面向格密码的能耗分析攻击技术

李延斌[1),2)] 朱嘉杰[1)] 唐 明[3)] 张焕国[3)]

[1)](南京农业大学人工智能学院 南京 210095)

[2)](密码科学技术国家重点实验室 北京 100878)

[3)](武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)

摘 要 量子计算的飞速发展对传统密码的安全性带来巨大挑战,Peter Shor 提出的量子计算模型下分解整数和计算离散对数的多项式时间算法对基于传统数论难题的密码系统构成了威胁.美国国家标准与技术研究院(NIST)于 2016 年开始征集后量子公钥密码算法标准,其中,大多基于格、基于哈希、基于编码、基于多变量这四种密码体制,而基于格的密码体制在其公钥尺寸、计算效率和安全性方面具有更好的平衡性,所占比例最大.然而,格密码的实现在实际环境中易遭受能耗分析攻击(Power Analysis Attacks).能耗分析攻击是利用密码设备运行过程中产生的功耗、电磁等信息,攻击者建立这些旁路信息与密码算法中间值之间的联系从而恢复密钥等敏感信息.自从能耗分析攻击出现以来,该类攻击手段严重威胁了密码系统的安全.随着量子计算的发展,后量子密码的安全性日益成为密码研究的热点,特别地,近期 NIST 公布了最新轮的后量子密码算法,作为占据比例最多的格密码,其侧信道安全性也受到了学术界的广泛关注.本文针对格密码的能耗分析攻击技术从攻击模型、攻击目标、攻击条件开展研究,分析了面向格密码的攻击原理、格密码的各个算子的侧信道安全性,重点介绍了适用于 NIST 第三轮格密码的攻击技术,以及相应防护方案的攻击技术,最后讨论了现有面向格密码的能耗分析攻击面临的问题及未来研究方向.

关键词 能耗分析攻击;格密码;后量子密码;硬件安全;侧信道泄露

中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2023.00331

Power Analysis Attacks for Lattice-Based Cryptography

LI Yan-Bin[1),2)] ZHU Jia-Jie[1)] TANG Ming[3)] ZHANG Huan-Guo[3)]

[1)](*College of Artificial Intelligence, Nanjing Agricultural University, Nanjing* 210095)

[2)](*State Key Laboratory of Cryptology, P.O. Box* 5159, *Beijing* 100878)

[3)](*Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan University, Wuhan* 430072)

Abstract With the rapid development of quantum computer research, design, and manufacturing technology, the era of quantum computing is gradually coming. Cryptosystems based on traditional number theory problems are threatened. The development of cryptosystems in the post-quantum era has become a hot spot in the field of cryptography. The National Institute of Standards and Technology (NIST) began to solicit standards for post-quantum public key cryptography algorithms. It announced seven candidate algorithms for the third round, five of which are lattice cryptographic schemes. Lattice-based cryptosystems rely on adding noise to linear equations to solve complex problems and have the largest share in the Post-Quantum Cryptography (PQC) due to their better balance in public key size, computational efficiency, and security. However, implementing lattice ciphers is vulnerable to power analysis attacks in the application of practical environments. Power analysis attacks have been viewed as a physical attack method to recover the sensitive information of cryptographic algorithms effectively. The attackers capture the power

收稿日期:2022-01-20;在线发布日期:2022-08-18.本课题得到国家自然科学基金项目(62072247,61972295)资助.**李延斌**,博士,副教授,主要研究方向为侧信道攻击、密码学和密码芯片安全.E-mail:yanbinli@njau.edu.cn.**朱嘉杰**,硕士研究生,主要研究方向为侧信道攻击、密码学.**唐 明**(通信作者),博士,教授,博士生导师,主要研究领域为密码学、硬件安全、侧信道攻击与防御等.E-mail:m.tang@126.com.**张焕国**,博士,教授,博士生导师,主要研究领域为信息安全和密码学.

consumption, electromagnetic or other information generated during the operation of cryptographic devices and establish the relationship between this information and the intermediate value of the cryptographic algorithm. Since the emergence of power analysis attacks as an important attack method at the hardware level, it has seriously threatened the security of the cryptographic system. In particular, NIST announced the candidate post-quantum cryptographic algorithms in the third round of the PQC project. The academic community has also been widely concerned about the resistance against power analysis attacks of lattice-based cryptography. Lattice ciphers play a vital role in post-quantum cryptography, and its side-channel security is an indispensable indicator to comprehensively measure algorithm security. Therefore, the research on power analysis attack techniques for lattice ciphers results from the current NIST post-quantum algorithm standard and even post-quantum cryptography is an important topic for practical applications. Power analysis attacks greatly threaten the development and evaluation of lattice cipher schemes. Due to the novelty of many lattice-based cipher schemes, many security vulnerabilities have still not been evaluated. There are various types of existing attack models, all of which can recover the key information or message of the lattice cipher. Many works have also proposed the protection schemes for lattice ciphers to resist these power analysis attacks. Still, the existing protection schemes hardly satisfy the security and efficiency requirements. This work studies the side-channel attack technology of lattice-based cryptography in view of the attack model, target, and condition. We analyze the attack mechanism and the security of each operation of lattice-based cryptography. This work starts with analyzing the cryptographic scheme, the attacking methods of different operators, and investigates the cause of the vulnerability in the scheme from the perspective of designers. In addition, the attack principle of the latest protection scheme is analyzed, and the internal reasons for the breach of the protection scheme are explained. It focuses on the attack methods against the third round of NIST lattice-based cryptography. Moreover, we analyze the attack technologies for countermeasures. Finally, we present the drawbacks and trends of power analysis attacks for lattice-based cryptography.

Keywords power analysis attack; lattice-based cryptography; post-quantum cryptography; hardware security; side-channel leakage

1 引 言

随着量子计算机研究、设计和制造技术的飞速发展，量子计算时代逐渐到来. 当前保障网络空间安全的密码体制大多基于传统数论难题，而 Peter Shor 给出的量子计算模型下分解整数和计算离散对数的多项式时间算法[1]，它对传统的密码系统构成了威胁. 因此，后量子时代下的密码体制发展是密码学领域关注的一个研究热点[2-3].

美国国家标准与技术研究院(NIST)于 2016 年开始征集后量子公钥密码算法标准，共接收到 64 份算法[4]，其中有 26 份是基于格密码的. NIST 于 2019 年公布了进入第 2 轮的 26 种密码方案(17 个公钥加密和密钥封装方案以及 9 个数字签名方案)，包含 12 种格密码方案，其余的为基于同源的、基于对称的等；并于 2020 年 7 月 22 日公布了最新的第 3 轮候选的 7 个算法，有 5 个是格密码方案包括 3 个公钥加密(PKE)/密钥封装算法(KEM)和 2 个零知识证明协议构造的数字签名算法. 另外两个算法，一个是基于编码的方案，一个是基于多变量的方案. 中国密码学会 2019 年举办的密码竞赛共收到 38 份后量子密码，有 26 份是基于格密码的；而在第 2 轮共 14 个密码算法[5]之中，更是有 11 份是格密码方案. 目前，无论是 NIST 标准还是国内竞赛算法，大多基于格、基于哈希、基于编码、基于多变量这四种密码体制[6-8]，而基于格的密码体制在其公钥尺寸、计算效率和安全性方面具有更好的平衡性，所占比例最大.

格密码在国内外后量子密码征集算法中占比如表 1 所示.

表 1　格密码在国内外后量子密码征集算法中占比

	第 1 轮	第 2 轮	第 3 轮
NIST	26/64	12/26	5/7
中国密码学会	26/38	11/14	—

基于格的密码体制依赖于向线性等式中添加噪声等的求解困难问题. 然而,格密码的实现在实际环境中易遭受侧信道攻击[9-11]. 侧信道攻击是指在密码设备运行过程中,攻击者通过获取功耗、电磁、时间等侧信道上的信息[12-14],建立这些信息与密码算法中间值之间的联系,进而恢复密钥等敏感信息的攻击技术. 能耗分析攻击作为硬件层面的重要攻击手段,从分组密码[15]到 RSA、ECC 等一些公钥算法[16-17]已经被验证了其对于密码算法的严重威胁.

面向格密码的侧信道攻击研究近几年来成为密码工程方向的研究热点之一. 一方面,这是由于 NIST 表明在后量子密码标准项目中“考虑后量子密码的抗侧信道攻击特性作为评判算法的一项重要标准”[18];另一方面,2021 年 10 月 4 日美国国土安全部(DHS)与美国国家标准与技术研究院(NIST)合作发布了“后量子密码过渡”路线图,在后量子化的发展进程中,格密码如何在物联网设备中高效且安全实现也是必须考虑的问题. 侧信道攻击作为密码设备物理层的主要威胁之一,现有很多工作针对各种格密码在 ARM Cortex M4[19-21]、8051 微控制器[22]等平台上已经验证了攻击可行性.

随着 NIST 后量子密码标准的发展,近年来出现了一些针对格密码的侧信道攻击的相关综述. 文献[23]初步整理了后量子密码在侧信道攻击和故障攻击中所面临的攻击威胁,文献[24]描述了对基于格、基于编码、基于哈希、基于多变量的侧信道和故障注入的攻击现状,该文献分析对象为 NIST 后量子标准第 2 轮候选算法,如介绍基于格的攻击原理分析的算法为 Round5,该算法并未进入 NIST 最终轮,且对于此算法的攻击思路对入选最终轮的格密码方案不适用. Drăgoi 等人[25]研究了基于编码的硬件攻击分析,主要分析了 Goppa 编码和 MDPC 编码的攻击方法,并给出了可能的防护思路;Chowdhury 等人[26]针对后量子密码的后量子随机数发生器、后量子不可克隆函数、侧信道攻击等硬件安全性进行了研究,分析了这些硬件单元的特性、优点和不足.

现有这些研究均是介绍后量子密码在侧信道方面的攻击现状,没有从攻击模型的角度对格密码的脆弱性进行分析,同时对 NIST 最新的候选标准格密码的攻击关注较少,本文与现有工作的区别在于两点:(1)分析对象及涵盖范围不同. 现有工作分析对象为 NIST 后量子标准第 1 轮或第 2 轮候选算法,其中大量算法并未进入 NIST 第 3 轮,且对于其中一些算法的攻击思路对入选最终轮的格密码方案不适用. 本文分析的对象锁定为 NIST 后量子标准第 3 轮入选的格密码方案,而针对第 3 轮结果公布后出现的大量针对进入标准的格密码的攻击方案,对于这些密集的且最新提出的工作尚未有详细的分析;(2)分析的思路不同. 本文的目标不在于罗列现有攻击方法对何种方案是否能够成功攻击、攻击成功率多少,而是从密码方案入手,依次分析不同算子的攻击思路,从格密码方案设计的角度分析方案中出现脆弱点的根本原因. 此外,对于最新的防护方案的攻击原理进行分析,说明防护方案被攻破的内在原因.

本文的主要贡献有三个方面:

(1)分析了现有针对格密码的能耗分析攻击技术,梳理了不同攻击方法的攻击原理和攻击条件;

(2)对于格密码的能耗分析攻击方法按攻击原理、攻击目标等维度进行分类,构建格密码的攻击全景图;

(3)讨论最新 NIST 第 3 轮候选格密码的能耗分析攻击威胁及防护方案的攻击技术.

2　基于格的密码系统

2.1　格理论基础

格是离散的向量空间 R^m 上的一个子群,其定义如下.

定义 1.　设 $\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n$ 为 R^m 上的一组向量,其满足线性无关,由 $\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n$ 的线性组合构成一个格 L,线性组合系数均为整数域 Z 中的元素. 即 $L(\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n)=\{b_1\boldsymbol{u}_1+\cdots+b_n\boldsymbol{u}_n\,|\,b_1,\cdots,b_n\in Z\}$,其中,$\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n$ 是 L 的一组基,格 L 的维度为 n. 对于格 L,它不止有一组基. 如果 $\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n$ 是格 L 的一组基,那么相应的 $-\boldsymbol{u}_1,-\boldsymbol{u}_2,\cdots,-\boldsymbol{u}_n$ 也是它的一组基. 由基的行列式得到的格的体积是一个固定值,可以用来估计格中最短向量长度等问题.

由于格上困难问题暂时还不存在多项式时间内解决的办法,包括量子计算机. 有很多经典格难题存在,这里仅简单列举一些.

(1)最短向量问题(Shortest Vector Problem,SVP)

对于给定的格 L，寄希望于找到一个非零格向量 $\boldsymbol{u}$，使得对于任意的非零向量 $\boldsymbol{v}\in L$，满足 $\|\boldsymbol{u}\|\leq\|\boldsymbol{v}\|$.

(2)最近向量问题(Closest Vector Problem，CVP)

对于给定的格 L 和目标向量 $\boldsymbol{g}\in R^m$，希望找到一个非零的格向量 $\boldsymbol{u}$，使得对于任意的非零向量 $\boldsymbol{v}\in L$，满足 $\|\boldsymbol{u}-\boldsymbol{g}\|\leq\|\boldsymbol{v}-\boldsymbol{g}\|$.

(3)有界距离解码问题(Bounded Distance Decoding，BDD)

对于给定的格 L 和不在格中的目标向量 $\boldsymbol{g}\in R^m$，$dist(\boldsymbol{g},L)<\gamma\lambda_1(L)$，希望找到一个非零的格向量 $\boldsymbol{u}$，使得对于任意的非零向量 $\boldsymbol{v}\in L$，满足 $\|\boldsymbol{u}-\boldsymbol{g}\|\leq\|\boldsymbol{v}-\boldsymbol{g}\|$.

密码学主要是建立在多项式近似因子上，正是因为目前尚未找到求解近似因子为多项式的格难题的多项式时间量子算法，使得基于格理论的公钥密码方案能够有效抵挡住量子攻击[27].

2.2 格密码分类

(1)容错学习问题(Learning with Errors，LWE)

设二元组$(\boldsymbol{A},\boldsymbol{u})$，其中 $\boldsymbol{A}\in Z_p^{m\times n}$ 是随机矩阵，向量 $\boldsymbol{u}\in Z_p^m$，其中 $e\in Z_p^m$ 为误差且服从概率分布 χ，p 为整数模数. 那么有搜索版本的 LWE 问题(Search LWE)是求解 $\boldsymbol{u}\in Z_p^m$ 满足 $\boldsymbol{v}=\boldsymbol{A}\boldsymbol{u}+e$，而判定版本的 LWE 问题(Decisional LWE)是判断由 $\boldsymbol{v}=\boldsymbol{A}\boldsymbol{u}+e$ 计算得到 $\boldsymbol{v}$ 还是均匀取自 Z_p^m[28].

(2)环上容错学习问题(Ring Learning with Errors，RLWE)

设二元组$(\boldsymbol{A},\boldsymbol{u})$，其中 $a\in R_p$ 是随机多项式，其中 $\boldsymbol{u}\in R_p$ 和 $e\in R_p$ 为误差且服从概率分布 χ，p 为整数模数. 那么有搜索版本的 RLWE 问题(Search RLWE)是求解 $\boldsymbol{v}$ 满足 $\boldsymbol{v}=\boldsymbol{A}\boldsymbol{u}+e$，而判定版本的 RLWE 问题(Decisional RLWE)是判断由 $\boldsymbol{v}=\boldsymbol{A}\boldsymbol{u}+e$ 计算得到 $\boldsymbol{v}$ 还是均匀取自 R_p[28].

另外，还有一些 LWE、RLWE 问题的变种，如 Module Learning with Errors(MLWE)问题[29]，和 RLWE相比，MLWE具有更灵活的参数选择. Learning with Rounding(LWR)则省略了错误项 e 而使用丢掉系数的最低有效位的方法产生确定性错误[30]，可以减小计算和通信开销.

(3)NTRU 问题

设环 R 秩为 n 且被赋予内积，q 是正整数，γ 是 R 上的一个概率分布，τ 是正实数. 以(R,q,γ,τ)为参数的 NTRU 问题是，对于以 γ 随机选择的环元素 f 和 $g\leftarrow\gamma$，且 f 模 q 可逆，在格 $L_h^q=\{(\boldsymbol{x},\boldsymbol{y})\in R^2:h\boldsymbol{x}-\boldsymbol{y}=0(\mathrm{mod}\,q)\}$ 中使得$(\boldsymbol{x},\boldsymbol{y})\neq(0,0)(\mathrm{mod}\,q)$并且$(\boldsymbol{x},\boldsymbol{y})$的欧几里得范数小于 $\tau\sqrt{2n}$ 的向量$(\boldsymbol{x},\boldsymbol{y})\in R^2$[31].

近几年提出的格密码大多基于 LWE、RLWE、MLWE、LWR 及其变种问题，按照困难问题可以将 NIST 第 2 轮以来的主流格密码进行分类，如图 1 所示. 图中显示了于 2019 年 1 月入选 NIST 第 2 轮的算法及 2020 年 7 月入选 NIST 第 3 轮的算法，虚线框表示进入第 3 轮备选算法.

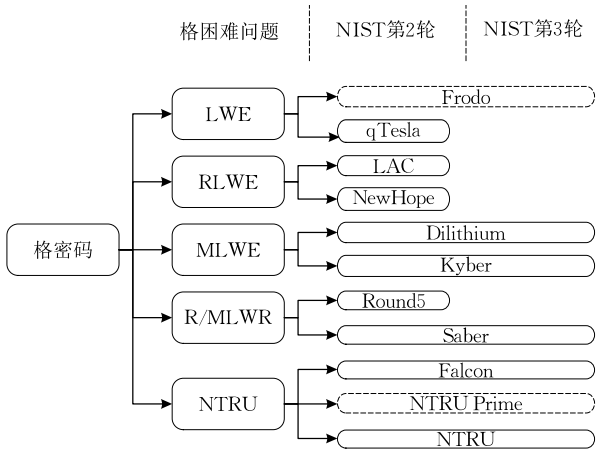

图 1 格密码分类图

3 能耗分析攻击模型

能耗分析攻击的特点就是利用旁路信息攻击物理实现后的密码算法，从黑盒模型未曾防范的物理信息泄漏的角度找到密钥相关信息. 加密信息在主信道传输，但是在密码设备进行数据处理时，会产生功耗、电磁辐射、热量等其他信息. 泄漏的这些信息会因为设备操作及其操作数的不同而产生差异.

假设 $Q=(q_1,\cdots,q_m)$ 为一个加密算法执行 m 次加密的明文或密文序列，攻击者采集到加密过程中设备的能耗信息为 $L=(l_1,\cdots,l_m)$，任意元素 l_i 对应 q_i 在正确密钥 k 下的加密所产生的能耗信息. 对于不同猜测密钥 k^*，攻击者可以根据加密算法计算出攻击所选中间值 $f(q_i,k^*)$，f 表示加密算法中计算中间值的函数. 攻击者通过建立中间值与能耗信息之间的联系来恢复正确密钥. 常见的攻击技术有简单能耗攻击(SPA)[32]、差分能耗攻击(DPA)[33]、相关能耗攻击(CPA)[34]和模板攻击(TA)[35]等.

3.1 简单能耗攻击(SPA)

简单能耗攻击的目标是仅仅通过少量的能量迹揭示出密钥或者与之相关的敏感信息. SPA 攻击可以分为单迹攻击和多迹攻击. 在单能量迹攻击中，攻击者只能采样一条能量迹. 根据一条能量迹中正确密钥对应的中间值与错误密钥对应的中间值对应的能耗特征不同区分密钥，假设正确密钥对应能耗特征 l^k，猜测密钥对应能耗特征为 l^{k^*}，即

《计算机学报》

$$k=\arg\max_{k^*\in K}(O(l_i,l_{k^*})) \tag{1}$$

其中，O 为衡量两种能耗特征相似的评估指标，可以通过人工观测，也可以利用相关性系数计算. 多迹 SPA 攻击中，攻击者可以采样多条能量迹，计算得到均值能耗曲线后同样利用该公式推测密钥.

SPA 攻击使用依赖于密钥变化的能量迹，只需要使用一条或很少量的能量迹. 攻击者需要具备能够监测被攻击设备瞬时能量消耗的能力. 被攻击设备中的密钥必须对能耗有显著的直接或间接影响.

3.2　差分能耗攻击(DPA)

差分能耗攻击利用密码设备能量消耗的数据依赖性，在加密的过程中，设备消耗的能量依赖于处理数据的不同进而会有微小变化，可以通过这种变化确定处理的数据是 0 还是 1. 这种攻击使用大量的能量迹来分析固定时刻设备的能量消耗，并将能量消耗点视作被处理数据函数的泄漏点.

攻击者为了建立算法中间值与能耗值之间的关系，利用泄漏模型 h 将中间值 $f(q_i,k^*)$ 映射为假设能耗值 $h(f(q_1,k^*))$. 猜测密钥 k^* 得到假设能耗向量 $\boldsymbol{H}_m^{k^*}=(h(f(q_1,k^*)),\cdots,h(f(q_m,k^*)))$. 在差分攻击中，选取一个阈值 δ，将假设能耗值分别大于 δ 和小于 δ 的能耗曲线放入两个集合，计算两个集合的均值曲线，并计算两条均值曲线之间的差分. 每组猜测密钥都会得到差分值，差分值最大对应的猜测密钥即为正确密钥，即：

$$k=\arg\max_{k^*\in K}(D(L,\boldsymbol{H}_m^{k^*})) \tag{2}$$

其中，D 为上述计算差分的区分器函数.

3.3　相关能耗攻击(CPA)

相关能耗攻击使用相关性计算来确定能量消耗与假设能量值的相关性. 相关性系数是确定数据间线性关系的最普遍方法，与 DPA 类似，不同之处在于它是计算能耗向量与假设能耗向量之间的皮尔逊相关系数，每组猜测密钥都会得到相关性系数，相关性系数最大对应的猜测密钥即为正确密钥，即：

$$k=\arg\max_{k^*\in K}(C(L,\boldsymbol{H}_m^{k^*})) \tag{3}$$

其中，C 为上述计算皮尔逊相关性系数的函数.

3.4　模板攻击(TA)

模板攻击利用了能量消耗取决于设备正在处理的数据这一事实，并使用多元正态分布来描述能量迹的特征. 与其他能耗分析攻击不同的是，模板攻击分为两个阶段：第一阶段描述了能量消耗的特征，将样本曲线集合 L 按照假设能耗值 $\boldsymbol{H}_m^{k^*}$ 划分至不同集合，并计算均值曲线 $\overline{M}_i$ 和协方差矩阵 $\boldsymbol{\Sigma}_i$ 作为该类的模板 $\{\overline{M}_i,\boldsymbol{\Sigma}_i\}$.

第二个阶段利用该特征进行匹配. 利用正态分布概率公式分别计算目标曲线 l 与各类模板匹配的概率值：

$$p_i=\frac{1}{\sqrt{\pi^N|\boldsymbol{\Sigma}_i|}}\exp\left(-\frac{1}{2}(l-\overline{M}_i)\boldsymbol{\Sigma}_i(l-\overline{M}_i)^{-1}\right).$$

因此，正确密钥可以被成功恢复：

$$k=\{k\,|h(f(q,k))=h_j,j=\arg\max_i p_i\} \tag{4}$$

4　面向格密码的攻击技术

本节对面向格密码的能耗分析攻击技术进行研究，首先按照能耗分析攻击模型进行分类，然后根据格密码的应用场景对攻击性质和攻击目标进行分析，以给出格密码的能耗分析攻击全览. 同时，针对 Saber 密钥封装方案，给出了不同攻击模型的攻击效果.

4.1　攻击模型

能耗分析攻击常用的攻击模型可分为简单能耗攻击(SPA)、差分能耗攻击(DPA)、相关能耗攻击(CPA)、模板攻击(TA)等. 面向格密码的攻击技术可以按照攻击过程中的区分器模型划分，如图 2 所示.

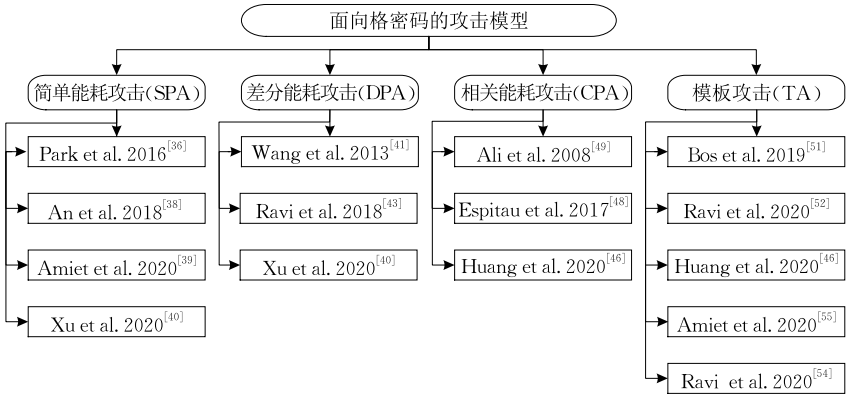

图 2　面向格密码的攻击模型分类

4.1.1 SPA

SPA 是在公钥密码中常用且简单的能耗分析攻击手段. Park 等人[36]于 2016 年 AsianHOST 国际会议上提出了第 1 个针对 RLWE 方案的 SPA 攻击.

RLWE 方案是在 2010 年提出的,随后使用 NTT 运算有效地对 RLWE 加密方案进行了优化. 本文简单介绍一下优化后的方案,如下所述.

(1)密钥生成阶段

从离散高斯分布中选取两个多项式 r_1、$r_2 \in R_p$,并且将其和多项式 $a \in R_p$ 一起进行 NTT 运算.

$\tilde{r}_1 = NTT(r_1)$, $\tilde{r}_2 = NTT(r_2)$, $\tilde{a} = NTT(a)$.

然后,执行操作 $\tilde{q} = \tilde{r}_1 - \tilde{a} \cdot \tilde{r}_2 \in R_p$,私钥即 $\tilde{r}_2$,$(\tilde{a}, \tilde{q})$则是公钥.

(2)加密阶段

二进制输入向量 $\boldsymbol{m} \in \{0,1\}^n$ 为 n 位. 向量 $\boldsymbol{m}$ 通过多项式乘于$\frac{p-1}{2}$被编码为 $\bar{m}$. 然后,计算密文,从离散高斯分布中采样三个误差多项式 e_1、e_2、e_3,然后对 e_1 和 e_2 进行 NTT 运算. 密文会被计算为一对多项式$(\tilde{c}_1, \tilde{c}_2)$:

$\tilde{e}_1 = NTT(e_1)$, $\tilde{e}_2 = NTT(e_2)$,

$\tilde{c}_1 = \tilde{a} \cdot \tilde{e}_1 + \tilde{e}_2$, $\tilde{c}_2 = \tilde{q} \cdot \tilde{e}_1 + NTT(e_3 + \bar{m})$.

(3)解密阶段

在解密操作中,利用私钥 $\tilde{r}_2$ 来计算 $\bar{m}$:

$$\bar{m} = INTT(\tilde{c}_1 \cdot \tilde{r}_2 + \tilde{c}_2).$$

然后使用解码器用 $\bar{m}$ 恢复输入向量 $\boldsymbol{m}$.

随着物联网技术的发展,基于格的密码方案在 8 比特物联网设备的实现方案被提出[37],但是并未考虑侧信道攻击威胁. 在 RLWE 方案的解密阶段,私钥 r_2 参与运算得到消息:

$$\bar{m} = INTT(\tilde{c}_1 \cdot \tilde{r}_2 + \tilde{c}_2).$$

在计算过程中如果中间值大于 q 需要进行模约减操作,那么进行模约减的情况对应的能耗特征时间更长. 因此可以选择密文进行攻击,通过采集计算过程中的能耗信息判断是否存在模约减操作来恢复私钥 $\tilde{r}_2$,再通过 INTT 求得私钥. 由于 SPA 直接通过能耗曲线特征进行判断从而恢复密钥,易受噪声干扰而存在误差. 因此,许多攻击方法在 SPA 前进行曲线预处理或特殊处理. An 等人[38]在攻击 NTRU 解密阶段私钥时,通过选取加操作的参考曲线段,计算目标曲线与参考曲线段之间的相关性系数,区分不同密钥操作的区域是否存在加操作,再进行阈值筛选进行 SPA,一定程度上降低了噪声的影响.

Amiet 等人[39]在 2020 年 PQC 会议上报告了对 NewHope 中消息编码 *ploy_frommsg* 函数的攻击方案,如过程 1 所示,该函数的功能是将二进制消息封装为多项式表示,若当前消息比特为 0,对应的多项式系数为 0;反之,若消息比特为 1,则多项式系数为 $q/2 = 6144$. 在计算中,若消息比特为 0,则 $mask = 0$;若为 1,则 $mask = -1$(0xFFFF…). 因此,当消息比特为 0 或 1 时,$mask$ 的能耗特征差异非常大(汉明重差异大,能耗特征遵循汉明重模型). 对于无优化的 NewHope 实现,直接对消息编码函数区域的能耗特征 SPA 即可推断出消息;对于优化实现版本,需要借助参考曲线,计算目标曲线与参考曲线之间的欧氏距离进而判断消息比特.

过程 1. NewHope 方案的消息编码函数.

```
1. void poly_frommsg (poly *r, const unsigned char *msg)
2. {
3.   unsigned int i,j,mask;
4.   FOR(i=0;i<32;i++)
5.    FOR(j=0;j<8;j++)
6.     mask=-((msg[i]≫j)&1);
7.     r->coeffs[8*i+j+0]=mask&(NEWHOPEQ/2);
8.     r->coeffs[8*i+j+256]=mask&(NEWHOPEQ/2);
9.   END FOR
10. END FOR
11. }
```

对于无防护的密码算法,格密码算法中存在多个与敏感信息相关的中间值,但是这些中间值的相关性程度会受到具体操作和算法参数影响. Xu 等人[40]在 2020 年提出了选择密文的 SPA 攻击,通过选择不同密文对,可以最大差异化 Kyber 多项式乘法中的 *fqmul* 函数输出的能耗特征,中间值的能耗 P 在汉明重模型下可以形式化表示为

$$P = a \cdot HW(\boldsymbol{s}^{\mathrm{T}} \cdot \boldsymbol{u} \bmod q) + N,$$

其中,a 是比例因子,N 是高斯噪声. 私钥 s 可能的取值为$\{-2,-1,0,1,2\}$. 因此可以构造不同的密文使得 5 个密钥对应产生的能耗 P 具有差异,经过分析发现只需要 4 组密文即可区分出密钥的正确值.

必备条件:利用 SPA 分析格密码方案的 SCA 脆弱性,更依赖于能耗曲线的特征进行直观的区分,而且 SPA 容易受到噪声等的影响,可以对能耗曲线做预处理减小影响. 所以,具有可以被区分的特征是做 SPA 的必备条件. 此外,对不同的加密方案做攻击,其他必备条件也不一. 如对于 Park 等人[36]提出

《计算机学报》

的 SPA 攻击，除了具备可区分的特征之外，还要求在 8 位微控制器设备上运行 RLWE 加密方案，并假设攻击者可以在解密操作中选择不同的密文测量获取它们的功耗，同时认为 RLWE 加密方案的模量参数 q 为奇数.

4.1.2　DPA

DPA 是能耗分析攻击中使用范围较广、成功率较高的一种攻击方式. Wang 等人[41]对 NTRU 解密算法成功利用 DPA 恢复了私钥. 设密文为 c，私钥为 s，解密算法中核心计算 $m=s\cdot c \bmod q$，其中密文 $c=c_0+c_1X+c_2X^2+\cdots+c_{N-1}X^{N-1}$，密钥为 $s=s_0+s_1X+s_2X^2+\cdots+s_{N-1}X^{N-1}$，$s_i\in\{-1,0,1\}$，乘法过程采用 schoolbook 算法[42]. 攻击过程第一步将密文 $c_0,c_1,c_2,\cdots,c_{N-1}$ 设置为 $(0,0,0,\cdots,0)$，采集 100 条曲线取平均得到均值曲线；第二步将密文设置为 $(a,0,0,\cdots,0)$，其中 a 为密文数值范围中汉明重最大值，同样采集 100 条能耗曲线后得到均值曲线；最后计算两条均值的差分曲线，根据峰值情况判断密钥系数的值.

Xu 等人[40]于2020年在ARM平台对 Kyber KEM 用 DPA 进行了消息恢复. Kyber 实现为 pqm4 库中的标准实现，pqm4 为 ARM Cortex-M4 的后量子密码库. 通过算法 1 可以看出，变量 *mask* 的值和多项式系数的输出结果根据对应的消息比特不同而变化，根据参考曲线预先定位出最大泄漏点和最小泄漏点位置，对目标曲线的最大泄漏点与最小泄漏点功耗做差分，若大于阈值则认为消息比特为 1，反之为 0.

算法 1.　*poly_frommsg* 解码函数算法.

输入：Input message in *msg*[32]

输出：*coeffs*[ ]

1. FOR $i=0,\cdots,31$ do
2. FOR $j=0,\cdots,7$ do
3. $mask=-((msg[i]\_j)\&1)$;
4. $coeffs[8\cdot i+j]=mask\&((q+1)/2)$;
5. END FOR
6. END FOR
7. RETURN *coeffs*[ ];

另外，DPA 在格密码中也可被用于辅助其它目标的攻击. 如 Ravi 等人[43]利用 DPA 攻击 schoolbook 多项式乘法器和稀疏多项式乘法器得到私钥，进而辅助伪造签名，实施了针对 Dilithium 算法的签名伪造攻击.

必备条件：利用 DPA 攻击基于格的加密方案，攻击者无需预先了解被攻击设备的硬件架构即可执行分析，利用了能耗的数据依赖性. 而且，在“差分”的思想中，最重要的条件是两个能耗曲线之间的水平对齐. 另外，基于汉明距离或者汉明重模型的 DPA，通常认为能量消耗与中间值的汉明距离或汉明重之间具有正线性关系.

4.1.3　CPA

最初，文献[44]对 NTRU 在 RFID 卡上的实现进行了攻击，通过猜测 schoolbook 多项式乘法中密文系数和私钥系数乘法结果，计算中间值向量与功耗向量之间的皮尔逊相关系数，可在 25 000 条能耗曲线量下成功恢复私钥. 2020 年 Huang 等人对 NTRU Prime[45]进行了 CPA 攻击[46]，通过对多项式乘法中的乘法扫描法分析[47]，如过程 2 所示. 首先计算 e_i 的汉明重向量与能耗曲线之间的相关性，攻击出第一个非零的密钥比特，然后在此基础上猜测 e_i 的状态恢复其它比特.

过程 2.　多项式乘法的乘积扫描法.

1. $e_i=0, i\in\{0,1,\cdots,(2p-2)\}$
2. FOR $i=0$ to $(p-1)$
3. FOR $j=0$ to i
4. $e_i+=f_{i-j}\cdot c_j \pmod q$
5. FOR $i=p$ to $(2p-2)$
6. FOR $j=(i-p+1)$ to $(p-1)$
7. $e_i+=f_{i-j}\cdot c_j \pmod q$

2017 年 CCS 会议上 Espitau 等人[48]用电磁 CPA 攻击了 BLISS 签名中的多项式乘法；Aysu 等人[49]在 2018 年 HOST 会议上提出了一种针对格密码协议的水平 CPA 攻击，攻击通过猜测单次执行的多个中间值，并截取多个中间值对应的能耗特征放入曲线集合中计算相关性系数，对 NewHope 和 Frodo 的密钥交换协议进行了实验验证，单条能量迹下恢复密钥的成功率为 99%.

2020 年，Fournaris 等人[50]对 Dilithium 签名算法实施了 CPA 攻击. 在签名算法中需要执行 $Z=Y+C\cdot S_1$，其中 S_1 为密钥，C 为攻击者已知，因此可以选取 $C\cdot S_1$ 的结果存储到寄存器时的功耗进行分析. 攻击可以分为三个阶段：(1) 首先对除了密钥外的变量随机选取，多次执行签名，进而采集能耗曲线；(2) 然后根据多组 C 值计算攻击中间值的假设功耗向量；(3) 最后计算假设功耗向量与实测能耗向量之间的皮尔逊相关系数. 经过实验分析，CPA 可以有效地获取密钥的值.

必备条件：明文或密文是已知的，同时可以采集

计算机学报

密码设备在加密或解密过程中产生的能耗曲线. CPA 与 DPA 比较接近,更多的分析攻击是利用统计学中的皮尔逊相关系数进行的. Aysu 等人[49]提出的水平 CPA 攻击,这种攻击需要假设针对目标特定的中间寄存器架构的知识,并且认为汉明距离是特定设备的泄漏的很好近似.

4.1.4 TA

模板攻击需要建模阶段,属于一种 profile 的攻击手段. 2019 年 Bos 等人[51]针对 Frodo 方案,利用 TA 攻击成功恢复了 KEM 中的私钥. 攻击的核心思想为对 $sum=sum+\mathbf{A}[r,i]\cdot s[i]$ 操作的功耗建立模板,如算法 2 所示,然后对目标功耗曲线进行匹配,计算出贝叶斯条件概率,推断出正确密钥 $s[i]$.

算法 2. Frodo 中的矩阵向量乘法.

输入:$\mathbf{A}\in Z_q^{n\times n}, s, e\in Z_q^n$

输出:$b\leftarrow\mathbf{A}s+e$

1. $b\leftarrow e$
2. FOR $r=1,\cdots,n$ do
3. $sum\leftarrow 0$
4. FOR $i=1,\cdots,n$ do
5. $sum\leftarrow sum+\mathbf{A}[r,i]\cdot s[i]$
6. $b[r]\leftarrow(b[r]+sum) \bmod q$
7. RETURN b

2020 年,Ravi 等人[52]利用 PKE 及 KEM 中消息解码函数的泄漏,通过 TA 可以得到 100%成功率恢复消息. 整个攻击分为两个阶段,第一阶段利用泄漏检测方法 TVLA[53]进行泄漏点的选择,在此基础上采集不同消息值的能耗曲线,构建模板;那么在第二阶段,计算目标曲线与模板曲线之间的平方和作为评估相似度的标准,选择最相似的类别作为目标曲线对应的消息值. 同样地,对于 Saber、NewHope、Round5、LAC 和 Kyber 的解码函数都可以用该攻击思路进行攻击[54].

必备条件:模板攻击分析格密码方案的 SCA 脆弱性,首先需要攻击者有能力分析目标设备,或者能够获得与被攻击设备一致的且可被编程的加密设备,且攻击者需要获取大量的能耗曲线构建模板.

近两年逐渐出现了使用机器学习和深度学习进行格密码攻击. Aydin 等人[55]在 2020 年使用了 VGG 网络对 Frodo 和 NewHope 密钥交换协议成功进行了攻击,并且将此攻击扩展到并行硬件实现上,经过实验发现,该深度学习攻击的成功率比水平 CPA 攻击、TA 分别提高了 900%和 25%.

必备条件:一个高效的网络架构是利用机器学习和深度学习攻击格密码加密方案不可缺少的条件,如对 CNN 网络的超参数,学习率和训练迭代次数的合理选择,会影响到实际攻击的成功率.

4.2 攻击目标

本节针对格密码的各个算子进行侧信道安全性分析,探讨基于 LWE、RLWE 等问题格密码算法的通用性模块面临的侧信道攻击威胁,以及针对算子特点的侧信道攻击技术. 针对格密码算子的攻击分布图如图 3 所示.

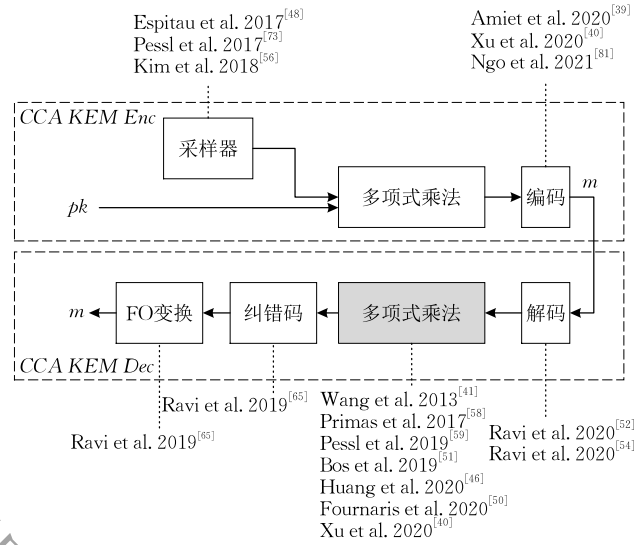

图 3 攻击格密码算子分布

4.2.1 高斯采样

高斯采样是格密码中不可或缺的一部分,直接影响到格密码的整体安全性和效率. 因此,高斯采样实际实现时的安全性是格密码在密码设备实际环境中所必须考虑的因素. 许多基于格的加密方案需要从离散高斯分布中采样,而离散高斯分布的参数是由特定方案的安全性证明来控制. 限定的设备并不能从一个离散的高斯分布中采样,所以限制在统计范围内接近它的分布中进行采样.

攻击目标:高斯采样产生侧信道泄漏的地方是其在签名生成期间生成的随机掩码 y_1、y_2. 离散高斯采样算法一般分为两种:积累分布表反演采样法(CDT)和 Knuth-Yao 采样法. 然而,这些算法有一个缺点是,本质上是在可变时间内运行的:迭代次数是未知的,会泄漏随机掩码 y_1、y_2. 由于算法的自身结构(需要多次启动等),从噪声迹线上的泄漏提取信息很困难,但仍然不能排除这种时序可变性造成的侧信道泄漏.

Espitau 等人[48] 2017 年在 CCS 会议上利用分支跟踪存储(BTS)分析 Knuth-Yao 采样算法,通过时间攻击恢复了 BLISS 签名生成算法中的密钥. 为了抵抗时间攻击,现有采样算法一般都为恒定时间

《计算机学报》

实现. Kim 等人[56]对恒定时间的高斯采样算法成功进行了单条侧信道攻击.

如算法 3 所示，攻击目标为算法的第 4～6 步，由于恒定时间的要求，对任意随机数，第 5 步都需要执行 l 次. 当随机数大于 CDT 表 T 中值时，'1'被累加到变量 G 中，而当相减的结果为正数时，'0'被累加到变量 G 中. 例如在 Frodo KEM 中，变量为 16 位，其中有 9 位用来采样，因此可以统计出对于负数值情况下，平均汉明重为 11.5，而正数情况下平均汉明重为 4.5. 因此，可以对于误差变量 e 采样过程进行 SPA，通过功耗特征推测 e 的值，再根据 $\boldsymbol{A}\cdot s=b-e$ 公式进行高斯消除求得密钥 s.

算法 3.　Frodo 中的矩阵向量乘法.

输入：CDF table T of length l,σ,τ

输出：Sampled value G

1. $G\leftarrow 0$
2. $rnd\leftarrow[0,\tau\sigma)\cap Z$ uniformly at random
3. $sign\leftarrow[0,1)\cap Z$ uniformly at random
4. FOR $i=0$ up to $l-1$ do
5. $\quad G+=(T[i]-rnd)\gg 15$
6. $G\leftarrow((-sign)\wedge G)+sign$
7. RETURN G

泄漏分析：根据式(1)可知，攻击中间值可选为第 5 行等号右边的值，该中间值对应的能耗值与敏感信息 $T[i]-rand$ 之间存在关联性，即 $l(T[i]-rand=1)<l(T[i]-rand=0)$，通过式(1)，可以根据采集到的能量迹特征推测出 $T[i]-rand$ 的值.

根据一条能量迹中正确密钥对应的中间值与错误密钥对应的中间值对应的能耗特征不同区分密钥，假设正确密钥对应能耗特征为 l^k，猜测密钥对应能耗特征为 l^{k^*}，根据式(1)可求出正确密钥 k.

4.2.2　多项式乘法

多项式乘法作为所有格密码中不可避免的关键操作，由于该操作的输入一个是已知的信息，一个是未知的敏感信息，这种情况非常适合实施侧信道攻击，所以一直以来都是侧信道攻击的重点. 而且多项式乘法是几乎所有基于格的加密方案高效实现的核心，对其攻击的成功意味着也可以攻击大量其他基于格的结构及其各自的实现.

Schoolbook 算法是常用的一种多项式乘法. Wang 等人[41]对 NTRU 解密算法中的 schoolbook 算法成功利用 DPA 恢复了私钥.

Huang 等人[46]提出了针对 NTRU Prime 算法中的多项式乘法的多种攻击方法. 针对操作数扫描法、稀疏乘法、乘积扫描法，分别提出了垂直相关能量攻击、水平深度相关能量攻击、在线模板攻击，均可以有效恢复密钥. NTRU Prime 算法是 NIST 后量子密码标准化项目第 2 轮的候选. 它的多项式环区别于基于 RLWE 的密码系统，同时避免了潜在的代数攻击. NTRU Prime 有两种基于格的密钥封装机制：Streamlined NTRU Prime 和 NTRU LPRime. Huang 等人[46]提出的多种攻击方法并不涉及上述两种机制的错误检测、编码和解码阶段. 传统的 NTRU 实现支持操作数扫描方法和稀疏乘法，相比之下，NTRU Prime 算法实现中采用了乘积扫描方法. 如过程 2 所示.

攻击目标：NTRU Prime 算法的参考实现在恒定时间的条件下利用乘积扫描方法实现了多项式乘法，这与其他具有数据依赖时间差异的实现不同. 如过程 2 第 4 行的操作，N 个随机密文 c 和一个固定的密钥 s，在每一次扫描进行多项式乘法的独立过程中，会生成相应的 e_{p-1}. 该信号可以作为中间值即攻击目标，通过采集其对应的轨迹进行侧信道分析.

在线模板攻击最初是针对椭圆曲线密码而提出来的，每个秘密标量位只有一个模板跟踪，因此可以实现单目标跟踪的完全私钥恢复. Huang 等人利用的在线模板攻击针对的是乘积扫描方法中的 e_{p-1}，工作原理如算法 4 所示. 首先，攻击者会从目标设备获取单个目标轨迹，将其划分为 p 个 n 维的目标向量，每个向量执行算法 4 的操作. 然后攻击者收集到三个模板踪迹，通过第 8 行的操作提取出三个模板向量. 通过比较目标向量和三个模板向量之间的相似性，相似性最高的模板向量成为最优猜测.

算法 4.　在线模板攻击.

输入：a ciphertext c

the power trace P of the e_{p-1} calculation

输出：a small weight-w polynomial $f\in R$

1. Partition P into $P_0,P_1,\cdots,P_{p-}$
2. P_i FOR $e_{p-1}+=f_{p-1-i}\cdot c_i(\mathrm{mod}\,q)$
3. $e_{p-1}\leftarrow 0$
4. FOR $i=0$ to $(p-1)$ do
5. $\quad$ FOR x in $\{-1,0,1\}$ do
6. $\quad\quad T_x\leftarrow$template vector of $(e_{p-1}+x\cdot c_i)$ mod
7. $\quad\quad f_{p-1-i}\leftarrow x^*$, where $\|P_i-T_{x^*}\|^2=\min\{\|P_i-T_{-1}\|^2,\|P_i-T_0\|^2,\|P_i-T_1\|^2\}$
8. $\quad\quad e_{p-1}+=f_{p-1-i}\cdot c_i(\mathrm{mod}\,q)$
9. RETURN f

泄漏分析：根据式(4)可知，攻击者根据算法 4，可以通过采集到的能量迹特征提取出三个模板向

量,即将样本曲线集合 L 按照假设能耗值 $\boldsymbol{H}_m^{k^*}$ 划分至不同集合,并计算均值曲线 $\overline{M}_i$ 和协方差矩阵 $\boldsymbol{\Sigma}_i$ 作为该类的模板$\{\overline{M},\boldsymbol{\Sigma}_i\}$.然后利用概率公式计算目标向量与模板匹配的概率值,再由式(4),正确密钥 k 可以被成功恢复.

为了提高多项式乘法的效率,数论变换算法(NTT)被用于实现多项式乘法.目前已经成为了格密码算法实现的必要模块(只要参数符合 NTT 要求,对于不符合参数要求的格密码需要额外转换的也可应用 NTT[57]).2017 年 Primas 等人[58]在 CHES 上提出了针对 NTT 的 SASCA(Soft Analytical Side-Channel Attacks)攻击.由于 NTT 的执行过程具有大量中间节点,而通过侧信道的方式可以充分利用这些节点的侧信息,共同推测输入值密钥的信息.攻击思路分为三步:(1)解密过程中选取 $INTT(NTT(c_1)\cdot NTT(r_2)+NTT(c_2))$为攻击目标,利用模板攻击对 INTT 功耗进行训练和匹配得到概率;(2)根据 NTT 算法构造因子图,并利用信任传播算法对因子图各个节点的概率计算得到 $INTT(NTT(c_1)\cdot NTT(r_2)+NTT(c_2))$的值;(3)利用格解码求解私钥 r_2.该攻击工作需要接近 100 万个模板,而且攻击过程在第 1 步需要目标操作具有时间差异信息.2019 年 Pessl 等人[59]在此基础上提出了更加具有实际应用意义的攻击,首先不再针对解密攻击私钥,而是攻击加密的交换对称密钥,这样 NTT 的输入数据范围也更窄,攻击复杂度低.另外,还做了两点优化:(1)在 NTT 变换中合并了节点,使得因子图变得更加简洁,信任传播算法效率更高;(2)利用消息阻尼以保证信任传播算法收敛,通过计算新消息和前一消息的加权平均值来抑制振荡.最终,将模板数量降低到 213 个,在 STM32F4 微控制器上对恒定时间的 Kyber 方案实现成功进行了攻击.

4.2.3 消息封装/解封装

密钥封装机制是一种包括公钥和私钥的方案,其中公钥用于创建包含随机选择的对称密钥的密文(封装),而私钥则被用于对密文的解密.消息编码和解码函数的泄漏是近两年的研究热点.并且与对前一个攻击算子的攻击目标不同,并不识别私钥,而是处理消息.2020 年 PQC 国际会议上,Amiet 等人[39]分析了消息编码 *ploy_frommsg* 函数的侧信道泄漏.

攻击目标:攻击是在消息编码期间执行的,消息编码函数将 256 位的消息或者封装密钥转换为其多项式表示,简单的实现容易受到定时攻击,所以 *refC* 通过 for 循环始终以恒定时间运行实现消息编码,如过程 1 所示.掩码计算如过程 1 第 5 行所示,处理后的消息位既不会在分支中泄漏,也不会在执行时间差异中泄漏,但是因为掩码仅包含 0 或 1.而消息比特为 0 和 1 时,对应的中间值能耗特征差异大,因此可以通过 SPA 的方式直接观测,即根据式(1)可以轻松区分出不同中间值,或者通过计算目标曲线与参考曲线的差距反推消息比特.

Sim 等人[60]在 2020 年报告了其利用消息编码对格密码的攻击效果.攻击目标为格密码 KEM 的封装过程的消息编码,利用机器学习的方法对能耗曲线进行训练和匹配,单条攻击得到短暂的会话密钥.在 ChipWhisperer UFO STM32F3 板卡上 Kyber,Saber 的攻击成功率 100%,FrodoKEM 的攻击成功率 79%.

同样地,消息解码的过程也存在侧信道泄漏.Ravi 等人[52,54]利用 PKE 及 KEM 中消息解码函数的泄漏,成功攻击了 Saber,NewHope,Round5,LAC,Kyber.

泄漏分析:首先进行泄漏点定位,然后构建解码泄漏不同消息值的模板,利用下面的公式计算目标曲线与各个模板之间得相似度:

$$p_i=\frac{1}{\sqrt{\pi^N|\boldsymbol{\Sigma}_i|}}\exp\left(-\frac{1}{2}(l-\overline{M}_i)\boldsymbol{\Sigma}_i(l-\overline{M}_i)^{-1}\right).$$

然后利用式(4)的原理,选择最相似的类别作为目标曲线对应的消息值.

4.2.4 纠错码

格密码的安全性建立在引入的噪声上,但是由于噪声的存在,无论是 LWE 方案还是 LWR 方案都存在一定的解密失败概率.许多方案通过调整它们的参数集来降低解密失败概率[61-62],还有许多方案依赖纠错码(ECC)来提高鲁棒性[63-64].

纠错码采用的是 XEf 纠错方案,是一种 f 位前向纠错分组码,在任何给定的码字中总能纠正至少 f 个错误.让待编码的 k 位消息编码为 $m=(m_{k-1},\cdots,m_0)$,其相应的二元多项式被定义为 $mp=m_{k-1}x^{k-1}+\cdots+m_0$.$XEf$ 是一个线性奇偶校验码,与一个有 $2f$ 个寄存器的大小为 l_i 的寄存器集 r 一起工作,其中满足 $r_i=mp \bmod (x^{l_i}-1)$,$i\in\{0,2f-1\}$.码字 c 由 μ 位的附加寄存器集 r 的消息 m 组成,其中 $\mu=k+\sum_{i=0}^{2f-1}l_i$.让我们将解密逻辑的解密码字输出表示为 $c=(m|r)$,解码计算通过接受到的消息 m 以及和 r 比较得到寄存器集 r',满足 $\sum_{i=1}^{2f}(r'_{(i,j \bmod l_i)}-$

$r_{(i,j \bmod l_i)}) \bmod 2 \geq (f+1)$条件的信息位将被反转. XEf 最大的优势在于它的编码和解码过程可以在恒定时间内实现，从而可以抵抗定时攻击，但是会通过电磁旁道泄漏关于码字的可利用信息. XEf 解码涉及决策操作，决定要在恢复的消息中翻转的位的位置.

攻击目标：2019 年 Ravi 等人[65]在 CHES 上分析了纠错码在侧信道方面的脆弱性. 其攻击目标为 XEf 纠错码，在 XEf 解码过程中的恢复消息步骤中包含了一个多位逻辑运算的操作，即判断对码字是否纠错的最后一个操作.

泄漏分析：当码字是合法时，与码字带有一个或多个错误位的内部通用寄存器值具有明显差异，采集到的电磁特征也有差别. 与式(1)或式(3)类似，在上述基础上，攻击者在解密过程中精心地选择密文，使生成的码字能够唯一地识别某个目标密钥系数的值，从而可以达到恢复私钥的目的.

4.2.5　FO 变换

基于格的密码 PKE 方案通常在选择明文模型下是安全的，但是却抵抗不了选择密文攻击(CCA)[66-67]. 因此，PKE/KEM 方案需要借助 Fujisaki-Okamoto 即 FO 变换[68]，进而转换为 CCA 下安全.

攻击目标：如算法 5 所示，当 $Ecc\_Used=0$ 时，PKE 之后的操作依赖于解密后得到的消息 m，作为攻击者，寄希望于可以通过侧信道观察到这些后续操作有关于 m 的差异行为，进而可以区分 $m=0$ 和 $m=1$，哈希操作 $\mathcal{G}$(算法 5 的第 8 行)是攻击者的攻击目标.

算法 5.　FO 转换中的 KEM.Decaps.

输入：sk, pk, ct, Ecc_Used

输出：K

1. $c'=PKE.Decrypt(sk, ct)$
2. IF $Ecc\_used=1$ THEN
3. 　$m=Ecc\_Dec(c')$
4. ELSE
5. 　$m=c'$
6. END
7. $r'=\mathcal{G}(m, pk)$
8. $ct'=PKE.Decrypt(pk, m, r')$
9. IF $ct'=ct$ THEN
10. 　RETURN $K=\mathcal{H}(r' \| rt')$
11. ELSE
12. 　RETURN $K=\perp$ or $K=\mathcal{H}(z \| rt')$　/* $z \in \mathcal{B}^{32}$
13. END

选择密文攻击是假设攻击者想要找到密文 c 的解密 $m \equiv c^d \pmod n$，其中 c 是任意整数. 攻击者选择整数 s，计算 $c' \equiv cs^e \pmod n$，并将 c' 发送给 Oracle. 如果 Oracle 说 c' 是 PKCS(The Public-Key Cryptography Standards 是一组公钥密码学标准)一致性，那么攻击者知道 ms 的前两个字节是 00 和 02. 同时这也意味着满足式子 $2 \cdot 2^{8(k-2)} \leq ms \bmod n < 3 \cdot 2^{8(k-2)}$. 通过收集几条这样的信息，可以得出 m.

攻击可以分为三个阶段. 在第一阶段，消息被隐藏，给出对应于未知消息 m_0 的密文 c_0. 在第二阶段，攻击者试图找到一个小值 s_i，满足 $c_0 (s_i)^e \bmod n$ 同时满足 PKCS 一致. 对于 s_i 的每一个成功值，攻击者利用以前关于 m_0 的知识计算出一组必须包含 m_0 的区间. 当只剩下一个区间时，第三阶段开始. 然后，攻击者有足够的关于 m_0 的信息来选择 s_i，使得 $c_0 (s_i)^e \bmod n$ 比随机选择的消息更有可能符合 PKCS. s_i 的大小逐渐增加，进而缩小 m_0 的可能范围，直到只剩下一个可能的值.

泄漏分析：FO 变换主要是通过解密后重加密，检查加密结果和密文是否一致来识别恶意/无效密文，若识别出恶意密文或无效密文则不会返回任何有用信息给攻击者. FO 变换在传统选择密文的数学模型下是安全的，主要原因在于在传统攻击模型下，FO 变换的操作对攻击者来说是一个黑盒. 若采用侧信道攻击的方式，则可以不通过最终返回结果推测敏感信息，而通过 FO 变换执行过程中的功耗或电磁信息即可推测.

Ravi 等人[65]在 2019 年 CHES 上提出了利用 FO 变换泄漏的选择密文攻击. 攻击目标选择为 CCA 安全的 KEM 解封装阶段，在解密操作之后的哈希函数操作. 在哈希函数中会对解密的消息进行运算，根据运算的功耗特征可以区分消息比特. 另外，结合选择密文实现了私钥的恢复.

4.3　攻击条件

格密码的密钥封装、签名等方案在实际应用场景中的侧信道攻击条件不同. 基于格的密钥交换协议建立一个会话密钥，以通过公共信道秘密地传递数字信息，然而，对密钥交换协议应用的侧信道攻击是更具挑战性的，因为密钥在协议每次执行后都会发生变化，因此对于这种场景下，侧信道攻击的条件就被限制在了单条能量迹上.

通常地，根据成功攻击所需要的能量迹(能耗曲线)数量可以将攻击方法分为单能量迹攻击和多能量迹攻击，如表 2 所示. 表中主要为针对 NIST 第 3 轮入

计算机学报

选算法(NTRU、Saber、Kyber 及备选算法 Frodo、NTRU Prime)对攻击对象的两种攻击技术,更多的攻击技术为单能量迹攻击即可恢复密钥或消息.为了提高单能量迹攻击的效果,可结合选择密文、在线模板、深度学习训练等模式开展新型攻击.

表 2 格密码的单条能量迹攻击与多能量迹攻击

	相关工作	敏感信息	攻击模型	攻击对象
单能量迹攻击	Amiet 等人 2020[39]	消息	SPA	NewHope
	Xu 等人 2020[40]	消息	选择密文+DPA	Kyber
	Ravi 等人 2020[52]	消息	Profile+DPA	Kyber,Saber 等
	Ravi 等人 2020[54]	消息	TA	Kyber,Saber 等
	An 等人[38]	私钥	SPA	NTRU
	Huang 等人 2020[46]	私钥	在线 TA	NTRU Prime
	Primas 等人 2017[58]	私钥	SASCA	Using NTT
	Pessl 等人 2019[59]	私钥	SASCA	Using NTT
	Bos 等人 2019[51]	私钥	TA	Frodo
	Kim 等人 2018[56]	私钥	SPA	Frodo
多能量迹攻击	Sim 等人 2020[60]	会话密钥	机器学习	NTRU Prime,NTRU 等
	Wang 等人 2013[41]	私钥	DPA	NTRU
	Xu 等人 2020[40]	私钥	选择密文+SPA	Kyber
	Huang 等人 2020[46]	私钥	CPA	NTRU Prime

密钥封装算法的直接应用是经过身份验证的密钥交换协议.新的协议标准,包括 TLS 1.3,越来越多地提倡和要求 PKE/KEM 使用临时的密钥对来实现正向保密.TLS 1.3 中使用 Diffie-Hellman 密钥交换的思路.如果每个连接使用新的(EC)DHE 密钥,则输出密钥是正向秘密.在 TLS 1.3 草图设计的密钥交换中,DH 密钥交换可以作为 KEM 的模块,其中 keygen 对应选择一个参数 x 作为密钥,得到 g^x.封装对应于选择一个参数 y,计算密文 g^y 和共享秘密 g^{xy}.然后去封装相应的共享秘密 g^{xy}.

TLS 会话开始时的密钥交换涉及量子后 TLS 密钥交换方案[69-70]中的一个 keygen、一个封装和一个去封装,如图 4 所示.一些实现以有限的正向保密为代价重复使用密钥.它通常限制更新规则.例如,Microsoft Windows TLS 库 Schannel 缓存密钥两小时[71].它限制了 DPA/CPA 所需的跟踪次数,使单能量迹线攻击更具威胁性.

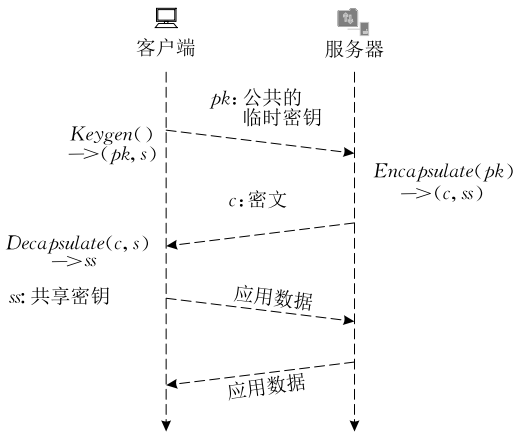

图 4 TLS 1.3 握手中的后量子 TLS 密钥交换

4.4 攻击实验

本节把目标放在 Saber 密钥封装方案,使用简单能耗攻击(SPA)、差分能耗攻击(DPA)、水平相关能耗攻击(HCPA)和模板攻击(TA)对其消息解码和多项式乘法进行攻击实验.展示了不同攻击模型的实际攻击效果.

在这一步中,我们使用了 Visual Studio 2019,PyCharm Community Edition 2021.2.2 等工具,它们运行在英特尔(R)核心(TM)i5-7300HQCPU 上,时钟频率为 2.50 GHz,16 GB 内存,运行在 64 位 Windows 环境下.而且,所有攻击实验中能耗曲线皆以仿真的形式得到,且实验均在相同的实验环境条件下进行.

4.4.1 Saber 密钥封装方案

目前,Saber 是 NIST 后量子标准化的第 3 轮后量子密钥封装机制入选算法.Saber 的安全性是基于带有舍入问题的模块学习(MLWR)的.PKE 的密钥生成、加密和解密如算法 6~8 所示.KEM 就是通过对 PKE 作 Fujisaki-Okamoto(FO)变换得到的.LWR 中的噪声是由舍入操作产生的,如果这种噪声在生成密钥时产生影响,会造成加密方案面临安全问题.Saber 设计者巧妙地避免了这种噪声的产生.而且由于模量,Saber 参考实现使用了 Toom-Cook、Karatsuba 和 schoolbook 乘法相结合的混合方法.

算法 6. Saber.PKE.*KeyGen*.

输入:l

输出:$pk=(seed_A,b),s$

1. $seed_A \leftarrow \mathcal{U}(\{0,1\}^{256})$
2. $\boldsymbol{A}=gen(seed_A)\in R_q^{l\times l}$
3. $r=\mathcal{U}(\{0,1\}^{256})$
4. $s=\beta_\mu(R_q^{l\times l};r)$

《计算机学报》

5. $b=((\boldsymbol{A}^{\mathrm{T}}s+h)\bmod q)\gg(\epsilon_q-\epsilon_p)\in R_p^{l\times 1}$

6. RETURN $pk=(seed_A,b),s$

算法 7.　Saber.PKE.*Enc*.

输入：$pk=(seed_A,b),m,r$

输出：$c=(c_m,b')$

1. $\boldsymbol{A}=gen(seed_A)\in R_q^{l\times l}$
2. IF r is not specified then THEN
3. $r=\mathcal{U}(\{0,1\}^{256})$
4. END IF
5. $s'=\beta_\mu(R_q^{l\times l};r)$
6. $b'=((\boldsymbol{A}^{\mathrm{T}}s+h)\bmod q)\gg(\epsilon_q-\epsilon_p)\in R_p^{l\times 1}$
7. $v'=\boldsymbol{b}^{\mathrm{T}}(s' \bmod p)\in R_p$
8. $c_m=(v'+h_1-2^{\epsilon_p-1}m \bmod p)\gg(\epsilon_q-\epsilon_T)\in R_T$
9. RETURN $c=(c_m,b')$

算法 8.　Saber.PKE.*Dnc*.

输入：$c=(c_m,b'),s$

输出：m'

1. $v'=\boldsymbol{b}'^{\mathrm{T}}(s \bmod p)\in R_p$
2. $m'=(v-2^{\epsilon_q-\epsilon_T}c_m+h_2 \bmod p)\gg(\epsilon_p-1)\in R_2$
3. RETURN m'

4.4.2　针对 Saber 消息解码函数的 SPA

由于 SPA 直接通过能耗曲线特征进行判断从进而恢复信息，本小节选择 Saber 的消息解码函数作为攻击目标，如过程 3 所示，$bytes[j]$可以作为中间值，能够区分 0 和 1 的 SCA 攻击者可以恢复 $m[i]$，并随后在单个跟踪中执行完整的消息恢复.

过程 3.　Saber KEM 的消息解码后打包操作.

```
1. void POLmsg2BS(uint8_t bytes[KEYBYTES],
   const unit16_t data[]SABER_N)
2. {
3.  size_t i,j;
4.  memset(bytes,0,KEYBYTES);
5.  FOR (j=0;j<KEYBYTES;j++)
6.  {
7.   FOR (i=0;i<8;i++)
8.   {
9.    bytes[j]=
10.     bytes[j]|((data[j*8+i]&0x01)≪i);
11.  }
12. }
13. }
```

必备条件：$bytes[j]$的 0 比特只存在两个可能的值 0 或 1，可以直接被区分，这满足执行简单能耗攻击的条件.

攻击目标：Saber 消息解码操作中的 $bytes[j]$的 0 比特位可以作为中间值被攻击，目标是恢复出解码后的消息. 如过程 3 的 9、10 行，内层第一次循环时，$bytes[j]$的值只能是 0 或 1，我们通过获得它的能耗值，可以建模区分出两个不同值得界限，从而确定目标密文解码时对应的值，处理消息恢复.

首先，针对 Saber 的 C 语言代码，基于 HW(汉明重)模型仿真出所需中间值 $bytes[j]$的能耗曲线，这里为了评估不同方差下的攻击成功率，分别在添加了不同方差 σ^2 的高斯噪声基础上进行仿真，得到能耗曲线 $L=HW(O)+N(0,\sigma^2)$，其中方差 σ^2 取值分别为 0.01、0.05、0.1、0.5、1、5、10. 我们选取了相同密文和固定密钥下的 2000 条和 5000 条仿真能耗曲线生成模板对其做攻击实验，分别记录成功率，如图 5、图 6 所示.

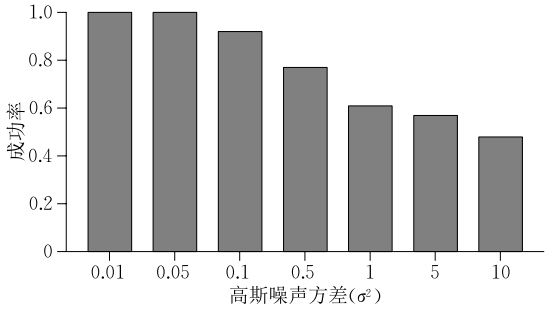

图 5　2000 条能耗曲线下简单能耗攻击

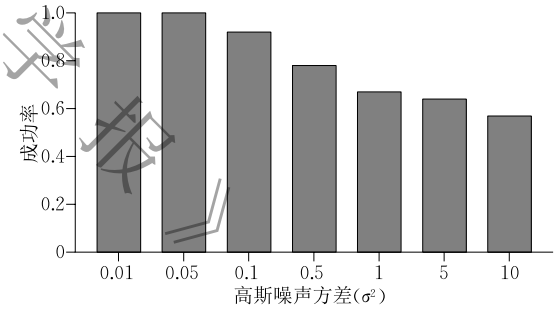

图 6　5000 条能耗曲线下简单能耗攻击

泄漏分析：在每条能耗曲线中，$bytes[j]$总是以相同的顺序出现在固定的位置，因此，0 和 1 的区别在整个能耗曲线中很容易分辨出来，所以通过 SPA 可以成功恢复出密文解码得到的信息. 而且可以看出，在攻击过程中，SPA 的成功率会受到噪声条件的影响，噪声的存在使得可以区分的能耗特征区分性减小，所以随着噪声的增大，攻击的成功率会随之降低. 目前已经有研究者注意到了这一点，他们选择在攻击之前对获得的仿真能耗曲线或者真实能耗曲线做预处理或者其他特殊处理，从而减小噪声对 SPA 的影响. 通过图 5 和图 6 的实验对比，在大量能耗曲线的基础上生成模板，可以一定程度上提高 SPA 的成功率，尤其是噪声较高的条件下.

《计算机学报》

4.4.3 针对 Saber 消息解码函数的 TA

在消息解码的基础上，Saber 随后会执行一个额外的操作，将消息位打包到一个字节数组 m 中，内存，表示为 $POLmsg2BS$，即过程 3. 在编译时，我们观察到编译器展开最内部的循环 8 次，从而导致字节存储消息，因此，这个操作是可以利用来作为攻击目标恢复信息. 这里，选择利用 Ravi 等人[52]提出的模板攻击做攻击实验.

必备条件：我们选择在仿真功耗条件下做模板攻击实验，完全具备作模板攻击必要的所有条件，如具备操作和目标设备上使用的相同加密方案的能力.

攻击目标：Saber 消息解码后打包操作中的 $bytes[j]$可以作为中间值被攻击，恢复出解码后的消息. 它涉及到为解密消息的不同值构建侧通道模板. 对于一个给定的目标设备，这只是一个一次性的过程，因为相同的模板可以用于多次攻击. 我们通过对 $bytes[j]$一个字节中的每一比特位建立模板，从而确定目标密文解密时该值的汉明重，进而恢复消息.

首先，我们假设可以获得与被攻击设备一致的且可被编程的加密设备. 这里为了评估不同方差下的攻击成功率，分别在添加了不同方差 σ^2 的高斯噪声基础上进行仿真，得到能耗曲线，其中方差 σ^2 取值分别为 0.01、0.05、0.1、0.5、1、5、10. 整个攻击分为两个阶段，第一阶段利用已知密文对能耗曲线依照 HW 模型分类，计算能耗曲线的平均值，构建模板，我们选择使用 2000 条仿真能耗曲线构建模板. 因为在仿真的过程中，由于攻击过相似，我们刻意地减少了每条能耗曲线上记录的能耗点，所以没有考虑原本方案中兴趣点的选择. 第二阶段，将获得的 HW 模板与从目标密文后获得的仿真能耗曲线进行匹配，根据匹配结果以执行消息恢复. 记录不同噪声条件下的攻击效果，如图 7 所示.

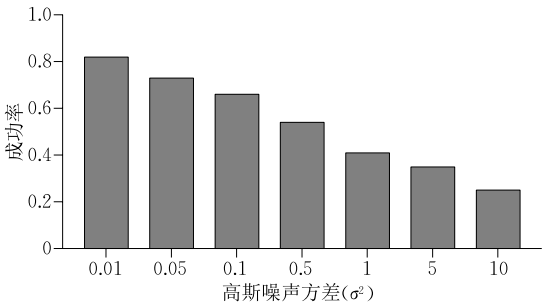

图 7 模板攻击 Saber 消息解码函数

泄漏分析：首先进行泄漏点定位，在 Saber 密钥封装方案中，找到了 $bytes[j]$这个泄漏点，然后构建解码泄漏不同消息值的模板，计算能耗曲线与各个模板之间得相似度. 然后利用式(4)的原理，选择最相似的类别作为目标曲线对应的消息值. 而且，从攻击的结果来看，模板攻击也会受到噪声的影响，随着噪声水平的不断升高，攻击成功率随之不断下降. 并且模板的建立需要大量仿真能耗曲线或者真实能耗曲线，模板的准确性也会影响到消息恢复的准确性.

4.4.4 针对 Saber 多项式乘法的 DPA

对于 Saber 密钥封装方案的多项式乘法，我们选择使用差分能耗攻击做攻击实验. 首先，我们将一组密文数据作为输入，执行加密运算，得到一组仿真能耗样本. 然后，将功耗样本根据中间值的 HW 模型输出分为两组，计算这两组样本均值的差分值，如果可以明显观察到能耗的偏差，则猜测密钥正确.

必备条件：只需要保证能耗曲线之间是水平对齐的，显然，仿真得到的能耗曲线是满足作攻击的要求的.

攻击目标：BS2POLVECq 和 BS2POLVECp 函数执行转换操作，然后过程 4 会调用 $InnerProd$ 函数，进而调用 $poly\_mul\_acc$ 函数和 $toom\_cook\_4way$ 函数来实现乘法，如过程 5、过程 6 所示，即差分能耗攻击主要针对的目标. 如过程 8 所示，$acc1$、$acc2$、$acc3$、$acc4$ 即密文，而 $acc5$、$acc6$ 则为私钥，$toom\_cook\_4way$ 函数调用的 $karatsuba\_simple$ 函数中，如过程 7 所示，$result\_final$ 值可作为攻击点，进而恢复私钥.

过程 4. Saber KEM.*Dec*.

```
1. void indcpa_kem_dec (const uint8_t sk[],const unit8_t ciphertext[],const unit8_t m[])
2. {
3.   BS2POLVECq(sk,s);
4.   BS2POLVECp(ciphertext,b);
5.   InnerProd(b,s,v);
6. }
```

过程 5. Saber KEM.*InnerProd*.

```
1. void InnerProd (const uint16_t b[][], const uint16_t s[][], unit16_t res[])
2. {
3.   FOR (i=0;i<SABER_L;i++)
4.     poly_mul_acc(b[i],s[i],res);
5. }
```

过程 6. Saber KEM.*poly_mul_acc*.

```
1. void poly_mul_acc (const uint16_t b[][], const uint16_t s[][], unit16_t res[])
2. {
3.   toom_cook_4way(b,s,res);
4. }
```

过程 7. Saber KEM.*toom_cook_4way*.

```
1. void poly_mul_acc (const uint16_t *a, const uint16_t
   *b, unit16_t *res)
2. {
3.  Split a1 to A0,A1,A2,A3;
4.  Split b1 to B0,B1,B2,B3;
5.  Calculate aw1,…,aw7;
6.  Calculate bw1,…,bw7;
7.  karatsuba_simple(aw1,bw1,w1);
8.  …;
9.  karatsuba_simple(aw7,bw7,w7);
10. }
```

过程 8. Saber KEM.*karatsuba_simple*.

```
1. void karatsuba_simple (const uint16_t *a_1, const
   unit16_t *b_1, const unit16_t *result_final)
2. {
3.  FOR (i=0; i<16; i++)
4.  {
5.   acc1=a_1[i]; acc2=a_1[i+16];
6.   acc3=a_1[i+32]; acc4=a_1[i+48];
7.   FOR (j=0; j<16; j++)
8.   {
9.    acc5=b_1[j]; acc6=b_1[j];
10.   result_final[i+j]=result_final[i+j]+
11.     overflowing_mul(acc1,acc5);
12.  }
13. }}
```

能耗曲线的获取仍然采取仿真的形式. 将多组密文数据输入 Saber 的加密方案中，将多项式乘法过程中 *result_final* 的值作为中间值 O，这里为了评估不同方差下的攻击成功率，分别在添加了不同方差 σ^2 的高斯噪声基础上进行仿真，得到能耗曲线 $L=HW(O)+N(0,\sigma^2)$，其中方差 σ^2 取值有三个水平，分别为 1、5、10. 分别利用不同数量的仿真能耗曲线对做攻击实验，记录 10 次攻击成功率，如图 8 所示. 在仿真能耗曲线的过程中，要求加密所使用的密钥保持不变.

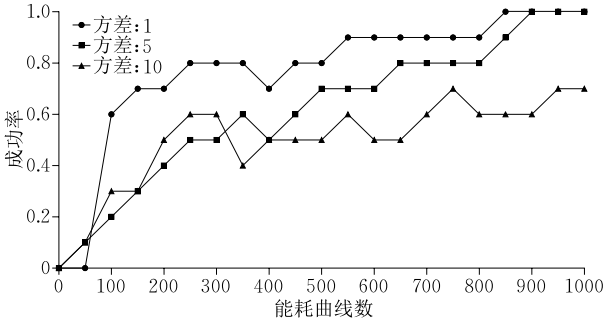

图 8　差分能耗攻击 Saber 多项式乘法

泄漏分析：从攻击的结果可以看到的是，不同噪声条件下差分能耗攻击的表现效果仍有差别. 由于我们只针对 1 个字节的密钥进行攻击，在较少的仿真能耗曲线数量下，仍然可以成功对 Saber 密钥封装方案中多项式乘法进行攻击. 较大噪声条件下的能耗曲线，即使利用大量的能耗曲线数，攻击的成功率仍然很低.

4.4.5　针对 Saber 多项式乘法的 HCPA

与 DPA 攻击类似，Saber 密钥封装方案的多项式乘法还有另一个可攻击点，我们选择水平相关能耗攻击(HCPA)，利用能耗曲线与被处理数据的汉明权重之间的相关性因子进行分析. *overflowing_mul* 操作的输出作为攻击利用的中间值 O，如过程 8 所示. 为了评估在不同噪声条件下相关能耗攻击的攻击成功率，在 HW 模型基础上，加上方差 σ^2 分别为 1、5、10 的高斯噪声，获得能耗曲线 $L=HW(O)+N(0,\sigma^2)$. 在仿真能耗曲线的过程中，仍然要求使用同一种密钥. 然后猜测 Saber 密钥封装的时候所使用的密钥，根据密文和密钥计算出中间值 *overflowing_mul* 输出的汉明权重，计算其和能耗之间的相关系数. 相关系数最高的即对应猜测正确的密钥. 分别利用不同数量的仿真能耗曲线对其做攻击实验，记录 10 组攻击成功率，如图 9 所示.

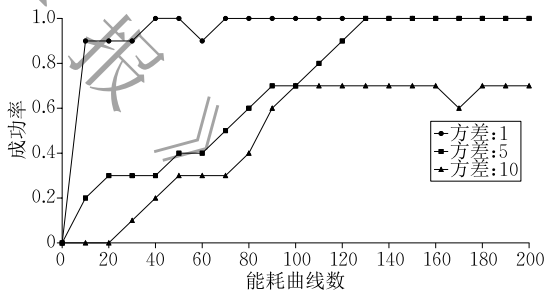

图 9　水平相关能耗攻击 Saber 多项式乘法

必备条件：对 *overflowing_mul* 函数有着足够的认知，并且认为汉明重是特定设备的泄漏的很好近似.

攻击目标：与差分能耗攻击类似，同样选择 Saber 封装方案中的多项式乘法操作作为分析目标. 不同的是，把多项式乘法 *karatsuba_simple* 函数中的 *overflowing_mul* 输出作为水平相关能耗分析的攻击点，从而恢复出加密私钥.

泄漏分析：*overflowing_mul* 函数的输出可以作为中间值，可以计算得到仿真能耗向量与假设能耗向量之间的皮尔逊相关系数，根据式(3)，即可得

《计算机学报》

到猜测密钥,相关性最大即为正确密钥.这里可以从结果中看出,噪声同样会对水平相关能耗攻击有影响.同时,在相同能耗曲线数基础上,与差分能耗攻击的攻击效果相比,由于对每条能耗曲线上的能耗点都作分析操作,水平相关能耗攻击的攻击成功率更高.而且攻击成功所需要的仿真能耗曲线量更少,差分能耗攻击则需要攻击大量的能耗曲线.

4.4.6 对已有攻击方法的小结

为了进一步展示已有攻击方法的攻击思路和攻击算子,本小节对文中出现的主要攻击方法,从攻击条件、攻击原理、攻击目标和敏感信息等多个维度作了对比,如表 3 所示.

表 3 对已有攻击模型的横向比较

	简单能耗攻击	模板攻击	差分能耗攻击	相关能耗攻击
攻击条件	具有直观区分的能耗特征	具有分析目标设备的能力	能耗曲线之间水平对齐	具有分析目标设备的能力
敏感信息	消息、私钥	消息、私钥	消息、私钥	消息、私钥
攻击原理	建立可区分能耗特征的模板	利用大量能耗曲线建立完美的模板	建立中间值与能耗值之间的关系,计算不同能耗曲线的差分值	计算能耗向量与假设能耗向量之间的皮尔逊相关系数
是否需要建模	是	是	否	否
单(多)能量迹攻击	两者皆可	单能量迹攻击	两者皆可	两者皆可
已有研究及其攻击目标	Park 等人 2016[36](消息封装/解封装) An 等人 2018[38](消息封装/解封装) Amiet 等人 2020[39](消息封装/解封装) Xu 等人 2020[40](消息封装/解封装)	Huang 等人 2020[46](多项式乘法) Bos 等人 2019[51](多项式乘法) Ravi 等人 2020[52](消息封装/解封装) Ravi 等人 2020[54](消息封装/解封装)	Xu 等人 2020[40](消息封装/解封装) Wang 等人 2013[41](多项式乘法) Ravi 等人 2018[43](多项式乘法)	Huang 等人 2020[46](多项式乘法) Espitau 等人 2017[48](高斯采样) Aysu 等人 2018[49](多项式乘法) Fournaris 等人 2020[50](多项式乘法)

从攻击条件来看,简单能耗攻击是从时间维度之间对能耗曲线之间的特征区分,而差分能耗攻击则需要能耗曲线之间为水平对齐的,这也说明,不同的能耗攻击方法对攻击条件的需求是有所差别的.多项式乘法作为所有格密码加密方案中的核心操作,因为其本身的特点,即该操作的输入一个是已知的信息,一个是未知的敏感信息,成为了已有攻击方法的重点目标.

此外,大部分的攻击方法主要聚焦的敏感信息是在加密方案的消息和私钥两个方面.

5 格密码防护方案的攻击

由于格密码面临着侧信道攻击威胁,为了安全起见,逐渐发展了适合格密码的侧信道防护方案.侧通道攻击的实现基于这样一个事实,即加密设备的能量消耗取决于该设备执行的加密算法的中间值.因此,抵抗能耗分析攻击的想法是减少甚至消除这种依赖性.常用的方法是隐藏技术和掩码技术,隐藏技术和掩码技术的目标即切断被处理的数据值与设备能耗之间的联系,使能量消耗与所执行的密码算法的中间值之间不存在依赖关系.

隐藏对策的目标是减轻密码设备的能量消耗与设备所执行的操作和所处理的中间值之间的相关性.为了抵抗格密码的侧信道攻击,乱序操作被用做高斯采样器的低代价防护手段[72].Pessl 等人[73]在 2017 年对 BLISS 格密码签名方案的乱序防护进行了攻击.对于乱序操作的攻击难点在于无法知道功耗特征恢复出来的信息对应的真实顺序,因此,对于第一个位置所有可能的对应关系进行穷举,通过匹配功耗特征得到一个概率,再对下一个位置用贝叶斯条件概率计算,直到所有位置计算完成,对应概率最大的即为恢复结果.

乱序操作和插入时间片等在时间维度上对能耗特征造成偏移,可以一定程度上减轻侧信道攻击威胁,但是侧信道泄漏并未从本质上消除.通过对加密过程中的所有数据进行随机化,掩码方案破坏了功耗/电磁信号与敏感数据之间的相关性,从而在算法层面实现了可验证的安全保护.在现有的方法中,它已成为应用最广泛的侧信道防护方法.

2015 年 Reparaz 等人[74]在 CHES 会议上提出了一种 RLWE 的掩码方案.在无保护的 RLWE 解密过程中,恢复的明文是首先通过对密钥执行多项式算术然后解码结果来计算的.所以这种主要是一阶掩码的方案,它的防护思想是将密钥算术拆分为两个共享因子,利用掩码解码器进行掩码.掩码

RLWE 解密的输出是布尔掩码共享因子，适用于对称密钥派生. 在 Virtex-II FPGA 硬件上实现需要大约 2000LUT，比无防护增加了 20%，需要 7478 时钟周期，无防护的 2.6 倍；在 ARM cortex-M4 上实现比无防护需要多 5.2 倍周期. 为了避免掩码方案中解码器的开销，Reparaz 等人[75]在 2016 年 PQC 会议上又提出了可利用现有 RLWE 加密方案的加法同态特性，对随机消息的加密计算加法掩码. 与 CHES2015 掩码方案不同的是，不需要掩码解码器，依然用传统无掩码的解码器，这是因为在他们的加法同态掩蔽方案中，解码器的输入是对密钥 s 进行适当解密后产生的系数，因此输入系数分布在 0 或 $q/2$ 附近. 此外，该方案不仅容易实现，而且无论是软件实现还是硬件实现，实现复杂度都低于 CHES2015 掩码方案. 并且这种掩码方案思路是较为通用的，也可用于其他加法同态的加密方案中. Oder 等人[76]在 2018 年 CHES 上通过对算数掩码的变换，使得不需要 CHES 2015 工作里面的解码器，同样可以解码出消息，而且为了充分保护探针模型中的密钥和消息，他们需要一个掩码噪声采样器进行重新加密，并提供了相应的保护二项式采样器的第一个设计.

Barthe 等人[77]在 2018 年 CCS 会议上提出了针对格密码签名的可证明安全任意阶掩码方案. Bos 等人[78]针对 Kyber 加密方案提出了一阶和高阶的掩码实现. 他们在实现中引入了两种新技术来实现的，一是提出了用于一位压缩运算的高阶算法，这种算法基于一个可以应用于素数模的掩码位切片的二进制搜索. 二是为了避免对密文压缩的掩码同时能够以任意顺序进行实例化，提出了能够比较未压缩的掩码多项式和压缩的公共多项式的新技术. 除此之外，针对 Saber、NTRU、Dilithium 等格密码的掩码方案也不断被提出[79-81].

2017 年 Primas 等人[58]在 CHES 上提出的 SASCA 对掩码 RLWE 方案成功进行了攻击. 在 2015 年 CHES 提出的 RLWE 掩码方案中[74]，私钥 r_2 被拆分为 r_2' 和 r_2''，满足 $r_2 = r_2' + r_2'' \bmod q$. 随后多项式乘法、加法、INTT 对两个因子分别执行. 最后解码步骤需要将两个 INTT 输出输入到解码器中，输出 m' 和 m''，满足 $m = m' + m'' \bmod q$. 因此，Primas 等人对两个 INTT 操作分别构建因子图，并用信任传播算法计算得到 r_2' 和 r_2'' 的值，即可得到私钥的值.

同样地，针对 NTT 实现的多项式乘法，Kim 等人对 Dilithium 的掩码方案[81]进行了单条攻击[82]. 区别在于攻击目标为两个因子的 NTT 变换，采用 CNN 网络对两个因子 NTT 变换的能耗曲线进行训练，每一条曲线的标签为私钥值，攻击阶段对单条能量迹的相应位置放入训练好的 CNN 网络中，输出的预测标签即为攻击的私钥. 2019 年 Schamberger 等人实现了对 NTRU 的掩码方案的二阶攻击[83]，攻击目标是多项式乘法的掩码实现[80]，解密阶段对密文分拆为两个因子：$e_m = e + masks$，私钥 f 分别与 e_m 和 $masks$ 进行多项式乘法，$m' = f \cdot e_m = f \cdot (e + masks)$，$m'' = f \cdot masks$. 攻击者通过对 $f \cdot e_m$ 和 $f \cdot masks$ 的功耗做归一化乘法处理，得到的结果再和中间值的汉明重向量计算相关性系数，选择相关性系数最大值对应的值即为私钥.

2021 年 Ngo 等人针对 Saber 的掩码方案[79]成功进行了攻击[84]. 攻击思路为利用对掩码后变量 $m[j] \oplus r[j]$ 单比特功耗和掩码变量 $r[j]$ 单比特功耗进行深度学习训练和匹配. 攻击的函数为 $poly2MSG$ 或者 $ploy\_A2A$ 函数. 执行过程中对消息单比特编码操作. 用 TVLA 对不同函数或不同字节不同比特的泄漏高低进行解释. 在恢复消息 m 存在误差的情况下，进行长密钥的恢复. 利用私钥比特和消息比特之间的代数关系对恢复的消息修正.

6　面临的问题与挑战

格密码在后量子密码中占据了重要角色，其侧信道安全性是综合衡量算法安全性的必不可少的指标，因此，面向格密码的能耗分析攻击技术研究是当前 NIST 后量子算法征集形成标准乃至后量子密码走向实际应用的重要课题.

针对格密码的能耗分析攻击相关研究发展具有以下几个特点：

(1) 攻击对象方案新，安全评估不全.

能耗分析攻击对于开发和评估格密码方案安全具有很大的威胁，由于许多格密码方案的新颖性，还有很多安全漏洞尚未评估. 因此近两年针对新标准中或改进的格密码方案不断提出攻击方法，目前仍有许多方案中的操作脆弱性有待评估.

(2) 攻击复杂度高，效率有待提高.

现有攻击点主要为采样器、消息封装/解封装、多项式乘法、FO 变换等操作，对于一条能量迹中只利用了单点泄漏信息，效率较低. 根据不同算子的输入参数和运算特点，泄漏程度也不同，如何联立不同

算子的泄漏进而提高攻击成功率或效率是待研究的问题.

(3)攻击种类多,缺少统一度量.

现有攻击模型种类多样,均可恢复格密码的密钥信息或消息,但对于格密码与传统密码的侧信道攻击不同之处在于,传统密码的攻击中间值相对固定,而挖掘格密码的与敏感信息相关中间值相对困难,单纯把攻击所需能量迹条数或成功率、猜测熵等传统侧信道度量指标作为评价格密码侧信道脆弱性标准,不能全面反映攻击成本,因此,缺少统一的针对格密码甚至后量子密码的侧信道脆弱性度量方法.

(4)防护手段单一,难以抵抗攻击.

针对这些侧信道攻击,许多工作也提出了格密码的防护方案,相比于针对传统加密算法的基于感知放大逻辑、波形动态差分逻辑、t 隐私逻辑电路,当前的防护方案发展仍在初期.

而且从图 10 中可以看出,大多防护方案均已被攻破,剩下的三个防护方案中,有一个方案用的是同态加密的思想,开销较大;另外两个是满足可证明安全的高阶安全掩码方案,难以在实际场景特别是物联网嵌入式密码设备中应用,开销仍然是当前未解决的问题.

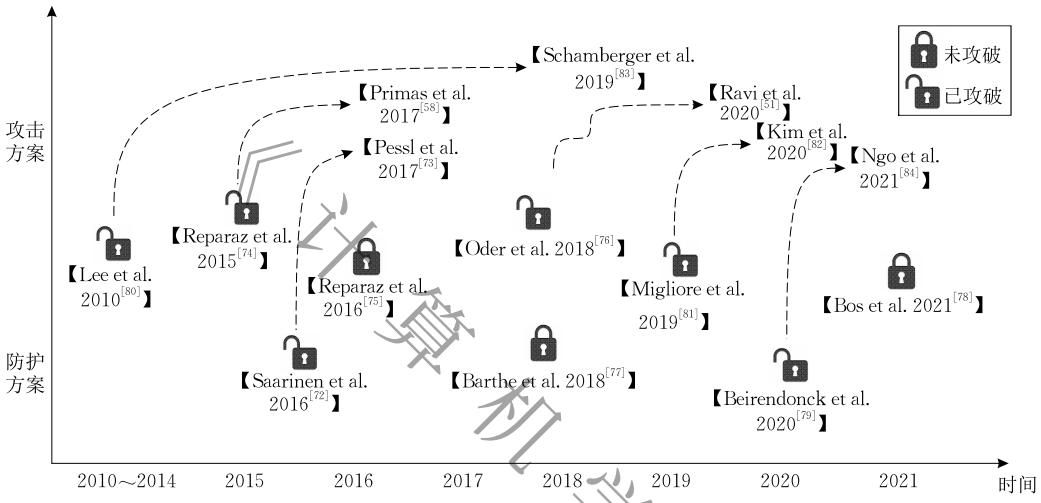

图 10 格密码的防护方案及针对防护的攻击

通常地,抵抗能耗分析攻击的方式主要包含乱序、掩码、互补逻辑等,互补逻辑的原理是在除原来功能电路外,额外设计功耗互补电路,以使得整体功耗平衡,然而其缺点也显而易见,即实现代价较高,目前该方式在格密码方案上的效果尚未被验证.另外,如何将乱序与掩码更好的有机结合在一起一直是防护方案的研究方向[85],对于格密码的高效结合防护方案将是标准成熟过程中的研究热点之一.

7 总 结

能耗分析攻击已经被证明了在密码设备上的严重威胁,因此对于格密码等新型密码的侧信道安全性引起了学术界和工业界的广泛关注.本文从攻击模型、攻击目标、攻击条件等不同角度对面向格密码的攻击技术进行了分类和描述,从攻击模型对比传统密码的侧信道攻击区分,从攻击目标分析格密码各个算子模块的安全性程度,从攻击条件角度梳理当前格密码在不同应用场景的侧信道威胁性.当前针对格密码的侧信道攻击已经有了一些攻击成果,但在攻击效率、评价指标等方面仍然存在不足,另外,现有防护方案无法满足安全和效率的需求,设计兼顾效率与安全的轻量化防护方案是未来的研究方向之一.

参 考 文 献

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 1999, 41(2): 303-332

[2] Sui Han, Wu Wen-Ling. Research status and development trend of posterior quantum symmetric cryptography. Journal of Electronics & Information Technology, 2020, 42(2): 287-294(in Chinese)
(眭晗, 吴文玲. 后量子对称密码的研究现状与发展趋势. 电子与信息学报, 2020, 42(2): 287-294)

[3] Wang Yong-Li, Xu Qiu-Liang. Review on the principle and research progress of quantum computing and quantum cryptography. Journal of Computer Research & Development, 2020, 57(10): 2015-2026(in Chinese)

(王永利，徐秋亮. 量子计算与量子密码的原理及研究进展综述. 计算机研究与发展，2020，57(10)：2015-2026)

[4] Alagic G，Alperin-Sheriff J M，Apon D，et al. Status report on the first round of the NIST post-quantum cryptography standardization process. USA：US Department of Commerce，NIST，NISTIR 8240，2019

[5] Second Round Public Key Algorithm. [2020-10-25]. https://sfjs.cacrnet.org.cn/site/term/list_77_1.html(in Chinese)
(第 2 轮公钥算法. [2020-10-25]. https://sfjs.cacrnet.org.cn/site/term/list_77_1.html)

[6] Roy K S，Kalita H K. A survey on post-quantum cryptography for constrained devices. International Journal of Applied Engineering Research，2019，14(11)：2608-2615

[7] Lu X，Liu Y，Zhang Z，et al. LAC：Practical ring-LWE based public-key encryption with byte-level modulus. IACR Cryptology ePrint Archive，2018：1009

[8] Zhang J，Yu Y，Fan S，et al. Improved lattice-based CCA2-secure PKE in the standard model. Science China Information Sciences，2020，63(8)：1-22

[9] Li Y，Zhu J，Huang Y，et al. Single-trace side-channel attacks on the toom-cook：The case study of saber. IACR Transactions on Cryptographic Hardware and Embedded Systems，2022(4)：285-310

[10] Bhasin S，D'Anvers J P，Heinz D，et al. Attacking and defending masked polynomial comparison for lattice-based cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems，2021，2021(3)：334-359

[11] Xagawa K，Ito A，Ueno R，et al. Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Singapore，Singapore，2021：33-61

[12] Zhang F，Yang B，Dong X，et al. Side-channel analysis and countermeasure design on arm-based quantum-resistant SIKE. IEEE Transactions on Computers，2020，69(11)：1681-1693

[13] Kannwischer M J，Pessl P，Primas R. Single-trace attacks on Keccak. IACR Transactions on Cryptographic Hardware and Embedded Systems，2020，2020(3)：243-268

[14] Hassan S，Gridin I，Delgado-Lozano I M，et al. Déjà Vu：Side-channel analysis of Mozilla's NSS//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York，USA，2020：1887-1902

[15] Kubota T，Yoshida K，Shiozaki M，et al. Deep learning side-channel attack against hardware implementations of AES. Microprocessors and Microsystems，2020，87：103383

[16] Xu S，Wang W，Lu X，et al. Side channel attack of multiplication in GF(q)-application to secure RSA-CRT. Science China Information Sciences，2018，62(3)：1-3

[17] Abarzúa R，Valencia C，Lopez J. Survey on performance and security problems of countermeasures for passive side-channel attacks on ECC. Journal of Cryptographic Engineering，2021，11(1)：71-102

[18] Alagic G，Alperin-Sheriff J，Apon D，et al. Status report on the second round of the NIST post-quantum cryptography standardization process. USA：US Department of Commerce，NIST，NISTIR 8309，2020

[19] Walters M，Roy S S. Constant-time BCH error-correcting code//Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS). Seville，Spain，2020：1-5

[20] Schamberger T，Renner J，Sigl G，et al. A power side-channel attack on the CCA2-secure HQCKEM//Proceedings of the 19th Smart Card Research and Advanced Application Conference (CARDIS2020). Virtual Event，2020：119-134

[21] Gellersen T，Seker O，Eisenbarth T. Differential power analysis of the picnic signature scheme//Proceedings of the 12th International Conference on Post-Quantum Cryptography. Daejeon，Republic of Korea，2021：177-194

[22] Liu Y，Zhou Y，Sun S，et al. On the security of lattice-based fiat-shamir signatures in the presence of randomness leakage. IEEE Transactions on Information Forensics and Security，2020，16：1868-1879

[23] Taha M，Eisenbarth T. Implementation attacks on post-quantum cryptographic schemes. IACR Cryptology ePrint Archive，2015：1083

[24] Wu Wei-Bin，Liu Zhe，Yang Hao，Zhang Ji-Peng. Survey of side-channel attacks and countermeasures on post-quantum cryptography. Journal of Software，2021，32(4)：1165-1185 (in Chinese)
(吴伟彬，刘哲，杨昊，张吉鹏. 后量子密码算法的侧信道攻击与防御综述. 软件学报，2021，32(4)：1165-1185)

[25] Drăgoi V，Richmond T，Bucerzan D，et al. Survey on cryptanalysis of code-based cryptography：from theoretical to physical attacks//Proceedings of the 2018 7th International Conference on Computers Communications and Control (ICCCC). Oradea，Romania，2018：215-223

[26] Chowdhury S，Covic A，Acharya R Y，et al. Physical security in the post-quantum era. Journal of Cryptographic Engineering，2022(12)：1-37

[27] Dong Ya-Hui. Research on LWE Public Key Encryption Scheme and Circuit Realization[M. S. dissertation]. Huazhong University of Science and Technology，Wuhan，2016(in Chinese)
(董亚辉. LWE 公钥加密方案的研究与电路实现[硕士学位论文]. 华中科技大学，武汉，2016)

[28] Gao Xin-Wei. Construction and Application of Post-Quantum Key Exchange Protocol Based on RLWE [Ph. D. dissertation]. Beijing Jiaotong University，Beijing，2019(in Chinese)
(高昕炜. 基于 RLWE 的后量子密钥交换协议构造和应用[博士学位论文]. 北京交通大学，北京，2019)

[29] Micciancio D，Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing，2007，37(1)：267-302

[30] Banerjee A，Peikert C，Rosen A. Pseudorandom functions and lattices//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin，Heidelberg，Germany，2012：719-737

[31] Xia Kun-Xian. Implementation of NTRU subdomain attack algorithm and realization of mathematical transformation [M. S. dissertation]. Shandong University，Jinan，2017(in Chinese)

《计算机学报》

(夏坤贤. NTRU 问题子域攻击算法实现及数论变换的实现[硕士学位论文]. 山东大学, 济南, 2017)

[32] Le T H, Canovas C, Clédiere J. An overview of side channel analysis attacks//Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. Tokyo, Japan, 2008: 33-43

[33] Kocher P, Jaffe J, Jun B. Differential power analysis//Proceedings of the Annual International Cryptology Conference. Berlin, Germany, 1999: 388-397

[34] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany, 2004: 16-29

[35] Chari S, Rao J R, Rohatgi P. Template attacks//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany, 2002: 13-28

[36] Park A, Han D G. Chosen ciphertext simple power analysis on software 8-bit implementation of Ring-LWE encryption//Proceedings of the 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST). Yilan, China, 2016: 1-6

[37] Liu Z, Seo H, Roy S S, et al. Efficient Ring-LWE encryption on 8-bit AVR processors//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany, 2015: 663-682

[38] An S, Kim S, Jin S, et al. Single trace side channel analysis on NTRU implementation. Applied Sciences, 2018, 8(11): 2014

[39] Amiet D, Curiger A, Leuenberger L, et al. Defeating NewHope with a single trace//Proceedings of the International Conference on Post-Quantum Cryptography. Paris, France, 2020: 189-205

[40] Xu Z, Pemberton O, Roy S S, et al. Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of Kyber. IEEE Transactions on Computers, 2021, 71(9): 2163-2176

[41] Wang A, Zheng X, Wang Z. Power analysis attacks and countermeasures on NTRU-based wireless body area networks. KSII Transactions on Internet and Information Systems (TIIS), 2013, 7(5): 1094-1107

[42] Khachatrian G H, Kuregian M K, Ispiryan K R, et al. Fast multiplication of integers for public-key applications//Proceedings of the International Workshop on Selected Areas in Cryptography. Berlin, Germany, 2001: 245-254

[43] Ravi P, Jhanwar M P, Howe J, et al. Side-channel assisted existential forgery attack on Dilithium—A NIST PQC candidate. IACR Cryptology ePrint Archive, 2018: 821

[44] Atıcı A C, Batina L, Gierlichs B, et al. Power analysis on NTRU implementations for RFIDs: First results//Proceedings of the 4th Workshop on RFID Security 2008. Budapest, Magyarország, 2008: 1-11

[45] Bernstein D J, Chuengsatiansup C, Lange T, et al. NTRU prime: Reducing attack surface at low cost//Proceedings of the International Conference on Selected Areas in Cryptography. Ottawa, Canada, 2017: 235-260

[46] Huang W L, Chen J P, Yang B Y. Power analysis on NTRU prime. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1): 123-151

[47] Hutter M, Wenger E. Fast multi-precision multiplication for public-key cryptography on embedded microprocessors//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany, 2011: 459-474

[48] Espitau T, Fouque P A, Gérard B, et al. Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongSwan and electromagnetic emanations in microcontrollers//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 1857-1874

[49] Aysu A, Tobah Y, Tiwari M, et al. Horizontal side-channel vulnerabilities of post-quantum key exchange protocols//Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). Washington, USA, 2018: 81-88

[50] Fournaris A P, Dimopoulos C, Koufopavlou O. Profiling dilithium digital signature traces for correlation differential side channel attacks//Proceedings of the International Conference on Embedded Computer Systems. Samos, Greece, 2020: 281-294

[51] Bos J W, Friedberger S, Martinoli M, et al. Assessing the feasibility of single trace power analysis of frodo//Proceedings of the International Conference on Selected Areas in Cryptography. Calgary, AB, Canada, 2018: 216-234

[52] Ravi P, Bhasin S, Roy S S, et al. Drop by drop you break the rock-exploiting generic vulnerabilities in lattice-based PKE/KEMs using EM-based physical attacks. IACR Cryptology ePrint Archive, 2020: 549

[53] Standaert F X. How (not) to use Welch's T-test in side-channel security evaluations//Proceedings of the International Conference on Smart Card Research and Advanced Applications. Montpellier, France, 2018: 65-79

[54] Ravi P, Bhasin S, Roy S S, et al. On exploiting message leakage in (few) NIST PQC candidates for practical message recovery and key recovery attacks. IACR Cryptology ePrint Archive, 2020: 1559

[55] Aydin F, Kashyap P, Potluri S, et al. DeePar-SCA: Breaking parallel architectures of lattice cryptography via learning based side-channel attacks//Proceedings of the International Conference on Embedded Computer Systems. Samos, Greece, 2020: 262-280

[56] Kim S, Hong S. Single trace analysis on constant time CDT sampler and its countermeasure. Applied Sciences, 2018, 8(10): 1809

[57] Chung C M M, Hwang V, Kannwischer M J, et al. NTT multiplication for NTT-unfriendly rings: New speed records for saber and NTRU on cortex-M4 and AVX2. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021(2): 159-188

[58] Primas R, Pessl P, Mangard S. Single-trace side-channel attacks on masked lattice-based encryption//Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems. Taipei, China, 2017: 513-533

[59] Pessl P, Primas R. More practical single-trace attacks on the number theoretic transform//Proceedings of the 6th International Conference on Cryptology and Information Security in Latin America. Santiago de Chile, Chile, 2019: 130-149

[60] Sim B Y, Kwon J, Lee J, et al. Single-trace attacks on message encoding in lattice-based KEMs. IEEE Access, 2020, 8: 183175-183191

[61] Bos J, Ducas L, Kiltz E, et al. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM//Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P). London, UK, 2018: 353-367

[62] Alkim E, Ducas L, Pöppelmann T, et al. Post-quantum key exchange—A NewHope//Proceedings of the 25th Security Symposium. Vancouver, Canada, 2016: 327-343

[63] Baan H, Bhattacharya S, Fluhrer S, et al. Round5: Compact and fast post-quantum public-key encryption//Proceedings of the 10th International Conference on Post-Quantum Cryptography. Chongqing, China, 2019: 83-102

[64] De Clercq R, Roy S S, Vercauteren F, et al. Efficient software implementation of ring-LWE encryption//Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE). Grenoble, France, 2015: 339-344

[65] Ravi P, Roy S S, Chattopadhyay A, et al. Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(3): 307-335

[66] Ding J, Cheng C, Qin Y. A simple key reuse attack on LWE and ring LWE encryption schemes as key encapsulation mechanisms (KEMs). IACR Cryptology ePrint Archive, 2019: 271

[67] Qin Y, Cheng C, Ding J. A complete and optimized key mismatch attack on NIST candidate NewHope//Proceedings of the 24th European Symposium on Research in Computer Security. Luxembourg, The Grand Duchy of Luxembourg, 2019: 504-520

[68] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes//Proceedings of the 19th Annual International Cryptology Conference. Santa Barbara, USA, 1999: 537-554

[69] Schwabe P, Stebila D, Wiggers T. Post-quantum TLS without handshake signatures//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. Los Angeles, USA, 2020: 1461-1480

[70] Bernstein D J, Brumley B B, Chen M S, et al. OpenSSLNTRU: Faster post-quantum TLS key exchange//Proceedings of the 31st USENIX Security Symposium (USENIX Security 22). Boston, USA, 2022: 845-862

[71] Checkoway S, Niederhagen R, Everspaugh A, et al. On the practical exploitability of dual EC in TLS implementations//Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14). San Diego, USA, 2014: 319-335

[72] Saarinen M J O. Arithmetic coding and blinding countermeasures for lattice signatures. Journal of Cryptographic Engineering, 2018, 8(1): 71-84

[73] Pessl P. Analyzing the shuffling side-channel countermeasure for lattice-based signatures//Proceedings of the International Conference on Cryptology in India. Kolkata, India, 2016: 153-170

[74] Reparaz O, Roy S S, De Clercq R, et al. Masking ring-LWE. Journal of Cryptographic Engineering, 2016, 6(2): 139-153

[75] Reparaz O, de Clercq R, Roy S S, et al. Additively homomorphic ring-LWE masking//Proceedings of the 7th International Workshop (PQCrypto 2016). Fukuoka, Japan, 2016: 233-244

[76] Oder T, Schneider T, Pöppelmann T, et al. Practical CCA2-secure and masked ring-LWE implementation. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018(1): 142-174

[77] Barthe G, Belaïd S, Espitau T, et al. Masking the GLP lattice-based signature scheme at any order//Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tel Aviv, Israel, 2018: 354-384

[78] Bos J W, Gourjon M, Renes J, et al. Masking Kyber: First- and higher-order implementations. IACR Cryptology ePrint Archive, 2021: 483

[79] Beirendonck M V, D'anvers J P, Karmakar A, et al. A side-channel-resistant implementation of SABER. ACM Journal on Emerging Technologies in Computing Systems (JETC), 2021, 17(2): 1-26

[80] Lee M K, Song J E, Choi D, et al. Countermeasures against power analysis attacks for the NTRU public key cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, 93(1): 153-163

[81] Migliore V, Gérard B, Tibouchi M, et al. Masking dilithium//Proceedings of the International Conference on Applied Cryptography and Network Security. Bogota, Colombia, 2019: 344-362

[82] Kim I J, Lee T, Han J, et al. Novel single-trace ML profiling attacks on NIST 3 round candidate dilithium. IACR Cryptology ePrint Archive, 2020: 1383

[83] Schamberger T, Mischke O, Sepulveda J. Practical evaluation of masking for NTRUEncrypt on ARM cortex-M4//Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design. Darmstadt, Germany, 2019: 253-269

[84] Ngo K, Dubrova E, Guo Q, et al. A side-channel attack on a masked IND-CCA secure saber KEM implementation. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021(4): 676-707

[85] Azouaoui M, Bronchain O, Grosso V, et al. Bitslice masking and improved shuffling: How and when to mix them in software? IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022, 2022(2): 140-165

《计算机学报》

LI Yan-Bin, Ph. D., associate professor. His main research interests include side-channel attack, cryptography and cryptographic chip security.

ZHU Jia-Jie, M. S. candidate. His research interests include side-channel attack and cryptography.

TANG Ming, Ph. D., professor, Ph. D. supervisor. Her main research interests include cryptography, hardware security, side-channel attacks and countermeasures.

ZHANG Huan-Guo, Ph. D., professor, Ph. D. supervisor. His main research interests include information security and cryptography.

Background

The impending realization of scalable quantum computers will have a significant impact on current security infrastructure. In particular, NIST announced the post-quantum cryptographic algorithms in third round of PQC project. Among the various classes of quantum-resistant cryptography schemes, lattice-based cryptography stands out for its advantages of performance and security. While most considerable effort has been focused the design and implementation of lattice-based cryptography, little effort has been devoted to physical security.

By drawing attention to the positive side and negative side of the lattice-based cryptography for physical security, this survey investigates the state-of-the-art techniques proposed in the literature. Our survey aims at examining the research landscape in physical security and strengthening research. It forms the basis for a systematic and comprehensive view on physical security in the lattice-based cryptography area.

Our research team has researched on the field of power, electro-magnetic analysis for 10 years. We completed a prototype system about side-channel analysis, protection and testing. This research is supported by the National Natural Science Foundation of China (62072247, 61972295). It aims at putting forward a set of efficient leakage detection scheme for cryptographic circuits.

《计算机学报》