基于格的高效范围证明方案

胡春雅 [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 早在 1985 年, Goldwasser、Michali 和 Rackoff 就提出了零知识证明。近年来, 区块链这一新技术越来越为人们所熟悉。由于区块链的应用和发展, 在实现零知识证明的相关结构方面取得了很大进展。同时, 随着量子计算机的研究, 许多传统的密码体制受到了严重的威胁。因此, 如何构造一个既高效又能抵抗量子攻击的密码方案是密码学领域的一个新的难题。

范围证明是一种特殊的零知识证明协议。范围证明可应用于各种实际应用中, 如电子投票系统或匿名凭证场景, 以确保匿名性和隐私性。在这种协议中, 证明者可以使验证者确信他知道一个属于开放连续整数区间的秘密整数。并且证明者不会泄漏有关秘密值的任何信息, 除了它位于特定区间的事实。通常, 这个秘密整数会被加密方案或承诺方案隐藏。但是现有的范围证明方案要么是不抗量子的, 要么在实际应用中效率很低。最糟糕的是, 在目前的范围证明方案中, 可以证明范围集合是有限的。换言之, 如果我们需要证明一个属于任意范围的秘密整数, 现有的方案无法做到这一点。针对上述问题, 本文提出了两种更有效的基于格的范围证明方案, 它们都是后量子方案。首先, 我们针对 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, 例如: 证明秘密整数 a 在范围 $[\alpha,\beta]$, 其中 α, β 是 $\mathbb{Z}_q$ 中整数。同时, 我们针对 KTX08 承诺方案也给出了一个高效的范围证明方案。该范围证明协议能够证明在 $[0,2^d]$ 中的被承诺值。与目前已有的基于格假设的范围证明方案相比, 我们的方案都有着更小的合理性错误和更低的通信成本。

关键词 格密码; 范围证明; 零知识证明; 基于分解技术
中图法分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2021.11.06

Lattice-based Efficient Range Proofs

HU Chunya[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract As early as 1985, zero-knowledge proof was proposed by Goldwasser, Micali and Rackoff. In recent years, blockchain, a new technology, is becoming familiar to people. Due to the application and development of blockchain, great progress has been made in the implementation of related structures of zero-knowledge proof. At the same time, with the research on quantum computer, many traditional cryptographic schemes are under serious threat. Therefore, how to construct a cryptographic scheme that is both efficient and resistant to quantum attacks is a new difficult problem in the field of cryptography.

Range proof is one kind of special zero-knowledge proof protocol. Range proof can be applied in various practical applications, such as electronic voting system or anonymous credential scenarios, to ensure anonymity and privacy. In this kind of protocol, the prover can convince the verifier that he knows a secret integer which belongs to an open continuous integer interval. The prover does not leak any information about the secret value, other than the fact that it lies in the certain interval. Usually, this secret integer will be hidden by encryption schemes or commitment schemes. But the present range proofs are either not quantum resistant or very inefficient in practical application. What's worst, the range sets that can be proved are limited. In other words, if we need to prove a secret integer that belongs to any range, the existing schemes can not do it. In view of the above problems, in this paper, we propose two more efficient lattice-based range proof schemes which are all post-quantum schemes. In the first scheme, we give an efficient range proof for Regev's classical encryption scheme. In contrast to the present range proof schemes, our range proof scheme can prove the encrypted secret integer that belongs to arbitrary integer range. Specifically, it can prove that the secret integer a is in the range $[\alpha,\beta]$, where α, β are the integers in $\mathbb{Z}_q$.In the meantime, we also give an efficient range proof for KTX08 commitment scheme. The protocol can prove that the committed values are in $[0,2^d]$, where d is the integer in $\mathbb{Z}_q$. Compared with the present lattice-based range proofs, our range proofs have smaller soundness error and lower communication costs.

通讯作者: 胡春雅, 硕士, Email: huchunya@iie.ac.cn。
本课题得到国家自然科学基金项目(No. 61772521); 中科院前沿科学重点研究项目(No.QYZDB-SSW-SYS035)资助。
收稿日期: 2020-01-17; 修改日期: 2020-03-16; 定稿日期: 2021-10-19

Key words lattice-based cryptography; range proof; zero-knowledge proof; decomposition-based method

1 绪论

零知识证明是由 Goldwasser、Micali 和 Rackoff 在 20 世纪 80 年代首次提出[1-2]的交互证明系统。简单地说, 它提供了一种在不直接揭示秘密的情况下证明秘密的能力。本文主要研究一种特殊的零知识证明协议——范围证明。

1987 年, Brickell 等人[3]首次提出了范围证明协议的概念。范围证明是运行在证明者和验证者之间的两方协议。在范围证明中, 证明者能够在不泄露任何其他信息的情况下, 向验证者证明被加密或者被承诺的秘密整数属于某个给定的区间内。目前, 范围证明已被广泛地应用于电子商务、电子投票、电子审计、匿名凭证、区块链等多个领域, 它能够在不影响功能性的同时, 最大限度地保证证明者的隐私信息。

随着量子计算机技术的不断发展, 所有基于传统数论假设构造的密码方案的安全性正在遭受着严重的威胁。近年来, 格密码因其强大的功能性和抗量子攻击的特点越来越受到密码学界的广泛关注与重视, 利用格困难假设构造抗量子的密码方案是目前密码学热点问题之一。但是现有的基于格的范围证明方案不是非常高效, 因此如何构造更加高效的范围证明方案仍是一个待解决的问题。

1.1 相关工作

早在几十年前, Brickell 等人[3]就提出了第一个范围证明方案。该方案是一个三轮的Σ协议, 其安全性依赖于离散对数假设。之后 Damgard[4]以及 Fujisaki、Okamoto[5]分别在 1995 年和 1997 年提出了各自的范围证明方案, 但是这些方案的效率都非常低, 无法在实际中应用。

第一个切实可行的范围证明构造由 Boudot 在其 2000 年发表的文献[6]中被提出。Boudot 范围证明方案的高层次思想可以直观地描述为: 证明者将需要进行范围证明的秘密整数 a 分解成平方和的形式进行证明。在此之后范围证明方案不断发展, 不同的构造方案层出不穷。2003 年, Lipmaa 利用著名的 Lagrange 定理[7]: 任何非负整数都可以由 4 个整数的平方组成, 对 Boudot 范围证明方案进行了改进, 构造了一个能够对任意范围秘密整数进行证明的范围证明方案[8]。2005 年, Groth[9]提出如果秘密整数 a 的形式是 $4n+1$, 那么只分解成 3 个数的平方之和就可以得到需要的范围证明方案。该方案进一步优化了 Boudot 范围证明方案, 但在实际应用中却导致了证明者效率的降低。上述这些协议的非交互式证明都需要依赖 Fiat-Shamir[10]启发式。2009 年, Yuen 等人[11]尝试构造了一个在标准模型下的非交互式高效范围证明。但是后来的研究表明, 这种方法不够安全。2017 年, Couteau、Peters 和 Pointcheval 展示了如何移除强 RSA 假设要求[12], 对以前的方案进行了优雅的描述,并且不需要修改原始结构。

Bellare 和 Goldwasser 在 1997 年首次使用“分解技术”构造了一个范围证明方案[13]。该方案建议使用部分密钥托管来解决个人隐私高度依赖于存储机构的问题, 并首次提出了将秘密整数 a 用二进制表达后构造证明。但是他们的方案只能够证明形式为 $[0,2^d]$ 的秘密整数范围, 其中 d 为“分解”后的向量长度。基于上述思想, Damgård 和 Jurik 给出了他们的范围证明方案[14]。随后在 2005 年[15-16], Schoenmakers 提出了更加一般的范围证明构造。该方案将整数属于 $[0,2^d]$ 的证明协议重复两次, 从而得到了能够证明秘密整数 a 属于 $[\alpha,\beta]$ 的范围证明方案, 其中 α 、β 都是 2 的次方。更一般地, 如果使用 u 进制分解, 我们将会得到更有效的构造方案, 如文献[17]中给出的范围证明方案。针对秘密整数 a 属于区间 $[0,\beta]$, 其中为 β 任意整数, Lipmaa、Asokan 和 Niemi 给出了一个范围证明方案[18]。该方案对秘密整数 a 进行多基分解, 是上述 u 进制分解的推广。同样利用文献[15]中提出的技术, 他们将方案推广到了更加一般的证明区间: $[\alpha,\beta]$, 其中 α , β 为任意整数。

利用签名算法也可以构造高效的范围证明方案。构造思想可以简单描述为: 证明者需要向验证者证明其拥有秘密整数 a 的签名, 但是同时不能泄露 a 。在初始阶段, 证明范围内的所有值都被签名, 如果证明者知道其中的一个签名, 那么就意味着秘密整数 a 是属于声明的区间的。2008 年, Camenisch、Chaaboni 和 Shelat 的方案使用双线性对构造了一个特定的成员的零知识证明方案[17]。为了减小通信量, 方案考虑了一般情形 $u \geqslant 2$ 。该范围证明方案能够证明秘密值 $a \in [0,u^d-1]$, 容易得到 a 可以表示为 $a=\sum_{i=1}^{d} u_i b_i$ 。验证者对 $[0,u-1]$ 中的每个整数都进行签名, 如果证明者能够证明他知道被承诺的 b_i 的签

名, 那么就可以说明 $b_i \in [0,u-1]$。然后利用两个 Σ 协议完成对秘密值 a 的范围证明。2010 年, Chaabouni 、Lipmaa 和 Shelat 改进了 Camenisch 等人[19]的方案, 将证明范围扩展到了任意区间 $[\alpha,\beta]$, 其中 α, β 为任意整数, 并且降低了方案的通信量复杂度。随后, Canard 等人[20]优化了上述方案, 降低了证明过程中的计算开销, 进一步提高了方案的效率。2015 年, 针对保密交易(Confidential Transaction, CT)Maxwell 利用 Borromean 环签名变形[21], 设计了一种基于环签名的范围证明方案[22]。保密交易能够用来构造匿名货币, 而在匿名货币 Monero[23]中, 为了确保隐私交易, 利用了一种聚合签名算法构造范围证明[24]。

近年来, 出现了很多其他不同的构造高效范围证明方案的方法。2011 年, Groth[25]利用两层同态承诺构造了一个范围证明方案。2013 年, Gennaro 等人[26]提出了一个新的非交互式简洁零知识证明协议——ZK-SNARK。ZK-SNARK 有着很短的验证时间和证明长度, 并且能够能够证明所有 NP(Non-deterministic Polynomial)问题。因此利用 ZK-SNARK, 我们也可以得到非常高效的范围证明。

上述提到的所有方案都依赖于可信的设置。文献[27]中, Bootle 等人通过内积论证协议构造了一个证明长度为对数大小, 并且验证者证明者计算时间都非常短的零知识证明协议。在此基础上, 2018 年, Bunz 等人[28]给出了目前最高效的范围证明方案——Bulletproof, 并且避免了可信设置。Bulletproof 主要思想可以简单描述为: 首先通过“分解技术”将被承诺值的范围证明转换到对向量是否为比特串的证明, 这可以通过向量的内积完成, 再利用内积论证协议完成零知识的证明。此外, Bulletproof 还展示了如何使用称为多重指数的组件来优化其结构, 使得证明长度进一步缩短。

虽然基于数论假设的范围证明方案已经非常高效, 但是这些方案都不是抗量子安全的方案。2018 年, Libert 等人[29]针对 KTX08 承诺方案给出了第一个基于格的范围证明方案。2019 年, Nguyen 等人[30]首次构造了一个基于编码的范围证明方案, 方案的证明长度与证明范围相关。但是这两个方案都使用了 Stern 协议[31]框架, 由于框架中一些无法优化的非代数步骤, 利用该框架构造的协议都会有很大的合理性错误(2/3)。如果要得到较小的合理性错误就必须多次重复执行协议, 因此在实际应用中该方案并不十分高效。

1.2 本文的贡献

本文针对目前抗量子范围证明方案都不高效的问题, 利用 Bootle 等人在文献[32]提出的零知识证明框架以及在范围证明中常用的“分解技术”构造了以下两个高效的范围证明方案:

第一个方案是针对 Regev 基于 LWE(Learning With Errors)假设的经典加密方案[33]构造的一个高效范围证明协议。该协议能够证明任意区间的被加密值 a, 比如: $a \in [\alpha,\beta]$, 其中 $\alpha+\beta<q$, $\alpha,\beta \in \mathbb{Z}_q$, 且合理性错误是 $1/ql$。据我们所知, 该范围证明协议是目前唯一的针对较小的被承诺值的范围证明方案。

第二个方案是针对 Kawachi、Tanaka 和 Xagawa 在 2008 年提出基于 SIS(Short Integer Solution)假设的承诺方案[34]——KTX08 承诺方案, 构造的一个高效范围证明协议。虽然这个协议只能够证明被承诺值 a 边界范围是 2 的次方的情况, 例如: $a \in [0,2^d-1]$, 但是因为 KTX08 承诺方案是一个串承诺, 承诺向量的长度能做到非常大, 被承诺值可以大于 q。因此与我们构造的第一个范围证明协议相比, 该范围证明协议能够证明的被承诺值可以非常大。同时该协议相比于目前基于格假设的最高效的范围证明协议[29]有着更小的合理性错误, 在相同情况下, 我们的方案比文献[29]的方案更加高效。

接下来, 将我们的方案和当前基于经典数论假设的最高效的范围证明方案[28]以及现有的基于格假设的范围证明方案[29]进行对比, 具体的对比结果可以参考表 1。

表 1 现有范围证明方案与本方案的对比

Table 1 Comparison between the Existing Range Proofs and Ours

范围证明方案	文献[28]	文献[29]	我们的方案 1	我们的方案 2
是否抗量子?	×	√	√	√
可证明的范围	$[0,2^d-1]$	$[\alpha,\beta]$	$[\alpha,\beta]$	$[0,2^d-1]$
合理性错误	*negl*	2/3	$1/ql$	$1/ql$
可证明的承诺/加密方案	Pedersen 承诺方案[35]	KTX 承诺方案[34]	Regev 基于格的加密方案[33]	KTX 承诺方案[34]

2 预备知识

2.1 符号定义

我们用粗体字母表示环和多项式的元素。如果$\mathcal{C}$是一个集合, 我们用$c \xleftarrow{\$} \mathcal{C}$表示$c$是从$\mathcal{C}$中随机选择的。我们用带箭头的符号表示一个向量, 例如: $\vec{v}$, 以及用$\|\vec{v}\|_2$表示为它的 2-范式, $\|\vec{v}\|_\infty$表示为它的无穷范式。我们将前面带点的符号表示为属于集合$\mathcal{R}_q$的元素, 例如: $\grave{a}$。

当矩阵$\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$和$\boldsymbol{B} \in \mathbb{Z}_q^{m\times k}$连接时, 我们使用符号$[\boldsymbol{A}|\boldsymbol{B}] \in \mathbb{Z}_q^{m\times(n+k)}$表示。类似的我们用$(\vec{x}\|\vec{y}) \in \mathbb{Z}_q^{n+k}$表示$\vec{x} \in \mathbb{Z}_q^n$和$\vec{y} \in \mathbb{Z}_q^k$的列连接。符号“$\circ$”表示的是两个向量之间对位相乘。例如, 向量$\vec{a} \in \mathbb{Z}^n$和向量$\vec{b} \in \mathbb{Z}^n$对位相乘可以表示为$\vec{a} \circ \vec{b} = \vec{c}$, 其中向量$\vec{c} \in \mathbb{Z}^n$中的每个分量都是$\vec{a}$和$\vec{b}$中对应位置的乘积, 即$c_i = a_i b_i$。

我们在表 2 中列出了本文中所需的符号和参数。

表 2 参数和符号概述

Table 2 Overview of Parameters and Notation

符号	描述
q	一个完全分裂的素数且$q \equiv 1 \mod l$
$\mathbb{Z}_q$	$=\mathbb{Z}/q\mathbb{Z}$; 一个整数域。
Φ_l	一个l次分圆多项式。
$\mathcal{R}$	$=\mathbb{Z}[X]/(\Phi_l)$; 一个整环。
$\mathcal{R}_q$	$=\mathbb{Z}_q[X]/(\Phi_l)$; 一个模$q$整环。
$\mathcal{C}$	$\mathcal{C}=\{0, X^i \mid 0 \leqslant i < l\}$; 挑战空间。
$\overline{\mathcal{C}}$	$\overline{\mathcal{C}}=(\mathcal{C}-\mathcal{C})/\{0\}$; 不包括 0 的一组挑战差值。
D_σ^n	标准差为σ的$\mathcal{R}$上的离散高斯分布。

2.2 困难假设

本文提出了两个基于 RSIS(Ring Short Integer Solution)[36]假设和 RLWE(Ring Learning With Errors)[37]假设的高效范围证明方案。RSIS 假设和 RLWE 假设的定义分别在定义 1 和定义 2 中给出。与 SIS 假设相比, RSIS 假设中给定向量$\grave{a}$和所求向量$\grave{z}$中的分量都是环上的元素, 而在 SIS 假设中给定向量和所求向量的分量都是整数。和 RSIS 假设类似, 在RLWE假设中给定向量$(\vec{a},\vec{b})$中的分量都是环上的元素, 而在 LWE 假设中它们都是整数。

定义 1. (RSIS 假设)m、q为整数, 对于给定的一个向量$\vec{a} \in \mathcal{R}_q^m$, 由$m$个$\grave{a} \xleftarrow{\$} \mathcal{R}_q$组成, 求一个非零向量$\grave{z} \in \mathcal{R}^m$且$\|\vec{z}\|_2 \leqslant B$, 满足$\vec{a}^T \cdot \vec{z} = \sum_{i=0}^{m} \grave{a}_i \cdot \grave{z}_i = 0 \in \mathcal{R}_q$是困难的。

定义 2. (判定 RLWE 假设)m、q为整数, χ是$\mathcal{R}$上某个分布, 通常为高斯分布, 以下两个分布是不可区分的:

(1) $(\vec{a},\vec{b}) \xleftarrow{\$} \mathcal{R}_q^m \times \mathcal{R}_q^m$,

(2) $(\vec{a},\vec{a}^T \cdot \grave{s} + \vec{e})$, 其中$\grave{a} \xleftarrow{\$} \mathcal{R}_q^m$, $\grave{s} \xleftarrow{\$} \mathcal{R}_q$, $\vec{e} \xleftarrow{\$} \chi^m$。

2.3 快速数论变换

快速数论变换[38-39](Number Theoretic Transform, NTT)类似于快速傅里叶变换(Fast Fourier Transform, FFT), 区别在于快速数论变换是在$\mathbb{Z}_q$上的计算。假设g为模素数q的原根, 那么对于一个长度为N, 且各元素小于q的正整数序列$x(n)$, 有快速数论变换公式:

$$X(k) = \sum_{n=0}^{N-1} x(n) a^{nk} \mod q,$$

其中$a = g^{\frac{q-1}{N}}$, $X(n)$为变换后所得到的序列。且逆快速数论变换(Inverse Number Theoretic Transform, INTT)的公式为:

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) a^{-kn} \mod q。$$

NTT 变换有如下性质: ①线性性; ②正交性; ③对称性; ④平移性; ⑤循环卷积性。

2.4 零知识证明

零知识证明协议是证明者$\mathcal{P}$和验证者$\mathcal{V}$之间的一种双方协议, 它允许前者使后者相信它知道一些秘密信息, 除了断言本身已经披露的内容之外, 不披露任何关于秘密的内容。正式地说, 令$R = \{(y,w)\} \in \{0,1\}^* \times \{0,1\}^*$是一种 NP 关系。一个知识的零知识论证协议需要满足以下三个性质:

- 完备性: 如果$(y,w) \in R$, 并且证明者和验证者都按照协议诚实地执行, 那么验证者至少会有$1-\alpha$的概率接受。
- 特殊的合理性: 对于一个实例y, 存在一个多项式时间内运行的模拟器$\mathcal{E}$, 给定不同挑战的相应交互副本, $\mathcal{E}$能够有效抽取出证据w, 使

得 $(y,w)\in R$。

- 零知识性: 存在一个多项式时间的模拟器 $\mathcal{S}$, 输入实例 y 和挑战 t, $\mathcal{S}$ 能够输出一个与真实交互产生的副本不可区分的副本。

其中, α 为协议的完备性错误。

本文构造的零知识协议是一种称为诚实验证者的零知识协议。在这一类协议中, 验证者会诚实地执行协议内容。

2.5 拒绝采样

对于一个零知识的协议, 证明者的回答不能依赖于它的秘密输入。但是, 在我们的协议中, 证明者的回答是一个离散的正态分布, 该正态分布根据密钥的不同而变化。为了纠正这一点, 我们采用拒绝抽样[40-41], 其中证明者的回答仅以一定的概率输出。

下面的定理表明, 对于足够大的 σ, 拒绝抽样过程输出的结果与秘密无关。该方法在输出一个值之前只需要常数轮的迭代次数。

定义 3. 定义在 $\mathcal{R}^k$ 以 $\vec{v}$ 为中心, 标准差为 $\sigma>0$ 的离散高斯分布为:

$$D_{\vec{v},\sigma}^{kn}(\vec{z})=\frac{e^{-\|\vec{z}-\vec{v}\|_2^2/2\sigma^2}}{\sum_{\vec{z}\in\mathcal{R}^k}e^{-\|\vec{z}\|_2^2/2\sigma^2}}$$

当 $\vec{v}=\vec{0}$ 时, 我们可以把 $D_{0,\sigma}^{kn}$ 写成 D_{σ}^{kn}。

引理 1. 令 $\vec{z}\xleftarrow{\$}D_{\sigma}^{kn}$, 则

$$\Pr[\|\vec{z}\|_2\leqslant\sigma\sqrt{2kn}]\geqslant 1-2^{-\log(e/2)kn/4}$$

对于引理 1 的证明我们可以参考文献[32]。

算法 1. Reject$(\vec{z},\vec{v},\sigma)$.

$u\xleftarrow{\$}[0,1)$

IF $u>\frac{1}{12}\cdot\exp(\frac{-2<\vec{z},\vec{v}>+\|\vec{v}\|_2}{2\sigma^2})$, THEN

RETURN 0

ELSE RETURN 1

END IF

引理 2. 假设 V 是 $\mathcal{R}^k$ 的子集, 并且 V 中所有元素的 2-范数都小于 T, 设 H 是 V 上的概率分布。然后, 对于任何常数 M, 存在一个 $\sigma\geqslant 5T$, 使得以下算法 $\mathcal{A}$、$\mathcal{F}$ 的输出分布在统计上接近, 且算法 $\mathcal{A}$、$\mathcal{F}$ 输出 $(\vec{z},\vec{v})$ 的概率约为 1/12:

(1) $\mathcal{A}:\vec{v}\xleftarrow{\$}H;\quad\vec{z}\xleftarrow{\$}D_{\vec{v},\sigma}^{kn}$,

(2) $\mathcal{F}:\vec{v}\xleftarrow{\$}H;\quad\vec{z}\xleftarrow{\$}D_{\vec{0},\sigma}^{kn}$。

引理 2 的证明可以参考文献[32]引理 2.4 的证明。

2.6 承诺方案

一个承诺方案[42]由三个算法(KeyGen, Commit, Verify)组成, KeyGen 为生成承诺公钥的算法, Commit 为承诺算法, Verify 为承诺的验证算法:

- KeyGen$(1^{\lambda})\to ck$ 算法输入安全参数 λ, 输出承诺公钥 ck。
- Commit$(ck,m)\to(r,c)$ 算法输入承诺的公钥 ck, 以及被承诺值 m, 输出承诺打开对 (r,c)。
- Verify$(ck,m,c,r)\to b$ 算法输入承诺的公钥 ck, 消息 m, 以及承诺打开对 (r,c), 输出 $b\in\{0,1\}$。

并且一个安全的承诺方案需要满足以下两条性质:

- 隐藏性(Hiding): 对于任何概率多项式时间的敌手 $\mathcal{A}$ 都满足:

$$\Pr\begin{bmatrix} & ck\leftarrow\mathrm{Setup}(1^{\lambda}) & \\ & (m_0,m_1)\leftarrow\mathcal{A}(ck) & \\ b=b' & b\leftarrow\{0,1\} & \\ & (c,r)\leftarrow\mathrm{Commit}_{\mathrm{ck}}(m_{\mathrm{b}}) & \\ & b'\leftarrow\mathcal{A}(ck,c) & \end{bmatrix}=\frac{1}{2}+negl(\lambda)$$

- 绑定性(Binding): 对于任何概率多项式时间的敌手 $\mathcal{A}$ 都满足:

$$\Pr\begin{bmatrix} m\neq m' \text{ and} & ck\leftarrow\mathrm{Setup}(1^{\lambda}) \\ \mathrm{Open}_{\mathrm{ck}}(m,c,r) & (m,m',r,r',c)\leftarrow\mathcal{A}(ck) \\ =\mathrm{Open}_{\mathrm{ck}}(m',c,r) & \end{bmatrix}=negl(\lambda)$$

其中 $negl(\lambda)$ 表示一个可忽略的函数。

辅助承诺方案: 在我们的范围证明协议中需要一个辅助的承诺方案完成零知识的证明。在本项工作中我们利用的是文献[43]中提出的基于格的承诺方案。该承诺方案的具体构造过程如下:

- KeyGen$(1^{\lambda})\to B$ 是一个概率多项式时间的算法, 输出 B 为承诺的公钥。

$$\grave{B}=\begin{pmatrix}\vec{b}_1^T\\ \vec{b}_2^T\\ \vec{b}_3^T\\ \vec{b}_4^T\end{pmatrix}=\begin{pmatrix}1 & \grave{b}_{1,2} & \grave{b}_{1,3} & \grave{b}_{1,4} & \grave{b}_{1,5}\\ 0 & 1 & 0 & 0 & \grave{b}_{2,5}\\ 0 & 0 & 1 & 0 & \grave{b}_{3,5}\\ 0 & 0 & 0 & 1 & \grave{b}_{4,5}\end{pmatrix}\in\mathcal{R}_q^{4\times 5}$$

- $\mathrm{Commit}(\grave{B},\vec{\grave{m}})\to(\vec{\grave{r}},\vec{\grave{c}})$ 是一个概率多项式时间的算法, 输入为承诺的公钥 $\grave{B}$ 和被承诺值 $\vec{\grave{m}}$, 其中被承诺值的消息空间为 $\mathcal{R}_q^3$。输出为随机数 $\vec{\grave{r}}\in\beta^{5n}$, β^n 为错误分布, 并且输出承诺 $\vec{\grave{c}}$。具体算法如下:

$$\mathrm{Commit}(\grave{B},\vec{\grave{m}})=\vec{\grave{c}}=\begin{pmatrix}\vec{\grave{t}}_1\\ \vec{\grave{t}}_2\\ \vec{\grave{t}}_3\\ \vec{\grave{t}}_4\end{pmatrix}=\grave{B}\cdot\vec{\grave{r}}+\begin{pmatrix}\vec{0}\\ \vec{\grave{m}}_2\\ \vec{\grave{m}}_3\\ \vec{\grave{m}}_4\end{pmatrix}$$

- $\mathrm{Verify}(\grave{B},\vec{\grave{m}},\vec{\grave{c}},\vec{\grave{r}},\grave{f})\to b$ 是一个确定性多项式时间内的算法, 其输入为承诺的公钥 $\grave{B}$, 被承诺值 $\vec{\grave{m}}\in\mathcal{R}_q^4$, 承诺 $\vec{\grave{c}}\in\mathcal{R}_q^4$ 以及随机数 $\vec{\grave{r}}\in\mathcal{R}_q^5$, 挑战值 $\grave{f}\in\overline{C}$ 或者 $\grave{f}=1$。输出一个比特 $b\in\{0,1\}$。

在这个承诺方案中, 承诺方案的打开是一个有效的(宽松)打开, 验证算法中, 验证者首先验证 $\left\|\vec{\grave{r}}\right\|\leqslant 2B$ 以及 $\grave{f}\vec{\grave{c}}\overset{?}{=}\grave{B}\vec{\grave{r}}+\grave{f}\begin{pmatrix}0\\ \vec{\grave{m}}\end{pmatrix}$, 其中 $B=\sigma\sqrt{10n}$。如果能够通过验证, 则输出 1, 否则输出 0。

引理 3. [43, Lemma 7] 对于任意的多项式算法 $\mathcal{A}$, 假设 $\mathcal{A}$ 有 ε 的优势去打破承诺的绑定性, 那么存在另一个算法 $\mathcal{A}'$ 与 $\mathcal{A}$ 有相同的运行时间以及有 ε 的优势解决 $RSIS_{4,8B}$。

引理 4. [43, Lemma 6] 对于任意的多项式算法 $\mathcal{A}$, 假设 $\mathcal{A}$ 有 ε 的优势去打破承诺的隐藏性, 那么存在另一个算法 $\mathcal{A}'$ 与 $\mathcal{A}$ 有相同的运行时间以及有 ε 的优势区分 $RLWE_4$。

2.7 分解技术

本文利用的是文献[44]中的分解算法。对于任意的 $B\in\mathbb{Z}^+$, 定义: $\delta_B:=\lfloor\log_2 B\rfloor+1=\lceil\log_2 B+1\rceil$, 以及序列 $B_1,\cdots,B_{\delta_B}$, 其中 $B_j=\lfloor\frac{B+2^{j-1}}{2^j}\rfloor$, $j\in[1,\delta_B]$。因为 $\sum_{j=1}^{\delta_B}B_j=B$ 以及任意在 $[0,B]$ 中的整数 v 都可以被分解成 $\overrightarrow{\mathrm{idec}_B(v)}=(v^{(1)},\cdots,v^{(\delta_B)})^T\in\{0,1\}^{\delta_B}$, 并且 $v^{(j)}$ 满足 $\sum_{j=1}^{v^{(\delta_B)}}B_j v^{(j)}=v$。具体算法如下:

算法 2. Decompose(v,B).

$v'=v$
FOR $j=i$ to δ_B
IF $v'\geqslant B_j$, THEN
$v^{(j)}:=1$
ELSE $v':=v'-B_j\cdot v^{(j)}$
END IF
RETURN $\overrightarrow{\mathrm{idec}_B(v)}=(v^{(1)},\cdots,v^{(\delta_B)})^T$

然后, 对于任意的正整数 l 和 B, 我们定义以下的矩阵:

$$H_{l,B}:=\begin{bmatrix}B_1,\cdots,B_{\delta_B} & & & \\ & B_1,\cdots,B_{\delta_B} & & \\ & & \ddots & \\ & & & B_1,\cdots,B_{\delta_B}\end{bmatrix}\in\mathbb{Z}_q^{l\times l\delta_B}$$

以及以下的映射函数:

$\mathrm{vdec}_{l,B}:[0,B]^l\leftarrow\{0,1\}^{l\delta_B}$ 是将向量 $\vec{v}=(v_1,\cdots,v_l)$ 映射到向量 $\overrightarrow{\mathrm{vdec}_{l,B}(\vec{v})}=(\mathrm{idec}(v_1)\|\cdots\|\,\mathrm{idec}(v_{\delta_B}))$。其中向量 $\overrightarrow{\mathrm{vdec}_{l,B}(\vec{v})}$ 满足 $H_{l,B}\cdot\overrightarrow{\mathrm{vdec}_{l,B}(\vec{v})}=\vec{v}$。

3 针对 Regev 经典加密方案的范围证明

在范围证明协议中, 证明者和验证者在证明开始之前就会得到需要秘密整数的承诺或者密文。因此, 需要一个安全的承诺方案或者加密方案, 隐藏秘密值。在部分节中, 我们针对 Regev 基于 LWE 假设的经典加密方案[33], 构造出了一个高效的范围证明协议。

3.1 回顾 Regev 经典加密方案

首先, 我们简单介绍一下 Regev 公钥加密方案, 加密方案由三个算法(KenGen, Encrypt, Decrypt)组成,

KeyGen 为生成加密公私钥的算法, Encrypt 为加密算法, Decrypt 为解密算法:

- KeyGen$(1^\lambda)\to(A,\vec{b},\vec{s})$ 输出私钥 $\vec{s}$，公钥 $(A,\vec{b})$。其中 $\vec{s}\xleftarrow{\$}\mathbb{Z}_q^m$，$A\xleftarrow{\$}\mathbb{Z}_q^{m\times n}$，$\vec{e}\xleftarrow{\$}(\bar{\Psi}(q))^n$，$\vec{b}=A^T\vec{s}+\vec{e}$。$\bar{\Psi}(q)$ 为 LWE 困难问题的错误分布[12,24]。
- Encrypt$(A,\vec{b},\mathfrak{m})\to(\vec{u},c)$ 加密的消息空间为 $\{0,\cdots,p-1\}$，给定消息 $\mathfrak{m}$ 以及公钥 $(A,\vec{b})$，从整数向量集合 $\{0,\cdots,p-1\}^n$ 中均匀随机选取向量 $\vec{r}$，加密算法输出密文:
$$(\vec{u},c)=(A\vec{r},\vec{b}^T\vec{r}+\mathfrak{m}\cdot\lfloor q/p\rfloor)\in\mathbb{Z}_q^m\times\mathbb{Z}_q。$$
- Decrypt$(\vec{u},c,\vec{s})\to\mathfrak{m}$ 输入密文 $(\vec{u},c)$，以及私钥 $\vec{s}$，输出消息:
$$\mathfrak{m}=\lfloor(c-\vec{s}^T\cdot\vec{u})\cdot p/q\rceil。$$

对于以上加密方案的正确性、安全性以及相关参数的选取, 可以参考文献[45]。

3.2 针对 Regev 加密方案的范围证明构造思想

一般来说, 针对关系 R 的零知识证明可以记作: 关系{(公共输入; 证据): 满足的关系}。范围证明是一种特殊的诚实验证者零知识协议, 因此也可以记作: {(公共参数, 承诺 $\vec{c}$; 被承诺值 m, 随机数 $\vec{r}$): $\vec{c}$=Com(m,$\vec{r}$) $\wedge$ m 属于某一给定区间}。

本范围证明协议能够证明的被加密的秘密整数 $\mathfrak{m}$ 的范围为 $[\alpha,\beta]$，其中 $0<\alpha<\beta<p$ 且 $\alpha+\beta\leqslant p$。针对 Regev 经典加密方案的范围证明可以记作关系 R_1:

$$\mathrm{R}_1=\{((A,\vec{b}),(\vec{u},c),(\vec{r},\mathfrak{m}))\in(\mathbb{Z}_q^{m\times n}\times\mathbb{Z}_q^n)$$
$$\times(\mathbb{Z}_q^m\times\mathbb{Z}_q)\times(\{0,\cdots,p-1\}^n\times[\alpha,\beta]):$$
$$A\vec{r}=\vec{u}\mod q\wedge(c=\vec{b}^T\vec{r}+\mathfrak{m}\cdot\lfloor q/p\rfloor)\}$$

然后定义 $A'=\begin{bmatrix}A & 0^m\\ \vec{b}^T & \lfloor q/p\rfloor\end{bmatrix}\in\mathbb{Z}_q^{(m+1)\times(n+1)}$，$\vec{y}=(\vec{u}\|\ c)\in\mathbb{Z}_q^{m+1}$，上述关系 R_1 也可以写成如下关系 R_2:

$$\mathrm{R}_2=\{((A',\vec{y}),\vec{x}=\vec{r}\|\ \mathfrak{m})\in(\mathbb{Z}_q^{(m+1)\times(n+1)}\times\mathbb{Z}_q^{(m+1)})\times\mathbb{Z}_q^{(n+1)}:$$
$$A'\vec{x}=\vec{y}\mod q\wedge\vec{r}\in\{0,\cdots,p-1\}^n\wedge\mathfrak{m}\in[\alpha,\beta]\}$$

为了证明秘密整数 $\mathfrak{m}$ 的范围, 在本方案中我们通过计算 $\mathfrak{m}'=\mathfrak{m}-\alpha$，将证明 $\mathfrak{m}$ 属于区间 $[\alpha,\beta]$ 转换到证明另一个秘密整数 $\mathfrak{m}'$ 属于区间 $[0,\beta-\alpha]$。虽然我们能够利用进制转换的方法构造一个 u 进制串来表示秘密整数 $\mathfrak{m}'$, 但是利用进制转换“分解”得到的范围证明方案只能构造出范围边界是 u 次方的范围证明方案, 显然, 这是对于可证明范围来说是一个非常严格的约束。具体地说, 利用进制转换“分解”得到的范围证明方案, 只能够证明秘密整数 $\mathfrak{m}'$ 属于 $[0,\beta]$, 当且仅当 $\beta=u^d-1$, 其中 d 为 u 进制串的长度。因此一旦 $\mathfrak{m}'$ 的范围边界无法被 u^d-1 的形式表达, 那么 $\mathfrak{m}'$ 范围就无法被精确证明。因此关键问题在于找到与秘密整数 $\mathfrak{m}'$ 的范围边界完全等价的表达形式。我们利用第 2.6 节的“分解”算法, 使得所有属于 $[0,\beta-\alpha]$ 的整数都有等价的比特串表达形式。首先令 $\gamma=\beta-\alpha$，$\delta_\gamma=\lceil\log_2\gamma+1\rceil$，$\gamma_i=\left\lfloor\frac{\gamma+2^{j-1}}{2^j}\right\rfloor$，以及 $\vec{h}_{1,\gamma}:=\gamma_1,\cdots,\gamma_{\delta_\gamma}\in\mathbb{Z}_q^{\delta_\gamma}$，其中 $j\in[1,\delta_\gamma]$。计算向量 $\vec{b}=\overrightarrow{\mathrm{idec}_P(\mathfrak{m}')}\in\{0,1\}^{\delta_\gamma}$，且 $\vec{h}_{1,\gamma}\cdot\vec{b}=c$。

然后, 我们考虑如何证明向量 $\vec{b}$ 为一个比特串, 这里使用的证明思想最早由 Bunz 等人在文献[28]中提出。其主要思想是: 如果整数 b_i 属于 $\{0,1\}$, 那么 b_i 一定满足 $b_i(b_i-1)=0$，推广到向量的形式, 则向量 $\vec{b}$ 一定满足 $\vec{b}\circ(\vec{b}-\vec{1})=\vec{0}$。

但是由于在证明关系 R_2 时, 不仅仅需要证明秘密整数 $\mathfrak{m}$ 的范围, 还要证明加密算法中的随机向量 $\vec{r}$ 各个分量的范围, 并且 $\vec{r}$ 各分量的范围要求与秘密整数 $\mathfrak{m}$ 的范围并不同。同样, 我们首先利用“分解技术”将随机向量 $\vec{r}$ “分解”为一个比特串。令 $P=p-1$，$\delta_P=\lceil\log_2 P+1\rceil$，$P_i=\left\lfloor\frac{P+2^{j-1}}{2^j}\right\rfloor$，其中 $j\in[1,\delta_P]$，

$$H_{n,P}:=\begin{bmatrix}P_1,\cdots,P_{\delta_P} & & & \\ & P_1,\cdots,P_{\delta_P} & & \\ & & \ddots & \\ & & & P_1,\cdots,P_{\delta_P}\end{bmatrix}\in\mathbb{Z}_q^{n\times n\delta_P}$$

。

计算向量 $\overrightarrow{\mathrm{vdec}_{n,P}(\vec{r})}\in\{0,1\}^{n\delta_P}$，且有以下等式:

$H_{n,P}\cdot\overrightarrow{\mathrm{vdec}_{n,P}(\vec{r})}=\vec{u}$。将上述的两个分解合并, 定义

$$\vec{g}=(0^n\|\ \alpha),\ \ \vec{y}'=\vec{y}-A'\cdot\vec{g},$$

$$H:=\begin{bmatrix} P_1,\cdots,P_{\delta_P} & & & & \\ & P_1,\cdots,P_{\delta_P} & & & \\ & & \ddots & & \\ & & & P_1,\cdots,P_{\delta_P} & \\ & & & & \gamma_1,\cdots,\gamma_{\delta_\gamma} \end{bmatrix},$$

$$\vec{x}''=(\overrightarrow{\mathrm{vdec}_{n,P}(\vec{r})}\|\overrightarrow{\mathrm{idec}_P(\mathfrak{m}')})\in\{0,1\}^{n\delta_P+\delta_\gamma},$$

$A''\coloneqq A'\cdot H\in\mathbb{Z}_q^{(m+1)\times(n\delta_P+\delta_\gamma)}$，有 $A''\cdot\vec{x}''=\vec{y}'$。

因此，证明者只需要证明拥有秘密向量 $\vec{x}''$ 满足 $A''\cdot\vec{x}''=\vec{y}'$，并且 $\vec{x}''\in\{0,1\}^{n\delta_P+\delta_\gamma}$。这里我们利用与文献[28]中提到的相似技术证明断言 R_3:

$$\mathrm{R}_3=\{((A'',\vec{y}'),\vec{x}''):A''\cdot\vec{x}''=\vec{y}'\mod q$$
$$\wedge\grave{x}(\grave{x}-\grave{1})=\grave{0}\}$$

上述 $\grave{x}\in\mathcal{R}_q$ 是秘密向量 $\vec{x}''$ 的 INTT 表达。

针对关系 R_3 我们利用了两个子协议分别证明 $A''\cdot\vec{x}''=\vec{y}'$ 和 $\grave{x}(\grave{x}-\grave{1})=\grave{0}$。在图 1 中给出了我们方案的框架，可以更加直观地看到证明的大致思想，便于理解。

接下来，我们对于图 1 中的证明框架进行简单说明。首先对于 $A''\cdot\vec{x}''=\vec{y}'$ 来说，可以非常简单地利用一个三轮的 Σ 协议作为一个子协议完成所需要的零知识证明。在这个子协议中 t 为验证者均匀随机抽取的挑战，$\vec{z}=\vec{v}+t\vec{x}$ 为证明者的回答，验证者验证 $A''\cdot\vec{z}\overset{?}{=}\vec{w}+t\vec{y}'$。通过这个子协议证明者向验证者证明了他知道一个向量 $\vec{x}''$ 满足:

$$A''\cdot\vec{x}''=\vec{y}'。$$

然后利用第二个子协议证明向量 $\vec{x}''$ 是一个比特串。在这个子协议中，证明者通过证明两个多项式: $\grave{z}(\grave{z}-\grave{t})$ 和 $\grave{v}^2+(2\grave{x}-1)\grave{t}\cdot\grave{v}$ 相等，去证明等式 $\grave{x}(\grave{x}-\grave{1})=\grave{0}$ 成立，其中 $\grave{z}$ 为向量 $\vec{z}$ 的 INTT 表达，$\grave{t}$ 为 t 的 INTT 表达。接下来，我们简述这个子协议的证明过程。因为 $\grave{z}=\grave{v}+\grave{t}\grave{x}$ 代入多项 $\grave{z}(\grave{z}-\grave{t})$ 中，可得:

$$\begin{aligned}&\grave{z}(\grave{z}-\grave{t})\\ =\ &(\grave{v}+\grave{t}\grave{x})(\grave{v}+\grave{t}(\grave{x}-1))\\ =\ &\grave{v}^2+(2\grave{x}-1)\grave{t}\grave{v}+\grave{t}^2(\grave{x}-1)\grave{x}\end{aligned}$$

$\mathcal{P}[A''\cdot\vec{x}''=\vec{y}']$
$\mathcal{V}[A'',\vec{y}']$
随机选取向量 $\vec{v}$，
计算 $\vec{w}=A''\cdot\vec{v}\ \xrightarrow{\vec{w}}$
$\xleftarrow{t}$ 随机选取挑战 t
计算 $\vec{w}=A''\cdot\vec{v}\ \xrightarrow{z}$ 验证: $A''\cdot\vec{z}\overset{?}{=}\vec{w}+t\vec{y}'$
随机选取向量 $\vec{r}$，计算承诺:
$\vec{c}=\mathrm{Commit}(\vec{r};\grave{v}^2\|(2\grave{x}-1)\grave{v})\ \xrightarrow{\vec{c}}$
$\xrightarrow{\vec{r}}$ 验证:
$\mathrm{Commit}(\vec{r};\grave{z}(\grave{z}-\grave{t}))$
$\overset{?}{=}\grave{c}_1+\grave{c}_2\grave{t}$

图 1 针对 Regev 加密方案的范围证明框架

Figure 1 Framework of range proof for regev's encryption scheme

所以在验证者随机选取挑战 $\grave{t}$ 时，如果证明者能够证明等式 $\grave{z}(\grave{z}-\grave{t})=\grave{v}^2+(2\grave{x}-1)\grave{t}\grave{v}$ 成立，就可以说明等式 $\grave{x}(\grave{x}-1)=0$ 成立。

但是以上的证明不是零知识的，因为验证者在验证等式 $\grave{z}(\grave{z}-\grave{t})=\grave{v}^2+(2\grave{x}-1)\grave{t}\grave{v}$ 是否成立，需要计算 $\grave{v}^2+(2\grave{x}-1)\grave{t}\grave{v}$，如果证明者直接发送 $\grave{v}$ 和 $\grave{x}$ 就会泄露证据。因此如何在验证者不知道这两个元素的值的同时又能够接收等式 $\grave{z}(\grave{z}-\grave{t})=\grave{v}^2+(2\grave{x}-1)\grave{t}\grave{v}$ 成立？在我们的方案中用了一个很简单的解决方法——利用一个加法同态的承诺方案完成上述的证明。简单的想法就是证明者将需要验证者计算需要用到的值先进行承诺，然后将承诺发送给验证者。例如: 我们可以将 $\grave{v}^2$ 和 $(2\grave{x}-1)\grave{v}$ 的承诺发送给验证者，因为 $\grave{t}$ 是验证者选取的挑战值，$\grave{z}$ 为证明者对 $\grave{t}$ 的回答，因此验证者是知道这两个值的。所以可以通过计算判断多项式 $\grave{z}(\grave{z}-\grave{t})$ 和 $\grave{v}^2+(2\grave{x}-1)\grave{t}\grave{v}$ 是否相等。

显然，这样简单构造的方案依然没有达到零知识的性质。原因是如果我们利用一个简单的承诺方案构造证明协议，那么在承诺的打开阶段，证明者依然需要发送被承诺值 $\grave{v}^2$ 和 $(2\grave{x}-1)\grave{v}$，还有承诺所用到的随机数 $\vec{r}$ 给验证者进行验证承诺是否正确。为了解决上述问题，我们利用文献[43]中的零知识承诺打开协议构造出一个零知识交互协议，使得证明者在零知识的情况下能够让验证者验证承诺的打开。

其证明的过程与一个 Σ 协议类似, 因此第二个子协议也是一个三轮的零知识证明协议, 并且有在多项式时间内运行的精确提取器。

为了简化证明过程, 减少需要被承诺的值, 我们可以用 x 替换 $z(z-t)$ 中左边的 z。通过计算可以得到:

$$\begin{aligned} & x(z-t) \\ = \quad & x(v+t(x-1)) \\ = \quad & xv+x(x-1)t \end{aligned}$$

在这种情况下, 证明者只需要计算 x, v, xv 三个值的承诺。

3.3 针对 Regev 加密方案的范围证明

本部分中, 利用第二章中描述的辅助承诺算法, 我们构造了一个针对 Regev 经典加密方案的范围证明协议。完整的构造过程如下:

协议 1

公共输入:

$(A,\vec{b}=A^T\vec{s}+\vec{e})\in\mathbb{Z}_q^{m\times n}\times\mathbb{Z}_q^n$, $(\vec{u},c)\in\mathbb{Z}_q^m\times\mathbb{Z}_q$, 承诺公钥 $B=(\vec{b}_1,\cdots,\vec{b}_4)\in\mathcal{R}_q^{4\times 5}$。

证明者 $\mathcal{P}$ 私钥:

$$\vec{r}\in\{0,\cdots,p-1\}^n\wedge \mathfrak{m}\in[\alpha,\beta]\}。$$

证明的断言:

$$\mathrm{R}_3=\{((A'',\vec{y}'),\vec{x}''):A''\cdot\vec{x}''=\vec{y}' \mod q \wedge x(x-1)=0\}。$$

生成证明:

第一轮: 定义 $m'=m+1$, $n'=n\delta_P+\delta_\gamma$ 首先证明者 $\mathcal{P}$ 按照之前的描述计算出 $A''\in\mathbb{Z}_q^{m'\times n'}$, $\vec{y}'\in\mathbb{Z}_q^{m'}$ 以及秘密 $\vec{x}''\in\{0,1\}^{n'}$。

证明者 $\mathcal{P}$ 在均匀分布 $\mathcal{R}_q$ 中随机选取一个随机数 $v\xleftarrow{\$}\mathcal{R}_q$, 以及在 $\mathcal{X}^{5n'}$ 中随机选取一个向量 $\vec{r}\xleftarrow{\$}\mathcal{X}^{5n'}$。并且 $\mathcal{P}$ 利用辅助承诺计算向量 $\vec{m}=(v\|x\|vx)$ 的承诺 $\vec{c}$ 以及向量 $\vec{w}$:

$$\vec{c}=COM(v\|x\|vx)=B\cdot\vec{r}+(0\|v\|x\|vx)^T,$$

$$\vec{w}=A''\vec{v}。$$

$$\mathcal{P}\to\mathcal{V}:\vec{c},\vec{w}。$$

第二轮: 验证者 $\mathcal{V}$ 随机选取第一个挑战:

$$t\xleftarrow{\$}\mathbb{Z}_q,$$

$$\mathcal{V}\leftarrow\mathcal{P}:t。$$

第三轮: 证明者 $\mathcal{P}$ 根据验证者 $\mathcal{V}$ 的挑战, 做出相应的回答 z。并且随机选取向量 $\vec{v}'\xleftarrow{\$}D_\sigma^{5n'}$, $\mathcal{P}$ 计算回答 z、w' 以及辅助信息 x_1、x_2:

$$z=v+tx,$$

$$w'=\vec{b}_1^T\vec{v}',$$

$$x_1=(\vec{b}_2^T+t\vec{b}_3^T)\vec{v}',$$

$$x_2=((z-t\cdot 1)\vec{b}_3^T-\vec{b}_4^T)\vec{v}'。$$

$$\mathcal{P}\to\mathcal{V}:z,w',x_1,x_2。$$

第四轮: 验证者 $\mathcal{V}$ 随机选取第二个挑战:

$$f\xleftarrow{\$}\mathcal{C},$$

$$\mathcal{V}\leftarrow\mathcal{P}:f。$$

第五轮: 证明者 $\mathcal{P}$ 根据验证者 $\mathcal{V}$ 的挑战, 做出相应的回答 $\vec{z}'$, 计算 $\vec{z}'$:

$$\vec{z}'=\vec{v}'+f\vec{r},$$

并且调用 Reject$(\vec{z},\vec{v},\sigma)$ 算法, 如果算法输出为 1, 则退出协议, 否则继续。

$$\mathcal{P}\to\mathcal{V}:\vec{z}'。$$

验证者 $\mathcal{V}$ 验证:

验证者 $\mathcal{V}$ 首先按照协议计算出 $A''\in\mathbb{Z}_q^{(m+1)\times(n\delta_P+\delta_\gamma)}$ 以及 $\vec{y}'\in\mathbb{Z}_q^{(m+1)}$。$\mathcal{V}$ 接受证明, 当且仅当:

$$\left\|\vec{z}'\right\|_2\leqslant\sigma\sqrt{10n'},$$

$$A''\vec{z}=\vec{w}+t\vec{y}',$$

$$\vec{b}_1^T\vec{z}'=w'+fc_1,$$

$$(\vec{b}_2^T+t\vec{b}_3^T)\vec{z}'+fz=x_1+f(c_2+tc_3),$$

$$((z-t)\vec{b}_3^T-\vec{b}_4^T)\vec{z}'=x_2+f((z-t)c_3-c_4)。$$

3.4 协议 1 的安全性分析

在本部分中, 我们针对协议 1 进行安全性证明。

引理 5. 如果辅助承诺方案是安全的, 则协议 1 是一个合理性错误为 $1-1/ql$, 且有有效抽取器的诚实验证者范围证明协议。

证明: 根据定义我们需要证明协议 1 满足以下的三个性质:

完备性: 首先根据引理 2, 我们可以易知证明者将以概率 $\approx 1/12$ 回答, 因此协议的完备性错误约为 11/12。如果协议没有中止, 且证明者是诚实的, 那么证明者的回答 z 和 $\vec{z}'$ 一定满足:

$$A''\vec{z}=\vec{w}+t\vec{y}',$$

$$\vec{b}_1^T\vec{z}' = w' + f c_1,$$

$$(\vec{b}_2^T + t\vec{b}_3^T)\vec{z}' + fz = x_1 + f(c_2 + tc_3),$$

$((z-t)\vec{b}_3^T - \vec{b}_4^T)\vec{z}' = x_2 + f((z-t)c_3 - c_4)$。对于 $\vec{z}'$ 范数的判断可知，有极大的概率通过 $\left\|\vec{z}'\right\|_2 \leqslant \sigma\sqrt{10n'}$ 的验证。

特殊的合理性: 因为第一个挑战的挑战空间为 q，第二个挑战的挑战空间为 l，因此我们范围证明的合理性错误为 $1-1/ql$。

假设通过重绕协议，我们得到四个通过验证者验证的副本:

$$(\vec{c}, \vec{w}, t_1, z_1, w_1', x_{1,1}, x_{1,2}, f_{1,1}, \vec{z}_{1,1}),$$

$$(\vec{c}, \vec{w}, t_1, z_1, w_1', x_{1,1}, x_{1,2}, f_{2,1}, \vec{z}_{2,1}),$$

$$(\vec{c}, \vec{w}, t_2, z_2, w_2', x_{2,1}, x_{2,2}, f_{1,2}, \vec{z}_{1,2}),$$

$$(\vec{c}, \vec{w}, t_2, z_2, w_2', x_{2,1}, x_{2,2}, f_{2,2}, \vec{z}_{2,2})。$$

首先，我们利用上述的第一个和第三个副本，证明第一个子协议的知识证明。由 $A''\cdot\vec{z}_1 = \vec{w} + t_1\cdot\vec{y}'$ 以及 $A''\cdot\vec{z}_2 = \vec{w} + t_2\cdot\vec{y}'$，可知

$$\frac{\vec{z}_1 - \vec{z}_2}{t_1 - t_2} = \vec{x}。$$

其中 $\vec{z}_1$ 和 $\vec{z}_2$ 分别为 z_1，z_2 的 NTT 表达(快速数论变换)。

然后，利用第二个子协议，我们可以证明向量 $\vec{s}$ 为 0, 1 比特串。令 $\vec{z}_i' = \vec{z}_{i,1}' - \vec{z}_{i,2}'$ 以及 $\overline{f}_i = f_{i,1} - f_{i,2}$，$i = 1,2$。因为 $\vec{b}_1^T\vec{z}_{i,j}' = w' + f_{i,j}c_1$，$j = 1,2$，可得 $\vec{b}_1^T\vec{z}_i' = \overline{f}_i c_1$。同时利用文献[43]中已经证明的结论，得到承诺 c_2，c_3 和 c_4 的打开 m_2，m_3，m_4 为:

$$m_k = c_k - \vec{b}_k^T\cdot\frac{\vec{z}_1'}{\overline{f}_1}。$$

根据承诺的绑定性，可知:

$$m_k = m_k' = c_k - \vec{b}_k^T\cdot\frac{\vec{z}_2'}{\overline{f}_2}。$$

根据 $(\vec{b}_2^T + t_i\vec{b}_3^T)\vec{z}_{i,j}' + f_{i,j}z_1 = x_{1,1} + f_{i,j}(c_2 + t_i c_3)$，可得:

$$(\vec{b}_2^T + t_i\vec{b}_3^T)\cdot\frac{\vec{z}_i'}{\overline{f}_i} + z_1 = c_2 + t_i c_3。$$

根据承诺 $c_2 + t_i c_3$ 的打开，我们可以得到:

$$m_2 + t_i m_3 = c_2 + t_i c_3 - (\vec{b}_2^T + t_i\vec{b}_3^T)\cdot\frac{\vec{z}_i'}{\overline{f}_i}。$$

因此 $z_1 = m_2 + t_i m_3 = v + t_i x$。得到 $m_2 = v$，$m_3 = x$。

由以下等式:

$$((z_1 - t_i)\vec{b}_3^T - \vec{b}_4^T)\vec{z}_{i,j}' = x_{1,2} + f_{i,j}((z_1 - t_i)c_3 - c_4)$$

可知，$(z_1 - t_i)c_3 - c_4$ 为 0 的承诺，即 $(z_1 - t_i)x - m_4 = 0$。将 $z_1 = m_2 + t_i m_3 = v + t_i x$ 代入上式中，得到:

$$\begin{aligned}&(z_1 - t_i)x - m_4\\ =\ &(v + t_i(x-1))x - m_4\\ =\ &(x-1)x\cdot t_i + vx - m\\ =\ &0\end{aligned}$$

因为挑战 t_i 是由诚实验证者随机均匀抽取的，因此由上述等式可知 $(x-1)x = 0$。

综上所述，我们能够构造出一个多项式时间内的抽取器，抽取出秘密向量 $\vec{x}$ 并且 $\vec{x}$ 的所有分量都属于 $\{0,1\}$。

诚实验证者零知识性: 首先因为我们的构造方案会有 $\approx 11/12$ 的概率中止协议。因此，在这个证明中我们考虑的是模拟一个在诚实证明者 $\mathcal{P}$ 和诚实验证者 $\mathcal{V}$ 之间交互没有中止的副本，模拟器 $\mathcal{S}$ 进行如下操作:

首先因为 $\mathcal{P}$ 随机均匀抽取了 v，因此 $z = v + tx$ 是均匀随机的。而且根据引理 2，$\vec{z}'$ 与 D_σ^{5n} 中随机抽取的向量是统计不可区分的。因此模拟器 $\mathcal{S}$ 可以简单地抽取 $z \xleftarrow{\$} \mathcal{R}_q$ 以及 $\vec{z}' \xleftarrow{\$} D_\sigma^{5n}$。因为诚实验证者 $\mathcal{V}$ 是随机均匀随机抽取的两个挑战，因此 $\mathcal{S}$ 从 t 和 f 挑战空间随机均匀抽取。由承诺的隐藏性可知，承诺 $\vec{c}$ 可以由 $\mathcal{S}$ 从承诺空间 $\mathcal{R}_q^4$ 中随机均匀抽取。然后剩下的交互副本 $\vec{w}$，w'，x_1 和 x_2 都可以由以上随机均匀抽取的值计算得到。因此，输出的副本可以通过验证者 $\mathcal{V}$ 的验证。综上所述，由模拟器 $\mathcal{S}$ 得到的副本与 $\mathcal{P}$ 和 $\mathcal{V}$ 之间的交互副本是不可区分的。因此，我们的协议具有零知识性。

3.5 协议 1 的证明长度

在本部分中，我们给出了协议 1 执行一次的通信量，即协议 1 的证明长度。通信副本为:

$(\vec{c},\vec{w},t,\grave{z},\overrightarrow{\grave{w}},\grave{x}_1,\grave{x}_2,\grave{f},\vec{z})$。其中 $\vec{c}\in\mathcal{R}_q^4$ 为承诺的向量, $\vec{w}\in\mathbb{Z}_q^{n'}$, $t\in\mathbb{Z}_q$ 为诚实验证者 $\mathcal{V}$ 的第一个挑战, $\grave{z}\in\mathcal{R}_q$ 为证明者 $\mathcal{P}$ 的一个回答, $\overrightarrow{\grave{w}},\grave{x}_1,\grave{x}_2\in\mathcal{R}_q$, $\grave{f}\in\mathcal{C}$ 为 $\mathcal{V}$ 的第二个挑战, $\vec{\grave{z}}\in\mathcal{R}$ 为 $\mathcal{P}$ 的一个回答。易知在 $\mathbb{Z}_q$ 中的元素需要 $\log q$ 个比特表示, 在 $\mathcal{R}_q$ 中的元素, 我们可以用 $n'\log q$ 个比特表示, 而挑战 $\grave{f}$ 也可以用 $\log q$ 比特表示。因为 $\vec{\grave{z}}\in\mathcal{R}$ 的分量是符合离散高斯分布的, 所以对于各个分量小于 6σ 的概率至少为 $1-2^{-24}$ [41]。因此, $\vec{\grave{z}}$ 需要 $5n'\lceil\log(12\sigma)\rceil$ 比特。协议 1 的证明长度为:

$$(8n\delta_P+m+8\delta_\gamma+3)\lceil\log q\rceil+5(n\delta_P+\delta_\gamma)\lceil\log(12\sigma)\rceil$$

比特。

4 针对 KTX08 承诺方案的范围证明

KTX08 承诺方案是 Kawachi、Tanaka 和 Xagawa 在 2008 年提出的一个基于 SIS 假设的高效承诺方案[34]。本文我们采用的是在文献[29]中提到的 KTX08 承诺方案的变型, 并且针对这个承诺方案构造了一个高效的范围证明协议。

4.1 回顾 KTX08 承诺方案

首先, 我们先简单介绍一下 KTX08 承诺方案。承诺方案由三个算法(KeyGen, Commit, Verify)组成, 以下为具体的算法:

- $\text{KeyGen}(1^\lambda)\to(\vec{a}_0,\cdots,\vec{a}_k,\vec{b}_0,\cdots,\vec{b}_n)$ 算法输出承诺公钥 $\vec{a}_0,\cdots,\vec{a}_k$, $\vec{b}_0,\cdots,\vec{b}_n$, 且 $a_i,b_i\in\mathbb{Z}_q^m$。
- $\text{Commit}(\vec{a}_0,\cdots,\vec{a}_k,\vec{b}_0,\cdots,\vec{b}_n,\vec{s})\to\vec{c}$ 被承诺值的空间为 $\vec{s}\in\{0,1\}^{k+1}$, 承诺方 $\mathcal{S}$ 在 $\{0,1\}^{n+1}$ 中随机抽取一个比特串 $\vec{r}=(r_0,\cdots,r_n)$。计算承诺 $\vec{c}\in\mathbb{Z}_q^m$:

$$\vec{c}=\sum_{i=0}^{k}\vec{a}_i\cdot s_i+\sum_{j=0}^{n}\vec{b}_j\cdot r_j \mod q,$$

并且将 $\vec{c}$ 发送给接收方 $\mathcal{R}$。

- $\text{Verify}(\vec{a}_0,\cdots,\vec{a}_k,\vec{b}_0,\cdots,\vec{b}_n,\vec{s},\vec{c},\vec{r})\to b$ 承诺方 $\mathcal{S}$ 将被承诺值 $\vec{s}$ 与随机比特串 $\vec{r}$ 发送给接收方 $\mathcal{R}$。接收方 $\mathcal{R}$ 收到 $\vec{s}$ 和 $\vec{r}$ 之后, 首先验证 $\vec{s}$ 与 $\vec{r}$ 是否分别在 $\{0,1\}^{k+1}$ 和 $\{0,1\}^{n+1}$ 中, 并且验证:

$$\sum_{i=0}^{k}\vec{a}_i\cdot s_i+\sum_{j=0}^{n}\vec{b}_j\cdot r_j \mod q\overset{?}{=}\vec{c}。$$

如果通过验证, 则输出 1, 否则输出 0。

同样对于以上加密方案的正确性、安全性以及相关参数的选取, 可以参考文献[34], 这里不再赘述。

4.2 针对 KTX08 承诺方案的范围证明构造思想

对于本部分中的承诺方案构造的范围证明的关系 R 可以记作: 关系{(公共输入; 证据): 满足的关系}。与第三章中所证明的关系不同的是, 因为本部分我们针对的承诺方案是一个可以对比特串进行承诺的方案。因此在构造范围证明时, 我们需要证明的是一个向量中的所有分量的范围。因此也可以记作: {(公共参数, 承诺 $\vec{c}$; 被承诺值 $\vec{m}$, 随机数 $\vec{r}$): $\vec{c}$=Com($\vec{m}$,$\vec{r}$) $\wedge$ $\vec{m}$ 属于某一给定区间}。

同时, 在 KTX08 承诺方案承诺一个秘密整数 a 时, 首先需要得到 a 二进制表达的向量, 记为: $\vec{x}'=(x_0',\cdots,x_r')$, 其中 $r=\lfloor\log a\rfloor$, 有 $a=\sum_{i=0}^{r}2^i\cdot x_i'$。因此上述承诺可以用于承诺非常大的整数值, 即被承诺值 a 可以大于 q。在我们构造的范围证明方案中, 为了防止泄露被承诺值的信息, 被承诺的秘密向量是定长的, 我们定义秘密向量的长度为 k, 在被承诺值的二进制表达的向量长度小于 k 时, 我们用 0 填充, 可以得到 $\vec{x}=(\vec{x}'\|0^{k-r})\in\mathbb{Z}_q^k$。

假设需要证明范围为 $[0,2^d]$, 其中 $k>d\geqslant r$。在本方案中, 首先证明者 $\mathcal{P}$ 通过一个简单的 Σ 协议向验证者 $\mathcal{V}$ 证明他知道一个秘密向量 $\vec{x}$, 并且 $\vec{x}$ 满足 $A\cdot\vec{x}=\vec{c} \mod q$, 并且 $\mathcal{P}$ 也要向 $\mathcal{V}$ 证明等式 $x_i(x_i-1)=0$ 成立, 来说明向量 $\vec{x}$ 是一个比特串。最后需要证明秘密向量 $\vec{x}$ 的后 $k-d+1$ 个分量为 0, 即证明整数 $a\in[0,2^d]$, 即给出如下关系 R_4 的零知识证明协议。

$$\mathrm{R}_4=\{((A,\vec{c}),\vec{x}):A\cdot\vec{x}=\vec{c} \mod q\wedge\vec{x}^\circ(\vec{x}-\vec{1})=\vec{0}$$
$$\wedge x_j=0,\ j\in[n+d+1,n+k+1]\}$$

其中 $A=(\vec{b}_0,\cdots,\vec{b}_n,\vec{a}_0,\cdots,\vec{a}_k)$, $\vec{x}=(\vec{r}\|\vec{s})$。

针对 KTX08 承诺方案的范围证明协议的构造框架与第 3.3 节给出的协议构造框架类似, 因此这里不再赘述。

4.3 针对 KTX08 承诺方案的范围证明

接下来我们将直接给出针对 KTX08 承诺方案的范围证明协议的具体构造, 定义 $n'=n+k+2$:

协议 2

公共输入:

$A=(\vec{b}_0,\cdots,\vec{b}_n,\vec{a}_0,\cdots,\vec{a}_k)\in\mathbb{Z}_q^{m\times n'}$, $\vec{c}\in\mathbb{Z}_q^m$, 承诺

公钥 $B=(\vec{b}_1,\cdots,\vec{b}_4)\in\mathcal{R}_q^{4\times5}$。

证明者私钥:

$$\vec{x}=(\vec{r}\|\vec{s})\in\{0,1\}^{n'}。$$

证明的断言:

$$\mathrm{R}_4=\{((A,\vec{c}),\vec{x}):A\cdot\vec{x}=\vec{c}\mod q\wedge\vec{x}\circ(\vec{x}-\vec{1})=\vec{0}\wedge x_j=0,\ j\in[n+d+1,n+k+1]\}。$$

生成证明:

第一轮:证明者 $\mathcal{P}$ 在均匀分布 $\mathcal{R}_q$ 中随机选取四个随机向量 $\vec{v}'\xleftarrow{\$}\mathbb{Z}_q^{n+d+1}$，定义 $\vec{v}=(\vec{v}'\|0^{k-d+1})\in\mathbb{Z}_q^{n+k+1}$。以及选取随机向量 $\vec{r}$。并且 $\mathcal{P}$ 利用辅助承诺得到相应的承诺 $\vec{c}$，$\mathcal{P}$ 计算:

$$\vec{w}=A\cdot\vec{v},$$

$$\vec{c}=COM(v\|x\|vx;\vec{r})$$

$$\mathcal{P}\to\mathcal{V}:\vec{w},\vec{c}。$$

第二轮: 验证者 $\mathcal{V}$ 随机选取第一个挑战:

$$t\xleftarrow{\$}\mathbb{Z}_q,$$

$$\mathcal{V}\leftarrow\mathcal{P}:t。$$

第三轮: 证明者 $\mathcal{P}$ 根据验证者 $\mathcal{V}$ 的挑战，做出相应的回答 $\vec{z}$。并且随机选取向量 $\vec{v}'\xleftarrow{\$}D_\sigma^{n'}$，$\mathcal{P}$ 计算回答 $\vec{z}$、w' 以及辅助信息 y_1、y_2:

$$\vec{z}=\vec{v}+t\cdot\vec{x},$$

$$w_1'=\vec{b}_{i,1}^T\cdot\vec{v}'_i,$$

$$y_1=(\vec{b}_2^T+t\vec{b}_3^T)\vec{v}',$$

$$y_2=((z-t\cdot1)\vec{b}_3^T-\vec{b}_4^T)\vec{v}'。$$

$$\mathcal{P}\to\mathcal{V}:\vec{z},w',y_1,y_2。$$

第四轮: 验证者 $\mathcal{V}$ 随机选取第二个挑战:

$$f\xleftarrow{\$}\mathcal{C},$$

$$\mathcal{V}\leftarrow\mathcal{P}:f。$$

第五轮: 证明者 $\mathcal{P}$ 根据验证者 $\mathcal{V}$ 的挑战，做出相应的回答 $\vec{z}'$，计算 $\vec{z}'$:

$$\vec{z}'=\vec{v}'+f\vec{r},$$

并且调用 Reject$(\vec{z},\vec{v},\sigma)$ 算法，如果算法输出为 1，则退出协议，否则继续。

$$\mathcal{P}\to\mathcal{V}:\vec{z}'。$$

验证:

验证者 $\mathcal{V}$ 接受证明，当且仅当:

$$z_i=0,\ i=n+d+1,\cdots,n+k+1,$$

$$\left\|\vec{z}'\right\|_2\leqslant\sigma\sqrt{10n'},$$

$$A\cdot\vec{z}=\vec{w}+t\vec{c},$$

$$\vec{b}_1^T\vec{z}'=w'+fc_1,$$

$$(\vec{b}_2^T+t\vec{b}_3^T)\vec{z}'+fz=x_1+f(c_2+tc_3),$$

$$((z-t)b_3^T-b_4^T)\vec{z}'=x_2+f((z-t)c_3-c_4)。$$

4.4 协议 2 的安全性分析

引理 6.如果辅助承诺方案是安全的，则协议 2 是一个合理性错误为 $1-1/ql$，且有有效抽取器的诚实验证者范围证明协议。

安全性证明与第三章中协议的安全性证明相似。

完备性: 易知，如果协议没有中止，且证明者 $\mathcal{P}$ 是诚实的，那么 $\mathcal{P}$ 的回答一定能够通过验证者 $\mathcal{V}$ 的验证。

特殊的合理性: 因为第一个挑战的挑战空间为 q，第二个挑战的挑战空间为 l，因此我们范围证明的合理性错误为 $1-1/ql$。

通过重绕协议，我们可以得到需要的四个副本完成证明:

$$(\vec{c},\vec{w},t_1,z_1,w_1',x_{1,1},x_{1,2},f_{1,1},\vec{z}_{1,1}),$$

$$(\vec{c},\vec{w},t_1,z_1,w_1',x_{1,1},x_{1,2},f_{2,1},\vec{z}_{2,1}),$$

$$(\vec{c},\vec{w},t_2,z_2,w_2',x_{2,1},x_{2,2},f_{1,2},\vec{z}_{1,2}),$$

$$(\vec{c},\vec{w},t_2,z_2,w_2',x_{2,1},x_{2,2},f_{2,2},\vec{z}_{2,2})。$$

首先，我们利用上述的第一个和第三个副本，证明存在向量 $\vec{x}$ 满足 $A\cdot\vec{x}=\vec{c}$。

由 $A''\cdot\vec{z}_1=\vec{w}+t_1\cdot\vec{c}$ 以及 $A''\cdot\vec{z}_2=\vec{w}+t_2\cdot\vec{c}$，可知:

$$\frac{\vec{z}_1-\vec{z}_2}{t_1-t_2}=\vec{x}。$$

因为当 $j=1,2$，$i=n+d+1,\cdots,n+k+1$ 时 $z_{j,i}=0$，所以可易知在向量 $\vec{x}$ 中，$x_i=0$，当 $i=n+d+1,\cdots,n+k+1$ 时。

然后，利用第二个子协议的四个副本:

$$(\vec{c},w_1',x_{1,1},x_{1,2},f_{1,1},\vec{z}_{1,1}),$$

$$(\vec{c},w_1',x_{1,1},x_{1,2},f_{2,1},\vec{z}_{2,1}),$$

$$(\vec{c},w_2',x_{2,1},x_{2,2},f_{1,2},\vec{z}_{1,2}),$$

$$(\vec{c},w_2',x_{2,1},x_{2,2},f_{2,2},\vec{z}_{2,2})。$$

我们可以证明向量 $\vec{s}$ 为 0，1 比特串。令 $\vec{z}'_i=\vec{z}'_{i,1}-\vec{z}'_{i,2}$ 以及 $\overline{f}_i=f_{i,1}-f_{i,2}$，$i=1,2$。因为

$\vec{b}_1^T\vec{z}'_{i,j} = w' + f_{i,j}c_1$, $j=1,2$, 可得 $\vec{b}_1^T\vec{z}'_i = \overline{f}_i c_1$。利用文献[43]中已经证明的结论, 得到承诺 c_2, c_3 和 c_4 的打开 m_2, m_3, m_4 为:

$$m_k = c_k - \vec{b}_k^T \cdot \frac{\vec{z}'_1}{\overline{f}_1}。$$

由承诺的绑定性, 可以得到:

$$m_k = m'_k = c_k - \vec{b}_k^T \cdot \frac{\vec{z}'_2}{\overline{f}_2}。$$

根据 $(\vec{b}_2^T + t_i\vec{b}_3^T)\vec{z}'_{i,j} + f_{i,j}z_1 = x_{1,1} + f_{i,j}(c_2 + t_i c_3)$, 可以得到:

$$(\vec{b}_2^T + t_i\vec{b}_3^T)\cdot\frac{\vec{z}'_i}{\overline{f}_i} + z_1 = c_2 + t_i c_3,$$

同时根据承诺 $c_2 + t_i c_3$ 的打开, 得到:

$$m_2 + t_i m_3 = c_2 + t_i c_3 - (\vec{b}_2^T + t_i\vec{b}_3^T)\cdot\frac{\vec{z}'_i}{\overline{f}_i}。$$

因此 $z_1 = m_2 + t_i m_3 = v + t_i x$。得到 $m_2 = v$, $m_3 = x$。

由以下等式:

$$((z_1 - t_i)b_3^T - b_4^T)\vec{z}_{i,j'} = x_{1,2} + f_{i,j}((z_1 - t_i)c_3 - c_4)$$

可知, $(z_1 - t_i)c_3 - c_4$ 为 0 的承诺, 即 $(z_1 - t_i)x - m_4 = 0$。将 $z_1 = m_2 + t_i m_3 = v + t_i x$ 代入上式中, 得到:

$$\begin{aligned}&(z_1 - t_i)x - m_4\\ =\ &(v + t_i(x-1))x - m_4\\ =\ &(x-1)x\cdot t_i + vx - m\\ =\ &0\end{aligned}$$

因为挑战 t_i 是由诚实验证者随机均匀抽取的, 因此由上述等式可知 $(x-1)x = 0$。

综上所述, 我们能够构造出一个多项式时间内的抽取器, 抽取出秘密向量 $\vec{x}$, 并且 $\vec{x}$ 是一个比特串, $x_i = 0$, $i = n+d+1, \cdots, n+k+1$。

诚实验证者零知识性: 首先因为我们的构造方案会有一定的概率中止协议。因此, 在这个证明中我们考虑的是模拟一个在诚实证明者 $\mathcal{P}$ 和诚实验证者 $\mathcal{V}$ 之间交互没有中止的副本, 模拟器 $\mathcal{S}$ 进行如下操作:

首先, 因为 $\mathcal{P}$ 随机均匀抽取了 $\vec{v}'$, 因此 $\vec{z}' = \vec{v}' + t\cdot\vec{x}'$ 是均匀随机的。而且根据引理 2, $\vec{z}'$ 与随机抽取的向量是统计不可区分的。因此模拟器 $\mathcal{S}$ 可以简单地抽取 $\vec{z} \xleftarrow{\$} \mathbb{Z}_q^{n+d+1}$ 以及 $\vec{z}' \xleftarrow{\$} D_\sigma^{n'}$, 定义 $\vec{z} = (\vec{z}' \| 0^{k-d+1})$。因为诚实验证者 $\mathcal{V}$ 是随机均匀随机抽取的两个挑战, 因此 $\mathcal{S}$ 从 t 和 f 挑战空间随机均匀抽取。由承诺的隐藏性可知, 承诺 $\vec{c}$ 可以由 $\mathcal{S}$ 从承诺空间中随机均匀抽取。然后剩下的交互副本 $\vec{w}$, w' 和 y_1, y_2 都可以由以上随机均匀抽取的值计算得到。因此, 输出的副本可以通过验证者 $\mathcal{V}$ 的验证。综上所述, 由模拟器 $\mathcal{S}$ 得到的副本与 $\mathcal{P}$ 和 $\mathcal{V}$ 之间的交互副本是不可区分的。因此, 我们的协议具有零知识性。

接下来我们将针对 KTX08 承诺方案构造的范围证明方案与文献[29]中同样针对 KTX08 承诺方案构造的范围证明方案进行对比。在文献[29]的范围证明中, 证明长度为:

$$(3n + 2(k+1+m))\lceil \log q \rceil + 3m + 23(k+1)$$

比特, 其中 $k \approx poly(n)$, $m \approx n\log q$。但是该方案的合理性错误很大$(2/3)$, 并且不会随着参数选取的变化而变化。因此该方案如果想要达到可忽略的合理性错误, 就需要将协议重复执行很多次。在表 3 中我们给出了协议 2 与文献[29]范围证明协议的具体比较, 可以看出在相同情况下, 协议 2 的通信量明显小于文献[29]中协议的通信量。

4.5 协议 2 的证明长度

在本部分中, 我们给出了协议 2 执行一次的通信量。通信副本为: $(\vec{c}, \vec{w}, t, z, \vec{w}, y_1, y_2, f, \vec{z})$。证明长度与第三章相似的计算过程, 此处不再赘述。协议 2 的证明长度为: $(8n + 8k + m + 18)\lceil \log q \rceil + 5(n+k+2)\lceil \log(12\sigma) \rceil$ 比特。

5 效率分析

我们将本文的范围证明方案的效率与目前已有的范围证明方案[29]进行对比。因为文献[29]的方案针对的是较大的秘密整数的范围证明, 而本文针对 Regev 加密方案的范围证明针的是较小秘密整数的范围证明, 即被证明整数 a 满足 $a < q$, 因此该方案效率无法与文献[29]的方案进行横向比较。在效率方面无法进行很好的说明, 因此在这里不进行比较。但是本文针对 Regev 加密方案的范围证明的合理性错误也较小, 因此也可以说明其效率较高。并且该方案是目前我们已知的唯一针对较小秘密整数基于格的范围证明。

表 3 协议 2 与文献[9]中协议通信量的对比

Table 3 Comparison of Communication Costs between Protocol 2 and Protocol in Reference [9]

协议	协议 2		文献[29]协议	
方案合理性错误	2^{-56}	2^{-128}	2^{-56}	2^{-128}
n	256	1024	256	1024
k	256	1024	256	1024
$\lceil \log q \rceil$	15	30	15	30
重复协议次数	3	4	96	219
通信量(比特)	4.5×10^5	6.2×10^6	1.4×10^7	4.6×10^8

6 总结

目前已知的抗量子范围证明方案屈指可数, 并且这些方案并不十分高效。针对这种情况, 我们利用了文献[32]中提出的一个基于格的零知识证明协议的框架和思想, 分别提出了针对 Regev 加密方案和针对 KTX08 承诺方案的两个范围证明协议。

虽然我们提出的基于格的范围证明方案比现有的抗量子方案更高效, 但是相比于目前最高效的基于经典数论假设构造的范围证明方案——Bulletproofs, 我们的方案在证明长度、验证者验证时间上还有一定的差距。并且基于格的范围证明方案都只能证明秘密整数属于连续的非负整数区间。因此如何构造能够证明负整数区间的基于格假设的范围证明方案, 并且进一步提升方案效率, 是我们下一步的工作方向。

参考文献

[1] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof-Systems[C]. *The seventeenth annual ACM symposium on Theory of computing - STOC '85*, 1985: 291-304.

[2] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof Systems[J]. *SIAM Journal on Computing*, 1989, 18(1): 186-208.

[3] Brickell E F, Chaum D, Damgård I B, et al. Gradual and Verifiable Release of a Secret (Extended Abstract)[M]. Advances in Cryptology —CRYPTO '87. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988: 156-166.

[4] Damgård I B. Practical and Provably Secure Release of a Secret and Exchange of Signatures[J]. *Journal of Cryptology*, 1995, 8(4): 201-222.

[5] Fujisaki E, Okamoto T. Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations[M]. Advances in Cryptology — CRYPTO '97. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997: 16-30.

[6] Boudot F. Efficient Proofs that a Committed Number Lies In an Interval[M]. Advances in Cryptology — EUROCRYPT 2000. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000: 431-444.

[7] Rabin M O, Shallit J O. Randomized Algorithms In Number Theory[J]. *Communications on Pure and Applied Mathematics*, 1986, 39(S1): S239-S256.

[8] Lipmaa H. On Diophantine Complexity and Statistical Zero-Knowledge Arguments[M]. Advances in Cryptology - ASIACRYPT 2003. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 398-415.

[9] Groth J. Non-Interactive Zero-Knowledge Arguments for Voting[M]. Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 467-482.

[10] Fiat A, Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[M]. Advances in Cryptology — CRYPTO' 86. Berlin, Heidelberg: Springer Berlin Heidelberg, : 186-194.

[11] Yuen T H, Huang Q, Mu Y, et al. Efficient Non-Interactive Range Proof[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 138-147.

[12] Couteau G, Peters T, Pointcheval D. Removing the Strong RSA Assumption from Arguments over the Integers[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017: 321-350.

[13] Bellare M, Goldwasser S. Verifiable Partial Key Escrow[C]. *The 4th ACM conference on Computer and communications security - CCS '97*, 1997: 78-91.

[14] Damgård I, Jurik M. A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System[C]. *Public Key Cryptography*, 2001: 119-136.

[15] Berry Schoenmakers, "Some efficient zero-knowledge proof techniques"[D]. in Workshop on Cryptographic Protocols, 2001.

[16] Berry Schoenmakers, "Interval proofs revisited"[D]. in International Workshop on Frontiers, in Electronic Elections. 2005.

[17] Camenisch J, Chaabouni R, Shelat A. Efficient Protocols for Set Membership and Range Proofs[M]. Advances in Cryptology - ASIACRYPT 2008. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 234-252.

[18] Lipmaa H, Asokan N, Niemi V. Secure Vickrey Auctions without Threshold Trust[M]. Financial Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 87-101.

[19] Chaabouni R, Lipmaa H, Shelat A. Additive Combinatorics and Discrete Logarithm Based Range Protocols[C]. *Information Security and Privacy*, 2010: 336-351.

[20] Canard S, Coisel I, Jambert A, et al. New Results for the Practical Use of Range Proofs[M]. Public Key Infrastructures, Services and Applications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 47-64.

[21] Gregory Maxwell, Andrew Poelstra, “Borromean ring signatures”[OL]. https://github.com/Blockstream/borromean_paper. Nov. 2015.

[22] Gregory Maxwell. “Confidential transactions”.[OL]. https://www.weusecoins.com/confidential-transactions/. June 16, 2015.

[23] Noether S, MacKenzie A, Research Lab T M. Ring Confidential Transactions[J]. *Ledger*, 2016, 1: 1-18.

[24] Herranz J. Deterministic Identity-Based Signatures for Partial Aggregation[J]. *The Computer Journal*, 2005, 49(3): 322-330.

[25] Groth J. Efficient Zero-Knowledge Arguments from Two-Tiered Homomorphic Commitments[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 431-448.

[26] Gennaro R, Gentry C, Parno B, et al. Quadratic Span Programs and Succinct NIZKs without PCPS[M]. Advances in Cryptology – EUROCRYPT 2013. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 626-645.

[27] Bootle J, Cerulli A, Chaidos P, et al. Efficient Zero-Knowledge Arguments for Arithmetic Circuits In the Discrete Log Setting[M]. Advances in Cryptology – EUROCRYPT 2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 327-357.

[28] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short Proofs for Confidential Transactions and more[C]. *2018 IEEE Symposium on Security and Privacy*, 2018: 315-334.

[29] Libert B, Ling S, Nguyen K, et al. Lattice-Based Zero-Knowledge Arguments for Integer Relations[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018: 700-732.

[30] Nguyen K, Tang H, Wang H X, et al. New Code-Based Privacy-Preserving Cryptographic Constructions[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019: 25-55.

[31] Stern J. A New Paradigm for Public Key Identification[J]. *IEEE Transactions on Information Theory*, 1996, 42(6): 1757-1768.

[32] Bootle J, Lyubashevsky V, Seiler G. Algebraic Techniques for Short(Er) Exact Lattice-Based Zero-Knowledge Proofs[M]. Advances in Cryptology – CRYPTO 2019. Cham: Springer International Publishing, 2019: 176-202.

[33] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[C]. *The thirty-seventh annual ACM symposium on Theory of computing - STOC '05*, 2005: 84-93.

[34] Kawachi A, Tanaka K, Xagawa K. Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems[M]. Advances in Cryptology - ASIACRYPT 2008. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 372-389.

[35] Pedersen T P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing[M]. Advances in Cryptology — CRYPTO ’91. Berlin, Heidelberg: Springer Berlin Heidelberg: 129-140.

[36] Micciancio D. Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions[J]. *Computational Complexity*, 2007, 16(4): 365-411.

[37] 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.

[38] Agarwal R C, Burrus C S. Number Theoretic Transforms to Implement Fast Digital Convolution[J]. *Proceedings of the IEEE*, 1975, 63(4): 550-560.

[39] Agarwal R, Burrus C. Fast Convolution Using Fermat Number Transforms with Applications to Digital Filtering[J]. *IEEE Transactions on Acoustics*, *Speech*, *and Signal Processing*, 1974, 22(2): 87-97.

[40] Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures[M]. Advances in Cryptology – ASIACRYPT 2009. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 598-616.

[41] Lyubashevsky V. Lattice Signatures without Trapdoors[M]. Advances in Cryptology – EUROCRYPT 2012. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 738-755.

[42] Blum M. Coin Flipping by Telephone a Protocol for Solving Impossible Problems[J]. *ACM SIGACT News*, 1983, 15(1): 23-27.

[43] Baum C, Damgård I, Lyubashevsky V, et al. More Efficient Commitments from Structured Lattice Assumptions[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018: 368-385.

[44] Libert B, Ling S, Nguyen K, et al. Zero-Knowledge Arguments for Lattice-Based PRFS and Applications to E-Cash[M]. Advances in Cryptology – ASIACRYPT 2017. Cham: Springer International Publishing, 2017: 304-335.

[45] Regev O. The Learning with Errors Problem (Invited Survey)[C]. *2010 IEEE 25th Annual Conference on Computational Complexity*, 2010: 191-204.

胡春雅 于 2017 年在合肥工业大学信息安全专业获得工学学士学位。现在中国科学院信息工程研究所信息安全国家重点攻读硕士学位。研究领域为格密码和零知识证明。研究兴趣包括: 基于格的高效零知识证明、基于格的高效范围证明、简短零知识证明。Email: huchunya@iie.ac.cn