

基于 BRLWE 的物联网后量子加密技术研究

高艺恬, 陈立全, 屠天扬, 高原, 陈芊叶

(东南大学网络空间安全学院, 江苏 南京 210096)

摘要: 随着量子计算机的发展, 现有的公钥加密体系无法保障物联网通信的安全性。后量子加密算法所基于的数学难题目前还不能被量子计算机攻破, 因此具备良好的抗量子安全性, 尤其是基于格的公钥密码体制, 有望成为下一代公钥加密体系的主流。然而, 后量子加密算法存在计算量大、存储空间大等问题, 如果将其直接应用于物联网终端的轻量级设备中, 会降低物联网环境的通信效率。为了更好地保护物联网通信安全, 保障物联网通信效率, 提出了 Sym-BRLWE (symmetrical binary RLWE) 后量子加密算法。该算法在基于二进制环上容错学习 (BRLWE, binary ring-learning with errors) 问题的加密算法的基础上, 改进了离散均匀分布上的随机数选取方式和多项式乘法的计算方式, 从而满足物联网通信的效率要求, 增加了加密安全性防护措施以保证算法在取得高效率的同时具有高安全性, 更加适应于物联网轻量设备。安全性分析表明, Sym-BRLWE 加密算法具有高安全性, 从理论上能够抵抗格攻击、时序攻击、简单能量分析和差分能量分析; 仿真实验结果表明, Sym-BRLWE 加密算法具有通信效率高的优势, 加密解密效率高且密钥尺寸小, 在模拟 8 bit 微型设备的二进制运算环境下, 选择 140 bit 的抗量子安全级别参数时, 相较于其他已有的基于 BRLWE 的加密算法, 同等加密条件下 Sym-BRLWE 加密算法能够在加密总时间上减少 30%~40%。

关键词: 后量子密码; 物联网; 公钥加密; 基于格的加密; 环上容错学习问题

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022024

Post-quantum encryption technology based on BRLWE for internet of things

GAO Yitian, CHEN Liquan, TU Tianyang, GAO Yuan, CHEN Qianye

School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China

Abstract: With the development of quantum computers, the classical public key encryption system is not capable enough to guarantee the communication security of internet of things (IoT). Because the mathematical puzzles which post-quantum encryption algorithms are based on cannot yet be broken by quantum computers, these new

收稿日期: 2021-08-31; 修回日期: 2021-10-15

通信作者: 陈立全, Lqchen@seu.edu.cn

基金项目: 国家重点研发计划 (2020YFE0200600)

Foundation Item: The National Key R&D Program of China (2020YFE0200600)

引用格式: 高艺恬, 陈立全, 屠天扬, 等. 基于 BRLWE 的物联网后量子加密技术研究[J]. 网络与信息安全学报, 2022, 8(5): 140-149.

Citation Format: GAO Y T, CHEN L Q, TU T Y, et al. Post-quantum encryption technology based on BRLWE for internet of things[J]. Chinese Journal of Network and Information Security, 2022, 8(5): 140-149.

algorithms have good anti-quantum computing security. In particular, the lattice-based cryptography is expected to become the main technology of the next generation public key cryptosystem. However, post-quantum encryption algorithms have the disadvantages of large amount of computation and high storage space. The communication efficiency of IoT will be affected if post-quantum encryption algorithms are directly applied to the lightweight device under IoT environment. In order to better guarantee the communication security and improve the commutation efficiency of IoT, Sym-BRLWE (symmetrical binary RLWE) encryption scheme was proposed. Sym-BRLWE was improved from the existing post-quantum encryption scheme based on BRLWE (binary ring-learning with errors) problem. Specifically, Sym-BRLWE encryption algorithm met the efficiency requirements of IoT via improving the random number selection on the discrete uniform distribution and the calculation of the polynomial multiplication. Sym-BRLWE encryption algorithm achieved high efficiency and high security via adding encryption security precautions, then it is more suitable for IoT lightweight devices. From the security analysis, the proposed Sym-BRLWE encryption scheme had high security. It could theoretically resist lattice attacks, timing attacks, simple power analysis (SPA) and differential power analysis (DPA). From simulation experiments, which were carried out in a binary computing environment simulating an 8-bit micro-device, the proposed Sym-BRLWE encryption scheme has high efficiency and small key size in encryption and decryption. It could reduce the total encryption time by 30% to 40% when compared with other BRLWE-based encryption schemes with the parameter selection of the 140 bit quantum security level.

Keywords: post-quantum cryptography, internet of things, public key encryption, lattice-based encryption system, ring-learning with errors

0 引言

网络安全问题不仅影响着人们的数据隐私,也关乎国家与社会的利益。互联网通信安全保障的基础在于信息加密技术的安全性。信息加密正面临着两大难题:一是物联网的蓬勃发展引发了物联网终端电子设备的应用热潮,给信息加密带来了极大的需求和挑战^[1];二是量子计算机的横空出世降低了处理海量数据的难度,给传统加密算法带来了致命的威胁^[2]。传统的公钥加密技术已被证明无法抵御量子计算的攻击,量子计算机的产生导致现有密码体制不再安全。有专家预估在不久的将来,大规模量子计算机的商用将伴随着 6G 时代一起到来^[3]。面对量子计算对加密领域造成的威胁,后量子密码应运而生。后量子加密算法具有抗量子性,可以弥补传统加密算法无法抵御量子攻击的不足。但是在复杂的物联网场景中,已知的后量子算法是否仍然可以有效运行并维护物联网安全,需要进一步探索。

(1) 物联网环境加密需求

物联网安全最大的挑战在于:① 物联网终端通常采用多种多样的嵌入式设备和轻量级处理

器,相较于普通计算机,它们具有存储容量小、算力不足、数据存储时间长、更新难度大等特点,以及低成本、低功耗的需求;② 物联网具有大规模、多协议、多种业务技术并存等特性,移动边缘计算的发展使得物联网面临众多异构终端用户接入,安全认证计算量大、通信安全性要求高^[4]。

因此,新形势下物联网环境所采用的公钥加密体制必须满足以下需求。

1) 抗量子攻击:为了抵抗量子计算对传统加密算法的威胁,必须在物联网环境中采用后量子加密系统代替传统加密系统。

2) 轻量级架构:不同于普通互联网中的加密系统可以依靠大型服务器与高内存用户端进行密钥计算与存储,物联网终端设备往往数据容量小、计算力低、传输时延长,不适合采用过于复杂的加密体制。

3) 多参数方案:不同物联网环境对安全级别的要求不同,过高的安全级别对硬件的要求更高,提供多种参数选择可以针对不同的加密环境与硬件配置选择最适加密方案。

4) 模块化运算:在算法实施的各个环节中,尽量模块化处理,便于硬件调用。

5) 适配性良好: 构造简洁, 经过封装能够良好地应用于各种硬件电路, 满足各种通信协议。

现有的用于物联网设备的加密算法中使用的大多是椭圆曲线加密算法。但是椭圆曲线加密算法不具备抗量子性, 且其加密效率并不高。基于格的公钥加密算法的硬件实现在最近几年得到蓬勃发展, 许多研究人员已经在嵌入式处理器上进行实验并报告了他们的实验结果。尤其是自 2010 年, 环上容错学习 (RLWE, ring-learning with error) 问题被提出以来, 密码学领域一直有科研人员尝试将基于 RLWE 问题的加密算法应用至硬件中。而在近 5 年中, 伴随物联网的快速发展, 对轻型物联网终端设备的 RLWE 加密应用更加成为研究热点, 其中包括对现场可编程门阵列 (FPGA, field programmable gate array) 电路、Cortex-M 系列微控制器、AVR-ATxmega 系列单片机等小型硬件设备的加密应用与改进。

(2) 基于格的公钥密码体制

基于格的公钥密码体制 (lattice-based cryptography) 是被研究最多的后量子加密体制之一。格是线性空间上确定的一组线性无关向量的整数线性组合。基于格的公钥加密体制根据不同的格上困难问题所构造, 如最短向量问题 (SVP, shortest vector problem)、最近向量问题 (CVP, closest vector problem)、最短独立向量问题 (SIVP, shortest independent vector problem) 等。基于格的公钥密码体制通常将困难问题从平均情况难解性归约到可证明的最坏情况难解性, 因此可以证明其具有很高的抗量子安全性。

基于格的公钥密码体制发展迅速, 目前被认为具有前景的方案包括 NTRU (n-th degree truncated polynomial ring units) 加密、基于容错学习 (LWE, learning with errors) 困难问题的加密和基于 RLWE 困难问题的加密等。

本文的主要贡献如下。

1) 在基于二进制环上容错学习问题的加密算法——BRLWE 的基础上, 将二进制分布范围由 $\{0,1\}$ 改为 $\{-1,1\}$, 并对其中的多项式环计算进行了简化, 即将多项式乘法和多项式加法运算融合为一个乘加模块, 减少了计算过程中产生的设备内存消耗, 更加适用于物联网轻量设备。

2) 在改进的 RBLWE 算法中增加了加密安全性防护措施, 从而能够抵御物联网环境中常见的侧信道攻击 (具体包括时序攻击、简单功耗分析、差分功耗分析等), 且加密效率依然很高。

1 相关工作

1.1 基于格的 RLWE 加密算法

Lyubashevsky 等^[5]2010 年首次提出了 RLWE 问题, 它是 LWE 问题在多项式环上进行改进后的表现形式。基于 RLWE 问题的加密算法被称为 RLWE 加密算法, 它相较于 LWE 加密算法, 具有密钥尺寸小、加密效率高等特性。

近年来, RLWE 加密算法在基于格的后量子密码中愈发得到重视, 其简洁的计算方式和小尺寸的密钥被认为在物联网环境下具有广阔的应用前景。

Pöppelmann 等^[6]首次将基于快速傅里叶变换 (FFT, fast Fourier transform) 的快速数论变换 (NTT, number theoretic transform) 算法应用在 RLWE 加密中的多项式乘法中, 并通过实验验证 NTT 可以在硬件上得到很好的应用效果, 提高了加密效率。此后, 在不同轻量级设备上的 RLWE 加密研究越来越受到关注。

Roy 等^[7]、Fritzmam 等^[8]基于 FPGA 架构对 RLWE 加密中的 NTT 算法进行了进一步优化与仿真实验。Clercq 等^[9]使用了 32 位 ARM 的 Cortex-M4F 微处理器作为实验平台, 并对高斯抽样算法和多项式乘法进行了优化, 使得 RLWE 加密在软件上的应用速度提升了至少 7 倍。Boorghany 等^[10]首次在 8 bit 处理器上实现基于格的加密方案。Liu 等^[11]在 8 bit AVR 处理器上对 NTT 算法进行了改进, 使用特殊的系数存储方法减少了多项式乘法的 RAM 占用空间。2020 年, 他们在 ARM NEON 和 MSP430 架构上首次实现了 RLWE 加密。Seo 等^[12]提出了一种基于 8 bit AVR 微控制器的安全紧凑的 Ring-LWE 加密方案, 并给出了针对简单功耗分析和时序攻击的对策。

然而, 对于物联网终端设备, 尤其是一些需要长期运行并存储数据的小型设备而言, 高斯分布和 NTT 算法的应用仍然被认为不够轻量。因此基于 RLWE 加密算法提出了 BRLWE 加密算法。

1.2 BRLWE 加密

当 LWE 问题中引入的误差不服从高斯分布，而服从 $\{0,1\}$ 上的离散均匀分布，则称该问题为 BLWE (binary-LWE) 问题。通过对 RLWE 问题进行相似简化，将引入的误差由高斯分布简化为 $\{0,1\}$ 上的二元离散均匀分布，这种问题被称为 BRLWE (binary-RLWE) 问题，相应的加密算法则称为 BRLWE 加密算法。

BRLWE 加密算法最早由 Buchmann 等^[13]于 2016 年在 8 bit 微型处理器 ATXmega128 和 32 bit Cortex M0 上进行了应用。不同于经典的 RLWE 加密算法，Buchmann 等对 n 和 q 两个参数的选择均使用 2 的次幂，即在二进制中，模 2^n 相当于仅保留数值的低 n 位，从而大大提高了模 q 运算的效率。

Aysu 等^[14]针对 BRLWE 加密算法使用包括简单能量分析 (SPA, simple power analysis)、差分能量分析 (DPA, differential power analysis) 和高阶 DPA 攻击在内的不同侧信道攻击进行了深入分析，并提出了相应的对策。由于满足 $\{0,1\}$ 离散均匀分布的多项式系数向量在多项式乘法过程中具有明显的功率差异，BRLWE 加密的直接实现在抵抗侧信道攻击时十分脆弱，甚至不能够有效抵御 SPA。为此，Aysu 等分析了 RBLWE 加密算法的效率和硬件成本，并添加了冗余计算和内存更新以抵抗 SPA。同时他们构建了基于中间状态随机化和屏蔽阈值解码的轻量级的有效保护对策，并在 SAKURA-G FPGA 板上进行了仿真与比较。与未受保护的设计相比，该对策能够将 DPA 攻击所需的测量次数增加 40 倍。

Shahriar 等^[15]在 BRLWE 算法上进行了一系列优化。2019 年，他们提出了 InvRBLWE 加密方案，该方案对环上多项式的乘法进行了优化，选择多项式系数范围为 $[-q/2, q/2-1]$ 并对应至 8 bit 二进制补码，在乘法过程中通过逆向取二进制补码形式的系数进行循环运算。此外，Shahriar 等还为 InvRBLWE 提出了两种硬件架构，一种是针对边缘物联网设备的高速架构，具有高效率加密的优势；另一种是超轻量级架构，适用于物联网中资源受限的节点上的应用。针对侧信道攻击，Shahriar 等继续提出了一系列改进措施。文献[16]所提方案能够抵御 DPA 攻击，而文献[17]所述方

案能够良好地抵御错误注入 (FI, fault injection) 攻击。并且上述方案均在不同硬件设备上进行了测试与验证。Shahriar 等的研究成果推进了 RBLWE 加密在物联网应用技术上的发展，具有很大的参考价值。

此外，Xie 等^[18]提出了一种 novel LUT-like 的多项式乘法方案。他们利用 4 输入乘法器作为多项式乘法的最小计算单元，在每次进行多项式乘法时，将 n 项系数两两拆分，再通过乘法器进行分别运算。He 等^[19]对多项式乘法从硬件角度进行了解构，在硬件配置上做了相关改进。上述研究成果选取了一些新颖的角度进行研究，也十分具有启发性。

BRLWE 算法的多项式运算模块的改进与安全性保障是将 BRLWE 真正应用于物联网终端的研究重点。

2 算法改进

2.1 符号说明

为更好地理解本文加密算法的实现过程，对本文常用符号进行如下约定和说明。

n : 多项式项数。

q : 取模运算模值。

R_q : 模 q 多项式环。

m : 二进制明文序列。

$\bar{m}$: 编码后明文序列。

s : 私钥。

p : 公钥。

u, v : 密文。

e_0, e_1, e_2, e_3 : 随机生成的环上多项式系数向量。

2.2 算法介绍

本文提出了 Sym-BRLWE (symmetrical binary RLWE) 算法，该算法改进了 BRLWE 加密，具体为调整了离散均匀分布上的随机数选取，优化了多项式乘法的计算细节。

在前文提及的 BRLWE 算法中，其运用的 $\{0,1\}$ 离散均匀分布已具备以下应用于物联网终端的优势：

1) 数据量更小，计算更便捷，能够更好地在轻量级设备上快速运算；

2) 省去了离散高斯分布抽样过程，加快了运

算时间;

3) $\{0,1\}$ 分布更便于直接进行二进制存储;

4) 由于加密过程中涉及的多项式乘法均有一个多项式的系数全为 $\{0,1\}$, 称之为二进制多项式, 因此多项式乘法有更简洁的运算方法代替 NTT。

本算法不同于其他已提出的 BRLWE 算法, 该算法在离散均匀分布上将选取对称的 $\{-1,1\}$ 分布代替 $\{0,1\}$ 分布。 $\{-1,1\}$ 分布与 $\{0,1\}$ 分布具有相同的优点, 同时能够更好地抵抗 SPA 攻击。为对应于 $\{-1,1\}$ 分布, 环 R_q 的范围为 $[-q/2, q/2-1]$, 使 $\{-1,1\} \in R_q$ 。

BRLWE 加密算法如算法 1 所示, 由于 $\{-1,1\}$ 分布的改变, 对明文的编、解码将有所调整。算法的所有运算均在模 q 条件下进行。

算法 1 BRLWE 加密算法

输入 参数: n, q , 明文: m

密钥生成

1) 随机选择 $e_0, s \in \{-1,1\}^n$

2) 随机选择 $a \in R_q$

3) $p \leftarrow e_0 - as \in R_q$

私钥为 s , 公钥为 (a, p)

加密

1) 对长度为 n 的二进制明文序列 $m \in \mathbb{Z}_2^n$ 进行编码 $\bar{m}_i \leftarrow \lfloor q/2 \rfloor m_i$, 得到 $\bar{m} \in R_q$

2) 随机选择 $e_1, e_2, e_3 \in \{-1,1\}^n$

3) $v \leftarrow pe_1 + e_3 + \bar{m} \in R_q$

4) $u \leftarrow ae_1 + e_2 \in R_q$

密文为 (u, v)

解密

1) $\bar{m}' \leftarrow su + v \in R_q$

2) 译码后得到解密结果 $m'_i \leftarrow \begin{cases} 1, & \frac{q}{4} \leq \bar{m}'_i < \frac{3q}{4} \\ 0, & \text{其他} \end{cases}$

若解密成功, 则 $m' = m$

BRLWE 解密正确性分析如下:

$$\begin{aligned} m' &= \text{Decode}(\bar{m}') = \text{Decode}(su + v) = \\ &= \text{Decode}(s(ae_1 + e_2) + pe_1 + e_3 + \bar{m}) = \\ &= \text{Decode}(s(ae_1 + e_2) + (e_0 - as)e_1 + e_3 + \bar{m}) = \\ &= \text{Decode}(\bar{m} + se_2 + e_0e_1 + e_3) \end{aligned} \quad (1)$$

由式(1)可知, 使得 $m' = \bar{m}'$ 解密正确的标准是 $se_2 + e_0e_1 + e_3$ 极小, 可以忽略不计。由于 se_2 和 e_0e_1 都是两个 $\{-1,1\}$ 分布的多项式进行相乘, 下面以 e_0e_1 为例进行分析, e_0e_1 的第 i 项表示如下。

$$[e_0e_1]_i = \sum_{j=0}^i [e_0]_j [e_1]_{i-j} - \sum_{j=i+1}^{n-1} [e_0]_j [e_1]_{n+i-j} \quad (2)$$

则其均值为:

$$\begin{aligned} E[e_0e_1]_i &= E\left(\sum_{j=0}^i [e_0]_j [e_1]_{i-j}\right) - \\ &E\left(\sum_{j=i+1}^{n-1} [e_0]_j [e_1]_{n+i-j}\right) = 0 \end{aligned} \quad (3)$$

因此可得 $se_2 + e_0e_1 + e_3$ 的均值:

$$E(se_2 + e_0e_1 + e_3) = 0 + 0 + 0 = 0 \quad (4)$$

所以对 $\bar{m}'$ 的解码公式为

$$m'_i = \begin{cases} 1, & \frac{q}{4} \leq \bar{m}'_i < \frac{3q}{4} \\ 0, & \text{其他} \end{cases} \quad (5)$$

而在使用 $\{0,1\}$ 分布时, 有以下明文解码公式:

$$m'_i = \begin{cases} 1, & \frac{q}{4} \leq \bar{m}'_i + i - \frac{n}{2} + \frac{1}{2} < \frac{3q}{4} \\ 0, & \text{其他} \end{cases} \quad (6)$$

因为 $\{0,1\}$ 分布的均值为 $1/2$, 随着多项式项数的增加, 该均值误差造成的偏移会相应增加, 因此需要解码时进行修正。相比较而言, 选取 $\{-1,1\}$ 分布, 计算中形成的误差均值为 0, 在 0 点处对称, 与经典的 RLWE 中的高斯分布误差更加接近, 因此在解码时也无须额外修正。

2.3 物联网环境下算法的实现

本节基于物联网背景对各加密环节进行具体分析。已被应用在 BRLWE 方案中的参数主要有: $n = 256, q = 256$ 能够满足 84 bit 安全和 73 bit 后量子安全; $n = 512, q = 256$ 满足 190 bit 安全和 140 bit 后量子安全^[20]。下面以 8 bit 微处理器环境为背景, 选择 $n = 256, q = 256$ 进行改进算法的阐述。

(1) 随机数生成

为了能够随机生成满足 $\{-1,1\}$ 分布或 R_q 环上均匀分布的多项式系数向量, 同时不浪费内存空间, 本文使用 8 bit 二进制随机数生成器。对于 R_q

环上均匀分布的多项式系数向量, 8 bit 二进制数的范围为 $\{00000000, 00000001, \dots, 11111111\}$, 正好满足 R_q 中 $[-q/2, q/2-1]$ 各个整数的补码。则生成多项式 $a \in R_q$ 只需进行 n 次 8 bit 二进制随机数选取。对于 $\{-1, 1\}$ 分布, 在硬件中仍然生成 $\{0, 1\}$ 分布, 在后续运算中再通过对 0 和 1 的判断转换为实际上满足 $\{-1, 1\}$ 分布的运算。这样做的优势在于, 由于 0 和 1 是二进制的基本组成数字, 在 8 bit 随机数生成器中, 进行 $n/8$ 次的 8 bit 二进制随机数选取再进行各 bit 的截取, 即可得到 n bit 二进制随机数, 大大缩短了随机数生成时间。

(2) 环上多项式运算

在 BRLWE 加密过程中, 最关键的是多项式乘法和多项式加法运算。由于计算是在 R_q 多项式环上进行, 因此在计算过程中需要对系数模 q , 即保证每一项系数都在 $0 \sim q-1$ 。当 $q=256$, 在 8 bit 微处理器中只需对每个系数截取低 8 位即可达到取模效果。多项式环运算的另一个特点是, 由于:

$$R_q = \frac{f(x)}{x^n + 1} \quad (7)$$

$$x^n \equiv -1 \pmod{q} \quad (8)$$

多项式项数恒定为 n , 因此在多项式乘法计算中, 对于大于 $n-1$ 次幂的高次项需进行 n 位平移约减。

对于 $\{-1, 1\}$ 分布的多项式而言, 因为在寄存器中所有系数是以二进制 8 bit 一组存储的, 所以需对二进制字符串进行从 $\{0, 1\}$ 分布向 $\{-1, 1\}$ 分布的转换。

环上多项式加法计算如算法 2、算法 3 所示。

算法 2 环上多项式加法计算 (含二进制多项式)

输入 多项式 $a \in R_q, b \in \{0x00, 0x01, \dots, 0xFF\}^{n/8}$

输出 a

- 1) loop = 0
- 2) for $i = 0, 1, \dots, (n/8-1)$ do
- 3) for $j = 7, 6, \dots, 0$ do
- 4) tempbit = $b_i \gg j \& 1$
- 5) $a_{loop} = (a_{loop} + (\text{tempbit} \ll 1-1)) \& 0xFF$
- 6) loop ++

7) end for

8) end for

算法 3 环上多项式加法计算 (不含二进制多项式)

输入 多项式 $a \in R_q, b \in R_q$

输出 a

- 1) for $i = 0, 1, \dots, n-1$ do
- 2) $a_i = (a_i + b_i) \& 0xFF$
- 3) end for

多项式乘法计算如算法 4 所示, 本算法在文献[15]中所述的循环移位方法的基础上, 简化了多项乘法计算步骤。

算法 4 环上多项式乘法计算

输入 多项式 $a \in R_q, b \in \{0x00, 0x01, \dots, 0xFF\}^{n/8}$

输出 res

- 1) temp_a = $a[0]$
- 2) for $i = 0, 1, \dots, (n/8-1)$ do
- 3) for $j = 7, 6, \dots, 0$ do
- 4) tempbit = $b_i \gg j \& 1$
- 5) pos = $(\sim \text{tempbit} + 1) \& 0xFF$
- 6) neg = $(\text{tempbit} - 1) \& 0xFF$
- 7) for $k = 0, 1, \dots, n-2$ do
- 8) $a_k = (c_k \& \text{pos} - c_k \& \text{neg} + a_{k+1}) \& 0xFF$
- 9) end for
- 10) $a_{n-1} = (c_{n-1} \& \text{pos} - c_{n-1} \& \text{neg} - \text{temp_a}) \& 0xFF$
- 11) end for
- 12) end for

第 5)、6) 行中的 pos 和 neg 用于分别将 1 和 0 转化为 $\{-1, 1\}$, 具体如下:

$$\text{pos} = (\sim \text{tempbit} + 1) \& 0xFF = \begin{cases} 0x00, \text{tempbit} = 0 \\ 0xFF, \text{tempbit} = 1 \end{cases} \quad (9)$$

$$\text{neg} = (\text{tempbit} - 1) \& 0xFF = \begin{cases} 0xFF, \text{tempbit} = 0 \\ 0x00, \text{tempbit} = 1 \end{cases} \quad (10)$$

其中, “ $\sim$ ” 表示按位取反。式(9)、(10)使得多项式乘法运算中不需要判断乘数是 1 还是 -1, 整个循环过程中没有类似 if/else 的判断流程, 这将有

助于保护密钥的隐秘性,同时快速地将寄存器中的 $\{0,1\}$ 转换至实际上的 $\{-1,1\}$ 分布进行运算。

原始的 n 项多项式的乘法运算共需 n^2 次乘法和 $n(n-1)$ 次加法运算。在本文所提算法中,没有乘法运算,只需进行 $2n^2$ 次加法运算和 $2n+2n^2$ 次位操作,效率更高。

表 1、表 2 分别给出了 Sym-BRLWE 在 8 bit 微处理器上加密过程中几个重要数据的理论所需时间和存储空间。表 1 中 T_{random} 表示随机生成一位二进制数所需时间, T_{add} 表示进行 n 项多项式加法所需时间, T_{mul} 表示进行 n 项多项式环上乘法所需时间。表 2 中 m 表示明文长度是多项式项数 n 的 m 倍。

表 1 Sym-BRLWE 加密时间
Table 1 Encryption time of Sym-BRLWE

算法环节	理论时间
密钥生成	$9nT_{\text{random}} + T_{\text{add}} + T_{\text{mul}}$
加密	$nT_{\text{shift}} + 3nT_{\text{random}} + (2+m)T_{\text{add}} + 2T_{\text{mul}}$
解密	$nT_{\text{shift}} + T_{\text{mul}} + T_{\text{add}}$

表 2 Sym-BRLWE 各数据存储空间
Table 2 Data storage space of Sym-BRLWE

数据内容	存储空间/bit
私钥	n
公钥	$16n$
明文	mn
密文	$16mn$

3 安全性分析

3.1 格攻击

对于基于格的后量子加密算法而言,存在许多根据格困难问题本身进行的攻击,称之为格攻击。常见的格攻击方法主要是一些格基约减算法如 LLL (Lenstra-Lenstra-Lovász)、BKZ (Block Korkine-Zolotarev) 等,它们通过将格基进行约减变化使格上困难问题的求解变得容易。BRLWE 算法基于的 BRLWE 问题是 RLWE 问题的变体。文献[21]简单地证明了 BRLWE 问题至少与标准 LWE 问题一样困难,因此本文认为 BRLWE 问题基于的格上数学难题是足够难解的,算法理论是足够安全的。

3.2 侧信道攻击

侧信道攻击 (SCA, side channel attack) 是一

种对加密硬件的攻击方式,包括时序攻击、能量分析、错误注入等方式。不同于针对算法本身的软件攻击,它通过对加密时的信道进行监测,对各硬件计算和传输数据时泄露的信息进行攻击,而无须侵入算法内部。下面将从侧信道攻击的角度对 Sym-BRLWE 进行安全分析。

(1) 时序攻击

时序攻击 (timing attack) 是通过分析加密过程中执行不同具体运算产生的时间差异进行的侧信道攻击。例如,当 $s=0$ 时加密所需时间比 $s=1$ 时要快,则时序攻击将很容易通过比较时间消耗进行攻击。

在本文提出的 Sym-BRLWE 加密算法中,由于使用了 $\{-1,1\}$ 分布的二进制多项式,没有根据明文或密钥产生的程序运行分支,所有语句在任何情况下都要执行,即该算法在每个时钟周期内独立于输入值运行,所以时钟周期数是恒定的。具体来说, Sym-BRLWE 在密钥生成、加密和解密 3 个环节中所需的时钟周期数分别是 $n+1$, $2n+3$, $n+1$, 都只与 n 有关。因此, Sym-BRLWE 能够抵抗时序攻击。

(2) SPA 攻击

SPA 攻击对硬件电流随时间变化的情况进行监测与分析,电子元件在执行不同操作时,功耗会发生变化^[22]。

在原始的 BRLWE 加密中,当二进制多项式系数遇“0”时不进行任何计算,只有在遇“1”时才进行加法运算,这将给 SPA 攻击提供可乘之机。例如,在解密过程中, SPA 攻击能够判断是否进行了加法运算产生的功耗差异,从而破解私钥。而在 Sym-BRLWE 中,由于将“0”实际上视作“-1”,无论二进制多项式的系数是“0”还是“1”,都要进行加法和减法以及与运算,运算相同则功耗也相同,因此该算法可以抵抗 SPA 攻击。

(3) DPA 攻击

SPA 攻击只在分析单个运算操作下有效,而对于同时进行多个操作的系统,由于信号的混合, SPA 将无能为力。DPA 则将有加密操作的信号减去没有加密操作的噪声从而得到需要分析的关键信号。只要获取足够多的能量迹线并进行统计分析, DPA 攻击就能够发掘细微的功耗与密钥之间

的联系, 因此 DPA 更难预防^[23]。

文献[15]和[16]采用的 InvBRLWE 加密方案对乘数系数为 0 或 1 两种情况都进行了加法运算, 但加 0 和加 a_{j-1} 所产生的功耗差异依然明显, 虽然能够抵御 SPA 攻击, 但不能抵御 DPA 攻击。文献[14]和[16]中分别针对 BRLWE 算法给出了抵抗 DPA 的方法。文献[14]在解密阶段增加了一个随机数生成器, 使得多项式乘法的结果不仅仅依赖于私钥, 还与一个随机数有关, 从而对 DPA 攻击产生干扰。文献[16]则在每项系数的乘法中将“0”和“1”两种情况均进行计算, 然后在结果处判断选择真正需要的结果。在本文提出的 Sym-BRLWE 加密算法中, 采用 $\{-1, 1\}$ 分布本身就对 DPA 攻击有一定的防御性。因为无论是 0 还是 1, 都必须进行加 a_{j-1} 或减 a_{j-1} 的操作, 这样算法本身便将运算过程与私钥值分离, 而且无论是加还是减, 数值上都存在正或负的变化, 功耗差异将大大缩小。

(4) FI 攻击

FI 攻击能够针对系统中的数据或控制单元进行攻击。攻击者将错误信息注入内存或信号以利用函数的错误执行从而提取秘密数据 (如未加密的明文或私钥等)。

文献[17]中提到的应对 FI 攻击的措施同样可以应用到本文方案中, 关于错误注入攻击的防御将在未来进行进一步研究。

4 实验分析

本节对文献[13]、[14]和[16]中提出的基于 BRLWE 加密算法和本文提出的 Sym-BRLWE 加密算法进行实验仿真与比较。算法代码基于 Python 语言编写, 仿真环境为 64 bit Windows10 专业版, Python 3.7.2, 硬件配置为 Intel(R) Core(TM) i5-7200U 2.50 GHz 2.70 GHz CPU 处理器及 8 GB RAM。本仿真实验对各算法分别根据 n 的取值选择两种参数方案, 如表 3 所示, 然后对 512 bit 的二进制明文加密, 进行 200 次实验取均值, 并根据结果比较包括密钥生成时间、加密时间、解密时间、私钥大小、公钥大小、密文大小等加密特征。

经过仿真后得到的各加密算法的时间消耗和数据大小统计分别如表 4、表 5 所示。

表 3 RBLWE 加密参数及对应安全级别
Table 3 Parameters and security level of RBLWE

加密方案	安全级别/bit	n	q
RBLWE-I	84/73	256	256
RBLWE-II	190/140	512	256

注: 安全级别中的“/”前后数字表示传统安全级别和量子安全级别。

表 4 各加密算法时间消耗统计
Table 4 Time consumption of each encryption algorithm

加密算法	参考文献	密钥生成时间/ms	加密时间/ms	解密时间/ms
R-BinLWE-I	文献[13]	21.54	57.525	41.94
R-BinLWE-II	文献[13]	78.455	144.18	69.705
B-RLWE-I	文献[14]	50.275	92.365	92.765
B-RLWE-II	文献[14]	201.315	379.715	181.745
InvRBLWE-I	文献[16]	59.8	112.735	112.065
InvRBLWE-II	文献[16]	237.86	446.9	218.275
Sym-BRLWE-I	本文算法	47.89	84.795	71.65
Sym-BRLWE-II	本文算法	148.655	263.005	122.74

表 5 各加密算法数据大小统计
Table 5 Data size of each encryption algorithm

加密算法	参考文献	私钥大小/byte	公钥大小/byte	密文大小/byte
R-BinLWE-I	文献[13]	511	2 051.82	2 740.15
R-BinLWE-II	文献[13]	1023	4 111.325	3 652.6
B-RLWE-I	文献[14]	127	2 051.97	2 740.98
B-RLWE-II	文献[14]	255	4 110.85	3 655.005
InvRBLWE-I	文献[16]	127	2 051.46	2 739.625
InvRBLWE-II	文献[16]	255	4 110.91	3 655.685
Sym-BRLWE-I	本文算法	127	2 053.495	2 740.245
Sym-BRLWE-II	本文算法	255	4 112.455	3 656.85

从表 4 能够看出, 在各算法中, 更高的安全级别必然需要更大的时间消耗。而比较同一安全级别下的各个加密算法, 可以看出 R-BinLWE 在各阶段所需时间均为最短, 这是因为 R-BinLWE 仅仅基于原始的 BRLWE 构造, 没有任何安全措施, 缺乏抵抗侧信道攻击的能力。R-BinLWE 是最原始的理想化算法, 安全性很弱, 仅作为其他算法的比较参考。InvRBLWE 所需时间在 4 种加密算法中相对最长, 这是因为 InvRBLWE 为抵抗 SPA、DPA 攻击在加密过程中采用了掩码操作,

做出了一定的效率牺牲。它的安全性能保证，但效率低于 Sym-BRLWE。此外，Sym-BRLWE 相较于 B-RLWE 也有一定效率优势。B-RLWE 的时间消耗主要源于其在抵御 DPA 攻击时增加了一次环上随机数生成环节。

图 1 为各算法加/解密总时间比较（包括密钥生成时间、加密时间和解密时间），其中红色虚线和蓝色虚线分别标明了 Sym-BRLWE 在 $n = 256$ ， $n = 512$ 时的时间水平线。可以看出，在 $n = 512$ ，各算法之间的效率差距更为明显。这是因为随着 n 值的增大，B-RLWE 和 InvRBLWE 为保障安全性而添加的掩码操作等措施将消耗更多的时间。从具体数据来看，Sym-BRLWE 的总时间消耗仅占 B-RLWE 的 70.1%，占 InvRBLWE 的 59.2%。因此本文提出的 Sym-BRLWE 加密算法在选择 140 bit 的量子安全级别参数时，相较于其他 BRLWE 算法，加密总时间至少能够减少 30%，最多能够减少约 40%。

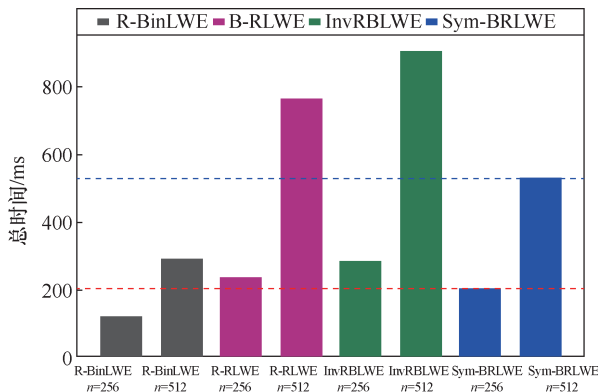


图 1 各算法加解密总时间比较

Figure 1 Comparison of the total encryption time of each algorithm

Sym-BRLWE 的效率优势在根本上主要体现在：多项式乘法上减去了一个判断分支；解密时不需要额外的解码运算；省去了一些耗时的安全性措施。因此 Sym-BRLWE 在安全性不弱于其他上述算法的情况下，效率上具有明显的优势。

从表 5 给出的加密算法数据大小统计中可以看到，Sym-BRLWE 保证了与 B-RLWE 和 InvRBLWE 的一致，即私钥大小比原始 R-BinLWE 方案要小 75%，而公钥大小、密文大小与原始方案不变。由于 R-BinLWE 在生成二进制多项式时，没有使用 8 bit 二进制随机数生成器生成数字再进

行按位截取，因此占用了大量冗余空间。其他 3 个算法均针对轻量硬件设备考虑到这一点，因此私钥大小得到了大幅缩小。

5 结束语

本文提出了一种后量子加密算法 Sym-BRLWE，该算法具有更高的加密效率，更小的密钥尺寸，同时能够抵御时序攻击、SPA、DPA 等侧信道攻击，因此更加适用于物联网应用。经过仿真实验验证，在 8 bit 运算背景选择 140 bit 的量子安全级别参数时，相较于其他已有 BRLWE 算法，加密总时间能够减少至少 30%，证明了 Sym-BRLWE 加密算法比其他已提出的 BRLWE 相关算法加密效率更高。本文的研究存在一些尚未解决的问题有待后续的进一步拓展研究，包括仿真实验可以拓展到更真实的硬件环境中进行，探讨更适宜于新型物联网硬件框架的优化机制与方法等。

参考文献：

- [1] SCHNEIER B. IoT cybersecurity: what's plan B[R]. 2017.
- [2] 朱小伶. 2020 年量子计算技术发展综述[J]. 无人系统技术, 2021, 4(2): 26-32.
ZHU X L. Survey of quantum computing technology in 2020[J]. Unmanned Systems Technology, 2021, 4(2): 26-32.
- [3] 张成磊, 付玉龙, 李晖, 等. 6G 网络安全场景分析及安全模型研究[J]. 网络与信息安全学报, 2021, 7(1): 28-45.
ZHANG C L, FU Y L, LI H, et al. Research on security scenarios and security models for 6G networking[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 28-45.
- [4] 陈璐, 汤红波, 游伟, 等. 移动边缘计算安全防御研究[J]. 网络与信息安全学报, 2021, 7(1): 130-142.
CHEN L, TANG H B, YOU W, et al. Research on security defense of mobile edge computing[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 130-142.
- [5] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[M]//Advances in Cryptology – EUROCRYPT 2010. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 1-23.
- [6] PÖPPELMANN T, GÜNEYSU T. Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware[M]//Progress in Cryptology-LATINCRYPT 2012. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 139-158.
- [7] ROY S S, VERCAUTEREN F, MENTENS N, et al. Compact ring-LWE cryptoprocessor[C]//Cryptographic Hardware and Embedded Systems – CHES 2014. 2014: 371-391.
- [8] FRITZMANN T, SEPÚLVEDA J. Efficient and flexible low-power

- NTT for lattice-based cryptography[C]//Proceedings of 2019 IEEE International Symposium on Hardware Oriented Security and Trust. 2019: 141-150.
- [9] DE CLERCQ R, ROY S S, VERCAUTEREN F, et al. Efficient software implementation of ring-LWE encryption[C]//Proceedings of Design, Automation & Test in Europe Conference & Exhibition (DATE). 2015: 339-344.
- [10] BOORGHANY A, SARMADI S B, JALILI R. On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards[J]. ACM Transactions on Embedded Computing Systems, 2015, 14(3): 1-25.
- [11] LIU Z, AZARDEKRAKSH R, KIM H, et al. Efficient software implementation of ring-LWE encryption on IoT processors[J]. IEEE Transactions on Computers, 2020, 69(10): 1424-1433.
- [12] SEO H, KWON H, KWON Y, et al. Fast number theoretic transform for ring-LWE on 8-bit AVR embedded processor[J]. Sensors, 2020, 20(7): 2039.
- [13] BUCHMANN J, GÖPFERT F, GÜNEYSU T, et al. High-performance and lightweight lattice-based public-key encryption[C]//Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. 2016: 2-9.
- [14] AYSU A, ORSHANSKY M, TIWARI M. Binary Ring-LWE hardware with power side-channel countermeasures[C]//Proceedings of 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE). 2018: 1253-1258.
- [15] EBRAHIMI S, BAYAT-SARMADI S, MOSANAEI-BOORANI H. Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT[J]. IEEE Internet of Things Journal, 2019, 6(3): 5500-5507.
- [16] EBRAHIMI S, BAYAT-SARMADI S. Lightweight and DPA-resistant post-quantum cryptoprocessor based on binary ring-LWE[C]//Proceedings of 2020 20th International Symposium on Computer Architecture and Digital Systems (CADSD). 2020: 1-6.
- [17] EBRAHIMI S, BAYAT-SARMADI S. Lightweight and fault-resilient implementations of binary ring-LWE for IoT devices[J]. IEEE Internet of Things Journal, 2020, 7(8): 6970-6978.
- [18] XIE J F, HE P Z, WEN W J. Efficient implementation of finite field arithmetic for binary ring-LWE post-quantum cryptography through a novel lookup-table-like method[C]//Proceedings of 2021 58th ACM/IEEE Design Automation Conference. 2021: 1279-1284.
- [19] HE P Z, GUIN U, XIE J F. Novel low-complexity polynomial multiplication over hybrid fields for efficient implementation of binary ring-LWE post-quantum cryptography[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11(2): 383-394.
- [20] 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.
- [21] BUCHMANN J, GÖPFERT F, PLAYER R, et al. On the hardness of LWE with binary error: Revisiting the hybrid lattice-reduction and meet-in-the-middle attack[C]//International Conference on Cryptology in Africa. 2016: 24-43.
- [22] PARK A, HAN D G. Chosen ciphertext simple power analysis on software 8-bit implementation of ring-LWE encryption[C]//Proceedings of 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST). 2016: 1-6.
- [23] KOCHER P, JAFFE J, JUN B, et al. Introduction to differential power analysis[J]. Journal of Cryptographic Engineering, 2011, 1(1): 5-27.

[作者简介]



高艺恬(1998-),女,江苏南京人,东南大学硕士生,主要研究方向为后量子密码、物联网安全。



陈立全(1976-),男,广西玉林人,东南大学教授、博士生导师,主要研究方向为物联网安全、密码协议等。



屠天扬(1997-),女,浙江嘉兴人,东南大学硕士生,主要研究方向为后量子密码、物联网安全。



高原(1994-),女,山东烟台人,东南大学博士生,主要研究方向为云数据去重、物联网数据安全。



陈芊叶(1997-),女,江苏扬州人,东南大学硕士生,主要研究方向为物联网安全、量子密钥分发。