

Article

Amortized Σ -Protocol for MLWE Problem

Qi Li ¹ and Shaojun Yang ^{1,2,*}

¹ School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350108, China; liqimoxie@outlook.com

² Key Laboratory of Analytical Mathematics and Applications (Ministry of Education), Fujian Normal University, Fuzhou 350007, China

* Correspondence: shaojunyang@fjnu.edu.cn

Abstract

MLWE is a fundamental hard problem in post-quantum lattice cryptography. Standard Σ -protocols perform poorly for multiple MLWE statements due to high communication and computation costs. This paper presents an amortized Σ -protocol for MLWE using a lightweight fold-split-fold technique that decomposes norm-bounded error vectors without relying on NTT, MLE, or sum-check protocols. The protocol achieves completeness, special soundness, and non-abort SHVZK with constant-round interaction and lightweight verification. The construction avoids complex tools and provides an efficient batch proof mechanism, offering a simple and practical solution for post-quantum cryptographic applications.

Keywords: Σ -protocol; zero-knowledge proofs; MLWE; amortization

1. Introduction

Zero-knowledge proofs (ZKPs) [1] allow a prover to convince a verifier of the validity of a statement without revealing any secret information. As a classic three-round public-coin zero-knowledge framework, Σ -protocols [2] are widely adopted for their high efficiency, easy composition, and straightforward security proofs.

In scenarios such as authenticated key agreement protocols [3–5], secret sharing [6,7], post-quantum signatures [8–12], and cryptographic building blocks [13,14], we often need multiple Σ -protocols. In these cases, the number of instances to be proven by traditional Σ -protocols increases linearly, resulting in low efficiency. Against this background, Cramer and Damgård proposed amortized Σ -protocols [15]. Since their introduction, amortized Σ -protocols have been widely applied in anonymous transactions [16], identity management systems [17], and encryption [18]. These protocols greatly reduce communication and verification costs, supporting practical large-scale privacy-preserving systems [19,20].

Lattice-based cryptography has emerged as a leading candidate for post-quantum security due to its strong worst-case hardness and algebraic simplicity. However, early constructions based on standard LWE or Ring LWE suffer from either large key sizes (LWE) or restricted algebraic structures (Ring-LWE). To balance security, efficiency, and flexibility, the Module Learning with Errors (MLWE) problem [21,22] was introduced. MLWE works over module lattices, which offer a middle ground between the high dimensionality of LWE and the strong constraints of Ring-LWE. As a result, MLWE is now a core hardness assumption for lattice cryptography. Many practical zero-knowledge proofs rely on it. It is also used in other primitives, like encryption [23].

This paper considers the Σ -protocol for MLWE, as detailed below. Section 2 presents the definitions of Σ -protocols, MLWE, and relevant notations. Section 3 details the construc-



Academic Editor: Josef Pieprzyk

Received: 25 June 2026

Revised: 24 July 2026

Accepted: 29 July 2026

Published: 2 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

tion and security proofs of the proposed amortized MLWE Σ -protocol. Section 4 analyzes parameter selection and performance. Finally, Section 5 concludes the whole study.

1.1. Related Work

In 1991, Schnorr [24] proposed the first three-round interactive proof based on the discrete logarithm problem, pioneering the Σ -protocol. Cramer [2] further formalized the definition of Σ -protocols in 1997, defining them as three-round protocols with completeness, special soundness, and the SHVZK property. In recent studies, Albrecht and Lai [25] achieved tight standard soundness but incurred high soundness error, while the protocol in [26] proves small-norm witnesses and realizes security via soundness slack.

Lyubashevsky [27] proposed the first LWE-based Σ -protocol in 2009, establishing the fundamental framework for lattice-based zero-knowledge proofs. In 2012, Lyubashevsky [28] constructed a lightweight three-round LWE Σ -protocol using Fiat–Shamir transformation and rejection sampling. This trapdoor-free scheme simplifies protocol design and supports practical signature implementations. Recently, Nguyen [29] presented the first straight-line extractable zero-knowledge proof system from MLWE in 2025, which reduces nearly half of the proof size and greatly improves both proving and verifying efficiency.

To improve the scalability of multi-instance proofs, amortized zero-knowledge proofs for lattice problems have attracted intensive research attention. Amortized zero-knowledge proofs enhance the scalability of multi-instance lattice proofs and have been widely studied. Liu et al. [30] proposed a lattice inner product argument in 2019, cutting the proof size of LWE-based Σ -protocols from $O(n)$ to $O(\sqrt{n})$. In 2021, Bootle et al. [31] constructed an amortized proof system for LWE. For instances sharing the same secret $\vec{s}$, its proof size is independent of instance quantity and is linear in secret length. When all instances share matrix A , the size is further reduced to $O(\sqrt{n})$, yielding efficient batch proofs.

Recently, Boneh and Chen proposed LatticeFold [32]. It is a folding-based framework that constructs succinct lattice proof systems. It uses polynomial commitments and sum-check protocols. These tools compress multiple lattice instances. In a closely related direction, Zhang et al. [14] designed Σ -protocols for polynomial relations over lattices, focusing on the MSIS problem. To handle these complex polynomial constraints, their work integrates key techniques including the number theoretic transform (NTT) and multilinear extensions (MLEs).

1.2. Our Contribution

The amortization methods in Zhang et al.'s work target MSIS, which has a single bounded witness. MLWE differs: its witness splits into unbounded $\vec{s}$ and bounded $\vec{e}$. We adapt their folding technique to this setting and construct an amortized Σ -protocol tailored to MLWE.

Our protocol achieves proof size $O((\ell + 3)m)$ (in $\mathcal{R}_q$ -elements). Since $\ell \ll k$, this is significantly better than the direct approach $O(km)$. Zhang et al. achieve better asymptotic efficiency using more advanced tools but with higher implementation overhead and deployment complexity.

Our protocol adopts a different design philosophy, involving low deployment barriers, simple implementation, and practically sufficient efficiency. It operates via the fold-split-fold method together with rejection sampling, resulting in a structure well-suited for scenarios where implementation cost and deployability are key. To our knowledge, this is the first amortized Σ -protocol for MLWE that achieves completeness, special soundness, and non-abort SHVZK simultaneously.

2. Preliminaries

For simplicity, we define the arrow " $\leftarrow$ " to denote random sampling from a distribution. Let $\mathcal{R} = \mathbb{Z}[X]/(X^d + 1)$ be a cyclotomic polynomial ring, where $d > 1$ is a power of

two. Let q be a modulus satisfying $q \equiv 1 \pmod{2d}$. Let $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ be the ring of integers modulo q , i.e., $\{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$. We use $\mathbb{Z}_q[X]$ to denote the set of polynomials over $\mathbb{Z}_q$. Let $\mathcal{R}_q = \mathcal{R}/q\mathcal{R} = \mathbb{Z}_q[X]/(X^d + 1)$ denote its quotient ring modulo q .

2.1. Interactive Sigma Protocol

We review some concepts about zero-knowledge proofs and Σ -protocol as follows:

Definition 1 ([33] (Σ -protocol)). *A three-move protocol that is public-coin, complete, k -special sound, and SHVZK is said to be Σ -protocol.*

In this paper, we will more generally refer to Σ -protocols also for k -move protocols that are public-coin, complete (with some completeness error), $(k_1, \dots, k_n)$ -special sound, and (non-abort) SHVZK.

Definition 2 ([33] (Completeness)). *If P and V follow the protocol on input x and private input ω to P where $(x, \omega) \in R$, then V always accepts.*

Definition 3 ([34] (Special Soundness)). *There exists a polynomial-time algorithm A that given any x and any pair of accepting transcripts $(a, e, z), (a, e', z')$ for x , where $e \neq e'$, outputs w such that $(x, w) \in R$. A Σ -protocol is called k -special sound if there exists an efficient algorithm that, upon inputting any statement x and k accepting transcripts $(a, c_1, z_1), \dots, (a, c_k, z_k)$ with a common first message a and pairwise distinct challenges c_i , outputs a witness ω for x .*

A Σ -protocol is said to achieve an honest-verifier zero-knowledge (HVZK) [26] if there exists an efficient algorithm, referred to as a simulator, that takes a valid statement y (along with a corresponding witness x) and outputs an accepting transcript whose distribution is identical to that of transcripts generated by an interaction between an honest prover and an honest verifier. In many practical Σ protocols, the simulator operates by first choosing a random challenge c and then constructing the first message a and response z accordingly; this strengthened flavor is commonly known as special honest-verifier zero-knowledge (SHVZK). Furthermore, a protocol is called non-abort honest-verifier zero-knowledge if the transcript distribution produced by the simulator is statistically indistinguishable from the one produced in an honest protocol execution, provided that the honest prover never aborts during the process.

Definition 4 ([14]). We define a mapping as "extractive injective" if and only if during the extraction process, the extracted system comprising rewinding factors, private inputs, and public outputs is "perfectly injective". In other words, each output can only extract exactly one input set.

Definition 5 ([35]). Define a subset $\mathcal{C}$ of $\mathcal{R}_q$ as a challenge space if the difference of any two distinct elements in $\mathcal{C}$ is not a zero divisor. $\mathcal{C}$ is further a strong challenge space if the difference of any two distinct elements in it is invertible in $\mathcal{R}_q$.

Sometimes we need a strong challenge space $\mathcal{C} \subset \mathcal{R}_q$ whose elements have small norms. We use two quantities: the expansion factor $\bar{\omega}_{\mathcal{R}_q}(\mathcal{C})$ of $\mathcal{C}$ and the soundness slack $\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)$, with slack factor ζ introduced by extraction for vectors in [26].

$$\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}) = \max_{c \in \mathcal{C}, x \in \mathcal{R}_q^m \setminus \{0\}} \frac{\|cx\|}{\|x\|}; \quad \bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta) = \max_{c \neq c', x \in \mathcal{R}_q^m \setminus \{0\}} \max_{a \in \mathcal{R}_q: a(c-c')=\zeta} \frac{\|ax\|}{\|x\|}.$$

Theorem 1 ([36]). *Sequential composition: Let R_1 , R_2 , and R_3 be three relations. Given two reduction of knowledge protocols, Π_1 from R to R_2 and Π_2 from R_2 to R_3 , the composed protocol $\Pi_1 \diamond \Pi_2$ is a reduction of knowledge from R_1 to R_3 .*

2.2. Hard Problems on Lattice

The security of lattice-based Σ -protocols relies on the hardness of certain computational problems. We now define the Module Learning with Errors (MLWE) problem and its relevant properties.

Definition 6 ([37] (MLWE Problem)). Let $m, n, q \geq 1$ be any positive integers. Let χ_B be the probability distribution over $\mathcal{R}_q$ bounded by B . For $A \leftarrow \mathcal{U}(\mathcal{R}_q^{n \times m})$ and $\vec{s} \in \mathcal{R}_q^n$, $\vec{e} \leftarrow \chi_B^m$ defines the distribution consisting of $(A, \vec{t} = A\vec{s} + \vec{e})$ as $\mathcal{A}_{\vec{s}, \chi_B}^m$. The search MLWE $_{n,m,q,B}$ problem is defined as: given a sample $(A, \vec{t} = A\vec{s} + \vec{e}) \in \mathcal{R}_q^{m \times n} \times \mathcal{R}_q^m$, solve for $\vec{s} \in \mathcal{R}_q^n$. The decision MLWE $_{n,m,q,B}$ problem is defined as follows: determine whether multiple samples $(A, \vec{t} = A\vec{s} + \vec{e})$ are drawn from the distribution $\mathcal{A}_{\vec{s}, \chi_B}^m$ or from the distribution $\mathcal{U}(\mathcal{R}_q^{m \times n} \times \mathcal{R}_q^m)$.

Theorem 2 ([22] (Classical Hardness of MLWE)). Let $n, d, q \geq 2 \in \mathbb{N}$, defining $N = dn$. Let $\epsilon(N) = N^{-\omega(1)}$, $\alpha \in (0, 1)$ of known factorization such that $\alpha q > 2\sqrt{d} \cdot \omega(\sqrt{\log n})$. There is a quantum reduction from solving Mod-GIVP $_{\tilde{\gamma}}^{\eta_\epsilon}$ in polynomial time (in the worst case, with high probability) to solving MLWE $_{q, \Psi_{\leq \alpha}}$ in polynomial time with a non-negligible advantage, where

$$\tilde{\gamma} = \frac{\sqrt{8Nd} \cdot \omega(\sqrt{\log n})}{\alpha}.$$

3. Σ -Protocol of LWE Problem

In this section, we focus on the construction of amortized Σ -protocols for lattice MLWE problems and specifically design an MLWE $_{n,m,q,B}^\infty$ protocol following the classical amortized proof framework. The target proof relation of our amortized Σ -protocol is defined as follows:

$$R = \{(A \in \mathcal{R}_q^{m \times n}, \vec{t}_0, \dots, \vec{t}_{k-1} \in \mathcal{R}_q^m, \vec{s}_0, \dots, \vec{s}_{k-1} \in \mathcal{R}_q^n, \vec{e}_0, \dots, \vec{e}_{k-1} \in \mathcal{R}_q^m) : A\vec{s}_i + \vec{e}_i = \vec{t}_i, \|\vec{e}_i\|_\infty \leq B\}.$$

Our protocol integrates witness folding and rejection sampling. Folding compresses multiple MLWE witnesses to reduce proof size and communication cost via amortization. Rejection sampling controls the ℓ_∞ -norm of folded error vectors to avoid overflow and meet required constraints. We next present the folding process of MLWE $_{n,m,q,B}^\infty$, the amortized Σ -protocol construction, and formal proofs for completeness, special soundness, and zero-knowledge.

Based on the above MLWE $_{n,m,q,B}^\infty$ witness relation, we adopt witness splitting and folding operations to aggregate k independent MLWE instances into a single compact witness. The detailed folding protocol Π_0 is presented below.

Protocol Π_0

$\mathcal{P}(A, (\vec{t}_j)_{j=0}^{k-1}, B; (\vec{s}_j)_{j=0}^{k-1}, (\vec{e}_j)_{j=0}^{k-1}), \mathcal{V}(A, (\vec{t}_j)_{j=0}^{k-1}, B)$

1: $\mathcal{V} \rightarrow \mathcal{P}: \vec{\rho}_1 \leftarrow \mathcal{C}^k, \vec{\rho}_2 \leftarrow \mathcal{C}^\ell$.

2: $\mathcal{P}$: Compute $\vec{e} = \sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j, \vec{s} = \sum_{j=0}^{k-1} \rho_{1,j} \vec{s}_j$.

3: $\mathcal{V}$: Compute: $\sum_{i=0}^{\ell-1} \omega^i \vec{t}_i$

4: $\mathcal{P}$: Set $(\vec{e}_0, \dots, \vec{e}_{\ell-1}) := \text{split}(\vec{e}), (\vec{s}_0, \dots, \vec{s}_{\ell-1}) := \text{split}(\vec{s})$.

5: $\mathcal{P} \rightarrow \mathcal{V}$: $(\vec{f}_i)$ such that: $\vec{f}_i = A\vec{s}_i + \vec{e}_i \pmod{q}$.

6: $\mathcal{V}$: Check $\sum_{i=0}^{\ell-1} \omega^i \vec{f}_i \stackrel{?}{=} \sum_{j=0}^{k-1} \rho_{1,j} \vec{t}_j$.

7: $\mathcal{P}$: Compute $\vec{e}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{e}_i, \vec{s}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{s}_i$.

8: $\mathcal{P}$: Output $\vec{e}_*$ and $\vec{s}_*$

9: $\mathcal{V}$: Output $\vec{f}_*$ such that: $\vec{f}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{f}_i$.

Theorem 3. Let $pp := (k, n, m, \mathcal{B}, A, \gamma < q/2)$ be the public parameters such that $\mathcal{C} \subset \mathcal{R}_q$ are superpoly large strong sampling sets where $\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}) = c$. Let $k\mathcal{B} = \bar{\mathcal{B}}$, choose c, ω, ℓ such that $\omega^\ell = \bar{\mathcal{B}}, c\ell\omega = b$ and $b < \gamma$. Π_1 satisfies completeness and the extractive injective.

Proof. Completeness: From the parameter settings, we can directly obtain $\sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j = \sum_{i=0}^{\ell-1} \omega^i \vec{e}_i$ and $\sum_{j=0}^{k-1} \rho_{1,j} \vec{s}_j = \sum_{i=0}^{\ell-1} \omega^i \vec{s}_i$. The prover computes $\vec{e} = \sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j$, $\vec{s} = \sum_{j=0}^{k-1} \rho_{1,j} \vec{s}_j$. $\|\vec{e}\|_\infty \leq k\mathcal{B} = \bar{\mathcal{B}}$ then splits $\vec{e}$ and $\vec{s}$ into $(\vec{e}_0, \dots, \vec{e}_{\ell-1})$ and $(\vec{s}_0, \dots, \vec{s}_{\ell-1})$ and $\|\vec{e}_j\|_\infty \leq \omega$. Then, the prover sends $\vec{f}_i = A\vec{s}_i + \vec{e}_i \pmod q$ for each $i \in [\ell]$. The verifier verifies that $\sum_{i=0}^{\ell-1} \omega^i \vec{f}_i \stackrel{?}{=} \sum_{j=0}^{k-1} \rho_{1,j} \vec{t}_j$. If the check is passed, the prover computes and outputs $\vec{e}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{e}_i$ and $\vec{s}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{s}_i$. Moreover, $\|\vec{e}_*\|_\infty \leq c\ell\omega = b$. The verifier outputs $\vec{f}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{f}_i$.

Extractive injective: For any output $\vec{e}_*$ with a small norm bound, the analysis in [14] ensures that there exists a unique sequence $(\vec{e}_i)_{i=0}^{\ell-1}$ that maps to $\vec{e}_*$. As a result, summing $\sum_{i=0}^{\ell-1} \omega^i \vec{e}_i$ yields exactly one vector $\vec{e}$. Likewise, for this fixed $\vec{e}$, there exists a unique input solution sequence $(\vec{e}_j)_{j=0}^{k-1}$ that produces it. Similarly, for any output $\vec{s}_*$, there exists a unique sequence $(\vec{s}_i)_{i=0}^{\ell-1}$ that maps to $\vec{s}_*$. As a result, summing $\sum_{i=0}^{\ell-1} \omega^i \vec{s}_i$ yields exactly one vector $\vec{s}$. For a given output $\vec{s}$ that does not require a small norm bound, there exists a unique input solution sequence $(\vec{s}_j)_{j=0}^{k-1}$ that produces it. Therefore, Π_1 is extractive injective. $\square$

For positive integers $\bar{\mathcal{B}} = k\mathcal{B}$ and $b < \gamma$, choose ω, ℓ such that $\omega^\ell = \bar{\mathcal{B}}$ and $c\ell\omega = b$ (c is the norm bound of challenges). Initially, the verifier chooses a random challenge $\vec{\rho}_1 \in \mathcal{C}^k$ from a compact strong challenge space. Subsequently, the prover calculates the associated random linear combination $\vec{e} = \sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j$. For an m -size vector $\vec{e} \in \mathcal{R}_q^m$ where $\|\vec{e}\|_\infty \leq \bar{\mathcal{B}}$, we can split it into an $m \times \ell$ matrix $\mathbf{split}(\vec{e}) := (\vec{e}_0, \dots, \vec{e}_{\ell-1})$, such that $\|\vec{e}_i\|_\infty \leq \omega$ for all $i \in [\ell]$ and $\vec{e} := \sum_{i=0}^{\ell-1} \omega^i \vec{e}_i$. Furthermore, we can fold them into one $\vec{e}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{e}_i$ such that $\|\vec{e}_*\|_\infty \leq b$ by applying the same folding operation with the challenge $\vec{\rho}_2 \in \mathcal{C}^\ell$. With an analogy, we can split it into an $m \times \ell$ matrix $\mathbf{split}(\vec{s}) := (\vec{s}_0, \dots, \vec{s}_{\ell-1})$, such that $\vec{s} := \sum_{i=0}^{\ell-1} \omega^i \vec{s}_i$. The difference is that we cannot guarantee that the norm of vector $\vec{s}_i$ is bounded by some value for all $i \in [\ell]$.

Therefore, our protocol does not require bounding the norm of $\vec{s}_i$. We let $\vec{f}_i = A\vec{s}_i + \vec{e}_i \pmod q$ for $i \in [\ell]$. Compute $\vec{s}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{s}_i$, where the random challenge $\vec{\rho}_2 \in \mathcal{C}^\ell$. Then we can obtain that

$$A\vec{s}_* + \vec{e}_* = \sum_{i=0}^{\ell-1} \rho_{2,i} (A\vec{s}_i + \vec{e}_i) = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{f}_i, \|\vec{e}_*\|_\infty \leq b.$$

Next, we construct and prove the security of the protocol for the making operation with respect to the $\text{MLWE}_{n,m,q,b}^\infty$ problem. The construction and proof of this protocol involve the following two relations:

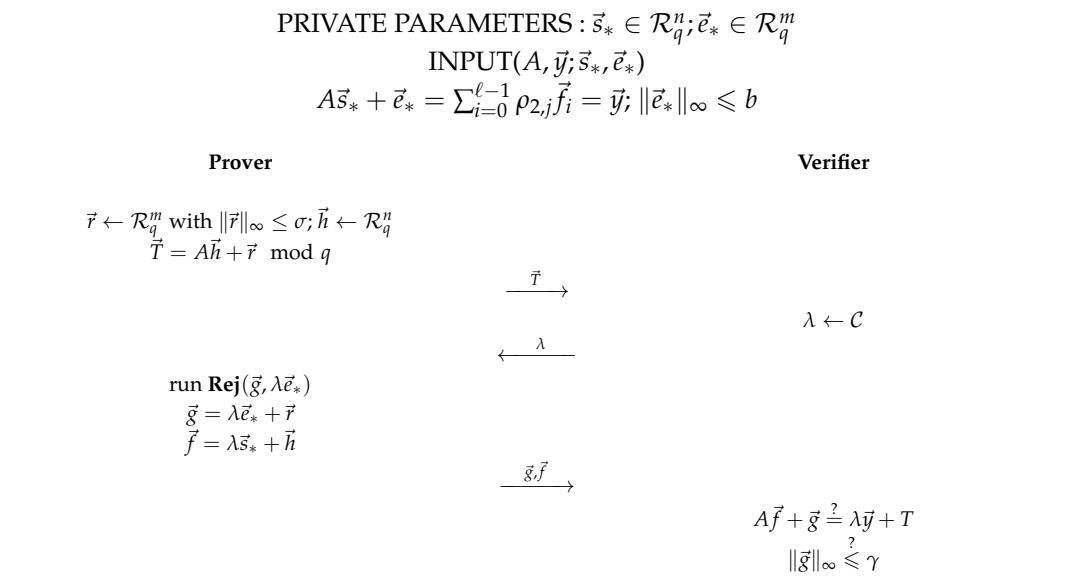
$$R(A, b) = \{(\vec{y}; \vec{s}_*, \vec{e}_*) : \vec{s}_* \in \mathcal{R}_q^n, \vec{e}_* \in \mathcal{R}_q^m, A\vec{s}_* + \vec{e}_* = \vec{y} \pmod q, \|\vec{e}_*\|_\infty \leq b\};$$

$$R(A, 2\gamma\bar{\omega}_{\mathbb{Z}_q}(\mathcal{C}, \zeta), \zeta) = \{(\vec{y}; \vec{s}_*, \vec{e}_*) : \vec{s}_* \in \mathcal{R}_q^n, \vec{e}_* \in \mathcal{R}_q^m, A\vec{s}_* + \vec{e}_* = \zeta\vec{y} \pmod q, \|\vec{e}_*\|_\infty \leq 2\gamma\bar{\omega}_{\mathbb{Z}_q}(\mathcal{C}, \zeta)\}.$$

where $R(A, b)$ corresponds to the $\text{MLWE}_{n,m,q,b}^\infty$ protocol to be proven and $R(A, 2\gamma\bar{\omega}_{\mathbb{Z}_q}(\mathcal{C}, \zeta), \zeta)$ is the relation to be verified for the protocol's special soundness.

To guarantee zero-knowledge and error vector bounds, we adopt rejection sampling. Existing studies use the algorithm **Rej** [28] to filter out-of-bound outputs, while we directly utilize rejection sampling results in our protocol.

Theorem 4. Let $\mathcal{B} = k\bar{\mathcal{B}}$ and $b < \gamma$. Choose ω, ℓ such that $\omega^\ell = \bar{\mathcal{B}}$. Π_1 is a three-move Σ -protocol for relation $R(A, b)$. The protocol Π_1 is complete, non-abort SHVZK, and special soundness.

Protocol Π_1 

Proof. Completeness: The honest prover computes: $\vec{g} = \lambda \vec{e}_* + \vec{r}$, $\vec{f} = \lambda \vec{s}_* + \vec{h}$. Then $A\vec{f} + \vec{g} = A(\lambda \vec{s}_* + \vec{h}) + (\lambda \vec{e}_* + \vec{r}) = \lambda(A\vec{s}_* + \vec{e}_*) + (A\vec{h} + \vec{r})$. By definitions $\vec{T} = A\vec{h} + \vec{r}$ and $A\vec{s}_* + \vec{e}_* = \vec{y}$, we obtain $A\vec{f} + \vec{g} = \lambda \vec{y} + \vec{T}$. Thus the first verification equation $A\vec{f} + \vec{g} \stackrel{?}{=} \lambda \vec{y} + \vec{T}$ holds with equality. Since $\|\vec{r}\|_\infty \leq \sigma$, $\|\lambda\|_\infty \leq c$, the norm of $\vec{g}$ is less than γ . Moreover, the rejection sampling condition **Rej**($\vec{g}, \lambda \vec{e}_*$) is satisfied for the honest prover. Therefore the second check $\|\vec{g}\|_\infty \stackrel{?}{\leq} \gamma$ is satisfied. The protocol is complete.

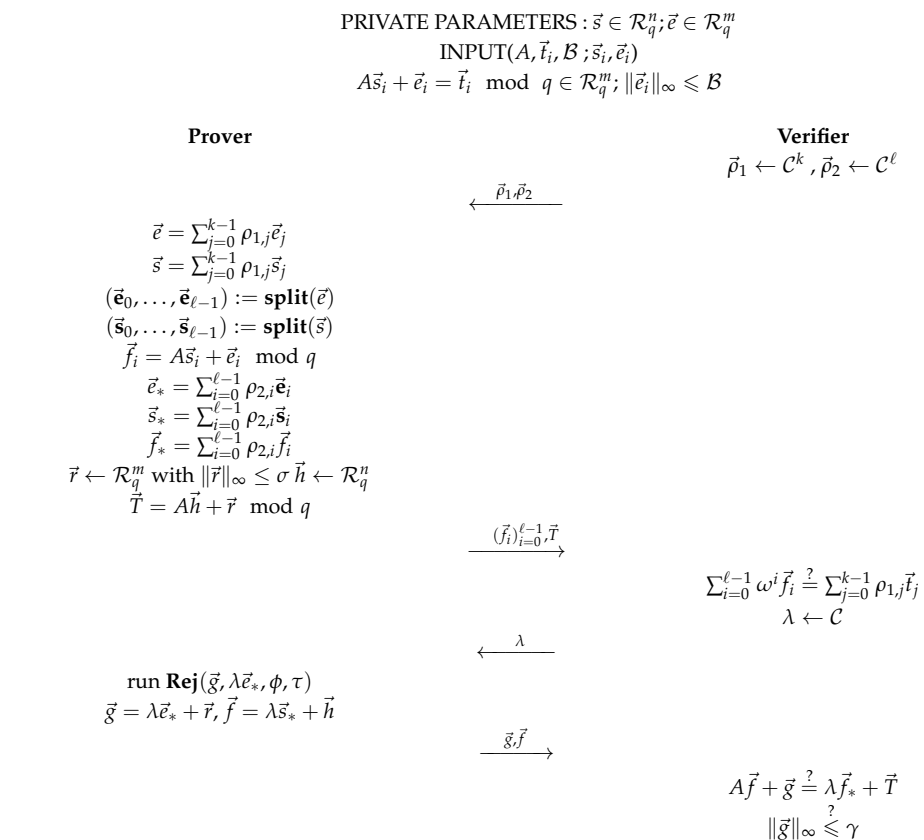
Special Soundness: Specifically, the extractor first requires two accepting transcripts of the same $\vec{T}$ but with different λ values to recover the amortized witness. Let $a(\lambda^{(1)} - \lambda^{(2)}) = \zeta$. Let $(\vec{T}, \lambda^{(1)}, \vec{g}^{(1)}, \vec{f}^{(1)})$ and $(\vec{T}, \lambda^{(2)}, \vec{g}^{(2)}, \vec{f}^{(2)})$ be two accepting transcripts for $\lambda^{(1)} \neq \lambda^{(2)} \in \mathcal{C}$. Define $\vec{e}'_* = a(\vec{g}^{(1)} - \vec{g}^{(2)})$ and $\vec{s}'_* = a(\vec{f}^{(1)} - \vec{f}^{(2)})$. $\|\vec{e}'_*\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\gamma$ and $A\vec{s}'_* + \vec{e}'_* = Aa(\vec{f}^{(1)} - \vec{f}^{(2)}) + a(\vec{g}^{(1)} - \vec{g}^{(2)}) = a(\lambda^{(1)} - \lambda^{(2)})\vec{y} = \zeta\vec{y}$ also apply.

Non-abort SHVZK: We simulate a transcript as follows: Sampling $\lambda_0 \leftarrow \mathcal{C}$, the simulator runs on input public parameters and challenge λ_0 . If **Rej**($\vec{g}, \lambda \vec{e}_*$) outputs $\perp$, the simulator returns $(\perp; \lambda_0; \perp, \perp)$. Otherwise, the simulator set $\vec{g}_0, \vec{f}_0$ computes the first message as $\vec{T} = A\vec{g}_0 + \vec{f}_0 - c\vec{y}$ and outputs $(\vec{T}, \lambda_0, \vec{g}_0, \vec{f}_0)$. Since the output distribution of the simulator and transcripts are statistically distinctive and $\vec{T}$ is determined by the values $\lambda_0, \vec{f}_0, \vec{g}_0$, and $\vec{y}$, statistical non-abort SHVZK follows. $\square$

To ensure the zero-knowledge property of this amortized MLWE Σ -protocol, we sequentially compose protocol Π_0 and the masking operation protocol Π_1 together. Protocol Π_0 reduces relation R to relation $R(A, b)$. Protocol Π_1 reduces relation $R(A, b)$ to relation $R(A, \gamma)$ where

$$R(A, \gamma) = \left\{ (\lambda \vec{f}_* + \vec{T}; \vec{f}, \vec{g}) : \vec{f} \in \mathcal{R}_q^n, \vec{g} \in \mathcal{R}_q^m, A\vec{f} + \vec{g} = \lambda \vec{f}_* + \vec{T} \pmod q, \|\vec{g}\|_\infty \leq \gamma \right\}.$$

According to Theorem 1, the protocol $\Pi_0 \diamond \Pi_1$ reduces relation R to $R(A, \gamma)$. The composite Σ -protocol Π_{ZKmain} is as follows:

Protocol Π_{ZKmain} 

Theorem 5. Let $pp := (k, n, m, \mathcal{B}, A, \gamma < q/2)$ be the public parameters such that $\mathcal{C} \subset R_q$ are strong sampling sets where $\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}) = c$. Choose b, ℓ, ω, σ , and $\bar{k}$ such that $k\mathcal{B} = \vec{\mathcal{B}} = \omega^\ell$, $c\ell\omega = b$, $(\sigma + cb) \leq \gamma$, and $\gamma = \bar{k}b$. Π_{ZKmain} satisfies completeness, special soundness, and non-abort SHVZK.

Proof. Completeness: From the parameter settings and the completeness of Π_1 , we have $\|\vec{e}_*\|_\infty \leq b = c\ell\omega$ and send $\vec{T} = A\vec{h} + \vec{r} \pmod q$ to the verifier. If the $\vec{e}_*$ pass the rejection sampling in the honest execution, the prover sends $\vec{g} = \lambda \vec{e}_* + \vec{r}, \vec{f} = \lambda \vec{s}_* + \vec{h}$. It can be proven that the verifier accepts in the honest execution. First, since

$$\sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j = \sum_{i=0}^{\ell-1} \omega^i \vec{e}_i = \vec{e}, \sum_{j=0}^{k-1} \rho_{1,j} \vec{s}_j = \sum_{i=0}^{\ell-1} \omega^i \vec{s}_i = \vec{s};$$

we have

$$\sum_{i=0}^{\ell-1} \omega^i \vec{f}_i = \sum_{i=0}^{\ell-1} \omega^i (A\vec{s}_i + \vec{e}_i) = A(\sum_{j=0}^{k-1} \vec{\rho}_{1,j} \vec{s}_j) + \sum_{j=0}^{k-1} \vec{\rho}_{1,j} \vec{e}_j = \sum_{j=0}^{k-1} \rho_{1,j} \vec{t}_j.$$

The verifier passes the check. According to Theorem 3, the verifier passes the check as follows:

$$A\vec{f} + \vec{g} = \lambda \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{f}_i + \vec{T}, \|\vec{g}\|_\infty \leq \gamma.$$

In summary, completeness is proved.

Special soundness: First, from Theorem 4 we have

$$A\vec{s}'_* + \vec{e}'_* = \zeta \vec{y} = \zeta (\sum_{i=0}^{\ell-1} \rho_{2,i} \vec{f}_i) = \vec{f}'_* \text{ and } \|\vec{e}'_*\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\gamma,$$

with

$$\vec{e}'_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{e}'_i, \quad \vec{s}'_* = \sum_{i=0}^{\ell-1} \rho_{2,i} \vec{s}'_i,$$

corresponding to the extraction process for a single $\vec{e}'_i$ for $i \in [\ell]$.

Secondly, we demonstrate that the fold-split-fold procession in Π_{ZKmain} is extractive injective. There is just one unique valid input set corresponding to the output. For a given output $\vec{e}'_*$ with a small norm bound of $\vec{g}$, the analysis in this paper guarantees that there is only one set of $(\vec{e}_i)_{i=0}^{\ell-1}$ corresponding to $\vec{e}'_*$. Hence, computing $\sum_{i=0}^{\ell-1} \omega^i \vec{e}_i$ will only yield one result vector $\vec{e}$. Similarly, for this fixed $\vec{e}$, there is only one set of input solutions $(\vec{e}_j)_{j=0}^{k-1}$ corresponding to it.

Rewinding $\vec{\rho}_2$ and constructing linear equations for fixed $A, \vec{t}_i, \vec{\rho}_1$, and $(\vec{f}_i)_{i=0}^{\ell-1}$, rewinding the verifier and choosing ℓ independently with $\vec{\rho}_2^{(1)}, \vec{\rho}_2^{(2)}, \dots, \vec{\rho}_2^{(\ell)} \in \mathcal{C}^\ell$, where every $\vec{\rho}_2^{(j)} = (\rho_{2,0}^{(j)}, \rho_{2,1}^{(j)}, \dots, \rho_{2,\ell-1}^{(j)})$, we can obtain the linear combinations

$$\vec{e}'_*^{(j)} = \sum_{i=0}^{\ell-1} \rho_{2,i}^{(j)} \vec{e}'_i \quad (j = 1, 2, \dots, \ell); \quad \vec{s}'_*^{(j)} = \sum_{i=0}^{\ell-1} \rho_{2,i}^{(j)} \vec{s}'_i \quad (j = 1, 2, \dots, \ell).$$

The coefficient matrix of the above linear combinations is denoted as $M \in \mathcal{C}^{\ell \times \ell}$. Obviously, M is invertible. Then

$$\begin{pmatrix} \vec{e}'_0 \\ \vec{e}'_1 \\ \vdots \\ \vec{e}'_{\ell-1} \end{pmatrix} = M^{-1} \begin{pmatrix} \vec{e}'_*^{(1)} \\ \vec{e}'_*^{(2)} \\ \vdots \\ \vec{e}'_*^{(\ell)} \end{pmatrix}; \quad \begin{pmatrix} \vec{s}'_0 \\ \vec{s}'_1 \\ \vdots \\ \vec{s}'_{\ell-1} \end{pmatrix} = M^{-1} \begin{pmatrix} \vec{s}'_*^{(1)} \\ \vec{s}'_*^{(2)} \\ \vdots \\ \vec{s}'_*^{(\ell)} \end{pmatrix}.$$

From this, all items can be enumerated and extracted as $\vec{e}'_0, \vec{e}'_1, \dots, \vec{e}'_{\ell-1}$ and $\vec{s}'_0, \vec{s}'_1, \dots, \vec{s}'_{\ell-1}$ one by one. We can obtain $A\vec{s}'_i + \vec{e}'_i \pmod{q} = \zeta \vec{f}_i$ for any $i \in [\ell]$.

Combining $\zeta \vec{f}_i = A\vec{s}'_i + \vec{e}'_i \pmod{q}$ ($i = 0, 1, \dots, \ell - 1$) in the protocol, we have

$$\sum_{j=0}^{k-1} \rho_{1,j} \vec{e}'_j = \sum_{i=0}^{\ell-1} \omega^i \vec{e}'_i = \vec{e}' \text{ and } \sum_{j=0}^{k-1} \rho_{1,j} \vec{s}'_j = \sum_{i=0}^{\ell-1} \omega^i \vec{s}'_i = \vec{s}'.$$

Suppose we have obtained k sets of linearly independent linear combinations of $\vec{e}'$ and $\vec{s}'$, which are generated by k linearly independent challenge vectors $\vec{\rho}_1^{(t)} = (\rho_{1,0}^{(t)}, \rho_{1,1}^{(t)}, \dots, \rho_{1,k-1}^{(t)})$ for $t = 1, 2, \dots, k$. Specifically, we have:

$$\vec{e}'^{(t)} = \sum_{j=0}^{k-1} \rho_{1,j}^{(t)} \vec{e}'_j, \quad \vec{s}'^{(t)} = \sum_{j=0}^{k-1} \rho_{1,j}^{(t)} \vec{s}'_j \quad (t = 1, 2, \dots, k).$$

The coefficient matrix of the above linear combinations is denoted as $M_0 \in \mathcal{C}^{k \times k}$. Obviously, the matrix M_0 is invertible. By left-multiplying both sides of the above equation by M_0^{-1} (the inverse of M_0), we can uniquely extract all $\vec{e}'_j$ and $\vec{s}'_j$ ($j = 0, 1, \dots, k - 1$):

$$\begin{pmatrix} \vec{e}'_0 \\ \vec{e}'_1 \\ \vdots \\ \vec{e}'_{k-1} \end{pmatrix} = M_0^{-1} \begin{pmatrix} \vec{e}'^{(1)} \\ \vec{e}'^{(2)} \\ \vdots \\ \vec{e}'^{(k)} \end{pmatrix}; \quad \begin{pmatrix} \vec{s}'_0 \\ \vec{s}'_1 \\ \vdots \\ \vec{s}'_{k-1} \end{pmatrix} = M_0^{-1} \begin{pmatrix} \vec{s}'^{(1)} \\ \vec{s}'^{(2)} \\ \vdots \\ \vec{s}'^{(k)} \end{pmatrix}.$$

In conclusion, with k linearly independent challenge vectors $\vec{\rho}_1^{(t)}$ and their corresponding linear combinations $\vec{e}'^{(t)}$ and $\vec{s}'^{(t)}$, we can uniquely extract all individual $\vec{e}'_j$ and $\vec{s}'_j$ ($j = 0, 1, \dots, k - 1$) by inverting the coefficient matrix M_0 . We can obtain that

$$A \sum_{i=0}^{\ell-1} \omega^i \vec{s}'_i + \sum_{i=0}^{\ell-1} \omega^i \vec{e}'_i = \sum_{i=0}^{\ell-1} \omega^i \zeta \vec{f}_i = \sum_{j=0}^{k-1} \rho_{1,j} \zeta \vec{t}_j.$$

Then, we can deduce that $A\vec{s}'_j + \vec{e}'_j = \zeta \vec{t}_j \pmod{q}$.

Meanwhile, since the Π_1 is extractive injective and $\|\vec{e}_*\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\gamma$, where $c\ell\omega = b$, $\bar{\mathcal{B}} = \omega^\ell$, $(\sigma + cb) \leq \gamma$, $\gamma = \bar{k}b$, and the coefficients of M and M_0 are of constant order (determined by the properties of the challenge domain $\mathcal{C}$), it follows that every

$$\vec{e}_*^{(j)} = \sum_{i=0}^{\ell-1} \rho_{2,i}^{(j)} \vec{e}_i \leq c\ell \cdot \|\vec{e}_i\|_\infty, j \in [\ell].$$

Then, we have $\|\vec{e}_i\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\bar{k}\omega$ and $2c\ell\bar{k}\omega\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta) = 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\gamma$. Now, we have

$$\sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j = \sum_{i=0}^{\ell-1} \omega^i \vec{e}_i = \vec{e}$$

and $\|\vec{e}'\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\bar{k}\bar{\mathcal{B}}$. Then we have $\|\sum_{j=0}^{k-1} \rho_{1,j} \vec{e}_j\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\bar{k}k\bar{\mathcal{B}} = 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\bar{k}\bar{\mathcal{B}}$. Then we can obtain $\vec{e}'_j$ that $\|\vec{e}'_j\|_\infty \leq 2\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta)\bar{k}\bar{\mathcal{B}}$. Therefore, the extracted $\vec{e}'_j$ is the error vector required.

In summary, the extractor $\mathcal{E}$ can extract all valid witnesses $(\vec{s}'_j, \vec{e}'_j)$ for $j \in [k]$ by solving the system of linear equations through multiple rewinds of the challenge $\vec{\rho}_1, \vec{\rho}_2$, and other transcripts. Therefore, Π_{ZKmain} demonstrates $(k, \ell, 2)$ special soundness.

Non-abort SHVZK: For Π_{ZKmain} , denote the folding challenge in the first folding operation as $\vec{\rho}_1$. Randomly sample the splitting operation, $\vec{f}'_1, \dots, \vec{f}'_{\ell-1} \leftarrow \mathcal{R}_q^m$ and set

$$\vec{f}'_0 = \sum_{j=0}^{k-1} \vec{\rho}_{1,j} \vec{t}_j - \sum_{i=1}^{\ell-1} \omega^i \vec{f}'_i.$$

Obviously, $(\vec{f}'_i)_{i=0}^{\ell-1}$ pass the check of Π_{ZKmain} . Moreover, $(\vec{f}'_i)_{i=0}^{\ell-1}$ are indistinguishable from real ones.

Similarly, denote the folding challenge as ρ_2 in the second folding operation. The simulator simply computes $\vec{f}_* := \sum_{i=0}^{\ell-1} \omega^i \vec{f}'_i$. Finally, from Protocol 1, it follows that the masking operation satisfies zero-knowledge. Since all steps pass, the simulated transcript is a valid one and indistinguishable from a real transcript. Therefore, the protocol Π_{ZKmain} is non-abort SHVZK. $\square$

4. Parameter

In this section, the rings $\mathcal{R}$ and their monomial challenge set $\mathcal{C} = \{0, \pm 1, \dots, \pm X^{d-1}\}$ have certain convenient properties. In particular, $|\mathcal{C}| = 2d + 1$ and $\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}) = 1$. More precisely, $2/(c - c') \in \mathcal{R}$ is a polynomial with coefficients in $\{-1, 0, 1\}$ for all distinct $c, c' \in \mathcal{C}$. This implies that the constant 2 is the slack factor value $\zeta = 2$ in this instantiation. From this, it follows that $\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, 2) \leq d$. For a more detailed discussion on optimal challenge sets, see [38].

In this section, let $pp := (n, m, A, \gamma < q/2)$ be the public parameters. Choose b, ℓ, ω , and σ such that $k\bar{\mathcal{B}} = \bar{\mathcal{B}} = \omega^\ell$, $c\ell\omega = b$, and $(\sigma + cb) \leq \gamma$. The problem $\text{MLWE}_{n,m,q,\bar{\mathcal{B}}}$ inherits classical worst-case hardness from module lattice problems if the following hold: the module rank satisfies $n \geq 2$, $q \geq 2(dn)^2$ and $q \equiv 1 \pmod{2d}$. Under these parameters, there exists a classical PPT reduction from worst-case $\text{Mod-GIVP}_{\gamma}^{\eta_e}$ to $\text{MLWE}_{q,\Psi \leq a}$ using $\text{poly}(dn)$ samples. From Theorem 2, we require $\alpha q \geq 2\sqrt{d} \cdot \omega(\sqrt{\log n})$. From Theorem 4 and the hardness of the MLWE problem, it follows that this problem is hard if $2\sqrt{d} \cdot \omega(\sqrt{\log n}) < 2\gamma\bar{\omega}_{\mathcal{R}_q}(\mathcal{C}, \zeta) = 2\gamma d < \frac{q}{2}$, then $\frac{\omega(\sqrt{\log n})}{\sqrt{d}} < \gamma < \frac{q}{4d}$.

5. Conclusions

This paper proposes a lightweight amortized Σ -protocol tailored for MLWE. Following existing lattice proof frameworks, our construction abandons complex tools such as NTT and relies only on fold-split-fold operations and rejection sampling. The protocol supports

efficient batch proofs for multiple MLWE statements and satisfies completeness, special soundness, and non-abort SHVZK. It can be applied to post-quantum signatures and secure data transmission, providing a practical and efficient solution for lattice-based cryptographic applications.

Author Contributions: Conceptualization, Q.L. and S.Y.; methodology, Q.L. and S.Y.; formal analysis, Q.L. and S.Y.; writing—original draft preparation, Q.L.; writing—review and editing, S.Y.; supervision, S.Y.; project administration, S.Y.; funding acquisition, S.Y. All authors have read and agreed to the published version of the manuscript.

Funding: The project is supported by the National Natural Science Foundation of China (62272104).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof Systems (Extended Abstract). In Proceedings of the ACM Symposium on Theory of Computing (STOC), Providence, RI, USA, 6–8 May 1985; pp. 291–304.
- Cramer, R. Modular Design of Secure Yet Practical Cryptographic Protocols. Ph.D. Thesis, University of Amsterdam, Amsterdam, The Netherlands, 1996.
- Islam, S.H.; Zeadally, S. Provably secure identity-based two-party authenticated key agreement protocol based on CBI-ISIS and Bi-ISIS problems on lattices. *J. Inf. Secur. Appl.* **2020**, *2020*, 102540.
- Far, S.B.; Asaar, M.R.; Haghbin, A. Zero-knowledge-based distributed auditing protocol. *Secur. Priv.* **2023**, *2023*, e289.
- Yang, Y.; Yuan, H.; Yan, L.; Ruan, Y. Post-quantum identity-based authenticated multiple key agreement protocol. *ETRI J.* **2023**, *45*, 1090–1102.
- Yang, C.; Li, P.; Kuo, H. (k, n) secret image sharing scheme with privileged set. *J. Inf. Secur. Appl.* **2023**, *2023*, 103413.
- Harn, L.; Hsu, C.; Xia, Z.; Xu, H.; Zeng, S.; Pang, F. Simple and efficient threshold changeable secret sharing. *J. Inf. Secur. Appl.* **2023**, *2023*, 103576.
- Feng, H.; Liu, J.; Wu, Q. Group Signatures and Ring Signatures with Post-Quantum Security. *J. Cryptologic Res.* **2021**, *2021*, 183–201. (In Chinese)
- Assidi, H.; Ayebe, E.B.; Souidi, E.M. An efficient code-based threshold ring signature scheme. *J. Inf. Secur. Appl.* **2019**, *2019*, 52–60.
- Wang, J.; Chen, X.; Li, H. Message Integration Authentication in the Internet-of-Things via Lattice-Based Batch Signatures. *Sensors* **2018**, *18*, 4056.
- Chen, X.; Gao, S.; Xu, S.; Chen, L.; Yiu, S.M.; Xiao, B. From Σ -Protocol-Based Signatures to Ring Signatures: General Construction and Applications. *IEEE Trans. Inf. Forensics Secur.* **2025**, *2025*, 3646–3661.
- Zhou, Y.; Liu, S.; Yang, Y.; Shi, W.; Ning, Z. Lattice-based dynamic decentralized anonymous credential scheme supporting batch verification. *Comput. Stand. Interfaces* **2026**, *95*, 104039.
- Xue, Y.; Zheng, T.; Gao, S.; Xiao, B.; Au, M.H. Compressed Sigma Protocols: New Model and Aggregation Techniques. In Proceedings of the Information Security and Privacy (IS&P), Melbourne, Australia, 14–16 July 2025; pp. 163–183.
- Zhang, L.; Gao, S.; Xiao, B. Lattice-based Σ -Protocols for Polynomial Relations with Standard Soundness. *IACR Cryptol. ePrint Arch. Paper 2025/313*. 2025. Available online: <https://eprint.iacr.org/2025/313> (accessed on 24 July 2026).
- Cramer, R.; Damgård, I. On the Amortized Complexity of Zero-Knowledge Protocols. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 16–20 August 2009; pp. 177–191.
- Esgin, M.F.; Zhao, R.K.; Steinfeld, R.; Liu, J.K.; Liu, D. MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS), London, UK, 11–15 November 2019; pp. 567–584.
- Prajapat, S.; Gautam, D.; Kumar, P.; Jangirala, S.; Das, A.K.; Park, Y.; Lorenz, P. Secure Lattice-Based Aggregate Signature Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2024**, *73*, 12370–12384.
- Wang, P.; Xiang, T.; Li, X.; Xiang, H. Public key encryption with conjunctive keyword search on lattice. *J. Inf. Secur. Appl.* **2020**, *2020*, 102433.
- Krzywiecki, I.; Klucznik, K.; Koziel, P.; Panwar, N. Privacy-oriented dependency via deniable SIGMA protocol. *Comput. Secur.* **2018**, *2018*, 53–67.
- Yuce, M.F.; Erturk, M.A.; Aydin, M.A. Privacy-preserving VPN handshakes with Schnorr-based zero-knowledge proofs. *Comput. Secur.* **2026**, *2026*, 104887.

21. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. (Leveled) fully homomorphic encryption without bootstrapping. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS), Cambridge, MA, USA, 8–10 January 2012; pp. 309–325.
22. Langlois, A.; Stehlé, D. Worst-Case to Average-Case Reductions for Module Lattices. *Des. Codes Cryptogr.* **2015**, *75*, 565–599.
23. Lyubashevsky, V. Basic Lattice Cryptography: The concepts behind Kyber (ML-KEM) and Dilithium (ML-DSA). *IACR Cryptol. ePrint Arch. Paper 2024/1287*. 2024. Available online: <https://eprint.iacr.org/2024/1287> (accessed on 24 July 2026).
24. Schnorr, C.P. Efficient Signature Generation by Smart Cards. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 11–15 August 1991; pp. 239–252.
25. Albrecht, M.R.; Lai, R.W.F. Subtractive Sets over Cyclotomic Rings: Limits of Schnorr-like Arguments over Lattice. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 18–22 August 2021; pp. 519–548.
26. Attema, T.; Cramer, R.; Kohl, L. A Compressed Σ -Protocol Theory for Lattices. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 18–22 August 2021; pp. 549–579.
27. Lyubashevsky, V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Tokyo, Japan, 6–10 December 2009; pp. 598–616.
28. Lyubashevsky, V. Lattice Signatures without Trapdoors. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Cambridge, UK, 15–19 April 2012; pp. 738–755.
29. Nguyen, N.K.; O’Rourke, G. More Efficient Lattice-Based Zero-Knowledge Proofs with Straight-Line Extractability. In Proceedings of the 12th ACM ASIA Public-Key Cryptography Workshop (APKC), Hanoi, Vietnam, 25–29 August 2025; pp. 34–43.
30. Esgin, M.F.; Steinfeld, R.; Liu, J.K.; Liu, D. Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 18–22 August 2019; pp. 115–146.
31. Bootle, J.; Lyubashevsky, V.; Nguyen, N.K.; Seiler, G. More Efficient Amortization of Exact Zero-Knowledge Proofs for LWE. In Proceedings of the Computer Security (ESORICS), Darmstadt, Germany, 4–8 October 2021; pp. 608–627.
32. Boneh, D.; Chen, B. LatticeFold: A Lattice-based Folding Scheme and its Applications to Succinct Proof Systems. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Hangzhou, China, 8–12 December 2025; pp. 330–362.
33. Zhao, Y.; Deng, R.H.; Zang, B.; Zhao, Y. Practical Zero-Knowledge Arguments from Σ -Protocols. In Proceedings of the Internet and Network Economics (WINE), Hong Kong, China, 15–17 December 2005; pp. 8880–8892.
34. Bootle, J.; Cerulli, A.; Chaidos, P.; Groth, J.; Petit, C. Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Vienna, Austria, 8–12 May 2016; pp. 327–357.
35. Chen, S.; Cheon, J.H.; Kim, D.; Park, D. Verifiable Computing for Approximate Computation. *IACR Cryptol. ePrint Arch. Paper 2019/762*. 2019. Available online: <https://eprint.iacr.org/2019/762> (accessed on 24 July 2026).
36. Kothapalli, A.; Parno, B. Algebraic Reductions of Knowledge. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 19–24 August 2023; pp. 669–701.
37. Regev, O. On Lattices, Learning With Errors, Random Linear Codes, and Cryptography. In Proceedings of the ACM Symposium on Theory of Computing (STOC), Baltimore, MD, USA, 21–22 May 2005; pp. 84–93.
38. Attema, T.; Cramer, R.; Xing, C. A note on short invertible ring elements and applications to cyclotomic and trinomial number fields. *Math. Cryptol.* **2021**, *1*, 45–70.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.