前　言

曹　元[1], 田　静[2], 叶　靖[3]

[1]物联网工程学院 河海大学 常州 中国 213000
[2]电子科学与工程学院 南京大学 南京 中国 210023
[3]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

随着量子计算机的快速发展, 经典密码算法受到了前所未有的挑战。为解决这个问题, 一个新的密码学领域, 即后量子密码学(Post-Quantum Cryptography, PQC)应运而生, 基于它的加密算法可以对抗量子计算机的攻击。由于后量子密码算法通常运算量巨大, 采用集成电路技术能够实现以较低资源开销获得满足应用需求的执行速度, 当前已成为国内外研究的热门课题之一。本期专题旨在总结当前国内外研究趋势, 并展示国内研究人员在后量子加密算法硬件实现上的最新研究成果。

本期专题征稿历时 10 个月, 从众多稿件中遴选出 8 篇收录。每篇稿件均经过多次审稿与复审。专题收录 1 篇综述性文章, 主要介绍了目前后量子加密算法的硬件实现方式, 讨论了后量子加密算法在硬件实现上的挑战及机遇; 收录 1 篇基于 FPGA 的签名算法的高速实现文章, 介绍了一种基于哈希的后量子签名方案 LMS 的硬件实现与加速; 收录 1 篇 SHA-3 的硬件单元设计文章, 该方案能够广泛应用于后量子密码算法中; 收录 4 篇关于格的后量子加密算法的优化或实现, 包括基于 MLWE 的格密码高效硬件实现、CRYSTAL-KYBER 后量子方案的硬件设计优化空间探索、基于格的高效范围证明方案以及基于格陷门的高效密钥封装算法设计; 收录 1 篇基于同源的后量子密码算法的研究文章, 介绍了 Montgomery 模型的 w-坐标对同源计算的加速。

《后量子加密算法的硬件实现综述》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。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。

《基于 FPGA 的 Leighton-Micali 签名方案的高速可配置实现》首次对 LMS 进行硬件实现与加速。设计了一个软硬件协同系统, 将核心的哈希运算用硬件进行实现, 同时其次提出了一个高速的密钥生成架构来加速 LMS。该架构具有可配置性, 降低了延迟和提高了硬件利用率。

《应用于后量子密码的高速高效 SHA-3 硬件单元设计》针对后量子密码硬件实现中 SHA-3 单元性能与面积相互制约的瓶颈, 提出了一种高效高速的 SHA-3 硬件结构。通过更简单的轮常数存储方式, 更高效的流水线结构以及展开的优化方法兼顾了性能和硬件资源消耗的平衡。

《基于 MLWE 的格密码高效硬件实现》首先分析了最新参数 q=3329 基于 MLWE 的格密码公钥加密方案的算法理论, 并针对其中的核心模块—多项式乘法模块提出了两种不同的实现方式。两种实现方式都是基于频率抽取的数论变换(Number Theoretic Transform, NTT)算法。与已有的先进设计相比, 其提出的流水型 NTT 结构具备更好的速度性能。

《CRYSTAL-KYBER 硬件设计优化空间探索》使用高层次综合工具(High-level synthesis, HLS), 针对 CRYSTALS-KYBER 的三个主模块在不同参数集下探索硬件设计的实现和优化空间。同时编写了一个 TCL-perl 协同脚本来自动探索最优设计。与已有工作相比, 该工作对 CRYSTALS-KYBER 的优化使得封装算法的性能提高了 75%, 解封装算法的性能提高了 55.1%。与基准数据相比, 密钥生成算法的性能提高了 44.2%。

《基于格的高效范围证明方案》提出了两个更加高效的基于格假设的范围证明协议。首先, 针对 Regev 经典加密方案给出了一个高效的范围证明。该范围证明协议可以证明任意范围内的被加密值。与目前已有的基于格假设的范围证明方案相比, 所提方案都有着更小的合理性错误和更低的通信成本。

《基于格陷门的高效密钥封装算法》基于格的单向陷门函数, 设计并实现了高效密钥封装算法, 算法避免了去随机化和误差采样等操作, 从算法设计

层面提升了方案的效率。

《同源密码中 Montgomery 模型的 w-坐标研究》提出利用 Montgomery 曲线上的 2-同源构造出 3 类新的 w-坐标，与 x-坐标相同，它们均可应用于 Montgomery ladder 算法, 且可用于奇数次同源计算的优化。

我们要特别感谢《信息安全学报》编委会对本期专题工作的信任和指导, 感谢编辑部各位工作人员从征稿启事发布、审稿专家邀请至评审意见汇总、论文定稿、修改、校对和出版所付出的辛勤工作和汗水, 非常感谢专题评审专家及时、专业、细致的评审。我们还要感谢向专题踊跃投稿的各位作者。

最后, 感谢本期专题的读者们, 希望专题能够有助于你们的技术研究工作。