析攻击基于数据依赖性，即操作数为比特 1 或比特 0 时产生的能量泄露不同. 在密码设备执行某次加密的过程中，能量的泄漏模型如图 1 所示：

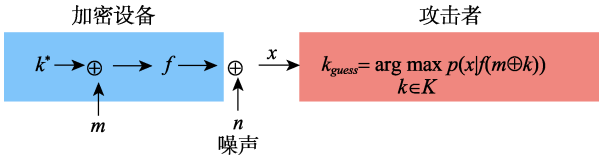


图 1　能量泄漏模型

其中 $\oplus$ 表示异或操作，k^* 是正确密钥，m 是已知的明文，f 是泄漏函数，如 S 盒输出值的单比特（或多比特）汉明重量（或汉明距离）[11]. $n\sim N(0,\Sigma)$ 是可加高斯噪声，$\Sigma=\sigma^2\mathrm{Id}_{Q\times Q}$，$\mathrm{Id}_{Q\times Q}$ 是 Q 阶单位矩阵. $x=f(k^*\oplus m)+n$ 是可观测的侧信息泄漏，攻击者观测到 x 后，通过最优区分器[12] $p(x\mid f(m\oplus k))$ 得到密钥 k 为正确密钥的概率，这里 k 应遍历密钥空间 K. 最优区分器是指使得区分正确密钥优势达到最大的判定模型，Annelie 等人[12]证明了当攻击者完全知道泄漏模型时，最优区分器只取决于噪声分布. 根据极大似然法则，攻击者恢复的猜测密钥 $k_{guess}=\arg\max\limits_{k\in K} p(x\mid f(m\oplus k))$.

2020 年，Carlet 等人[13]证明了在单比特侧信道攻击的情况下，攻击结果由目标 S 盒的自相关函数决定：要使区分器 $p(x\mid f(m\oplus k))$ 达到最大，需使 f 的自相关函数 $\sum\limits_m(-1)^{f(m)\oplus f(m\oplus d)}$ 达到最大，其中 $d=k\oplus k^*$. 对攻击者而言，所有 $k\neq k^*$ 自相关函数集合的最大值 $\max\left\{\sum\limits_m(-1)^{f(m)\oplus f(m\oplus d)}\mid d\neq 0\right\}$ 越小，攻击者越容易区分正确密钥. Carlet 对 S 盒的最佳情况和最差情况优化了自相关函数，研究了以鲁棒性为度量标准以优化自相关函数的一般构造，并利用旋转对称 S 盒的一些特殊构造揭示了抗侧信道攻击能力最强的 S 盒.

2.2.2　无参考设备的能量分析攻击

无参考设备能量分析攻击的基本假设是攻击者不能获得与被攻击设备完全相同的设备，但可以采集到被攻击设备在加密过程中产生的多条能量迹. 攻击者无须了解被攻击设备的详细知识，仍然可以恢复出设备中的密钥.

（1）简单能量分析

简单能量分析（Simpl Power Analysis, SPA）是一种在加密操作期间测量的一条（或极少数）能量迹的目视检查. 攻击者记录并检查密码系统设备的能量迹，以确定可用于破坏密码系统和检索密钥的可见特征. 简单能量分析仅适用于特征非常明显的加密算法实现，攻击者一般使用 SPA 对能量迹进行初步的分析和判断.

① 高效加密组标准（Standards for Efficient Cryptography Group, SECG)成立于 1998 年，旨在促进各种计算平台采用高效加密和互操作性的商业标准。

（2）差分能量分析

差分能量分析（Differential Power Analysis, DPA）使用大量的能量迹来分析固定时刻的能量消耗与被处理数据直接的依赖关系[14]. 假设攻击者获得 N 个明文 $m_1,m_2,\cdots,m_N$，其中 m_i 对应的能量迹为 $t_{i,1},t_{i,2},\cdots,t_{i,M}$，全部的猜测密钥为 $k_1,k_2,\cdots,k_K$. 在确定的能量泄漏模型下，明文与猜测密钥作为泄漏函数 f 的输入，输出为能量消耗矩阵 $\boldsymbol{H}$.

$$\begin{aligned}\boldsymbol{H}&=\begin{bmatrix}h_{1,1}&h_{1,2}&\cdots&h_{1,K}\\h_{2,1}&h_{2,2}&\cdots&h_{2,K}\\\vdots&\vdots&&\vdots\\h_{N,1}&h_{N,1}&\cdots&h_{N,K}\end{bmatrix}\\&=\begin{bmatrix}f(m_1,k_1)&f(m_1,k_2)&\cdots&f(m_1,k_K)\\f(m_2,k_1)&f(m_2,k_2)&\cdots&f(m_2,k_K)\\\vdots&\vdots&&\vdots\\f(m_N,k_1)&f(m_N,k_2)&\cdots&f(m_1,k_K)\end{bmatrix}\end{aligned}\tag{1}$$

DPA 攻击中使用相关系数 $r_{i,j}$ 表示列 h_i 与 t_j 之间的线性关系，$\overline{h_i}$ 与 $\overline{t_j}$ 为列 h_i 与 t_j 的均值，如公式(2)所示：

$$r_{i,j}=\frac{\sum_{s=1}^{N}(h_{s,i}-\overline{h_i})\cdot(t_{s,j}-\overline{t_j})}{\sqrt{\sum_{s=1}^{N}(h_{s,i}-\overline{h_i})^2\cdot\sum_{d=1}^{N}(t_{d,j}-\overline{t_j})^2}}\tag{2}$$

当猜测密钥错误时，能量消耗与实际能量迹之间的相关性并不显著；而猜测密钥是正确的，能量消耗与实际能量迹之间的相关系数十分显著. 根据极大似然判定准则，若计算相关系数矩阵并找到最大值 $r_{i',j'}$，则攻击者猜测密钥 $k_{guess}=k_{i'}$.

2014 年，Luke 等人[15]将单目标“标准”差分能量分析攻击推广至多目标攻击，通过将差分能量分析结果作为启发式概率进行组合，增加泄漏正确密钥的信息. 多目标攻击具有可预测的噪声规模，并且对于不精确的能量模型具有鲁棒性的特点. 当泄露点已知时，已知泄漏点攻击与多变量攻击的一般假设一致. 当泄漏点未知时，通过穷举搜索能量迹，利用“多数投票”的方法来确定“峰值”.

2015 年，Nicolas 等人[16]提出了一种侧信道密钥恢复新方法，即软分析侧信道攻击. 该方法将具有最佳数据复杂度的代数侧信道攻击和基于分而治之的差分能量分析的噪声容忍度结合在一起，具有低时间/空间复杂度. 攻击者利用实际泄漏迹的中间变量信息稀疏性，可以有效地解码.

2018 年，Wang 等人[17]提出了基于脊的差分能量分析（Ridge-based DPA）. Wang 等人用基于脊回归替代线性回归，解决了纳米级设备中密码实现的非线性泄漏问题，并在仿真环境和实际环境中测试了性能，证明了基于脊的 DPA 对纳米级芯片的泄漏具有良好的适应性.

2020 年，Gellersen 等人[18]实现了对 NIST①后量子密码标准化项目[19]的第三轮候选签名算法 Picnic 的差分能量分析. 他们首先对底层的 Multiparty LowMc 实现进行了差分能量分析，然后利用 Picnic 算法两个不同部分的泄漏来恢复整个密钥，继而可以伪造签名. Gellersen 在 FRDM-K66F 开发板上进行实验，只需观察少于 30 个 Picnic 签名即可成功恢复密钥.

（3）相关能量分析

相关能量分析（Correlation Power Analysis, CPA）利用了能量迹 T 与泄漏模型 F 之间的相关性. 设 k 为猜测密钥，能量迹 T 与泄漏模型 F 的相关系数由公式(3)给出[20]：

$$r_{T,F,k}=\frac{E(T\cdot F_k)-E(T)\cdot E(F_k)}{\sigma_T\cdot\sigma_{F_k}}\tag{3}$$

其中 $E(T),E(F_k),E(T\cdot F_k)$ 分别代表 $T,F_k,T\cdot F_k$ 的期望，σ_T 和 σ_{F_k} 代表 T 和 F_k 的方差.

攻击者通过遍历密钥空间，计算泄漏函数，并与采集到的能量迹求相关系数来判定此密钥猜测的正确性. 正确的猜测密钥计算得到的相关系数远高于错误的猜测密钥，根据极大似然法则，攻击者将计算出相关系数最高的猜测密钥视为正确密钥.

Thanh-Ha 等人[21]证明 CPA 攻击可以用 DPA 除以归一化因子的形式来表示. 对于归一化因子带来的高噪声问题，Thanh-Ha 提出在 σ_T 中加入偏差 ε 来减小归一化效应. ε 的选择取决于能量迹形式、噪声电平和能量迹数量等因素.

2018 年，Chakraborty 等人[22]提出一种针对自旋转移转矩磁随机存储器（STT-MRAM）的通用相关能量分析攻击策略. 在这个攻击方法中，攻击者在基于 STT-MRAM 的密码实现的写操作期间利用能量泄漏成功地恢复密钥. 为了验证此技术，Chakraborty 在由 STT-MRAM 和磁性隧道结（MTJ）组成的序列密码算法 MICKEY-128 2.0 上进行了实验. 实验结果表明，只要选择合适的假设能量模型，CPA 就可以攻破基于 STT-MRAM 的密码电路实现.

① 美国国家标准与技术研究院（National Institute of Standards and Technology，NIST)直属美国商务部，提供标准、标准参考数据及有关服务。

2020 年，Huang 等人[23]利用垂直相关能量分析（Vertical CPA）、水平深度相关能量分析（Horizontal In-Depth CPA）、在线模板攻击（Online Template Attacks, OTA）和选择输入简单功率分析（Chosen-Input SPA）攻击了 NIST 后量子密码标准化项目的第三轮候选算法 NTRU Prime. Huang 等人能够从 NTRU_LPRrime 的密钥生成中恢复私钥和会话密钥的种子，并在基于 Cortex-M4 的 STM32F3 和 STM32F4 微控制器上进行了实验.

2.2.3　有参考设备的能量分析攻击

有参考设备能量分析攻击的基本假设是攻击者可以获得与被攻击设备完全相同的设备，可以对任意明文进行加密并且采集能量迹. 相比于无参考设备的能量分析攻击，有参考设备能量分析攻击假设条件更强.

（1）模板攻击

模板攻击（Template Attack, TA）利用多元正态分布对能量迹的特征进行刻画，攻击过程分为建模阶段和密钥恢复阶段[24]. 在建模阶段，模板由能量迹的均值向量 $\boldsymbol{m}$ 和协方差矩阵 $\boldsymbol{C}$ 构成. 假设攻击者获得设备加密产生的 n 条能量迹 $\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_n$，并将这 n 条能量迹根据密钥空间分为 K 个集合 $A_1,A_2,\cdots,A_K,|A_i|=n_i$，其中第 i 个集合 A_i 是密钥 k_i 加密时所产生的能量迹.

定义均值向量 $\boldsymbol{m}_i$ 为

$$\boldsymbol{m}_i=\frac{\sum\limits_{\mathbf{T_j}\in A_i}\boldsymbol{T}_j}{n_i} \tag{4}$$

定义协方差矩阵 $\boldsymbol{C}_i$ 为

$$\boldsymbol{C}_i=\frac{1}{n_i-1}\sum_{\boldsymbol{T}_j\in A_i}(\boldsymbol{T}_j-\boldsymbol{m}_i)(\boldsymbol{T}_j-\boldsymbol{m}_i)' \tag{5}$$

将 $(\boldsymbol{m}_i,\boldsymbol{C}_i)$ 称为密钥 k_i 对应的模板.

在密钥恢复阶段，攻击者针对给定的一个被攻击设备加密时产生的能量迹 $\boldsymbol{Trace}$，计算如下概率：

$$p(\boldsymbol{Trace};(\boldsymbol{m}_i,\boldsymbol{C}_i)=\frac{\exp(-0.5\times(\boldsymbol{Trace}-\boldsymbol{m}_i)'\boldsymbol{C}_i^{-1}(\boldsymbol{Trace}-\boldsymbol{m}_i))}{\sqrt{(2\pi)^t\cdot\det(\boldsymbol{C}_i)}} \tag{6}$$

攻击者计算 $\boldsymbol{Trace}$ 与所有模板的匹配概率，若 $p(\boldsymbol{Trace};(\boldsymbol{m}_j,\boldsymbol{C_j})>p(\boldsymbol{Trace};(\boldsymbol{m}_i,\boldsymbol{C}_i)),\forall i\neq j$，那么根据极大似然准则，攻击者的猜测密钥 $k_{guess}=k_j$.

在 2014 年密码学和信息安全理论与应用国际会议上，由于椭圆曲线密码学的快速实现使用了 Gallant–Lambert–Vanstone（GLV）和 Galbraith–Lin–Scott（GLS）等技术，Diego 等人[25]利用 GLV/GLS 分解、能量分析和模板攻击的方法，使用单比特偏差攻击基于格的 ECDSA 方案，在物理设备上恢复了所有密钥.

2017 年，Choudary 等人[26]对模板攻击时在实践过程中可能出现的问题进行研究. 当使用大量样本或不同设备进行分析时，就会出现数值错误和模板不兼容性的问题. Choudary 指出，使用主成分分析和线性判别分析对数据进行降维可以有效提高模板攻击的效率.

2021 年，Ouladj 等人[27]针对高阶掩码防护改进了高阶模板攻击. Ouladj 将高阶攻击概念转化为 d 维掩码空间上的卷积，掩码方案中使用的线性运算影响卷积的类型. Ouladj 等人说明了这种新的攻击模式对 Boolean, IPM, DSM, polynomial DSM, RSM, leakage squeezing 六种类型高阶掩码方案的攻击结果.

（2）随机模型攻击

随机模型攻击（Stochastic Model Attack, SMA）同样分为建模和密钥匹配两个阶段[28]，但与模板攻击不同的是，在建模阶段，随机模型攻击不使用均值向量 $\boldsymbol{m}$，而是通过预定义的函数来估计能量泄漏. 若预定义函数定义为 S 盒输出 y 中的 n 位 $y_i(i=1,\cdots,n)$ 的值，那么将随机能量模型定义为

$$P(y)=\varepsilon_0+\sum_{i=1}^{n}\varepsilon_n y_n \tag{7}$$

其中常量 ε_0 表示非数据相关的能量泄漏，$\varepsilon_i(i=1,\cdots,n)$ 是与对应比特数据 y_i 相关的能量泄漏. 向量 $\varepsilon=(\varepsilon_0,\varepsilon_1,\cdots,\varepsilon_n)$ 的计算方式为

$$\varepsilon(t)=(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T s(t) \tag{8}$$

其中向量 $s(t)$ 对应于在建模阶段中使用的 N 条能量迹在特定时刻 t 的值，$A=\{a_{i,j}\}$ 是大小为 $N\times(n+1)$ 的矩阵，矩阵 A 的第一列的所有元素（对应于 β_0）为 1，元素 $a_{i,j}(j\neq 0)$ 对应于当明文被正确密钥加密时 $b_i(i=1,\cdots,n)$ 的值.

在密钥恢复阶段，攻击者使用在建模阶段计算的权重 $\varepsilon_i(i=1,\cdots,n)$ 来估计对应于每个能量迹 Trace 的泄漏，这是模板攻击和随机模型攻击的主要区别. 估计噪声和恢复密钥的常用方法有最小距离估计（Minimal Distance metric, MD）和极大似然估计（Maximum Likelihood metric, ML）.

2017 年，Bruneau 等人[29]将随机模型攻击于碰撞攻击结合，提出了随机碰撞攻击. 在有掩码保护的场景下，随机碰撞攻击趋向于最佳区分器. Bruneau 在 DPA contest v4 数据集中验证了随机碰撞

攻击的实用性.

2.3 缓存攻击

2.3.1 缓存层次结构

高性能处理器包含多级缓存，用于存储近期使用的数据和指令以提高访问效率，更靠近内核的缓存访问速度更快. 每个内核拥有其专属的 *L*1 和 *L*2 缓存，而 *L*3 缓存（也称为最后一级缓存 Last-Level Cache，LLC）根据内核数分为 *n* 个分区，这些分区通过环形总线连接，环形总线可确保每个内核都可以访问完整的 LLC. 缓存层次结构如图 2 所示：

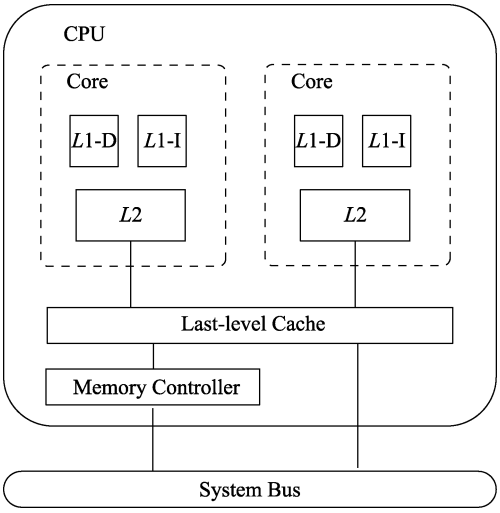


图 2 缓存层次结构

缓存攻击首先要确定目标数据内存地址映射的缓存地址，然后分三个步骤进行攻击：

（1）攻击者通过 clflush 指令或构造冲突集的方法从缓存中清除目标地址.

（2）等待受害者访问目标地址.

（3）测量目标地址或冲突集的访问时间.

攻击者需要根据所拥有的权限而使用不同的缓存攻击方案，如 Flush + Reload、Evict + Reload 和 Prime + Probe 等[4]. 攻击者利用缓存访问的时间差异获得受害者是否访问目标地址的信息，进而推断出受害者部分密钥信息，其主要思路有两种：指令追踪与数据追踪. 指令追踪的方法常用于公钥加密、数字签名和密钥协商等算法，例如在平方乘 RSA 算法中，攻击者追踪平方和乘法指令的地址，即可推断受害者的密钥信息. 数据追踪的方法常用于分组密码算法，例如针对 AES 算法的软件实现（大小为 4KB 的查找表），攻击者通过追踪受害者访问过哪些表项来恢复受害者的密钥信息. 缓存攻击本质上是一种利用缓存获得时间差异的时序攻击.

2.3.2 指令追踪

近几年，由于 *L*1 与 *L*2 缓存被设置为每个内核专用，缓存攻击的目标由 *L*1，*L*2 缓存逐渐转移到内核共享的 LLC. Liu 等人[5]通过对每个 LLC 分区的给定集合索引创建驱逐集，之后通过 Prime+Probe 方法探测目标地址在等待时间内有没有被用户访问，进而得到用户的秘密信息. Liu 提出的攻击需要在包容性缓存结构下才能进行，即高级别缓存的数据一定存在于低级别缓存之中. 对于非包容性缓存结构，攻击者构建的驱逐集中的地址可能只存在于 *L*2 中而不存在于 LLC 中，进而导致构建的驱逐集不能从缓存中逐出目标地址. 针对这一点，Yan 等人[6]在 Liu 的基础上构建了 *L*2 缓存的驱逐集，将驱逐集精准地放入 LLC 中，进而准确地逐出目标地址. Liu 与 Yan 的方案对比如图 3 所示，二者在不同缓存结构下实现了对 RSA 平方乘算法的攻击.

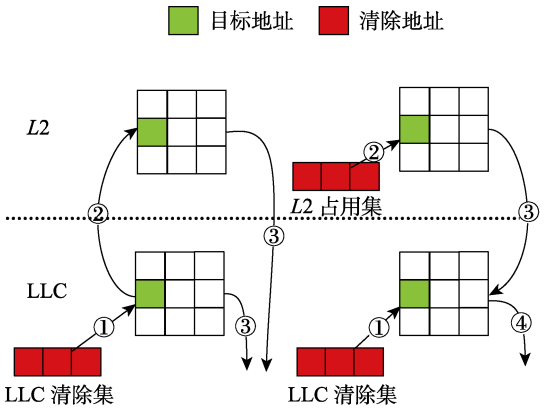


图 3 包容与非包容性缓存结构下 Prime+Probe 攻击

数字签名算法（Digital Signature Algorithm, DSA）和椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm, ECDSA）是缓存攻击的“重灾区”. 其原理在于利用了（EC）DSA 每次签名所选择的随机数 k 与密钥 α 满足公式(9)的线性关系：

$$s = k^{-1}(H(m) + \alpha \cdot r) \tag{9}$$

其中 (m, r, s) 是获得的签名，H 是公开的哈希函数.

攻击者首先需要获得随机数 k 的最高有效位（Most Significant Bit, MSB）或最低有效位（Least Significant Bit, LSB）的信息. Jancar 等人[7]利用随机数 k 的位长与运算时间成正比的关系，通过能量轨迹上的可见泄漏恢复出 k 的最高比特 0 位. Genkin 等人[8]通过测量移动设备在执行签名操作期间的电磁泄漏的频谱图特征来恢复加法与乘法操作，进而恢

复部分 LSB 信息. Aranha 等人[9]揭示了 Montgomery Ladder 标量乘法实现的 ECDSA 的第一次迭代根据 k 的第二个 MSB 的值调用不同的函数，因此产生了可以缓存时序攻击可以检测到的时间差，进而恢复 k 的第二个 MSB. Pereida 等人[30]发现了如果用户没有设置特定参数，那么恒定时间的加密代码将退化为存在泄漏的滑动窗口算法，攻击者可以使用 Prime+Probe 的缓存攻击方法跟踪平方（Square）和乘法（Multiplication）函数，进而得到用户加密过程中的 SM 序列，SM 序列泄漏了随机数 k 的部分 LSB 的值. Aldaya 等人[31]指出 Libgcrypt 等算法库在计算模逆运算时所使用的二进制扩展欧几里德算法并不安全，攻击者可以进行投影坐标攻击：首先攻击者猜测最后一个密钥比特 k_i 的值，假设 $k_i=b, b\in\{0,1\}$，然后攻击者可以根据投影坐标是否有解来判断猜测密钥的正确性，若方程有解，则说明 $k_i=b$ 可能是正确的. 若方程无解则说明假设错误，攻击者确认 $k_i=b\oplus 1$ 并继续推测 k_{i-1} 的值. 攻击者期望得到一些方程无解的信息，进而恢复出部分 LSB 信息.

在得到随机数 k 的部分 MSB 或 LSB 信息之后，攻击者可以将其转化为满足公式(10)形式的隐藏数问题（Hiden Number Problem, HNP）不等式：

$$|\alpha t_i - u_i| < q/2^{l_i} \tag{10}$$

其中 α 是密钥，t_i 和 u_i 是根据签名泄漏的信息构造的值.

当 MSB 或 LSB 信息的比特数 $b\geq 2$ 时，可以根据 HNP 不等式构建格基，进而将 HNP 问题转化为格上的最近向量问题（the Closest Vector Problem of lattice, CVP），可以使用最近平面算法、LLL 算法和 BKZ 算法等进行求解. 另一种思路是将 CVP 问题转化为最短向量问题（the Shortest Vector Problem of lattice, SVP）再进行格基约化. Jancar 等人[7]在 sim，sw，card 和 tpm 四个数据集上进行实验证明了将 CVP 问题转换为 SVP 问题再求解比直接求解 CVP 问题的效率高. 当 $b<2$ 时，Bleichenbacher 等人[32]指出格的方法很难恢复出正确的密钥，但基于傅立叶分析的攻击原则上可以解决任意小的随机数偏差，并且可以处理 S 盒的错误输入，其思想是用逆离散傅里叶变换（Discrete Fourier Transform，iDFT）形式的偏差函数来量化随机数的偏差. 在此基础上，Aranha 等人[8]使用 4-list sum 算法在给定最高有效位信息和攻击者计算资源的条件下，实现了时间、内存和输入数据复杂度之间的最佳平衡，但由于泄漏的信息少，这种方法需要更多的（EC）DSA 签名.

针对（EC）DSA 的缓存攻击思路如图 4 所示.

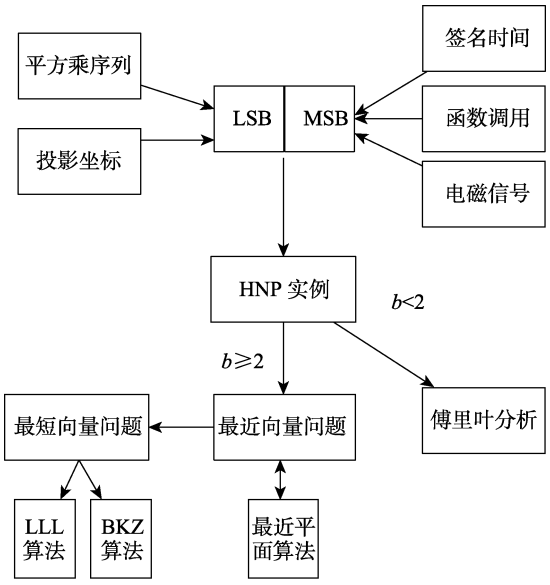


图 4　（EC）DSA 攻击思路

2.3.3　数据追踪

针对分组密码算法，攻击者一般选取 S 盒作为攻击目标. 当 S 盒的存储大小超过缓存行的大小时，就会产生缓存泄露. 以 AES 为例，为了提升性能，AES 的软件实现将 S 盒代换、行移位和列混合三个操作结合在一起，并进行预计算，然后将预计算的结果存储在四个输入为 1 字节而输出为 4 字节的大型查找表 T_0, T_1, T_2, T_3 中[33]，将第 i 轮的输入设为 X^i，$x_0^i, x_1^i, ..., x_{15}^i$ 为 X^i 的 16 字节，第 i 轮的输出可以由式(11)表示：

$$\begin{aligned} X^{i+1} = & \\ & \{\mathrm{T}_0[x_0^i]\oplus \mathrm{T}_1[x_5^i]\oplus \mathrm{T}_2[x_{10}^i]\oplus \mathrm{T}_3[x_{15}^i]\oplus\{k_0^i,k_1^i,k_2^i,k_3^i\}, \\ & \mathrm{T}_0[x_4^i]\oplus \mathrm{T}_1[x_9^i]\oplus \mathrm{T}_2[x_{14}^i]\oplus \mathrm{T}_3[x_3^i]\oplus\{k_4^i,k_5^i,k_6^i,k_7^i\}, \\ & \mathrm{T}_0[x_8^i]\oplus \mathrm{T}_1[x_{13}^i]\oplus \mathrm{T}_2[x_2^i]\oplus \mathrm{T}_3[x_7^i]\oplus\{k_8^i,k_9^i,k_{10}^i,k_{11}^i\}, \\ & \mathrm{T}_0[x_{12}^i]\oplus \mathrm{T}_1[x_1^i]\oplus \mathrm{T}_2[x_6^i]\oplus \mathrm{T}_3[x_{11}^i]\oplus\{k_{12}^i,k_{13}^i,k_{14}^i,k_{15}^i\}\}. \end{aligned} \tag{11}$$

以 AES-128 为例，其共有 10 轮加密. 通过对 16 个字节原始密钥执行密钥扩展算法生成了 10 个 16 字节轮密钥，由于密钥扩展算法是可逆的[33]，给定任意 16 个连续的密钥字节均能恢复原始密钥. 因此攻击者可以选择第一轮加密[34]、最后一轮加密[34-36]或全轮加密[37]作为攻击目标. AES 的缓存攻击依赖于缓存命中假设，即通过缓存攻击获知受害者加密程序的内存访问记录之后，可以推断出密钥字节的 $l=c-\max(0,b-d)$ 比特，其中缓存行大小为 2^b 字节，查找表有 2^c 个项，每个项占用 2^d 字节. 以 Intel

Pentium M 处理器为例，其缓存行大小为 2^6 字节，查找表有 2^8 个项，每个项占用 2^2 字节，则有 $l=4$，即攻击者观察到缓存命中时，可以恢复密钥字节的高 4 位，如图 5 所示.

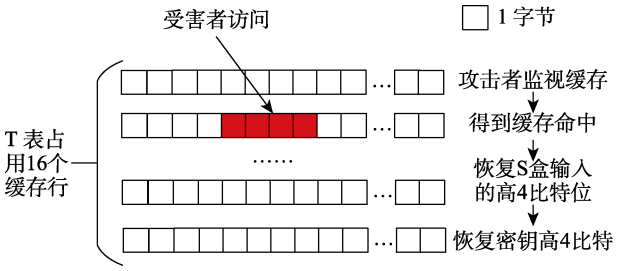


图 5 Pentium M 处理器上针对 AES 第一轮加密的缓存攻击

针对第一轮 AES 加密的缓存攻击在观察到缓存命中时，可以恢复 $m_i \oplus k_i$ 高 l 位，攻击者仍需穷举剩余比特以破解密钥[34]. 最后一轮 AES 加密满足式(12)：

$$c = K^{10} \oplus T_4(x^9) \tag{12}$$

其中 x^9 是第 9 轮加密的输出. 因此，K^{10} 可由式(13)计算：

$$K^{10} = c \oplus T_4(x^9) \tag{13}$$

在攻击者观测到缓存命中之后，Bonneau 等人[34]提出寻找碰撞的方法，Neve 等人[35]提出优势叠加的方法，而 Irazoqui 等人[36]提出访问命中或未命中计数器来恢复正确密钥.

2011 年，Gullasch 等人[37]提出了对全轮加密的攻击，且可以在不需要了解密文的情况下进行，其通过计算候选集得分来还原某一轮的轮密钥，进而恢复主密钥. Gullasch 使用 ANN 神经网络进行降噪，取得了良好的效果.

2020 年，Genkin 等人[38]针对朝鲜未开源的分组密码 Pilsung 进行了缓存攻击. Pilsung 的 S 盒代换与行移位操作由密钥决定，随密钥的变化而变化. Genkin 指出，依赖于密钥的 S 盒代换与行移位并不能提供对缓存攻击的保护，大量的 S 盒需要更庞大的缓存，反而促进了缓存攻击的实现.

2.4 故障攻击

故障攻击（Fault Attack, FA）是侧信道攻击中的一类主动攻击方法，其主要攻击对象是智能卡、射频识别技术（Radio Frequency Identification, RFID）以及嵌入式设备上的密码实现. 攻击者通过将设备暴露于电离、激光、微波辐射等物理环境中，或人为改变电源电压、时钟毛刺、温度等物理因素，进而改变密码算法执行过程中的状态，使得密码算法在计算过程中产生错误. 攻击者根据正确密文、错误密文、密钥三者之间的关联性，恢复密钥信息. 故障攻击与其他侧信道攻击方式相比具有更强的攻击能力.

2.4.1 基本原理

故障攻击的思想由贝尔实验室 Boneh 等人[39-40]于 1996 年提出，用于攻击基于中国剩余定理的 RSA 签名体制. 随后 Biham 和 Shamir[41]将这种攻击方法与差分密码分析相结合攻击对称密码算法 DES，提出了差分故障分析方法（Differential Fault Analysis, DFA）. 差分故障分析已成功应用于攻击 AES[42-49]、3DES[50]、Midori[51]、SKINNY[52]、LED[53]、SPECK[54]、Zorro[55]等分组密码以及 RC4[56]、ChaCha[57]等流密码. 随后，Clavier 等人[58]在 CHES 2007 上提出了利用无效的故障注入，恢复信息的无效故障分析方法（Ineffective Fault Analysis, IFA）. 2013 年，Fuhr 等人[59]提出了利用错误密文的统计特征，恢复密钥的统计故障分析方法（Statistical Fault Analysis, SFA）. Dobraunig 等人[60]在 CHES 2018 会议上将无效故障分析方法与统计故障分析方法相结合，提出了统计无效故障分析方法（Statistical Ineffective Fault Analysis, SIFA）. 同年，Dobraunig 等人[61]证明该方法在注入故障无效的情况下利用密文的统计特征恢复密钥，能够打破具有故障检测防御措施的掩码 AES 实现.

故障攻击分析方法有两大类，一类是基于差分的分析方法. 攻击者在密码算法执行过程中注入故障，利用同一明文对应的正确密文与错误密文之间的差分值，恢复密钥信息. 分析方法有差分故障分析[41]、代数故障分析（Algebraic Fault Analysis, AFA）[62]、故障率分析（Fault Rate Analysis, FRA）[63]等. 另一类是基于统计的分析方法，攻击者利用正确密文与错误密文之间的统计特征差异分析密钥信息. 该类方法适用于攻击者无法自主选择明文进行加密的情况，分析方法有统计故障分析（Statistical Fault Analysis, SFA）[64]、故障敏感度分析（Fault Sensitivity Analysis, FSA）[65]、持久性故障分析（Persistent Fault Analysis, PFA）[66]等.

根据注入故障持续时间的不同，将故障分为三类：暂时性故障，持久性故障和永久性故障. 永久性故障是指在芯片中引入一个永久性缺陷，使其永久性地改变某个功能[67]. 暂时性故障只会在很短的时间内影响设备，通常用来改变加密过程中某个状态的值从而破坏加密的单次执行[68]. 持久性故障持续的时间介于两者之间. 在注入持久性故障后，该故障会一直存在，直至内存被刷新或设备重置. 最

常用的持久性故障注入技术是 Rowhammer 注入技术[69]，该技术通过对动态随机存取存储器（Dynamic Random Access Memory, DRAM）内存行的反复激活，造成内存单元电荷的泄漏，导致内存数据比特翻转，从而完成持久性故障的注入.

基于持久性故障的特点，张帆等人[66]在 CHES 2018 会议上提出了持久性故障分析方法. 攻击者利用 Rowhammer 注入技术，在存储 *S* 盒的内存位置注入一个持久性故障，实现 AES-128 的密钥恢复攻击. 2019 年，张帆等人[70]针对 FPGA 中实现的 AES-128 算法进行持久性故障攻击，并成功恢复全部密钥. 同年，张帆等人[71]利用持久性故障攻击，注入一次故障，打破了具有任意高阶掩码防御措施模块的安全性. 同年，Menu 等人[72]给出了利用电磁辐射在微控制器上的数据传输中进行持久性故障注入的实验. 2020 年，张帆等人[73]利用传统的基于激光的故障注入方式，在 ATmega163L 微控制器中注入持久性故障，实现了对 AES 和轻量级算法 PRESENT 的持久性故障攻击，证明了持久性故障攻击在硬件平台上攻击密码算法的可实现性. 在 2020 年 ACM CCS 会议上，Mus 等人[74]实现了对 NIST 后量子密码标准化项目的第二轮候选签名算法 LUOV 的 QuantumHammer 攻击. 此攻击是两种攻击的组合，一种是通过 Rowhammer 错误注入而实施的比特跟踪攻击，另一种是使用比特跟踪作为 Oracle 的分而治之攻击. 通过比特跟踪，攻击者利用 Rowhammer 攻击收集的错误签名并可以恢复密钥位. 然后攻击者利用 LUOV 密钥生成部分的结构，采用分而治之的攻击方法，通过位跟踪恢复少量的密钥位，从而更有效地求解密钥方程组. Mus 用不到 4 小时的时间成功恢复了多变量签名算法 LUOV 的全部密钥.

攻击者在进行故障攻击之前首先需要得到执行密码算法的设备，或者具有远程访问执行密码算法的运行环境的权限，能够运行该密码算法. 其次攻击者需要知道设备中执行的密码算法的具体实现细节. 最后攻击者能够自主选择明文进行加密或者收集通信信道上传输的密文，对密文进行记录，采用选择明文攻击、选择密文攻击、唯密文攻击等方式进行密钥信息的恢复.

故障攻击由注入故障获取额外信息，根据额外信息进行密码分析. 故障攻击由故障注入和密码分析两个阶段组成：在注入故障阶段，攻击者根据攻击模型选取适当的注入故障的方式. 若密码设备无任何防护措施，攻击者通过将密码设备置于强电磁辐射、高温、低温等物理环境中完成故障的注入. 若攻击者对密码算法的执行过程能够准确控制，则通过改变供给密码设备的电源电压与时钟频率完成故障的注入. 这两种方式成本低，同时注入故障的准确度也较低. 准确度较高的故障注入方式是激光注入，激光注入需要使用专用的高精度仪器. 攻击者需要打开设备，暴露电子元件的硅表面，在指定的时间范围内，在特定的位置打出一定强度的激光完成精准故障的注入. 在成功注入故障后，攻击者选取一定数量的明文在故障状态下进行加密收集错误密文. 在密码分析阶段，攻击者选择合适的分析方法，利用故障引起的正确密文与错误密文的差异、注入故障的位置、注入故障的值以及密码算法的执行过程恢复密钥信息.

2.4.2　攻击模型

故障攻击模型为注入的故障提供了抽象描述，也为后续密码分析提供了前提假设. 攻击者根据具体攻击的密码算法的特征选取有利于密码分析的攻击模型. 攻击模型在分组密码、公钥密码等不同密码体制中具有不同的特点. 在分组密码攻击模型中，注入的故障用于改变密码算法执行过程中的数据. 在公钥密码攻击模型中，注入的故障不仅可以用于改变数据，也可以用于改变密码算法执行的指令，在循环、分支跳转语句中产生错误. 故障攻击模型通常由如下六个方面构成.

- 故障产生阶段：攻击者在注入故障之前首先确定在加解密阶段注入故障或在密钥编排阶段注入故障.
- 故障位置：攻击者根据密码分析的需要确定在某一轮、某一操作步骤或某两个操作步骤之间、某一内存单元注入具体的故障值. 故障位置的选择影响着攻击者注入故障的时刻与密码算法执行过程的同步性. 注入故障的时刻、位置越精确，其实现难度越大.
- 故障类型：攻击者注入故障的类型有单比特故障、单字节故障、多比特故障、多字节故障、随机单比特故障、随机单字节故障、随机多比特故障、随机多字节故障. 前四种故障类型需要攻击者指定在中间状态的某一比特，某一字节注入故障. 后四种故障类型需要攻击者在指定中间状态中注入故障.
- 故障动作：攻击者注入故障的动作分为比特翻转（Bit Fip, BF），即某一比特由 0 变 1 或由 1 变 0、故障位置取指定值（Bit Set or Reset，BSR）、故障位置取随机值（Random Fault，RF）三种情况.

• 故障数量：攻击者根据密码分析的需求一次或多次注入故障，每次注入单个故障或多个故障.

• 故障持续时间：攻击者根据需要故障持续的时间注入暂时性故障、持久性故障或永久性故障. 永久性故障可以作为持久性故障使用，持久性故障可以作为暂时性故障使用.

在完成攻击模型的构建后，攻击者执行故障攻击. 攻击方式有软件环境下对密码算法模拟攻击和实际物理环境下对密码设备进行攻击两种. 软件环境下模拟攻击是指在合理的攻击模型下，研究某一密码体制抵抗故障攻击的安全性；而在实际物理环境下进行攻击，需要借助一定的电子技术与实验仪器，研究密码设备抵抗故障攻击的安全性. 两者相互补充，相互促进. 攻击者在软件环境下进行模拟攻击的执行步骤如下：

（1）攻击者确定注入故障的阶段、位置、类型、动作、数量与持续时间，构建攻击模型.

（2）攻击者选取若干明文在正确状态下进行加密和在故障状态下进行加密，记录同一明文对应的正确密文和错误密文.

（3）攻击者确定合适的密码分析方法，有助于对正确密文、错误密文以及密码算法的执行过程进行分析利用，恢复轮密钥相关信息.

（4）攻击者利用软件模拟该攻击模型，编写计算机程序进行实验. 通过对实验数据进行处理、分析和计算，求出若干轮密钥，进行轮密钥筛选.

（5）攻击者根据密钥编排算法恢复出主密钥.

攻击者在实际物理环境下进行攻击与软件环境下模拟攻击相比，攻击者注入故障的环境较复杂，注入故障的准确度较低，需要对注入的故障进行检验. 攻击者需要在合适的物理环境中，根据内存的型号、使用的元器件注入故障，对故障状态下加密的错误密文进行筛选，获取有效的错误密文.

2.4.3 RSA-CRT 的故障攻击

故障攻击最早用于打破基于中国剩余定理（Chinese remainder theorem, CRT）RSA 签名系统的安全性[39]. 在 RSA-CRT 签名系统中，签名者生成消息 m 的签名 s 需要计算 $s=m^e \bmod N$，其中 e 为签名者的私钥. N 为公开模数，是两个大素数 p、q 的乘积. 为了提升签名效率，签名者计算 $s_p=m^e \bmod p$ 和 $s_q=m^e \bmod q$，使用两个预计算的值 a，b 结合中国剩余定理计算签名 $s=as_p+bs_q$. 其中 a，b 满足公式(14)：

$$\begin{cases} a \equiv 1 \bmod p \\ a \equiv 0 \bmod q \end{cases}, \begin{cases} b \equiv 0 \bmod p \\ b \equiv 1 \bmod q \end{cases} \tag{14}$$

Boneh 等人[39]指出：攻击者在模指数运算过程中注入随机单比特故障产生错误签名，利用同一消息 m 的正确签名 s 与错误签名 s' 能够分解公开模数 N，从而打破 RSA-CRT 签名系统的安全性. 整个攻击过程仅需要 1 对正确签名/错误签名.

根据签名过程可知：$s=as_p+bs_q$，$s'=as'_p+bs'_q$. 攻击者在计算 s'_p 的过程中注入故障使得 $s'_p \neq s_p$，$s'_q=s_q$，则有公式(15)成立：

$$s-s'=(as_p+bs_q)-(as'_p+bs'_q)=a(s_p-s'_p) \tag{15}$$

若 p 不整除 $s-s'$，则有公式(16)成立，从而分解了公开模数 N. 同理，攻击者在计算 s'_q 的过程中注入故障也能够分解公开模数 N.

$$\gcd(s-s',N)=\gcd(a(s_p-s'_p),N)=q \tag{16}$$

公钥密码的故障攻击需要结合密码算法的数学原理进行分析，不具有通用性. 而分组密码的结构固定，对其进行故障攻击具有通用的攻击方式，结合分组密码分析中常用的差分分析、不可能差分分析等分析方法，能够提升故障攻击的攻击能力.

2.4.4 AES 的差分故障分析

差分故障分析将故障攻击的思想与差分密码分析相结合，是分组密码的有效攻击方式. 攻击者在加密算法执行过程中注入故障，选取一定数量的明文，分别在正确加密算法和故障加密算法进行同一明文的加密，得到正确密文和错误密文，结合故障的传播过程分析加密密钥. 差分故障分析模型如图 6 所示. 由于在注入故障之前，两个加密算法过程完全相同，因此将两个密文视为输入未知的约减轮的分组密码的输出. 两个未知输入的差分受注入故障的影响. 攻击者通过分析差分传播过程，构造差分方程，在约减轮的密码算法中获取轮密钥信息.

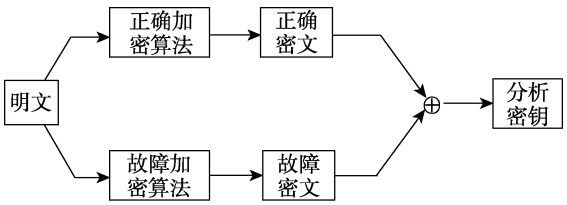


图 6 差分故障分析模型

差分故障分析的一个经典案例是对 AES 的攻击. 目前有许多学者对 AES 的差分故障分析进行研究，注入故障的阶段有加解密算法以及密钥编排算法. 研究目标主要有增加注入故障的轮数范围，减少使用故障密文的数量，将 AES-128 差分故障攻击模型扩展至 AES-192 和 AES-256 等.

Piret 等人[43]采用随机单字节故障模型，在

AES-128 第 8 轮列混淆与第 9 轮列混淆之间注入故障，使用 2 对正确密文/错误密文能够恢复 AES-128 最后一轮子密钥的 4 个字节，成功概率为 98%；使用 8 个错误密文能够恢复 AES-128 主密钥. 在 AES-128 第 7 轮列混淆与第 8 轮列混淆之间注入故障，使用 2 对正确密文/错误密文能够恢复 AES-128 主密钥，成功概率为 92%. 攻击者在第 9 轮列混淆的输入注入随机单字节故障，任意位置的故障最终会影响密文的 4 个字节. 图 7 描述了在第 9 轮列混淆输入的第 0 号字节注入单字节故障的故障传播过程，即该故障最终会影响密文的第 0、7、10、13 号字节.

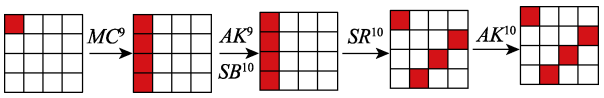


图 7　第 9 轮列混淆输入注入单字节故障传播过程

攻击者利用故障传播过程执行如下的攻击过程：

（1）攻击者遍历 $4\times255=1020$ 个非 0 列混淆单字节输入差分，预计算对应的列混淆输出差分，将 1020 个输出差分存储在输出差分表中，表中每个表项大小均是 4 个字节.

（2）攻击者选取若干明文在正确状态下进行加密，记录每个明文对应的正确密文 C.

（3）攻击者在第 9 轮列混淆输入的某一列注入故障，在故障状态下加密相同的明文记录对应的错误密文 C^*. 若在第一列注入故障，则 C 与 C^* 的第 0、7、10、13 号字节不同. 若在第二列注入故障，则 C 与 C^* 的第 1、4、11、14 号字节不同. 若在第三列注入故障，则 C 与 C^* 的第 2、5、8、15 号字节不同. 若在第四列注入故障，则 C 与 C^* 的第 3、6、9、12 号字节不同. 这 4 个不同的字节位于中间状态的不同列上.

（4）攻击者记录 C 与 C^* 的不同字节的位置 i,j,k,l，遍历最后一轮轮密钥的 4 个字节 RK_i^{10}, $RK_j^{10},RK_k^{10},RK_l^{10}$，共 2^{32} 种可能值，计算公式(17):

$$\begin{cases}\Delta_i = SB^{-1}(C_i \oplus RK_i^{10}) \oplus SB^{-1}(C_i^* \oplus RK_i^{10}) \\ \Delta_j = SB^{-1}(C_j \oplus RK_j^{10}) \oplus SB^{-1}(C_j^* \oplus RK_j^{10}) \\ \Delta_k = SB^{-1}(C_k \oplus RK_k^{10}) \oplus SB^{-1}(C_k^* \oplus RK_k^{10}) \\ \Delta_l = SB^{-1}(C_l \oplus RK_l^{10}) \oplus SB^{-1}(C_l^* \oplus RK_l^{10})\end{cases} \tag{17}$$

若 $(\Delta_i,\Delta_j,\Delta_k,\Delta_l)$ 在输出差分表中，则遍历的 $RK_i^{10},RK_j^{10},RK_k^{10},RK_l^{10}$ 作为候选值. 平均使用 1 对正确密文/错误密文能够得到 1036 个候选值，使用 2 对正确密文/错误密文能够唯一恢复 RK_i^{10}, $RK_j^{10},RK_k^{10},RK_l^{10}$. RK^{10} 的其余 12 个字节仍需 6 对正确密文/错误密文. 在恢复 RK^{10} 后，根据密钥编排算法恢复主密钥.

当在第 8 轮列混淆的输入注入随机单字节故障时，其任意位置的故障会影响第 9 轮列混淆输入的 4 个字节，这 4 个字节位于中间状态的不同列上，最终会影响密文的 16 个字节. 攻击者利用上述攻击方法逐个分析第 9 轮列混淆输入的 4 个字节差分的传播过程，从而恢复每个差分影响的最后一轮轮密钥的 4 个字节，在恢复最后一轮轮密钥后结合密钥编排过程恢复 128 比特主密钥. 由于在第 8 轮列混淆的输入注入随机单字节故障相当于在第 9 轮列混淆的输入注入 4 个单字节故障，因此前者的 1 个故障密文相当于后者的 4 个故障密文，从而减少了使用的故障密文数，增加了注入故障的轮数范围.

随着对 AES 的密码结构与数据依赖关系的研究不断深入，许多密码学者在 AES-128 加密过程的不同位置注入不同类型的故障，选取不同的故障模型，得到了不同的差分故障攻击结果，如表 1 所示：

2.5　侧信道攻击方案对比

Grosso 等人[75]对比了代数侧信道攻击、软分析侧信道攻击和带枚举的差分能量分析攻击三种侧信道攻击方案. 在无噪声模拟环境中，软分析侧信道攻击比代数侧信道攻击更有利于密钥恢复；在实际

表 1　针对 AES-128 的差分故障攻击结果

参考文献	故障类型	故障位置	错误密文数	候选密钥数量
[39]	随机单字节故障	第 8 轮列混淆与第 9 轮列混淆之间	40	1
[43]	随机单字节故障	第 7 轮列混淆与第 8 轮列混淆之间	2	1
[44]	单比特故障	与 RK^0 异或后	128	1
[45]	随机单字节故障	最后一轮输入	50	1
[46]	随机多字节故障	第 8 轮列混淆与第 9 轮列混淆之间	1500	1
[47]	随机多字节故障	第 8 轮列混淆与第 9 轮列混淆之间	1500	1
[48]	随机多字节故障	第 7 轮列混淆与第 8 轮列混淆之间	4	1

的 AES 实现中，软分析侧信道攻击在密钥恢复攻击中需要的能量迹的数量比差分能量分析攻击更少. 利用已知明文攻击可以使用标准的带枚举的差分能量分析攻击. 当攻击未知的明文/密文，或攻击具有抗泄漏的密码原语时，软分析侧信道攻击是最好的选择. 在攻击之后，确定每部分子密钥最有可能的密钥信息，减少密钥空间，采用枚举算法恢复最终密钥，当信息量不够多时，仍需在比较大的密钥空间里寻找密钥.

攻击者需要解决两个问题：密钥在剩下的密钥空间里有多“深”；将密钥枚举到一定深度有多“昂贵”. Martin 等人[76]构造一个高效且能准确计算加密密钥在密钥空间中范围的算法，算法根据侧信道攻击分数对所有已知可能的密钥进行排序，得到最有可能的密钥. 其次给出智能并行密钥枚举算法，以并行方式枚举最有可能的密钥，从而解决了这两个问题.

3 侧信道防御

侧信道防御的难度要远远大于攻击的难度，攻击可以只攻其一点，但是防御要兼顾方方面面. 侧信道防御的关键是阻止攻击者获得有效侧信息，从而增加攻击难度. 针对单一侧信道攻击方法的防御措施有两类思路：第一类思路是去除侧信息的数据依赖性；第二类思路是通过掩盖侧信息，弱化其某些特征，使得攻击者难以分辨和利用. 研究者还需从系统级层面综合应用多种防御措施以达到最优的防御效果.

在去除侧信息的数据依赖性方面，主要有对侧信息进行均衡化、转移侧信息的数据依赖性两种方法. 在掩盖侧信息方面，主要有对侧信息进行随机化、加入噪声或屏蔽隔离技术，降低侧信息的信噪比两种方法.

从系统级层面综合考虑方面，需要考虑多个侧信道防御措技术之间的相互影响. 系统防御主要考虑两个因素：其一，并不是所有密码系统的所有侧信息都能实现防御，其二，一种侧信道防御技术会带来其他的侧信道攻击. 系统防御的目的是权衡各种方案以达到全局最优.

侧信道防御技术可以由硬件、软件或者两者结合实现. 相对来说，软件防御技术具有灵活性、扩展性和成本低的特点，但防御效果有限. 侧信道防御技术的实施，对系统的成本、运行效率等方面会产生一定的影响. 本节主要介绍掩码方案、隐藏方案、软件防御与故障防御方法.

3.1 掩码方案

许多理论上证明安全的密码算法都遭受到了侧信道攻击的威胁. 掩码方案旨在屏蔽加密数据与侧信道泄漏之间的关系，是抵抗能量分析攻击、故障攻击和缓存攻击等侧信道攻击的应用最广泛的对策. 掩码方案的实现如图 8 所示，其中 p 为明文，k 为密钥，m' 与 m'' 是为明文和密钥添加的掩码：

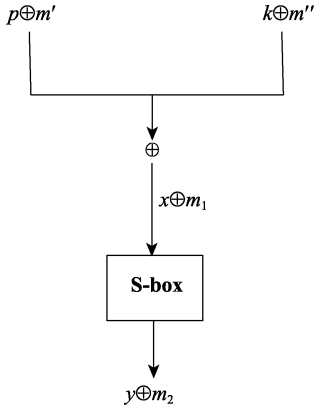


图 8 掩码方案实现

掩码方案研究至今，大致经过了三个阶段：

（1）第一个阶段：1999 年到 2005 年，研究一阶掩码方案；

（2）第二个阶段：2006 年到 2009 年，高阶差分能量分析与高阶掩码方案的研究交替进行.

（3）第三个阶段，2010 年至今，发展轻量化掩码方案.

掩码方案实现主要有三类：

（1）门级别：易受时钟毛刺攻击.

（2）逻辑器件级别：开销较大，实现复杂，需要定制的开发环境.

（3）算法级别：基于查找表、复合域运算或秘密共享的掩码方案.

在明文和密钥相同的条件下，掩码方案与密码算法输出相同的密文. 但掩码方案在与明文和密钥有关的运算中执行掩码操作，使得密码设备执行时泄露的侧信息不与密钥直接相关，从而增加了侧信道攻击的难度. 掩码方案是算法层面的防护技术，具有实现简单和成本低廉的特点. 此外，掩码方案具有可证明安全性：$n+1$ 阶掩码方案能够抵抗 n 阶侧信道攻击.

3.1.1 掩码方案的随机性

掩码方案随机化敏感变量，使得来自设备的物理泄漏难以利用，但一些在资源受限的环境下实现掩码方案的设备仍可能存在一些一阶泄漏. Chen 等

人[77]对两种轻量级分组密码 SIMON 与 PRESENT 给出了第一个双方共享门限实现. 门限实现是一种硬件实现的掩码方案，通过仿真对实际结果进行分析，结果表明该方案完美的抗一阶泄漏，强抗二阶泄漏. Moradi 等人[78]研究低延迟设备抗侧信道攻击的安全性，对轻量级分组密码 PRINCE 与 Midori 进行了抗侧信道攻击的分析，并给出了几种低延迟设计架构，此架构可通过掩码和门限方案来抵抗一阶泄漏.

随机性是每一个安全的掩码方案重要组成部分，但实际中产生随机性的代价很高（需要伪随机数生成器 Pseudo Random Number Henerator, PRNG 或真随机数生成器 True Random Number Generator, TRNG），是否可以降低需要的随机性且仍然保证安全性是研究的一个主题. Faust 等人[79]研究掩码方案的内部组件是否可以重复利用随机数，从而降低需要的随机性的总量，同时提出了一个新的掩码算法，可以大量减少所需要的随机性数量且比已知构造更加高效. Balasch 等人[80]提出了降低所需的随机性的新算法，提高了内积掩码方案的效率，在 t 探测模型中具有安全性，并在 ARM 微处理器上进行实现. Belaïd 等人[81]给出了用于掩码方案的两种有限域上隐私乘法算法，这两种算法在双线性乘法和随机掩码方面分别具有最低的复杂度. 两种算法的缺点是它们安全实例取决于满足一定条件的矩阵，限制了构造的实用性. Karpman 等人[82]在此基础上利用代数方法、启发式方法以及实验方法找到算法的更多安全实例，扩展了算法的使用范围.

3.1.2　掩码方案的编码函数

掩码方案中的另一个核心成分是其编码函数，核心思想是用固定的汉明权重对敏感数据进行编码，适用于所有泄漏内部变量汉明重量的设备. 许多掩码方案基于布尔编码，算术掩码. 对于将布尔运算与算术运算相结合的密码算法，必须在布尔掩码和算术掩码之间进行转换. Goubin 等人[83]描述了一种只需要常数次操作，就可以将布尔掩码转换为算术掩码的算法. Goubin 还描述了一种从算术掩码转换到布尔掩码的算法，需要使用 $O(k)$ 次操作，其中 k 是加法比特规模. Coron 等人[84]描述了一种仅具有时间复杂度 $O(\log k)$ 的改进算法，新算法基于 Kogge-Stone 带进位的超前加法器，在 $O(\log k)$ 操作内计算出进位信号，而经典纹波进位加法器需要在 $O(k)$ 操作内计算出进位信号. Maghrebi 等人[85]给出了一个框架，根据分析的泄漏模型构造定制的编码函数，利用物理泄漏知识来选择相应的最佳编码方案，将侧信道泄漏最小化. 该方案可应用于保护轻量级分组密码 PRESENT 的 S 盒，实验证实了方案的实用性. Bhasin 等人[86]在微控制器的模拟和实际设置中评估定制编码的安全性. 在模拟设置中，Bhasin 等人验证了定制编码在正确的泄漏估计和噪声方差假设下具有强大的安全性. 然而在实际设置中，Bhasin 等人将定制编码在 8 位 AVR 和 32 位 ARM 微控制器中进行实现，但实现方案存在侧信道泄漏，说明了该方法的不足.

3.1.3　掩码方案的安全性

为了证明设计的掩码方案在理论上具有安全性，首先需要定义安全模型. 2003 年，Ishai、Sahai 和 Wagner[87]引入了一个正式的安全模型：t 探测模型，在此模型下可以证明许多小型掩码组件具有安全性，但是掩码组件的组合是否具有安全性仍在研究中. 直到 2016 年，Barthe 等人[88]提出 maskComp 工具，maskComp 是一种检查由多个掩码组件组成的掩码方案的安全性的工具，通过在精心选择的位置插入掩码刷新组件，利用紧共享数来实现可证明安全性. 但该方法并不严格，其存在一些组件无法表现出缺陷或无法证明其安全性的问题. 因此可能需要插入比确保 t 探测安全实际所需更多的刷新组件. Belaïd 等人[89]给出了一个新的工具：tightPROVE，用于证明由标准组件组成的共享电路是否是 t 探测安全的. 基于此要么产生探测安全性证明（在任何顺序上都是有效的），要么表现出安全隐患，直接暗示着在给定顺序下的探测攻击. 与 maskComp 相比，tightPROVE 可以大大减少所需的刷新组件的数量，达到探测安全性需求，从而可以降低某些安全共享电路的随机性要求. 即使密码设备使用掩码方案进行保护，高阶侧信道攻击也可以攻破这样的密码设备.

具有掩码方案的设备有较好的编码函数和无偏差的编码，可以消除一阶泄漏，但对于二阶或者高阶泄漏仍然是易受到攻击的. Bruneau 等人[90]给出了用于高阶掩码的最佳区分器：高阶最优区分器，分析了二阶区分器和区分器在掩码表中的应用. 通常认为高阶掩码方案是分组密码实现中抵抗侧信道攻击的可靠方案. 2015 年，Barthe 等人[91]研究了基于程序验证技术的高阶掩码的自动验证问题. 布尔掩码简单易实现，性能开销小，在具有更高代数复杂度时可以提供更强安全性，但是此时性能开销大；而内积掩码在安全参数大时可以保证定义域抗泄漏的安全性，并且是可实现的. Balasch 等人[92]平衡了安全性和效率，提出了变形的内积掩码，并在探测

模型下证明了其安全性. 2017 年，Goudarzi 等人[93]在 ARM 上研究高效的高阶掩码方案：首先研究在分配级别的域上乘法的实现；然后研究 ISW（Ishai-Sahai-Wagner）方案以及 CPRR（Coron-Prouff-Rivain-Roche）方案的实现；最后提出改进后的最优的多项式分解方法，用于各种参数的 S 盒，并给出 AES 和 PRESENT 的更快的按比特的掩码方案的实现. 2018 年，Barthe 等人[94]在 ISW 模型下，构造了基于格的GLP签名方案的可证明安全的掩码实现，这是第一个基于格的签名算法的掩码方案. Bloem 等人[95]提出了研究掩码硬件实现安全性的形式化验证方法，并考虑到了硬件故障对掩码的安全性影响.

掩码方案在白盒原语中也发挥着作用. 在黑盒模型中，攻击者只能访问密码原语的输入和输出. 在白盒模型中，攻击者可以完全访问内部实现，通常攻击者可以同时使用静态分析，动态分析以及故障分析等方法来破解密码系统，例如提取嵌入式系统中的密钥等. 为了防止差分计算分析攻击，Biryukov 等人[96]提出了利用掩码方案抵抗白盒实现的攻击，推断出任何安全的白盒实现都必须满足的约束，基于这种约束，给出了一种保护白盒实现的通用方法，该方法包括两个独立的组件：值隐藏和结构隐藏. 值隐藏保护防止依赖于计算迹分析的被动差分计算分析攻击，结构隐藏提供对电路分析攻击的保护.

掩码方案对密码系统抵抗侧信道攻击是十分重要的，可以阻止对嵌入式系统的侧信道攻击. 然而在掩码方案实现之前，检测其是否有缺陷同样重要. 由于安全验证过程是一个冗长、乏味、手动的过程，因此 Reparaz 等人[97]给出了一种在设备上实现掩码方案之前，验证其可靠性的方法. Reparaz 的方法利用泄漏检测技术对掩码方案的实现进行检测，系统设计者可以在设计时序快速评估掩码方案之前检查其是否存在缺陷，因此可以在设计的早期阶段使用. 在有限计算资源的情况下，该方法可以在几秒钟内以自动化的方式发现方案中的缺陷，因此对检验在硬件上实现的掩码方案具有一定的参考价值.

3.2 隐藏方案

隐藏对策的目的是隐藏电路引起的侧信道泄漏，不仅要控制侧信道泄漏的幅度（垂直方向），而且要调整侧信道泄漏的位置（水平方向）. 垂直隐藏包括随机化方法以及均匀化方法. 随机化方法使泄漏模式看起来不同从而难以检测，均匀化方法使泄漏模式看起来相似从而难以分析. 水平隐藏本质上是泄漏去同步，目的在于使泄漏发生在不同的时间段.

3.2.1 垂直隐藏

垂直隐藏包括随机化方法与均匀化方法. 随机化方法旨在通过从加密到加密产生不同的泄漏模式（例如能量/电磁）来迷惑敌手. 包括随机复用两个不同的 S-Box[98]、动态电压频率缩放（Dynamic Voltage Frequency Scaling, DVFS）[99]、注入噪声[100]、控制流量数据[101]等. 均匀化方法旨在通过从加密到加密产生类似的泄漏模式来掩盖泄漏. 这可以在系统、模块和逻辑级别上实现. 系统级别的实现包括通过低压差线性稳压器[102]、感应电压控制器[103]和电流均衡器[104]来调节功率/电压. 模块级别的实现包括引入功率平衡的 S-box [105] 或复制 AES 子系统和 S-Box[106]以均匀化能量/电磁泄漏. 电路级别的实现包括采用各种开关平衡逻辑样式，如相位逻辑[107] 和时间封闭逻辑[108].

3.2.2 水平隐藏

水平隐藏的本质是使泄漏去同步，使得泄漏模式难以对齐. 一种方法是利用同步逻辑，通过随机移动时钟、插入虚拟操作或通过 DVFS 调整时钟延迟变化. 另一种方法使用基于捆绑数据[109]或自检测[110]的异步逻辑方法. 延迟变化不是周期性时钟采样而是任意自定时间，因此具有一定的局限性. 为了实现更高程度的去同步，自检测方法是首选，因为其利用细粒度的数据驱动电压-温度感知（Process Voltage-Temperature（PVT））进行去同步.

异步逻辑通过异步执行加密硬件，可以同时实现垂直和水平隐藏. 2015 年，Chong 等人[111]证明了重置操作可能会泄漏异步逻辑 S 盒中的密钥，异步逻辑设计可能无法按预期工作. 这是因为触发器往往会在正/负时钟边缘泄漏密钥，而异步逻辑设计中，在下一次操作之前一些内部信号仍然必须同步，因此很可能存在泄漏. 2019 年，Chong 等人[112]提供了一种异步逻辑设计和异步逻辑库单元，并评估它们对许多不同攻击假设模型的侧信道攻击抵抗能力. 2021 年，Chong 等人[113]提出了一种具有相对定时的双轨异步逻辑设计流程，以简化 AES 在 FPGA 中的实现，并利用异步逻辑操作插入随机延迟线控制和数据传播控制来提高侧信道防御能力，最后在 Sakura-X 和 Arty-A7 两个 FPGA 平台上验证了其提出的双隐藏异步逻辑 AES 加速器.

3.3 软件防御

由于密码算法在执行过程中会泄漏一定的信息，设计者可以在软件或协议上做一些更改，从而

降低密码算法实现过程中的信息的泄漏，这也是一种抵抗侧信道攻击方式. 比如构造时序侧信道来攻击 AWS Labs 发布的 s2n 库中的 MEE-CBC（MAC then Encode then CBC Encrypt）组件来获得侧信息泄漏. 虽然只能在单独使用 MEE-CBC 组件时才能发起这种攻击，但 Albrecht 和 Paterson 证实，s2n 的第二道防线一旦得到加强，就能够降低当前攻击者的能力，进一步证明了传统软件在安全性的研究和验证中并不有效. 为了解决这个问题，Almeida 等人[114]定义了一种存在时序攻击者的情况下证明安全性的方法：首先证明密码构造算法描述的黑盒安全性，然后根据算法描述建立实现功能的正确性，最后证明该实现是泄漏安全的. 同时，Almeida 等人提出了基于 MEE-CBC 的概念验证应用，将形式化验证工具结合在一起，抵抗可以获得时序泄漏的攻击者，且具有可证明安全性，为部署在 OpenSSL 中抵抗时序攻击的对策提供了第一个可证明安全验证.

白盒密码的安全性是指在白盒模型中分析密码算法的安全性，其中攻击者可以完全访问执行环境. 在这种情况下获得安全性是一个具有挑战性的问题. 迄今为止，所有已发布的标准对称密码算法（如 AES）的白盒实现都已被破坏. 但是实际产品中的白盒实现没有受到密钥恢复攻击，这是因为商业产品在白盒实现之上部署了额外的软件保护机制，使得攻击在实际应用中不可行. 有许多软件保护机制可以防止标准的白盒攻击，其一是控制流混淆，使得每次执行白盒加密模块时，表的查找顺序随机化；其二是随机化存储器地址空间中各种查找表（Lookup Table, LUT）的位置. Banik 等人[115]研究了抵抗差分计算分析攻击和零差分枚举攻击的有效对策. 差分计算分析攻击由 Bos 等人[116]在 2016 年 CHES 会议中提出. 这种攻击收集几个明文加密的软件执行踪迹，并利用收集的数据执行差分能量分析攻击来恢复密钥，当泄漏了足够的信息可以进行能量攻击. 零差分枚举攻击攻击记录了几对可选择的明文的软件踪迹，并对踪迹进行有效差分，进行简单的统计测试以提取密钥. 为了防止这两种攻击，除了控制流混淆之外，Banik 等人还要将 LUT 的位置随机化到存储器中，使得在系统上执行差分计算分析攻击并且在合理的时间内提取密钥是非常困难的. 同时，Banik 等人提出了一种基于插入随机延迟来保护白盒二进制文件的新对策，在泄漏给攻击者的信息中添加随机噪声来使零差分枚举攻击和差分计算分析攻击变得困难.

3.4　故障防御技术

双模块冗余（Dual Modular Redundancy，DMR）是一种使用两个模块来防御故障攻击的机制[117]，其中一个模块用于加密，另一个模块用于错误检测. DMR 具有可靠性、安全性的特点，提升了密码系统的鲁棒性，目前已被许多商业解决方案采用.

若 DMR 使用的两个模块执行相同的加密算法，则称其为基于冗余加密的双模块冗余（Redundant Encryption Based Dual Modular Redundancy，REDMR）. 如图 9 所示.

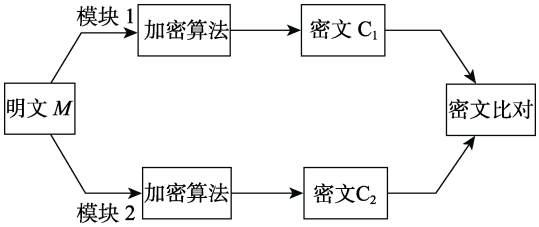


图 9　基于冗余加密的双模块冗余

若两个模块加密得到的密文结果相同，则输出密文结果，即通过了 REDMR 的安全性检查. 若密文结果不同，则无输出、输出随机值或输出全 0 值. 对于攻击者注入单个故障的情况，REDMR 具有良好的防御能力. 攻击者为了打破 REDMR 安全性，则需在两个模块注入相同的故障或者绕过安全性检查. 若两个模块采用共享内存的方式实现，则 REDMR 的防御能力失效.

若 DMR 使用的模块 1 执行加密算法，模块 2 执行对应的解密算法，则称其为基于逆向解密的双模块冗余（Inversive Decryption Based Dual Modular Redundancy，IDDMR）. 如图 10 所示：

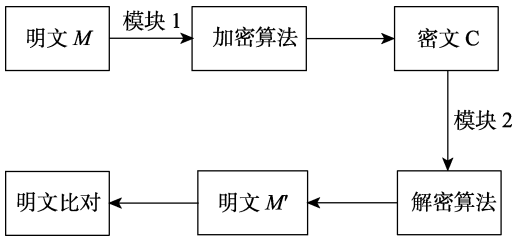


图 10　基于逆向解密的双模块冗余

若解密算法得到的明文结果与原始明文相同，则输出密文，即通过了 IDDMR 的安全性检查. 若明文结果不同，则无输出、输出随机值或输出全 0 值. 由于两个模块执行不同的操作，在不同的内存单元中实现，为攻击者注入故障增加了难度. IDDMR 的防御能力强于 REDMR.

4 抗泄漏密码学

2004 年, Micali 等人[118]提出了抗泄漏密码学的概念. 在此框架下，攻击者可以适应性的获取部分泄漏信息. 抗泄漏密码学的提出是为了量化密码算法执行过程中的侧信道泄漏，其主要研究两方面问题，其一是如何准确给出密码系统的信息泄漏量，其二是如何构造抗泄漏安全性的密码方案.

4.1 信息泄漏量

如何完整地评估一个系统在不同侧信道攻击下的脆弱性/容忍度是个很重要的问题. 合理的量化指标可以用来知道对策的实现难度，也能公平的比较不同对策的强度.

Zhang 等人[119]提出了一个新的统一指标信息泄漏量（Information Leakage Amount, ILA）来量化密码算法和软件代码各种能量攻击下的信息泄漏，该指标适用于未受保护的密文和受掩码保护的密文. 理论研究的抗泄漏隐藏和具体的侧信道安全估计之间是相对独立的.

Duc 等人[120]利用统计距离、互信息度量、信噪比等工具与掩码对策的形式化分析以及侧信道密钥恢复攻击评估框架联系起来，给出了基于互信息度量的掩码对策的相关证明，该理论能够在物理安全评估中使用. 此外，Duc 等人通过实验推测了互信息度量与敌手成功率之间的联系，并给出使用非独立泄漏进行掩码可以提高密码设备安全级别的结论. 该研究将最坏情况下的侧信道评估问题转化为评估单个指标的挑战，从而大大减少了认证机构的评估成本.

Bogdanov 等人[121]研究了攻击者能力逐渐增强的情况下，AES 在具有泄漏的情况下的安全性；同时提出了几种新的密码分析方法（如差分偏差攻击）用于有泄漏的情况下恢复密钥. 结果表明，在具有不确定性或基本对策下，具有一定泄漏的 AES 的安全性仍是可观的.

4.2 抗泄漏密码方案

密码学家研究抗泄漏密码学的同时，一些满足抗泄漏安全性的方案也随之产生. 抗泄漏是指在一定泄漏模型下（计算模型，有界泄漏模型，无界泄漏模型和连续泄漏模型等），假设攻击者得到部分信息，设备仍然是安全的. 在此框架下，许多抗泄漏密码方案相继被提出，如公钥加密[122-126]、数字签名[125-126]、身份基加密[126-127]、消息编码[128-130]和伪随机生成器[122, 123]等.

在公钥加密与数字签名方面，Dachman-Soled 等人[122]用不可区分混淆（Indistinguishability Obfuscation, iO）构造了抗泄漏的公钥加密方案；Hajiabadi 等人[123]利用同态哈希证明系统（Homomorphic Hash Proof System, HHPS）给出了同时满足抗泄漏和 KDM 安全的公钥加密方案. Faonio 等人[124]给出了抗有界泄漏与内存篡改攻击标准模型下的公钥加密与数字签名方案. Fujisaki 等人[125]给出了第一个选择密文攻击安全（Chosen-Ciphertext Attack, CCA）抵抗连续任意函数篡改的公钥加密方案，且有高效的实例，并证明了在更强的连续篡改变种攻击下，不存在抵抗任意函数篡改的安全的数字签名方案.

在身份基加密方面，Barwell 等人[126]给出了利用抗泄漏伪随机函数，构造防误用与防泄漏的认证加密方案，并提出了一个基于配对的抗泄漏认证加密方案具体实现. Nishimaki 等人[127]用基于身份的哈希证明系统（Identity-Based Hash Proof Systems, IB-HPS）构造有界检索模型（Bounded Retrieval Model, BRM）下的抗泄漏公钥加密方案与基于身份的加密.

在消息编码方面，Faonio 等人[128]用 Diffie-Hellman 假设构造了抗泄漏的不可延展的消息编码并给出了应用；Dachman-Soled 等人[129]给出了可本地解码与更新的不可延展编码满足抗泄漏的上界与下界. Chen 等人[130]给出了一个在有界泄漏模型下利用可穿透组件与 iO 构造泄漏容忍系统的框架.

在伪随机生成器方面，Faust 等人[131]提出了通用的随机存取存储器（Random Access Memory, RAM）抗篡改和抗泄漏计算框架；Medwed 等人[132]提出了一种抗泄漏伪随机函数，利用带未知输入的分组密码并行实现.

5 前沿技术展望

5.1 深度学习技术的应用

深度学习自产生以来，在能量分析攻击中得到了广泛应用. 这是因为深度学习技术可以解决能量分析的两个重点问题：其一是特征点的选择，如何使尽可能少的特征点包含尽可能多的信息，以提高计算效率；其二是区分器的选择，即构建从侧信息泄漏到正确密钥模型的能力. 主成分分析和线性判别分析等降维方法[26]可以精确高效地选择特征点，解决了第一个问题；多层感知机（Multilayer Perceptron, MLP）、卷积神经网络（Convolutional Neural Networks, CNN）和残差网络（Residual Network, ResNet）等神经网络[27,28]可以通过训练逼

近最优区分器，从而解决了第二个问题. 此外，由于现实因素影响，侧信道攻击所利用的侧信息数据会伴有一定噪声. 因为神经网络的设计依赖于数据，而不依赖于噪声的概率分布，所以对不同强度和不同类型的噪声具有一定的鲁棒性. 因此深度学习技术在侧信道攻击和防御的降噪方面也有应用[37,74,86,116].

2013 年，Martinasek 等人[133]使用单隐藏层全连接网络攻击了 PIC16F84 单片机上软件实现的 AES 算法. 该网络结构如图 11 所示，输入层维数为单条能量曲线维数 12000，含有一个节点数为 100 的隐藏层，输出层包含 256 个节点，对应 256 个候选密钥的概率. 单条能量曲线的攻击成功率为 85.23%. 同年，Martinasek 等人对之前的数据集，采用计算所有能量曲线的均值，然后每条能量曲线减去这个均值的方法进行预处理，使用同样的神经网络结构，将攻击的成功率提升到了 94.57%.

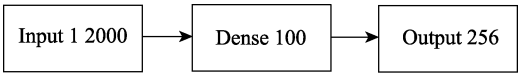


图 11　单隐藏层神经网络结构

2015 年，Martinasek 等人[134]攻击了掩码防护的 AES 软件实现数据集 DPA Contest V4，先使用多层感知机恢复了循环掩码方案中的掩码偏移量，然后使用 DPA 恢复了密钥值. 恢复掩码偏移量的神经网络结构如图 12 所示，神经网络的输入值是 48 个通过计算相关系数得到的与掩码值相关的特征点，中间是一个 1000 节点的隐藏层，输出层包含 16 个节点，对应 16 个掩码偏移量的概率. 在攻击阶段一条能量曲线恢复掩码偏移量的概率是 99.7%，最多需要 20 条能量曲线即可使用 DPA 恢复全部密钥.

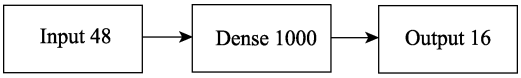


图 12　恢复掩码偏移量的神经网络结构

2016 年，Maghrebi 等人[135]攻击了 FPGA 上实现的无防护 AES 数据集 DPA Contest V2 和 ChipWhisperer-Capture Rev2 上实现的一阶掩码防护 AES. 在攻击中对比了模板攻击、RF、MLP、卷积神经网络、自编码器（Auto-Encoder，AE）、长短时记忆网络（Long Short Term Memory Network, LSTM）等方法，评价标准是每种方法成功恢复密钥所需的平均能量曲线数目，结果证实了深度学习方法在攻击无防护和掩码防护 AES 算法时的优越性. 其中 MLP 和 CNN 的网络结构如图 13 和图 14 所示. 其中神经网络的输入值是能量曲线预处理后的采样点数量，不是一个定值，CNN 由两个卷积层，一个池化层和一个全连接层组成.

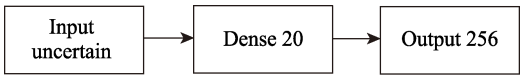


图 13　Maghrebi 的 MLP 网络结构

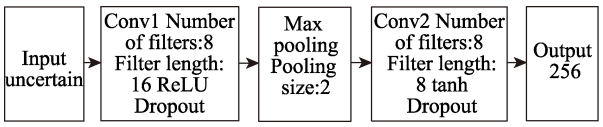


图 14　Maghrebi 的 CNN 网络结构

2017 年，Cagli 等人[136]攻击了 Atmega328P 上软件实现的和 90nm 智能卡上硬件实现的带随机时延中断（Random Delay Interruption，RDI）防护的 AES 算法. 使用了 CNN 结构进行攻击，结果表明 CNN 可以直接攻击未对齐的能量曲线，表现出其他攻击方法没有的攻击效果. 其使用的 CNN 结构如图 15 所示，包含 4 个卷积层、4 个池化层和 1 个全连接层.

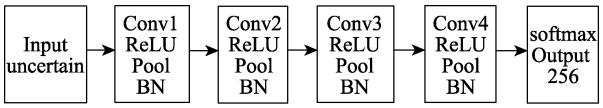


图 15　Cagli 的 CNN 结构

2018 年，Picek 等人[137]在 DPA Contest V2 和 DPA Contest V4 数据集上比较了 CNN 和机器学习方法的性能，指出在低噪声无预处理情况下 CNN 的表现更好，但是在其他情况下机器学习模型计算量更小，性能与 CNN 相似甚至更好. 因此 CNN 在某些情况下没有比较大的优势，不一定是必选的方法. 采用的 CNN 结构如图 16 所示，由于采用汉明重量模型，最终输出为 9 个汉明重量的概率值.

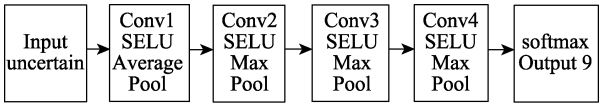


图 16　Picek 的 CNN 结构

2018 年，Benadjila 等人[138]攻击了掩码防护 AES 实现的 ASCAD 数据集，具体展现了 MLP 和 CNN 网络结构选择和超参数调整的过程，公开了数据集和源码. 最好的 MLP 和 CNN 模型命名为 MLP_best 和 CNN_best，网络结构如图 17 和图 18 所示.

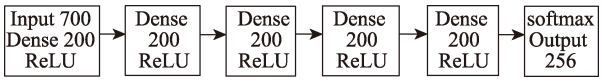


图 17 Benadjila 提出的 MLP_best 结构

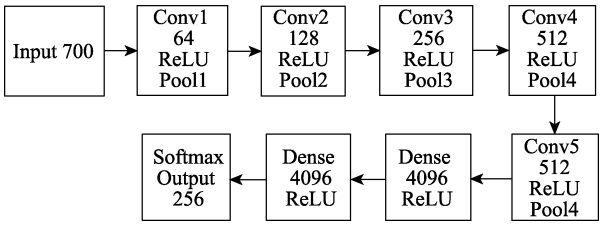


图 18 Benadjila 提出的 CNN_best 结构

2019 年，Kim 等人[139]在输入能量曲线中加入人工噪声来提高神经网络的性能. 这种噪声的加入相当于目标函数中的正则项. 通过使用这种技术，攻击者可以将神经网络恢复密钥所需的能量曲线减少几个数量级[140]. 同年，杨光等人使用短时傅里叶变换（Short-time Fourier Transform，STFT）将单条能量曲线从 1 维数据转换成 2 维数据，使 CNN 的输入包含泄露的时域信息，使用转换后的能量曲线进行攻击，提高了 CNN 攻击的效率与成功率.

2020 年，Gabriel 等人[141]针对 CNN 的超参数选择问题，利用一些特定的可视化技术（包括权重可视化、梯度可视化和热力图）以解释每个超参数在特征选择阶段的作用，并以此为基础提出了在去同步的情况下构建高效 CNN 的方法. Gabriel 在去同步和未去同步的公共数据集上验证，结果表明其模型优于以前最先进的 CNN 模型，同时降低了网络复杂性.

2021 年，Jorai 等人[142]使用强化学习来调整卷积神经网络的超参数，具体工作是设计了以猜测熵和准确率为标准的两个奖励函数，并利用 Q-Learnings 算法调整网络的超参数. Jorai 等人对三个常用数据集（ASCAD 数据集的固定密钥版本和随机密钥版本，CHES CTF 数据集）和两个泄漏模型（汉明泄露模型，身份泄露模型）进行验证，结果表明强化学习可以在训练少量参数的情况下找到表现出最佳性能的卷积神经网络.

5.2 云环境上的侧信道攻击

随着移动互联网、物联网等技术的兴起，数据的种类和规模正在以前所未有的速度不断增长. 在大数据时代下快速处理海量数据成为用户共有的需求，为此云环境应运而生，为构建大数据服务提供了强大的技术支撑[143]. 随着越来越多的敏感信息被集中存储到云端，数据的安全性与云环境的安全性息息相关. 云环境具有平台开放、服务外包和多租户资源共享等特征，任何合法用户都可以通过网络接入云环境，云环境面临来自内部和外部的各种攻击. 为了保证云端数据的安全性，行之有效的方法是对敏感数据进行加密后存储到云中[144].

然而，云环境上共享的资源为侧信道攻击提供了条件. 侧信道攻击给云环境上加密系统的安全性带来了严重考验，例如 OpenSSL 密码算法库的“心脏滴血”漏洞，以及高速缓存、熔断和幽灵等微体系结构侧信道攻击等. 与传统密码分析技术不同，密码实现面临的安全威胁呈现多样化（故障、微体系结构和 Rowhammer 等）和实用化（云环境、浏览器、移动终端等导致的跨用户、跨安全域的资源共享）的安全趋势，因此更加难以应对和防范. 云环境产生的经济效益从根本上基于硬件共享，以缓存攻击为例，随着每个处理器中内核数量的增加，共享资源也可能增加，因此通过基于减少共享这种最简单防御措施是不可能实现的. 最初，缓存攻击者将攻击目标设定为硬件线程的平台上共享的 L1 缓存[4]，但随着 L1 和 L2 缓存被设置为内核专用，攻击者将目标转移到共享的 LLC 缓存[5-6]. 尽管 Intel 在推出 Skylake-X CPU 时使用非包容性缓存结构以防范缓存攻击，但仍有工作通过逆向其目录结构而设计出针对 LLC 的缓存攻击. 由于 CPU 等硬件设施在部署之后难以更改，因此在未来的一段时间里，LLC 仍会是攻击者的主要目标，攻击者需要针对不同处理器的微体系结构设计缓存攻击.

5.3 针对后量子密码体制的侧信道攻击

为了抵抗量子计算机对 RSA 和 ElGamal 等传统公钥密码带来的灾难性影响，NIST 于 2017 年发起了一场针对数字签名、公钥加密和密钥封装机制的量子安全公钥密码系统的算法征集[19]，并于 2020 年 7 月 22 日公布了通过了第二轮的 7 个入围方案和 8 个候选方案. 于同一时期，中国密码管理局委托中国密码学会举办了后量子密码算法竞赛的征集，这是中国后量子密码算法标准制定的预赛. 传统的基于 RSA 和 ECC 的算法的实现容易受到侧信道攻击和故障攻击的威胁，后量子算法具有潜在的抗量子计算机攻击的特性，其依赖的数学问题和代数结构与 RSA 和 ECC 具有较大的区别，具有不同的侧信道安全性. 如果后量子密码算法的实现不安全，则能够抵抗量子计算机破译的密码算法甚至能够被经典计算机轻松攻破，因此亟需研究后量子密码算法的侧信道安全性问题. 后量子密码算法具有区别于传统密码算法的特点，例如基于格构造的方案需要从某个离散高斯分布中提取格点，基于编码的方案

往往需要实现有限域上的乘法，部分实现采用查表的方法加速此计算过程，容易受到存在侧信道泄露.

2016 年，Groot 等人[145]提出了针对 BLISS 签名方案的 Flush+Reload 攻击. 由于 BLISS 签名方案使用恒定时间累积分布表（Constant-time cumulative distribution table, CDT）实现高斯采样器，而 CDT 采样器占用了大量的内存空间，因此攻击者可以通过观察缓存的访问情况以确定签名的部分系数，并以此构建方程，这样就将密钥的恢复转化为一个格问题，利用 LLL 算法即可求解. 在完美侧信道环境中，对 CDT 的攻击需要观察 441 次 BLISS 签名并以 0.66 的概率恢复密钥；在真实环境中，对 CDT 的攻击需要观察 3294 次 BLISS 签名并以 0.88 的概率恢复密钥. 此外，Groot 等人针对伯努利采样器进行攻击，在观察 1671 次 BLISS 签名后，成功的概率达到 1.0. 最后，Groot 等人说明 Knuth-Yao 和 Ziggurath 采样器同样存在缓存泄露，使用这两种方法的签名方案亦有受到缓存攻击的可能.

2020 年，Huang 等人[23]将垂直相关功率分析、水平深度相关功率分析、在线模板攻击和选择输入简单功率分析应用于 NTRU Prime 的 3 种实现，分别是参考实现、使用 DSP 指令优化的实现和受保护的实现. 他们的攻击目标是使用恒定时间算法实现的多项式乘法，并在基于 Cortex-M4 的 STM32F3 和 STM32F4 微控制器上进行了实验. Huang 等人证明敌手只需要观察一天能量迹就可以从多项式乘法中恢复私钥，并且水平深度相关功率分析和在线模板攻击还能够从 NTRU LPRime 的密钥生成中恢复种子密钥. 此外，Huang 等人说明即使 NTRU Prime 使用 Karatsuba 的方法优化其多项式乘法，那么相关功率分析仍然有效. 这是因为 Karatsuba 的方法本身并没有阻止 VCPA、OTA 和 CISPA 进行最低级别的乘法. 如果低水平的教科书乘法足够长，那么 HIDCPA 也可以工作.

2021 年，Gellersen 等人[18]通过分析 Picnic 签名方案核心组件 MPC-LowMC，并利用 MPC-LowMC 在秘密共享过程和 S 盒加密过程的侧信息泄露，首次实现了对 Picnic 签名方案的差分能量分析. Gellersen 等人在 FRDM-K66F 开发板采集 Picnic 签名方案运行时电磁辐射，并利用约 30 条能量迹即可恢复 Picnic 的密钥.

2020 年，针对多变量后量子签名方案 LUOV 的恒定时间 AVX2 优化实现，Mus 等人[74]提出 QuantumHammer 故障攻击技术. QuantumHammer 技术通过注入错误、收集错误的签名并利用分而治之的思想进行攻击. 这些故障是通过 Rowhammer 攻击使用现实的纯软件方法实现的. 此外，Mus 等人提出 QuantumHammer 攻击适用于 LUOV 方案的所有变体.

2021 年，Pessl 等人[146]针对 Kyber 密钥封装机制提出了故障攻击，其以解码过程为目标，跳过解码器中的一条指令，然后观察此故障是否造成解码错误并导致重新加密（有效故障），或者尽管注入了故障但仍然计算出正确的明文（无效故障）. 这一单比特信息可用于构建密钥的方程，在给定足够多的不等式的情况下，攻击者可以恢复密钥. 在模逆环境下，攻击者需要观察到 6,500 次错误解密方能恢复 Kyber512 的完整密钥；在实际环境中，Pessl 等人对运行在 Cortex M4 上的 Kyber512 算法进行了攻击实验，结果表明，攻击者需要观察 60,000—12,500 次错误解密方能恢复完整密钥.

虽然对后量子密码算法的侧信道攻击已取得很多成果，但还有大部分算法的安全性并没有被讨论，尤其是 NIST 后量子密码标准化项目第三轮入围及候选算法的侧信道安全性仍值得进一步研究. 此外，另一个重要的问题在于如何提高侧信道攻击的准确率与效率. 一方面，通过侧信道泄露的密钥信息往往是不完整的、包含噪音的，这导致攻击需要更大数据量和计算量. 另一方面，通过格基约化算法求解也是攻击中重要的一环，所选取的格基和参数影响到攻击的成功率与效率. 因此如何提升侧信道攻击的精确度和优化格基约化算法的参数是进一步研究的重要方向.

5.4　侧信道防御技术展望

侧信道防御的挑战在于难以设计出一个通用的框架来防御所有的攻击，侧信道防御技术通过在根源上消除侧信息泄漏、修改电路设计，增加噪声，使得侧信息少泄漏、加入掩码使得侧信息泄漏与运算无关、或者使用分级防御技术，使得攻击者无法利用有限的侧信息泄露恢复出关键的秘密信息. 密码系统的实现需要电路技术、密码算法、密码协议和密码应用等多个层次相辅相成. 因此，密码系统的安全性需要各个抽象层次的安全性来保证. 目前，针对单个抽象层次的防御技术发展迅速，但是缺少将几种防御技术相结合的通用框架，不能保证防御对策对种类繁多的侧信道攻击方法都是有效的. 侧信道防御技术的可复合性和有效性是重要的研究方向.

侧信道防御的只能限制具有一定条件的攻击者. 不可避免的，防御者必须从经济的角度考虑安

全问题. 因此，在安全芯片密码检测准则[147]中将安全等级分为 3 级，不同安全等级对时序攻击、能量分析攻击、电磁攻击、光攻击和故障攻击具有不同的防护能力. 用户需要根据信息的重要程度来选择防御等级. 安全与效率的权衡，依旧是侧信道防御技术的主旋律.

6 总 结

本文系统地介绍了侧信道攻击与防御技术发展，剖析了能量分析攻击，缓存攻击和故障攻击的基本原理、攻击方法、应用场景和发展现状，并提炼出每一类攻击的通用模型，然后指出了侧信道防御技术的本质特征，并分析了侧信道防御技术的基本原理、安全模型和应用场景，最后总结了抗泄漏密码学的基本原理与发展现状，梳理了抗泄漏密码方案.

侧信道攻击技术主要包括时序攻击、能量分析攻击、缓存攻击和故障攻击. 时序攻击是最早提出的侧信道攻击，主要利用了非对称密码体制实现的时间泄漏来破解密钥. 表面上看，恒定时间的加密算法足以一劳永逸的解决此问题. 但一些工作表明，要想真正实现恒定时间算法，就不仅要保证相同顺序、数量和类型的字段操作，而且要保证调用的所有子算法都是恒定时间实现的.

缓存攻击主要分为针对非对称密码体制的指令追踪和针对对称密码的数据追踪. 指令追踪可以视为利用缓存泄漏的时序攻击，即利用缓存访问信息推断时序，进而破解密钥. RSA,（EC）DSA,（EC）DH 等算法调用的加法、乘法或者平方操作如果与密钥相关，那么攻击者很有可能通过缓存攻击破解整个密钥. 数据追踪则利用了 S 盒存储大小大于缓存行大小这一事实. 当 S 盒存储于多个缓存行时，用户对 S 盒的访问将泄漏部分比特信息. 现有 CPU 的缓存行大小是 64 字节或 128 字节，AES、SM4 和 AREA 等具有 8 比特 S 盒的分组密码都难以抵抗缓存攻击，而轻量级分组密码算法大多具有 4 比特 S 盒，因此不会受到缓存攻击的威胁. 针对指令追踪的缓存攻击，；针对数据追踪的缓存攻击，消除缓存泄漏的根本方法有两个，其一是增加 CPU 的缓存行大小，其二是使用轻量级分组密码算法.

能量分析攻击主要分为两大类：无参考设备的攻击（如差分功率分析、相关功率分析）和有参考设备的攻击（如模板攻击、随机模型攻击）. 从攻击效果来说，有参考设备的攻击需要的能量迹数目远小于无参考设备的攻击，但有参考设备的攻击必须有一个标准化的数据库来刻画被攻击设备的能量和噪声分布，这要求参考设备与被攻击设备相同或非常接近，否则模板和随机攻击的效率将大大降低. 攻击者需要根据现实条件选择合适的攻击方法.

故障攻击是一类主动攻击方法，与其他侧信道攻击相比具有更强大的攻击能力. 故障根据持续时间的长短分为暂时性故障，持久性故障和永久性故障. 攻击者主动注入故障得到错误密文，并通过基于差分或基于统计的分析方法恢复密钥. 在进行故障攻击之前，攻击者首先需要得到执行密码算法的设备或者具有远程访问执行密码算法运行环境的权限，其次需要知道设备中执行的密码算法的具体实现细节，最后还需要能够自主选择明文进行加密或者收集通信信道上传输的密文，对密文进行记录. 比其他侧信道攻击方法相比，故障攻击的执行条件更为苛刻，在现实环境中也更难实现.

侧信道防御在不同层次有不同的含义. 在硬件层面采用隐藏方案，在算法层面采用掩码方案，在系统层面采用软件防御. 隐藏方案的目的是隐藏由于其中的电路引起的侧信息泄漏，包括垂直和水平两个方向. 掩码方案旨在掩蔽加密数据与侧信道泄漏之间的关系. 软件防御旨在软件或协议上做一些更改，从而降低密码算法实现过程中的侧信息泄漏.

掩码方案是过去十年中进展最快的侧信道防御对策，这在很大程度上归功于实践和理论进展的完美结合. 在实践方面，掩码方案在不同情境下都已正式确定了具体的解决方案，即使在出现故障等物理默认情况下也能保持安全性. 在理论方面，研究者引入了允许自动安全证明的抽象模型，扩展到支持可组合性推理，并连接到越来越多的实际相关模型. 最近的工作甚至将这些实践和理论进展结合成统一的方法. 这些结果的结合为讨论掩码实现的安全与性能权衡奠定了坚实的基础. 它还为研究不同的优化提供了充分的背景，例如为了降低这些实现的随机性成本.

相比之下，关于低级别保护的隐藏方案的进展则相对较少. 原因主要有两条：其一是如双轨逻辑样式之类的隐藏方案难以从理论的角度分析，它们没有安全参数，其进展只能依赖于技术的改进. 其二是更具可扩展性的增噪方案不能提供令人满意的安全参数，因为它们本质上以线性成本为代价，从而得到线性安全性的改进.

在软件防御层面，白盒模型较传统的黑盒模型、灰盒模型具有更强的假设. 在白盒模型中，攻击者拥有一切权限，包括控制输入输出、观察内存中的数据、为程序设置断点、记录中间变量、篡改执行

内容等，并且攻击者能够利用静态分析、动态调试等方法获取密码算法中的密钥信息. 在实际应用中，可以通过其他防护技术来减弱这种假设. 目前主要的白盒密码实现方案都是利用代码混淆技术来实现的. 首先确定程序的功能，证明在黑盒攻击模型下是安全的；再针对程序来构造安全混淆器. 白盒密码在移动代理、软件保护、无线传感网络、移动设备等领域都有重要作用，然而白盒密码在其理论上的研究并未系统化，其安全性上的度量也没有标准化. 基于传统密码构造白盒实现方案是否具有可证明安全性仍有待研究.

传统的安全模型主要考虑理论安全，而抗泄漏密码学则关注实现安全. 其主要研究如何准确给出密码系统的信息泄漏量和如何构造抗泄漏安全性的密码方案两方面问题. 前者面临的关键问题在于如何将理论研究的信息泄漏量与具体的侧信道安全紧密结合，后者则需要考虑到攻击者在现实应用中所具备的攻击能力，并针对攻击构造可证明安全的密码算法. 抗泄漏密码学不仅具备理论价值，而且具有重要的现实意义.

7　结束语

侧信道攻击自提出以来受到研究者的广泛关注，已经发展出应用于不同场景的多个分支，其中能量分析攻击、缓存攻击和故障攻击应用最广泛. 侧信道攻击利用侧信息缩减密钥的穷举空间，因此与传统的密码分析相比，侧信道攻击具有成本上的优势. 在未来发展中，侧信道攻击与防御技术仍将是研究者关注的重点，是系统安全中不可或缺的重要一环.

参　考　文　献

[1] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. Annual International Cryptology Conference. Berlin, Germany: Springer, 1996. 104-113

[2] Brumley D, Boneh D. Remote timing attacks are practical. Computer Networks, 2005, 48(5): 701-716

[3] Brumley B B, Tuveri N. Remote timing attacks are still practical//European Symposium on Research in Computer Security. Berlin, Germany: Springer, 2011: 355-371

[4] Ge Q, Yarom Y, Cock D, et al. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. Journal of Cryptographic Engineering, 2018, 8(1): 1-27

[5] Liu F, Yarom Y, Ge Q, et al. Last-level cache side-channel attacks are practical//2015 IEEE symposium on security and privacy. San Jose, USA, 2015: 605-622

[6] Yan M, Sprabery R, Gopireddy B, et al. Attack directories, not caches: Side-channel attacks in a non-inclusive world//2019 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2019: 888-904

[7] Jancar J, Sedlacek V, Svenda P, et al. Minerva: The curse of ECDSA nonces: Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(4): 281-308

[8] Genkin D, Pachmanov L, Pipman I, et al. ECDSA key extraction from mobile devices via nonintrusive physical side-channels// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 1626-1638

[9] Aranha D F, Novaes F R, Takahashi A, et al. Ladderleak: Breaking ecdsa with less than one bit of nonce leakage// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, USA, 2020: 225-242

[10] Genkin D, Valenta L, Yarom Y. May the fourth be with you: A microarchitectural side-channel attack on several real-world applications of curve25519//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 845-858

[11] Guilley S, Heuser A, Ming T, et al. Stochastic Side-Channel Leakage Analysis via Orthonormal Decomposition//International Conference on Security for Information Technology and Communications. Hong Kong, China, 2017: 12-27

[12] Heuser A, Rioul O, Guilley S. Good is not good enough// International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2014: 55-74

[13] Carlet C, de Chérisey E, Guilley S, et al. Intrinsic resiliency of S-boxes against side-channel attacks–best and worst scenarios. IEEE Transactions on Information Forensics and Security, 2020, 16: 203-218

[14] Kocher P, Jaffe J, Jun B. Differential power analysis//Annual international cryptology conference. Berlin, Germany: Springer, 1999: 388-397

[15] Mather L, Oswald E, Whitnall C. Multi-target DPA attacks: Pushing DPA beyond the limits of a desktop computer// International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2014: 243-261

[16] Veyrat-Charvillon N, Gérard B, Standaert F X. Soft analytical side-channel attacks//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2014: 282-296

[17] Wang W, Yu Y, Standaert F X, et al. Ridge-based DPA: Improvement of differential power analysis for nanoscale chips. IEEE Transactions on Information Forensics and Security, 2017, 13(5): 1301-1316

[18] Gellersen T, Seker O, Eisenbarth T. Differential power analysis of the picnic signature scheme//International Conference on Post-Quantum Cryptography. Daejeon, South Korea, 2021: 177-194

[19] NIST. Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantumcrypt

ography-standardization, 2017
[20] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model//International workshop on cryptographic hardware and embedded systems. Berlin, Germany: Springer, 2004: 16-29
[21] Le T H, Clédière J, Canovas C, et al. A proposition for correlation power analysis enhancement//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2006: 174-186
[22] Chakraborty A , Mondal A , Srivastava A . Correlation power analysis attack against STT-MRAM based cyptosystems// IEEE International Symposium on Hardware Oriented Security & Trust. McLean, USA, 2017: 171-177
[23] Huang W L, Chen J P, Yang B Y. Power analysis on NTRU prime. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(1): 123-151
[24] Chari S, Rao J R, Rohatgi P. Template attacks//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer 2002: 13-28
[25] Aranha D F, Fouque P A, Gérard B, et al. GLV/GLS decomposition, power analysis, and attacks on ECDSA signatures with single-bit nonce bias//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer , 2014: 262-281
[26] Choudary M O, Kuhn M G. Efficient, portable template attacks. IEEE Transactions on Information Forensics and Security, 2017, 13(2): 490-501
[27] Ouladj M, Guilley S, Guillot P, et al. Spectral approach to process the (multivariate) high-order template attack against any masking scheme. Journal of Cryptographic Engineering, 2022, 12(1): 75-93
[28] Schindler W, Lemke K, Paar C. A stochastic model for differential side-channel cryptanalysis//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2005: 30-46
[29] Bruneau N, Carlet C, Guilley S, et al. Stochastic collision attack. IEEE Transactions on Information Forensics and Security, 2017, 12(9): 2090-2104
[30] Pereida García C, Brumley B B, Yarom Y. Make sure DSA signing exponentiations really are constant-time//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 1639-1650
[31] Aldaya A C, García C P, Brumley B B. From A to Z: Projective coordinates leakage in the wild. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(3): 428-453
[32] Bleichenbacher D. On the generation of one-time keys in DL signature schemes//Presentation at IEEE P1363 working group meeting. Berlin, Germany: Springer, 2000: 81
[33] Daemen J, Rijmen V. The Design of Rijndael: AES-the advanced encryption standard. Information Security & Cryptography, 2001, 26(3):137-139
[34] Bonneau J, Mironov I. Cache-collision timing attacks against AES//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2006: 201-215
[35] Neve M, Seifert J P. Advances on access-driven cache attacks on AES//International Workshop on Selected Areas in Cryptography. Berlin, Germany: Springer, 2006: 147-162
[36] Irazoqui G, Eisenbarth T, Sunar B. S $ A: A shared cache attack that works across cores and defies VM sandboxing--and its application to AES//2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 591-604
[37] Gullasch D, Bangerter E, Krenn S. Cache games--bringing access-based cache attacks on AES to practice//2011 IEEE Symposium on Security and Privacy. Berkeley, USA, 2011: 490-505
[38] Genkin D, Poussier R, Sim R Q, et al. Cache vs. Key-Dependency: Side channeling an implementation of pilsung. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(1): 231-255
[39] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 1997: 37-51
[40] Boneh D, DeMillo R A, Lipton R J. On the importance of eliminating errors in cryptographic computations. Journal of Cryptology, 2001, 14(2): 101-119
[41] Biham E, Shamir A.Differential fault analysis of secret key cryptosystems//Annual International Cryptology Conference. Berlin, Germany: Springer, 1997: 513-525
[42] Dusart P, Letourneux G, Vivolo O. Differential fault analysis on AES//International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer, 2003: 293-306
[43] Piret G, Quisquater J J. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2003: 77-88
[44] Blömer J, Seifert J P. Fault based cryptanalysis of the advanced encryption standard (AES)//International Conference on Financial Cryptography. Berlin, Germany: Springer, 2003: 162-181
[45] Giraud C. Dfa on aes//International Conference on Advanced Encryption Standard. Berlin, Germany: Springer , 2004: 27-41
[46] Moradi A, Shalmani M T M, Salmasizadeh M. A generalized method of differential fault attack against AES cryptosystem// International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer , 2006: 91-100
[47] Li W, Gu D, Wang Y, et al. An extension of differential fault analysis on AES//2009 Third International Conference on Network and System Security. Gold Coast, Australia, 2009: 443-446
[48] Saha D, Mukhopadhyay D, Chowdhury D R. A Diagonal Fault Attack on the Advanced Encryption Standard. IACR Cryptol. ePrint Arch., 2009, 2009(581):1-17
[49] Derbez P, Fouque P A, Leresteux D. Meet-in-the-middle and impossible differential fault analysis on AES//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2011: 274-291
[50] Hemme L. A differential fault attack against early rounds of (triple-) DES//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2004: 254-267
[51] Cheng W, Zhou Y, Sauvage L. Differential fault analysis on Midori//International Conference on Information and Communications Security. Singapore, 2016: 307-317
[52] Vafaei N, Bagheri N, Saha S, et al. Differential fault attack on

SKINNY block cipher//International Conference on Security, Privacy, and Applied Cryptography Engineering. Kanpur, India: Springer, 2018: 177-197

[53] Zhao G, Li R, Cheng L, et al. Differential fault analysis on LED using Super-Sbox. IET Information Security, 2014, 9(4): 209-218

[54] Tupsamudre H, Bisht S, Mukhopadhyay D. Differential fault analysis on the families of SIMON and SPECK ciphers//2014 Workshop on Fault Diagnosis and Tolerance in Cryptography. Busan, South Korea, 2014: 40-48

[55] Shi D, Hu L, Song L, et al. Differential fault attack on Zorro block cipher. Security and Communication Networks, 2015, 8(16): 2826-2835

[56] Biham E, Granboulan L, Nguyễn P Q. Impossible fault analysis of RC4 and differential fault analysis of RC4//International Workshop on Fast Software Encryption. Berlin, Germany: Springer , 2005: 359-367

[57] Kumar S V D, Patranabis S, Breier J, et al. A practical fault attack on arx-like ciphers with a case study on chacha20//2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). Taipei, China, 2017: 33-40

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

[59] Fuhr T, Jaulmes E, Lomné V, et al. Fault attacks on AES with faulty ciphertexts only//2013 Workshop on Fault Diagnosis and Tolerance in Cryptography. Los Alamitos, USA, 2013: 108-118

[60] Dobraunig C, Eichlseder M, Korak T, et al. SIFA: exploiting ineffective fault inductions on symmetric cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018(3): 547-572

[61] Dobraunig C, Eichlseder M, Groß H, et al. Statistical ineffective fault attacks on masked AES with fault countermeasures// International Conference on the Theory and Application of Cryptology and Information Security. Brisbane, Austrilia: Springer, 2018: 315-342

[62] Zhang F, Zhao X, Guo S, et al. Improved algebraic fault analysis: A case study on piccolo and applications to other lightweight block ciphers//International Workshop on Constructive Side-Channel Analysis and Secure Design. Berlin, Germany: Springer, 2013: 62-79

[63] Wang A, Chen M, Wang Z, et al. Fault rate analysis: Breaking masked AES hardware implementations efficiently. IEEE Transactions on Circuits and Systems II: Express Briefs, 2013, 60(8): 517-521

[64] Rivain M. Differential fault analysis on DES middle rounds//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2009: 457-469

[65] Li Y, Sakiyama K, Gomisawa S, et al. Fault sensitivity analysis//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2010: 320-334

[66] Zhang F, Lou X, Zhao X, et al. Persistent fault analysis on block ciphers. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018(3): 150-172

[67] Skorobogatov S. Optical fault masking attacks//2010 Workshop on Fault Diagnosis and Tolerance in Cryptography. Santa Barbara, USA, 2010: 23-29

[68] Bar-El H, Choukri H, Naccache D, et al. The sorcerer's apprentice guide to fault attacks. Proceedings of the IEEE, 2006, 94(2): 370-382

[69] Kim Y, Daly R, Kim J, et al. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. ACM SIGARCH Computer Architecture News, 2014, 42(3): 361-372

[70] Zhang Y, Zhang F, Yang B, et al. Persistent fault injection in fpga via bram modification//2019 IEEE Conference on Dependable and Secure Computing (DSC). Hangzhou, China, 2019: 1-6

[71] Pan J, Zhang F, Ren K, et al. One fault is all it needs: breaking higher-order masking with persistent fault analysis//2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). Florence, Italy, 2019: 1-6

[72] Menu A, Bhasin S, Dutertre J M, et al. Precise spatio-temporal electromagnetic fault injections on data transfers//2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). Atlanta, USA, 2019: 1-8

[73] Zhang F, Zhang Y, Jiang H, et al. Persistent fault attack in practice. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(2): 172-195

[74] Mus K, Islam S, Sunar B. QuantumHammer: A Practical Hybrid Attack on the LUOV Signature Scheme//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, USA, 2020: 1071-1084

[75] Grosso V, Standaert F X. ASCA, SASCA and DPA with Enumeration: Which One Beats the Other and When?// International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2015: 291-312

[76] Martin D P, O'connell J F, Oswald E, et al. Counting keys in parallel after a side-channel attack//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2015: 313-337

[77] Chen C, Farmani M, Eisenbarth T. A tale of two shares: why two-share threshold implementation seems worthwhile—and why it is not//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2016: 819-843

[78] Moradi A, Schneider T. Side-channel analysis protection and low-latency in action//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2016: 517-547

[79] Faust S, Paglialonga C, Schneider T. Amortizing randomness complexity in private circuits//International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China: Springer, 2017: 781-810

[80] Balasch J, Faust S, Gierlichs B, et al. Consolidating inner product masking//International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China: Springer, 2017: 724-754

[81] Belaïd S, Benhamouda F, Passelègue A, et al. Private multiplication over finite fields//Annual International Cryptology Conference. Santa Barbara, USA: Springer,2017: 397-426

[82] Karpman P, Roche D S. New instantiations of the CRYPTO 2017 masking schemes//International Conference on the Theory and

Application of Cryptology and Information Security. Brisbane, Australia : Springer, 2018: 285-314

[83] Goubin L. A sound method for switching between boolean and arithmetic masking//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2001: 3-15

[84] Coron J S, Großschädl J, Tibouchi M, et al. Conversion from arithmetic to boolean masking with logarithmic complexity// International Workshop on Fast Software Encryption. Berlin, Germany: Springer, 2015: 130-149

[85] Maghrebi H, Servant V, Bringer J. There is wisdom in harnessing the strengths of your enemy: customized encoding to thwart side-channel attacks//International Conference on Fast Software Encryption. Berlin, Germany: Springer , 2016: 223-243

[86] Bhasin S, Jap D, Peyrin T. Practical evaluation of fse 2016 customized encoding countermeasure. IACR Transactions on Symmetric Cryptology, 2017, 2017(3): 108-129

[87] Ishai Y, Sahai A, Wagner D. Private circuits: Securing hardware against probing attacks//Annual International Cryptology Conference. Berlin, Germany: Springer , 2003: 463-481

[88] Barthe G, Belaïd S, Dupressoir F, et al. Strong non-interference and type-directed higher-order masking//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 116-129

[89] Belaïd S, Goudarzi D, Rivain M. Tight private circuits: Achieving probing security with the least refreshing//International Conference on the Theory and Application of Cryptology and Information Security. Brisbane, Australia: Springer, 2018: 343-372

[90] Bruneau N, Guilley S, Heuser A, et al. Masks will fall off//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer , 2014: 344-365

[91] Barthe G, Belaïd S, Dupressoir F, et al. Verified proofs of higher-order masking//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer , 2015: 457-485

[92] Balasch J, Faust S, Gierlichs B. Inner product masking revisited//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2015: 486-510

[93] Goudarzi D, Rivain M. How fast can higher-order masking be in software?//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Paris, France: Springer, 2017: 567-597

[94] Barthe G, Belaïd S, Espitau T, et al. Masking the GLP lattice-based signature scheme at any order//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tel Aviv, Israel: Springer,2018: 354-384

[95] Bloem R, Gross H, Iusupov R, et al. Formal verification of masked hardware implementations in the presence of glitches// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tel Aviv, Israel: Springer,2018: 321-353

[96] Biryukov A, Udovenko A. Attacks and countermeasures for white-box designs//International Conference on the Theory and Application of Cryptology and Information Security. Brisbane, Australia: Springer,2018: 373-402

[97] Reparaz O. Detecting flawed masking schemes with leakage detection tests//International Conference on Fast Software Encryption. Berlin, Germany: Springer, 2016: 204-222

[98] Kumar R, Suresh V, Kar M, et al. A 4900-$\mu $ m 2 839-Mb/s side-channel attack-resistant AES-128 in 14-nm CMOS with heterogeneous sboxes, linear masked MixColumns, and Dual-Rail key addition. IEEE Journal of Solid-State Circuits, 2020, 55(4): 945-955

[99] Singh A, Kar M, Mathew S K, et al. Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering. IEEE Journal of Solid-State Circuits, 2018, 54(2): 569-583

[100] Das D, Maity S, Nasir S B, et al. ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity. IEEE Transactions on Circuits and Systems I: Regular Papers, 2018, 65(10): 3300-3311

[101] Dhanuskodi S N, Holcomb D. Enabling microarchitectural randomization in serialized AES implementations to mitigate side-channel susceptibility//2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). Miami, Florida, 2019: 314-319

[102] Kar M, Singh A, Mathew S K, et al. Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator. IEEE Journal of Solid-State Circuits, 2018, 53(8): 2399-2414

[103] Tokunaga C, Blaauw D. Securing encryption systems with a switched capacitor current equalizer. IEEE Journal of Solid-State Circuits, 2009, 45(1): 23-31

[104] Ratanpal G B, Williams R D, Blalock T N. An on-chip signal suppression countermeasure to power analysis attacks. IEEE Transactions on Dependable and Secure Computing, 2004, 1(3): 179-189

[105] Bucci M, Giancane L, Luzzi R, et al. A dynamic and differential CMOS lookup table with data independent power consumption for cryptographic applications on chip cards. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 245-251

[106] Li X, Yang C, Ma J, et al. Energy-efficient side-channel attack countermeasure with awareness and hybrid configuration based on it. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25(12): 3355-3368

[107] Bucci M, Giancane L, Luzzi R, et al. Three-phase dual-rail pre-charge logic//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2006: 232-241

[108] Bellizia D, Bongiovanni S, Olivieri M, et al. SC-DDPL: A novel standard-cell based approach for counteracting power analysis attacks in the presence of unbalanced routing. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67(7): 2317-2330

[109] Chong K S, Gwee B H, Chang J S. Energy-efficient synchronous-logic and asynchronous-logic FFT/IFFT processors. IEEE journal of solid-state circuits, 2007, 42(9): 2034-2045

[110] Spars J, Furber S. Principles asynchronous circuit design. Dordrecht, The Netherland: Kluwer Academic Publishers, 2002

[111] Chong K S, Ne K Z L, Ho W G, et al. Counteracting differential power analysis: Hiding encrypted data from circuit cells//2015 IEEE International Conference on Electron Devices and

Solid-State Circuits (EDSSC). Chengdu, China, 2015: 297-300

[112] Chong K S, Shreedhar A, Lwin N K Z, et al. Side-channel-attack resistant dual-rail asynchronous-logic AES accelerator based on standard library cells//2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). Xi'an China, 2019: 1-7

[113] Chong K S, Ng J S, Chen J, et al. Dual-hiding side-channel-attack resistant fpga-based asynchronous-logic aes: design, countermeasures and evaluation. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11(2): 343-356

[114] Almeida J B, Barbosa M, Barthe G, et al. Verifiable side-channel security of cryptographic implementations: constant-time MEE-CBC//International Conference on Fast Software Encryption. Berlin, Germany: Springer , 2016: 163-184

[115] Banik S, Bogdanov A, Isobe T, et al. Analysis of software countermeasures for whitebox encryption. IACR Transactions on Symmetric Cryptology, 2017, 2017(1): 307-328

[116] Bos J W, Hubain C, Michiels W, et al. Differential computation analysis: Hiding your white-box designs is not enough// International Conference on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2016: 215-236

[117] Joye M , Tunstall M. Fault analysis in cryptography. Heidelberg, Germany: Springer, 2012

[118] Micali S, Reyzin L. Physically observable cryptography//Theory of Cryptography Conference. Berlin, Germany: Springer , 2004: 278-296

[119] Zhang L, Ding A A, Fei Y, et al. A unified metric for quantifying information leakage of cryptographic devices under power analysis attacks//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2015: 338-360

[120] Duc A, Faust S, Standaert F X. Making masking security proofs concrete (or how to evaluate the security of any leaking device), extended version. Journal of Cryptology, 2019, 32(4): 1263-1297

[121] Bogdanov A, Isobe T. How secure is AES under leakage// International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2015: 361-385

[122] Dachman-Soled D, Gordon S D, Liu F H, et al. Leakage-resilient public-key encryption from obfuscation//Public-Key Cryptography--PKC 2016. Berlin, Germany: Springer , 2016: 101-128

[123] Hajiabadi M, Kapron B M, Srinivasan V. On generic constructions of circularly-secure, leakage-resilient public-key encryption schemes//Public-Key Cryptography--PKC 2016. Berlin, Germany: Springer , 2016: 129-158

[124] Faonio A, Venturi D. Efficient public-key cryptography with bounded leakage and tamper resilience//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2016: 877-907

[125] Fujisaki E, Xagawa K. Public-key cryptosystems resilient to continuous tampering and leakage of arbitrary functions// International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2016: 908-938

[126] Nishimaki R, Yamakawa T. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio//IACR International Workshop on Public Key Cryptography. Cham, Germany: Springer, 2019: 466-495

[127] Barwell G, Martin D P, Oswald E, et al. Authenticated encryption in the face of protocol and side-channel leakage//International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China: Springer, 2017: 693-723

[128] Faonio A, Nielsen J B. Non-malleable codes with split-state refresh//IACR International Workshop on Public Key Cryptography. Berlin, Germany: Springer , 2017: 279-309

[129] Dachman-Soled D, Kulkarni M, Shahverdi A. Tight upper and lower bounds for leakage-resilient, locally decodable and updatable non-malleable codes. Information and Computation, 2019, 2019(268): 104428-104473

[130] Chen Y, Wang Y, Zhou H S. Leakage-resilient cryptography from puncturable primitives and obfuscation//International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China: Springer, 2018: 575-606

[131] Faust S, Mukherjee P, Nielsen J B, et al. A tamper and leakage resilient von Neumann architecture//IACR International Workshop on Public Key Cryptography. Berlin, Germany: Springer , 2015: 579-603

[132] Medwed M, Standaert F X, Nikov V, et al. Unknown-input attacks in the parallel setting: Improving the security of the CHES 2012 leakage-resilient PRF//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer , 2016: 602-623

[133] Martinasek Z, Clupek V, Krisztina T. General scheme of differential power analysis//2013 36th International Conference on Telecommunications and Signal Processing (TSP). Rome, Italy, 2013: 358-362

[134] Martinasek Z, Zapletal O, Vrba K, et al. Power analysis attack based on the MLP in DPA contest v4//2015 38th International Conference on Telecommunications and Signal Processing (TSP). Prague, Czech Republic, 2015: 154-158

[135] Mpalane K, Gasela N, Esiefarienrhe B M, et al. Vulnerability of advanced encryption standard algorithm to differential power analysis attacks implemented on ATmega-128 microcontroller// 2016 3rd International Conference on Artificial Intelligence and Pattern Recognition (AIPR). Shanghai, China, 2016: 1-5

[136] Cagli E, Dumas C, Prouff E. Convolutional neural networks with data augmentation against jitter-based countermeasures// International Conference on Cryptographic Hardware and Embedded Systems. Taipei, China: Springer, 2017: 45-68

[137] Picek S, Heuser A, Jovic A, et al. The curse of class imbalance and conflicting metrics with machine learning for side-channel evaluations. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 2019(1): 1-29

[138] Prouff E, Strullu R, Benadjila R, et al. Study of deep learning techniques for side-channel analysis and introduction to ASCAD database. Cryptology ePrint Archive, 2018, 2018(53): 1-45

[139] Yang G, Li H, Ming J, et al. Convolutional neural network based side-channel attacks in time-frequency representations// International Conference on Smart Card Research and Advanced Applications. Toulouse, France: Springer, 2018: 1-17

[140] Hettwer B, Gehrer S, Güneysu T. Applications of machine learning techniques in side-channel attacks: a survey. Journal of Cryptographic Engineering, 2020, 10(2): 135-162

[141] Zaid G, Bossuet L, Habrard A, et al. Methodology for efficient CNN architectures in profiling attacks. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(1): 1-36

[142] Rijsdijk J, Wu L, Perin G, et al. Reinforcement learning for hyperparameter tuning in deep learning-based side-channel analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021(3): 677-707

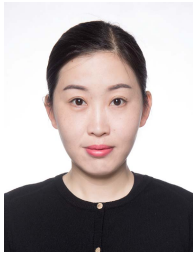
[143] Gu K, Wu N, Yin B, et al. Secure data query framework for cloud and fog computing. IEEE Transactions on Network and Service Management, 2019, 17(1): 332-345

[144] Liu Q, Peng Y, Wu J, et al. Secure multi-keyword fuzzy searches with enhanced service quality in cloud computing. IEEE Transactions on Network and Service Management, 2021, 18(2):2046-2062

[145] Groot Bruinderink L, Hülsing A, Lange T, et al. Flush, gauss, and reload–a cache attack on the BLISS lattice-based signature scheme//International Conference on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer , 2016: 323-345

[146] Pessl P, Prokop L. Fault attacks on CCA-secure lattice KEMs. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021(2): 37-60

[147] State Cryptography Administration. GM/T 0008–2012 Cryptography Test Criteria for Security IC. Beijing: Standards Press of China, 2012(in Chinese)
国家密码管理局. GM/T 0008–2012 安全芯片密码检测准则. 北京: 中国标准出版社, 2012



WANG Yong-Juan, Ph. D., professor, M. S. supervisor. Her research interests include information security, artificial intelligence, and side-channel analysis.

FAN Hao-Peng, M. S. candidate. His research interests include information security and side-channel analysis.

DAI Zheng-Yi, M. S. candidate. His research interests include cryptography and side-channel analysis.

YUAN Qing-Jun, Ph.D. candidate,lecturer. His research interests include information side-channel analysis and network traffic analysis.

WANG Xiang-Bin, M. S. candidate. His research interests include side-channel analysis.

Background

Since proposed in 1996, side-channel attacks have given rise to many kinds. Power analysis attacks try to obtain physical information such as energy and electromagnetic; cache attacks try to recover key information by obtaining the shared cache state and fault attacks try to actively destroy the device state. These attack methods are diverse, and their basic principles, attack models and application scene are very different.

This paper summarizes the above three types of side-channel attacks and systematically introduces side-channel attack techniques, detailing their basic principles, attack models and application scene. In addition, this paper dissects the basic principles, security models and application scene of side-channel countermeasures, and finally summarizes the basic principles and development of leakage-resilient cryptography. In the end, this paper points out the existing problems and the possible research trend in the future. We hope this paper can help the other researchers.

This project is supported by the National Natural Science Foundation of China (NSFC) (61602512). This project aims to promote the development of information security, reduce the security threat of cryptosystems, and reach the international leading level. The group is dedicated to the research of side-channel attacks and countermeasures, and has published several papers in international conferences and journals, such as IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), IEICE TRANSACTIONS on Information and Systems and International Conference on Artificial Intelligence and Security (ICAIS) , etc.