后量子加密算法的硬件实现综述

曹 元[1], 陆 旭[1], 吴彦泽[1], 谢浩东[1], 乔云凯[1],
姚恩义[2,3], 陈 帅[4], 叶 靖[5]

[1] 物联网工程学院 河海大学 常州 中国 213000
[2] 微电子学院 华南理工大学 广州 中国 511442
[3] 人工智能与数字经济广东省实验室(广州) 广州 中国 511442
[4] 磐石安全实验室 常州 中国 213000
[5] 计算机体系结构国家重点实验室 中国科学院计算技术研究所 北京 中国 100190

摘要 现有的密码体制大多基于 RSA、ECC 等公钥密码体制, 在信息安全系统中实现密钥交换、数字签名和身份认证等, 有其独特的优势, 其安全性分别依赖于解决整数分解问题和离散对数问题的难度。近年来, 随着量子计算机的快速发展, 破解上述数学问题的时间大幅减少, 这将严重损害数字通信的安全性、保密性和完整性。与此同时, 一个新的密码学领域, 即后量子密码学应运而生, 基于它的加密算法可以对抗量子计算机的攻击, 因此成为近年来的热点研究方向。2016 年以来, NIST 向世界各地的研究者征集候选抗量子密码学方案, 并对全部方案进行安全性、成本和性能的评估, 最终通过评估的候选方案将被标准化。本文比较了 NIST 后量子密码学算法征集(第 2 轮、第 3 轮)的各个方案, 概述目前后量子加密算法的主要实现方法: 基于哈希、基于编码、基于格和基于多变量, 分析了各自的安全性, 签名参数及计算量的特点以及后期的优化方向。PQC 算法在硬件实现上的挑战其一是算法规范的数学复杂性, 这些规范通常是由密码学家编写的, 关注的重点是其安全性而非实现的效率, 其二需要存储大型公钥、私钥和内部状态, 这可能会导致不能实现真正的轻量级, 从而降低硬件实现的效率。本文重点介绍了目前后量子加密算法的硬件实现方式, 包括 PQC 硬件应用程序编程接口的开发, 基于 HLS 的抽象实现和基于 FPGA/ASIC 平台的硬件实现。PQC 方案的硬件化过程中不仅需要算法的高效实现, 同时需要抵抗针对硬件结构的侧信道攻击。侧信道攻击可以通过来自目标设备泄露的相关信息来提取密码设备的密钥。本文讨论了后量子加密算法在具体实现和应用中受到侧信道攻击类别和防御对策。

关键词 量子计算; 后量子密码; 加密算法; 硬件实现
中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2021.11.01

The Survey of Post-quantum Cryptography Hardware Implementation

CAO Yuan[1], LU Xu[1], WU Yanze[1], XIE Haodong[1], QIAO Yunkai[1],
YAO Enyi[2,3], CHEN Shuai[4], YE Jing[5]

[1] College of Computer Internet of Things Engineering, Hohai University, Changzhou 213000, China
[2] School of Microelectronics, South China University of Technology, Guangzhou 511442, China
[3] Guangdong Laboratory of Artificial Intelligence and Digital Economy (Guangzhou), Guangzhou 511442, China
[4] Rock-solid Security Lab, Changzhou 213000, China
[5] State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China

Abstract The majority of existing cryptosystems are based on public key cryptosystems such as RSA and ECC. This sort of encryption technology has specific benefits in the information security system when it comes to key exchange, digital signatures and identity authentication. Their security depends on the difficulty of solving integer factorization problem and the discrete logarithm problem. In recent years, with the rapid development of quantum computers, the time to solve the above mathematical problems is expected to be greatly reduced, which will seriously damage the security, confidentiality and comprehensiveness of digital communications. Under such circumstances, a new field of cryptography, namely Post-Quantum Cryptography (PQC) emerged. The encryption algorithm based on it can defend the attacks from quantum computers, so it has become a hot research topic recently. Since 2016, NIST has solicited candidate anti-quantum cryptog-

通讯作者: 曹元, 博士, 教授, Email:caoyuan0908@gmail.com。
本课题得到 2021 年度中央引导地方科技发展资金“车规级 MCU 与专用芯片及控制器研制”、江苏省自然科学基金(No. BK20191160)、计算机架构国家重点实验室开放研究项目(No. CARCH201901)、青蓝工程、常州市应用基础研究计划(No. CJ20200071)、常州市科技成果转化专项基金(No. 2020029)专项资助。
收稿日期: 2021-08-29; 修改日期: 2021-10-08; 定稿日期: 2021-10-20

raphy schemes from researchers all over the world and evaluated the security, cost, and performance of all solutions. The candidate solutions that passed the evaluation will be standardized. This article compares the various proposals of the NIST post-quantum cryptography algorithm solicitation (round 2 and 3), outlines the current main implementation methods of post-quantum encryption algorithms: hash-based, code-based, lattice-based and multivariate-based and analyzes their respective security, signature parameters and the characteristics of the amount of calculation, and the later optimization direction. The challenge of the PQC algorithm in hardware implementation is the mathematical complexity of the algorithm specifications. These specifications are usually written by cryptographers. The focus is on its security rather than the efficiency of implementation. The second is the requirement of storing large public keys, private keys and internal state, which may lead to the inability to achieve real lightweight, thereby reducing the efficiency of hardware implementation. This brief focuses on the current hardware implementation of post-quantum encryption algorithms, including the development of PQC hardware application programming interface, abstract implementation based on HLS and hardware implementation based on FPGA/ASIC platform. The hardware design of PQC scheme necessitates not only an efficient implementation of the algorithm but also the ability to withstand side-channel attacks on the hardware structure. A side-channel attack can obtain the key of a cryptographic device through relevant information leaked from the target device. This article discusses the types of side-channel attacks and countermeasures for post-quantum encryption algorithms in specific implementation and applications.

Key words quantum computer; post-quantum cryptography; encryption algorithm; hardware implementation

1 介绍

密码学是研究与信息安全相关的数学技术科学。它可以保证通信的机密性、数据的完整性、认证实体和数据源[1]。其密码体制可分为对称密码与非对称密码, 非对称密码也称公钥密码。现有的密码体制大多基于 RSA (Rivest-Shamir-Adleman)、ECC (Elliptic Curve Cryptography)等公钥密码体制, 在信息安全系统中实现密钥交换、数字签名和身份认证等, 有其独特的优势, 其安全性分别依赖于解决整数分解问题(Integer Factorization Problem, IFP)和离散对数问题(Discrete Logarithm Problem, DLP)的难度[2]。

然而, 基于量子计算机特殊的计算能力, Shor 等人[3]给出了基于模幂运算的量子求阶算法: 一个用于整数分解和离散对数计算的多项式时间算法, 依赖于合适的能用量子计算机实现的量子傅里叶变换, 由此产生计算机处理能力爆炸性增长, 可成功解决整数分解和离散对数等困难问题, 而这些问题则是几大著名公钥体制 RSA、ECC 等的理论基础, 这意味着量子计算机可以对这几大著名的公钥体制形成致命的攻击, 即与目前的二进制计算机相比, 大大缩短了其密钥的破解时间[4]。另外, Grover 等人[5]提出的量子搜索算法可对非结构化搜索问题进行二次加速, 尽管这种加速不会使加密技术过时, 但即使在对称加密的情况下, 它也会导致人们不得不采用更大的密钥以确保安全性。表 1 总结了量子计算机对密码算法的影响, 量子计算机的出现使 RSA 等公钥密码不再安全。

表 1 量子计算机对密码算法的影响

Table 1 The influence of quantum computer on cryptographic algorithms

密码算法	类型	目的	受大规模量子计算机的影响
AES (Advanced Encryption Standard)	对称密钥	加密	密钥规模增大
SHA-2 (Secure Hash Algorithm 2), SHA-3 (Secure Hash Algorithm 3)	Hash 函数	完整性	输出长度增加
RSA	公钥密码	加密, 签名, 密钥建立	密钥可以被破解
ECDSA (Elliptic Curve Digital Signature Algorithm), ECDH (Elliptic Curve Diffie-Hellman)	公钥密码	签名, 密钥交换	密钥可以被破解
DSA (Digital Signature Algorithm)	公钥密码	签名	密钥可以被破解

这促使研究人员设计能够抵抗量子计算机攻击的密码: 后量子密码(Post Quantum Cryptography, PQC), 又称抗量子密码。所谓“后”, 是指在实用级量子计算机实现后, 现有的绝大多数公钥算法将会被足够大且稳定的量子计算机攻破, 而能够抵抗这种攻击的密码算法可以在量子计算和其之后时代存活下来。这些后量子密码算法有两个共同特点: 1)即使假设全规模量子计算机的可用性, 也没有已知的攻击能够破解这些密码系统; 2)所有的后量子密码算法都可以使用传统的计算平台, 基于标准半导体技术, 如微处理器(Central Processing Unit, CPU)和现场可编程逻辑门阵列(Field Programmable Gate Array,

FPGA)。

为了实现在应用上的安全性、可靠性, 后量子密码学针对量子计算的特点, 结合传统密码学的优势, 设计了能够抵御量子计算机攻击的密码方案[6]。目前, 表现良好的 PQC 方案有基于哈希的、基于编码的、基于格的、基于多变量等。目前的研究尚不明确这些方案中哪一个会成为未来的标准。此外, 尽管大规模量子计算攻击仍在现代工程能力的范围之外, 但开发抵抗量子攻击的替代方案的工作已经在国内外积极的开展[7]。

本文的其余部分组织如下: 第 2 节概述了 NIST PQC 第 2、3 轮算法征集; 第 3 节介绍了 4 种后量子加密算法; 第 4 节提出了 PQC 算法在硬件的实现以及挑战; 第 5 节分析了 PQC 算法中的侧信道攻击, 最后给出了总结。

2 NIST 后量子密码算法征集

2009 年, 国家标准与技术研究所 (National Institute of Standards and Technology, NIST)启动了 PQC 计划来标准化一个或多个抗量子密码方案[8]。NIST 是一个负责开发技术、标准和指导方针的非监管的政府机构, 以帮助联邦机构满足联邦信息安全现代化法案(Federal Information Security Modernization Act, FISMA)[9]的要求。NIST 还负责根据 FISMA 制定联邦信息处理标准(Federal Information Processing Standards, FIPS)。

2015 年 4 月, 美国国家标准与技术研究所(NIST)举办了“后量子世界的网络安全研讨会”, 讨论了后量子密码系统未来可能的标准化, 同年 8 月, 美国国家安全局(NSA)就“在不久的将来过渡到量子稳定算法”的计划发表了一份重要声明。2016 年, NIST 宣布了 NIST PQC 算法征集, 邀请来自世界各地的研究者提交候选抗量子密码学方案进行评估和最终标准化。NIST 打算从中挑出多个算法[10], 将选出的候选算法进行标准化, 并将增强联邦信息处理标准(FIPS) 186-4[11]中指定的密码算法。

在 PQC 算法征集中, 经过筛选的算法将被指定为最终的候选算法。进入最终一轮的方案更有可能被考虑标准化, 而候补方案则是有一些方案被标准化的可能性很小。

提交的算法被正式分为两类, 公钥加密、密钥封装方案, 以及数字签名方案。除了上述分类之外, 候选算法又可以根据它们构造密码方案所依赖的底层数学难题类型不同分为多个类别, 这些类别是: 1)基于哈希的密码学; 2)基于编码的密码学; 3)基于格的密码学; 4)基于多变量的密码学。

2016 年 2 月, NIST 发布了《后量子密码学报告》, 强调信息安全系统需要部署后量子密码学[12]。NIST 于 2017 年开始后量子密码学标准化, 有 69 种公钥加密、密钥封装和数字签名候选算法在 2017 年 12 月 20 日被接受为第一轮候选算法, 标志着 NIST 应对量子计算机发展的后量子密码标准化进程的第一轮行动的开始[13]。

NIST 组织一场大型比赛对后量子密码算法进行选择, 这个类似竞争的过程被称为 NIST PQC 标准化过程[14]。问题是这些算法目前还很新, 我们不知道哪个(些)最终会赢得比赛, 所以还需要付出很多努力来了解这些后量子算法。想使用这些算法并不简单, 用新的算法替换不再安全的 RSA 等公钥密码算法, 在评估过程中需要考虑多方面的因素, 同时进行标准化。

PQC 标准化过程是 NIST 对量子计算机发展进步的回应。这些机器利用量子力学原理来解决传统计算机难以解决的数学问题。如果大规模量子计算机建成, 它们将能够破解目前由 NIST 标准化的公钥密码系统[14]。

在 NIST PQC 标准化过程中评估算法的标准主要涉及 3 个方面: 1)安全性; 2)成本和性能; 3)算法和实现特征。具体如下:

1) 安全性: 与过去的 AES[15]和 SHA-3[16]竞赛一样, 安全性是评估候选后量子算法时最重要的因素。NIST 目前的密码标准已经被广泛使用, 如传输层安全协议(Transport Layer Security, TLS)、安全外壳协议(Secure Shell, SSH)、网络密钥交换协议(Internet Key Exchange, IKE)、互联网安全协议(Internet Protocol Security, IPsec)和域名系统安全扩展协议(Domain Name System Security Extensions, DNSSEC)等互联网协议。需要用新的标准来为这些应用程序提供安全性保证。NIST 认识到在评估后量子候选算法的安全强度时存在重大的不确定性, 因此定义了 5 种安全类别, 以便更好地比较提交算法的安全强度等级。NIST 还提到了其他可取的安全特性, 如完美的前向保密, 抗侧信道和多密钥攻击, 以及抗误用等。

2) 成本和性能: 将成本确定为评估候选算法时的第二重要标准。在这种情况下, 成本包括计算效率和内存需求。这包括:

- 公钥、密文和签名的大小。
- 密钥生成的计算效率, 以及公钥和私钥操作的计算效率。

• 解密失败的概率。

计算效率本质上是指算法的速度。NIST 希望候选算法能够提供与目前标准化的公钥密码算法相当或更好的性能。内存要求是指软件实现的代码大小和随机存取内存(Random Access Memory, RAM)的要求, 以及硬件实现的门数。

所有提交者需提供 NIST 参考平台的性能评估, NIST 参考平台是 Intel x64, 运行 Windows 或 Linux, 并支持 GNU Compiler Collection (GCC) 编译器。NIST 在参考平台上进行了初步的效率分析, 但也邀请公众在其他平台上进行类似的测试。

3) 算法与实现特征: NIST PQC 标准化过程中收到了许多新的、有趣的候选算法, 它们具有当前 NIST 标准化公钥算法所没有的独特特征。具有更大灵活性的候选算法可能优先于其他算法。这包括能够在各种平台上高效运行以及使用并行性或指令集扩展来实现更高性能的算法。此外, 简单优秀的设计能更好地反映了设计团队的理解和信心, 鼓励进一步分析。最后, NIST 将考虑任何可能阻碍和促进算法实现的因素。

2019 年 1 月, 基于对其安全性、性能、密钥长度等特征的评估、分析, 26 种算法进入第 2 轮进一步分析[17]。17 个公钥加密、密钥封装算法, 9 个数字签名算法如表 2 所示。2020 年 7 月, 有 15 个进入第 3 轮, 其中 7 个是候选算法, 8 个是备选算法[18], 如表 2 所示。图 1 显示了第 3 轮候选算法及其在各种算法类别中的位置。在第 3 轮决赛中, 基于格的方案是最常见的。因为格密码的数学原理相似, 因此容易受到类似的攻击, 很可能最多会选择一个基于格的算法来标准化。基于格的方案由于其相对简单的结构和即使在最坏的情况下也可以提供很好的安全性而成为热门的候选方案。

NIST 预计再需要两年左右的时间对最终入选算法进行标准制定, 在 2022—2024 年间公布抗量子密码的标准化草案; 另一方面, 我国对于抗量子密码算法标准化的工作预计将于 2022 年左右展开, 并于 2025 年左右完成商业化。完成抗量子加密标准化进程后, 新的密码体系将替代现有的密码体系以应对量子计算机发展带来的威胁。这种可以抵御量子计算机攻击的密码体系将运用在 SSL, TLS 等现有通信安全协议上, 为保密信息、证明信息、软件升级、信息访问、签名等应用提供安全性、授权控制并保证信息的可鉴别性、完整性和不可否认性。

表 2 NIST PQC 第 2 轮和第 3 轮提交算法

Table 2 NIST PQC round 2 and round 3 submission algorithms

第 2 轮		第 3 轮			
		候选算法		备选算法	
公钥加密、密钥封装	数字签名	公钥加密、密钥封装	数字签名	公钥加密、密钥封装	数字签名
BIKE, Classic-McEliece, CRYSTALS-Kyber, Frodo-KEM, HQC, LAC, LEDAcrypt, NewHope, NTRU, NTRU-Prime, NTS-KEM, ROLL, Round5, RQC, SABER, SIKE, Three Bears	CRYSTALS-Dilithium FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, SPHINCS+	ClassicMcEliece, CRYSTALS-Kyber, NTRU, SABER	CRYSTAL,Dilithium, FALCON, Rainbow	BIKE, FrodoKEM, HQC, NTRU Prime, SIKE	GeMSS, Picnic, SPHINCS+

3 后量子加密算法概述

量子计算机是依靠量子级现象来运行的计算机, 而量子计算机中的比特, 我们称之为量子比特, 它是一个最简单的量子系统, 一个量子比特不仅可以用 0 和 1 来表示, 而且还可以处于 0 和 1 的叠加状态[19], 从计算的方式来看, 比经典计算机更为复杂。这些计算机将能够做很多有趣的事情, 帮助我们解决某些难以用经典计算机解决的问题, 但从安全的角度来看, 它们有一个“副作用”, 我们每次建立 TLS 连接[20]时都会在客户端和服务器之间的网络上使用现有的密码学, 以保护用于签名的数据等, 对于信息安全来说非常重要。但是如果我们建造一个位数足够多的量子计算机, 可以在可接受时间内破解现有的密码体制[21]。因此, 我们需要准备好应对当大型量子计算机可以构建后带来的副作用, 需要更换现有的密码学, 特别是公钥密码学。

公钥密码学在电子商务中用于身份验证(签名)和安全通信(加密)。正如前文所提到的大规模量子计算机的构建将使许多此类公钥密码系统变得不安全,

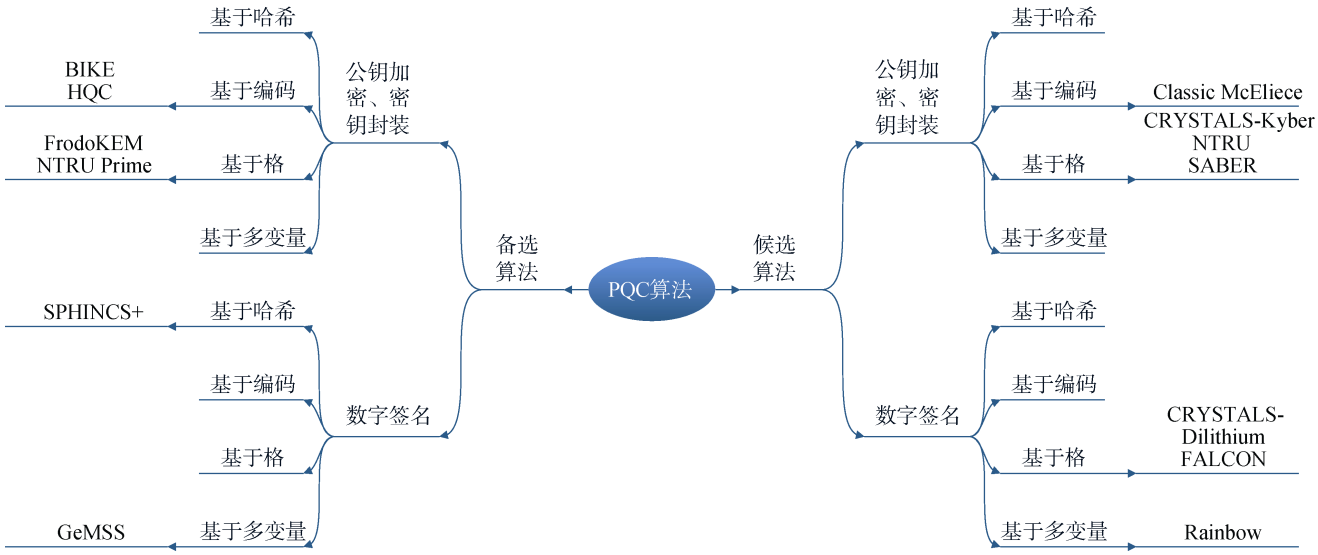

图 1　NIST PQC 比赛第 3 轮决赛算法按类别分组

Figure 1　NIST PQC competition round 3 finals algorithm grouped by category

特别是那些安全性是基于整数分解问题难度或基于离散对数问题难度的公钥密码系统。相比之下，对对称密钥系统的影响不会那么巨大[22]。因此，对于那些被认为能够抵抗来自量子计算机的攻击算法的研究，主要集中在基于非对称加密的公钥密码算法上。我们简要概述目前后量子密码学的主要实现方法[23]。

3.1　基于哈希(Hash)的公钥密码学

图 2 给出了基于哈希的签名方案的分类，表 3 给出了图 2 涉及的缩略语及其解释，基于哈希的签名方案的安全性来源于 Hash 函数的安全性[25]，典型方案为默克尔(Merkle)签名方案，由一次性签名方案 OTS (One Time Signature)[26]演变而来的，并结合了 Merkle 的哈希树认证机制，共同构造出一个完全的二叉树来实现数字签名。哈希树的根是公钥，一次性的认证私钥是树中的叶子节点。

一次签名方案主要优势在于：每对公私钥只能用于一条消息的签名。防止了重放攻击(Replay Attack)，即如果使用了同一个公私密钥对来签署两个

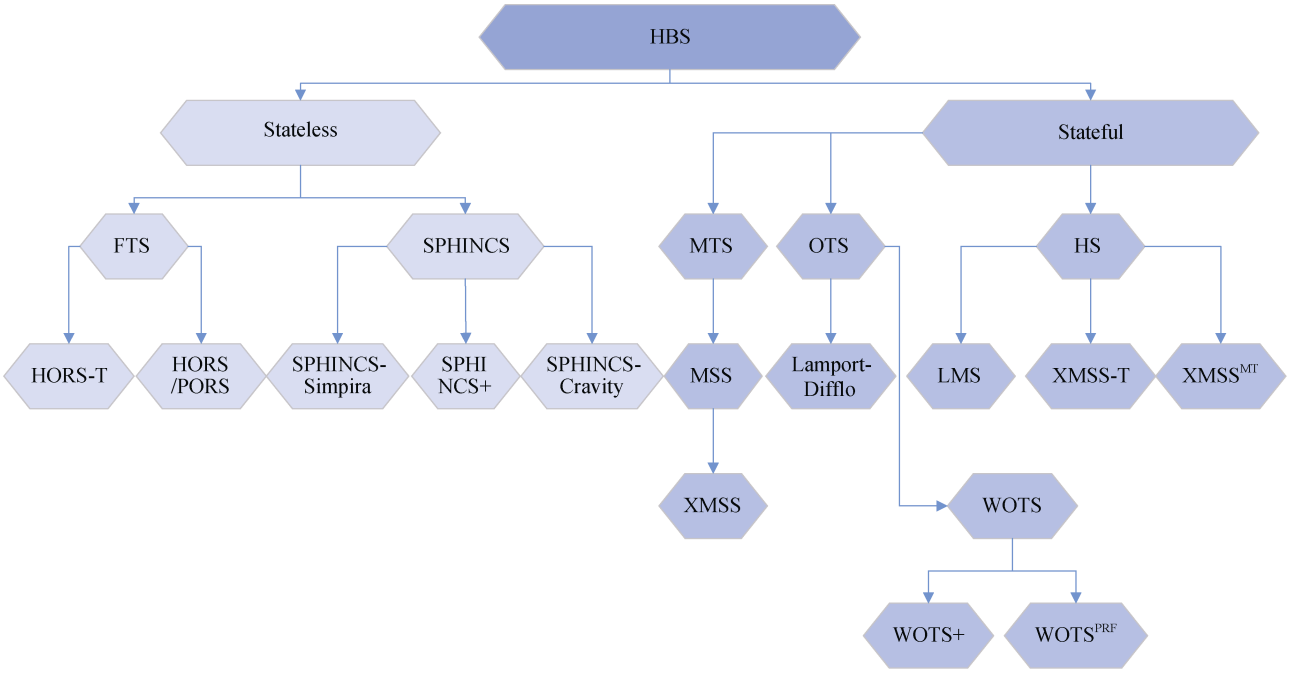

图 2　基于哈希签名方案的分类

Figure 2　Classification of Hash-based signature schemes

表 3　基于哈希签名方案缩略语及其解释

Table 3　Abbreviations and explanations of Hash-based signature schemes

缩略语	全称	解释
HBS	Hash-based Signature	基于哈希签名
FTS	Few-Time Signature	少次签名
MTS	Multi-Time Signature	多次签名
OTS	One-Time Signature	一次签名
HS	Hierarchical Signature	分层签名
HORS-T	HORS (with Tree)	--
MSS	Merkle Signature Scheme	默克尔签名方案
LMS	Leighton Micali Scheme	--
XMSS	Extended MSS	扩展的默克尔签名方案
XMSS-T	XMSS with tightened security	扩展的默克尔签名方案(具有加强版本)
$XMSS^{MT}$	XMSS (Multi Tree)	扩展的默克尔签名方案(多树)
WOTS	Winternitz OTS	温特尼茨一次签名
$WOTS^{PRF}$	WOTS (Pseudo Random Function)	温特尼茨一次签名(伪随机函数)

不同的消息, 那么消息很容易被攻击者伪造。

Merkle 哈希树是一种典型的二叉树结构, 包括一个根节点、一组中间节点和一组叶节点。为了获得唯一一个根节点, 许多的叶节点使用二进制 Merkle 树将其简化[24]。在二叉树的每一层上, 相邻的节点成对碰撞, 形成上一层的一个节点, 以此类推, 最终形成公钥的一个根节点。XMSS 是扩展的 Merkle 签名方案, 图 3 介绍了 XMSS 树的结构。

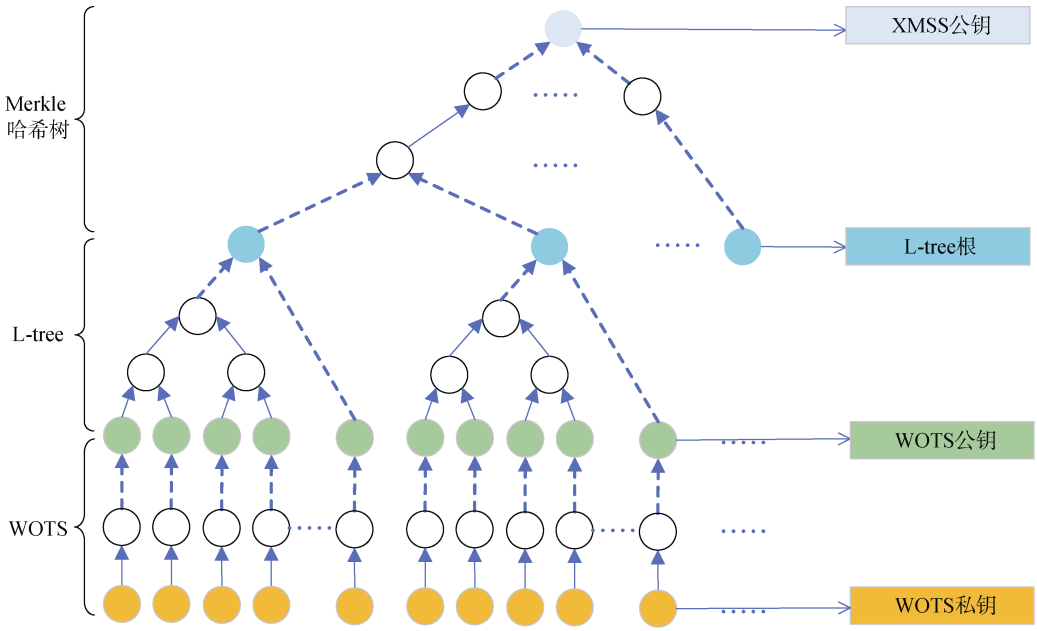

图 3　XMSS 树结构[24]

Figure 3　XMSS tree structure[24]

因为该体制的安全性不依赖于大整数分解和离散对数这两类困难问题, 所以被认为是可以抵抗量子密码分析。其优点是签名和验证效率高, 缺点为签名和密钥较长, 产生密钥的代价较大。目前面临的挑战是有状态性和参数优化。

3.2　基于编码的公钥密码学

基于编码理论构造的公钥体制, 其理论基础是解码问题的困难性, 换句话说就是在已知生成矩阵的情况下, 在码空间寻找一个码字与已知码的 Hamming 距离最短。如果已知码为 0 则问题就是最小权重问题。它的任意线性码的译码问题是 NP 完全问题[27]。

表 4 给出了基于编码的家族以及何时被提出和破坏的, 从本质上来说, 基于编码的密码系统有两

种类型。第一个系统是 McEliece 密码系统, 第二个系统是 Niederreiter 密码系统。McEliece 密码系统是 Robert J. McEliece 在 1978 年提出的, 利用二进制 Goppa 代码开发的基于编码的公钥密码系统[28]。Goppa 码成为 McEliece 密码系统的主要选择有以下两个原因。其一, Goppa 码采用了快速多项式时间解码算法。其二, Goppa 码“易于生成但很难找到”: 有限域 $F(2^m)$ 上的任何不可约多项式都可以用来创建 Goppa 码, 但是 Goppa 码的生成矩阵几乎是随机的。

表 4 基于编码的家族

Table 4 Code-based family

家族	被提出	被破坏
Goppa	McEliece (1978)	
Reed-Solomon	Niederreiter (1986)	Sidelnikov, Chestakov (1992)
Concatenated	Niederreiter (1986)	Sendrier (1998)
Reed-Muller	Sidelnikov (1994)	Minder, Shokrollahi (2007)
AG codes	Janwa, Moreno (1996)	Faure, Minder (2008) Couvreur, Pellikaan (2014)
LDPC	Monico, Rosenthal, Shokrollahi (2000)	
Convolutional codes	Johansson (2012)	Landais, Tillich (2013)

下面简单描述 McEliece 密码系统的加密解密过程[29], 假设通信双方分别为 Alice 和 Bob。

第一步: 密钥对生成

(1) Alice 选择一个能够纠正 t 个错误的二进制[n, k] Goppa 码的生成器矩阵 $\boldsymbol{G}$, 其大小为 $k\times n$。

(2) 再选择一个 $k\times k$ 矩阵 $\boldsymbol{S}$(可逆矩阵), 还有一个 $n\times n$ 矩阵 $\boldsymbol{P}$(可置换阵, 这意味着 $\boldsymbol{P}$ 的每行每列都只有一个 1)。

(3) 定义 $G_1=\boldsymbol{S}\times\boldsymbol{G}\times\boldsymbol{P}$。

(4) 她公开了她的公钥 G_1。

(5) 她保留了自己的私钥 ($\boldsymbol{S}$, $\boldsymbol{G}$, $\boldsymbol{P}$)。

第二步: 假设 Bob 必须向 Alice 发送加密消息

(1) Bob 有一个长度为 k 的明文 m。

(2) 他加载 Alice 的公钥 G_1。

(3) 他生成一个 Hamming 权重为 t 的 n 位向量 $\boldsymbol{e}$。

(4) Bob 计算密文 $c=mG_1+\boldsymbol{e}$ 并发送给 Alice。

第三步: 假设 Alice 收到了密文 c, 她将收到的密文解密

(1) Alice 使用她的私钥计算 P^{-1}。

(2) 计算

$$\begin{aligned} cP^{-1}&=(mG_1+\boldsymbol{e})P^{-1}\\ &=mSGPP^{-1}+\boldsymbol{e}P^{-1}\\ &=mSG+\boldsymbol{e}P^{-1}\end{aligned}$$

(3) 最后, Alice 使用 Goppa 码的解码算法(Patterson 算法)来确定 m 值。

尽管该算法运行速度非常快, 但是大多数基于编码的方案密钥量大, 签名效率低[30]。因此, 如何降低密钥量, 提高效率成为该算法研究领域的热点问题。

3.3 基于格的公钥密码学

格公钥密码体制是在大维数的格上, 基于最短向量问题 SVP (Shortest Vector Problem)和最近向量问题 CVP (Closest Vector Problem)等数学难题而构造的公钥密码体制。SVP 问题是指在大维数格中寻找长度最短的非零向量, 而 CVP 是指在大维数格中寻找和固定向量距离最近的向量, 这两个问题都是 NP 难问题[31]。

目前基于格的公钥实现分为三类[32]: 一类是对 NTRU 以及其改进算法的实现研究; 二是对基于 LWE (Learning With Errors) 问题或者其变形问题的格公钥密码体制方案的实现研究, LWE 问题的高效和简洁性使得基于 LWE 问题的格公钥密码体制实现效率较高; 第三类是对基于格上特殊性质算法的实现研究。

基于格的算法的安全性依赖于求解格中问题的困难性[33]。在达到相同(甚至更高)的安全强度时, 基于格的算法的公私钥尺寸更小, 计算速度更快, 且能被用于构造多种密码学原语, 因此更适用于真实世界中的应用。缺点是参数往往较大。目前该领域的挑战为参数优化和提升效率。近年来, 基于 LWE 问题和 RLWE (Ring-LWE) 问题的格密码学构造发展迅速, 被认为是最有希望被标准化的后量子加密技术路线之一。

3.4 基于多变量的公钥密码学

基于多变量的算法使用有限域上具有多个变量的二次多项式组构造加密、签名、密钥交换等算法。它的安全性来源于求解有限域上随机生成的多变量非线性多项式方程组。该问题被证明为非确定性多

项式时间困难。目前没有已知的经典和量子算法可以快速求解有限域上的多变量方程组[34]。

多变量密码系统的研究, 最早是在 1988 年 Matsumoto 和 Imai 提出了著名的 MI 密码体制, 这是多变量公钥密码史上的一个里程碑, MI 密码体制的提出开启了多变量公钥密码研究和发展的大门。Patarin 在 1995 年提出的线性化方程攻破了 MI 密码体制并在 1996 年提出了隐藏域方程(Hidden Field Equation, HFE)方案。 Kipnis 和 Shamir 分析证明了 HFE 方案的不安全性。Patarin 又在 1997 年利用线性化方程攻击的思想, 设计了 OV (Oil-Vinegar) 签名算法, Kipnis 和 Shamir 进一步改进该方案提出了 UOV (Unbalance Oil Vinegar)方案。

基于多变量的方案效率较高, 但缺点是公钥量大, 并且安全性不稳定。目前该方案的挑战为可证明的密码安全体制以及降低密钥量。

表 5 总结了后量子密码学的研究方向对比。以上这些算法, 当参数选择恰当, 目前没有已知的经典和量子算法可以快速求解这些问题。事实上, 这些算法的安全性都依赖于有没有可以快速求解其底层数学问题或直接对算法本身的高效攻击算法, 这也正是量子计算机对于现有公钥密码算法存在很大威胁的原因。

表 5 后量子密码学的研究方向对比

Table 5 Comparison of research directions of post-quantum cryptography

	基于 Hash 的公钥密码学	基于编码的公钥密码学	基于格的公钥密码学	基于多变量的公钥密码学
安全性	Hash 函数的安全性	任意线性码的译码问题是 NP-完全问题	格中困难问题如最短向量问题(SVP)、最近向量问题(CVP)、带错误学习问题(LWE)和小整数解问题 (SIS)	求解有限域上随机生成的多变量非线性多项式方程组是 NP-困难的
优点	签名和验证签名效率较高	加解密效率高(McEliece), 签名长度短 (Courtois-Finiasz-Sendrier , CFS)	强安全性(允许最坏情形困难性规约到一般情形困难性)	效率较高
缺点	签名和密钥较长, 产生密钥的代价较大	密钥量大, 签名效率较低 (CFS)	参数较大	公钥量大, 安全性不确定
挑战[6]	有状态性和参数优化	降低密钥量, 提高效率	参数优化, 效率提升	可证明安全的密码体制, 降低密钥量

4 PQC 算法在硬件上实现及挑战

PQC 算法在硬件实现上的挑战一是算法规范的数学复杂性, 这些规范通常是由密码学家编写的, 关注的重点是其安全性而非实现的效率。理解这些规范需要具备以下能力: 扎实的数论、抽象代数、编码理论和相关学科的背景知识, 而工程方面的硬件工作者往往对这些充斥着复杂公式和高级数学运算的规范无法理解[35]。在标准化的进程中剩下的候选对象属于 5 个不同的类, 每个类又可以分为各个子类。例如基于格的候选方案分为结构化格(随机格)和非结构化格(理想格)。每个类甚至子类都需要不同的数学背景, 涉及不同的基本操作数。

二是在硬件实现上需要存储大型公钥、私钥和内部状态, 这可能会导致不能实现真正的轻量级, 而且会影响硬件实现的效率[36]。例如, 作为早期 PQC 标准采用的主要候选算法之一 Classic McEliece, 其三个主要参数集的公钥大小分别超过 1/4 MB、1/2 MB 和 1 MB, 其安全级别相当于各种 AES 变体。对于传统公钥密码而言, RSA 的公钥大小为 256~512 B(2048~4096 位), ECC 的公钥大小为 32~64 B (256~512 位)。NIST 第 2 轮 PQC 候选算法属于基于非结构化格的子类有第二大的密钥大小集, 在 4096~8192 B 的范围内。

大型公钥可能会不利于物联网低面积低功耗的实现, 还会增加加密的总时间。而解密的失败, 会造成更多的时间消耗, 从而增加最坏和平均的解密时间。另一方面, 随机数被用于加密、签名生成和密钥封装。使用随机采样器可能需要访问真随机数生成器, 以及不同分布的随机值之间的转换。这类电路很少应用于其他数字系统, 可能需要从头开始开发。这些电路也很难验证, 并且可能是相当大的侧通道泄漏的来源[37]。

解决上述问题首先是对 PQC 硬件应用程序编程接口(Application Programming Interface, API)[38]的开发。这个新的硬件 API 旨在满足后量子密码系统的各种需求, 包括: 最低遵从标准、接口、通信协议和 PQC 核支持的时间特性。PQC 核接口的总体思路如

图 4 所示。该接口由六大数据总线组成: 公共数据输入(Public Data Inputs, PDI), 私密数据输入(Secret Data Inputs, SDI), 随机数据输入(Random Data Inputs, RDI), 公共数据输出(Public Data Outputs, PDO), 私密数据输出(Secret Data Outputs , SDO)和外部内存输入/输出(External Memory Inputs/Outputs, MEM), 表 6 显示了公钥加密、数字签名和密钥封装机制所需的数据总线。

这 6 根总线中的前 5 根伴随着相应的握手控制信号, 命名为 valid 和 ready。valid 信号表明数据已在源端就绪, 而 ready 信号表明目的地已准备好接收它们。

外部存储器输入/输出有一组不同的伴随端口。内存控制信号支持多种内存配置。mem_addr 信号用于指定内存地址, mem_do 和 mem_di 信号分别用于从内存发送和接收数据。可以通过使用多个 mem_wr 信号写入多个内存块。当一个状态码在 PDO 端口是可用的, status_ready 信号是高电平。

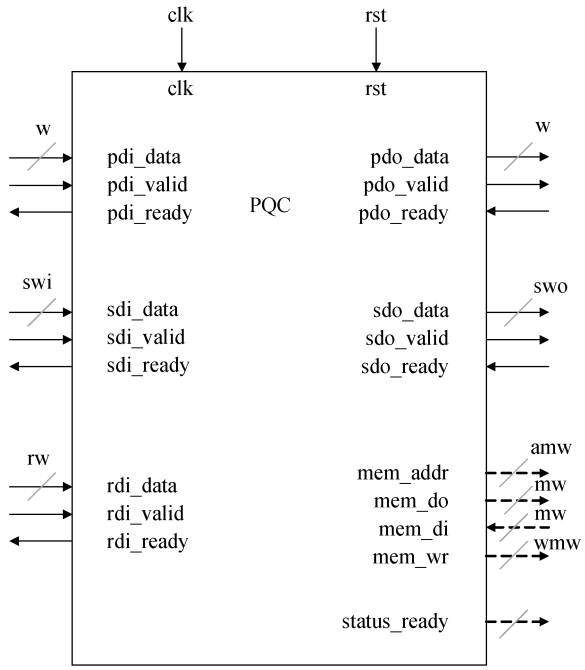

图 4 PQC 接口

Figure 4 PQC interface

表 6 PQC 核数据总线

Table 6 Data bus for PQC cores

	公钥加密	数字签名	密钥封装
需要	PDI, SDI, PDO	PDI, SDI, PDO	PDI, SDI, PDO, SDO, RDI
可选	RDI, MEM	RDI, MEM	MEM
不需要	SDO	SDO	

有两种方法可以用来减少开发时间。第一种是软硬件协同设计, 二是使用高级综合(High Level Synthesis, HLS)[39]。PQC 加密算法的硬件实现既可以通过传统 RTL 实现, 也可以通过基于 HLS 来实现[40]。HLS 之所以被更多地使用, 一是因为验证被加速。通常可以使用软件验证工具来验证设计的行为, 该软件验证工具比 RTL 仿真工具更容易使用。此外, HLS 工具的 RTL 输出可以使用原始的行为测试台进行验证, 因为该工具可以检查两个模型的结果是否相同。二是因为设计空间探索(Design Space Explorer, DSE)更快[40]。可以通过在 HLS 工具中进行选择来探索微体系结构, 这些选择几乎不需要修改代码。因此, 可以在数小时内探索几种转换, 例如流水线化和各种循环展开因子[41]。这是对 RTL 方法论的巨大改进, 在原 RTL 方法论上, 此类更改将需要对源代码进行重大修改。

为了提高设计数字硬件组件的效率, HLS 被视为提高设计抽象水平的下一步方向。接下来简单描述基于 HLS 的 PQC 算法设计流程, 如图 5。C 代码设计是 HLS 设计流程的输入, 接下来, 我们对 C 代码执行 HLS, 使用 Xilinx Vivado HLS 生成 RTL。之后进行预期值与输出的对比来决定是否需要优化, 如果需要优化, 则不断调整指令再次进行 HLS, 如果不需要优化, 则输出最终的 RTL。

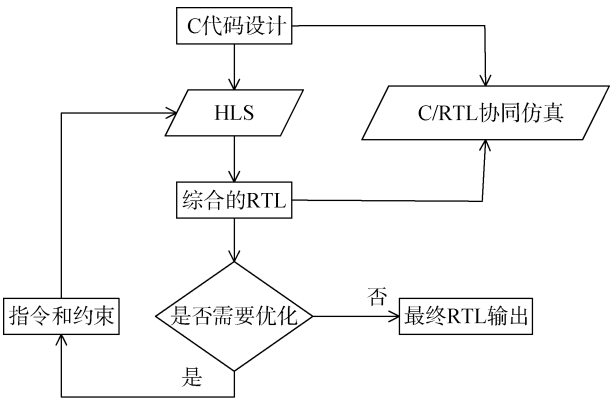

图 5 基于 HLS 的 PQC 算法设计过程

Figure 5 HLS-based design exploration of PQC algorithms

将 HLS 应用于后量子密码加速器设计是在文献[40,42]中首次提出的, Basu 等人研究的目的是提

供一个基于硬件的 NIST PQC 加密算法(其中 7 种是密钥封装算法, 6 种是数字签名算法)的比较, 这些算法在 Xilinx Virtex-7 FPGA 上实现, 使用高级 C 规范映射到 FPGA 和 ASIC 设计流程来找到功率、面积、速度和安全性(PASS)的最优点, 还开发了两种 PQC 算法: qTESLA 和 Crystals Dilithium 的 ASIC 设计。这是第一个硬件基准测试, 并使用一个通用的评估框架来研究区域、性能和安全之间的权衡。[43]主要研究 PQC 算法的优化来提高性能, 利用 HLS 为 PQC 算法提供了面积优化和速度优化的解决方案。这些解决方案创建了高效和恒定时间的 PQC 设计保证了硬件的安全性, 防止了定时侧通道攻击。优化后的 PQC 算法提供了一种高效、安全的硬件实现。实验结果表明, 与传统 RTL 实现相比, 使用 HLS 生成 Kyber512 的面积和延迟分别减少了 2 倍和 3 倍。[44]对基于 HLS 对数论变换(Number Theoretic Transform, NTT)的设计方法进行了深入研究。NTT 是基于格的后量子密码系统的核心数学函数。NTT 常被环型和模块型 LWE PQC 算法使用, 例如: Kyber 和 NewHope。通过使用 Vivado HLS 工具展示了对 NTT 的快速而广泛的设计空间探索, 分析了优化配置的缺点和挑战, 与传统 RTL 的硬件设计相比, HLS 提供了更低的设计成本。

对于任何资源受限的应用程序来说, 对 PQC 加密算法的高效实现是迫切需要的[45]。但是关于 PQC 标准候选硬件实现的出版物数量仍然相对较少, 由于假设和优化目标的不同, 报告的结果很难进行比较。因此, 对于在硬件平台上实现这些方案的最佳方法仍未有结论, 但目标是优化各个方面, 如最小面积、最大速度等。Nejatollahi 等人在文献[46]中提出了基于格的加密算法实现的趋势、挑战和需求, 在此基础上进一步研究, 描述了基于格的密码在软件和硬件实现方面的挑战, 以及它们在身份验证、密钥交换和数字签名方面的应用, 使用软件、硬件、软件/硬件协同设计和数字信号处理(Digital Signal Processing, DSP)技术实现了基于格的密码方案[47]。Wang 等人[48]提出了在 Stratix V FPGA 上实现经典 McEliece, 介绍了基于二进制 Goppa 码的 Niederreiter 密码系统 FPGA 实现, 包括加密、解密和密钥生成模块。Karmakar 等人[49]研究了 SABER 在 ARM Cortex-M 系列资源受限微控制器上的实现, 并将速度优化和内存优化的 SABER 实现与其他已报道的基于格的方案在 ARM Cortex-M 微控制器上的实现进行比较。Hülsing 等人[50]在 ARM CORTEX-M3 处理器实现了无状态的哈希签名方案 SPHINCS, 证明了在嵌入式微处理器上实现无状态的哈希签名方案是可行的。在[51]中, 现有的加密协处理器被重新用于 Kyber KEM, 并与其他 PKE 或 KEM 方案在不同微控制器平台上的时钟周期比较。Ferozpuri 等人[52]介绍了 Rainbow 的高速 FPGA 实现。该设计支持许多参数集, 这些参数集需要在 GF(16)和 GF(256)字段中进行操作。为了使基准测试更容易和更公平, 该设计遵循通用的 PQC 硬件 API, 允许与其他后量子签名方案进行比较。这个设计是开源的, 来增加透明度和加速进一步的优化。Huang 等人[53]在 XilinxFPGA 上实现 CRYSTALS-Kyber 算法的纯硬件实现, NTT 模块采用了高效的并行和流水线计算。通过仿真和综合结果的分析, 发现该方法具有频率高、执行时间短的优点。该方案在 Xilinx Artix-7 和 Virtex-7 FPGA 上分别工作在 155 MHz 和 192 MHz 频率。与嵌入式 Cortex-M4 处理器相比, 硬件实现加密、解密的最大加速可达 129 倍。Tian 等人[54]提出了一种基于超低延迟乘法器、加法器和减法器的 SIKE 算法的快速 FPGA 实现。使用 Verilog 语言编写代码, 并将其集成到 SIKE 库中。在 Xilinx Virtex-7 FPGA 上的实现结果表明, 对于 SIKEp751, 该设计成本仅为 9.3 ms, 频率为 155.8 MHz, 比最先进的速度快 2 倍, 并实现了现有工作中最好的面积优化。特别是, 模块化乘法器只需要 16 个时钟周期, 将延迟减少了近一个数量级。

大多数 PQC 算法还处在审查阶段, 大家的工作重点都在算法层面的优化以及安全性(如抗测信道攻击)的评估, 在这基础上硬件实现相对较少。目前只有少量 PQC 方案(LMS、XMSS)已经被 NIST 标准化并开源了相关代码, 所以硬件实现与优化也更多集中在这一方向。在对 XMSS 研究的初始阶段, XMSS 计算的加速主要是通过指令集架构的软件优化来实现的[55-57]。通常, 它们的性能往往取决于 CPU 的性能。设计[24,45,58]通过构造专用硬件加速器的方式加速 XMSS 计算。在 2018 年, Wang 等人[24]提出了软硬协同的工作架构, 用于在 RISC-V 嵌入式处理器上高效实现 XMSS, 其中最密集的 SHA-256 操作被放到几个硬件优化特定 XMSS 的 SHA-256 加速器上来加速计算。Prashanthet 等人[58]将流水线思想应用到 SHA256 硬件加速器中, 使得 SHA256 具有更快的工作频率。他们在文中列出了 SHA256 以及 pipe-SH256 在 FPGA 和 ASIC 下各自的功耗、速度以及面积等性能, 为硬件进一步实现与优化提供了参考。这些设计极大的加速了 XMSS 计算速度, 并将其应用范围扩大到了资源受限的嵌入式设备, 然而还是无法满足

在个别应用领域的需求, 如汽车芯片通信中的验签速度。文献[59]是对 XMSS 的全硬件实现, 包括了密钥生成、签名生成和签名验证三个部分。该设计完全还原了 XMSS 计算过程, 在 28 nm 的 Xilinx XC7A200T-2FBG676I FPGA 芯片上进行了综合、验证和物理实现, 并在 Xilinx Artix-7 系列评估板上进行测试。FPGA 平台上的评估结果表明, 作者的实现将密钥生成和签名生成的速度分别提高了 20%和50%左右, 而且也优于文献[45]中 FPGA 中签名验证最快的硬件实现。与 XMSS 相比, 在相同的安全级别下, LMS 需要进行更多的计算。密钥生成是 LMS 中最耗时的过程, 大约是平均时间的一半[60]。因此, 加速密钥生成过程可以有效地提高全部实现过程的速度。Song 等人[61]提出了一种高效的密钥生成硬件加速器。该体系结构经过精心设计, 具有可扩展性, 可以支持所有的参数集。设计并行性来获得低延迟。作者使用 Verilog 语言编写代码, 并在 Xilinx Zynq UltraScale+ FPGA 上实现。实验结果表明, 与在 Intel(R) Core(TM) i7-6850K 3.60GHz CPU 上启用线程的优化软件实现相比, 该设计在不同参数配置下实现了 55~2091 倍的加速。

5 PQC 算法中的侧信道攻击分析

后量子密码通过数学理论保证了其算法的安全性, 但是由于其在具体实现和应用中易受到侧信道攻击而对安全性和性能有着不可忽视的影响, 因此需要对侧信道攻击进行分析, 从而进行防御。侧信道攻击可以通过来自目标设备泄露的这些信息(在执行密码算法时所用的时间、消耗的能量或者发射的电磁波等)来提取密码设备的密钥。这些可能源于设备的时间或功率轨迹, 或者是设备产生的错误输出。典型的侧信道攻击方法包括冷启动攻击、故障攻击、定时攻击和功率分析等[62]。

冷启动攻击(Cold Boot Attack, CBA)[63]是一种新型的旁路攻击(Side Channel Attack)。PQC 方案也被证明容易受到冷启动攻击。在这种攻击中, 攻击者针对动态随机存储器(Dynamic Random Access Memory, DRAM)可以使用液氮或压缩空气冷冻来减缓其信息衰减的速度。利用冷启动攻击, 攻击者可以对其进行物理访问正在运行的计算机执行冷启动操作以绕过其软硬件防护机制, 获取正在运行的计算机的内存快照, 并进一步从快照中提取出密钥等敏感信息。文献[64]演示了一种针对 NTT 的冷启动攻击, 文中提出两种编码方式, 第一种是将多项式系数直接存储在内存中, 该方式分析证实在非常低的位翻转率下容易受到冷启动攻击。第二种编码是在存储密钥之前执行 NTT, 对 Kyber 参数的冷启动攻击的需要操作 2^{43} 次, 提高了实现的效率。

时间攻击(Timing Attack, TA)[65]: 是通过分析在不同的输入上处理密码算法所需的时间不同, 并使用这些数据恢复密钥的信息来完成的, 时间攻击是另一种提取密钥信息的常见方法。针对这种攻击的主要对策是在恒定时间内实现算法。然而, 这可能会给算法带来很大的开销。时间攻击已经被发现对许多 PQC 算法有效, 包括 FrodoKEM, HQC 和 FALCON。

能量分析攻击(Power Analysis Attack, PA)[66]: 密码设备的功耗可以提供有关发生的操作和相关参数的大量信息, 通过这些功耗信息可以获取与功耗相关的操作和数据信息。简单能量分析攻击(Simple Power Analysis Attack, SPA)[67]是侧信道能量分析攻击中最简单的一种攻击。在大多数情况下, 这类攻击需要直接分析观察到的能量痕迹[68]。简单一点说, 就是把能量轨迹显示出来之后用眼睛“看”, 当然, 也有很多辅助看的方法, 比如模板碰撞[69]。简单能量分析攻击的优点是需要的能量轨迹少, 缺点是需要泄露比较明显, 对噪音的敏感性大。差分能量攻击(Differential Power Analysis Attack, DPA)[70]: 它需应用额外的分析技术, 如统计相关或设备处理和模板[71]。分析是在几个甚至数以千计的轨迹上执行的, 同时深入了解算法的内部工作原理。能量分析攻击比其他类型的侧信道攻击更广泛、更多样。差分能量攻击的优点是即使泄露较小, 也可以有效识别, 有天然的对噪音的过滤, 缺点是需要的能量轨迹很多。DPA 的基本想法就是, 通过大量的能量轨迹计算能量轨迹和数据的依赖性。能量分析攻击比其他类型的侧信道攻击更广泛、更多样。

另一种用于从加密设备中提取机密信息的常见攻击方法是故障攻击(也称故障注入攻击)(Fault Attack, FA)[72]。这种攻击的操作方式是让攻击者在加密设备中诱发错误, 导致意外的操作泄露可能导致密钥恢复的密钥信息。

近年来, 一些后量子密码算法的侧信道攻击与防御的研究学者进行了相关的调研工作。在 2016 年, Bindel 和 Buchmann 等人[73]分析了基于格的签名方案 BLISS、ring-TESLA 和 GLP 方案以及它们在故障攻击方面的实现, 考虑了多种不同类型(随机化、归零和跳过)的一阶故障攻击, 而为了提高签名方案的安全性, 针对发现的六种攻击又提出了相应的防御对策。在 2017 年, 文献[74]调查了在 FHEW 和 HElib

两个基于格的密码库中的定时攻击和故障攻击并针对定时攻击提出了一种利用填充来实现消息恒定时间加密的方法的防御对策。在 2018 年, Khalid 和 Rafferty 等人[75]调查了基于格的加密技术中一个关键组件——错误采样器, 针对侧信道攻击的漏洞和相关对策, 给出了错误采样器建议以实现基于格的加密技术的实用性、安全性和未来的广泛部署。在 2018 年, 文献[76]调查了基于格的侧信道攻击(SCA)方面的研究情况, 包括入侵攻击和被动攻击并提出了防御的方案, 但是这些方案在多个实施平台上的成本、实用性和有效性仍未得到充分研究。同年, 文献[77]系统地探讨了 R-LWE 加密对故障攻击的抵御能力, 讨论这些攻击的实用性并且根据攻击点和手段的分析, 提出了加强 R-LWE 的防御对策。在 2020 年, Ravi 等人[78]针对基于格的多种密码算法进行了选择密文攻击, 其主要攻击目标是纠错码, 在 ARM Cortex-M4 微控制器上运行的开源 PQM4 库中的进行了实验验证。该攻击可以在几分钟内完成所有目标方案的密钥恢复, 从而显示攻击的有效性。在 2020 年, Danner 等人[79]描述了使用二进制不可约 Goppa 码和 Niederreiter 公钥密码系统解密算法的故障攻击, 随后又提出了两种防御对策, 一是通过检查解码后输出值的权重来发现故障注入, 二是给出检测故障攻击的另一种方法——重新加密输出。针对 NIST 一再强调 SCA 的重要性及对策, 表 7 给出了 NIST PQC 候选人的攻击总结。一直以来, 能够以最小代价抵抗侧信道攻击的方案受到欢迎, 最新的 PQC 总结文件(NISTIR 8309)中指出: “NIST 希望在第三轮测试中看到更多更好的数据, 有更多的对时间攻击、能量分析攻击、故障攻击等侧信道攻击的防御对策。”

表 7 对 NIST PQC 候选人的攻击总结

Table 7 A summary of the attacks on NIST PQC candidates

PQC 方案	故障攻击	简单能量分析攻击	差分能量分析攻击	时间攻击
Classic McEliece	√			
Kyber	√	√		√
NTRU		√		
SABER				
Dilithium	√			
FALCON	√			
Rainbow			√	
BIKE	√			
FrodoKEM		√	√	√
HQC			√	
NTRU Prime			√	√
SIKE				
GeMSS			√	
Picnic			√	
SPHINCS$^+$	√			

针对不同的攻击以及不同应用应当考虑不同的防御对策。对于高速硬件和硬件/软件实现(用于高端服务器的加速器), 防止定时攻击可能就足够了, 因为潜在的攻击者不会对加速器进行物理访问。对于轻量级实现, 目标是受约束的环境和移动设备, 攻击者被假定在设备的常规操作期间易于物理访问设备。因此, 对电磁攻击的额外保护是可以预期的。而任何嵌入式软件实现, 特别是针对多个用户共享公共资源的平台, 可能需要防止缓存泄漏。

针对侧通道攻击的大多数防御对策都是特定于算法的, 但大多数 PQC 加密算法都尚未得到研究。它们的开发和实验验证可能需要相当长的时间, 包括大量修改和扩展实验框架。即使是保护高速和轻量级实现免受强大的定时攻击所必需的恒定时间实现, 对于许多 PQC 算法的开发也是非常重要的。

同样重要的是防止故障攻击, 在这种攻击中, 攻击者在硬件实现的特定单元或特定计算阶段引发故障。攻击者对故障的确切性质、位置(时间和空间)和结果的控制越强, 就越难防范这些攻击。

6 总结

虽然我们仍然不知道何时甚至是否能够建造大型而可靠的量子计算机, 但我们知道建造实用的量子计算机理论上是可行的, 而且量子计算机的发展

已经从理论发展到了小规模实验实践。因此, 我们必须正视量子计算机对信息安全的威胁, 提前做好向后量子密码的过渡, 为量子计算机成为现实做好准备。

后量子密码学研究的目标是提供能够安全抵御量子计算机攻击的密码方案。它所研究的是一类量子计算机在多项式时间内无法攻破的密码算法。目前有几个后量子算法已被很好地理解, 并被认为是标准化和实际应用的有力候选方案。

为了广泛部署量子安全方案, 重要的任务是:

标准化: NIST 标准化机构已经开始对后量子密码学进行标准化。标准化过程需要对后量子方案的强度、效率、安全性和实际适用性进行反馈[17]。

实现: 行业需要高效和安全的(标准化)后量子方案的软件实现, 该方案提供与当前软件兼容的接口, 并与当前硬件兼容。此外, 需要开发新的硬件设备, 例如智能卡、安全令牌、硬件安全模块(Hardware Security Module, HSM)和密码协处理器来实现后量子加密。

测试: 测试后量子安全方案的软件和硬件实现: 理论上安全的密码方案可能会因为错误的实现而被破坏。需要检查实现并保护其免受侧通道攻击。

教育: 工业界、政界和公众需要了解量子计算机的精确计算能力, 以及后量子密码学的存在和需求。除了密码分析, 量子计算机在物理、生物、化学等领域有许多积极的实际应用, 但还有许多关于量子计算机的谜题需要解开。

参考文献

[1] Alese B K, Philemon E D, Falaki S O. Comparative analysis of Public-Key Encryption Schemes[J]. *International Journal of Engineering and Technology*, 2012, 2(9): 1552-1568.

[2] Shor P W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring[C]. *The 35th Annual Symposium on Foundations of Computer Science*, 1994: 124-134.

[3] Shor P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. *SIAM Review*, 1999, 41(2): 303-332.

[4] Mavroeidis V, Vishi K, Zych M D, et al. The Impact of Quantum Computing on Present Cryptography[EB/OL]. 2018: arXiv: 1804.00200[cs.CR]. https://arxiv.org/abs/1804.00200

[5] Gabriel A J, Alese B K, Adetunmbi A O, et al. Post-Quantum Crystography: A Combination of Post-Quantum Cryptography and Steganography[C]. *8th International Conference for Internet Technology and Secured Transactions*, 2013: 449-452.

[6] Bernstein D J, Lange T. Post-Quantum Cryptography[J]. *Nature*, 2017, 549(7671): 188-194.

[7] Howe J, Prest T, Apon D. SoK: How (not) to Design and Implement Post-Quantum Cryptography[J]. *IACR Cryptol. ePrint Arch.*, 2021, 2021: 462.

[8] Chen L, Jordan S, Liu Y K, et al. Report on Post-Quantum Cryptography[R]. National Institute of Standards and Technology, 2016.

[9] Congress U S. Federal information security modernization act of 2014[J]. *Public Law*, 2014: 113-283.

[10] D. Moody. Let's get ready to rumble. the Nist PQC "Competition"[C]. *First PQC Standardization Conference*, 2018, 11-13.

[11] Kerry C F, Director C R. Federal Information Processing Standards Publication: Digital Signature Standard (DSS)[R]. National Institute of Standards and Technology, 1994.

[12] Bobrysheva J, Zapechnikov S. Post-Quantum Security of Communication and Messaging Protocols: Achievements, Challenges and New Perspectives[C]. *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, 2019: 1803-1806.

[13] Kuznetsov A A, Gorbenko Y I, Prokopovych-Tkachenko D I, et al. Nist PQC: Code-Based Cryptosystems[J]. *Telecommunications and Radio Engineering*, 2019, 78(5): 429-441.

[14] Alagic G, Alperin-Sheriff J, Apon D, et al. Status Report on the First round of the NIST Post-Quantum Cryptography Standardization Process[R]. National Institute of Standards and Technology, 2019.

[15] Nechvatal J, Barker E, Bassham L, et al. Report on the Development of the Advanced Encryption Standard (AES)[J]. *Journal of Research of the National Institute of Standards and Technology*, 2001, 106(3): 511-577.

[16] Dworkin M J. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions[R]. National Institute of Standards and Technology, 2015.

[17] Alagic G, Alperin-Sheriff J, Apon D, et al. Status Report on the First round of the NIST Post-Quantum Cryptography Standardization Process[R]. National Institute of Standards and Technology, 2019.

[18] Kumar M, Pattnaik P. Post Quantum Cryptography(PQC) - an Overview: (Invited Paper)[C]. *2020 IEEE High Performance Extreme Computing Conference*, 2020: 1-9.

[19] Braunstein S L, van Loock P. Quantum Information with Continuous Variables[J]. *Reviews of Modern Physics*, 2005, 77(2): 513-577.

[20] Banerjee U, Juvekar C, Fuller S H, et al. EeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things[C]. *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017: 1-6.

[21] Fernández-Caramés T M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things[J]. *IEEE Internet of Things Journal*, 2020, 7(7): 6457-6480.

[22] Chailloux A, Naya-Plasencia M, Schrottenloher A. An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography [C]. *International Conference on the Theory and Application of Cryptology and Information Security*, 2017: 211-240.

[23] Bernstein D J. Introduction to Post-Quantum Cryptography[M].

Post-Quantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 1-14.

[24] Wang W, Jungk B, Wälde J, et al. XMSS and Embedded Systems[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020: 523-550.

[25] Suhail S, Hussain R, Khan A, et al. On the Role of Hash-Based Signatures In Quantum-Safe Internet of Things: Current Solutions and Future Directions[J]. *IEEE Internet of Things Journal*, 2021, 8(1): 1-17.

[26] Buchmann J, Dahmen E, Ereth S, et al. On the Security of the Winternitz One-Time Signature Scheme [C]. *International conference on cryptology in Africa*, 2011: 363-378.

[27] Wieschebrink C. Two NP-Complete Problems In Coding Theory with an Application In Code Based Cryptography[C]. *2006 IEEE International Symposium on Information Theory*, 2006: 1733-1737.

[28] Samokhina M, Trushina O. Code-Based Cryptosystems Evolution[C]. *2017 IVth International Conference on Engineering and Telecommunication*, 2017: 15-17.

[29] Singh H. Code Based Cryptography: Classic McEliece[EB/OL]. 2019.

[30] Sendrier N. Code-Based Cryptography: State of the Art and Perspectives[J]. *IEEE Security & Privacy*, 2017, 15(4): 44-50.

[31] Regev O. Lattice-Based Cryptography[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 131-141.

[32] Buchmann J, Göpfert F, Güneysu T, et al. High-Performance and Lightweight Lattice-Based Public-Key Encryption[C]. *The 2nd ACM International Workshop on IoT Privacy*, *Trust*, *and Security*, 2016: 2-9.

[33] Du C H, Bai G Q. Towards Efficient Discrete Gaussian Sampling for Lattice-Based Cryptography[C]. *2015 25th International Conference on Field Programmable Logic and Applications*, 2015: 1-6.

[34] Gao S H, Heindl R. Multivariate Public Key Cryptosystems from Diophantine Equations[J]. *Designs*, *Codes and Cryptography*, 2013, 67(1): 1-18.

[35] Xie J F, Basu K, Gaj K, et al. Special Session: The Recent Advance In Hardware Implementation of Post-Quantum Cryptography[C]. *2020 IEEE 38th VLSI Test Symposium*, 2020: 1-10.

[36] Baldi M, Santini P, Cancellieri G. Post-Quantum Cryptography Based on Codes: State of the Art and Open Challenges[C]. *2017 AEIT International Annual Conference*, 2017: 1-6.

[37] Standaert F X. Introduction to Side-Channel Attacks[M]. Integrated Circuits and Systems. Boston, MA: Springer US, 2009: 27-42.

[38] Ferozpuri A, Farahmand F, Dang V, et al. Hardware api for Post-Quantum Public Key Cryptosystems[J]. *Technical Report*, 2018.

[39] Nguyen D T, Dang V B, Gaj K. High-Level Synthesis in Implementing and Benchmarking Number Theoretic Transform in Lattice-Based Post-Quantum Cryptography Using Software/Hardware Codesign[C]. *ARC*. 2020: 247-257.

[40] Basu K, Soni D, Nabeel M, et al. NIST Post-Quantum Cryptography-A Hardware Evaluation Study[J]. *IACR Cryptol. ePrint Arch.*, 2019, 2019: 47.

[41] Farahmand F, Nguyen D T, Dang V B, et al. Software/Hardware Codesign of the Post Quantum Cryptography Algorithm NTRUEncrypt Using High-Level Synthesis and Register-Transfer Level Design Methodologies[C]. *2019 29th International Conference on Field Programmable Logic and Applications*, 2019: 225-231.

[42] Soni D, Basu K, Nabeel M, et al. Conclusion[M]. Hardware Architectures for Post-Quantum Digital Signature Schemes. Cham: Springer International Publishing, 2020: 163-166.

[43] Soni D, Karri R. Efficient Hardware Implementation of PQC Primitives and PQC Algorithms Using High-Level Synthesis[C]. *2021 IEEE Computer Society Annual Symposium on VLSI*, 2021: 296-301.

[44] Ozcan E, Aysu A. High-Level Synthesis of Number-Theoretic Transform: A Case Study for Future Cryptosystems[J]. *IEEE Embedded Systems Letters*, 2020, 12(4): 133-136.

[45] Kumar V B Y, Gupta N, Chattopadhyay A, et al. Post-Quantum Secure Boot[C]. *2020 Design*, *Automation & Test in Europe Conference & Exhibition*, 2020: 1582-1585.

[46] Nejatollahi H, Dutt N, Cammarota R. Special Session: Trends, Challenges and Needs for Lattice-Based Cryptography Implementations[C]. *2017 International Conference on Hardware/Software Codesign and System Synthesis*, 2017: 1-3.

[47] Nejatollahi H, Dutt N, Ray S, et al. Post-Quantum Lattice-Based Cryptography Implementations[J]. *ACM Computing Surveys*, 2019, 51(6): 1-41.

[48] Wang W, Szefer J, Niederhagen R. FPGA-Based Niederreiter Cryptosystem Using Binary Goppa Codes [C]. *International Conference on Post-Quantum Cryptography*, 2018: 77-98.

[49] Karmakar A, Bermudo Mera J M, Sinha Roy S, et al. Saber on ARM[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018: 243-266.

[50] Hülsing A, Rijneveld J, Schwabe P. ARMed SPHINCS[M]. Public-Key Cryptography – PKC 2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 446-470.

[51] Albrecht M R, Hanser C, Hoeller A, et al. Implementing RLWE-Based Schemes Using an RSA Co-Processor[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018: 169-208.

[52] Ferozpuri A, Gaj K. High-Speed FPGA Implementation of the NIST round 1 Rainbow Signature Scheme[C]. *2018 International Conference on ReConFigurable Computing and FPGAs*, 2018: 1-8.

[53] Huang Y M, Huang M Q, Lei Z K, et al. A Pure Hardware Implementation of CRYSTALS-KYBER PQC Algorithm through Resource Reuse[J]. *IEICE Electronics Express*, 2020, 17(17): 20200234.

[54] Tian J, Wu B, Wang Z F. High-Speed FPGA Implementation of SIKE Based on an Ultra-Low-Latency Modular Multiplier[J]. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, 2021, 68(9): 3719-3731.

[55] Buchmann J, Dahmen E, Hülsing A. XMSS - a Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions [C]. *International Workshop on Post-Quantum Cryptography*, 2011:

117-129.

[56] Campos F, Kohlstadt T, Reith S, et al. LMS Vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4[C]. *International Conference on Cryptology in Africa*, 2020: 258-277.

[57] Bos J W, Hülsing A, Renes J, et al. Rapidly Verifiable XMSS Signatures[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020: 137-168.

[58] Mohan P, Wang W, Jungk B, et al. ASIC Accelerator In 28 nm for the Post-Quantum Digital Signature Scheme XMSS[C]. *2020 IEEE 38th International Conference on Computer Design*, 2020: 656-662.

[59] Cao Y, Wu Y Z, Wang W, et al. An Efficient Full Hardware Implementation of Extended Merkle Signature Scheme[J]. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, 2021, PP(99): 1-12.

[60] McGrew D, Curcio M, Fluhrer S. Leighton-Micali Hash-Based Signatures[R]. RFC Editor, 2019.

[61] Song Y F, Hu X, Wang W H, et al. High-Speed and Scalable FPGA Implementation of the Key Generation for the Leighton-Micali Signature Protocol[C]. *2021 IEEE International Symposium on Circuits and Systems*, 2021: 1-5.

[62] Schamberger T, Renner J, Sigl G, et al. A Power Side-Channel Attack on the CCA2-Secure HQC KEM [C]. *International Conference on Smart Card Research and Advanced Applications*, 2020: 119-134.

[63] Simmons P. Security through Amnesia: A Software-Based Solution to the Cold Boot Attack on Disk Encryption[C]. *The 27th Annual Computer Security Applications Conference on - ACSAC '11*, 2011: 73-82.

[64] Albrecht M R, Deo A, Paterson K G. Cold Boot Attacks on Ring and Module LWE Keys under the NTT[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018: 173-213.

[65] Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems [C]. *Annual International Cryptology Conference*, 1996: 104-113.

[66] Lerman L, Bontempi G, Markowitch O. Power Analysis Attack: An Approach Based on Machine Learning[J]. *International Journal of Applied Cryptography*, 2014, 3(2): 97.

[67] Fabšič T, Gallo O, Hromada V. Simple Power Analysis Attack on the QC-LDPC McEliece Cryptosystem[J]. *Tatra Mountains Mathematical Publications*, 2016, 67(1): 85-92.

[68] 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[J]. *IACR Cryptol. ePrint Arch.*, 2020, 2020: 912.

[69] Luo C, Fei Y S, Kaeli D. Effective Simple-Power Analysis Attacks of Elliptic Curve Cryptography on Embedded Systems[C]. *The International Conference on Computer-Aided Design*, 2018: 1-7.

[70] Shanmugam D, Selvam R, Annadurai S. Differential Power Analysis Attack on SIMON and LED Block Ciphers[M]. Security, Privacy, and Applied Cryptography Engineering. Cham: Springer International Publishing, 2014: 110-125.

[71] Aysu A, Tobah Y, Tiwari M, et al. Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange Protocols[C]. *2018 IEEE International Symposium on Hardware Oriented Security and Trust*, 2018: 81-88.

[72] Zhang F, Zhang Y R, Jiang H L, et al. Persistent Fault Attack In Practice[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020: 172-195.

[73] Bindel N, Buchmann J, Krämer J. Lattice-Based Signature Schemes and Their Sensitivity to Fault Attacks[C]. *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography*, 2016: 63-77.

[74] An H, Kim S, Lee J, et al. Timing and Fault Attacks on Lattice-based Cryptographic Libraries[C]. *2017 Symposium on Cryptography and Information Security (SCIS 2017). IEICE Technical Committee on Information Security*, 2017: 1-8.

[75] Khalid A, Rafferty C, Howe J, et al. Error Samplers for Lattice-Based Cryptography -Challenges, Vulnerabilities and Solutions[C]. *2018 IEEE Asia Pacific Conference on Circuits and Systems*, 2018: 411-414.

[76] Khalid A, Oder T, Valencia F, et al. Physical Protection of Lattice-Based Cryptography: Challenges and Solutions[C]. *The 2018 on Great Lakes Symposium on VLSI*, 2018: 365-370.

[77] Valencia F, Oder T, Güneysu T, et al. Exploring the Vulnerability of R-LWE Encryption to Fault Attacks[C]. *The Fifth Workshop on Cryptography and Security in Computing Systems*, 2018: 7-12.

[78] Ravi P, Sinha Roy S, Chattopadhyay A, et al. Generic Side-Channel Attacks on CCA-Secure Lattice-Based PKE and KEMs[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020: 307-335.

[79] Danner J, Kreuzer M. A Fault Attack on the Niederreiter Cryptosystem Using Binary Irreducible Goppa Codes[EB/OL]. 2020: arXiv: 2002.01455[cs.IT]. https://arxiv.org/abs/2002.01455.

曹元 于2015年在新加坡南洋理工大学电气与电子工程专业获得博士学位。现任河海大学物联网工程学院教授。研究领域为硬件安全、物理不可克隆函数。Email: caoyuan0908@gmail.com

姚恩义 于2016年在新加坡南洋理工大学电气与电子工程专业获得博士学位。现任华南理工大学微电子学院副教授。研究领域为数字及数模混合集成电路设计。Email: yaoenyi@scut.edu.cn

陆旭 于2018年在金陵科技学院通信工程专业获得学士学位。现在河海大学电子信息专业攻读硕士学位。研究领域为后量子密码密码学和硬件安全。Email: 547375542@qq.com

陈帅 于 2021 年在东南大学获得博士学位。现任磐石安全实验室主任。研究领域为硬件安全和后量子密码学。Email: chenshuai_ic@163.com

吴彦泽 于 2020 年在河海大学电子科学与技术专业获得学士学位。现在河海大学通信与信息系统专业攻读硕士学位。研究领域为应用密码学和硬件安全。Email: 3252221616@qq.com

叶靖 于 2014 年在中国科学院计算技术研究所获得博士学位。现任中国科学院信息通信技术计算机体系结构国家重点实验室副教授。研究领域为 VLSI 测试和安全。Email: yejing@ict.ac.cn

谢浩东 于 2020 年在河海大学物联网专业获得学士学位, 现在伦敦大学国王学院 Advanced computing 专业攻读硕士学位。研究领域为后量子密码密码学和硬件安全。Email: 3252221616@qq.com

乔云凯 现在河海大学通信工程专业攻读学士学位。研究领域为电磁场与波、数字图像处理等。Email: qiaoyk@hhu.edu.cn