# 基于格陷门的高效密钥封装算法

谭高升[1,2], 张 锐[1,2], 姜子铭[1,2], 孙 硕[1,2]

[1]中国科学院信息工程研究所 信息安全国家重点实验室 北京 中国 100093
[2]中国科学院大学 网络空间安全学院 北京 中国 100049

**摘要** 量子计算机的深入研究已经威胁到基于离散对数和大整数分解问题的传统公钥密码, 美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)于 2017 年开始了后量子密码算法征集, 希望从全球提交的算法中评选出可以代替传统公钥密码的后量子公钥密码标准。在征集的后量子密码算法中, 基于格的密码算法占比最多, 基于格的密码算法具有抵抗量子算法攻击、困难问题存在“最坏情形”到“平均情形”的安全归约、计算简单等优势, 是后量子密码算法中最具应用前景的密码算法。目前为止, 提交的基于格的密钥封装算法均需要去随机化、误差采样等操作。去随机化即将底层概率性加密算法, 通过引入随机喻言机模型(Random Oracle Model, ROM), 将加密算法转化为确定性算法, 以实现量子随机喻言机模型下的安全归约。误差采样指模空间上的离散高斯采样, 在基于格的公钥加密中, 通常需要特殊的算法设计, 以满足加密算法性能与安全性需求。去随机化和误差采样操作既降低了算法运行效率, 又增加了遭受侧信道攻击的风险。本文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。首先, 本文提出了针对密钥封装算法设计场景的格上单向陷门优化技术, 显著减小了格陷门的长度; 其次, 基于优化的格上陷门单向函数, 构造了高效的量子随机喻言机模型(Quantum Random Oracle Model, QROM)下选择密文攻击不可区分安全(Indistinguishability against Chosen Ciphertext, IND-CCA)的密钥封装方案; 最后, 对密钥封装方案进行了攻击分析和实用参数设置分析, 并对方案进行了软件实现和性能分析。

**关键词** 格; 单向陷门函数; 密钥封装方案
**中图法分类号** TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2021.11.07

# The Efficient Key Encapsulation Algorithm from the Lattice Trapdoor

TAN Gaosheng[1,2], ZHANG Rui[1,2], JIANG Ziming[1,2], SUN Shuo[1,2]

[1] State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering (IIE), Chinese Academy of Sciences (CAS), Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences (UCAS), Beijing 100049, China

**Abstract** The in-depth study of quantum computers has threatened the traditional public key cryptography based on the discrete logarithm or large integer factor problem. National Institute of Standards and Technology (NIST) has announced a competition for the post-quantum cryptography from 2017, which hopes to select the post-quantum public key cryptography standard which can replace the traditional public key cryptography from the algorithms submitted worldwide. The lattice-based cryptography algorithms account for the largest proportion among the collected post-quantum cryptography algorithms. Lattice-based cryptography is one of the most promising post-quantum cryptography algorithms because of its advantages of resisting attacks from quantum algorithms, security reduction from “worst-case” to “average-case” for difficult problems, and simplicity of calculation. However, up to now, these lattice-based key encapsulation algorithms need de-randomization and error sampling. De-randomization refers to the conversion of the underlying probabilistic encryption algorithm into a deterministic algorithm by introducing the random oracle model, so as to realize the security reduction under the quantum random oracle model. Error sampling refers to discrete Gaussian sampling in modular space. In the lattice-based public key encryption, special algorithm design is usually required to meet the performance and security requirements of encryption algorithm. These two operations not only reduce the efficiency of the algorithm, but also increase the risk of the side channel attack. In this paper, we design and implement an efficient key encapsulation algorithm, which avoids the de-randomization and error sampling, from the lattice-based one-way trapdoor function. Then, we improve the efficiency of our key encapsulation mechanism (KEM) from the algorithm design. Concretely, we first optimize the lattice-based one-way trapdoor function for designing the KEM. Then, we construct the efficient KEM, which satisfies the

**通讯作者:** 张锐, 博士, 研究员, Email:r-zhang@iie.ac.cn。

本课题得到国家自然科学基金(No. 61632020, No. 61472416, No. 61772520, No. 61802392, No. 61972094)和浙江省重点研究项目(No. 2017C01062)资助。
收稿日期: 2019-11-07; 修改日期: 2020-04-15; 定稿日期: 2021-10-19

indistinguishability security against chosen ciphertext attack (IND-CCA) in the quantum random oracle model (QROM), based on the optimizing one-way trapdoor function. Finally, we analyze the security of the KEM by attack methods, propose the practical parameters for the scheme, give a reference implementation and analyze the performance of our scheme.

**Key words** lattice; one-way trapdoor function; key encapsulation mechanism

# 1 引言

## 1.1 研究背景

密钥封装机制(Key Encapsulation Mechanism, KEM)是密码系统中重要的密码原语之一, 结合数据封装机制(Data Encapsulation Mechanism, DEM), 可以构造实用的公钥加密方案, 这种混合加密方式已经被国际标准化组织采纳为公钥加密标准[1], 广泛应用于互联网等通信系统。密钥封装方案还可以用来构造密钥交换协议、认证密钥交换协议[2-3], 为网络安全通信提供基础保障。传统密钥封装方案通常基于大整数分解问题或离散对数问题构造, 随着量子计算机研究的深入, 传统密钥封装方案将面临被彻底攻破的风险[4], 因此, 研究抵抗量子计算攻击的密钥封装方案已经成为密码学界关心的热点。

美国国家标准与技术研究院(NIST)于 2017 年开始向全球征集后量子公钥密码算法标准, 中国密码学会(Chinese Association for Cryptologic Research, CACR)于 2018 年末同样开展了密码算法设计竞赛活动, 并鼓励提供后量子密码算法。其中, 从提交算法的数量分析, 基于格的密钥封装算法是后量子密钥封装算法的主流算法。基于格的密钥封装算法具有抵抗已知量子攻击[4-5]、计算简单[5-8]、底层困难问题存在“最坏情形(Worst-Case)”到“平均情形(Average-Case)”的安全归约[6, 9]等优势, 是后量子密钥封装算法中最具应用前景的基础算法。NIST 和 CACR 均要求从算法设计、可证明安全分析、参数选取、攻击分析和高速实现等方面对提交算法进行全面设计与分析, 这是后量子算法设计的标准规范。据此设计完成的密钥封装算法为后量子算法标准化提供了重要的算法支持。

密钥封装方案作为基础的密码算法之一, 支持计算资源受限设备之间的安全通信同样重要。综合考虑后量子通信及计算资源受限设备等新型网络机密通信的需求, 本文的研究目标定位设计并实现高效的基于格的密钥封装算法。

## 1.2 相关工作

在 IND-CCA 安全的密钥封装算法构造中, 存在两种构造模型, 分别是标准模型和随机喻言机模型。标准模型下的方案可以避免随机喻言机实例化带来的安全隐患[10-11], 但通常效率较低, 无法满足实用性要求; 随机喻言机模型下的方案则结构简单, 算法效率高, 更容易满足实用性要求。

Micciancio 与 Peikert、Zhang 等人分别利用 BCHK 变换[12]构造了基于格的 IND-CCA 安全的公钥加密(密钥封装)方案[13-14], 但方案效率较低, 在 LWE (Learning With Error)假设[5]下, 达到近似 128 比特经典安全性, 参考文献[14]中统计的两种方案的密文长度分别为 24.74KB 与 13.80KB, 不利于构造高效的 IND-CCA 安全的密钥封装方案。参考文献[15]利用有损陷门函数(Lossy Trapdoor Function)构造了标准模型下, 基于 LWE 假设的 IND-CCA 安全的公钥加密方案, 与文献[13]和[14]相比, 其方案密文长度更长, 算法效率更低, 更不利于构造高效的公钥加密方案。

为构造基于格的 IND-CCA 安全的高效密钥封装方案, NIST 后量子标准化竞赛的候选算法均采用量子随机喻言机模型下的构造方式。遗憾的是, 在基于基础公钥加密方案(低安全性公钥加密)构造 IND-CCA 安全的密钥封装算法时, NIST 提案都采用了非常相似的方式进行构造, 即利用量子随机喻言机模型下的 Fujisaki-Okamoto (FO)变换[16], 将不同假设下的 Lindner-Peikert (LP)加密方案[17]转化为 IND-CCA 安全的密钥封装方案。

Naehrig 等人[18]基于 LWE 假设构造密钥封装方案, 其基础公钥加密方案本质上是基于 LWE 的 LP 加密方案, 然后利用 Hofheinz 等人[19] 提出的量子随机喻言机模型下的 FO 变换, 将基础公钥加密方案转化为 IND-CCA 安全的密钥封装方案。基于 LWE 的密钥封装方案优势在于降低了因特殊环结构带来的安全风险, 因此安全性更高, 缺点在于公钥较大, 密文扩展因子(密文长度/明文长度)较大, 近似 128 比特经典安全性下, 密文长度为 15.40KB, 不利于方案的实际应用。

为避免 LWE 假设带来的密文扩展问题, NIST 后量子算法竞赛的大部分提案采用环结构进行方案构造。Poppelmann 等人基于 Ring-LWE (RLWE)假设[7]构造了满足 IND-CCA 安全性的密钥封装方案[20], 显著地解决了公钥长度、密文扩展因子较大的问题。Schwabe 等人对 LWE 和 RLWE 假设进行了折衷处理, 提出了基于 Module-LWE (MLWE) 假设[8]的密钥封装方案[21], 方案既保留了 RLWE 类方案公钥和密文扩展因子较小的优势, 同时降低了环代数结构带来

的安全风险。Lu 等人[22]结合纠错码, 构造了基于 RLWE 的密钥封装方案, 其方案可以使用非常小的模数($q$=251), 显著压缩了公钥和密文长度。D'Anvers 等人基于 RLWR (Ring Learning With Rounding)假设[23-24]构造了 IND-CCA 安全的密钥封装方案[25], 部分解决了加密算法误差采样的问题, 但并未彻底解决, 其密钥封装方案依然需要部分误差采样。Chen 与 Bernstein 等人分别提出了基于 NTRU 假设[26]的密钥封装方案[27-28]。Garcia-Morchon 等人[29]则基于 RLWE 假设利用 Reconciliation 机制直接构造了密钥交换协议, 但并未达到 CCA 的安全性。在环结构下, 达到近似 256 比特经典安全性, 大部分方案的公钥在 2KB 左右, 基本满足实用要求。

虽然这些基于格的密钥封装方案在算法安全性和效率上均达到了较优的水平, 但是, 这些方案仍然存在一定的不足。首先, 在构造 IND-CCA 安全的密钥封装方案时, 需要对基础加密方案进行去随机化操作, 即将其转化为确定性加密。去随机化操作既增加了计算开销, 又增加了安全性证明中安全归约的复杂度(去随机化的哈希函数需要作为量子随机喻言机处理)[19, 30]。其次, 加密和密钥封装算法均需要进行随机数和误差采样操作, 降低了算法效率且容易受到侧信道攻击。

显然, 如果基础公钥加密采用基于格的确定性公钥加密, 则加密算法不需要随机数采样和误差采样的操作, 这种基础加密方案更利于构造量子随机喻言机模型下, IND-CCA 安全的高效密钥封装方案。但是, 目前基于格的确定性公钥加密方案效率较低[31]。一方面, 如果基于 Gentry-Peikert-Vaikuntanathan (GPV)陷门[32]构造基础加密方案, 则方案的密钥生成算法耗时很长, 难以大规模应用。另一方面, 如果基于 Micciancio-Peikert (MP)陷门[13]构造基础方案, 则方案的公钥和密文较大, 同样无法满足应用需求。因此, 目前两种陷门均无法构造出高效的确定性公钥加密方案。

### 1.3 本文贡献

本文的主要贡献是基于优化的格上单向陷门函数, 构造了 IND-CCA 安全的高效密钥封装方案, 具体贡献如下:

(1) 针对密钥封装场景, 构造了高效的基于格的单向陷门函数, 从而构造了高效的确定性基础公钥加密方案。具体地, 当加密消息为比特或比特向量(多项式)时, 可以极大地压缩 MP 陷门, 从而显著地减小了基于 MP 陷门的确定性公钥加密的公钥、私钥和密文的长度。设 RLWE (RLWR)假设中的模数为 $q$, 则公钥、私钥和密文的长度比(压缩后长度/压缩前长度)分别为 $2/(\log q+1)$、$1/\log q$ 和 $3/(\log q+2)$, 当 $\log q$ 取较为常用的参数值 13 时, 公钥、私钥和密文的压缩率(1-长度比)分别为 86%、92% 和 80%。

(2) 基于优化的格上单向陷门函数和量子随机喻言机模型下的 FO 变换[30], 构造了 IND-CCA 安全的高效密钥封装方案。方案避免了去随机化、随机数生成、误差采样等操作, 提升了方案效率。

(3) 对方案进行攻击分析、参数设置分析以及软件实现。通过攻击分析, 在 256 比特经典安全性下, 密钥封装方案的公钥长度约为 2KB。在 Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz 平台下, 达到 256 比特经典安全性, 密钥封装算法的运行时间仅为 452 μs, 验证了密钥封装算法高效的预期。

### 1.4 技术原理

在基础公钥加密构造中, 本文首次使用了 RLWR (RLWE)假设的陷门作为解密私钥。困难点在于, 当前 RLWR 的陷门均不高效, 要么生成陷门的算法运行时间较长[32], 要么存储开销较大[13]。本文选择对参考文献[13]中的陷门进行优化。在 MP 陷门构造中, 结构向量 $\boldsymbol{g}=(1,2,\cdots,2^{\ell-1})^T$ 具有重要的作用, 其中 $\ell=\lceil\log q\rceil$。MP 陷门为多项式矩阵 $\boldsymbol{R}\in R^{\ell\times(m-\ell)}$, 满足对 $m$ 维多项式向量 $\boldsymbol{a}\in R_q^m$ (可以作为 $m$ 个 RLWR 实例的校验多项式), $[\boldsymbol{R}\quad \boldsymbol{I}_\ell]\boldsymbol{a}=\boldsymbol{g}$, 且 $\boldsymbol{R}$ 的二范数 $\|\boldsymbol{R}\|_2$ 在一定的范围内取值。设 RLWR 的秘密信息为 $s\leftarrow R_q$, 如果生成 $m$ 个 RLWR 实例 $(\boldsymbol{a},\boldsymbol{b}=\lfloor\boldsymbol{a}s\rceil_p)\in R_q^m\times R_p^m$ (符号具体定义参见第 2 章的符号定义), 将 RLWR 实例转化为 RLWE 实例的形式, 即计算 $\bar{\boldsymbol{b}}=\lfloor\frac{q}{p}\boldsymbol{b}\rceil=\boldsymbol{a}s+\bar{\boldsymbol{e}}$, 其中 $\|\bar{\boldsymbol{e}}\|_\infty\leqslant\frac{q}{2p}+\frac{1}{2}$, 进一步, 计算

$$\bar{\boldsymbol{b}'}=[\boldsymbol{R}\quad \boldsymbol{I}_\ell]\bar{\boldsymbol{b}}=\boldsymbol{g}s+[\boldsymbol{R}\quad \boldsymbol{I}_\ell]\bar{\boldsymbol{e}}$$

由于 $\boldsymbol{g}$ 特殊的结构形式, 当误差项 $\bar{\boldsymbol{e}'}=[\boldsymbol{R}\quad \boldsymbol{I}_\ell]\bar{\boldsymbol{e}}$ 的长度(二范数)"较小"时, 可以容易的利用最近平面算法[33]求出 $s$。但是, 如果直接利用 MP 陷门, 校验多项式向量 $\boldsymbol{a}$ 的维数至少为 $\log q$+1 维。由于 $\boldsymbol{a}$ 与公钥和密文直接相关, 当 $\log q$ 较大时, 导致方案的公钥和密文长度快速扩张, 无法满足实用要求。

值得注意的是, 密钥封装方案中, 基础加密方案的消息通常只取系数为二进制的多项式 $m\in R_2$, 并作为导出会话密钥的随机种子。我们发现, 此时的

$\boldsymbol{g}$ 向量只选取 $2^{\ell-1}$ 一项即可实现秘密信息的求解。基于这个观察, 可以对 MP 陷门进行显著压缩, 进一步, 实现了对校验多项式向量 $\boldsymbol{a}$ 的显著压缩。在第 4 章方案构造中, 可以看到 $\boldsymbol{R}$ 作为私钥只包含 1 个多项式, $\boldsymbol{a}$ 作为公钥只包含 2 个多项式元素, 极大地减小了基于 MP 陷门的基础公钥加密方案的存储开销(自然降低计算开销), 为构造基于格的 IND-CCA 安全的高效密钥封装方案奠定了基础。基于 RLWR 假设构造的基础加密方案满足确定性 OW-CPA 安全性, 因此, 结合量子随机喻言机模型下的 FO 变换[30], 可以构造不需要去随机化、随机数采样和误差采样的 IND-CCA 安全的密钥封装方案, 使得方案效率更高、安全归约更简单。

由于基于 RLWR 假设的密钥封装方案对模数 $q$ 要求更高, 因此, 在 RLWR 假设的模数 $q$ 下, 很难使用 Number Theorem Transform (NTT)计算模多项式乘法运算, 使得方案实现效率较低。本文为使用 NTT 进行快速计算, 首先在足够大的素数下使用 NTT 计算整数域上的多项式乘法, 计算结束后再通过模 $q$ 运算将多项式的模数转化到 RLWR 模数下。这种实现方式显著提高了算法运行效率, 同时扩展了基于格的密码算法参数选取空间, 保证了算法的运行效率。

## 1.5 对比分析

与NIST征集的基于格的后量子密钥封装算法相比, 本文的密钥封装算法具有如下特点。

第一, 方案的设计具有创新性。由于基于格的单向陷门函数要么陷门生成算法较为耗时, 要么需要较大存储空间, 因此, 所有提案均未直接使用单向陷门函数作为基础原语, 构造 IND-CCA 安全的密钥封装方案或公钥加密方案。本方案首次对基于格的单向陷门函数进行了压缩优化, 并利用优化的单向陷门函数构造了高效的密钥封装方案, 丰富了基于格的密钥封装方案的构造方式, 从而可以满足更多应用场景的需求, 例如, 缺少计算资源进行误差分布采样的设备。

第二, 本方案的密钥封装(加密算法)算法不需要去随机化、误差采样、随机数采样等操作, 降低了对计算资源的要求, 减小了遭受侧信道攻击的风险。理论上, 更利于在资源受限设备上应用部署, 例如多种传感器网络、物联网等。

第三, 虽然方案的模数与多项式的次数不满足直接使用 NTT 的一般性条件要求($q \equiv 1 (\mathrm{mod}\, 2n)$ 且 $q$ 为素数, $n$ 为 2 的幂次, 模多项式为 $X^n+1$), 但我们先在大模数下利用 NTT 计算多项式乘法, 得到多项式在整数域上的乘积, 再通过模运算将其转化为 $\mathbb{Z}_q$ 上的多项式, 依然实现了使用 NTT 计算多项式乘法[34]。我们发现, 计算多项式乘法时大模数 NTT 与小模数 NTT 的实现效率十分接近。因此, 本文的实现方法可以扩展 RLWE 或 RLWR 假设[7, 23-24, 35]参数选取空间。

本文提出的算法不足之处在于密钥封装算法传递的随机种子空间受限, 只适用于分量为比特的向量(多项式)。其次, 由于 RLWR 假设的误差分布为 $[-\frac{q}{2p}, \frac{q}{2p}]$ 上的均匀分布, 为保证方案的正确性, $p$ 的取值具有下界要求, 为保证RLWR的安全性, $q$ 与 $p$ 的比值同样具有下界要求, 导致模数 $q$ 比同等安全强度下 RLWE 假设模数大, 从而算法的公钥和密文长度较长。图 1 与图 2 分别为近似(AES) 128 比特与(AES) 256 比特(NTRU 算法均为 128 比特, NTRUPrime 算法最高为 192 比特)经典安全性下, 本

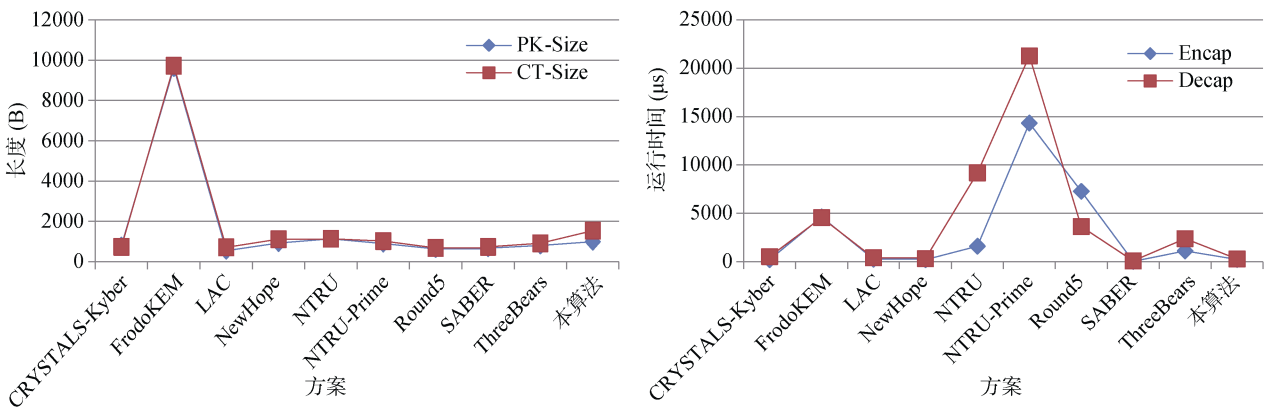


**图 1 128 比特经典安全性下本算法与 NIST 二轮密钥封装(交换)算法性能对比**

**Figure 1 The comparison of the performance on NIST round 2 candidates and ours in 128-Bit classical security**

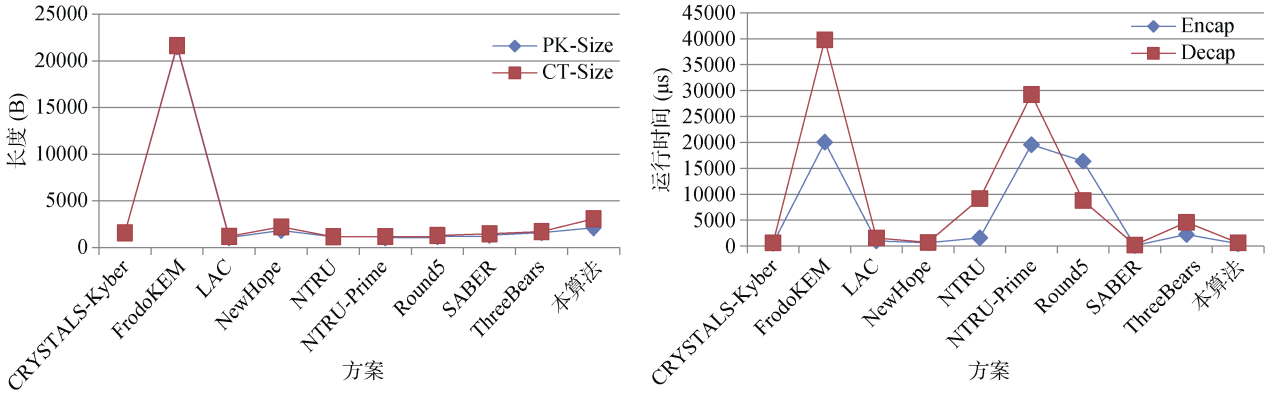


**图 2　256 比特经典安全性下本算法与 NIST 二轮密钥封装(交换)算法性能对比(256 比特)**

**Figure 2　The comparison of the performance on NIST round 2 candidates and ours in 256-Bit classical security**

文密钥封装算法与 NIST 二轮候选算法在公钥、密文长度和封装算法、解封装算法运行时间的对比图。

如图 1 与图 2 中公钥长度与密文长度对比图所示，除 FrodoKME 外，其他 NIST 算法的密文长度和公钥长度较为接近。在 128 比特经典安全性下，公钥长度与密文长度均约为 1KB，在 256 比特经典安全性下，公钥长度和密文长度均约为 2KB，基本满足实用性要求。而 FrodoKEM 公钥和密文长度较长的原因是，此算法基于 LWE 假设，而其他算法基于环结构下的基本假设，在存储和传输开销方面，基于环结构的基本假设更具优势。由于本文算法的模数 $q$ 取值较大，相对而言，本文算法的公钥长度与密文长度相对较大。其中，相应安全强度下，公钥长度约为 1KB 或 2KB，与 NIST 征集算法公钥长度近似，而密文长度约为 2KB 或 3KB。虽然在使用密文压缩算法下，密文长度会减小，但出于方案安全性考虑，本文未对密文进行压缩。即使如此，在当前终端设备存储能力和网络速度不断提高的环境下，方案依然满足实用性要求，模数较大是本算法获得算法效率提升的代价。

如图 1 与图 2 中封装算法与解封装算法运行时间对比图所示，本文算法运行时间优势较为突出。本文在统一的实验环境(Intel (R) Core (TM) i5-7200U CPU @ 2.50GHz, 8GB RAM, Ubuntu 16.04 LTS, gcc 5.4.0, OpenSSL 1.1.1c)下，测量了 NIST 二轮候选算法中基于格的密钥封装算法，并选取“参考实现”进行测量。从图中可以看出，无论 128 比特经典安全性还是 256 经典比特安全性，提案算法的运行时间均为数百微秒，且与运行平台无关。而对比的 NIST 方案有些则需要特定平台优化。我们相信，针对特定平台，本文方案效率还有提升空间。

## 2　预备知识

**符号定义**:

小写黑体字母表示向量，例如 $\boldsymbol{a}$，大写黑体字母表示矩阵，例如 $\boldsymbol{A}$；

设 $f$ 是 $\mathbb{Z}[X]$ 中的 $n$ 次多项式，$q$ 为正整数，记模 $f$ 生成的理想的剩余类多项式环为 $R=\mathbb{Z}[X]/(f)$，进一步 $R_q=\mathbb{Z}_q[X]/(f)$；

如果 $D$ 是集合，则 $x\leftarrow D$ 表示从 $D$ 中均匀随机选取元素 $x$，如果 $D$ 是分布，则 $x\leftarrow D$ 表示按照 $D$ 分布选取元素 $x$；

令 $a=\sum_{i=0}^{n-1}a_iX^i\leftarrow R$，则 $a$ 的无穷范数与二范数分别表示系数向量的无穷范数与二范数，即 $\|a\|_\infty=\max_i\{|a_i|\}$ 、$\|a\|_2=\sqrt{\sum_i a_i^2}$ ；

设 $x$ 为实数，$\lfloor x\rceil$ 表示 $x$ 的近似取整，$\lceil x\rceil$ 表示 $x$ 的上取整;

设正整数 $p<q$，任意 $x\in\mathbb{Z}_q$，$\lfloor x\rceil_p=\lfloor\frac{p}{q}x\rceil$;

$\mathrm{negl}(k)$ 表示关于 $k$ 的可忽略函数，即对任意正多项式 $p(x)$，存在 $k_0>0$，对 $\forall\ k>k_0$，均有 $\mathrm{negl}(k)<\frac{1}{p(k)}$。

**定义 1 (D-RLWE 假设)** 设 $\chi$ 表示环 $R$ 上的误差分布，给定 $s\leftarrow R_q$ (或 $s\leftarrow\chi$)，构造分布

$$A_{s,\chi,q}=\{(a,b)\in R_q\times R_q\mid a\leftarrow R_q,e\leftarrow\chi,b=as+e\in R_q\}$$

D-RLWE 假设是指给定多项式个采样，对任意多项式时间区分算法，区分采样来自分布 $A_{s,\chi,q}$ 还是

$R_q \times R_q$ 上的均分分布是困难的, 即区分成功的概率是可忽略的。当 $s \leftarrow \chi$ 时, 称此为 D-RLWE 假设的 Normal Form 形式[17], 与标准假设下的 D-RLWE 假设具有相似的安全性, 由于后文均采用此种形式下的 D-RLWE 假设, , 本文统称为 D-RLWE 假设, 多项式 $s$ 的次数称为 RLWE 假设的维数。

**定义 2 (S-RLWR 假设)** 设正整数 $p < q$, 给定 $s \leftarrow R_q$, 构造分布 $A_{s,p,q}$ 如下

$$A_{s,p,q} = \{(a,b) \in R_q \times R_p \mid a \leftarrow R_q, b = \lfloor as \rceil_p \in R_p\}$$

类似地, S-RLWR 假设指给定多项式个取自分布 $A_{s,p,q}$ 的采样, 对任意多项式时间算法, 求出 $s$ 的概率是可忽略的。特别地, 对于 S-RLWR 假设, 当 $s \leftarrow R_2$ 时, 假设同样成立[24]。

**定义 3 ($\boldsymbol{g}$-陷门)** 设 $m$ 和 $q$ 为正整数, 令 $\ell = \lceil \log q \rceil$, 且满足 $m > \ell$, 记 $\boldsymbol{g} = (1,2,\cdots,2^{\ell-1})^T$, 设 $h \in R_q$ 是可逆元素, 取 $\boldsymbol{a} \in R_q^m$, 称 $\boldsymbol{R} \in R^{\ell \times (m-\ell)}$ 是 $\boldsymbol{a}$ 以 $h$ 为标识的 $\boldsymbol{g}$-陷门, 如果 $\boldsymbol{R}$ 满足

$$\begin{bmatrix} \boldsymbol{R} & \boldsymbol{I}_\ell \end{bmatrix} \boldsymbol{a} = \boldsymbol{g}h \in R_q^\ell$$

陷门 $\boldsymbol{R}$ 的“质量”在文献[13]中由 $\boldsymbol{R}$ 的最大奇异值衡量, 本文将其放宽为 $\|\boldsymbol{R}\|_2$, 且 $\|\boldsymbol{R}\|_2$ 越小表示 $\boldsymbol{R}$ 质量越高, 后文取 $h = 1$。

**定义 4 (密钥封装方案)** 密钥封装方案由三个多项式时间算法构成, 记作 KEM=(KG, Encap, Decap), 设安全参数为 $\lambda$、密文空间为 $\mathcal{C}$、会话密钥空间为 $\mathcal{K}$, 三个算法定义为: $(pk,sk) \leftarrow \mathrm{KG}(1^\lambda)$, 概率性密钥生成算法, 输入安全参数 $\lambda$, 输出一对公钥和私钥 $(pk,sk)$; $(c,k) \leftarrow \mathrm{Encap}(pk)$, 概率性封装算法, 输入公钥 $pk$, 输出密文 $c \in \mathcal{C}$ 和会话密钥 $k \in \mathcal{K}$; $k' \leftarrow \mathrm{Decap}(sk,c)$, 确定性解封装算法, 输入私钥 $sk$ 和密文 $c$, 输出会话密钥 $k'$, 这里 $k'$ 可以为 $\perp$, 即允许解封装失败。

**定义 5 (KEM 方案的 IND-CCA 安全性)** 设安全参数为 $\lambda$, 称 KEM 方案满足 IND-CCA 安全性, 如果对任意多项式时间敌手 $\mathcal{A}$, 如下定义的攻击优势满足

$$Adv^{ind-cca}_{\mathcal{A},\mathrm{KEM}}(\lambda) = \left| \Pr \begin{bmatrix} (pk,sk) \leftarrow \mathrm{KG}(1^\lambda); \\ (c^*,k_0) \leftarrow \mathrm{Encap}(pk); \\ k_1 \leftarrow \mathcal{K}; b \leftarrow \{0,1\}; \\ b' \leftarrow \mathcal{A}^{\mathcal{O}_{Decap}(\cdot)}(pk,c^*,k_b): \\ b' = b \end{bmatrix} - \frac{1}{2} \right| \leqslant \mathrm{negl}(\lambda)$$

$\mathcal{O}_{Decap}(\cdot)$ 表示解封装喻言机, 即输入密文, 返回会话密钥; 注意, 敌手不能用 $c^*$ 查询解封装喻言机。

公钥加密方案同样由三个多项式时间算法构成, 记 PKE=(KG, Enc, Dec), 设明文、密文空间分别为 $\mathcal{M}$ 与 $\mathcal{C}$, 则有 $(pk,sk) \leftarrow \mathrm{KG}(1^\lambda)$, 概率性密钥生成算法, 输入安全参数 $\lambda$, 输出一对公钥、私钥 $(pk,sk)$; $c \leftarrow \mathrm{Enc}(pk,m)$, 概率性或确定性加密算法, 输入公钥 $pk$ 与消息 $m$, 输出密文 $c$; $m' \leftarrow \mathrm{Dec}(sk,c)$, 确定性解密算法, 输入私钥 $sk$ 和密文 $c$, 输出消息 $m'$。定义 PKE 方案解密失败的概率为

$$\underset{(pk,sk) \leftarrow \mathrm{KG}(1^\lambda)}{E} (\max_{m \in \mathcal{M}} \{\Pr[\mathrm{Dec}(sk, \mathrm{Enc}(pk,m)) \neq m]\})$$

$E$ 表示求期望, 即此处定义了平均意义下, 解密失败的概率。在完美解密(Perfect Decryption)意义下, 方案解密失败的概率定义为对任意 $(pk,sk)$, 失败概率定义为 $\max_{m \in \mathcal{M}} \{\Pr[\mathrm{Dec}(sk, \mathrm{Enc}(pk,m)) \neq m]\}$。此处使用平均意义下的定义是因为, 本文构造的方案无法实现完美解密, 而在我们的安全性定义下, 使用平均意义下的定义即可。进一步, 参考文献[19, 30]亦采用平均意义下的定义, 为正确利用其中的相关结论, 本方案也必须采用平均意义下的定义。PKE 满足选择明文攻击(Chosen Plaintext Attack, CPA)下单向安全性, 如果对任意概率多项式时间敌手 $\mathcal{A}$, 如下定义的攻击优势满足

$$Adv^{ow-cpa}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \Pr \begin{bmatrix} (pk,sk) \leftarrow \mathrm{KG}(1^\lambda); \\ m \leftarrow \mathcal{M}; \\ c \leftarrow \mathrm{Enc}(pk,m); \\ m' \leftarrow \mathcal{A}(pk,c): m' = m \end{bmatrix} \leqslant \mathrm{negl}(\lambda)$$

进一步, 可以定义关于 PKE 的选择密文攻击下不可区分安全性(IND-CCA), 即对任意概率多项式时间敌手 $\mathcal{A}$, 如下定义的攻击优势满足

$$Adv^{ind-cca}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \left| \Pr \begin{bmatrix} (pk,sk) \leftarrow \mathrm{KG}(1^\lambda); \\ (m_0,m_1) \leftarrow \mathcal{A}^{\mathcal{O}_{Dec}(\cdot)}(\lambda, pk); \\ |m_0| = |m_1|, b \leftarrow \{0,1\}; \\ c^* \leftarrow \mathrm{Enc}(pk,m_b); \\ b' \leftarrow \mathcal{A}^{\mathcal{O}^*_{Dec}(\cdot)}(\lambda, pk, c^*): b' = b \end{bmatrix} \right.$$

$$-\frac{1}{2}|\leqslant \mathrm{negl}(\lambda)$$

$\mathcal{O}_{Dec}(\cdot)$ 与 $\mathcal{O}^{*}_{Dec}(\cdot)$ 均表示解密随机喻言机, 即输入密文, 返回解密消息, 注意, $\mathcal{O}^{*}_{Dec}(\cdot)$ 中, 敌手 $\mathcal{A}$ 不能查询挑战密文 $c^{*}$。

## 3 RLWE 陷门优化

本节主要介绍如何利用 MP 陷门求解 RLWE 或 RLWR 问题, 并且, 针对特殊的秘密信息 $s$, 实现对 MP 陷门的优化。RLWE 与 RLWR 假设具有非常相似的结构形式, 唯一的区别在于两种假设下误差分布不同, 在 MP 陷门求解 RLWE 或 RLWR 问题中, 只有误差的长度对求解过程有影响, 而误差分布的形式对求解过程没有影响, 因此, 本节将以 RLWE 假设为目标, 分析 RLWE 问题的求解和陷门优化, 对于 RLWR 假设, 具有完全相同的求解和优化方法。

在 RLWE 问题求解中, $\boldsymbol{g}$-陷门中的向量 $\boldsymbol{g}$ 起到至关重要的作用, 给定 $s\leftarrow R_q$, $\boldsymbol{e}\leftarrow\chi^{\ell}$, 计算 $\boldsymbol{b}=\boldsymbol{g}s+\boldsymbol{e}$, 由于 $\boldsymbol{g}$ 具有特殊的结构, 当误差向量 $\boldsymbol{e}$ 的无穷范数较小时, 根据 $\boldsymbol{b}$ 可以容易的求得 $s$。特别地, 当 $q=2^{\ell}$ 即等于 2 的幂次且 $\|\boldsymbol{e}\|_{\infty}<\frac{q}{4}$ 时, 对于 $s$ 的每一个系数 $s_i$, 可以逐比特对 $s_i$ 进行求解。令 $s_i=\sum_{j=0}^{\ell-1}s_{ij}2^{j}$, $\boldsymbol{b}_{k,i}$ 表示 $\boldsymbol{b}$ 的第 $k$ 个分量多项式中 $x^{i}$ 项的系数($0\leqslant i\leqslant n-1$), $\boldsymbol{e}_{k,i}$ 具有相同的定义, 则有

$$\boldsymbol{b}_{k,i}=2^{k}s_i+\boldsymbol{e}_{k,i}=\sum_{j=0}^{\ell-k-1}2^{k+j}s_{ij}+\boldsymbol{e}_{k,i}(\mathrm{mod}\,q)$$

首先取 $k=\ell-1$, 则有 $\boldsymbol{b}_{\ell-1,i}=2^{\ell-1}s_{i0}+\boldsymbol{e}_{\ell-1,i}$, 因为 $\|\boldsymbol{e}\|_{\infty}<\frac{q}{4}$, 所以, 如果 $|\boldsymbol{b}_{\ell-1,i}|<\frac{q}{4}$, 输出 $s_{i0}=0$; 如果 $|\boldsymbol{b}_{\ell-1,i}|\geq\frac{q}{4}$, 输出 $s_{i0}$=1。计算 $\boldsymbol{b}'_{\ell-2,i}=\boldsymbol{b}_{\ell-2,i}-2^{\ell-2}s_{i0}=2^{\ell-1}s_{i1}+\boldsymbol{e}_{\ell-2,i}(\mathrm{mod}\,q)$, 利用相同的判定条件求得 $s_{i1}$, 可用相同的方法求解 $s_i$ 的其他比特。注意, 逐比特求解的方式只适合模数 $q=2^{\ell}$ 的形式, 对于非 2 的幂次形式的模数, 则需要使用最近平面算法[33]。对于 RLWE 问题, 需要利用 $\boldsymbol{g}$-陷门将其转化为利于求解的特殊形式, 即对于 $\boldsymbol{b}=\boldsymbol{a}s+\boldsymbol{e}\in R_q^{m}$, 假设 $\boldsymbol{R}\in R^{\ell\times(m-\ell)}$ 是 $\boldsymbol{a}$ 的 $\boldsymbol{g}$-陷门, 则计算

$$\boldsymbol{b}'=\begin{bmatrix}\boldsymbol{R} & \boldsymbol{I}_{\ell}\end{bmatrix}\boldsymbol{b}=\boldsymbol{g}s+\begin{bmatrix}\boldsymbol{R} & \boldsymbol{I}_{\ell}\end{bmatrix}\boldsymbol{e}=\boldsymbol{g}s+\boldsymbol{e}'$$

根据最近平面算法, 需要 $\|\boldsymbol{e}\|_2<\frac{q}{4d}$ ($q=2^{\ell}$)或 $\|\boldsymbol{e}\|_2<\frac{q}{2\sqrt{5d}}$ ($q\neq 2^{\ell}$), 其中 $d$ 是 $\begin{bmatrix}\boldsymbol{R} & \boldsymbol{I}_{\ell}\end{bmatrix}$ 的最大奇异值。当加密比特类消息(分量为比特的向量或系数为比特的多项式)时, 存在更加简单的陷门结构和更加简洁的求解方法。

为了构造 $\boldsymbol{g}$-陷门中的公开多项式向量 $\boldsymbol{a}$, 需要 $\boldsymbol{a}$ 满足一定的结构要求, 令 $\boldsymbol{a}=\begin{pmatrix}\boldsymbol{a}_1 & \boldsymbol{a}_2\end{pmatrix}^{T}$, 根据参考文献[13]中的构造方法得 $\boldsymbol{a}_2=\boldsymbol{g}-\boldsymbol{R}\boldsymbol{a}_1$。在 $\boldsymbol{a}_2$ 与 $R_q^{m-\ell}$ 上的均匀分布计算不可区分意义下, 可令 $\boldsymbol{a}_1=\begin{pmatrix}1 & a_1\end{pmatrix}^{T}$, 其中 $a_1\leftarrow R_q$, $\boldsymbol{R}$ 的行向量 $\boldsymbol{r}_i=\begin{pmatrix}r_{i1} & r_{i2}\end{pmatrix}\leftarrow\chi^{2}$。显然, $\boldsymbol{a}$ 至少需要存储 $\ell+1$ 个多项式, 在实际应用中, $\ell$ 通常选取 12 或 13, 当 $\boldsymbol{a}$ 作为公钥时, 极大地增加了公钥、甚至密文的长度。有趣的是, 当秘密信息 $s\leftarrow R_2$ 时, 向量 $\boldsymbol{g}$ 实际上只需要 $2^{\ell-1}$ 一项即可以实现对秘密信息的求解。已知 $b=2^{\ell-1}s+e$, 其中 $s\leftarrow R_2$, $e\leftarrow\chi$ 且 $\|e\|_{\infty}<\frac{q}{4}$, 如果 $|b_i|<\frac{q}{4}$, 则输出 $s_i$=0; 否则, 输出 $s_i$=1。根据参考文献[13]中 $\boldsymbol{g}$-陷门构造方式, $\boldsymbol{g}$-陷门可取 $\boldsymbol{r}=(r_1,r_2)\leftarrow\chi^{2}$, $a_2=2^{\ell-1}-(r_1+r_2a_1)$, 其中 $a_1\leftarrow R_q$。令 $\boldsymbol{a}=(1,a_1,a_2)^{T}$, 已知 $\boldsymbol{b}=\boldsymbol{a}s+\boldsymbol{e}\in R_q^{3}$, 则有

$$\begin{aligned}b'&=\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}\boldsymbol{b}=2^{\ell-1}s+\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}\boldsymbol{e}\\&\triangleq 2^{\ell-1}s+e'\end{aligned}$$

因为 $s\in R_2$, 无论 $q$ 是否为 2 的幂次形式, 只要满足 $\|e'\|_{\infty}<\frac{q}{4}$, 即可通过判断 $b'$ 系数靠近 0 还是 $\frac{q}{2}$ 恢复 $s$ 的每一个系数。针对系数取自 {0,1} 空间的秘密信息 $s$, RLWE (RLWR)问题的 $\boldsymbol{g}$-陷门与公开矩阵 $\boldsymbol{a}$ 均有显著的压缩, 如果将 $\boldsymbol{g}$-陷门作为私钥、$\boldsymbol{a}$ 作为公钥、$\boldsymbol{b}$ 作为密文, 则私钥、公钥和密文长度比(压缩后/压缩前)分别为 $1/\ell$、$2/(\ell+1)$ 与 $3/(\ell+2)$, 当 $\ell=13$ 时, 压缩率(1-长度比)分别为 92%、86%与 80%, 可以用来构造高效的加密方案等。

## 4 方案构造

本节基于 RLWR 假设, 首先构造满足 OW-CPA 安全性的公钥加密方案, 再利用 QROM 模型下的 FO

变换, 将 OW-CPA 的公钥加密方案转化为 IND-CCA 安全的密钥封装方案。在构造 OW-CPA 公钥加密方案时, 利用优化的 $\boldsymbol{g}$-陷门作为解密私钥, 加密算法中将明文消息作为 RLWR 假设的秘密消息, 而密文则是 RLWR 假设的样本实例。方案的优势在于, 加密算法不需要误差采样和随机数采样, 提高了加密算法的运行效率, 避免了采样带来的侧信道攻击风险。构造的 IND-CCA 安全的密钥封装方案自然地继承了这种优势, 从而同样提升了密钥封装算法的效率, 降低了遭受侧信道攻击的风险。同时, 由于 OW-CPA 方案又是确定性公钥加密方案, 避免了 QROM 模型下使用 FO 变换时去随机化操作, 减少了安全性证明中量子随机喻言机的个数, 降低了安全归约损失。

### 4.1 OW-CPA 公钥加密

在构造 $\boldsymbol{g}$-陷门中特定结构的公开向量(矩阵) $\boldsymbol{a}$ 时, 存在两种构造方式, 分别得到与 $R_q^2$ ($\boldsymbol{a}$ 中的分量 1 不包含在内)上的均匀分布统计或计算不可区分的公开向量, 在实际应用中, 采用计算不可区分就已经足够。同时, 满足计算不可区分的参数使得方案公钥、私钥和密文长度更小, 从而提高了加密方案的性能。本文采用计算意义下不可区分性, 并且通过 RLWE 假设保证公开向量 $\boldsymbol{a}$ 的计算不可区分性。假设方案的安全参数为 $\lambda$, RLWE 假设中误差分布为 $R$ 上参数为 $\sigma$ 的高斯分布, 即误差多项式的每个系数服从 $\mathbb{Z}_q$ 上参数为 $\sigma$ 的离散高斯分布, 记作 $\chi$。RLWR 假设中, 令 $2p<q$ 即 $\frac{p}{q}<\frac{1}{2}$, $\bmod q$ 运算取值空间为 $(-\frac{q}{2},\frac{q}{2}]$, OW-CPA 基础加密方案的具体构造如图 3。

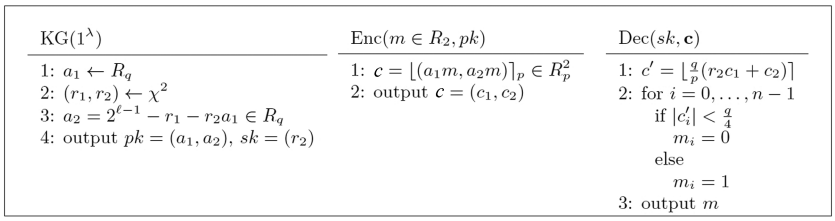


**图 3 OW-CPA 公钥加密方案**

**Figure 3 Public key encryption with OW-CPA security**

**定理 1 (公钥加密方案正确性)** 构造如图 3 所示的公钥加密方案, 记 $\boldsymbol{a}=\begin{pmatrix}1 & a_1 & a_2\end{pmatrix}^T \in R_q^3$, 对任意 $m \in R_2$, 令 $\boldsymbol{e}=\frac{p}{q}\boldsymbol{a}m-\lfloor \boldsymbol{a}m \rceil_p$, 注意, 由于 $\frac{p}{q}<\frac{1}{2}$ 且 $m \in R_2$, 所以 $\lfloor m \rceil_p = \lfloor \frac{p}{q} m \rceil = 0$, 即 $\lfloor \boldsymbol{a}m \rceil_p = \begin{pmatrix}0 & \boldsymbol{c}\end{pmatrix}^T$, 易得 $\|\boldsymbol{e}\|_\infty \leqslant \frac{1}{2}$, 如果公钥加密方案的参数满足

$$\|\frac{q}{p}\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}\boldsymbol{e}\|_\infty + 1 < \frac{q}{4}$$

则构造的公钥加密方案可正确解密。

**证明**: 根据解密算法可知

$$\begin{aligned} c' &= \lfloor \frac{q}{p}(r_2 c_1 + c_2) \rceil = \lfloor \frac{q}{p}\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}\begin{pmatrix}0 & \boldsymbol{c}\end{pmatrix}^T \rceil \\ &= \lfloor \frac{q}{p}\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}(\frac{p}{q}\boldsymbol{a}m - \boldsymbol{e}) \rceil \\ &= 2^{\ell-1}m - \frac{q}{p}\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}\boldsymbol{e} + \tilde{e} \\ &\triangleq 2^{\ell-1}m + e' \end{aligned}$$

根据近似取整得 $\|\tilde{e}\|_\infty \leqslant \frac{1}{2}$, 根据定理 1 的条件得

$$\|e'\|_\infty \leqslant \|\frac{q}{p}\begin{pmatrix}r_1 & r_2 & 1\end{pmatrix}\boldsymbol{e}\|_\infty + \|\tilde{e}\|_\infty < \frac{q}{4}$$

根据 $\boldsymbol{g}$-陷门恢复 RLWR 假设的秘密信息算法可知, 解密算法可正确输出明文信息。

**定理 2 (公钥加密方案安全性)** 构造如图 3 所示的公钥加密方案, 假设在方案的参数设置下, D-RLWE 假设与 S-RLWR 假设成立, 则构造的公钥加密方案满足 OW-CPA 安全性。特别地, 如果存在多项式时间敌手 $\mathcal{A}$ 攻破 OW-CPA 的公钥加密方案, 则可构造攻击 D-RLWE 假设的敌手 $\mathcal{B}$ 或攻击 S-RLWR 假设的敌手 $\mathcal{C}$, 敌手攻击优势之间满足

$$\begin{aligned} Adv^{ow-cpa}_{\mathcal{A},\mathrm{PKE}}(\lambda) &\leqslant Adv_{\mathcal{B},\text{D-RLWE}}(\lambda) \\ &+ Adv_{\mathcal{C},\text{S-RLWR}}(\lambda) \end{aligned}$$

敌手 $\mathcal{B}$ 与 $\mathcal{C}$ 的运行时间与 $\mathcal{A}$ 的运行时间近似。

**证明**: 我们采用“游戏”跳转的方式对定理 2 进行证明。记事件 $G_i^{\mathcal{A}} \Rightarrow m$ 表示在 Game $i$ 中敌手 $\mathcal{A}$ 返

回挑战密文中加密的消息 $m$。

Game 1: 在 Game 1 中, 利用公钥加密方案中的密钥生成算法生成公钥与私钥, 挑战者将公钥 $pk$ 发送给 $\mathcal{A}$。挑战者均匀随机选取明文 $m^* \in R_2$, 生成挑战密文 $\boldsymbol{c}^*$ 发送给 $\mathcal{A}$, 最终 $\mathcal{A}$ 返回对挑战密文加密消息的猜测值, 根据 Game 1 的定义得 $Adv^{ow-cpa}_{\mathcal{A},\mathrm{PKE}}(\lambda)=\Pr[G_1^{\mathcal{A}} \Rightarrow m^*]$。

Game 2: Game 2 与 Game 1 几乎相同, 只是 Game 2 不再利用密钥生成算法生成公钥, 而是从 $R_q^2$ 中均匀随机选取公钥, 则 Game 2 与 Game 1 中 $\mathcal{A}$ 返回 $m^*$ 的概率是计算不可区分的。否则, 可以构造敌手 $\mathcal{B}$, 将 D-RLWE 的挑战 $(a,b)\in R_q^2$ 作为公钥, 如果 $b$ 是 D-RLWE 实例, 则公钥的分布与 Game 1 相同; 如果 $b$ 的分布是均匀随机的, 则公钥的分布与 Game 2 相同。所以,

$$\begin{aligned}&|\Pr[G_1^{\mathcal{A}} \Rightarrow m^*]-\Pr[G_2^{\mathcal{A}} \Rightarrow m^*]|\\&\leqslant Adv_{\mathcal{B},\text{D-RLWE}}(\lambda)\end{aligned}$$

利用 Game 2 中的敌手 $\mathcal{A}$, 可以构造敌手 $\mathcal{C}$ 攻击 S-RLWR 假设。假设 $\mathcal{C}$ 至少可以获得两个 S-RLWR 实例 $(a_1,b_1)$ 和 $(a_2, b_2)$, 并将 $(a_1, a_2)$ 作为公钥发送给 $\mathcal{A}$, $\mathcal{C}$ 将 $(b_1,b_2)$ 作为挑战密文发送给 $\mathcal{A}$, 并返回 $\mathcal{A}$ 的明文猜测值 $m^*$, 易得 $\Pr[G_2^{\mathcal{A}} \Rightarrow m^*]\leqslant Adv_{\mathcal{C},\text{S-RLWR}}(\lambda)$。综合以上分析得

$$\begin{aligned}&Adv^{ow-cpa}_{\mathcal{A},\mathrm{PKE}}(\lambda)=|\Pr[G_1^{\mathcal{A}} \Rightarrow m^*]-\Pr[G_2^{\mathcal{A}} \Rightarrow m^*]\\&+\Pr[G_2^{\mathcal{A}} \Rightarrow m^*]|\\&\leqslant Adv_{\mathcal{B},\text{D-RLWE}}(\lambda)+Adv_{\mathcal{C},\text{S-RLWR}}(\lambda)\end{aligned}$$

定理证毕。

本文构造的 OW-CPA 公钥加密方案非常适合构造 QROM 模型下, IND-CCA 安全的密钥封装方案。首先, 密钥封装方案的密文只用来传递导出会话密钥的随机种子, 通常为 256 比特或 512 比特的随机字符串, 满足高效 OW-CPA 加密方案对明文空间的要求。其次, 构造的 OW-CPA 方案加密算法既不需要随机数采样, 又不需要误差采样, 提高了加密算法效率的同时, 避免了去随机化操作。

## 4.2 IND-CCA 密钥封装方案

本节主要利用 QROM 模型下的 FO 变换和 OW-CPA 安全的公钥加密方案构造 IND-CCA 安全的密钥封装方案。本文使用目前 QROM 模型下最优的 FO 变换[30], 可在降低通信开销的同时减小归约损失。本文构造的 OW-CPA 公钥加密方案其明文多项式即为 RLWR 假设下的秘密信息(多项式)。在 RLWR 假设中, 维数越高, 安全性越高, 维数越低, 安全性则越低。在密钥封装算法中, 本文将导出会话密钥的随机种子按位映射成明文多项式的系数, 例如, 随机种子为比特向量 $(a_n,\cdots,a_0)$, 则明文多项式为 $\sum_{i=0}^{n}a_i x^i$。在实际方案中, 为节省随机比特, 随机种子的比特数通常小于 RLWR 的维数, 因此, 在实现中, 我们采用输出扩展函数(Extendable Output Function)对随机种子进行扩展, 补充缺失的高位系数。

设安全参数为 $\lambda$, 记 OW-CPA 的公钥加密方案为 $\mathrm{PKE}=(\mathrm{KG}',\mathrm{Enc}',\mathrm{Dec}')$, OW-CPA 公钥加密方案的明文空间为 $\mathcal{M}$, 密文空间为 $\mathcal{C}$, 密钥封装方案的会话密钥空间为 $\mathcal{K}$, 哈希函数 $H:\mathcal{M}\times\mathcal{C}\to\mathcal{K}$ 是会话密钥导出函数。图 4 显示了 QROM 模型下, 基于确定性 OW-CPA 安全的公钥加密方案构造的 IND-CCA 安全的密钥封装方案。

图 4 构造的密钥封装方案与参考文献[30]中的 KEM-V 变换有两点不同。第一点, 文献[30]通过直接哈希随机种子的方式导出会话密钥, 本文将随机种子与密文一起哈希导出会话密钥, 由于方案是确定性加密, 所以本文的哈希方式不会增加会话密钥的随机性, 两种导出方式没有本质区别。第二点, 当解密出现错误时, 文献[30]利用伪随机函数将密文导出为会话密钥, 本文则利用哈希函数 $H$ 将私钥中的随机串 $ss$ 与密文导出为会话密钥, 在安全性证明中 $H$ 作为量子随机喻言机。这两种改变本质上与 KEM-V 构造是相同的, 可以将 $ss$ 视为伪随机函数的密钥, 因此, 本文的两种改变不会对方案的安全性证明造成影响。

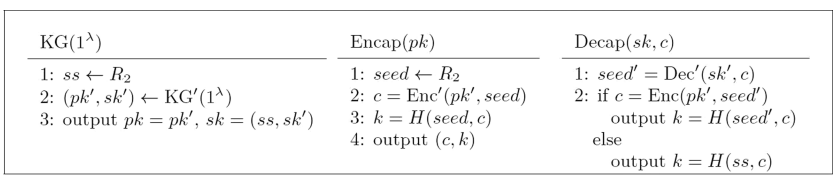


**图 4 IND-CCA 密钥封装方案**

**Figure 4 Key encapsulation mechanism with IND-CCA security**

根据密钥封装方案的构造方式, 易得密钥封装方案解封装失败的概率与 OW-CPA 安全的公钥加密方案解密失败的概率相同。密钥封装方案的安全性满足如下定理(与参考文献[30]的定理 6 类似)。

**定理 3 (密钥封装方案的安全性)** 假设安全参数为 $\lambda$, PKE 满足确定性(量子) OW-CPA 安全性, 且解密失败的概率为 $\delta$, 则图 4 构造的密钥封装方案在 QROM 模型下, 满足 IND-CCA 的安全性。具体地, 如果存在敌手 $\mathcal{A}$ 攻击密钥封装方案, 且 $\mathcal{A}$ 可以量子查询 $q_E$ 次加密喻言机、量子查询 $q_H$ 次随机喻言机 $H$ 和经典查询 $q_D$ 次解封装喻言机, 则可以构造敌手 $\mathcal{B}$ 攻击 OW-CPA 的公钥加密, 满足

$$Adv^{ind-cca}_{\mathcal{A},\mathrm{KEM}}(\lambda)\leqslant\frac{2q_H}{\sqrt{|\mathcal{M}|}}+4q_E\sqrt{\delta}$$

$$+2q_H\sqrt{Adv^{ow-cpa}_{\mathcal{B},\mathrm{PKE}}(\lambda)}$$

$\mathcal{B}$ 的运行时间与 $\mathcal{A}$ 的运行时间类似。

定理 3 的证明与文献[30]中定理 6 的证明非常类似, 这里不再赘述。利用图 3 构造的 OW-CPA 公钥加密方案作为密钥封装方案中的基础公钥加密方案, 即可得到高效的 IND-CCA 安全的密钥封装方案。进一步, 利用 IND-CCA 的密钥封装方案与 IND-CCA 的数据封装方案即可构造 IND-CCA 安全的公钥加密方案。这是构造 IND-CCA 安全的公钥加密方案的一种国际标准, 也是 NIST 后量子公钥加密算法标准竞赛中, 构造 IND-CCA 的公钥加密方案的通用方式。

## 5 实现与性能分析

本节对构造的 IND-CCA 安全的公钥加密方案进行实现并做性能分析。首先, 根据安全参数, 设置方案的所有参数, 包括 D-RLWE 假设的维数 $n$、模数 $q$、高斯分布的参数 $\sigma$, S-RLWR 假设维数 $n$、模数 $p$ 与模数 $q$。其次, 需要对密钥封装方案中的哈希函数进行实例化, 并且为了节省随机比特, 设置合适的填充方式实现随机种子的填充。参数设置原则为保证方案正确性和安全性的前提下, 尽量采用小的参数, 从而提高方案的效率。注意, 在安全性分析中, 由于目前的安全性证明归约损失严重, 无法指导选取实用的安全参数。因此, 本文通过攻击分析的方式衡量参数的安全强度, 这也是国际上分析此类方案参数安全性的通用方法。

在参数设置时, 需要满足正确性和安全性要求。为了衡量密钥封装方案解封装失败的概率, 需要引入衡量高斯分布向量长度的引理 1, 本文称为高斯分布向量尾部有界性引理(文献[36]引理 4.3)。

**引理 1 (高斯分布向量尾部有界性引理)** 任取实向量 $\boldsymbol{v}\in\mathbb{Z}_q^m$, 对于任意正数 $\sigma$ 与 $r>0$, 记 $\mathcal{D}_{\sigma,\mathbb{Z}_q}$ 是整数集上标准差为 $\sigma$, 均值为 0 的离散高斯分布, 则有

$$\Pr[\boldsymbol{z}\leftarrow\mathcal{D}^m_{\sigma,\mathbb{Z}_q}:|\langle\boldsymbol{z},\boldsymbol{v}\rangle|>r]\leqslant 2e^{-\frac{r^2}{2\|\boldsymbol{v}\|_2^2\sigma^2}}$$

其中, $\boldsymbol{z}$ 的每个分量独立同分布于 $\mathcal{D}_{\sigma,\mathbb{Z}_q}$。

由 OW-CPA 公钥加密方案的正确性定理(定理 1), 只需密文的误差向量满足

$$\|e'\|_\infty\leqslant\|\frac{q}{p}(r_1\quad r_2\quad 1)\boldsymbol{e}\|_\infty+\|\tilde{e}\|_\infty<\frac{q}{4}$$

即可正确解密。记 $\boldsymbol{r}$ 是 $r_1$ 和 $r_2$ 的系数构成的向量, $\tilde{\boldsymbol{e}}$ 由 $\boldsymbol{e}$ 的前 2 个多项式分量系数构成的向量, 已知 $\|\boldsymbol{e}\|_\infty\leqslant\frac{1}{2}$, 所以 $\|\tilde{\boldsymbol{e}}\|_2^2\leqslant 2n\cdot\frac{1}{4}=\frac{n}{2}$, 由于 $\boldsymbol{r}\leftarrow\mathcal{D}^{2n}_{\sigma,\mathbb{Z}}$, 根据引理 1, 令 $r=7\sigma\sqrt{2n}$, 则有

$$\Pr[|\langle\boldsymbol{r},\tilde{\boldsymbol{e}}\rangle|>7\sigma\sqrt{2n}]\leqslant 2e^{-98}\approx 2^{-140}$$

由 $(r_1\quad r_2)(e_1\quad e_2)^T$ 计算所得的多项式其系数即为 $\boldsymbol{r}$ (或 $\boldsymbol{r}$ 的轮换) 与 $\tilde{\boldsymbol{e}}$ 内积的形式, 所以 $\Pr[\|e'\|_\infty>\frac{q}{p}(7\sigma\sqrt{2n}+\frac{1}{2})+\frac{1}{2}]\approx 2^{-140}$, 即如果

$$\frac{q}{p}(7\sigma\sqrt{2n}+\frac{1}{2})+\frac{1}{2}<\frac{q}{4}$$

则 OW-CPA 加密方案解密或 IND-CCA 密钥封装方案解封装失败的概率不超过 $2^{-140}$。注意, 由于解密失败概率分析中, 要求误差多项式的无穷范数满足正确解密的条件, 因此, 只要保证误差多项式的无穷范数小于 $\frac{q}{4}$, 则误差多项式的每一个系数均小于 $\frac{q}{4}$, 所以, 不需要对每个系数解密失败的概率进行累加。通过分析整理得, 如果 $p>\frac{28\sigma\sqrt{2n}+2}{1-\frac{2}{q}}$, 则方案至少以 $1-2^{-140}$ 的概率解密成功; 如果 $p\mid q$, 则简化为 $p>28\sigma\sqrt{2n}+2$。

本文利用 Primal Attack 攻击[37]与 Dual Attack 攻击对方案进行攻击分析, 当前, 这两种攻击是 LWE 类问题最优的攻击方式。分析所选参数下 D-RLWE 假设与 S-RLWR 假设的安全强度。在衡量 BKZ 算法[38]复杂度时, 经典模型下复杂度评估模型为 $b2^{0.292b}$[39], 其中, $b$ 为 BKZ 算法 Block 的维数; 量子

加速模型下复杂度评估模型为 $b2^{0.265b}$ [40]。评估 S-RLWR 假设的安全性时, 将 S-RLWR 假设中的误差分布视为 $[-\frac{q}{2p},\frac{q}{2p}]$ 上的均匀分布, 其标准差为 $\frac{q}{\sqrt{12}p}$。根据正确性和安全性的参数约束条件, 本文利用参数搜索脚本从多组参数空间中搜索出满足条件约束的较优参数。取多项式的次数 $n$ 分别为 512 或 1024, 记对应阶数下的密钥封装方案分别为 KEM-512 与 KEM-1024, 搜索所得参数如表 1。

**表 1 密钥封装方案参数选取**

**Table 1 Parameters of key encapsulation mechanism**

| $n$ | $q$ | $p$ | $\sigma$ | C-Sec | Q-Sec | $\delta$ |
|---|---|---|---|---|---|---|
| 512 | 23492 | 2467 | 2.75 | 118 | 108 | $2^{-140}$ |
| 1024 | 33215 | 3847 | 2.75 | 255 | 232 | $2^{-140}$ |
| 512* | 16384 | 2048 | 2.25 | 119 | 109 | $2^{-140}$ |
| 1024* | 32768 | 4096 | 2.25 | 244 | 222 | $2^{-140}$ |

(*: 表示 RLWR 模数满足 $p|q$ )

表 1 中“C-Sec”与“Q-Sec”分表表示攻击分析下, 方案参数可以达到的经典安全性与量子安全性。在正确性分析中, 分析始终保持方案解密失败的概率约为 $2^{-140}$, 因此, 不同安全参数下解封装失败的概率均约为 $2^{-140}$。通过引理 1 可以得到解密失败概率更小的参数, 但 $2^{-140}$ 已经满足当前正确性和安全性的需求。在多项式次数取 512 和 1024 时, 分别选取了两组参数, 即 $p\nmid q$ 与 $p|q$ 两种形式下的参数。其中, $p|q$ 的优势在于 S-RLWR 假设中的误差分布在这种情况下是无偏分布, 虽然, 目前不存在对有偏误差的攻击, 但是, 有偏误差分布可能会成为潜在的攻击目标, 因此, 本文提供两种形式下的参数设置。

与 NIST 后量子算法标准竞赛中的参数相比, 本文的模数 $q$ 较大, 导致方案的公钥、私钥和密文相对较大。为了压缩公钥长度, 本文采用伪随机生成的方式生成公钥中的随机多项式, 即首先生成相应安全强度下的随机种子, 再利用伪随机函数对随机种子进行扩展, 扩展后的字符串转化为随机多项式的系数。在伪随机生成的方式下, 只需要存储和传输随机种子, 从而实现公钥长度压缩。KEM-512 中随机种子为 256 比特随机字符串, KEM-1024 中随机种子为 512 比特随机字符串。由于私钥多项式 $r_2$ 的每个分量取自 $\mathcal{D}_{\sigma,\mathbb{Z}_q}$, 此时, 我们取采样区间为 $[-5\sigma,5\sigma]$, 这会极大地节省私钥的存储空间。导出会话密钥的随机种子 *seed* 在 KEM-512 与 KEM-1024 下分别取 256 比特随机字符串与 512 比特随机字符串。本文使用输出扩展函数 $F(\cdot)$ 对随机种子进行高位填充, 实际实现中使用 CSHAKE 哈希函数[41], 使得密钥封装中加密消息的长度达到 512 或 1024 比特。密钥封装方案公钥、私钥与密文长度计算公式分别为 $n\lceil\log q\rceil+\rho_{a_1}$、$n\lceil\log(10\sigma+1)\rceil+\rho_{ss}$、$2n\lceil\log p\rceil$, $\rho_{a_1}$ 表示生成 $a_1$ 所用随机种子的长度, $\rho_{ss}$ 表示私钥中随机字符串 *ss* 的长度。

表 2 显示了 IND-CCA 安全的密钥封装方案的尺寸指标。目前, 近似 256 比特经典安全强度下, NIST 后量子算法标准竞赛中, 基于理想格的二轮候选方案, 其公钥长度与密文长度均在 2KB 左右, 结合纠错码优化参数的方案公钥长度在 1KB 左右。虽然, 本文提出的密钥封装方案的存储效率未达到最优, 但是, 依然与 NIST 征集的二轮提案较为接近, 具体对比参见图 2。

**表 2 密钥封装方案尺寸指标**

**Table 2 The size of KEM**

| 方案 | C-Sec(Bit) | PK-Size (B) | SK-Size(B) | CT-Size (B) |
|---|---|---|---|---|
| KEM-512 | 118 | 992 | 352 | 1536 |
| KEM-1024 | 255 | 2112 | 704 | 3072 |
| KEM-512* | 119 | 928 | 352 | 1048 |
| KEM-1024* | 244 | 1984 | 704 | 3072 |

(注: CT 表示密文的长度)

进一步, 本文对密钥封装方案进行了软件参考实现, 实验环境为 Intel (R) Core (TM) i5-7200U CPU @ 2.50GHz, 8GB RAM, Ubuntu 16.04 LTS, gcc 5.4.0, OpenSSL 1.1.1c 开源代码库, 所有算法的运行时间为 1000 次试验结果的平均值。表 3 为相应参数下, IND-CCA 安全的密钥封装方案的运行时间。

**表 3 密钥封装方案算法运行时间**

**Table 3 The performance of KEM**

| 方案 | C-Sec (Bit) | KG (μs) | Encap (μs) | Decap (μs) |
|---|---|---|---|---|
| KEM-512 | 118 | 215 | 234 | 291 |
| KEM-1024 | 255 | 381 | 454 | 622 |
| KEM-512* | 119 | 260 | 291 | 355 |
| KEM-1024* | 244 | 348 | 452 | 608 |

根据表 3, 本文提出的密钥封装算法其软件参考实现性能达到较优水平。在近似 128 比特经典安全性下, 密钥生成算法、封装算法与解封装算法在普通

笔记本上的运行时间均在 0.5ms 以下。即使达到近似 256 比特经典安全性, 密钥封装算法每个算法的运行时间依旧保持在 0.5ms 左右。当前, 在 NIST 二轮候选方案中, 大部分方案的参考实现以及部分方案的优化实现, 也仅仅与本文算法参考实现效率相当。因此, 本文的密钥封装算法效率较高, 且本文算法的运行效率还具有进一步提升的空间。如果将本文算法的公钥和密文长度进行合理压缩, 加之本文算法计算简单, 不需要去随机化和误差采样, 算法效率高, 理论上更适用于于物联网等计算资源受限设备。

## 6 结论

本文利用优化的基于格的单向陷门函数, 构造了高效的 IND-CCA 安全的密钥封装(公钥加密)算法。首先, 针对密钥封装机制的构造场景, 优化了 MP 陷门, 压缩了陷门的长度。其次, 基于优化的陷门, 构造了基于 RLWE 与 RLWR 假设的确定性 OW-CPA 公钥加密方案, 方案的优势在于避免了去随机化、误差采样、随机数采样等复杂操作, 提高了方案的运行效率和实现安全性。进一步, 基于 OW-CPA 公钥加密方案构造了 QROM 模型下, 高效的 IND-CCA 安全的密钥封装方案。最后, 利用攻击分析的方法并结合方案正确性要求, 给出了方案的参数设置, 并对方案进行了软件参考实现, 在 Intel (R) Core (TM) i5-7200U CPU @ 2.50GHz 8GB RAM 的运行环境下, 算法的效率与国际最优水平相当, 从而验证了算法高效的特点。

## 参考文献


[1] V. Shoup, A Proposal for an ISO Standard for Public Key Encryption (Version 2.1). https://www.shoup.net/papers/iso-2_1.pdf, 2001.

[2] Boyd C, Cliff Y, Gonzalez Nieto J, et al. One-round Key Exchange In the Standard Model[C]. *Information Security and Privacy, 13th Australasian Conference*, 2008: 69-83.

[3] Fujioka A, Suzuki K, Xagawa K, et al. Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices[J]. *Designs*, *Codes and Cryptography*, 2015, 76(3): 469-504.

[4] Shor P W. Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer[C]. *Algorithmic Number Theory, First International Symposium*, 1994: 289.

[5] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[C]. *The 37th Annual ACM Symposium on Theory of Computing - STOC '05*, 2005: 84–93.

[6] Peikert C. Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem: Extended Abstract[C]. *The 41st Annual ACM Symposium on Theory of Computing - STOC '09*, 2009: 333–342.

[7] Lyubashevsky V, Peikert C, Regev O. On Ideal Lattices and Learning with Errors over Rings [C]. *Advances in Cryptology*, 2010: 1-23.

[8] Langlois A, Stehlé D. Worst-Case to Average-Case Reductions for Module Lattices[J]. *Designs*, *Codes and Cryptography*, 2015, 75(3): 565-599.

[9] Ajtai M, Dwork C. A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence[C]. *The 29th Annual ACM Symposium on Theory of Computing - STOC '97*, 1997: 284-293.

[10] Maurer U, Renner R, Holenstein C. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology[C]. *Theory of Cryptography*, 2004: 1-39.

[11] Leurent G, Nguyen P Q. How Risky Is the Random-Oracle Model? [C]. *Advances in Cryptology*, 2009: 445-464.

[12] Boneh D, Canetti R, Halevi S, et al. Chosen-Ciphertext Security from Identity-Based Encryption[J]. *SIAM Journal on Computing*, 2007, 36(5): 1301-1328.

[13] Micciancio D, Peikert C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller[C]. *Advances in Cryptology*, 2012: 700-718.

[14] J. Zhang, Y. Yu, S Q. Fan, et al. Improved Lattice-Based CCA2-Secure PKE in the Standard Model. https://eprint.iacr.org/2019/149.pdf. 2019.

[15] Peikert C, Waters B. Lossy Trapdoor Functions and Their Applications[C]. *The 40th Annual ACM Symposium on Theory of Computing*, 2008: 187-196.

[16] Fujisaki E, Okamoto T. Secure Integration of Asymmetric and Symmetric Encryption Schemes[J]. *Journal of Cryptology*, 2013, 26(1): 80-101.

[17] Lindner R, Peikert C. Better Key Sizes (and Attacks) for LWE-Based Encryption [C]. *Cryptographers' Track at the RSA*, 2011: 319-339.

[18] M. Naehrig, E. Alkim, J. Bos, et al. FrodoKEM-Learning with Errors Key Encapsulation [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[19] Hofheinz D, Hövelmanns K, Kiltz E. A Modular Analysis of the Fujisaki-Okamoto Transformation[C]. *Theory of Cryptography*, 2017: 341-371.

[20] T. Poppelmann, E. Alkim, R. Avanzi, et al. NewHope-Algorithm specifications and Supporting Documentation [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[21] P. Schwabe, R. Avanzi, J. Bos, et al. CRYSTALS-KYBER- Algorithm Specifications and Supporting Documentation [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[22] X H. Lu, Y M. Liu, D D. Jia, et al. LAC: Lattice-Based Cryp-tosystems [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[23] Banerjee A, Peikert C, Rosen A . Pseudorandom Functions and Lattices[C]. *Advances in Cryptology*, 2012: 719-737.

[24] Bogdanov A, Guo S Y, Masny D, et al. On the Hardness of Learning with Rounding over Small Modulus[C]. *Theory of Cryptography*, 2016: 209-224.

[25] J P. D'Anvers, A. Karmakar, S S. Roy, et al. SABER: Mod-LWR

Based KEM [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[26] Hoffstein J, Pipher J, Silverman J H, et al. NTRU: A Ring-Based Public Key Cryptosystem [C]. *Algorithmic Number Theory, Third International Symposium*, 1998: 267-288.

[27] C. Chen, O. Danba, J. Hoffstein, et al. NTRU: (Merger NTRUEncrypt and NTRU-HRSS-KEM) [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[28] D J. Bernstein, C. Chuengsatiansup, T. Lange, et al. NTRU Prime [R]. Call for Proposals for the Post Quantum Cryptog-raphy Standardization, National Institute of Standards and Technology, Round 2, 2019.

[29] O G. Morchon, Z. Zhang, S. Bhattacharya, et al. Round5 (Merger of HILA5 and Round2) [R]. Call for Proposals for the Post Quantum Cryptography Standardization, National Institute of Standards and Technology, Round 2, 2019.

[30] Jiang H D, Zhang Z F, Chen L, et al. IND-CCA-Secure Key Encapsulation Mechanism In the Quantum Random Oracle Model, Revisited[C]. *Advances in Cryptology*, 2018: 96-125.

[31] Xie X, Xue R, Zhang R. Inner-Product Lossy Trapdoor Functions and Applications[C]. *Applied Cryptography and Network Security*, 2012: 188-205.

[32] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions[C]. *Symposium on Theory of Computing*, 2008: 197-206.

[33] Babai L. On Lovász' Lattice Reduction and the Nearest Lattice Point Problem[J]. *Combinatorica*, 1986, 6(1): 1-13.

[34] K X. Xia. Implementation of Subfield Lattice Attack and Number Theoretic Transform [D]. Shandong University, 2017.

[35] Alwen J, Krenn S, Pietrzak K, et al. Learning with Rounding, Revisited - New Reduction, Properties and Applications[C]. *Advances in Cryptology*, 2013:57-74.

[36] V. Lyubashevsky. Lattice Signatures without Trapdoors (full version). https://eprint.iacr.org/2011/537.pdf, 2011.

[37] Albrecht M R, Göpfert F, Virdia F, et al. Revisiting the Expected Cost of Solving uSVP and Applications to LWE[C]. *Advances in Cryptology - ASIACRYPT 2017*, 2017: 297-322.

[38] Chen Y M, Nguyen P Q. BKZ 2.0: Better Lattice Security Estimates [C]. *Advances in Cryptology – Asiacrypt*, 2011: 1–20.

[39] Becker A, Ducas L, Gama N, et al. New Directions In Nearest Neighbor Searching with Applications to Lattice Sieving[C]. *The Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, 2016: 10–24.

[40] T. Laarhoven. Search Problems in Cryptography [D]. Eindhoven University of Technology, 2015.

[41] J. Kelsey, S. Chang, R. Perlner. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash. NIST Special Publication 800-185. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-185.pdf, 2016.

**谭高升** 于 2013 年在中国石油大学（华东）数学与应用数学专业获得理学学士学位。现在中国科学院信息工程研究所信息安全专业攻读博士学位。研究领域为公钥密码。研究兴趣包括：全同态加密、格加密。Email：tangaosheng@iie.ac.cn

**张锐** 于 2005 年在日本东京大学信息理工学专业获得博士学位。现任中国科学院信息工程研究所研究员。研究领域为信息安全、密码学、密码工程学。研究兴趣包括：公钥密码、对称密码。Email: r-zhang@iie.ac.cn

**姜子铭** 于 2017 年在山东大学信息安全专业获得理学学士学位。现在中国科学院信息工程研究所信息安全专业攻读博士学位。研究领域为公钥密码。研究兴趣包括：格加密、多项式乘法。Email: jiangziming@iie.ac.cn

**孙硕** 于 2015 年在电子科技大学数学与应用数学专业获得理学学士学位。现在中国科学院信息工程研究所信息安全专业攻读博士学位。研究领域为公钥密码。研究兴趣包括：格加密、格签名。Email: sunshuo@iie.ac.cn