1 项目研究工作总结报告

随着5G/6G通信技术的普及和量子计算技术的快速发展，密码算法在受限环境下的高效实现已成为信息安全领域的核心挑战。物联网设备、车联网节点等资源受限的硬件平台由于指令集限制、寄存器约束和功耗要求，无法直接使用传统密码算法的标准实现。同时，后量子密码时代的来临使得高性能密码计算需求愈发迫切，GPU 等并行计算平台为大规模密码操作提供了新的可能。因此，研究密码算法在不同硬件平台上的优化实现技术，构建高效的密码工程解决方案，对于保障未来信息系统安全具有重要意义。

项目研究目标主要包括六个方面：第一，研究轻量级密码算法在 IoT 处理器上的位切片优化实现，针对 32 位处理器的指令集限制和寄存器约束，设计高效的位切片 SPN 密码实现方案；第二，研究后量子密码算法在 GPU 平台的高吞吐量并行架构，针对 FIPS 205 标准的 SLH-DSA 算法，设计自适应线程分配和函数级并行的 GPU 加速方案；第三，研究密码算法组件的跨平台优化技术，通过置换优化算法和改进的位切片门复杂度模型，实现密码组件在不同硬件平台上的高效映射；第四，研究深度学习在侧信道分析中的标签相关性优化技术，采用核密度估计方法计算标签间分布关系，结合样本局部相关性学习技术实现高效侧信道攻击；第五，研究多字节侧信道攻击的深度学习模型，设计基于标签分组和权重共享的多标签深度学习架构，实现单次训练同时恢复多个密钥字节；第六，研究密码实现的性能评估与基准测试方法，建立标准化的轻量级密码基准测试框架。项目采用文献研究法深入了解密码工程领域的相关研究进展，运用对比分析法比较不同硬件平台上的实现效率，通过实验论证分析法在 ARM Cortex-M 微控制器、NVIDIA RTX 4090 GPU 等实际硬件平台上验证优化方法的有效性。

在上述研究基础上，项目获得的主要研究成果有五个方面。第一，针对 IoT 处理器的位切片密码优化实现，本项目设计了置换优化算法（OPO）和改进的位切片门复杂度（BGC）模型编码方法。OPO 算法通过分割合并技术将复杂的置换操作转化为较少的指令序列，递归识别较优指令组合，以 QARMAv2 密码为例实现了 64.3% 的指令数量减少。改进的 BGC 模型基于代数标准形（ANF）框架设计新的编码方案，在 7 种密码 S 盒上实现了 11.7%-86.1% 的时间减少，平均加速比达到 3.19 倍。对 AES 和 QARMAv2 两种代表性 SPN 密码进行优化实现，AES 在 STM32L476 平台上实现 252.06 每字节周期数（CPB），相比基准实现提升 9.7%；QARMAv2 在相同平台上达到 684.50 CPB，相比查找表实现具有优势。第二，针对 GPU 平台的后量子密码加速，本项目设计了线程自适应的高吞吐量并行架构。提出自适应线程分配（ATA）方法，建立执行时间模型$T(g_i, t) = \alpha_i + \frac{\beta_i}{t} + \gamma_i \cdot t$，导出优化的线程分配公式$t_i^* = \sqrt{\frac{\beta_i}{\gamma_i}}$，通过精确性能建模动态优化线程配置。设计函数级并行（FLP）方法，将密码操作分解为可并发执行的细粒度计算任务。在 NVIDIA RTX 4090 GPU 上实现了 62,239 签名/秒的吞吐量，相比已有方案提升 16%，其中密钥生成、签名生成和验证相比 Kim 等人的工作分别提升 2.20 倍、1.41 倍和 1.76 倍。第三，基于核密度估计的标签相关性优化技术为深度学习侧信道分析提供了新的技术路径。项目组合作采用核密度估计方法计算标签间的分布关系，无需预先假设参数而是通过高斯核函数和适当的带宽自动学习密度分布形状，在 ASCAD 数据集上相比传统概率密度函数方法减少了 1000-1500 条攻击所需轨迹。结合样本局部相关性学习（LDL-SCL）方法，仅需 800 条训练轨迹即可完成攻击，相比传统 LDL 方法减少了 75% 的训练需求。第四，基于多标签学习的多字节攻击模型实现了并行密钥恢复的技术突破。项目组合作设计的 TripM 模型通过标签分组概念和权重共享的双分支卷积神经网络架构，能够在单次训练中同时恢复三个密钥字节。该模型在 ASCAD 和 TinyPower 数据集上平均需要 80-89 条轨迹即可恢复密钥，相比传统单字节攻击方法将全轮攻击时间减少了 28.7%。第五，为验证密码算法优化效果和促进技术传播，本项目构建了开源基准测试平台并进行了全面性能评估。开发了轻量级密码基准测试（LCB）框架，支持 ARM Cortex-M 和 ESP32-S3 微控制器的标准化性能评估，提供每字节周期数（CPB）、内存使用、代码大小等关键指标的统一评估标准。

为了验证密码算法优化方案的有效性，项目组在多种实际硬件设备上进行了全面的性能测试，包括配备 STM32L475VET6 微控制器的 PanDuoLa 开发板和 ESP32-S3-DevKitM-1 开发板。实验结果表明，

优化后的 AES 实现相比查找表方案提升 22.5% 的性能优势，验证了位切片并行处理在相同硬件平台上的有效性。项目组将所有开源代码和工具发布在 GitHub 平台，包括 S 盒优化工具、轻量级密码基准测试框架和 SLH-DSA GPU 实现，为密码学研究社区提供了开发和测试资源。在学术贡献方面，项目负责人已发表论文《Efficient implementations of CRAFT cipher for Internet of Things》于 Computers and Electrical Engineering 期刊，另有《Low-Latency Implementation of Bitsliced SPN-Cipher on IoT Processors》（IEEE Transactions on Computers，CCF-A，二审阶段）和《Thread-Adaptive: High-Throughput Parallel Architectures of SLH-DSA on GPUs》（IEEE Computer Architecture Letters，一审阶段）两篇核心论文在审。项目组合作发表了《Optimizing label correlation in deep learning-based side-channel analysis》（Microelectronics Journal，2025）和《Tripm: a multi-label deep learning SCA model for multi-byte attacks》（International Journal of Machine Learning and Cybernetics，2025）两篇论文，为项目在侧信道分析方向提供了重要技术支撑。这些研究成果为密码算法在受限环境下的高效实现提供了系统性的解决方案，在理论方法、技术实现和应用验证方面均取得了一定的进展，为物联网安全、后量子密码部署、侧信道分析等领域的发展提供了技术支撑。