基于后量子假设的高效范围证明方案

滕瑜莹[1,3], 谢 翔[2], 邓 燚[1,3]

[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]矩阵元技术有限公司 上海 中国 200120
[3]中国科学院大学 网络空间安全学院 北京 中国 100049

摘要 作为零知识证明的一种特殊应用, 范围证明技术广泛地应用于密码货币、电子投票、匿名凭证等多个场景。这项技术使得证明者能够向验证者证明某一秘密整数属于一个给定的连续整数区间, 除此之外不泄露其他任何信息。大部分现有的范围证明方案都是针对基于经典的数论假设的承诺方案构造的, 在量子攻击下不能保证安全性。本文针对串承诺方案, 提出了一种构造后量子范围证明方案的新思路, 并分别基于 Exact Learning Parity with Noise (xLPN), Small Integer Solution (SIS) 和 Learning with Errors (LWE) 等假设, 给出了三类具体的范围证明方案。此外, 文章还提出了一个批承诺方案, 并针对该批承诺构造了适用于同时处理多个消息的批处理范围证明方案。该批处理范围证明方案中, 对于多个秘密值分别属于不同整数区间的情况, 证明者只需要产生一个证明。与对多个消息逐一生成证明的处理方式相比, 批处理的方式有效地节约了生成证明过程中需要的随机数个数, 明显地降低了双方的通信量和计算量。

关键词 范围证明; 串承诺; 后量子密码学
中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2020.11.08

Efficient Range Proofs from Post-Quantum Assumptions

TENG Yuying[1,3], XIE Xiang[2], DENG Yi[1,3]

[1] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100093, China
[2] Juzix Technology Co. Ltd., Shanghai 200120, China
[3]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100049, China

Abstract As a special case of zero knowledge proof, range proof enables a prover to convince a verifier that a secret number lies in a given public interval, without leaking any other information. It is widely used in cryptocurrencies, e-voting, anonymous credentials, etc. However, most of existing range proof schemes are constructed for commitments based on hard problems of number theory, which are vulnerable against quantum attacks. In this paper, we present several post-quantum range proof schemes, based on the Exact Learning Parity with Noise (xLPN), Small Integer Solution (SIS) and Learning with Errors (LWE) assumptions respectively. In addition, we also propose a batch commitment scheme, together with a batch range proof scheme. Our batch range proof generates only one proof for multiple messages which lie in different ranges. It is efficient in both communication and computation.

Key words range proof; string commitment; post-quantum cryptography

1 引言

范围证明是集合成员属性证明的一种特殊形式。给定一个秘密整数的承诺值, 证明者能够通过一个范围证明, 使验证者相信证明者知道承诺值对应的秘密整数, 并且这个整数属于某一给定区间, 除此之外不泄露其他任何信息。这项技术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, 最大限度地隐藏证明者的个人信息。

大部分已知的范围证明方案都是高效的 Σ 协议, 协议中包含三轮交互, 满足特殊的合理性及特殊的诚实验证者零知识性两种性质。Brickell 等人在 1987 年提出了第一个范围证明方案[1], 采用了 Σ 协议的形式。该方案中, 证明者将秘密信息隐藏在第三轮交互的消息中发送给验证者, 但隐藏秘密消息的处理方式会导致一个膨胀系数的产生, 因而证明结果存在一定的准确性偏差。此外, 使用该方案时, 通信双方

通讯作者: 邓燚, 博士, 研究员, Email: deng@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: 2018-12-05; 修改日期: 2019-02-26; 定稿日期: 2020-09-22

需要多次并行执行协议来降低合理性错误率。方案的安全性依赖于离散对数假设。Chan 等人[2]在上述方案的基础上做出了改进, 以增大膨胀系数为代价, 省去了为降低合理性错误率而多次并行执行的麻烦。1998 年, Fujisaki 和 Okamoto 提出了一个基于强 RSA 假设的范围证明方案[3], 同样采用了Σ协议的形式, 该方案达到了完美完备性并且是统计证据不可区分的。

文献[4-7]中的范围证明方案都是基于正性检测技术来构造的。这种构造方式的主要思想是: $x \in [A,B]$等价于两个不等式$x-A\geqslant 0$和$B-x\geqslant 0$, 而正数总是可以写成某一种特定的数学表达式, 比如: 四个数的平方和, 因而证明$x \in [A,B]$可以转化为证明$x-A$和$B-x$各自存在某一种特定的分解。

Bellare 和 Goldwasser 的范围证明方案[8]提出了将秘密值分解为比特向量再对每个分量进行承诺的想法。基于此, Damgård 等人和 Lipmaa 等人也分别提出了他们的方案[9-10]。这一类方案的主要思想是: 先对秘密值的二进制表示进行逐比特承诺, 再证明这些承诺值之间满足某种关系当且仅当原始的秘密值属于给定区间。比如: Moran 和 Naor 的方案[11]中, 证明者将每一比特的承诺值打乱顺序, 再证明新的序列是原来序列的一个重新排列。在此基础上, Canard 等人[12]通过引入 Fischlin 引理, 又提出了一个针对小范围的范围证明方案。

在 Camenisch, Chaabouni 和 Shelat 的方案[13]中, 证明者将秘密值分解为 u 进制的向量, 并将给定区间划分为小区间$[0,u^l)$, 然后通过成员集合属性证明方案来证明: 秘密值分解得到的向量中, 每一个分量都属于$[0,u)$。Chaabouni, Lipmaa 和 Shelat 在上述方案的基础上, 提出了一个相似的方案[14], 对分解秘密值时选取的基做了改变, 使得证明者可以对任意的范围$[0,H)$进行证明。

Bünz 等人提出了一个特别的高效范围证明方案 Bulletproof[15], 证明者将秘密值转化为二进制向量, 再用二进制向量构造多项式, 然后通过一个内积论证系统进行关于多项式的知识的证明, 其中递归的内积论证系统的引入有效地缩短了证明的长度, 方案的安全性基于离散对数假设。

范围证明方案的安全性很大程度上取决于隐藏信息所使用的承诺方案所提供的安全性。现有的范围证明方案几乎都是针对基于经典数论困难问题(如: 离散对数问题, 大整数分解问题等)的承诺方案构造的, 并不适用于基于格问题的承诺方案。然而, 随着对量子计算的研究不断向前推进, 传统的数论困难问题有了高效的量子求解算法, 这对大部分范围证明方案的安全性都产生了极大的威胁。要消除这种安全隐患, 就需要针对设计出能够抵抗量子攻击的范围证明方案。当然, 一些针对算术电路和线性等式的零知识证明方案, 比如: Baum 等人和 Xie 等人提出的方案[16-17], 可以被转化为范围证明方案, 但是这种转化本身会产生额外的计算量和通信量。2018 年的美密上, Libert 等人针对基于 SIS 假设的承诺方案[18]提出了一个高效的后量子范围证明方案[19]。该方案的主要思想是: $x \in [A,B]$等价于存在两个正整数 a 和 b, 满足$A+a=x$, $x+b=B$两个加法等式, 通过这种等价转化, 范围证明就能够由对线性等式关系的零知识证明方案来完成。

1.1 本文的贡献

针对现有的范围证明方案大多不能抵抗量子攻击这一情况, 我们在后量子假设下设计了新的范围证明方案, 具体的工作总结如下:

1. 受到 Jain 等人提出的零知识论证系统[20]的启发, 本文针对串承诺, 提出了一种构造高效的后量子范围证明方案的思想, 并分别针对基于 xLPN, SIS 和 LWE 等后量子假设的承诺方案, 给出了三类具体的范围证明方案, 适用于区间形式为$[0,u^{n-\lambda})$的情况。进一步地, 我们还将这种范围证明方案推广到了任意满足$b-a<u^{n-\lambda}$的区间$[a,b]$的情况。

2. 本文将 Jain 等人提出的基于 xLPN 的承诺方案进行扩展, 给出了一个能够同时对多个消息承诺的批承诺方案, 并在此基础上提出了从一般范围证明到批处理范围证明的转化方式, 将本文中的基于 xLPN 问题的范围证明方案转化成了批处理的方案。该批处理范围证明方案通过将多个消息级联成一个消息的方式, 减少了证明过程中使用的随机数个数, 有效地降低了方案中交互双方的通信量和计算量。特别地, 对于不同的值分别属于不同区间的情况, 该批处理方案仍然只产生一个证明。

就安全性假设、秘密值的范围、合理性错误率、明文空间、参数空间和使用的承诺方案等六个方面, 本文中的方案和一些现有的范围证明方案对比结果如表 1 所示:

2 预备知识

本节将介绍一些后文中涉及到的概念及承诺方案。为了方便叙述, 我们先对一些符号作如下规定和说明: 文中涉及到的向量都默认为列向量, 对于任意的整数$m \in \mathbb{Z}$, $\boldsymbol{m}=(m_1,m_2,\cdots,m_n)^T$表示其对应的 u 进制 n 维向量, 其中$m_i \in \mathbb{Z}_u$, i=1, …, n, 记

表 1 现有方案及本文方案对比

Table 1 The contrast between existing schemes and schemes in this paper.

	方案	假设	范围	合理性错误率	取值空间		承诺方案
					消息	公共参数	
现有方案	文献[12]	q-SDH	$[a,b]$	*negl*	Multi-base	$\mathbb{Z}$	Pedersen[21]
	文献[13]	q-SDH	$[0,u^l)$	*negl*	$\mathbb{Z}_u$	$\mathbb{Z}_p$	Pedersen
	文献[14]	q-SDH	$[0,H]$	*negl*	Multi-base	$\mathbb{Z}_p$	Pedersen
	文献[15]	DL	$[0,2^n-1]$	*negl*	$\mathbb{Z}_2$	$\mathbb{Z}_p$	Pedersen
	文献[22]	DL	$[0,2^n-1]$	*negl*	$\mathbb{Z}_2$	$\mathbb{Z}_p$	Pedersen
	文献[19]	SIS	$[a,b]$	2/3	$\mathbb{Z}_2$	$\mathbb{Z}_q$	文献[3]
本文方案	协议 1	xLPN	$[0,2^{n-\lambda})$	2/3	$\mathbb{Z}_2$	$\mathbb{Z}_2$	文献[20]
	协议 2	xLPN	$[0,2^{n-\lambda_l})$	2/3	$\mathbb{Z}_2$	$\mathbb{Z}_2$	本文批处理承诺
	协议 3	SIS	$[0,2^{n-\lambda})$	2/3	$\mathbb{Z}_2$	$\mathbb{Z}_q$	文献[18]
	协议 4	LWE	$[0,u^{n-\lambda})$	2/3	$\mathbb{Z}_u$	$\mathbb{Z}_q$	文献[17]
	协议 5	LWE	$[a,a+u^{n-\lambda})$	2/3	$\mathbb{Z}_u$	$\mathbb{Z}_q$	文献[17]
	协议 6	LWE	$(b-u^{n-\lambda},b]$	2/3	$\mathbb{Z}_u$	$\mathbb{Z}_q$	文献[17]

(注: p 和 q 是都是与 n 相关的素数, u 是小于 p(或 q)的任意正整数)

$\boldsymbol{u}^n=(u^{n-1},\ u^{n-2},\cdots,1)^T$，则有 $m=\boldsymbol{m}\cdot\boldsymbol{u}^n=m_1\cdot u^{n-1}+m_2\cdot u^{n-2}+\cdots+m_n$; 当 u=2 时, 即规定被承诺向量是 0-1 向量时, $\boldsymbol{m}=IntToVec_u(m)$表示十进制数转化为 u 进制向量的变换, $m=VecToInt_u(\boldsymbol{m})$表示其逆变换。对于一个给定的函数$f(\boldsymbol{x})=\boldsymbol{Ax}$, $img\boldsymbol{A}$表示函数的原象集, 即变量$\boldsymbol{x}$所有取值的集合。对于任意的多项式$p(n)$和$\mu(n)$, 如果存在一个正整数 N, 使得对任意的 $n\geqslant N$, 都有$\mu(n)\leq 1/p(n)$, 那么$\mu(n)$是一个可忽略函数。计算不可区分的定义参见文献[29]。

2.1 Σ 协议[23]

L是一种语言, $\mathcal{R}$ 是其对应的关系。针对关系$\mathcal{R}$的一个协议称为Σ 协议, 如果它满足以下三个性质:

(1) 完备性: 协议是一个三轮的公开抛币协议, 如果$x\in L$, 且证明者和验证者都按照协议执行, 那么验证者总是接受证明。

(2) 特殊的合理性: 根据任一输入$x\in L$以及相应的两个可接受交互副本(a,e,z)和(a,e',z'), 其中 $e\neq e'$, 敌手可以高效地计算出 x 对应的合法的证据 ω, 使得$(x,\omega)\in\mathcal{R}$.

(3) 特殊的诚实验证者零知识性(Special honest-verifier zero-knowledge, SHVZK): 存在一个多项式时间的模拟器 M, 输入 x 和一个随机数 e, M 能够输出一个与真实交互产生的副本不可区分的副本(a, e, z).

2.2 困难性假设

2.2.1 LWE 假设[23]

定义 1. (判定 LWE 假设)给定安全参数 λ, $n=n(\lambda)$, $m=m(\lambda)$, $q=q(\lambda)\geqslant 2$ 是一个整数, $\chi=\chi(\lambda)$是 $\mathbb{Z}$ 上的一个分布。以下两个分布是计算不可区分的:

(1) $\{(\boldsymbol{a}_i,b_i)\}_{i=1}^m,(\boldsymbol{a}_i,b_i)\xleftarrow{\$}\mathbb{Z}_q^{n+1}$,

(2) $\{(\boldsymbol{a}_i,<\boldsymbol{a}_i,\boldsymbol{s}>+e_i)\}_{i=1}^m$, 其中 $\boldsymbol{a}_i\xleftarrow{\$}\mathbb{Z}_q^n$, $\boldsymbol{s}\xleftarrow{\$}\mathbb{Z}_q^n$, $e_i\leftarrow\chi$.

2.2.2 LPN 假设[20]

定义 2. (判定 LPN 假设)给定$n,m\in\mathbb{N}$, $\tau\in[0,0.5]$, $e\leftarrow Ber_\tau$(伯努利分布)。以下两个分布是计算不可区分的:

(1) $\{(\boldsymbol{a}_i,b_i)\}_{i=1}^m,(\boldsymbol{a}_i,b_i)\xleftarrow{\$}\mathbb{Z}_2^{n+1}$,

(2) $\{(\boldsymbol{a}_i,<\boldsymbol{a}_i,\boldsymbol{s}_i>\oplus e_i)\}_{i=1}^m$, 其中 $\boldsymbol{a}_i\xleftarrow{\$}\mathbb{Z}_q^n$, $\boldsymbol{s}_i\xleftarrow{\$}\mathbb{Z}_q^n$, $e_i\leftarrow Ber_\tau$.

Jain 等人在文献[20]中提出了 LPN 问题的一种变体: xLPN 问题, 该问题在 LPN 的基础上要求噪声向量 **e** 的汉明重量是一个确定的值, 即$\|\boldsymbol{e}\|_1=\omega$, 其中 ω=⌈kτ⌋是分布Ber_τ^k的期望。该文章也指出了判定 $\text{xLPN}_{\tau,n}$ 问题的困难性和搜索 LPN_τ 问题的困难性是多项式相关的。

2.2.3 SIS 假设

定义 3. (SIS 假设)[25]: 给定一个矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$, 由 m 个向量$\boldsymbol{a}_i\xleftarrow{\$}\mathbb{Z}_q^n$组成, 求一个非零整数向量$\boldsymbol{z}\in\mathbb{Z}^m$, 满足$\|\boldsymbol{z}\|\leqslant\beta$, 使得$\boldsymbol{Az}=\sum_{i=1}^m\boldsymbol{a}_i\cdot z_i=\boldsymbol{0}$是困难的。

2.3 承诺方案

一个承诺方案包括两个阶段: 承诺和打开。承

诺阶段, 发送者 S 向接收者 R 发送他对某一消息 m 及一个相应随机数 r 的承诺值 c。打开阶段, S 将对应的消息和随机数(m, r)发送给 R, R 检验 c 是否的确是对(m, r)的承诺值。一个安全的承诺方案需要满足以下两条性质:

• 隐藏性: 对于任何概率多项式时间的敌手$\mathcal{A}$和一个诚实的发送者 S, 都满足:

$$Pr\left[b = b^* \middle| \begin{matrix} \sigma \leftarrow Setup(1^n) \\ m_0, m_1 \leftarrow \mathcal{A}(\sigma) \\ b \leftarrow \{0,1\} \\ r \leftarrow S(\sigma) \\ c = Com(m_b, r) \\ b^* \leftarrow \mathcal{A}(c, \sigma) \end{matrix}\right] = \frac{1}{2} \pm negl(n).$$

• 绑定性: 对于任何概率多项式时间的敌手$\mathcal{A}$, 都满足下式:

$$Pr\left[\begin{matrix} m_0 \neq m_1 \wedge \\ Com(m_0, r_0) \\ = Com(m_1, r_1) \end{matrix} \middle| \begin{matrix} \sigma \leftarrow Setup(1^n) \\ m_0, m_1, r_0, r_1 \leftarrow \mathcal{A}(\sigma) \end{matrix}\right] = negl(n).$$

2.3.1 基于 LWE 的承诺方案[2]

参数生成算法: 输入安全参数$(1^k, 1^{l+n})$, 输出公共参数: $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{k\times(l+n)}$.

承诺算法: 承诺阶段, 输入消息$\boldsymbol{m} \in \mathbb{Z}_q^n$和公共参数 **A**, 承诺者选取 $\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^l$, $\boldsymbol{e} \xleftarrow{\$} \chi^k$, 计算$\boldsymbol{y} = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}) + \boldsymbol{e}$, 并将 **y** 发送给验证者; 打开阶段, 承诺者将(**r**, **m**)发送给验证者。

验证算法: 当且仅当$\|\boldsymbol{y} - \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})\|_\infty \leq \beta$时, 验证者输出 1.

此承诺方案满足完美绑定性和计算隐藏性。

2.3.2 基于 xLPN 的承诺方案[5]

参数生成算法: 输入安全参数$(1^k, 1^{l+n})$, 输出公共参数: $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_2^{k\times(l+n)}$.

承诺算法: 承诺阶段, 输入消息$\boldsymbol{m} \in \mathbb{Z}_q^n$和公共参数 **A**, 承诺者选取$\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_q^l$, $\mathbf{e} \xleftarrow{\$} \{0,1\}_\omega^k$, 其中$\{0,1\}_\omega^k = \{\boldsymbol{a}|\boldsymbol{a} \in \{0,1\}^{\wedge k} \wedge \|\boldsymbol{a}\|_1 = \omega\}$, 计算$\boldsymbol{y} = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}) \oplus \boldsymbol{e}$, 并将 **y** 发送给验证者; 打开阶段, 验证者将(**r**, **m**)发送给验证者。

验证算法: 当且仅当$\|\boldsymbol{y} \oplus \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})\|_1 = \omega$时, 验证者输出 1.

此承诺方案满足完美绑定性和计算隐藏性。

2.3.3 基于 SIS 的承诺方案[3]

参数生成算法: 输入安全参数$(1^k, 1^{l+n})$, 输出公共参数: $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{k\times(l+n)}$.

承诺算法: 承诺阶段, 输入消息$\boldsymbol{m} \in \mathbb{Z}_2^n$和公共参数 **A**, 承诺者选取 $\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_2^l$, 计算 $\boldsymbol{y} = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}) \bmod q$, 并将 **y** 发送给验证者; 打开阶段, 验证者将(**r**, **m**)发送给验证者。

验证算法: 验证者输出 1 当且仅当$\boldsymbol{y} = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})$且$\boldsymbol{r} \in \mathbb{Z}_2^l, \mathbf{m} \in \mathbb{Z}_2^n$.

此承诺方案满足计算绑定性和统计隐藏性。

3 构造思想

通常, 针对某种关系的零知识证明可以记为: {(公共输入; 证据): 满足的关系}。根据证明的对象来划分, 零知识证明可以分为知识的零知识证明和成员的零知识证明两种。范围证明从定义上来看属于成员的零知识证明, 形式上可以记作: {(公共参数串, 承诺值 y; 被承诺值 m 及相应的随机数 r): $y = Com(m, r)$且 m 属于某一给定区间}。相对知识的零知识证明而言, 成员的零知识证明通常有更加复杂和庞大的公共参数串。为了解决这一问题, 我们可以将成员关系等价地转化为某种数学关系, 然后对这种数学关系构造知识的零知识证明。

现有的范围证明方案几乎都是针对基于离散对数问题的承诺方案构造的, 如 Pedersen 承诺, 这些方案并不适用于基于格问题和编码问题的承诺方案。与基于离散对数的承诺相比, 基于编码问题和格问题的承诺方案通常有相对比较庞大的公共参数, 但是由于方案中涉及到的主要运算是矩阵与向量的加法、减法和乘法, 不涉及幂运算, 因而有较快的运算速度, 在计算机中执行更有效率优势。基于编码问题和格问题的承诺方案都是串承诺, 其被承诺值通常是一个向量, 也就是说, 使用这类承诺对一个整数 m 承诺, 实际上是对 m 转化成的 n 维 u 进制串进行承诺, 即被承诺值是以$(u^{n-1}, \dots, u, 1)$为基分解 m 得到的系数向量, 其消息空间是$\mathbb{Z}_u^n$. 要针对串承诺构造范围证明, 最关键的问题在于找到与$m \in [0, u^{n-\lambda})$等价的特定数学关系。通过观察我们注意到, 当给定承诺方案的安全参数 n, 即向量维数时, 任一整数 m 如果满足$m \in [0, u^{n-\lambda})$, 那么其对应的 u 进制向量$\boldsymbol{m}$的前 λ 位都为 0, 即:

$$m = VecToInt_u(\boldsymbol{m}) \in [0, u^{n-\lambda}) \Leftrightarrow \begin{cases} m_1 = \cdots = m_\lambda = 0 \\ m_{\lambda+1}, \cdots, m_n \in \mathbb{Z}_u \end{cases}.$$

如果给定$n = 32$, 而要证明的是$m \in [0, u^{17})$, 那么此时取$\lambda = 15$, 即 m 对应的 u 进制向量 $\boldsymbol{m}$ 的前 15 位都为 0. 对任意的向量$\boldsymbol{m} \in \mathbb{Z}_u^n$, 记其后$n - \lambda$位为 $\boldsymbol{m}'$, 即 $\boldsymbol{m}' = (m_{\lambda+1}, \cdots, m_n)$, 此时显然有 $\boldsymbol{m} = 0^\lambda||\boldsymbol{m}'$.

综上所述, 要针对串承诺方案, 构造给定区间形式为$[0,u^{n-\lambda})$的范围证明方案, 只需要由证明者向验证者证明: 证明者知道给定的承诺对应的被承诺值, 且这个被承诺值是一个前 λ 个分量都为 0 的 u 进制 n 维向量, 其中n是承诺方案本身的安全参数, 而λ是由证明者根据$\boldsymbol{m}$确定的公共输入, λ的值等于$\boldsymbol{m}$中第一个 1 前面的 0 的个数, $0<\lambda<n$. 受到 Jain 的文章的启发, 证明向量是 u 进制向量可以通过引入随机变换来完成。这种随机变换定义为: 给定一个 k 维向量 $\boldsymbol{\alpha}$, π是一个可逆的随机变换, $\pi(\boldsymbol{\alpha})$表示将向量$\boldsymbol{\alpha}$中各分量的次序进行重排产生的新分量。根据定义, 这种随机变换满足以下性质: $\pi^{-1}(\pi(\boldsymbol{\alpha}))=\boldsymbol{\alpha}$, $\|\pi(\boldsymbol{\alpha})\|_1=\|\boldsymbol{\alpha}\|_1$, $\|\pi(\boldsymbol{\alpha})\|_\infty=\|\boldsymbol{\alpha}\|_\infty$. 在具体的应用中, π可以通过初等矩阵来实现, 所有上述随机变换的集合表示为S_u^k, 即: $S_u^k=\{\pi\mid\forall\boldsymbol{\alpha}\in\mathbb{Z}_u^k,\pi^{-1}(\pi(\boldsymbol{\alpha}))=\boldsymbol{\alpha}\wedge\pi(\boldsymbol{\alpha})\in\mathbb{Z}_u^k\wedge\|\pi(\boldsymbol{\alpha})\|_1=\|\boldsymbol{\alpha}\|_1\wedge\|\pi(\boldsymbol{\alpha})\|_\infty=\|\boldsymbol{\alpha}\|_\infty\}$.

对于任意的闭区间$[a,b]$, 我们观察到当区间$[a,b]$满足$0\leqslant b-a<u^{n-\lambda}$时, 如果有$m\in[a,a+u^{n-\lambda})$且$m\in(b-u^{n-\lambda},b]$, 那么就有$m\in[a,b]$. 这可以简化为:

$$\begin{cases}m-a\in[0,u^{n-\lambda})\\ b-m\in[0,u^{n-\lambda})\\ 0\leqslant b-a<u^{n-\lambda}\end{cases}\Rightarrow m\in[a,b].$$

由于不是所有的承诺方案都满足同态性, 当给定对消息m的承诺值时, 有时无法直接由对m的承诺值和对a、b的承诺值得到对$m-a$和$b-m$的承诺值, 从而无法直接套用上述思想证明$m-a$和$b-m$属于$[0,u^{n-\lambda})$。但是通过一些简单的数学运算技巧, 我们可以由对m的承诺值和方案的公开参数拼接出对$m-a$和$b-m$的承诺值, 再由针对$m\in[0,u^{n-\lambda})$的方案出发, 结合分割向量的思想, 来构造针对$m-a\in[0,u^{n-\lambda})$和$b-m\in[0,u^{n-\lambda})$的方案。5.2.2 节和 5.2.3 节将以基于 LWE 问题的范围证明方案为例, 分别构造对$m-a\in[0,u^{n-\lambda})$和$b-m\in[0,u^{n-\lambda})$的范围证明方案(见协议 5 和协议 6)。此时, 只要给定的区间$[a,b]$满足$0\leqslant b-a<u^{n-\lambda}$, 那么同时使用协议 5 和协议 6 就能够证明$x\in[a,b]$. 要说明的是, 基于 xLPN 和 SIS 问题的协议也可以通过相同的方式转化为针对$m-a\in[0,u^{n-\lambda})$和$b-m\in[0,u^{n-\lambda})$的协议。当给定区间为开区间(a,b)时, 由于 x 是整数, 从而有$x\in(a,b)$等价于$x\in[a+1,b-1]$. 半闭半开区间和半开半闭区间也可以用类似的方式转换为闭区间。

下一节起, 我们将根据这种思想, 针对基于不同后量子假设的承诺方案, 构造适用于不同区间形式的范围证明, 并对其安全性和计算量进行分析。

4 基于 xLPN 的范围证明方案和批处理范围证明方案

Jain 等人提出了 LPN 问题的一个变体 xLPN, 并基于此给出了一个定义在$\mathbb{Z}_2$上的串承诺方案, 及相应的对被承诺值的知识的零知识论证系统。这种二进制的方案在计算机上运行时有着天然的效率优势, 有很好的应用前景, 因而受到了很多关注。本节将基于xLPN问题, 给出一个定义在$\mathbb{Z}_2$上的范围证明方案, 并以该方案为例, 给出种从一般的范围证明方案到批处理的范围证明方案的转化方式。显然地, 在这一节中 u 的取值为 2, 方案中的所有向量都是 0-1 向量, 承诺密钥矩阵也是 0-1 矩阵。

4.1 基于 xLPN 的范围证明方案

本文给出的基于xLPN问题的范围证明方案, 本质上是 Jain 等人提出的零知识证明方案的一个延伸, 该方案以关于被承诺向量的知识的零知识证明方案为基础, 额外加入了关于被承诺向量是一个前λ位都为 0 的 0-1 向量的证明。基于 xLPN 的范围证明写为以下形式:

$$\{(\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_2^{k\times(l+n)},\boldsymbol{y}\xleftarrow{\$}\mathbb{Z}_2^k:\mathbf{r}\in\mathbb{Z}_2^l,\boldsymbol{m}\in\mathbb{Z}_2^n,\boldsymbol{e}\in\{0,1\}_\omega^k):\\ \boldsymbol{y}=\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})\oplus\boldsymbol{e}\wedge\|\boldsymbol{e}\|_1=\omega\wedge VecToInt_2(\boldsymbol{m})\\ \in[0,2^{n-\lambda})\}.$$

证明生成过程中, 证明者和验证者的公共输入为承诺密钥 $\boldsymbol{A}$ 和承诺值 $\boldsymbol{y}$, 证明者的证据是生成 $\boldsymbol{y}$ 时使用的随机数 $\boldsymbol{r}$, 消息 $\boldsymbol{m}$ 和噪声 $\boldsymbol{e}$。具体的证明生成过程如协议 1 所述。协议中使用的辅助承诺可以是任意的串承诺方案, 记为 *Com(·)*, 辅助承诺中使用的随机数(向量)统一记做 *R*. 本文中, 方便起见, 协议 1 中的辅助承诺采用 2.3.2 小节中介绍的承诺方案, 即$Com(\boldsymbol{x})=\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{x})\oplus\boldsymbol{e}$, 此时$R=\{\boldsymbol{r},\boldsymbol{e}\}$.

协议 1

生成证明:

1.证明者 $\mathcal{P}$ 首先选取两个随机置换$\pi\xleftarrow{\$}S_2^k$, $\pi_m\xleftarrow{\$}S_2^{n-\lambda}$, 以及三个随机向量$\boldsymbol{v}\xleftarrow{\$}\mathbb{Z}_2^l$, $\boldsymbol{f}\xleftarrow{\$}\mathbb{Z}_2^k$, $\boldsymbol{s}'\xleftarrow{\$}\mathbb{Z}_2^{n-\lambda}$. 令$\boldsymbol{s}=0^\lambda||\boldsymbol{s}'$, 然后 $\mathcal{P}$ 计算:

$$\boldsymbol{t}_0=\boldsymbol{A}(\boldsymbol{v}||\boldsymbol{s})\oplus\boldsymbol{f},$$
$$\boldsymbol{t}_1=\pi(\boldsymbol{f}),\boldsymbol{t}_2=\pi(\boldsymbol{f}\oplus\boldsymbol{e}),$$
$$\boldsymbol{t}_{m1}=\pi_m(\boldsymbol{s}'),\boldsymbol{t}_{m2}=\pi_m(\boldsymbol{s}'\oplus\boldsymbol{m}'),$$
$$\boldsymbol{C}_0=Com(\pi,\pi_m,\boldsymbol{t}_0,R_0),$$
$$\boldsymbol{C}_1=Com(\boldsymbol{t}_1,\boldsymbol{t}_{m1},R_1),$$
$$\boldsymbol{C}_2=Com(\boldsymbol{t}_2,\boldsymbol{t}_{m2},R_2),$$
$$\mathcal{P}\rightarrow\mathcal{V}::(\boldsymbol{C}_0,\boldsymbol{C}_1,\boldsymbol{C}_2).$$

2. $\mathcal{V}: \to \mathcal{P}: d \xleftarrow{\$} \{1,2,3\}$.

3. $\mathcal{P}$ 根据 $\mathcal{V}$ 的挑战值做出相应的回应:

1) $d=1$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0, \boldsymbol{C}_1$, 即 $\mathcal{P} \to \mathcal{V}:: OPEN_1 = \{\pi, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{t}_{m1}, R_0, R_1\}$.

2) $d=2$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0, \boldsymbol{C}_2$, 即 $\mathcal{P} \to \mathcal{V}:: OPEN_2 = \{\pi, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_2, \boldsymbol{t}_{m2}, R_0, R_2\}$.

3) $d=3$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_1, \boldsymbol{C}_2$, 即 $\mathcal{P} \to \mathcal{V}:: OPEN_3 = \{\boldsymbol{t}_1, \boldsymbol{t}_2, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}, R_1, R_2\}$.

验证:

将 **A** 划分为$\boldsymbol{A}_1 || \boldsymbol{A}_2$, 其中$\boldsymbol{A}_1 \in \mathbb{Z}_2^{k \times l}$, $\boldsymbol{A}_2 \in \mathbb{Z}_2^{k \times n}$. $\mathcal{V}$ 接受证明当且仅当:

1) $d=1$时,

$$\boldsymbol{t}_0 \oplus \pi^{-1}(\boldsymbol{t}_1) \oplus \boldsymbol{A}_2 \cdot (0^\lambda || \pi_m^{-1}(\boldsymbol{t}_{m1})) \in img\boldsymbol{A}_1 \wedge \pi \in S_2^k \wedge \pi_m \in S_2^{n-\lambda}..$$

2) $d=2$时,

$$\boldsymbol{y} \oplus \boldsymbol{t}_0 \oplus \pi^{-1}(\boldsymbol{t}_2) \oplus \boldsymbol{A}_2 \cdot (0^\lambda || \pi_m^{-1}(\boldsymbol{t}_{m2})) \in img\boldsymbol{A}_1 \wedge \pi \in S_2^k \wedge \pi_m \in S_2^{n-\lambda}..$$

3) $d=3$时,

$$\|\boldsymbol{t}_1 \oplus \boldsymbol{t}_2\|_1 = \omega \wedge \boldsymbol{t}_{m1} \oplus \boldsymbol{t}_{m2} \in \mathbb{Z}_2^{n-\lambda}.$$

整个证明, 即交互副本为: $(\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2, d, OPEN_d, R_i, R_j)$. 其中 *i, j* 的取值根据挑战值与要打开的承诺对应, 如: *d*=1 时, *i*=0, *j*=1, R_0表示生成$\boldsymbol{C}_0$时使用的随机向量和噪声向量, R_1表示了生成$\boldsymbol{C}_1$时使用的随机向量和噪声向量。$d=1$或 2 时, 判定算式的结果是否在集合$img\boldsymbol{A}_1$中, 实际上是求解 $\boldsymbol{r}$ 或者$\boldsymbol{r} \oplus \boldsymbol{v}$, 根据承诺方案的绑定性, 当且仅当根据算式可以得到唯一的$\boldsymbol{r} \in \mathbb{Z}_2^l$或者$\boldsymbol{r} \oplus \boldsymbol{v} \in \mathbb{Z}_2^l$时, 验证通过。本文其他几个协议中, 判定算式结果是否属于集合$img\boldsymbol{A}_1$的实际意义也是如此。

定理 1: 如果协议 1 中的辅助承诺满足完美绑定性和计算隐藏性, 那么协议 1 是一个满足完美完备性和计算 SHVZK 的Σ协议, 其合理性错误率为 2/3。

证明: **完备性**: 随机变换π, π'的证明是显然的。根据挑战值的不同:

1) $d=1$时,

$$\begin{aligned} &\boldsymbol{t}_0 \oplus \pi^{-1}(\boldsymbol{t}_1) \oplus \boldsymbol{A}_2(0^\lambda \| \pi_m^{-1}(\boldsymbol{t}_{m1})) \\ &= \boldsymbol{A}_1\boldsymbol{v} \oplus \boldsymbol{A}_2\boldsymbol{s} \oplus \boldsymbol{f} \oplus \boldsymbol{f} \oplus \boldsymbol{A}_2(0^\lambda \| \boldsymbol{s}') \\ &= \boldsymbol{A}_1\boldsymbol{v} \in img\boldsymbol{A}_1. \end{aligned}$$

2) $d=2$时,

$$\begin{aligned} &\boldsymbol{y} \oplus \boldsymbol{t}_0 \oplus \pi^{-1}(\boldsymbol{t}_2) \oplus \boldsymbol{A}_2(0^\lambda \| \pi_m^{-1}(\boldsymbol{t}_{m2})) \\ &= \boldsymbol{A}(\boldsymbol{r} \| \boldsymbol{m}) \oplus \boldsymbol{A}(\boldsymbol{v} \| \boldsymbol{s}) \oplus \boldsymbol{A}_2(0^\lambda \| (\boldsymbol{s}' \oplus \boldsymbol{m}')) \\ &= \boldsymbol{A}_1(\boldsymbol{r} \oplus \boldsymbol{v}) \oplus \boldsymbol{A}_2(\boldsymbol{m} \oplus \boldsymbol{s}) \oplus \boldsymbol{A}_2\boldsymbol{s} \oplus \boldsymbol{A}_2\boldsymbol{m} \\ &= \boldsymbol{A}_1(\boldsymbol{r} \oplus \boldsymbol{v}) \in img\boldsymbol{A}_1. \end{aligned}$$

3) $d=3$时,

$$\|\boldsymbol{t}_1 \oplus \boldsymbol{t}_2\|_1 = \|\pi(\boldsymbol{f}) \oplus \pi(\boldsymbol{f} \oplus \boldsymbol{e})\|_1 = \|\pi(\boldsymbol{e})\|_1 = \omega$$
$$\boldsymbol{t}_{m1} \oplus \boldsymbol{t}_{m2} = \pi_m(\boldsymbol{s}') \oplus \pi_m(\boldsymbol{s}' \oplus \boldsymbol{m}') = \pi_m(\boldsymbol{m}') \in \mathbb{Z}_2^{n-\lambda}.$$

特殊的合理性: 根据承诺方案的绑定性, 每个确定的承诺值只能被打开为唯一一组确定的被承诺值及其相应的随机数。如果一个没有证据的证明者 $\mathcal{P}^*$ 对固定的第一轮消息$(\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2)$, 得到了相应的三个挑战值分别为 1, 2, 3 的可接受交互副本, 那么 $\mathcal{P}^*$ 就得到了对应于同一组证据$(\boldsymbol{r}, \boldsymbol{m}, \boldsymbol{e})$的全部参数$\pi, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{t}_2, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}$. 通过以下两个算式:

$$\begin{aligned} \pi^{-1}(\boldsymbol{t}_1 \oplus \boldsymbol{t}_2) &= \pi^{-1}(\pi(\boldsymbol{f}) \oplus \pi(\boldsymbol{f} \oplus \boldsymbol{e})) \\ &= \pi^{-1}(\pi(\boldsymbol{e})) = \boldsymbol{e}, \end{aligned}$$
$$\boldsymbol{A}^{-1} \cdot (\boldsymbol{y} \oplus \boldsymbol{e}) = \boldsymbol{A}^{-1} \cdot (\boldsymbol{A} \cdot (\boldsymbol{r} || \boldsymbol{m}) \oplus \boldsymbol{e} \oplus \boldsymbol{e}) = \boldsymbol{r} || \boldsymbol{m}.$$

$\mathcal{P}^*$ 可以从中抽取出诚实(即拥有证据并严格按照协议执行的)证明者的合法证据$(\boldsymbol{r}, \boldsymbol{m}, \boldsymbol{e})$.

根据协议, 当验证者的挑战值为 1 或 3 时, 一个恶意(即没有证据$(\boldsymbol{r}, \boldsymbol{m}, \boldsymbol{e})$)的证明者 $\mathcal{P}^*$ 也可以生成能够通过验证的证明, 只有在挑战值为 2 时, 会进行关于证据的检验, 因而合理性错误率, 即恶意证明者能够欺骗验证者的概率是 2/3。

特殊的诚实验证者零知识性: 对于一个 Σ 协议, 如果存在一个高效的模拟器 S, 给定不同的挑战值, 它能够根据挑战值输出不同的可接受副本, 并且其输出的副本的分布与诚实的证明者在真实交互中产生的副本的分布不可区分, 那么这个协议就满足特殊的诚实验证者零知识性。S 的描述如下:

1) $d=1$时, 模拟器 S 像诚实的证明者一样计算$\boldsymbol{C}_0^*, \boldsymbol{C}_1^*$, 同时计算$\boldsymbol{C}_2^* = Com(\boldsymbol{0}^n)$, 即$\boldsymbol{C}_2^*$是对全 0 串的承诺。显然$\boldsymbol{C}_0^*, \boldsymbol{C}_1^*, OPEN_1^* = \{\pi^*, \pi_m^*, \boldsymbol{t}_0^*, \boldsymbol{t}_1^*, \boldsymbol{t}_{m1}^*, R_0^*, R_1^*\}$的分布与真实交互中的分布是完全相同的, 而由承诺方案的隐藏性可知, 此时的$\boldsymbol{C}_2^*$的分布与真实交互中证明者产生的$\boldsymbol{C}_2$的分布是计算不可区分的。容易验证, S 产生的这个交互副本是一个可接受副本。

2) $d=2$时, 模拟器 S 像真实交互一样选取$\pi^*, \pi_m^*, \boldsymbol{v}^*, \boldsymbol{f}^*, \boldsymbol{s}'^*, \boldsymbol{s}^*$, 计算:

$$\boldsymbol{t}_0^* = \boldsymbol{A}(\boldsymbol{v}^* || \boldsymbol{s}^*) \oplus \boldsymbol{f}^* \oplus \boldsymbol{y}, \boldsymbol{t}_2^* = \pi^*(\boldsymbol{f}^*)$$
$$\boldsymbol{t}_{m2}^* = \pi_m^*(\boldsymbol{s}'^*), \boldsymbol{C}_1^* = Com(\boldsymbol{0}^n)$$

然后按照真实协议计算$\boldsymbol{C}_0^*, \boldsymbol{C}_2^*$. 容易验证, 这种生成方式下产生的证明是能够通过验证的。根据承诺方案的隐藏性, $\boldsymbol{C}_1^*$的分布与真实交互中$\boldsymbol{C}_1$的分布计算不可区分, 而$\boldsymbol{C}_0^*, \boldsymbol{C}_2^*, OPEN_2^* = \{\pi^*, \pi_m^*, \boldsymbol{t}_0^*, \boldsymbol{t}_2^*, \boldsymbol{t}_{m2}^*, R_0^*, R_2^*\}$的分布

与真实交互中的分布显然是完全相同的。

3) $d=3$时, S 选取$\boldsymbol{h}^* \xleftarrow{\$}\{0,1\}_{\omega}^{k}$, $\boldsymbol{t}_1^* \xleftarrow{\$}\mathbb{Z}_2^k$, $\boldsymbol{t}_{m1}^*$, $\boldsymbol{t}_{m2}^* \xleftarrow{\$}\mathbb{Z}_2^{n-\lambda}$, 计算$\boldsymbol{t}_2^*=\boldsymbol{t}_1^*\oplus\boldsymbol{h}^*$, 取$\boldsymbol{C}_0^*=Com(\boldsymbol{0}^n)$. 然后按照真实协议计算$\boldsymbol{C}_1^*,\boldsymbol{C}_2^*$, 此时$\boldsymbol{C}_1^*,\boldsymbol{C}_2^*$ $OPEN_3^*=\{\boldsymbol{t}_1^*,\boldsymbol{t}_2^*,\boldsymbol{t}_{m1}^*,\boldsymbol{t}_{m2}^*,R_1^*,R_2^*\}$的分布与真实交互中的分布完全相同, 而由承诺方案的隐藏性可知, $\boldsymbol{C}_0^*$的分布与真实交互中$\boldsymbol{C}_0$的分布是计算不可区分的, 整个交互产生的副本是一个可接受副本。

4.2 批处理范围证明方案

现实生活中, 人们常会遇到一次需要处理多个消息的情况, 如一笔交易中包含多个订单, 需要对多个数值进行范围证明。这种情况下, 为了节约证明的计算和通信成本, 我们先对 2.3.2 中介绍的基于 xLPN 问题的承诺方案稍加改动, 提出一个批承诺方案, 然后针对这一批承诺, 给出一个高效、简洁的批处理范围证明方案。

4.2.1 批处理承诺方案

Jain 等人提出的承诺方案(见 2.3.2)输出的承诺值是定长的, 即无论消息多么大, 只要给定了安全参数 k, 最终输出的承诺值的长度都为 k 比特。根据这一特性, 本文通过将多个消息级联为一个消息的方式, 对该方案自然地拓展, 给出一个批承诺方案。相比普通的并行执行, 批承诺在效率提升和参数缩减两方面都有很好的表现。我们将在给出具体的批承诺方案后, 对其参数设置、优势以及安全性进行详细地分析说明。

基于 xLPN 的批承诺方案:

参数生成算法: 输入安全参数$(1^k,1^{l+bn})$, 输出公共参数: $\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_2^{k\times(l+bn)}$.

承诺算法: 承诺阶段, 输入公共参数 **A** 和消息$\boldsymbol{m}_1,\cdots,\boldsymbol{m}_b\in\mathbb{Z}_2^n$, 承诺者选取$\boldsymbol{r}\xleftarrow{\$}\mathbb{Z}_2^l$, $\boldsymbol{e}\xleftarrow{\$}\{0,1\}_{\omega}^{k}$, 计算: $\boldsymbol{y}=\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}_1||\cdots||\boldsymbol{m}_b)\oplus\boldsymbol{e}$, 并将 **y** 发送给验证者; 打开阶段, 验证者将$(\boldsymbol{r},\boldsymbol{m}_1,\cdots,\boldsymbol{m}_b)$发送给验证者。

验证算法: 验证者输出 1 当且仅当

$$\|\boldsymbol{y}\oplus\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}_1||\cdots||\boldsymbol{m}_b)\|_1=\omega.$$

将一个普通方案扩展为批处理方案, 主要有两个问题需要重点关注: 1) 消息之间的链接方式; 2) 参数的变化带来的安全性损失。针对第一点, 为了保证绑定性, 本文使用了级联的方式将多个消息合并为一个。而对第二点, 公共参数的选择不当可能会导致承诺方案不再满足绑定性。批处理承诺中, 承诺密钥 **A** 的选取首先应该满足原始方案中的要求, 即对任意的 **x** 都有$\|\boldsymbol{A}\cdot\boldsymbol{x}\|_1>2\omega$, 除此之外我们注意到: 令$\boldsymbol{A}=\boldsymbol{A}_0||\cdots||\boldsymbol{A}_b$, 其中$\boldsymbol{A}_0\in\mathbb{Z}_2^{k\times l}$, $\boldsymbol{A}_1,\cdots,\boldsymbol{A}_b\in\mathbb{Z}_2^{k\times n}$, 如果有至少两个矩阵$\boldsymbol{A}_i,\boldsymbol{A}_j$相等, 那么使用相同的随机向量和噪声$(\boldsymbol{r},\boldsymbol{e})$对两组消息$(\boldsymbol{m}_1,\ldots,\boldsymbol{m}_i,\ldots,\boldsymbol{m}_j,\ldots,\boldsymbol{m}_b),(\boldsymbol{m}_1,\cdots,\boldsymbol{m}_j,\cdots,\boldsymbol{m}_i,\cdots,\boldsymbol{m}_b)$承诺将会得到相同的承诺值, 这会打破承诺方案的绑定性。不过幸运的是, 所有的矩阵$\boldsymbol{A}_1,\cdots,\boldsymbol{A}_b$两两不同的概率为:

$$\Pr[\boldsymbol{A}_1\neq\cdots\neq\boldsymbol{A}_b]=\frac{\mathrm{A}_{2^{kn}}^{b}}{(2^{kn})^b}=\frac{2^{kn}\cdot(2^{kn}-1)\cdots(2^{kn}-b+1)}{(2^{kn})^b}.$$

当 kn 足够大且远大于 b 时, 相同矩阵出现的概率很小。为了避免这种情况, 每次参数生成时, 承诺者和验证者可以先检查 **A** 的形式是否满足要求, 如果发现上述情况, 就要求重新生成参数, 重复这个过程直到产生符合要求的 **A**。正式的安全性描述如定理 2。

定理 2. 选取$0<\tau<0.25$, $k,l\in\mathbb{N}$, 以及合适的$k=\Theta(l+bn)$, 使得规模为$k\times(bn+l)$的判定 xLPN_τ问题是困难的, 且矩阵$\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_2^{k\times(l+bn)}$能以极大的概率满足: 对任意的$\boldsymbol{x}\in\mathbb{Z}_2^{l+bn}$, $\|\boldsymbol{A}\cdot\boldsymbol{x}\|_1>2\omega$. 此外, 矩阵 **A** 满足形式: $\boldsymbol{A}=\boldsymbol{A}_0||\cdots||\boldsymbol{A}_b$, 其中$\boldsymbol{A}_1,\cdots,\boldsymbol{A}_b\in\mathbb{Z}_2^{k\times n}$, $\boldsymbol{A}_0\in\mathbb{Z}_2^{k\times l}$, 且对任意的$1\leqslant i,j\leqslant b$, $\boldsymbol{A}_i\neq\boldsymbol{A}_j$.此时, 上述基于 xLPN 的批承诺方案满足完美绑定性和计算隐藏性。

证明: 完美绑定性: 如果存在两组消息$(\boldsymbol{m}_1,\cdots,\boldsymbol{m}_b)\neq(\boldsymbol{m}_1',\cdots,\boldsymbol{m}_b')$, 它们的承诺值相同, 即满足:

$$\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}_1||\cdots||\boldsymbol{m}_b)\oplus\boldsymbol{e}=\boldsymbol{A}(\boldsymbol{r}'||\boldsymbol{m}_1'||\cdots||\boldsymbol{m}_b')\oplus\boldsymbol{e}'$$

那么可以由此推出:

$$\boldsymbol{A}((\boldsymbol{r}\oplus\boldsymbol{r}')||(\boldsymbol{m}_1\oplus\boldsymbol{m}_1')||\cdots||(\boldsymbol{m}_b\oplus\boldsymbol{m}_b'))=\boldsymbol{e}\oplus\boldsymbol{e}'.$$

由噪声的分布可知: $\|\boldsymbol{e}\oplus\boldsymbol{e}'\|_1\leqslant\|\boldsymbol{e}\|_1+\|\boldsymbol{e}'\|_1=2\omega$, 而承诺方案的参数设置要求: $\forall\boldsymbol{x}\in\mathbb{Z}_2^{l+bn}$, $\|\boldsymbol{A}\cdot\boldsymbol{x}\|_1>2\omega$, 两者相互矛盾。因而对同一个承诺值, 只能找到唯一的一组消息及对应的随机数。

计算隐藏性:

$$\begin{aligned}\boldsymbol{y}&=\boldsymbol{A}(\boldsymbol{r}\,\|\,\boldsymbol{m}_1\,\|\cdots\|\,\boldsymbol{m}_b)\oplus\boldsymbol{e}\\&=\boldsymbol{A}_0\boldsymbol{r}\oplus\boldsymbol{e}\oplus\boldsymbol{A}_1\boldsymbol{m}_1\oplus\cdots\oplus\boldsymbol{A}_b\boldsymbol{m}_b\\&\approx\boldsymbol{r}^*\oplus\boldsymbol{A}_1\boldsymbol{m}_1\oplus\cdots\oplus\boldsymbol{A}_b\boldsymbol{m}_b\\&\approx\boldsymbol{r}^{**}\end{aligned}$$

其中, $\boldsymbol{r}^*$和$\boldsymbol{r}^{**}$是随机数。上式表明, 对任意消息的承诺值的分布与均匀分布是不可区分的。

除了本文的批处理方案外, 同时对多个消息承诺还可以采用简单并行的方式。两种方式的对比如下:

1) 在并行处理的方案中, 承诺阶段承诺者分别对每个$\boldsymbol{m}_i$进行承诺: $\boldsymbol{y}_i = \boldsymbol{A}_i(\boldsymbol{r}_i \| \boldsymbol{m}_i) \oplus \boldsymbol{e}_i$, $i = 1, \cdots, b$, 然后将这 b 个承诺值一起发送给验证者; 打开时, 再将 b 个消息, b 个随机数和 b 个噪声都发送给验证者; 验证者需要验证 b 个等式。

2) 本文的批处理方案中, 承诺者只需要发送一个承诺值, 一个随机数, 一个噪声以及 b 个消息, 验证者只用验证 1 个等式。

两种方案的参数大小对比结果如表 2 所示:

表 2 批处理和并行处理方案中参数大小的对比

Table 2 The contrast of sizes of the parameters in Both batching and parallel schemes. (单位: 比特)

方案	并行处理	批处理
消息 **m**	*bn*	*bn*
随机数 **r**	*bl*	*l*
噪声 **e**	*bk*	*k*
公共参数 **A**	*bk(l+n)*	*k(l+bn)*

4.2.2 批处理范围证明

接下来给出的批处理范围证明方案, 是针对上一小节中的批承诺方案构造的, 它也可以看作是对 4.1 节中范围证明方案的一个拓展。对于多个消息, 这种批处理的范围证明方案只需要产生一个证明, 与简单地为所有消息逐一产生证明的方式相比, 一定程度上节省了通信双方的通信量和计算量。特别地, 该批处理方案适用于证明每个消息分别属于不同区间的情况, 即对于$i = 1, \cdots, b$, $VecToInt_2(\boldsymbol{m}_i) \in [0, 2^{n-\lambda_i})$, 其中$\lambda_1, \cdots, \lambda_b$各不相同。这个方案给出了一种由普通范围证明方案转化批处理方案的思路。这种转化方式, 除了适用于 4.1 节中的范围证明方案, 也适用于其他类似形式的、针对串承诺的范围证明方案, 如 5.1 节中基于 SIS 的方案和 5.2 节中基于 LWE 的方案, 转化的具体过程几乎与本小节的方案完全相同, 因而本文不再对其做具体地描述。

基于 xLPN 问题的批处理范围证明方案可以记作:

$$\{(\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_2^{k\times(l+bn)}, \boldsymbol{y} \in \mathbb{Z}_2^k); (\boldsymbol{r} \in \mathbb{Z}_2^l, \boldsymbol{m}_i \in \mathbb{Z}_2^n, \boldsymbol{e} \in \{0,1\}_\omega^k,\ i = 1, \cdots, b): \boldsymbol{y} = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}_1|| \cdots ||\boldsymbol{m}_b) \oplus \boldsymbol{e} \wedge \|\boldsymbol{e}\|_1 = \omega \wedge VecToInt_2(\boldsymbol{m}_i) \in [0, 2^{n-\lambda_i}), i = 1, \cdots, b\}.$$

其具体的证明过程如协议 2 所述:

协议 2

生成证明:

1.证明者 $\mathcal{P}$ 随机选取 b+1 个随机置换$\pi \xleftarrow{\$} S_2^k$, $\pi_{mi} \xleftarrow{\$} S_2^{n-\lambda_i}$, b+2 个随机向量$\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_2^l$, $\boldsymbol{f} \xleftarrow{\$} \mathbb{Z}_2^k$, $\boldsymbol{s}_i' \xleftarrow{\$} \mathbb{Z}_2^{n-\lambda_i}$, 令 $\boldsymbol{s}_i = 0^\lambda \| \boldsymbol{s}_i'$, 其中$i = 1, \cdots, b$. 然后计算:

$$\begin{gathered}
\boldsymbol{t}_0 = \boldsymbol{A}(\boldsymbol{v}||\boldsymbol{s}_1|| \cdots ||\boldsymbol{s}_b) \oplus \boldsymbol{f}, \\
\boldsymbol{t}_1 = \pi(\boldsymbol{f}), \boldsymbol{t}_2 = \pi(\boldsymbol{f} \oplus \boldsymbol{e}), \\
\boldsymbol{t}_{m1} = \pi_{m1}(\boldsymbol{s}_1')|| \cdots ||\pi_{mb}(\boldsymbol{s}_b'), \\
\boldsymbol{t}_{m2} = \pi_{m1}(\boldsymbol{s}_1' \oplus \boldsymbol{m}_1')|| \cdots ||\pi_{mb}(\boldsymbol{s}_b' \oplus \boldsymbol{m}_b'), \\
\boldsymbol{C}_0 = Com(\pi, \pi_{m1}, \cdots, \pi_{mb}, \boldsymbol{t}_0, R_0), \\
\boldsymbol{C}_1 = Com(\boldsymbol{t}_1, \boldsymbol{t}_{m1}, R_1), \\
\boldsymbol{C}_2 = Com(\boldsymbol{t}_2, \boldsymbol{t}_{m2}, R_2), \\
\mathcal{P} \to \mathcal{V}:: (\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2).
\end{gathered}$$

2. $\mathcal{V}: \to \mathcal{P}: d \xleftarrow{\$} \{1,2,3\}$.

3. $\mathcal{P}$ 根据 $\mathcal{V}$ 的挑战值, 做出相应的回应:

1) $d = 1$时, $\mathcal{P}$ 打开$\boldsymbol{C}_0, \boldsymbol{C}_1$, 即发送$OPEN_1 = \{\pi,\ \pi_{m1}, \cdots, \pi_{m2}, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{t}_{m1}, R_0, R_1\}$.

2) $d = 2$时, $\mathcal{P}$ 打开$\boldsymbol{C}_0, \boldsymbol{C}_2$, 即发送$OPEN_2 = \{\pi,\ \pi_{m1}, \cdots, \pi_{m2}, \boldsymbol{t}_0, \boldsymbol{t}_2, \boldsymbol{t}_{m2}, R_0, R_2\}$.

3) $d = 3$时, $\mathcal{P}$ 打开$\boldsymbol{C}_1, \boldsymbol{C}_2$, 即发送$OPEN_3 = \{\boldsymbol{t}_1,\ \boldsymbol{t}_2, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}, R_1, R_2\}$.

验证:

将 **A** 划分为$\boldsymbol{A}_1||\boldsymbol{A}_2$, 其中$\boldsymbol{A}_1 \in \mathbb{Z}_2^{k\times l}$, $\boldsymbol{A}_2 \in \mathbb{Z}_2^{k\times bn}$。$d = 1$或 2 时, 划分$\pi^{-1}(\boldsymbol{t}_{md}) = (\boldsymbol{sp}_1, \cdots, \boldsymbol{sp}_b)$,其中$|\boldsymbol{sp}_i| = \lambda_i$, $i = 1, \cdots, b$. $\mathcal{V}$ 接受证明当且仅当:

1) $d = 1$时,

$$\begin{gathered}
\boldsymbol{t}_0 \oplus \pi^{-1}(\boldsymbol{t}_1) \oplus \boldsymbol{A}_2 \cdot (0^{\lambda_1}||\boldsymbol{sp}_1|| \cdots ||0^{\lambda_b}||\boldsymbol{sp}_b) \\
\in img\boldsymbol{A}_1 \\
\wedge \pi \in S_2^k \wedge \pi_{mi} \in S_2^{n-\lambda_i}.
\end{gathered}$$

2) $d = 2$时,

$$\begin{gathered}
\boldsymbol{y} \oplus \boldsymbol{t}_0 \oplus \pi^{-1}(\boldsymbol{t}_2) \oplus \boldsymbol{A}_2 \\
\cdot ((0^{\lambda_1}||\boldsymbol{sp}_1)|| \cdots ||(0^{\lambda_b}||\boldsymbol{sp}_b)) \\
\in img\boldsymbol{A}_1 \wedge \pi \in S_2^k \wedge \pi_{mi} \in S_2^{n-\lambda_i}.
\end{gathered}$$

3) $d = 3$时,

$$\|\boldsymbol{t}_1 \oplus \boldsymbol{t}_2\|_1 = \omega \wedge \boldsymbol{t}_{m1} \oplus \boldsymbol{t}_{m2} \in \mathbb{Z}_2^{bn-(\lambda_1+\cdots+\lambda_b)}.$$

定理 3: 如果协议 2 中的辅助承诺满足完美绑定性和计算隐藏性, 那么协议 2 是一个满足完美完备性和计算 SHVZK 的 Σ 协议, 其合理性错误率为 2/3。

定理 3 的证明和定理 1 的证明是几乎一样的, 只是参数的长度有略微不同, 因此这里不再给出详细的证明过程。

5 基于格问题的范围证明方案

本节将给出针对基于 SIS 问题和 LWE 问题的承诺方案构造的范围证明。LWE 假设和 SIS 假设是格上常见的两个假设, 它们在量子攻击下仍能保证一

定的安全性, 且基于 SIS 问题和 LWE 问题的承诺方案都是串承诺方案, 与本文构造范围证明方案的前提要求相契合。从定义上来看, LPN 问题可以看作是 LWE 问题的特殊形式, 而 xLPN 问题又是 LPN 问题的特例, SIS 问题在形式上与 LWE 问题有一定的相似性, 且有更加简单的结构, 因而 4.1 节中基于 xLPN 的范围证明方案的构造方法也适用于构造基于 LWE 和 SIS 的范围证明方案。在基于 xLPN 的范围方案中, 证明者通过引入随机变换π打乱向量中各分量的排列顺序, 既隐藏了向量的确切值, 又保证了向量中的每个分量值不被改变, 且向量的范数不发生变化。本节将沿用这种技巧来证明被承诺向量是前 λ 个分量都为 0 的$\mathbb{Z}_u$上的向量, 其中 u 的取值根据承诺方案的不同而不同。5.1 节将基于 SIS 问题, 给出证明$m \in [0, 2^{n-\lambda})$的协议, 而在 5.2 节中, 我们除了给出基于 LWE 问题的、证明$m \in [0, u^{n-\lambda})$的协议, 还将在此基础上稍作改变, 给出证明$m-a \in [0, u^{n-\lambda})$和$b-m \in [0, u^{n-\lambda})$的协议。

5.1 基于 SIS 的范围证明方案

在 2.3.3 小节介绍的基于 SIS 问题的承诺方案中, 承诺密钥 **A** 是定义在$\mathbb{Z}_q$上的, 而方案的消息空间为 $\mathbb{Z}_2$, 即 u=2. 根据承诺方案的验证条件, 基于 SIS 的范围证明方案除了要证明消息向量 **m** 是 0-1 向量, 还要证明其对应的随机向量 **r** 也是 0-1 向量, 因而整个方案共需引入两个随机变换。基于 SIS 问题的范围证明描述如下:

$$\{(\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{k\times(1+n)}, \boldsymbol{y} \in \mathbb{Z}_q^k); (\boldsymbol{r} \in \mathbb{Z}_2^l, \boldsymbol{m} \in \mathbb{Z}_2^n): \ \boldsymbol{y} = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m}) \bmod q \wedge \boldsymbol{m} \in \mathbb{Z}_2^n, \boldsymbol{r} \in \mathbb{Z}_2^l \wedge VecToInt_2(\boldsymbol{m}) \in [0, 2^{n-\lambda})\}.$$

证明者和验证者的公共输入为承诺密钥 **A** 和承诺值 **y**, 证明者的证据是生成 **y** 使用的随机数 **r** 和消息 **m**。此方案中的辅助承诺方案使用基于 SIS 的承诺方案, 即$Com(\boldsymbol{x}) = \boldsymbol{A}(\boldsymbol{r}||\boldsymbol{x})$, 因而在验证阶段, 打开承诺时发送的随机数 R, 其具体形式是一个与承诺值对应的长为 l 比特的随机 0-1 向量。当然, 如果选用其他的串承诺方案作为辅助协议时, R 的形式也会随之变化。协议 3 描述了证明的具体过程。

协议 3

生成证明:

1. 证明者 $\mathcal{P}$ 首先选取两个随机向量$\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_2^l$, $\boldsymbol{s}' \xleftarrow{\$} \mathbb{Z}_2^{n-\lambda}$, 和两个随机置换 $\pi_r \xleftarrow{\$} S_2^l$, $\pi_m \xleftarrow{\$} S_2^{n-\lambda}$, 然后令$\boldsymbol{s} = 0^\lambda||\boldsymbol{s}'$. $\mathcal{P}$ 计算:

$$\boldsymbol{t}_0 = \boldsymbol{A}(\boldsymbol{v}||\boldsymbol{s}),$$
$$\boldsymbol{t}_{r1} = \pi_r(\boldsymbol{v}), \boldsymbol{t}_{r2} = \pi_r(\boldsymbol{v}+\boldsymbol{r}),$$
$$\boldsymbol{t}_{m1} = \pi_m(\boldsymbol{s}'), \boldsymbol{t}_{m2} = \pi_m(\boldsymbol{s}'+\boldsymbol{m}'),$$
$$\boldsymbol{C}_0 = Com(\pi_r, \pi_m, \boldsymbol{t}_0, R_0),$$
$$\boldsymbol{C}_1 = Com(\boldsymbol{t}_{r1}, \boldsymbol{t}_{m1}, R_1),$$
$$\boldsymbol{C}_2 = Com(\boldsymbol{t}_{r2}, \boldsymbol{t}_{m2}, R_2),$$
$$\mathcal{P} \to \mathcal{V}: \ (\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2).$$

2. $\mathcal{V}: \to \mathcal{P}: d \xleftarrow{\$} \{1,2,3\}$.

3. $\mathcal{P}$ 根据 $\mathcal{V}$ 的挑战值, 做出相应的回应:

1) $d=1$时, $\mathcal{P}$ 打开$\boldsymbol{C}_0, \boldsymbol{C}_1$, 即发送$OPEN_1 = \{\pi_r, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_{r1}, \boldsymbol{t}_{m1}, R_0, R_1\}$.

2) $d=2$时, $\mathcal{P}$ 打开$\boldsymbol{C}_0, \boldsymbol{C}_2$, 即发送$OPEN_2 = \{\pi_r, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_{r2}, \boldsymbol{t}_{m2}, R_0, R_2\}$.

3) $d=3$时, $\mathcal{P}$ 打开$\boldsymbol{C}_1, \boldsymbol{C}_2$, 即发送$OPEN_3 = \{\pi_r, \boldsymbol{t}_{r2}, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}, R_1, R_2\}$.

验证:

将 **A** 划分为$\boldsymbol{A}_1||\boldsymbol{A}_2$, 其中$\boldsymbol{A}_1 \in \mathbb{Z}_q^{k\times l}$, $\boldsymbol{A}_2 \in \mathbb{Z}_q^{k\times n}$. $\mathcal{V}$ 接受证明当且仅当:

1) $d=1$时,

$$\boldsymbol{t}_0 = \boldsymbol{A} \cdot (\pi_r^{-1}(\boldsymbol{t}_{r1})||0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m1})) \wedge \pi_r \in S_2^l \wedge \pi_m \in S_2^{n-\lambda}.$$

2) $d=2$时,

$$\boldsymbol{y}+\boldsymbol{t}_0 = \boldsymbol{A} \cdot (\pi_r^{-1}(\boldsymbol{t}_{r2})||0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m2})) \wedge \pi_r \in S_2^l \wedge \pi_m \in S_2^{n-\lambda}.$$

3) $d=3$时,

$$\boldsymbol{t}_{r2}-\boldsymbol{t}_{r1} \in \mathbb{Z}_2^l \wedge \boldsymbol{t}_{m2}-\boldsymbol{t}_{m1} \in \mathbb{Z}_2^{n-\lambda}.$$

定理 4: 如果协议 3 中的辅助承诺满足计算绑定性和统计隐藏性, 那么协议 3 是一个满足完美完备性和统计 SHVZK 的 Σ 协议, 其合理性错误率为 2/3。

证明: **完备性**: 变换π_r, π_m容易验证。根据挑战值的不同:

1) $d=1$时,

$$\boldsymbol{A} \cdot (\pi_r^{-1}(\boldsymbol{t}_{r1})||0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m1})) = \boldsymbol{A} \cdot (\boldsymbol{v}||0^\lambda||\boldsymbol{s}') = \boldsymbol{t}_0.$$

2) $d=2$时,

$$\begin{aligned} &\boldsymbol{A} \cdot (\pi_r^{-1}(\boldsymbol{t}_{r2}) \,\|\, 0^\lambda \,\|\, \pi_m^{-1}(\boldsymbol{t}_{m2})) \\ &= \boldsymbol{A} \cdot ((\boldsymbol{v}+\boldsymbol{r}) \,\|\, 0^\lambda \,\|\, (\boldsymbol{s}'+\boldsymbol{m}')) \\ &= \boldsymbol{A} \cdot (\boldsymbol{r} \,\|\, 0^\lambda \,\|\, \boldsymbol{m}') + \boldsymbol{A} \cdot (\boldsymbol{v} \,\|\, 0^\lambda \,\|\, \boldsymbol{s}') \\ &= \boldsymbol{y} + \boldsymbol{t}_0. \end{aligned}$$

3) $d=3$时,

$$\boldsymbol{t}_{r2}-\boldsymbol{t}_{r1} = \pi_r(\boldsymbol{v}+\boldsymbol{r}) - \pi_r(\boldsymbol{v}) = \pi_r(\boldsymbol{r}) \in \mathbb{Z}_2^l,$$
$$\boldsymbol{t}_{m2}-\boldsymbol{t}_{m1} = \pi_m(\boldsymbol{s}'+\boldsymbol{m}') - \pi_m(\boldsymbol{s}') = \pi_m(\boldsymbol{m}') \in \mathbb{Z}_2^{n-\lambda}.$$

特殊的合理性: 根据辅助承诺方案的绑定性, 一个承诺值只能被打开为唯一一组被承诺值和对应的随机数。如果证明者 $\mathcal{P}^*$ 对于固定的$(\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2)$, 能

够得到的三个挑战值分别为 1, 2, 3 的可接受交互副本，那么 $\mathcal{P}^*$ 就能得从中得到对应同一组证据 $(\boldsymbol{r},\boldsymbol{m},\boldsymbol{e})$的全部参数$\pi_r,\pi_m,\boldsymbol{t}_0,\boldsymbol{t}_{r1},\boldsymbol{t}_{r2},\boldsymbol{t}_{m1},\boldsymbol{t}_{m2}$，此时，根据以下两式:

$$\pi_r^{-1}(\boldsymbol{t}_{r2}-\boldsymbol{t}_{r1})=\pi_r^{-1}(\pi_r(\boldsymbol{v}+\boldsymbol{r})-\pi_r(\boldsymbol{v}))=\boldsymbol{r},$$
$$\pi_m^{-1}(\boldsymbol{t}_{m2}-\boldsymbol{t}_{m1})=\pi_m^{-1}(\pi_m(\boldsymbol{s}'+\boldsymbol{m}')-\pi_m(\boldsymbol{s}'))=\boldsymbol{m}',$$

$\mathcal{P}^*$ 可以抽取出一组合法的证据$(\boldsymbol{r},\boldsymbol{m}=0^\lambda||\boldsymbol{m}')$。

与前文协议类似，在挑战值为 1 或 3 时，没有证据的恶意证明者 $\mathcal{P}^*$ 仍然能使验证者相信他拥有和承诺值对应的合法证据$(\boldsymbol{r},\boldsymbol{m})$，而挑战值为 2 时，只有真正拥有证据的证明者才能使验证者接受证明。因而合理性错误率为 2/3。

特殊的诚实验证者零知识性: 存在一个高效的模拟器 S，给定不同的挑战值，S 能够输出不同的可接受副本，并且 S 输出的副本的分布与诚实证明者在真实交换中产生的副本的分布是不可区分的。S 的描述如下:

1) $d=1$时，模拟器 S 像诚实的证明者一样计算 $\boldsymbol{C}_0^*,\boldsymbol{C}_1^*$，同时计算 $\boldsymbol{C}_2^*=Com(\boldsymbol{0}^n)$. 显然的，$\boldsymbol{C}_0^*$，$\boldsymbol{C}_1^*,OPEN_1^*=\{\pi_r^*,\pi_m^*,\boldsymbol{t}_0^*,\boldsymbol{t}_{r1}^*,\boldsymbol{t}_{m1}^*,R_0^*,R_1^*\}$的分布与真实交互中的分布是完全相同的，且整个交互副本是一个可接受副本。而由承诺方案的隐藏性可知，$\boldsymbol{C}_2^*$此时的分布与真实交互中$\boldsymbol{C}_2$的分布计算不可区分。

2) $d=2$时，模拟器 S 像真实交互一样选取 $\pi_r^*,\pi_m^*,\ \boldsymbol{v}^*,\boldsymbol{s}'^*,\boldsymbol{s}^*$，计算:

$$\boldsymbol{t}_0^*=\boldsymbol{A}(\boldsymbol{v}^*||\boldsymbol{s}^*)-\boldsymbol{y},\boldsymbol{t}_{r2}^*=\pi_r^*(\boldsymbol{v}^*),$$
$$\boldsymbol{t}_{m2}^*=\pi_m^*(\boldsymbol{s}'^*),\boldsymbol{C}_1^*=Com(\boldsymbol{0}^n).$$

然后按照真实协议计算$\boldsymbol{C}_0^*,\boldsymbol{C}_2^*$. 根据承诺方案的隐藏性，$\boldsymbol{C}_1^*$此时的分布与真实交互中$\boldsymbol{C}_1$的分布是计算不可区分的。此外，容易验证，通过这种方式生成的 $\boldsymbol{C}_0^*,\boldsymbol{C}_2^*,OPEN_2^*=\{\pi_r^*,\pi_m^*,\boldsymbol{t}_0^*,\boldsymbol{t}_{r2}^*,\boldsymbol{t}_{m2}^*,R_0^*,R_2^*\}$的分布与真实交互中的分布是完全相同的，且这个副本在第三轮交互中能够被验证者接受。

3) $d=3$ 时，模拟器 S 选取向量 $\boldsymbol{t}_{r1}^*,\boldsymbol{t}_{r2}^*\xleftarrow{\$}\mathbb{Z}_2^l,\boldsymbol{t}_{m1}^*,\boldsymbol{t}_{m2}^*\xleftarrow{\$}\mathbb{Z}_2^{n-\lambda}$，并计算 $\boldsymbol{C}_0^*=Com(\boldsymbol{0}^n)$. $\boldsymbol{C}_1^*,\boldsymbol{C}_2^*$按照真实协议计算。整个交互产生的副本是一个可接受副本。由承诺方案的隐藏性可知，$\boldsymbol{C}_0^*$的分布与真实交互中$\boldsymbol{C}_0$的分布是计算不可区分的。而 $\boldsymbol{C}_1^*,\boldsymbol{C}_2^*,OPEN_3^*=\{\boldsymbol{t}_{r1}^*,\boldsymbol{t}_{r2}^*,\boldsymbol{t}_{m1}^*,\boldsymbol{t}_{m2}^*,R_1^*,R_2^*\}$的分布与真实交互中的分布是完全相同的。

5.2 基于 LWE 的范围证明方案

受到所针对的承诺方案限制，4.1 节和 5.1 节给出的范围证明方案的消息空间都为$\mathbb{Z}_2$，这使得这两种方案只适用于给定区间形式为$[0,2^{n-\lambda})$的情况，即区间的上限只能是 2 的幂。而 2.3.1 小节中介绍的基于 LWE 问题的承诺方案，其参数空间和消息空间都为 $\mathbb{Z}_q$. 基于此，本节将构造更加灵活的范围证明方案，其消息空间为$\mathbb{Z}_u$，其中 u 可以根据通信双方的需求，选取 2 到 q 之间的任意正整数。此外，在前文中提出的各个协议中，给定区间都为$[0,2^{n-\lambda})$的形式，区间的上下界在形式上有一定的限制。为了解决这一问题，本小节将针对基于 LWE 问题的串承诺方案(见 2.3.1)，根据不同形式的给定区间，提出不同的范围证明方案。当给定对消息 m 的承诺值 **y** 时，协议 4 适用于证明$m\in[0,u^{n-\lambda})$，协议 5 和协议 6 分别针对区间形式为$m-a\in[0,u^{n-\lambda})$和$m-b\in[0,u^{n-\lambda})$的情况，其中 a 和 b 是公开的正整数。为了与前文的符号约定保持一致，此处记 a、b 对应的 n 维 u 进制向量为 $\boldsymbol{a}$、$\boldsymbol{b}$，并令$\boldsymbol{a}'$、$\boldsymbol{b}'$分别表示它们的后$n-\lambda$个分量。$m-a\in[0,u^{n-\lambda})$和$m-b\in[0,u^{n-\lambda})$可以等价地写成$m\in[a,a+u^{n-\lambda})$和$m\in(b-u^{n-\lambda},b]$的形式，据此，当$b-a<u^{n-\lambda}$时，同时使用协议 5 和协议 6 就能够证明$m\in[a,b]$.

5.2.1 针对$\boldsymbol{m}\in[\boldsymbol{0},\boldsymbol{u}^{\boldsymbol{n}-\boldsymbol{\lambda}})$的证明

本小节中的协议 4 与协议 1 在形式上几乎是一样的，只是针对的承诺方案是基于 LWE 问题的承诺方案，从而参数设置也随之产生了变化。该版本的范围证明方案描述如下:

$$\{(\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_q^{k\times(1+n)},\boldsymbol{y}\in\mathbb{Z}_q^k);(\boldsymbol{r}\in\mathbb{Z}_q^l,\boldsymbol{m}\in\mathbb{Z}_u^n,\boldsymbol{e}\in\mathbb{Z}_q^k):$$
$$\boldsymbol{y}=\boldsymbol{A}(\boldsymbol{r}\,||\,\boldsymbol{m})+\boldsymbol{e}\ \bmod q\wedge\|\boldsymbol{e}\|_\infty\leqslant\beta\wedge$$
$$\boldsymbol{m}\in\mathbb{Z}_u^n,\boldsymbol{r}\in\mathbb{Z}_q^l\wedge VecToInt_u(\boldsymbol{m})\in[0,u^{n-\lambda})\}.$$

证明者和验证者的公共输入为承诺密钥 $\boldsymbol{A}$ 和承诺值 $\boldsymbol{y}$，证明者的证据是生成 $\boldsymbol{y}$ 使用的随机向量 $\boldsymbol{r}$，消息 $\boldsymbol{m}$ 和噪声 $\boldsymbol{e}$. 辅助承诺可以选用任意的串承诺方案，R 表示辅助承诺中使用的随机数。方便起见，此处选取 2.3.1 中基于 LWE 的承诺方案，R 对应一个随机向量 $\boldsymbol{r}$ 和一个噪声向量 $\boldsymbol{e}$. 证明过程的具体描述如协议 4。

协议 4

生成证明:

1. 证明者 $\mathcal{P}$ 随机选取三个随机向量$\boldsymbol{v}\xleftarrow{\$}\mathbb{Z}_q^l$，$\boldsymbol{f}\xleftarrow{\$}\mathbb{Z}_q^k$，$\boldsymbol{s}'\xleftarrow{\$}\mathbb{Z}_u^{n-\lambda}$，两个置换：$\pi\xleftarrow{\$}S_q^k$，$\pi_m\xleftarrow{\$}S_u^{n-\lambda}$. 令$\boldsymbol{s}=0^\lambda||\boldsymbol{s}'$，$\mathcal{P}$ 计算:

$$\boldsymbol{t}_0=\boldsymbol{A}(\boldsymbol{v}||\boldsymbol{s})+\boldsymbol{f},$$
$$\boldsymbol{t}_1=\pi(\boldsymbol{f}),\boldsymbol{t}_2=\pi(\boldsymbol{f}+\boldsymbol{e}),$$
$$\boldsymbol{t}_{m1}=\pi_m(\boldsymbol{s}'),\boldsymbol{t}_{m2}=\pi_m(\boldsymbol{s}'+\boldsymbol{m}'),$$
$$\boldsymbol{C}_0=Com(\pi,\pi_m,\boldsymbol{t}_0,R_0),$$

$$\boldsymbol{C}_1 = Com(\boldsymbol{t}_1, \boldsymbol{t}_{m1}, R_1),$$
$$\boldsymbol{C}_2 = Com(\boldsymbol{t}_2, \boldsymbol{t}_{m2}, R_2),$$
$$\mathcal{P} \to \mathcal{V}:: (\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2).$$

2. $\mathcal{V}: \to \mathcal{P}: d \xleftarrow{\$} \{1,2,3\}$.

3. $\mathcal{P}$ 根据 $\mathcal{V}$ 的挑战值, 做出相应的回应:

1) $d = 1$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0, \boldsymbol{C}_1$, 即 $\mathcal{P} \to \mathcal{V}:: OPEN_1 = \{\pi, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{t}_{m1}, R_0, R_1\}$.

2) $d = 2$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0, \boldsymbol{C}_2$, 即 $\mathcal{P} \to \mathcal{V}:: OPEN_2 = \{\pi, \pi_m, \boldsymbol{t}_0, \boldsymbol{t}_2, \boldsymbol{t}_{m2}, R_0, R_2\}$.

3) $d = 3$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_1, \boldsymbol{C}_2$, 即 $\mathcal{P} \to \mathcal{V}:: OPEN_3 = \{\boldsymbol{t}_1, \boldsymbol{t}_2, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}, R_1, R_2\}$.

验证:

将 $\boldsymbol{A}$ 划分为$\boldsymbol{A}_1||\boldsymbol{A}_2$, 其中$\boldsymbol{A}_1 \in \mathbb{Z}_q^{k \times l}$, $\boldsymbol{A}_2 \in \mathbb{Z}_q^{k \times n}$。$\mathcal{V}$ 接受证明当且仅当:

1) $d = 1$时,

$$\boldsymbol{t}_0 - \boldsymbol{A}_2 \cdot (0^\lambda || \pi_m^{-1}(\boldsymbol{t}_{m1})) - \pi^{-1}(\boldsymbol{t}_1) \in img\boldsymbol{A}_1 \wedge \pi \in S_q^k \wedge \pi_m \in S_u^{n-\lambda}.$$

2) $d = 2$时,

$$\boldsymbol{y} + \boldsymbol{t}_0 - \boldsymbol{A}_2 \cdot (0^\lambda || \pi_m^{-1}(\boldsymbol{t}_{m2})) - \pi^{-1}(\boldsymbol{t}_2) \in img\boldsymbol{A}_1 \wedge \pi \in S_q^k \wedge \pi_m \in S_u^{n-\lambda}.$$

3) $d = 3$时,

$$\boldsymbol{t}_{m2} - \boldsymbol{t}_{m1} \in \mathbb{Z}_u^{n-\lambda} \wedge ||\boldsymbol{t}_2 - \boldsymbol{t}_1||_\infty \leqslant \beta.$$

定理 5: 如果协议 4 中的辅助承诺满足完美绑定性和计算隐藏性, 那么协议 4 是一个满足完美完备性和计算 SHVZK 的 Σ 协议, 其合理性错误率为 2/3。

证明: 完备性的证明是显然的。随机变换π, π_m容易验证。根据挑战值的不同:

1) $d = 1$时,

$$\begin{aligned}&\boldsymbol{t}_0 - \boldsymbol{A}_2 \cdot (0^\lambda \,||\, \pi_m^{-1}(\boldsymbol{t}_{m1})) - \pi^{-1}(\boldsymbol{t}_1)\\ &= \boldsymbol{A} \cdot (\mathbf{v} \,||\, \boldsymbol{s}) + \boldsymbol{f} - \boldsymbol{A}_2 \cdot (\boldsymbol{v} \,||\, 0^\lambda \,||\, \boldsymbol{s}') - \boldsymbol{f}\\ &= \boldsymbol{A}_1 \cdot \mathbf{v} \in img\mathbf{A}_1.\end{aligned}$$

2) $d = 2$时,

$$\begin{aligned}&\boldsymbol{y} + \boldsymbol{t}_0 - \boldsymbol{A}_2 \cdot (0^\lambda \,||\, \pi_m^{-1}(\boldsymbol{t}_{m2})) - \pi^{-1}(\boldsymbol{t}_2)\\ &= \boldsymbol{A}_1 \cdot (\boldsymbol{r} + \boldsymbol{v}) + \boldsymbol{A}_2 \cdot (\boldsymbol{m} + \boldsymbol{s}) - \boldsymbol{A}_2 \cdot (0^\lambda \,||\, (\boldsymbol{s}' + \boldsymbol{m}'))\\ &= \boldsymbol{A}_1 \cdot (\boldsymbol{r} + \boldsymbol{v}) \in img\boldsymbol{A}_1.\end{aligned}$$

3) $d = 3$时,

$$\boldsymbol{t}_{m2} - \boldsymbol{t}_{m1} = \pi_m(\boldsymbol{s}' + \boldsymbol{m}') - \pi_m(\boldsymbol{s}') = \pi_m(\boldsymbol{m}') \in \mathbb{Z}_u^{n-\lambda},$$
$$||\boldsymbol{t}_2 - \boldsymbol{t}_1||_\infty = ||\pi(\boldsymbol{f} + \boldsymbol{e}) - \pi(\boldsymbol{f})||_\infty = ||\pi(\boldsymbol{e})||_\infty \leqslant \beta.$$

特殊的合理性: 根据定理中对承诺方案绑定性的假设, 每个承诺值对应唯一一组被承诺值及相应的随机数。固定第一轮消息$(\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2)$, 如果一个(可能是恶意的)证明者 $\mathcal{P}^*$ 能够得到三个挑战值分别为 1, 2, 3 的可接受副本, 即得到了对应同一组证据的 $\pi, \pi', \boldsymbol{t}_0, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}, \boldsymbol{t}_1, \boldsymbol{t}_2$, 那么 $\mathcal{P}^*$ 就可以从中抽取出诚实证明者的证据$(\boldsymbol{r}, \boldsymbol{m}, \boldsymbol{e})$:

$$\pi^{-1}(\boldsymbol{t}_2 - \boldsymbol{t}_1) = \pi^{-1}(\pi(\boldsymbol{f} + \boldsymbol{e}) - \pi(\boldsymbol{f})) = \boldsymbol{e},$$
$$\boldsymbol{A}^{-1} \cdot (\boldsymbol{y} - \boldsymbol{e}) = \boldsymbol{r}||\boldsymbol{m}.$$

挑战值为 2 时, 只有真正拥有证据的诚实证明者才能使验证者接受证明, 而挑战值为 1 或 3 时, 没有证据的恶意证明者 $\mathcal{P}^*$ 仍然能生成合法的证明, 使验证者相信他拥有和承诺值对应的证据$(\boldsymbol{r}, \boldsymbol{m}, \boldsymbol{e})$, 据此, 合理性错误率为 2/3。

特殊的诚实验证者零知识性: 存在一个高效的模拟器 S, 根据给定的挑战值, 它能够输出不同的可接受副本, 并且 S 输出的副本的分布与诚实证明者在真实交互中产生的副本分布是不可区分的。S 的描述如下:

1) $d = 1$时, 模拟器 S 像诚实的证明者一样计算 $\boldsymbol{C}_0^*, \boldsymbol{C}_1^*$, 同时计算 $\boldsymbol{C}_2^* = Com(\mathbf{0}^*)$. 显然, $\boldsymbol{C}_0^*, \boldsymbol{C}_1^*$, $OPEN_1^* = \{\pi^*, \pi_m^*, \boldsymbol{t}_0^*, \boldsymbol{t}_1^*, \boldsymbol{t}_{m1}^*, R_0^*, R_1^*\}$的分布与真实交互中的分布是完全相同的, 且整个交互副本是一个可接受副本。而由承诺方案的隐藏性可知, $\boldsymbol{C}_2^*$此时的分布与真实交互中$\boldsymbol{C}_2$的分布计算不可区分。

2) $d = 2$时, 模拟器 S 像真实交互一样选取 $\pi^*, \pi_m^*, \boldsymbol{v}^*, \boldsymbol{s}'^*, \boldsymbol{s}^*$, 计算:

$$\boldsymbol{C}_1^* = Com(\mathbf{0}^n), \boldsymbol{t}_0^* = \boldsymbol{A}(\boldsymbol{v}^* || \boldsymbol{s}^*) + \boldsymbol{f}^* - \boldsymbol{y},$$
$$\boldsymbol{t}_2^* = \pi^*(\boldsymbol{f}^*), \boldsymbol{t}_{m2}^* = \pi'^*(\boldsymbol{s}'^*).$$

然后按照真实协议计算$\boldsymbol{C}_0^*, \boldsymbol{C}_2^*$. 容易验证, 在验证阶段, 打开$\boldsymbol{C}_0^*, \boldsymbol{C}_2^*$时发送的各参数能够通过验证。$\boldsymbol{C}_0^*, \boldsymbol{C}_2^*, OPEN_2^* = \{\pi^*, \pi_m^*, \boldsymbol{t}_0^*, \boldsymbol{t}_2^*, \boldsymbol{t}_{m2}^*, R_0^*, R_2^*\}$此时的分布与真实交互中的分布完全一致。根据承诺方案的隐藏性, $\boldsymbol{C}_1^*$此时的分布与真实交互中$\boldsymbol{C}_1$的分布是计算不可区分的。

3) $d = 3$时, S 选取$\mathbf{h}^* \xleftarrow{\$} \chi^k$, $\boldsymbol{t}_{m1}^*, \boldsymbol{t}_{m2}^* \xleftarrow{\$} \mathbb{Z}_u^{n-\lambda}$, $\boldsymbol{t}_1^* \xleftarrow{\$} \mathbb{Z}_q^k$, 令$\boldsymbol{t}_2^* = \boldsymbol{t}_1^* + \boldsymbol{h}^*$, $\boldsymbol{C}_0^* = Com(\mathbf{0}^n)$, $\boldsymbol{C}_1^*, \boldsymbol{C}_2^*$按照真实协议计算。整个交互产生的副本是一个可接受副本。可以看出此时 $\boldsymbol{C}_1^*, \boldsymbol{C}_2^*, OPEN_3^* = \{\boldsymbol{t}_1^*, \boldsymbol{t}_2^*, \boldsymbol{t}_{m1}^*, \boldsymbol{t}_{m2}^*, R_0^*, R_2^*\}$的分布与真实交互中的分布是完全相同的。而由承诺方案的隐藏性可知, $\boldsymbol{C}_0^*$的分布与真实交互中$\boldsymbol{C}_0$的分布计算不可区分。

5.2.2 针对$\boldsymbol{m} - \boldsymbol{a} \in [\mathbf{0}, \boldsymbol{u}^{n-\lambda})$的证明

根据本文的基本思想, 当$m - a \in [0, u^{n-\lambda})$时, 其对应的 u 进制向量 $\boldsymbol{m}$-$\boldsymbol{a}$ 的前$n - \lambda$位都为 0。然而此处基于 LWE 问题的承诺方案并不满足同态性, 不能直接

由对m的承诺值和对a的承诺值得到对$m-a$的承诺值, 从而无法直接套用之前的协议。注意到承诺密钥 **A** 和正整数 a 是公开的, 此处我们使用一些简单的数学拼接技巧, 就能由m的承诺值凑出对$m-a$的承诺值。首先将 **A** 划分为$\boldsymbol{A}_1||\boldsymbol{A}_2$, 其中$\boldsymbol{A}_1 \in \mathbb{Z}_q^{k\times l}$, $\boldsymbol{A}_2 \in \mathbb{Z}_q^{k\times n}$, 由 m 的承诺值$\boldsymbol{y}=\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})+\boldsymbol{e}$, 有如下变换:

$$\boldsymbol{y}-\boldsymbol{A}_2\cdot\boldsymbol{a}=\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})+\boldsymbol{e}-\boldsymbol{A}_2\cdot\boldsymbol{a}=\boldsymbol{A}_1\boldsymbol{r}+\boldsymbol{A}_2(\boldsymbol{m}-\boldsymbol{a})+\boldsymbol{e}.$$

即得到了对$m-a$的承诺值。根据这一等式, 再结合当$m-a\in[0,u^{n-\lambda})$时, 向量$\boldsymbol{m}-\boldsymbol{a}$可以划分为$0^\lambda||(\boldsymbol{m}'-\boldsymbol{a}')$, 我们只需在协议 4 的基础上稍作改变, 就能够得到针对$m-a\in[0,u^{n-\lambda})$的范围证明方案。该方案描述如下:

$$\{(a\in\mathbb{Z},\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_q^{k\times(1+n)},\boldsymbol{y}\in\mathbb{Z}_q^k);(\boldsymbol{r}\in\mathbb{Z}_q^l,\boldsymbol{m}\in\mathbb{Z}_u^n,\boldsymbol{e}\in\mathbb{Z}_q^k):$$
$$\boldsymbol{y}=\boldsymbol{A}(\boldsymbol{r}\,\|\,\boldsymbol{m})+\boldsymbol{e}\ \bmod q\wedge\|\boldsymbol{e}\|_\infty\leqslant\beta\wedge$$
$$\boldsymbol{m}\in\mathbb{Z}_u^n,\boldsymbol{r}\in\mathbb{Z}_q^l\wedge VecToInt_u(\boldsymbol{m}-\boldsymbol{a})\in[0,u^{n-\lambda})\}.$$

除去证明者和验证者的公共输入多了一项区间下界 a 之外, 方案中的各项参数与协议 4 一致。证明过程中的参数个数和尺寸并不发生变化, 只是在生成第一轮消息时, $\boldsymbol{t}_{m1}$和$\boldsymbol{t}_{m2}$的计算方式稍有变化, 验证过程也随之产生了一些改变。证明过程的具体描述如协议 5。

协议 5

生成证明:

1. 证明者 $\mathcal{P}$ 随机选取三个随机向量$\boldsymbol{v}\xleftarrow{\$}\mathbb{Z}_q^l$, $\boldsymbol{f}\xleftarrow{\$}\mathbb{Z}_q^k$, $\boldsymbol{s}'\xleftarrow{\$}\mathbb{Z}_u^{n-\lambda}$, 两个置换: $\pi\xleftarrow{\$}S_q^k$, $\pi_m\xleftarrow{\$}S_u^{n-\lambda}$. 令$\boldsymbol{s}=0^\lambda||\boldsymbol{s}'$, $\mathcal{P}$ 计算:

$$\boldsymbol{t}_0=\boldsymbol{A}(\boldsymbol{v}||\boldsymbol{s})+\boldsymbol{f},$$
$$\boldsymbol{t}_1=\pi(\boldsymbol{f}),\boldsymbol{t}_2=\pi(\boldsymbol{f}+\boldsymbol{e}),$$
$$\boldsymbol{t}_{m1}=\pi_m(\boldsymbol{s}'-\boldsymbol{a}'),\boldsymbol{t}_{m2}=\pi_m(\boldsymbol{s}'+\boldsymbol{m}'-\boldsymbol{a}'),$$
$$\boldsymbol{C}_0=Com(\pi,\pi_m,\boldsymbol{t}_0,R_0),$$
$$\boldsymbol{C}_1=Com(\boldsymbol{t}_1,\boldsymbol{t}_{m1},R_1),$$
$$\boldsymbol{C}_2=Com(\boldsymbol{t}_2,\boldsymbol{t}_{m2},R_2),$$
$$\mathcal{P}\to\mathcal{V}::(\boldsymbol{C}_0,\boldsymbol{C}_1,\boldsymbol{C}_2).$$

2. $\mathcal{V}:\to\mathcal{P}:d\xleftarrow{\$}\{1,2,3\}$.

3. $\mathcal{P}$ 根据 $\mathcal{V}$ 的挑战值, 做出相应的回应:

1) $d=1$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0,\boldsymbol{C}_1$, 即 $\mathcal{P}\to\mathcal{V}::OPEN_1=\{\pi,\ \pi_m,\boldsymbol{t}_0,\boldsymbol{t}_1,\boldsymbol{t}_{m1},R_0,R_1\}$.

2) $d=2$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0,\boldsymbol{C}_2$, 即 $\mathcal{P}\to\mathcal{V}::OPEN_2=\{\pi,\pi_m,\boldsymbol{t}_0,\boldsymbol{t}_2,\boldsymbol{t}_{m2},R_0,R_2\}$.

3) $d=3$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_1,\boldsymbol{C}_2$, 即 $\mathcal{P}\to\mathcal{V}::OPEN_3=\{\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_{m1},\boldsymbol{t}_{m2},R_1,R_2\}$.

验证:

将 **A** 划分为$\boldsymbol{A}_1||\boldsymbol{A}_2$, 其中$\boldsymbol{A}_1\in\mathbb{Z}_q^{k\times l}$, $\boldsymbol{A}_2\in\mathbb{Z}_q^{k\times n}$。$\mathcal{V}$ 接受证明当且仅当:

1) $d=1$时,

$$\boldsymbol{t}_0-\boldsymbol{A}_2\cdot(0^\lambda||\boldsymbol{a}')-\boldsymbol{A}_2\cdot(0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m1}))-\pi^{-1}(\boldsymbol{t}_1)\in img\boldsymbol{A}_1$$
$$\wedge\pi\in S_q^k\wedge\pi_m\in S_u^{n-\lambda}.$$

2) $d=2$时,

$$\boldsymbol{y}+\boldsymbol{t}_0-\boldsymbol{A}_2\cdot\boldsymbol{a}-\boldsymbol{A}_2\cdot(0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m2}))-\pi^{-1}(\boldsymbol{t}_2)\in img\boldsymbol{A}_1$$
$$\wedge\pi\in S_q^k\wedge\pi_m\in S_u^{n-\lambda}.$$

3) $d=3$时,

$$\boldsymbol{t}_{m2}-\boldsymbol{t}_{m1}\in\mathbb{Z}_u^{n-\lambda}\wedge\ ||\boldsymbol{t}_2-\boldsymbol{t}_1||_\infty\leqslant\beta\ .$$

定理 6: 如果协议 5 中的辅助承诺满足完美绑定性和计算隐藏性, 那么协议 5 是一个满足完美完备性和计算 SHVZK 的 Σ 协议, 其合理性错误率为 2/3。

证明: 完备性的证明是显然的。随机变换π,π_m容易验证。根据挑战值的不同:

1) $d=1$时,

$$\boldsymbol{t}_0-\boldsymbol{A}_2\cdot(0^\lambda\,\|\,\boldsymbol{a}')-\boldsymbol{A}_2(0^\lambda\,\|\,\pi_m^{-1}(\boldsymbol{t}_{m1}))-\pi^{-1}(\boldsymbol{t}_1)$$
$$=\boldsymbol{A}_1\mathbf{v}+\boldsymbol{A}_2\boldsymbol{s}+\boldsymbol{f}-\boldsymbol{A}_2(0^\lambda\,\|\,\boldsymbol{a}')-\boldsymbol{A}_2(0^\lambda\,\|\,(\boldsymbol{s}'-\boldsymbol{a}'))-\boldsymbol{f}$$
$$=\boldsymbol{A}_1\mathbf{v}\in img\mathbf{A}_1.$$

2) $d=2$时,

$$\boldsymbol{y}+\boldsymbol{t}_0-\boldsymbol{A}_2\boldsymbol{a}-\boldsymbol{A}_2(0^\lambda\,\|\,\pi_m^{-1}(\boldsymbol{t}_{m1}))-\pi^{-1}(\boldsymbol{t}_2)$$
$$=\boldsymbol{A}_1(\boldsymbol{r}+\boldsymbol{v})+\boldsymbol{A}_2(\boldsymbol{m}+\boldsymbol{s}-\boldsymbol{a})-\boldsymbol{A}_2(0^\lambda\,\|\,(\boldsymbol{s}'+\boldsymbol{m}'-\boldsymbol{a}'))$$
$$=\boldsymbol{A}_1(\boldsymbol{r}+\boldsymbol{v})\in img\boldsymbol{A}_1.$$

3) $d=3$时,

$$\boldsymbol{t}_{m2}-\boldsymbol{t}_{m1}=\pi_m(\boldsymbol{m}')\in\mathbb{Z}_u^{n-\lambda},$$
$$||\boldsymbol{t}_2-\boldsymbol{t}_1||_\infty=||\pi(\boldsymbol{f}+\boldsymbol{e})-\pi(\boldsymbol{f})||_\infty=||\pi(\boldsymbol{e})||_\infty\leqslant\beta.$$

特殊的合理性: 固定第一轮消息$(\boldsymbol{C}_0,\boldsymbol{C}_1,\boldsymbol{C}_2)$, 如果一个(可能是恶意的)证明者 $\mathcal{P}^*$ 能够得到三个挑战值分别为 1, 2, 3 的可接受副本, 根据承诺方案的绑定性, $\mathcal{P}^*$ 就能得到对应于同一组证据的π,π', $\boldsymbol{t}_0,\boldsymbol{t}_{m1},\boldsymbol{t}_{m2},\boldsymbol{t}_1,\boldsymbol{t}_2$, 那么通过以下两式, 他就可以从中抽取出诚实证明者的合法证据$(\boldsymbol{r},\boldsymbol{m},\boldsymbol{e})$:

$$\pi^{-1}(\boldsymbol{t}_2-\boldsymbol{t}_1)=\pi^{-1}(\pi(\boldsymbol{f}+\boldsymbol{e})-\pi(\boldsymbol{f}))=\boldsymbol{e},$$
$$\boldsymbol{A}^{-1}\cdot(\boldsymbol{y}-\boldsymbol{e})=\boldsymbol{r}||\boldsymbol{m}.$$

挑战值为 2 时, 只有真正拥有证据的诚实证明者才能使验证者接受证明, 而挑战值为 1 或 3 时, 没有证据的恶意证明者 $\mathcal{P}^*$ 仍然能生成合法的证明, 使验证者相信他拥有和承诺值对应的证据$(\boldsymbol{r},\boldsymbol{m},\boldsymbol{e})$, 据此, 合理性错误率为 2/3。

特殊的诚实验证者零知识性: 存在一个高效的模拟器 S, 根据给定的挑战值, 它能够输出不同的可接受

副本, 并且 S 输出的副本的分布与诚实证明者在真实交互中产生的副本分布是不可区分的。S 的描述如下:

1) $d=1$时, 模拟器 S 像诚实的证明者一样计算$\boldsymbol{C}_0^*,\boldsymbol{C}_1^*$, 同时计算$\boldsymbol{C}_2^*=Com(\boldsymbol{0}^*)$. 显然, $\boldsymbol{C}_0^*,\boldsymbol{C}_1^*$, $OPEN_1^*=\{\pi^*,\pi_m^*,\boldsymbol{t}_0^*,\boldsymbol{t}_1^*,\boldsymbol{t}_{m1}^*,R_0^*,R_1^*\}$的分布与真实交互中的分布是完全相同的, 且整个交互副本是一个可接受副本。而由承诺方案的隐藏性可知, $\boldsymbol{C}_2^*$此时的分布与真实交互中$\boldsymbol{C}_2$的分布计算不可区分。

2) $d=2$时, 模拟器 S 像真实交互一样选取$\pi^*,\pi_m^*,\ \boldsymbol{v}^*,\boldsymbol{s}'^*,\boldsymbol{s}^*$, 计算:

$$\boldsymbol{C}_1^*=Com(\boldsymbol{0}^n),\boldsymbol{t}_0^*=\boldsymbol{A}(\boldsymbol{v}^*||\boldsymbol{s}^*)+\boldsymbol{f}^*-\boldsymbol{y}+\boldsymbol{A}_2\boldsymbol{a},$$
$$\boldsymbol{t}_2^*=\pi^*(\boldsymbol{f}^*),\boldsymbol{t}_{m2}^*=\pi'^*(\boldsymbol{s}'^*).$$

然后按照真实协议计算$\boldsymbol{C}_0^*,\boldsymbol{C}_2^*$. 容易验证, 在验证阶段, 打开$\boldsymbol{C}_0^*,\boldsymbol{C}_2^*$时发送的各参数能够通过验证。$\boldsymbol{C}_0^*,\boldsymbol{C}_2^*,OPEN_2^*=\{\pi^*,\pi_m^*,\boldsymbol{t}_0^*,\boldsymbol{t}_2^*,\boldsymbol{t}_{m2}^*,R_0^*,R_2^*\}$此时的分布与真实交互中的分布完全一致。根据承诺方案的隐藏性, $\boldsymbol{C}_1^*$此时的分布与真实交互中$\boldsymbol{C}_1$的分布是计算不可区分的。

3) $d=3$时, S 选取$\boldsymbol{h}^*\xleftarrow{\$}\chi^k$, $\boldsymbol{t}_{m1}^*,\boldsymbol{t}_{m2}^*\xleftarrow{\$}\mathbb{Z}_u^{n-\lambda}$, $\boldsymbol{t}_1^*\xleftarrow{\$}\mathbb{Z}_q^k$, 令$\boldsymbol{t}_2^*=\boldsymbol{t}_1^*+\boldsymbol{h}^*$, $\boldsymbol{C}_0^*=Com(\boldsymbol{0}^n)$, $\boldsymbol{C}_1^*,\boldsymbol{C}_2^*$按照真实协议计算。整个交互产生的副本是一个可接受副本。可以看出此时$\boldsymbol{C}_1^*,\boldsymbol{C}_2^*,OPEN_3^*=\{\boldsymbol{t}_1^*,\boldsymbol{t}_2^*,\boldsymbol{t}_{m1}^*,\boldsymbol{t}_{m2}^*,R_0^*,R_2^*\}$的分布与真实交互中的分布是完全相同的。而由承诺方案的隐藏性可知, $\boldsymbol{C}_0^*$的分布与真实交互中$\boldsymbol{C}_0$的分布计算不可区分。

5.2.3 针对$\boldsymbol{b}-\boldsymbol{m}\in[\boldsymbol{0},\boldsymbol{u}^{\boldsymbol{n}-\boldsymbol{\lambda}})$的证明

证明$b-m\in[0,u^{n-\lambda})$的方式与 5.2.2 小节中证明 $m-a\in[0,u^{n-\lambda})$的方式类似, 只是协议中的个别算式在加减法的设置上略有不同。由 m 的承诺值 **y**, 可作如下变换:

$$\boldsymbol{A}_2\boldsymbol{b}-\boldsymbol{y}=\boldsymbol{A}_2\boldsymbol{b}-\boldsymbol{A}(\boldsymbol{r}||\boldsymbol{m})-\boldsymbol{e}=-\boldsymbol{A}_1\boldsymbol{r}+\boldsymbol{A}_2(\boldsymbol{b}-\boldsymbol{m})-\boldsymbol{e}.$$

即得到了对$b-m$的承诺。当$b-m\in[0,u^{n-\lambda})$时, 向量$\boldsymbol{b}-\boldsymbol{m}=0^\lambda||(\boldsymbol{b}'-\boldsymbol{m}')$. 本节将由这两式出发, 给出针对$b-m\in[0,u^{n-\lambda})$的范围证明, 该方案的描述如下:

$$\{(b\in\mathbb{Z},\boldsymbol{A}\xleftarrow{\$}\mathbb{Z}_q^{k\times(1+n)},\boldsymbol{y}\in\mathbb{Z}_q^k);(\boldsymbol{r}\in\mathbb{Z}_q^l,\boldsymbol{m}\in\mathbb{Z}_u^n,\boldsymbol{e}\in\mathbb{Z}_q^k):$$
$$\boldsymbol{y}=\boldsymbol{A}(\boldsymbol{r}\,\|\,\boldsymbol{m})+\boldsymbol{e}\ \bmod q\wedge\|\boldsymbol{e}\|_\infty\leqslant\beta\wedge$$
$$\boldsymbol{m}\in\mathbb{Z}_u^n,\boldsymbol{r}\in\mathbb{Z}_q^l\wedge VecToInt_u(\boldsymbol{b}-\boldsymbol{m})\in[0,u^{n-\lambda})\}.$$

协议 6

生成证明:

1. 证明者 $\mathcal{P}$ 随机选取三个随机向量$\boldsymbol{v}\xleftarrow{\$}\mathbb{Z}_q^l$, $\boldsymbol{f}\xleftarrow{\$}\mathbb{Z}_q^k$, $\boldsymbol{s}'\xleftarrow{\$}\mathbb{Z}_u^{n-\lambda}$, 两个置换: $\pi\xleftarrow{\$}S_q^k$, $\pi_m\xleftarrow{\$}S_u^{n-\lambda}$. 令$\boldsymbol{s}=0^\lambda||\boldsymbol{s}'$, $\mathcal{P}$ 计算:

$$\boldsymbol{t}_0=\boldsymbol{A}(\boldsymbol{v}||\boldsymbol{s})+\boldsymbol{f},$$
$$\boldsymbol{t}_1=\pi(\boldsymbol{f}),\boldsymbol{t}_2=\pi(\boldsymbol{f}-\boldsymbol{e}),$$
$$\boldsymbol{t}_{m1}=\pi_m(\boldsymbol{s}'+\boldsymbol{b}'),\boldsymbol{t}_{m2}=\pi_m(\boldsymbol{s}'+\boldsymbol{b}'-\boldsymbol{m}'),$$
$$\boldsymbol{C}_0=Com(\pi,\pi_m,\boldsymbol{t}_0,R_0),$$
$$\boldsymbol{C}_1=Com(\boldsymbol{t}_1,\boldsymbol{t}_{m1},R_1),$$
$$\boldsymbol{C}_2=Com(\boldsymbol{t}_2,\boldsymbol{t}_{m2},R_2),$$
$$\mathcal{P}\to\mathcal{V}::(\boldsymbol{C}_0,\boldsymbol{C}_1,\boldsymbol{C}_2).$$

2. $\mathcal{V}:\to\mathcal{P}:d\xleftarrow{\$}\{1,2,3\}$.

3. $\mathcal{P}$ 根据 $\mathcal{V}$ 的挑战值, 做出相应的回应:

1) $d=1$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0,\boldsymbol{C}_1$, 即$\mathcal{P}\to\mathcal{V}::OPEN_1=\{\pi,\ \pi_m,\boldsymbol{t}_0,\boldsymbol{t}_1,\boldsymbol{t}_{m1},R_0,R_1\}$.

2) $d=2$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_0,\boldsymbol{C}_2$, 即$\mathcal{P}\to\mathcal{V}::OPEN_2=\{\pi,\pi_m,\boldsymbol{t}_0,\boldsymbol{t}_2,\boldsymbol{t}_{m2},R_0,R_2\}$.

3) $d=3$ 时, $\mathcal{P}$ 打开 $\boldsymbol{C}_1,\boldsymbol{C}_2$, 即$\mathcal{P}\to\mathcal{V}::OPEN_3=\{\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_{m1},\boldsymbol{t}_{m2},R_1,R_2\}$.

验证:

将 **A** 划分为$\boldsymbol{A}_1||\boldsymbol{A}_2$, 其中$\boldsymbol{A}_1\in\mathbb{Z}_q^{k\times l}$, $\boldsymbol{A}_2\in\mathbb{Z}_q^{k\times n}$。$\mathcal{V}$ 接受证明当且仅当:

1) $d=1$时,

$$\boldsymbol{t}_0+\boldsymbol{A}_2\cdot(0^\lambda||\boldsymbol{b}')-\boldsymbol{A}_2\cdot(0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m1}))-\pi^{-1}(\boldsymbol{t}_1)\in img\boldsymbol{A}_1$$
$$\wedge\pi\in S_q^k\wedge\pi_m\in S_u^{n-\lambda}.$$

2) $d=2$时,

$$\boldsymbol{t}_0+\boldsymbol{A}_2\cdot\boldsymbol{b}-\boldsymbol{y}-\boldsymbol{A}_2\cdot(0^\lambda||\pi_m^{-1}(\boldsymbol{t}_{m1}))-\pi^{-1}(\boldsymbol{t}_2)\in img\boldsymbol{A}_1$$
$$\wedge\pi\in S_q^k\wedge\pi_m\in S_u^{n-\lambda}.$$

3) $d=3$时,

$$\boldsymbol{t}_{m1}-\boldsymbol{t}_{m2}\in\mathbb{Z}_u^{n-\lambda}\wedge\ ||\boldsymbol{t}_1-\boldsymbol{t}_2||_\infty\leqslant\beta.$$

定理 7: 如果协议 6 中的辅助承诺满足完美绑定性和计算隐藏性, 那么协议 6 是一个满足完美完备性和计算 SHVZK 的 Σ 协议, 其合理性错误率为 2/3。

定理 7 的证明思路与定理 6 的证明思路几乎相同, 只在一些加减法选择等细节上略有不同, 因而此处不再给出详细的证明过程。

6 效率分析

本节将从公共参数长度、证明长度、证明者的计算量、验证者的验证量等四个方面, 对协议 1、协议 3 和协议 4 进行分析, 其中, 方案产生的证明长度即为通信双方的通信量。4.2.2 节中批处理的范围证明方案(协议 2)的提出主要是为了呈现一种批处理范围证明的构造方式, 可以看作是协议 1 的拓展, 我们

不再对其各项参数进行具体分析。而 5.2.2 和 5.2.3 节中的两个协议与 5.2.1 节中的协议 4 在参数大小和尺寸设置上完全相同, 此处也一并略去。

本文中的方案都是公开抛币的 Σ 协议, 通过 Fiat-Shamir 启发式[27], 可以转化为RO模型下安全的非交互式零知识论证协议, 其中的挑战值可以通过对第一轮消息计算哈希值来确定。从形式上来看, 在协议 1、3、4 中, 都是第一轮先由证明者发送三个承诺值, 第二轮验证者选择一个挑战值, 第三轮证明者根据挑战值打开第一轮消息中的两个承诺值。这三个协议的主要区别有两点, 一是方案所针对的承诺方案不同, 因而参数大小和随机数的形式不同, 二是第一轮消息中, 被承诺对象不同。三个协议中的各项参数总结如表 3 所示。其中, 关于证明长度的具体说明如下:

基于 xLPN 的范围证明方案(协议 1)作用在$\mathbb{Z}_2$上。该方案生成的证明可以分为以下三个部分: 第一轮发送的三个承诺值$\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2$及其中两个对应的随机数$R_i, R_j$, 总比特长为$O(k)$; 挑战值 d, 长 2 比特; 第三轮中消息除去R_i, R_j之外的部分, d=1 或 2 时, 包括两个随机变换π, π_m和三个向量$\boldsymbol{t}_0, \boldsymbol{t}_d, \boldsymbol{t}_{md}$, 长度分别为$k^2 + (n-\lambda)^2$比特和$2k + n - \lambda$比特, d=3 时, 包括四个向量$\boldsymbol{t}_1, \boldsymbol{t}_2, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}$, 长$2k + 2(n - \lambda)$比特。

基于 SIS 问题的范围证明方案(协议 2)产生的证明可以划分为: 三个承诺值$\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2$及其中两个对应的随机数$R_i, R_j$, 共长$O(k \cdot \lceil \log q \rceil)$比特; 挑战值 d, 长 2 比特; 第三轮消息中除去R_i, R_j之外的部分, d=1 或 2 时, 包括两个随机变换π_r, π_m和三个向量$\boldsymbol{t}_0, \boldsymbol{t}_{rd}, \boldsymbol{t}_{md}$, 长度分别为$l^2 + (n-\lambda)^2$比特和$l + n - \lambda + k \cdot \lceil \log q \rceil$比特, d=3 时, 包括四个向量$\boldsymbol{t}_{r1}, \boldsymbol{t}_{r2}, \boldsymbol{t}_{m1}$, $\boldsymbol{t}_{m2}$, 长度为$2l + 2(n - \lambda)$比特。

基于 LWE 问题的范围证明方案(协议 3)几乎与协议 1 是一样的, 只在参数的大小和运算的类型上略有不同。其证明也可以划分为三个部分: 三个承诺值$\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2$及其中两个对应的随机数$R_i, R_j$, 共长$O(k \cdot \lceil \log q \rceil)$比特; 2 比特长的挑战值 d; 第三轮消息中除R_i, R_j之外的部分, d=1 或 2 时, 包括两个随机变换π, π_m和三个向量$\boldsymbol{t}_0, \boldsymbol{t}_d, \boldsymbol{t}_{md}$, 长度分别为$k^2 + (n - \lambda)^2$比特和$2k \cdot \lceil \log q \rceil + (n - \lambda) \cdot \lceil \log u \rceil$比特, d=3 时, 包括四个向量$\boldsymbol{t}_1, \boldsymbol{t}_2, \boldsymbol{t}_{m1}, \boldsymbol{t}_{m2}$, 总的长度为$2k \cdot \lceil \log q \rceil + 2(n - \lambda) \cdot \lceil \log u \rceil$比特。

表 3　本文各方案的效率总结

Table 3　The summary of the efficiency of the schemes on this paper.

变量 协议	挑战值	公共参数(比特)	证明长度(比特)	证明者的计算量	验证者的验证量
协议 1	1 或 2	$\boldsymbol{A}$: $k \cdot (l+n)$ $\boldsymbol{y}$: k	$O(k) + k^2 + (n-\lambda)^2 + 2k + n - \lambda + 2$	4 个承诺 4 个变换	1 个算式, 2 个变换
	3		$O(k) + 2k + 2(n - \lambda) + 2$		2 个算式
协议 3	1 或 2	$\boldsymbol{A}$: $k \cdot (l+n) \cdot \lceil \log q \rceil$ $\boldsymbol{y}$: $k \cdot \lceil \log q \rceil$	$O(k \cdot \lceil \log q \rceil) + l^2 + (n-\lambda)^2 + k \cdot \lceil \log q \rceil + l + n - \lambda + 2$	4 个承诺 4 个变换	1 个算式, 2 个变换
	3		$O(k \cdot \lceil \log q \rceil) + 2l + 2n - 2\lambda + 2$		2 个算式
协议 4	1 或 2	$\boldsymbol{A}$: $k \cdot (l+n) \cdot \lceil \log q \rceil$ $\boldsymbol{y}$: $k \cdot \lceil \log q \rceil$	$O(k \cdot \lceil \log q \rceil) + k^2 + (n-\lambda)^2 + 2k \cdot \lceil \log q \rceil + (n - \lambda) \cdot \lceil \log u \rceil + 2$	4 个承诺 4 个变换	1 个算式, 2 个变换
	3		$O(k \cdot \lceil \log q \rceil) + 2k \cdot \lceil \log q \rceil + 2(n - \lambda) \cdot \lceil \log u \rceil + 2$		2 个算式

7　总结

目前已有的高效的、且能够抵抗量子攻击的范围证明方案屈指可数。针对这种情况, 本文提出了三个高效的、针对后量子承诺构造的范围证明方案, 并给出了从一般范围证明方案到批处理范围证明方案的转化方法, 使得人们在应对量子攻击时, 有更多的范围证明方案可以选择。本文中构造范围证明方案的主要思想是: 通过引入随机变换, 证明一个给定的秘密n维向量是前λ位都为 0 的u进制向量, 其中$\lambda < n$。事实上, 现有的后量子的范围证明方案, 包括本文中的方案, 还有一些格上的零知识证明方案, 几乎都采用了 Stern 在 1993 年提出的身份认证方案[28]的框架。这一类的方案存在一个共同的问题, 即有比较大的合理性错误率(2/3), 需要通过多项式次并行执行的操作来保证证明的准确率。如果能够解决这一问题, 那么这一类的方案的安全性和效率将会得到很大的提升。我们将在未来的工作中对此问题继续探究。

参考文献

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

[2] A. Chan, Y. Tsiounis, Y. Frankel. Easy Come-easy Go Divisible Cash. Advances in Cryptology (EUROCRYPT'98)[C], I*nternational Conference on the Theory and Application of Cryptographic Techniques*, 1998: 561-575.

[3] Fujisaki E, Okamoto T. A Practical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and Its Applications[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998: 32-46.

[4] Boudot F. Efficient Proofs that a Committed Number Lies in an Interval[J]. *Advances in Cryptology*, 2000: 431-444. DOI:10.1007/3-540-45539-6_31.

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

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

[7] A. Scemama. A cryptanalysis of the 2R Cryptosystem and an Improved Commitment Range proof[D]. Goethe University Frankfurt, Frankfurt am Main, Germany, 2009.

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

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

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

[11] Moran T, Naor M. Split-ballot Voting: Everlasting Privacy with Distributed Trust[C]. *the 14th ACM conference on Computer and communications security*, 2007: 246-255.

[12] S. Canard, I. Coisel, A. Jambert,et al. New Results for the Practical Use of Range Proofs[C]. *EuroPKI*, 2014:47-64.

[13] Camenisch J, Chaabouni R, Shelat A. Efficient Protocols for Set Membership and Range Proofs[J]. *Advances in Cryptology - ASIACRYPT 2008*, 2008: 234-252. DOI:10.1007/978-3-540-89255-7_15.

[14] Chaabouni R, Lipmaa H, Shelat A. Additive Combinatorics and Discrete Logarithm Based Range Protocols[M]. Information Security and Privacy. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 336-351.

[15] B. Bnz, J. Bootle, D. Boneh, et al. Bulletproofs: Short Proofs for Confidential Transactions and More[C]. *Symposium on Security and Privacy (SP'18)*, 2018: 315-334.

[16] Baum C, Bootle J, Cerulli A, et al. Sub-linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018: 669-699.

[17] X. Xie, R. Xue, M. Wang. Zero Knowledge Proofs from Ring-LWE[C]. *International Conference on Cryptology & Network Security*,2013: 57-73.

[18] 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.

[19] Libert B, Ling S, Nguyen K, et al. Lattice-Based Zero-Knowledge Arguments for Integer Relations[J]. *Advances in Cryptology - CRYPTO 2018*, 2018: 700-732. DOI:10.1007/978-3-319-96881-0_24.

[20] Jain A, Krenn S, Pietrzak K, et al. Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise[M]. Advances in Cryptology – ASIACRYPT 2012. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 663-680.

[21] 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.

[22] Li K, Yang R P, Au M H, et al. Practical Range Proof for Cryptocurrency Monero with Provable Security[M]. Information and Communications Security. Cham: Springer International Publishing, 2018: 255-262.

[23] I. Damgård. On Sigma-protocols[L]., University of Aarhus, Department for Computer Science, 2002.

[24] O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[C]. *ACM Symposium on Theory of computing*, 2005: 84-93.

[25] M. Ajtai. Generating Hard Instances of Lattice Problems (Extended Abstract)[C]. *Acm Symposium on the Theory of Computing (STOC'96)*, 1996: 99-108.

[26] D. Micciancio, C. Peikert. Hardness of SIS and LWE with Small Parameters[C]. *Advances in Cryptology (CRYPTO'13)*, 2013: 21-39.

[27] A. Fiat, A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[C]. *Advances in Cryptology (CRYPTO'86)*, 1987: 186-194.

[28] J. Stern. A New Identification Scheme Based on Syndrome Decoding[C]. *Advances in Cryptology (CRYPTO'93)*, 1994: 13-21.

[29] Oded Goldreich. T The Foundations of Cryptography[M], Basic Techniques. Cambridge University Press, 2001.

滕瑜莹 于 2016 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国家重点实验室攻读硕士学位。研究领域为安全协议和零知识证明。研究兴趣包括: 范围证明在区块链中的应用。Email: tengyuying@iie. ac.cn

邓燚 于 2008 年在中科院软件所获得博士学位。现任中科院信息工程研究所信息安全国家重点实验室研究员。研究领域为密码学与安全协议。研究兴趣包括: 零知识证明、安全规约方法、密码协议的轮/通信/计算复杂度以及这些技术在密码货币和区块链中的应用。Email: deng@iie.ac.cn

谢翔 于 2015 年在中科院软件所获得博士学位。现供职于矩阵元技术有限公司。研究兴趣包括: 公钥密码学、格密码、区块链安全和多方安全计算。Email: xiexiang@juzix.io