Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption

Debadrita Talapatra
IIT Kharagpur, India

Nimish Mishra
IIT Kharagpur, India

Debdeep Mukhopadhyay
IIT Kharagpur, India

Abstract

Prior research on ensuring trust in delegated computation through lattice-based zero-knowledge proofs mostly rely on Learning-With-Errors (LWE) assumption. In this work, we propose a zero-knowledge proof of knowledge using the Ring Learning with Rounding (RLWR) assumption for an interesting and useful class of statements: linear relations on polynomials. We begin by proposing, to the best of our knowledge, the first efficient commitment scheme in literature based on the hardness of RLWR assumption. We establish two properties on RLWR that aid in the construction of our commitments: ① closure under addition with double rounding, and ② closure under multiplication with a short polynomial. Building upon our RLWR commitment scheme, we consequently design a RLWR based Σ_2 protocol for proving knowledge of a single committed message under linear relations with public polynomials.

As an use-case of our proposed Σ_2 protocol, we showcase a construction of a quantum-safe Searchable Symmetric Encryption (SSE) scheme by plugging a prior LWR based SSE scheme from (EuroS&P 2023) with our Σ_2 protocol. Concretely, using our Σ_2 protocol for linear relations, we prove the correctness of an encrypted search result in a zero-knowledge manner. We implement our verifiable SSE framework and show that the overhead of an extra verification round is negligible (0.0023 seconds) and retains the asymptotic query execution time complexity of the original SSE scheme.

Our work establishes results on zero-knowledge proof systems that can be of independent interest. By shifting the setting from RLWE to RLWR, we gain significant ① efficiency improvements in terms of communication complexity by $O(M)$ (since some prior works on RLWE require rejection sampling by a factor of M), as well as ② very short proof size (8.4 KB) and tighter parameters (since RLWR does not explicitly manipulate error polynomials like RLWE).

Contents

1 Introduction **3**

1.1 Our Contribution 5

1.2 Related Work 6

2 Preliminaries **7**

2.1 Ring Learning With Rounding Problem (RLWR) 7

2.2 Commitment Scheme 8

2.3 Zero Knowledge Proofs 9

2.4 SSE: Syntax and Security Model 10

2.5 Brief Overview of [BKLP14] 11

3 Technical Contribution **11**

3.1 Establishing Properties on LWR samples 11

3.2 Ring-LWR (RLWR) Commitment Scheme 14

3.3 Σ_2 Protocol For Pre-image Proof 17

3.4 Σ_2 Protocol For Proving Linear Relations 19

4 Verifiable Quantum-safe SSE from RLWR Commitments **21**

4.1 OQXT Overview 21

4.2 Verifiable-OQXT 22

5 Results and Comparison **25**

6 Conclusion **28**

1 Introduction

Commitments and Proofs of Knowledge. Commitment schemes [Blu83] and their companion zero-knowledge proofs of knowledge (ZK-PoK) allow a prover to prove to a verifier some properties of a message m in a zero-knowledge manner (i.e. without revealing any additional information about m than what is already revealed by the proof itself). They form a fundamental building block in the design of generic zero-knowledge proofs and other advanced cryptographic primitives [DF89, RST01, CFSY96, Cha85, LN17, ASW00], since they can be used to realize any arithmetic circuit.

Succinct arguments enable an untrusted prover to convince a verifier of the correct execution of a computation while keeping communication and verification time significantly smaller than the computation itself [Kil92, Mic94]. Notable advancements transpired in constructing efficient succinct arguments that balance trade-offs between underlying assumptions and efficiency. One of the fundamental properties of zero-knowledge proofs (ZKPs) is soundness, meaning that a dishonest prover should not be able to produce a convincing proof. In the context of proofs of knowledge (PoK), this implies that a successful prover possesses the relevant secret (i.e., a witness). This is typically demonstrated by employing an extractor that efficiently retrieves the witness using two accepting protocol transcripts with the same initial message.

"Post-Quantum" Commitments. The holy grail of research in proof systems is to develop efficient quantum-safe proof systems with negligible soundness error and small proof sizes. There exist efficient hash-based commitment schemes [BCR+19, COS20, AHIV23] that can prove complex relations on one hand, but demand high memory storage overheads. Lattice-based commitment schemes [JKPT12, AJL+12, LNSW13, XXW13, BKLP14, BCK+14, BDL+18, ESLL19, LNP22] are an efficient and more coveted alternative, that are capable of generating small proofs with negligible soundness error but are restricted in terms of the relations they prove. Moreover, the selection of lattice-based schemes as the primary algorithms for key encapsulation and signatures in the NIST PQC competition, suggests that lattice-based schemes are more amenable to practical deployment and hold more chances to gain traction in real-world scenarios, also gaining by efforts in hardware acceleration.

To the best of our knowledge, all existing lattice-based commitment schemes and zero-knowledge proofs are essentially based on the hardness assumptions of Ring/Module SIS and Ring/Module LWE problems [Mic07, PR06, LS15, LPR13, LM06]. For instance, [BKLP14] introduced a commitment scheme and accompanying zero-knowledge protocols based on Ring-LWE assumption. The scheme enables committing to a vector over $\mathbb{Z}_q$, resulting in a commitment that is only a constant factor larger than the vector. They also provide protocols for proving knowledge of a committed string and demonstrating linear and multiplicative relations among committed values. By working in the setting of *special soundness*[1], they achieve negligible soundness error in just one iteration. The commitments are unconditionally binding and computationally hiding. A direct improvement of this work was proposed in [BDL+18] that proposes a statistically hiding and statistically binding commitment scheme and another construction of a practically efficient computationally hiding (based on

[1] Where the prover commits in relation R and the verifier verifies in another (statistically close) relation R'.

the hardness of Module-SIS) and computationally binding (relies on Module-LWE assumption) commitment scheme.

Issues with LWE based Proof Systems: Essentially, the existing literature on lattice-based proof systems can be broadly classified into *one-shot proofs* (initiated with "Fiat-Shamir with aborts" [Lyu09, Lyu12]) that achieve negligible soundness error in a single run but restricted to approximate zero-knowledge proofs; and *multi-shot proofs* [Ste96] that are suited to prove complex relations with very small challenge space but have non-negligible soundness error. While multi-shot proofs require a non-constant number of rounds to achieve negligible soundness error (thereby being inefficient in communication complexity), single-shot proofs require complicated rejection sampling and loose bounds on error polynomials in order to achieve acceptable soundness error. In this work, our main focus is thus the following:

Can we design a commitment scheme based on the Ring-LWR assumption (instead of the Ring-LWE or Module-LWE assumption) with its associated zero-knowledge proofs of knowledge achieving negligible soundness error without the need to perform expensive operations (like multi-shot proofs, rejection sampling etc.) as with existing LWE based systems?

We answer this question in the affirmative. We develop the first RLWR based commitment scheme, and associated proofs of knowledge for a class of linear relations (which have several interesting applications). Our RLWR based commitments and associated protocols achieve comparable guarantees as state-of-the-art RLWE protocols, while achieving tighter parameters and more efficient communication overhead.

Use-case for Our Proofs of Linear Relations. Efficient quantum-safe zero-knowledge proofs finds enormous application in multiple advanced cryptographic protocols like threshold encryption [DF89], ring signatures [RST01], anonymous credentials [Cha85], verifiable encryption [LN17], optimistic fair exchange protocols [ASW00] etc.

However, the most interesting use-case for proof systems is verifiable delegated computation[2]. There already exists literature on verifiable FHE [VKH23, ABPS24, AGT24, KVMGH23], verifiable MPC [RCPT19, TZ21], and so on. But an often overlooked class of delegated computation schemes from a zero-knowledge proof-of-knowledge verifiability perspective is Searchable Symmetric Encryption (SSE). SSE belongs to a class of delegated computation schemes that support encrypted searches over symmetrically encrypted data stored at third-party cloud servers. There exist a long line of research in the domain of SSE, in terms of query expressiveness, supporting dynamic updates, improved efficiency using memory architectures, leakage resilience [SWP00, CGKO06a, CK10, CJJ+13a, PM21, PPSY21, CT14, TPM23] etc. A very recent work proposed in [TPM23] develops a quantum-safe SSE scheme from lattice-based assumptions in a semi-honest server model. Most of the existing SSE schemes assume a semi-honest server threat model, where the cloud server is assumed to be capable of passively observing information during a search and cannot change/tamper

[2]Where a resource constrained client offloads some computation to an untrusted cloud server. Verifiability is paramount here because the client needs to *verify* whether it can trust the computations performed by the untrusted server.

with the user data or search results. SSE in a malicious server setting (server can tamper with user data) however, is a less explored direction [BFP16, KO12, CYG+15, JLZL25], with almost none of them based on quantum-safe lattice based commitments and zero-knowledge proofs. We thus address this gap in literature by answering the following question in the affirmative:

Can our efficient, RLWR based commitment scheme and companion zero-knowledge proofs of knowledge be used to efficiently verify a quantum-safe encrypted search (SSE) protocol?

To the best of our knowledge, this work gives the *first* construction of a verifiable, RLWR based quantum-safe SSE protocol under the assumption of a malicious server.

1.1 Our Contribution

In this work we propose the first Ring Learning With Rounding (RLWR) based commitment scheme and a companion zero-knowledge proof of knowledge that efficiently proves linear relations of the form $m_3 = m_1x_1 + m_2x_2$ for messages m_1, m_2, m_3 and arbitrary public $x_i \in \mathbb{Z}_q[x]/\langle x^n + 1\rangle$. In being an efficient lattice-based commitment scheme, our work is most closely related to [BKLP14], that is based on Ring-LWE problem. Our RLWR based commitment scheme is statistically binding and computationally hiding with a negligible knowledge error, while achieving tighter parameters than that in [BKLP14]. Due to the shift from approximate RLWE setting to a deterministic RLWR framework, our commitment scheme does not require an explicit error sampling and eliminates the need to employ rejection sampling [Lyu09, Lyu12] to simulate the responses of a prover independent of the secret key. This renders our commitment scheme to be lightweight and allows to choose tighter parameters. To summarize, in this work we propose the following -

1. **Efficient Commitment Schemes from RLWR assumption.** We propose the first RLWR based commitment scheme that is perfectly binding and computationally hiding. Our scheme is closely motivated by the RLWE based commitment scheme proposed in [BKLP14]. We improve upon their parameterization by several orders of magnitude, due to elimination of error sampling in our protocols[3]. We bypass the rejection sampling step incorporated in [BKLP14] and improve upon the computation complexity by a factor $O(M)$ where $M = e^{12/\alpha+1/(2\alpha^2)}$ is the rejection sampling factor[4] [Lyu12] and directly impacts the parameter size and expected number of times the protocol in [BKLP14] needs to be restarted.
2. **Efficient ZK-PoK for RLWR based Committed Values.** Using the above commitment scheme, we devise a lightweight and efficient pre-image proof that proves knowledge of the committed values. We follow a similar framework as [BKLP14], but differ in the underlying structure of the committed value of the message m. Our Σ_2

[3] In [BKLP14], n represents the degree of the ring, k represents the number of polynomials sampled from the ring, and γ is a bound that ensures correct parameterization of ring modulus q in order to ensure negligible soundness error.

[4] α is a factor that loosely encapsulates the distribution of error coefficients in RLWE.

protocol proves knowledge of a valid opening for a single committed message. The commitment is computed as an RLWR sample with appropriate rounding parameter, such that it satisfies completeness, soundness and honest verifier zero-knowledge properties. The commitment and proof size of our proposed protocol are 50 KB and 8.4 KB respectively, which is significantly less than the commitment and proof size of [BKLP14].

3. **Efficient ZK-PoK for Linear Relations.** Extending the basic Σ_2 protocol as done in [BKLP14], we construct protocols for proving linear relations for the committed values $m_1, m_2, m_3 \in R_q$, of the form $m_3 = m_1 x_1 + m_2 x_2$ for some public $x_i \in \mathbb{Z}_q[x]/\langle x^n+1\rangle$.

4. **Verifiable Quantum-safe SSE.** As a practical application of the Σ_2 protocol devised to prove linear relations using the RLWR based commitment scheme, we construct a pre-image proof for quantum-safe SSE scheme [TPM23] to prove the knowledge of a correct search result by a malicious server to an honest client[5]. We show that the correctness holds by the correctness guarantee of the underlying commitment scheme and the correct parameter choices. We formally prove that the proposed verifiable SSE construction is honest verifier zero-knowledge that satisfies completeness and special soundness properties.

1.2 Related Work

Proof Systems. There exist a long line of research on building commitment schemes and corresponding zero-knowledge proofs based on number theoretic assumptions [BDP00, IKOS07, IKOS09, CD09, CDP12, CDK14, BCC+15, GK15, BCC+16, BBB+18]. Discrete-logarithm (DL) based ZKPs [BCC+15, GK15, BCC+16, BBB+18] achieve a convincing soundness level (i.e., a negligible soundness error) in a single protocol run (i.e., they are one-shot). Such schemes although exhibit efficient communication complexity and proofs for algebraic circuit over large fields or integers, but are inherently quantum unsafe.

Quantum safe commitment schemes entail a wide research spectrum in literature. The current state-of-the-art shows that most efficient quantum safe commitment schemes are hash-based commitments [BCR+19, COS20, AHIV23], that provide poly-logarithmic proof sizes and can be efficiently used to solve arbitrary statements. However, hash-based commitment schemes include a "startup" cost or "base" cost (around $50KB$). While proving arbitrary big statements, this cost might not affect the asymptotic complexity but for specific applications like a signature scheme or a verification scheme, this could significantly blow up the cost. Furthermore, since they have to perform a lot of hashing they are not very fast and also requires considerably large memory storage because they use error correcting codes that in turn uses code words of the size linear with the size of the witness. Lattice-based commitment schemes and zero-knowledge proofs [JKPT12, AJL+12, LNSW13, XXW13, BKLP14, BCK+14, BDL+18, ESLL19, LNP22] can outperform hash-based commitments in these aspects, hence there is an active effort to construct succinct and efficient ZKPs from lattice-based assumptions that would be faster and have comparatively smaller proof size than the hash-based commitment schemes.

[5]Note that since our application is already a client-server protocol, we stick to a Σ_2 protocol and do not attempt verifiability with NIZK proofs.

Zero-Knowledge proofs based on lattice-based cryptography can be broadly classified into two categories. First, the combinatorial proofs that are based on Stern-type schemes [Ste96, LLNW23] whose challenge sets are extremely small, hence can be used to prove complex relations. But they have a non-negligible soundness error, hence they require multiple iterations to ensure security, implying the proof size and communication complexity is very high. On the other hand there exist another class of proofs called algebraic proofs that are based on Schnorr's protocol [Sch91] where there are no restrictions on the size of the challenge set. This leads to the development on one-shot proofs [Lyu09, Lyu12, BKLP14, LN17, BDL+18, ESLL19] that are more efficient and with short/fast proofs achieves negligible soundness error in a single run. However they are restricted in terms of the relations they can prove. Additionally the relations that are proved are relaxed or approximate.

Searchable Symmetric Encryption (SSE). SSE schemes [SWP00, CGKO06a, CK10, CJJ+13a] provision users with *search* capabilities over symmetrically encrypted data. There exist today efficient SSE schemes that support conjunctive (and more general Boolean) queries [CJJ+13a, CJJ+14, PM21, TPM23]. Modern SSE schemes trade-off security for efficiency. These schemes allow the server to learn "some" information during query execution, detailed by their *leakage* profile. While SSE schemes are extremely fast and highly scalable with arbitrarily large real-world datasets, very limited research [BFP16, KO12, CYG+15, JLZL25] has been conducted to verify SSE schemes and prove correctness of a search in presence of a malicious adversary, and (to the best of our knowledge) none of these schemes are in the post-quantum setting. In this work, we leverage our efficient RLWR based commitment scheme and the companion ZK-PoK developed for linear relations to prove knowledge of a correct search result in a quantum-safe SSE [TPM23].

2 Preliminaries

Table 1 lists basic notations used in this paper. Any other notation used is defined in-place within the context of the main text. We present a brief background on the RLWR based commitment scheme and associated ZKPoK as proposed in [BKLP14] in this section.

2.1 Ring Learning With Rounding Problem (RLWR)

Let $n \geq 1$ be the main security parameter and moduli $q \geq p \geq 2$ be integers. Let R_q and R_p denote polynomial rings $\mathbb{Z}_q[x]/(\phi)$ and $\mathbb{Z}_p[x]/(\phi)$ respectively, for $\phi = x^n + 1$. For a vector $s \in R_q$, the ring-LWR distribution L is defined as the distribution over $R_q \times R_p$ obtained by choosing a vector $a \xleftarrow{\$} R_q$ uniformly at random and outputting $(a, b = \lfloor \langle a, s \rangle \rceil_p)$ [BPR12]. For a given distribution over $s \in R_q$ the *decision*-$\mathsf{LWR}_{R,q,p}$ problem is to distinguish (with advantage non-negligible in n) between any desired number of independent samples $(a_i, b_i) \xleftarrow{\$} L$, and the same number of samples drawn uniformly and independently from $R_q \times R_p$.

Notations	Meaning
n	degree of a polynomial, power of 2, typical value: 2^9
q	prime number and modulus of the ring R_q
p	prime number and modulus of the ring R_p
p_1	prime number and modulus of the ring R_{p_1}
k	multiplicative overhead of commitment size
D	domain of challenge; $D = \{d \in \{0,1\}^n : d \neq 1 \wedge \parallel d \parallel_\infty \leq 1 \wedge \deg(d) < n/2\}$ (refer Claim 2)
$x \xleftarrow{\$} \chi$	uniformly sampling x from χ
$x = \mathcal{A}$	x is output of a deterministic algorithm
$x \leftarrow \mathcal{A}'$	x is output of a randomized algorithm
$\mathcal{L}(\mathcal{R})$	Language induced by a binary relation $\mathcal{R}$: $\mathcal{L}(\mathcal{R}) = \{c : \exists w\}$ such that $(c, w) \in \mathcal{R}$
$\mathbb{Z}_q$	quotient ring of integers modulo some prime q
F	Pseudo-random function with output range in $\{0,1\}^\lambda$
F'	Pseudo-random function with output range in a multiplicative group modulo some prime
$\mathbf{x}$	vector of polynomials from a well-defined ring (in bold small-case)

Table 1: Parameters and Notations

2.2 Commitment Scheme

We define a commitment scheme formally below.

A commitment scheme consists of three algorithms (KGen, Com, Ver) such that:

- $\mathsf{KGen}(1^\ell)$: The key generation algorithm outputs a public commitment key pk.
- $\mathsf{Com}(\mathsf{pk}, m)$: The commitment algorithm Com takes as inputs a message m from a message space $\mathcal{M}$ and a commitment key pk, and outputs a commitment/opening pair (c, d).
- $\mathsf{Ver}(\mathsf{pk}, m, c, d)$: The verification algorithm takes a key pk, a message m, a commitment c, and an opening d, and outputs accept or reject.

A commitment scheme has to satisfy the following security requirements:

- **Correctness:** Ver outputs accept whenever the inputs were computed by an honest party, i.e.,

$$\Pr[\mathsf{Ver}(\mathsf{pk}, m, c, d) = \mathsf{accept} : \mathsf{pk} \xleftarrow{\$} \mathsf{KGen}(1^\ell), m \in \mathcal{M}, (c, d) \xleftarrow{\$} \mathsf{Com}(m, \mathsf{pk})] = 1$$

- **Binding:** A commitment cannot be opened to different messages. A scheme is said to be *perfectly binding* if this holds unconditionally, i.e., with overwhelming probability over the choice of the public key $\mathsf{pk} \xleftarrow{\$} \mathsf{KGen}(1^\ell)$, we have that:

$$\big(\mathsf{Ver}(\mathsf{pk}, m, c, d) = \mathsf{accept}\big) \wedge \big(\mathsf{Ver}(\mathsf{pk}, m', c, d') = \mathsf{accept}\big) \implies m = m'$$

  On the other hand, a scheme is said to be *computationally binding* if no PPT adversary can come up with a commitment and two different openings, i.e., for every PPT

adversary $\mathcal{A}$ there exists a negligible function negl such that:

$$\Pr\left[\mathsf{Ver}(\mathsf{pk}, m, c, d) = \mathsf{Ver}(\mathsf{pk}, m', c, d')\right.$$

$$\left.: \mathsf{pk} \xleftarrow{\$} \mathsf{KGen}(1^\ell), (c, m, d, m', d') \xleftarrow{\$} \mathcal{A}(\mathsf{pk})\right] \leq \mathsf{negl}(n).$$

- **Computational Hiding:** A commitment computationally hides the committed message: for every probabilistic polynomial time (PPT) adversary $\mathcal{A}$, there is a negligible function negl such that:

$$\Pr\left[b = b' : \mathsf{pk} \leftarrow \mathsf{KGen}(1^\ell), (m_0, m_1, \mathsf{aux}) \xleftarrow{\$} \mathcal{A}_1(\mathsf{pk}), b \xleftarrow{\$} \{0,1\}\right.$$

$$\left.(c, d) = \mathsf{Com}(m_b, \mathsf{pk}), b' \leftarrow \mathcal{A}_2(c, \mathsf{aux})\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

2.3 Zero Knowledge Proofs

A zero-knowledge proof of knowledge is a two-party protocol between a prover and a verifier, which allows the former to convince the latter that it knows some secret piece of information, without revealing anything about the secret apart from what the claim itself already reveals.

Let (P, V) be a two-party protocol, where V is PPT, and let $\mathcal{R}, \mathcal{R}'$ be a binary relation such that $\mathcal{R} \subseteq \mathcal{R}'$. Then (P, V) is called a Σ_m-protocol for $\mathcal{R}, \mathcal{R}'$ with challenge set $\mathcal{C}$, public input c, and private input w, if and only if it satisfies the following conditions:

- The protocol is of the following form:
  - The prover P computes a commitment t and sends it to V.
  - The verifier V draws a challenge $d \xleftarrow{\$} \mathcal{C}$ and sends it to P.
  - The prover sends a response s to the verifier.

  Depending on the protocol transcript (t, d, s), the verifier accepts or rejects the proof. The protocol transcript (t, d, s) is called *accepting* if the verifier accepts the protocol run.

- **Completeness:** Whenever $(c, w) \in \mathcal{R}$, the verifier V accepts with probability at least $1 - \alpha$.

- **Special soundness:** There exists a PPT algorithm $\mathcal{E}$ (the knowledge extractor) that takes m accepting transcripts $(t, d_1, s_1), \ldots, (t, d_m, s_m)$ satisfying $d_i \neq d_j$ for $i \neq j$ as inputs, and outputs w' such that $(c, w') \in \mathcal{R}'$.

- **Special honest-verifier zero-knowledge:** There exists a PPT algorithm $\mathcal{S}$ (the simulator) taking $c \in \mathcal{L}(\mathcal{R})$ and $d \in \mathcal{C}$ as inputs, that outputs triples (t, d, s) whose distribution is *computationally indistinguishable* from the accepting transcripts generated by real protocol runs.

2.4 SSE: Syntax and Security Model

In this section, we formally define Searchable Symmetric Encryption (SSE) for static databases.

Static SSE. A *Searchable Symmetric Encryption (SSE) scheme* Π for static databases consists of an algorithm $\mathsf{EDBSetup}$ and a protocol Search between the client and server, mentioned as follows:

- $\mathsf{EDBSetup}$ takes as input a database $\mathbf{DB}$, and outputs a secret key K along with an encrypted database $\mathbf{EDB}$.
- The Search protocol is between a *client* and *server*, where the client takes as input the secret key K and a query q and the server takes as input $\mathbf{EDB}$. At the end, the client outputs a set of identifiers, and the server has no output.

Correctness of SSE. An SSE scheme is *correct* if for all inputs $\mathbf{DB}$ and queries q, if $(K, \mathbf{EDB}) \xleftarrow{\$} \mathsf{EDBSetup}(\mathbf{DB})$, after running Search with client input (K, q) and server input $\mathbf{EDB}$, the client outputs the set of indices $\mathbf{DB}(q)$.

Adaptive Security of SSE. We recall the semantic security definitions of SSE from [CGKO06b]. The definition is parameterized by a *leakage function* $\mathcal{L}$, which describes what an adversary (the server) is allowed to learn about the database and queries. Formally, security says that the server's view during an adaptive attack (where the server selects the database and queries) can be simulated given only the output of $\mathcal{L}$.

Definition 1. *Let* $\Pi = (\mathit{EDBSetup}, \mathit{Search})$ *be an SSE scheme and let* $\mathcal{L}$ *be a stateful algorithm. For algorithms* $\mathcal{A}$ *(denoting the adversary) and* $\mathcal{S}$ *(denoting a simulator), we define the experiments (algorithms)* $\mathbf{Real}^{\Pi}_{\mathcal{A}}(\lambda)$ *and* $\mathbf{Ideal}^{\Pi}_{\mathcal{A},\mathcal{S}}(\lambda)$ *as follows:*

$\mathbf{Real}^{\Pi}_{\mathcal{A}}(\lambda)$ *:* $\mathcal{A}(1^{\lambda})$ *chooses* $\mathbf{DB}$*. The experiment then runs* $(K, \mathbf{EDB}) \leftarrow \mathit{EDBSetup}(\mathbf{DB})$*, and gives* $\mathbf{EDB}$ *to* $\mathcal{A}$*. Then* $\mathcal{A}$ *repeatedly chooses a query* q*. To respond, the game runs the* Search *protocol with client input* (K, q) *and server input* $\mathbf{EDB}$ *and gives the transcript and client output to* $\mathcal{A}$*. Eventually* $\mathcal{A}$ *returns a bit that the game uses as its own output.*

$\mathbf{Ideal}^{\Pi}_{\mathcal{A},\mathcal{S}}(\lambda)$ *: The game initializes a counter* $\mathsf{cnt} = 0$ *and an empty list* $\mathbf{q}$*.* $\mathcal{A}(1^{\lambda})$ *chooses* $\mathbf{DB}$*. The experiment runs* $\mathbf{EDB} \leftarrow \mathcal{S}(\mathcal{L}(\mathbf{DB}))$ *and gives* $\mathbf{EDB}$ *to* $\mathcal{A}$*. Then* $\mathcal{A}$ *repeatedly chooses a query* q*. To respond, the game records this as* $\mathbf{q}[i]$*, increments* i*, and gives to* $\mathcal{A}$ *the output of* $\mathcal{S}(\mathcal{L}(\mathbf{DB}, \mathbf{q}))$*. (Note that here,* $\mathbf{q}$ *consists of all previous queries in addition to the latest query issued by* $\mathcal{A}$*.) Eventually* $\mathcal{A}$ *returns a bit that the game uses as its own output.*

We say that Π *is* $\mathcal{L}$*-semantically-secure against adaptive attacks if for all adversaries* $\mathcal{A}$ *there exists an algorithm* $\mathcal{S}$ *such that*

$$| \Pr[\mathbf{Real}^{\Pi}_{\mathcal{A}}(\lambda) = 1] - \Pr[\mathbf{Ideal}^{\Pi}_{\mathcal{A},\mathcal{S}}(\lambda) = 1] | \leq \mathsf{negl}(\lambda)$$

2.5 Brief Overview of [BKLP14]

In [BKLP14], the authors introduced a lattice-based commitment scheme and associated zero-knowledge proofs of knowledge, with security based in the hardness of the Ring-Learning with Errors (RLWE) problem. The main goal of their work was to construct an efficient commitment scheme that supports compact commitments to vectors over $\mathbb{Z}_q$, where the size of the commitment increases only by a small constant factor relative to the original vector. The commitments are unconditionally binding and computationally hiding. In their design, [BKLP14] presented zero-knowledge proofs of knowledge that allow a prover to convince a verifier of the knowledge of the committed message, as well as to prove certain relations among multiple committed messages, such as linear and multiplicative relations. A notable aspect of their protocol design is achieving negligible knowledge error in a single iteration, without requiring multiple rounds of interaction. This was achieved by adopting a framework based on special soundness, where the prover commits with respect to one relation R and the verifier checks a statistically close relation R$'$. Special soundness allows the extraction of a witness (i.e., the committed message) from two accepting transcripts with different verifier challenges, resulting in strong soundness guarantees without requiring repeated protocol executions.

To ensure the simulator's ability to produce transcripts that are independent of the prover's secret (essential for zero-knowledge), [BKLP14] employs explicit error sampling and a rejection sampling mechanism. The rejection sampling technique introduces a rejection factor M, which directly impacts the computational complexity and proof size. Smaller rejection rates are achievable by carefully tuning system parameters, but they come at the cost of increased commitment sizes and computational overhead. Despite these optimizations, reliance on approximate error sampling and rejection sampling introduces non-negligible efficiency costs, both in terms of communication and computation. The protocols proposed in [BKLP14] achieve a communication complexity of $O(Mn \log q)$, where n is the ring dimension, q is the modulus, and M is the rejection sampling factor. In practice, this results in noticeable proof sizes and execution times, especially for applications targeting lightweight or resource-constrained environments. Furthermore, [BKLP14] resolved an open problem posed by prior work [JKPT12] by constructing a commitment and zero-knowledge proof system that simultaneously achieves strong hiding and binding properties, negligible knowledge error in one round, and reasonable practical efficiency — all based on standard lattice hardness assumptions (specifically, RLWE and problems on ideal lattices).

3 Technical Contribution

3.1 Establishing Properties on LWR samples

We state the *Learning With Rounding* problem in a polynomial ring setting as defined in [BPR12] as follows -

Definition 2 (Ring Learning With Rounding Problem)**.** *Let $n \geq 1$ be the main security parameter and moduli $q \geq p \geq 2$ be integers. Let R_q and R_p denote polynomial rings $\mathbb{Z}_q[x]/\langle \phi \rangle$*

and $\mathbb{Z}_p[x]/\langle\phi\rangle$ *respectively, for* $\langle\phi\rangle = x^n + 1$. *For a polynomial* $s \in R_q$, *the Ring-LWR distribution* $\mathcal{L}_{R,p,q}$ *is defined as the distribution over* $(R_q \times R_p)$ *obtained by choosing a polynomial* $a \xleftarrow{\$} R_q$ *uniformly at random and outputting* $(a, b = \lfloor\langle a, s\rangle\rceil_p)$.

For a given distribution over $s \in R_q$ and if $\frac{q}{p} \geq \sqrt{n}$ holds, the *decision*-$\mathsf{LWR}_{R,q,p}$ problem is to distinguish (with advantage non-negligible in n) between any desired number of independent samples $(a_i, b_i) \leftarrow \mathcal{L}_{R,p,q}$, and the same number of samples drawn uniformly and independently from $(R_q \times R_p)$.

Properties. We now establish the following properties on $\mathcal{L}_{R,p_1,q}$ and $\mathcal{L}_{R,p,p_1}$ that help us develop interesting use-cases in later sections. In all subsequent discussions, assume $\frac{q}{p_1} \geq \sqrt{n}$ and $\frac{p_1}{p} \geq \sqrt{n}$ to hold, thereby not compromising satisfying the hardness of the *decision*-$\mathsf{LWR}_{R,q,p}$ problem on $\mathcal{L}_{R,p_1,q}$ and $\mathcal{L}_{R,p,p_1}$.

Claim 1 (Addition Under Double-Rounding)**.** *Let* $a \xleftarrow{\$} R_q$ *be a public polynomial chosen uniformly at random and* $s, x \in R_q$ *are secrets, then the following equality*

$$\lfloor\lfloor a \cdot s\rceil_{p_1} + \lfloor a \cdot x\rceil_{p_1}\rceil_p = \lfloor a \cdot s + a \cdot x\rceil_p$$

holds with probability $\left(1 - \frac{1}{2^{log_2(p_1) - log_2(p)}}\right)^n$. *For* $q > p_1 >> p$ *and* $\frac{q}{p_1}, \frac{q}{p} \geq \sqrt{n}$, *this probability is overwhelmingly close to* 1.

Proof. We first consider an alternative equality.

$$\lfloor a \cdot s\rceil_p + \lfloor a \cdot x\rceil_p = \lfloor a \cdot s + a \cdot x\rceil_p$$

In this equality, notice that each coefficient of the polynomial products $a \cdot s$ and $a \cdot x$ is an element in $\mathbb{Z}_q$ before rounding. Therefore, on the RHS, *all* $log_2(q)$ bits of the products $a \cdot s$ and $a \cdot x$ participate in the addition, post which the sum is rounded to an element in $\mathbb{Z}_p$. On the LHS however, only the most significant $log_2(p)$ bits of $a \cdot s$ and $a \cdot x$ are added up. The LHS and RHS hence disagree iff the carry generated by addition of the least significant $log_2(q) - log_2(p)$ bits is propagated to the most-significant $log_2(p)$ bits, and is not subsumed by the final polynomial reduction wrt. $\langle\phi\rangle$. Hence, the probability of LHS and RHS agreeing (after summation) is: $\left(1 - \frac{1}{2^{log_2(q) - log_2(p)}}\right)$.

For this probability to be overwhelmingly close to 1, it is clear that $q >> p$. Also note that for each element $x \in \mathbb{Z}_p$ after creating the LWR sample, there are at most $\frac{q}{p}$ pre-images in $\mathbb{Z}_q$ which map to x. For the use-cases discussed in this work, such high number of pre-images implies high knowledge error, which is undesirable.

We thus introduce a third modulus: p_1. Instead of creating LWR samples in $\mathcal{L}_{R,p,q}$, we rather create LWR samples in $\mathcal{L}_{R,p_1,q}$ where p_1 is *close* to q (thereby restricting the knowledge error in our protocol, as Section 3.2 also shows) while still satisfying $\frac{q}{p_1} \geq \sqrt{n}$. The addition is then performed in $\mathcal{L}_{R,p,p_1}$ where $p_1 >> p$ as follows:

$$\lfloor \lfloor a \cdot s \rceil_{p_1} + \lfloor a \cdot x \rceil_{p_1} \rceil_p = \lfloor a \cdot s + a \cdot x \rceil_p$$

The probability that a *single* coefficient hence matches on LHS and RHS is then $\left(1 - \frac{1}{2^{log_2(p_1)-log_2(p)}}\right)$. Finally, since coefficient-wise addition is mutually independent, for n coefficients, the overall probability that LHS agrees with the RHS is $\left(1 - \frac{1}{2^{log_2(p_1)-log_2(p)}}\right)^n$.

□

Claim 2 (Multiplication With A "Small" Polynomial)**.** *Let $a \xleftarrow{\$} R_q$ be a public polynomial chosen uniformly at random and let $s \in R_q$ be a secret. Let D be a family of all polynomials of degree $\leq \frac{n}{2}$ and $\| d \|_\infty \leq 1$. Then for any $d \xleftarrow{\$} D$, the following equality:*

$$\lfloor d \cdot \lfloor a \cdot s \rceil_{p_1} \rceil_p = \lfloor d \cdot a \cdot s \rceil_p$$

holds with probability $\left(1 - \frac{\|d\|_1}{2^{log_2(p_1)-log_2(p)}}\right)^n$ where $\| \, . \, \|_1$ represents l_1 norm. In the worst case, with probability $\frac{1}{3^{n/2}}$, we can derive the following lower-bound:

$$\left(1 - \frac{\| d \|_1}{2^{log_2(p_1)-log_2(p)}}\right)^n \geq \left(1 - \frac{\binom{n}{2}}{2^{log_2(p_1)-log_2(p)}}\right)^n$$

where the lower-bound is overwhelmingly close to 1 for $q > p_1 >> p$ and $\frac{q}{p_1} \geq \sqrt{n}$.

Proof. As with Claim 1, the rationale for creating the LWR sample in $\mathcal{L}_{R,p_1,q}$ and performing the polynomial multiplication in $\mathcal{L}_{R,p,p_1}$ remains related to achieving negligible knowledge error for our protocol (see Section 3.2).

From the proof of Claim 1, it follows that the probability of a *single* coefficient on LHS and RHS to agree upon a *single* addition is $\left(1 - \frac{1}{2^{log_2(p_1)-log_2(p)}}\right)$. Observe that by structure of D, the product $d \cdot \lfloor a \cdot s \rceil_{p_1}$ can be viewed as additions of $\lfloor a \cdot s \rceil_{p_1}$ repeated $\| d \|_1$ times (i.e. by the number of non-zero elements in d). Hence, the probability of a *single* coefficient agreeing on the LHS and RHS then is $\left(1 - \frac{\|d\|_1}{2^{log_2(p_1)-log_2(p)}}\right)$. Note that each coefficient in the resultant product polynomial $d \cdot \lfloor a \cdot s \rceil_{p_1}$ is computed independently in the polynomial multiplication; thereby for n coefficients in the resultant polynomial, the overall probability that LHS agrees with the RHS is $\left(1 - \frac{\|d\|_1}{2^{log_2(p_1)-log_2(p)}}\right)^n$.

Assuming uniform at random sampling $d \xleftarrow{\$} D$, the worst-case[6] $\| d \|_1$ occurs with probability $\frac{1}{|D|} = \frac{1}{3^{n/2}}$ where $|\cdot|$ represents set cardinality. This happens when *all* $\frac{n}{2}$ coefficients of d are non-zero, contributing to worst-case $\frac{n}{2}$ additions. We thus have the following lower-bound:

[6] In practice however, $\| d \|_1$ is reasonably bounded; see [BKLP14, BDL+18].

$$\left(1 - \frac{\| d \|_1}{2^{log_2(p_1)-log_2(p)}}\right)^n \geq \left(1 - \frac{\left(\frac{n}{2}\right)}{2^{log_2(p_1)-log_2(p)}}\right)^n$$

□

Claim 3 (Addition With Product of a "Small" Polynomial)**.** *Let $a \xleftarrow{\$} R_q$ be a public polynomial chosen uniformly at random and let $s, x \in R_q$ be a secret. Let D be a family of all polynomials of degree $\leq \frac{n}{2}$ and $\| d \|_\infty \leq 1$. Then for any $d \xleftarrow{\$} D$, the following equality:*

$$\lfloor \lfloor a \cdot s \rceil_{p_1} + d \cdot \lfloor a \cdot x \rceil_{p_1} \rceil_p = \lfloor a \cdot s + d \cdot a \cdot x \rceil_p$$

holds with probability $\left(1 - \frac{1+\|d\|_1}{2^{log_2(p_1)-log_2(p)}}\right)^n$ where $\| \, . \, \|_1$ represents l_1 norm. In the worst case, with probability $\frac{1}{3^{n/2}}$, we can derive the following lower bound:

$$\left(1 - \frac{1+ \| d \|_1}{2^{log_2(p_1)-log_2(p)}}\right)^n \geq \left(1 - \frac{1 + \left(\frac{n}{2}\right)}{2^{log_2(p_1)-log_2(p)}}\right)^n$$

where the lower-bound is overwhelmingly close to 1 for $q > p_1 >> p$ and $\frac{q}{p_1} \geq \sqrt{n}$ and $n >> 1$.

Proof. The bounds follow directly from Claim 2, except that in this case, *one* extra addition per coefficient is performed. Also note that since d is of degree $O(n)$ and $n >> 1$, $(1+ \| d \|_1), \approx \| d \|$, and thus the lower-bound follows. Finally, note that the claim holds with overwhelming probability for $q > p_1 >> p$ and $n >> 1$. □

3.2 Ring-LWR (RLWR) Commitment Scheme

In this section, we describe our RLWR commitment scheme. Table 1 describes the parameters that are used.

- `KeyGen:` The public commitment key $pk = \mathbf{a}$, sampled randomly as $\mathbf{a} \xleftarrow{\$} (\mathbb{Z}_q[x]/\langle x^n + 1 \rangle)^k$, where q is prime, and n is a power of 2.

- `Com:` To commit to a message m from a message space $\{0,1\}^l$ where $l > n$, `Com` first hashes m to a point in the ring as $\mathtt{H}(m \parallel r)$, where $r \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n+1 \rangle$ represents private randomness. The commitment is then computed as :

$$\mathbf{c} = \lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1}$$

and the opening information for $\mathbf{c}$ is given by $(m, r, 1)$.

- `Ver:` Given a commitment $\mathbf{c}$, a message m', a randomness r' and a *small* polynomial d , the verifier accepts iff,

$$d \cdot \lfloor \mathbf{a} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1} = \mathbf{c} \ \wedge \ q > p_1 \ \wedge \ \frac{q}{p_1} \geq \sqrt{n}$$

$$\wedge \ d \neq 0 \wedge \parallel d \parallel_\infty \leq 1 \ \wedge \ \mathtt{deg}(d) < \frac{n}{2}$$

The above scheme is inspired by RLWE based commitment scheme introduced by Benhamouda et.al, in [BKLP14]. Similar to their commitment scheme, we support an additional small polynomial d in a valid opening[7]. This forms the basis for proving the soundness of our protocol (which in turn allows for verifiability of the SSE scheme), as we discuss subsequently in Section 4.2. An honest prover can set $d = 1$ while opening $\mathbf{c}$ thereby preserving the *completeness* property. We now show how our commitment scheme is computationally hiding and statistically binding. We give a formal security proof in the following.

Theorem 1. *Let q and p_1 be moduli of rings R_q and R_{p_1}, $\mathcal{L}_{R,p_1,q}$ be the RLWR relation as defined by Definition 2, and $H : \{0,1\}^l \rightarrow R_q$ be a collision resistant hash function [PFH+17]. Also let the following inequalities hold:*

$$q > p_1 \quad \wedge \quad \frac{q}{p_1} \geq \sqrt{n} \quad \wedge \quad k > \frac{log_2(3) + 2 \cdot log_2(q)}{log_2(q) - log_2(p_1)}$$

Then, under the RLWR assumption, the triple of algorithms (`KeyGen, Com, Ver`) is a succinct, computationally hiding, and statistically binding commitment scheme with overwhelming probability over the choices of the public commitment key.

Proof. Our commitment scheme satisfies the following properties as proved below -

Succinctness: The commitments are succinct since H is used to hash an l-bit string to a point in R_q, allowing for message spaces with arbitrary $l > n$.

Correctness: For honest committer and prover, correctness holds by the validity of the opening $(m, r, 1)$.

Computational Hiding: By the RLWR assumption, $\lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1}$ is indistinguishable from a uniform element in $\mathbb{Z}_{p_1}[x]/\langle x^n + 1 \rangle$ by a PPT adversary. By extension, $\mathbf{c}$ is also computationally indistinguishable from uniformly at random sampled polynomials in $\mathbb{Z}_{p_1}[x]/\langle x^n + 1 \rangle$.

Statistical Binding: For the commitment scheme to be perfectly binding, we need to show the following:

[7]We thank Olejnik and Naskrecki [ON26] for their cryptanalysis effort in an earlier version of our commitment scheme, where $d = 0$ was not explicitly excluded from the verification predicate. We resolve this by requiring $d \neq 0$, ensuring invertibility of challenge differences during extraction. Nevertheless this modification does not affect honest execution, protocol efficiency, or the security guarantees of the construction.

$$\mathbf{c} = d\lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1} = d^{'} \lfloor \mathbf{a} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1}$$

$$\implies \quad m = m'$$

with overwhelming probability over the choices of $\mathbf{a}$. Assume by contradiction that $\mathbf{c} = d\lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1} = d^{'} \lfloor \mathbf{a} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1}$ holds for some $m \neq m'$. This implies the PPT adversary is successful in finding two valid openings (m, r, d) and $(m^{'}, r^{'}, d^{'})$ that generate the same commitment $\mathbf{c}$. The adversary can *win* thus in one of the two cases:

① *Hash Collision*: The first case where the PPT adversary wins is when $\mathtt{H}(m \parallel r) = \mathtt{H}(m' \parallel r')$ for $m \neq m'$. This is however equivalent to finding collisions in $H : \{0,1\}^{l} \rightarrow \mathbb{Z}_q / \langle x^n + 1 \rangle$, the probability of which is negligible in n over the choices of $\mathbf{a}$ (refer [PFH+17] for details).

② *Collisions in Rounding*: The second case where the PPT adversary wins is when $\mathbf{a} \cdot \mathtt{H}(m \parallel r) \neq \mathbf{a} \cdot \mathtt{H}(m' \parallel r')$ but $d\lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1} = d^{'} \lfloor \mathbf{a} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1}$. It is thus sufficient to show the probability of this event happening is negligible in n over choices of $\mathbf{a}$.

Rounding to most significant p_1 bits implies mapping a polynomial in $\mathbb{Z}_q[x]/\langle x^n + 1 \rangle$ to a polynomial in $\mathbb{Z}_{p_1}[x]/\langle x^n + 1 \rangle$ where $q > p_1$. For *each* coefficient of the polynomial in $\mathbb{Z}_q[x]/\langle x^n + 1 \rangle$, rounding is then essentially dividing the q elements in $\mathbb{Z}_q$ to $\mathbb{Z}_{p_1}$ buckets each of size $\frac{q}{p_1}$ [BPR12]. Put simply, given a scalar σ in $\mathbb{Z}_{p_1}$, the probability of another scalar in $\mathbb{Z}_q$ sampled uniformly at random mapping to $\lfloor \sigma \rceil_{p_1}$ is $\frac{1}{q/p_1}$. For fixed $d, H(m \parallel r)$, and $H(m^{'} \parallel r^{'})$, the probability that $d\lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1}$ equals $d^{'} \lfloor \mathbf{a} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1}$ through collisions in rounding is then equivalent to probability that *all* coefficients of the resultant polynomials face collisions in rounding:

$$\Pr\left[\begin{pmatrix} d\lfloor \mathbf{a_1} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1} \\ \vdots \\ d\lfloor \mathbf{a_k} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1} \end{pmatrix} = \begin{pmatrix} d'\lfloor \mathbf{a_1} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1} \\ \vdots \\ d'\lfloor \mathbf{a_k} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1} \end{pmatrix} : \mathbf{a} \xleftarrow{\$} R_q^k \right] \leq \frac{1}{\left(\frac{q}{p_1}\right)^{n \cdot k}}$$

where, R_q^k represents the polynomial ring $\mathbb{Z}_q[x]/\langle x^n + 1 \rangle$. Now taking a union bound over all $d, d^{'}, H(m \parallel r)$ and $H(m^{'} \parallel r^{'})$, the overall probability that $d\lfloor \mathbf{a} \cdot \mathtt{H}(m \parallel r) \rceil_{p_1} = d^{'} \lfloor \mathbf{a} \cdot \mathtt{H}(m' \parallel r') \rceil_{p_1}$ (without collisions in H) is then:

$$\leq \frac{q^{2n} \cdot 3^{\frac{2n}{2}}}{\left(\frac{q}{p_1}\right)^{n \cdot k}} \equiv \left[\frac{q^2 \cdot 3}{\left(\frac{q}{p_1}\right)^{k}} \right]^{n} \equiv 3^n \cdot q^{(2-k) \cdot n} \cdot p_1^{k \cdot n}$$

which is negligible in n if the bounds in Theorem 1 hold. □

Improvement. In comparison to the commitment scheme of Benhamouda et al. [BKLP14], we improve in the following ways - (i) Since there is no requirement of error sampling, we eliminate probability of error term from the inequality and choose tighter parameter ($q \geq n^6$ does not affect the bound); (ii) the knowledge error is thus reduced from $\binom{n/2}{\kappa}$ to $3^{n/2}$; (iii) since we bypass rejection sampling, there is no requirement of abort checks thereby making the scheme simpler, efficient and reducing the computation complexity from $O(M \cdot n \cdot log\ q)$ to $O(n \cdot log\ q)$ where, $M = e^{12/\alpha+1/(2\alpha^2)}$ is the constant from rejection sampling.

Security-level. The security of our proposed commitment scheme relies on the hardness guarantees of the Ring-Learning With Rounding (RLWR) problem. The choice of parameters for our proposed framework is motivated by [BPR12] that states as long as $q/p \geq \sqrt{n}$ is an integer, the LWR (equivalently RLWR) problem appears to be exponentially hard (in n) for any $p = poly(n)$, and super-polynomially hard for $p \leq 2^{n^\epsilon}$ for any $\epsilon < 1$. Concretely, we choose $n = 512, q = 2^{45}, p = 2^5$ for our implementations. With this set of parameters, we verified the bit-level security of our proposed scheme using the LWE Estimator [MRAS15]. The results show that our scheme provides 188-bit level of security, which essentially satisfies the NIST Benchmark [8].

3.3 Σ_2 Protocol For Pre-image Proof

In this section we present a protocol for proving knowledge of valid openings of commitments as defined in the previous subsection. We then use these pre-image proofs in the construction of verifiable SSE using a protocol that allows one to prove that the messages m_1, m_2, m_3 contained in commitments $\mathbf{c_1}, \mathbf{c_2}, \mathbf{c_3}$ satisfy a linear relation of form $m_3 = x_1 \cdot m_1 + x_2 \cdot m_2$ for some $x_1, x_2 \in R_q$.

In this section, we let $\Pi = (\mathtt{KeyGen}, \mathtt{Com}, \mathtt{Ver})$ to represent the commitment scheme described in the previous subsection. We write $(\mathbf{c}_{\text{aux}}, d_{\text{aux}}) = \mathtt{Com}(m)$, where $\mathbf{c}_{\text{aux}}$ is the commitment and d_{aux} is the opening of $\mathbf{c}_{\text{aux}}$.

Theorem 2. *If* $\Pi = \{\mathtt{KeyGen}, \mathtt{Com}, \mathtt{Ver}\}$ *is a statistically binding commitment scheme as defined in Section 3.2, then Protocol. 1 is an honest-verifier zero-knowledge proof of knowledge for the following relations with a knowledge error* $\frac{1}{3^{n/2}}$ *(assume* $\mathbf{x} = \mathtt{H}(m \parallel r)$ *henceforth):*

$$\mathcal{R}_{LWR} = \left\{ \Big((\mathbf{a}, \mathbf{c}), x \Big) : \lfloor \mathbf{c} \rceil_p = \lfloor \lfloor \mathbf{a} \cdot x \rceil_{p_1} \rceil_p \ \wedge \ (q > p_1 >> p) \ \wedge \ \frac{q}{p_1} \geq \sqrt{n} \right\}$$

and

$$\mathcal{R}'_{LWR} = \left\{ \Big((\mathbf{a}, \mathbf{c}), (x, d) \Big) : \lfloor \mathbf{c} \rceil_p = \lfloor d \cdot \lfloor \mathbf{a} \cdot x \rceil_{p_1} \rceil_p \ \wedge \ (q > p_1 >> p) \right.$$
$$\left. \frac{q}{p_1} \geq \sqrt{n} \ \wedge \ d \neq 0 \ \wedge \ \parallel d \parallel_\infty \leq 1 \ \wedge \ \deg(d) < \frac{n}{2} \right\}$$

[8] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

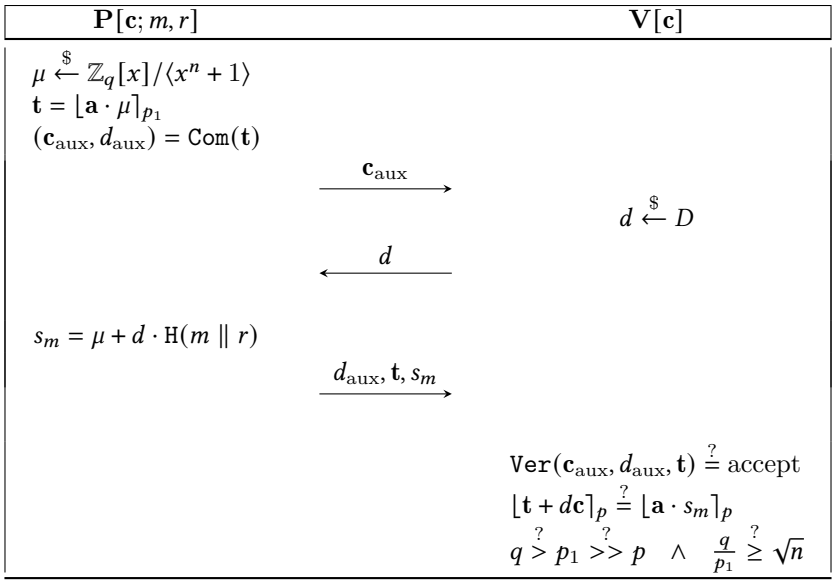

Figure 1: Zero-knowledge proof of pre-image. $\mathbf{V}$ accepts iff all conditions related to $^?$ are satisfied.

Where the prover $\boldsymbol{P}$ proves in the relation $\mathcal{R}_{LWR}$ while the verifier $\boldsymbol{V}$ accepts in the relation $\mathcal{R}'_{LWR}$.

Proof. We prove Theorem 2 by showing it is a Σ_2-protocol for the given relation. The claim then follows directly from the properties that ensure the protocol is accepting. We next prove the properties.

Completeness: An honest prover always responds to the challenge d. We then have:

$$\begin{aligned}
\lfloor \mathbf{t} + d \cdot \mathbf{c} \rceil_p &= \lfloor \lfloor \mathbf{a} \cdot \mu \rceil_{p_1} + d \cdot \lfloor \mathbf{a} \cdot \texttt{H}(m \parallel r) \rceil_{p_1} \rceil_p \\
&= \lfloor \mathbf{a} \cdot \mu + d \cdot \mathbf{a} \cdot \texttt{H}(m \parallel r)) \rceil_p \qquad \text{[By Claim 3]} \\
&= \lfloor \mathbf{a}(\mu + d \cdot \texttt{H}(m \parallel r)) \rceil_p \\
&= \lfloor \mathbf{a} \cdot s_m \rceil_p
\end{aligned}$$

Special Soundness: Let there be two accepting protocol transcripts $(\mathbf{c}'_{\text{aux}}, d', (d'_{\text{aux}}, \mathbf{t}', s'_m))$ and $(\mathbf{c}''_{\text{aux}}, d'', (d''_{\text{aux}}, \mathbf{t}'', s''_m))$ where $d' \neq d''$. By perfect binding property of $\texttt{Com}$ (refer Section 3.2), we get that $t' = t'' = t$. Following the protocol in Protocol 1, we have the following verification equations:

$$\begin{aligned}
\lfloor \mathbf{t}' + d'\mathbf{c} \rceil_p &= \lfloor \mathbf{a} \cdot s'_m \rceil_p \\
\lfloor \mathbf{t}'' + d''\mathbf{c} \rceil_p &= \lfloor \mathbf{a} \cdot s''_m \rceil_p
\end{aligned}$$

By subtracting the verification equations and then applying the rounding, we then obtain -

$$\begin{aligned}\mathbf{t}' + d'\mathbf{c} - \mathbf{t}'' - d''\mathbf{c} &\neq \mathbf{a} \cdot s'_m - \mathbf{a} \cdot s''_m \\ \Delta_d \cdot \mathbf{c} &\neq \mathbf{a} \cdot (s'_m - s''_m) \\ \Delta_d \cdot \mathbf{c} &\neq \mathbf{a} \cdot \Delta_m\end{aligned}$$

where we set $\Delta_d = d' - d''$ and $\Delta_m = s'_m - s''_m$. As $\mathtt{deg}(\Delta_d) < n/2$, we have Δ_d is invertible in R_q. We get the witness $\mathbf{w} = (\Delta_m, \Delta_d^{-1})$, where $\| \Delta_d \|_\infty \leq 1$. We show that $\mathbf{w}$ is a correct witness as -

$$\begin{aligned}\mathbf{c} &\neq \Delta_d^{-1} \cdot \mathbf{a} \cdot \Delta_m \\ \mathbf{c} &= \lfloor \Delta_d^{-1} \cdot \mathbf{a} \cdot \Delta_m \rceil_{p_1} \text{ [Note: } \mathbf{c} \text{ is already in } R_{p_1}] \\ \lfloor \mathbf{c} \rceil_p &= \lfloor \lfloor \Delta_d^{-1} \cdot \mathbf{a} \cdot \Delta_m \rceil_{p_1} \rceil_p \\ \lfloor \mathbf{c} \rceil_p &= \lfloor \Delta_d^{-1} \cdot \lfloor \mathbf{a} \cdot \Delta_m \rceil_{p_1} \rceil_p \text{ [By Claim 2]}\end{aligned}$$

Honest-verifier Zero-knowledge: Taking a challenge d as an input, the simulator first draws uniformly random element $s_m \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$. Simulator computes $\mathbf{t_S} = \mathbf{a} \cdot s_m - d \cdot \mathbf{c}$ and then outputs $(c'_{\text{aux}}, d, (d'_{\text{aux}}, \mathbf{t}', s'_m))$. By the hardness of RLWR assumption [BPR12], $\mathbf{t}'_{\mathbf{S}}$ (computed from a uniformly at random sampled s_m) is computationally indistinguishable from the real execution of Protocol 1 (where s_m depends upon the message m), thereby establishing honest-verifier zero-knowledge.

□

3.4 Σ_2 Protocol For Proving Linear Relations

In this section, we design a protocol to prove knowledge of messages $\{m_1, m_2, m_3\}$ contained in $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$ respectively, where the m_i additionally satisfy a linear relation of the form $m_3 = x_1 m_1 + x_2 m_2$ for arbitrary public $x_i \in \mathbb{Z}_q[x]/\langle x^n + 1\rangle$. Note that if $\{m_1, m_2, m_3\} \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, *the protocol does not require additional hashing* to map $\{m_1, m_2, m_3\}$ to the ring. If $\{m_1, m_2, m_3\} \in \{0,1\}^*$, an additional hashing is required to map the messages to the ring; to preserve linearity however, this hash function must be homomorphic[9] to preserve the linearity $m_3 = x_1 \cdot m_1 + x_2 \cdot m_2$ over the hashing. In this section, we give the instantiation of our Σ_2 protocol assuming $\{m_1, m_2, m_3\} \in \{0,1\}^*$ for completeness. Our usage of this Σ_2 protocol in Section 4 however is on $\{m_1, m_2, m_3\} \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n+1\rangle$ and thereby avoids hashing overheads in practice.

In our Σ_2 protocol, three instances of Protocol 1 are run in parallel for $\{m_1, m_2, m_3\}$ using the same challenge, but instead of choosing the randomness μ_3 for m_3 in the prover's first step at random, it is computed such that μ_1, μ_2, μ_3 satisfy the claimed linear relation.

[9]Lattice based homomorphic hashes are derived through homomorphic signature schemes like [BF11].

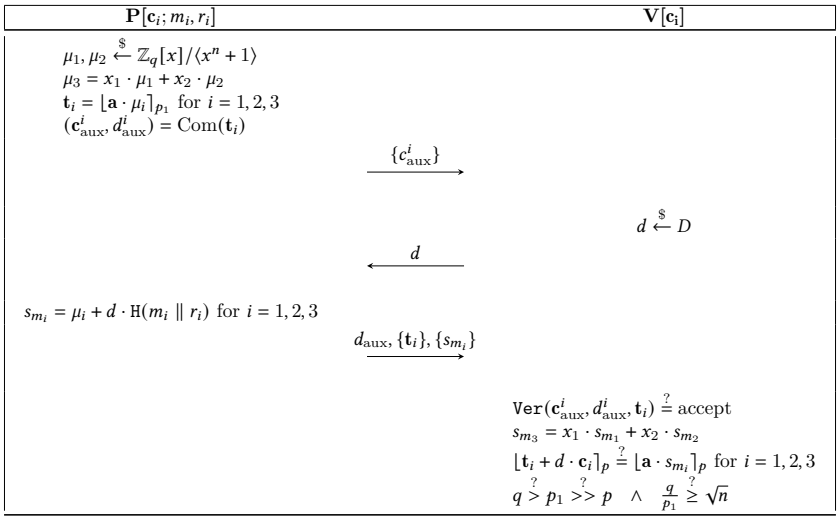

Figure 2: Proving Linear Relations. $\mathbf{V}$ accepts iff all conditions related to $^?$ are satisfied.

Theorem 3. *If* $\Pi = \{\texttt{KeyGen}, \texttt{Com}, \texttt{Ver}\}$ *is a statistically binding commitment scheme as defined in Section 3.2, then Protocol 2 is an honest-verifier zero-knowledge proof for the following relations (with a knowledge error* $\frac{2}{3^{n/2}}$*):*

$$\mathcal{R}_{Lin-LWR} = \Bigg\{\Big((\mathbf{a}, x_1, x_2, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3), (\{\text{H}(m_i \parallel r_i)\})\Big) :$$

$$\bigwedge_{i=1}^{3} \lfloor \mathbf{c_i} \rceil_p = \lfloor \lfloor \mathbf{a} \cdot \text{H}(m_i \parallel r_i) \rceil_{p_1} \rceil_p$$

$$\wedge\ (q > p_1 >> p)\ \wedge\ \frac{q}{p_1} \geq \sqrt{n}$$

$$\wedge\ H(m_3 \parallel r_3) = x_1 \cdot H(m_1 \parallel r_1) + x_2 \cdot H(m_2 \parallel r_2)\Bigg\}$$

and

$$\mathcal{R}'_{Lin-LWR} = \Bigg\{\Big((\mathbf{a}, x_1, x_2, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3), (\{\text{H}(m_i \parallel r_i)\}, \{d_i\})\Big) :$$

$$\bigwedge_{i=1}^{3} \lfloor \mathbf{c_i} \rceil_p = \lfloor d_i \cdot \lfloor \mathbf{a} \cdot \text{H}(m_i \parallel r_i) \rceil_{p_1} \rceil_p$$

$$\wedge\ (q > p_1 >> p)\ \wedge\ \frac{q}{p_1} \geq \sqrt{n}$$

$$\wedge\ H(m_3 \parallel r_3) = x_1 \cdot H(m_1 \parallel r_1) + x_2 \cdot H(m_2 \parallel r_2)\Bigg\}$$

Where the prover $\boldsymbol{P}$ *proves in the relation* $\mathcal{R}_{Lin-LWR}$ *while the verifier* $\boldsymbol{V}$ *accepts in the relation* $\mathcal{R}'_{Lin-LWR}$*.*

Proof. The theorem is proved by showing that the protocol is a Σ_2-protocol for the given relation. The claim then follows directly by showing that the following properties hold -

Completeness: This follows directly from the completeness of Protocol 1 and the following equality:

$$\begin{aligned}
s_{m_3} &= x_1 \cdot s_{m_1} + x_2 \cdot s_{m_2} \\
\mu_3 + d \cdot \mathtt{H}(m_3 \parallel r_3) &= x_1(\mu_1 + d \cdot \mathtt{H}(m_1 \parallel r_1)) + x_2(\mu_2 + d \cdot \mathtt{H}(m_2 \parallel r_2)) \\
\mu_3 + d \cdot \mathtt{H}(m_3 \parallel r_3) &= x_1\mu_1 + x_1 d \cdot \mathtt{H}(m_1 \parallel r_1) + x_2\mu_2 + x_2 d \cdot \mathtt{H}(m_2 \parallel r_2) \\
\mu_3 + d \cdot \mathtt{H}(m_3 \parallel r_3) &= x_1\mu_1 + x_2\mu_2 + x_1 d \cdot \mathtt{H}(m_1 \parallel r_1) + x_2 d \cdot \mathtt{H}(m_2 \parallel r_2) \\
\mu_3 + d \cdot \mathtt{H}(m_3 \parallel r_3) &= \mu_3 + x_1 d \cdot \mathtt{H}(m_1 \parallel r_1) + x_2 d \cdot \mathtt{H}(m_2 \parallel r_2) \\
d \cdot \mathtt{H}(m_3 \parallel r_3) &= x_1 d \cdot \mathtt{H}(m_1 \parallel r_1) + x_2 d \cdot \mathtt{H}(m_2 \parallel r_2) \\
\mathtt{H}(m_3 \parallel r_3) &= x_1 \mathtt{H}(m_1 \parallel r_1) + x_2 \mathtt{H}(m_2 \parallel r_2)
\end{aligned}$$

Special Soundness. Given two accepting transcripts, we can extract witnesses (Δ_{m_i}) for $\mathbf{c}_i$ $(i = 1, 2, 3)$ analogously to Theorem 2. We show the linear relation $\Delta_{m_3} = x_1 \cdot \Delta_{m_1} + x_2 \cdot \Delta_{m_2}$ is satisfied as follows:

$$\begin{aligned}
\Delta_{m_3} &= s'_{m_3} - s''_{m_3} \\
&= (x_1 s'_{m_1} + x_2 s'_{m_2}) - (x_1 s''_{m_1} + x_2 s''_{m_2}) \\
&= x_1(s'_{m_1} - s''_{m_1}) + x_2(s'_{m_2} - s''_{m_2}) \\
&= x_1 \Delta_{m_1} + x_2 \Delta_{m_2}
\end{aligned}$$

Special honest-verifier Zero-knowledge. The simulator essentially is given three independent instances of transcripts similar to that of Protocol 1 except that $s'_{m_3} = (x_1 s'_{m_1} + x_2 s'_{m_2})$. The correctness of this simulation is shown by a standard argument, as shown in [BKLP14]. □

4 Verifiable Quantum-safe SSE from RLWR Commitments

In this section we prove the correctness of a quantum-safe SSE [TPM23] using the protocol described in Section 3.4. We initiate by giving a brief overview of the SSE scheme OQXT proposed in [TPM23].

4.1 OQXT Overview

OQXT [TPM23] is a lattice-based quantum-safe conjunctive SSE scheme, that elevates the classically secure conjunctive SSE, OXT [CJJ+13b] to a post-quantum secure paradigm by

relying on hard lattices over which the *Learning with Rounding* (LWR) assumption holds (replacing OXT's reliance on a discrete-log hard group, the public-key component that is quantum unsafe). The premise of OQXT can be connected to the GPV hash-and-sign lattice-based signature scheme that essentially relies on the SIS problem to derive its security guarantees.

LWR based Cross-Tags. OQXT entails a cross-tag generation protocol with provable security guarantees derived from post-quantum secure hardness assumptions of the LWR problem. The cross-tags (**xtag**) are LWR samples generated from a public matrix $\mathbf{xw} \in \mathbb{Z}_q^{n\times n}$ and a secret $\mathbf{xid} \in \mathbb{Z}_q^{n\times n}$, which are outputs of a pseudorandom function. In particular, for some $p < q$, the elements of $\mathbb{Z}_q$ are divided into p contiguous intervals of roughly q/p elements each. Both q and p are considered as powers of 2, therefore, this results **xtag** to be the $log(p)$ most significant bits of $[\mathbf{xid} \cdot \mathbf{xw}]$.

$$\mathbf{xtag} = \lfloor \mathbf{xid} \cdot \mathbf{xw} \rceil_p$$

The **xtag** constitutes of two components - the public matrix **xw**, an element in $\mathbb{Z}_q^{n\times n}$ which is calculated for every keyword w. The LWR secret **xid**, which corresponds to all the documents in which w occurs.

Lattice Trapdoors For Oblivious Computations. The correlation of OQXT with the theoretical framework of GPV [GPV08] that derives its security guarantees from the hardness of SIS problem is motivated here. Essentially, the crux of GPV signature scheme is that given the hash of a message, $\mathtt{H}(\mathsf{m})$ and a public matrix $\mathbf{A}$, the signature of m is a *short* vector σ such that $\sigma\mathbf{A}^{\mathbf{t}} = \mathtt{H}(\mathsf{m})$; since σ is short, by the hardness of the SIS problem, it is difficult to find σ given the public matrix and the message without any information about the secret key (trapdoor).

To delegate the oblivious computation of cross-tags to the server during any conjunctive search in a post-quantum secure framework the client performs some pre-computations during Setup phase of OQXT. It incorporates the SampleD function from [MP12] to sample a (*short*) pre-image from a given coset of a discrete Gaussian distribution. A short $\mathbf{y}_{\mathsf{id}}$ is appropriately generated from a (nearly spherical) *discrete Gaussian* distribution $\mathbb{D}_{\Lambda^{\perp}_{\mathbf{xid}}(\mathbf{z}_{\mathbf{w}}),s}$ to ensure that the output *syndrome* (**xid**) is uniformly random i.e., for any random $\mathbf{y}_{\mathsf{id}}$, the product $\mathbf{y}_{\mathsf{id}} \cdot \mathbf{z}_{\mathbf{w}}^{\mathbf{t}}$ should be uniformly random. The hardness assumption here is given $\mathbf{z}_{\mathbf{w}}$ (a public matrix) and the coset $\mathbf{xid} \in \mathbb{Z}_q^{n\times n}$, it is hard to sample a *short* $\mathbf{y}_{\mathsf{id}} \in \mathbb{Z}_q^{n\times m}$ from $\Lambda^{\perp}_{\mathbf{xid}}(\mathbf{z}_{\mathbf{w}})$ (without any information about the secret trapdoor $\mathbf{T}$) by the hardness of *Short Integer Solution* (SIS) problem.

4.2 Verifiable-OQXT

In order to design a verifiable construction of OQXT we need to prove the following linear relation for the SSE scheme: $\mathbf{xtag} = \mathbf{y}_{\mathsf{id}} \cdot \mathbf{xtoken}$[10]. This linear relation can be analogously mapped to the linear relation proved in Section 3.4, i.e. $m_3 = x_1 m_1 + x_2 m_2$. In this application

[10]In original OQXT, the equality is checked for rounded values i.e. $\mathbf{xtag} = \lfloor \mathbf{y}_{\mathsf{id}} \cdot \mathbf{xtoken} \rceil_p$. We make a slight notational abuse here for sake of clarity; however, the correctness of the scheme is still proved under the rounding assumption.

we consider $m_3 = \mathbf{xtag},\ x_1 = \mathbf{y}_{\mathsf{id}},\ m_1 = \mathbf{xtoken},\ x_2 = 0,\ m_2 = 0$. Under this assumption, we design a verifiable quantum-safe SSE protocol.

Remark 1. We do not need a NIZK because our application (SSE) is already interactive client-server protocol. By choosing to develop an interactive protocol, we end up with an efficient SSE.

Remark 2. An astute reader may wonder about the analogy between $\mathbf{xtag} = \mathbf{y}_{\mathsf{id}} \cdot \mathbf{xtoken}$ *(where* $\mathbf{xtag}$, $\mathbf{xtoken}$ *and* $\mathbf{y}_{\mathsf{id}}$ *are integer matrices) and* $m_3 = x_1 m_1 + x_2 m_2$ *(where* $m_1, m_2, m_3 \in \mathbb{Z}_q[x]/\langle x^n + 1\rangle$*). We remark that such an analogy follows by hashing* $\mathbf{xtag}$, $\mathbf{xtoken}$ *and* $\mathbf{y}_{\mathsf{id}}$ *to a point in the ring* $\mathbb{Z}_q[x]/\langle x^n + 1\rangle$ *prior to executing the protocol in Figure 3. We abstract out these low-level details for simplicity of exposition.*

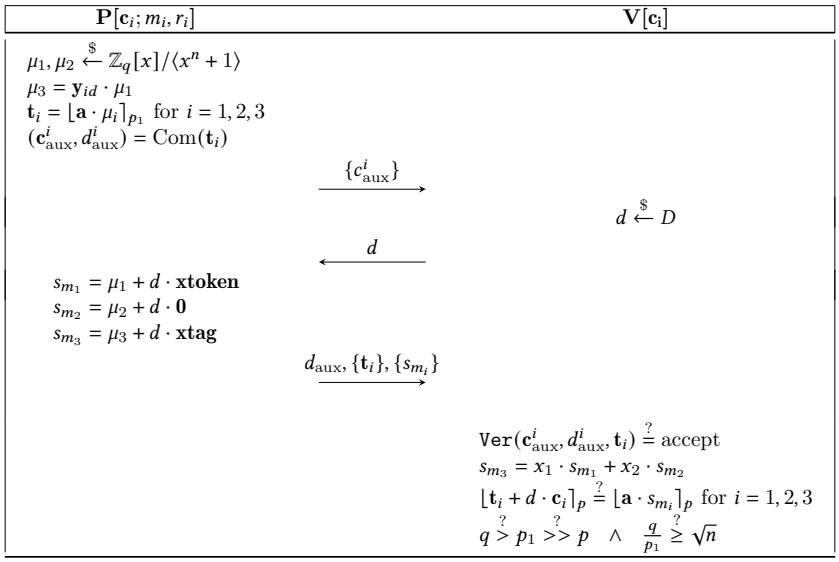

Figure 3: Protocol for Quantum-safe verifiable SSE. $\mathbf{V}$ accepts iff all conditions related to $^?$ are satisfied.

Theorem 4. *If* $\Pi = \{\mathtt{KeyGen}, \mathtt{Com}, \mathtt{Ver}\}$ *is a statistically binding commitment scheme as defined in Section 3.2, then Protocol 3 is an honest-verifier zero-knowledge proof for the following relations (with a knowledge error* $\frac{2}{3^{n/2}}$*):*

$$\mathcal{R}_{vSSE-LWR} = \Big\{\Big((\mathbf{a}, \mathbf{xtoken}, \mathbf{0}, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3), (\mathbf{yid}, \mathbf{0}, \mathbf{xtag})\Big) :$$
$$\lfloor \mathbf{c}_1 \rceil_p = \lfloor \lfloor \mathbf{a} \cdot \mathbf{yid} \rceil_{p_1} \rceil_p \ \wedge\ \lfloor \mathbf{c}_2 \rceil_p = \lfloor \lfloor \mathbf{a} \cdot \mathbf{0} \rceil_{p_1} \rceil_p$$
$$\wedge\ \lfloor \mathbf{c}_3 \rceil_p = \lfloor \lfloor \mathbf{a} \cdot \mathbf{xtag} \rceil_{p_1} \rceil_p$$
$$\wedge\ (q > p_1 >> p) \ \wedge\ \frac{q}{p_1} \geq \sqrt{n} \ \wedge$$
$$\mathbf{yid} \cdot \mathbf{xtoken} = \mathbf{xtag}\Big\}$$

and

$$\mathcal{R}'_{vSSE-LWR} = \Big\{\Big((\mathbf{a}, \mathbf{xtoken}, \mathbf{0}, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3), (\mathbf{yid}, \mathbf{0}, \mathbf{xtag}, d_1, d_2, d_3)\Big) :$$
$$\lfloor \mathbf{c}_1 \rceil_p = \lfloor d_1 \cdot \lfloor \mathbf{a} \cdot \mathbf{yid} \rceil_{p_1} \rceil_p \ \wedge \ \lfloor \mathbf{c}_2 \rceil_p = \lfloor d_2 \cdot \lfloor \mathbf{a} \cdot \mathbf{0} \rceil_{p_1} \rceil_p$$
$$\wedge \ \lfloor \mathbf{c}_3 \rceil_p = \lfloor d_3 \cdot \lfloor \mathbf{a} \cdot \mathbf{xtag} \rceil_{p_1} \rceil_p$$
$$\wedge \ (q > p_1 >> p) \ \wedge \ \frac{q}{p_1} \geq \sqrt{n} \ \wedge$$
$$\mathbf{yid} \cdot \mathbf{xtoken} = \mathbf{xtag}\Big\}$$

Where the prover $\boldsymbol{P}$ *proves in the relation* $\mathcal{R}_{vSSE-LWR}$ *while the verifier* $\boldsymbol{V}$ *accepts in the relation* $\mathcal{R}'_{vSSE-LWR}$.

Proof. The theorem is proved by showing that the protocol is a Σ_2-protocol for the given relations. The claim then follows directly by showing that the following properties hold -

Completeness. This follows directly from the completeness of Protocol 1 and -

$$\begin{aligned} s_{m_3} &= x_1 s_{m_1} + x_1 s_{m_1} \\ \mu_3 + d \cdot \mathbf{xtag} &= \mathbf{y}_{\mathsf{id}}(\mu_1 + d \cdot \mathbf{xtoken}) \\ &= \mu_3 + \mathbf{y}_{\mathsf{id}} d \cdot \mathbf{xtoken}) \\ &= \mu_3 + d(\mathbf{y}_{\mathsf{id}} \cdot \mathbf{xtoken})) \\ &= \mu_3 + d \cdot \mathbf{xtag} \end{aligned}$$

Special Soundness. Given two accepting transcripts, we can extract witnesses (Δ_{m_i}) for $\mathbf{c}_i$ ($i = 1, 2, 3$) analogously to Theorem 2. We show the linear relation $\Delta_{m_3} = x_1 \cdot \Delta_{m_1} + x_2 \cdot \Delta_{m_2}$ is satisfied as follows:

$$\begin{aligned} \Delta_{m_3} &= s'_{m_3} - s''_{m_3} \\ \Delta_{\mathbf{xtag}} &= \mathbf{y}_{\mathsf{id}} \Delta_{\mathbf{xtoken}} \\ &= \Delta'_{\mathbf{xtag}} - \Delta''_{\mathbf{xtag}} \\ &= \mathbf{y}_{\mathsf{id}} \cdot \mathbf{xtoken}' - \mathbf{y}_{\mathsf{id}} \cdot \mathbf{xtoken}'' \\ &= \mathbf{y}_{\mathsf{id}} \cdot \Delta_{\mathbf{xtoken}} \end{aligned}$$

Special honest-verifier Zero-knowledge. The simulator essentially is give three independent instances of transcripts similar to that of Protocol 1 except that $s'_{m_3} = \mathbf{y}_{\mathsf{id}} \cdot s'_{m_1}$. The correctness of this simulation is shown by a standard argument, as shown in [BKLP14]. □

Theorem 5. *If Protocol 3 is an honest-verifier zero-knowledge proof and* OQXT *[TPM23] is a post-quantum secure SSE scheme* Π_{OQXT} *under* $\mathsf{LWR}_{n,p_1,q}$ *and* $\mathsf{LWR}_{n,p,q}$ *assumption, then Verifiable-*OQXT = $\{\Pi_{\mathrm{OQXT}}$, *Protocol 3*$\}$ *is a post-quantum secure* RLWR *based verifiable SSE scheme.*

Proof. The proof follows naturally from Theorem 4 in this work and from Theorem 1 in [TPM23]. □

Parameter/Property	[BKLP14]	This Work
q	2^{71}	2^{45*}
p_1	N/A	2^{40}
p	N/A	2^5
n	512	512
σ	$\simeq 2700$	N/A
Commit size	54.5 KB	50 KB
Proof size	30 KB	8.4 KB
Hiding	Computational	Computational
Binding	Statistical	Statistical
Hardness Assumption	RLWE	RLWR

Table 2: Comparison of Parameter Setting/Property of Our Scheme (Figure 1) and [BKLP14]. $(*)$ More specifically we choose $q = 35184372088891 (\approx 2^{45})$.

5 Results and Comparison

In this section, we give give concrete parameters for which RLWR based commitment scheme and Σ_2 protocol can be instantiated along with a comparison with the parameters in the commitment scheme proposed in [BKLP14]. We also show instantiations of our proposed verifiable quantum-safe SSE, which we name Verifiable-OQXT. We instantiate the pre-image proof for linear linear relations that is curated for Verifiable-OQXT (Figure 3) on top of the original OQXT protocol and show comparisons in terms of conjunctive query execution time, storage overhead and Setup time.

Experimental Setup. The complete implementation of Protocol 3 and Verifiable-OQXT implementation was done using C++ (with GCC 9 compiler) and we used Redis as the database backend. We ran the experiments on a *single* node with Intel Xeon E5-2690 v4 2.6 GHz CPU with 128 GB RAM and 512 GB SSD storage.

Instantiation of RLWR based Σ_2 Protocol. Figure 4 shows the linear scaling of the verification time of our proposed Σ_2 protocol with increase in the number of linear relations to be verified. We emphasize that the number of linear relations verified here is done sequentially, however in the context Verifiable-OQXT we verify multiple linear relations in parallel, hence the overall verification overhead remains extremely small (equivalent to the verification time of a single linear relation $\simeq 0.0023$ seconds), thereby preserving the original sub-linear search complexity of OQXT.

Table 2 provides a comparative analysis of our proposed RLWR based Σ_2 protocol with the commitment scheme proposed in [BKLP14]. We choose q such that $\langle x^n + 1 \rangle$ splits into exactly two irreducible factors modulo q and Δd is invertible in R_q (as noted by [ON26]). We therefore choose $q = 35184372088891 \approx 2^{45}$. It is observed that our proposed RLWR based commitment scheme produces commitments of size $(n \cdot k \cdot log\ p_1)$ bits while that of [BKLP14] is $(n \cdot k \cdot log\ q)$ bits. Concretely, our commitments are of size 50 KB which is less than that of [BKLP14]. The proof size generated by our proposed scheme is $(3 \cdot n \cdot log\ q)$ bits where as [BKLP14] produces a proof size of $(n \cdot l \cdot log\ q) + (n \cdot k \cdot log\ 6\ \sigma)$ bits (σ is the standard deviation of error used in [BKLP14] and l is the dimension of the message

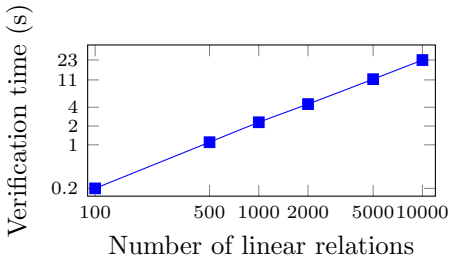

Figure 4: Time required for verifying a pre-image proof using our proposed Σ_2 Protocol (in Figure 1)

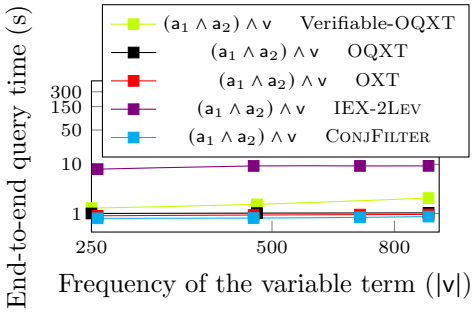

Figure 5: End-to-End Search latency with constant frequency of the least frequent term (both axes are in log scale)

space [BDL+18]). Concretely we see, that our proposed Σ_2 protocol produces proof size of around 8.4 KB which is around 4× less than [BKLP14]. We would like to emphasize that due to the elimination of explicit error sampling, we can choose tighter parameters and the ring modulus is significantly reduced (Table 2), whereas in [BKLP14], they choose the standard deviation of the randomness of error (σ_η) to be very large, in order to reduce M at the cost of blowing up parameters. This in turn results in an improved communication complexity of our protocol from $O(M\ n\ log\ q)$ to $O(n\ log\ q)$ (where M is the rejection sampling constant).

Conjunctive Query Complexity of Verifiable OQXT. We instantiate the protocol in Figure 3 with OQXT, the quantum-safe SSE protocol introduced in [TPM23] and compare the conjunctive query execution time as shown in [TPM23]. We compare the query execution time of the original OQXT protocol along with the state-of-the-art conjunctive SSE protocol as shown in [TPM23] with the Verifiable-OQXT construction.

Figure 5 and Figure 6 compares the end-to-end search latency of Verifiable-OQXT with that of OQXT, OXT [CJJ+13b], IEX-2Lev [KM17] and ConjFilter [PPSY21] for conjunctive queries. Search performance of Verifiable-OQXT scales linearly with the search performance of OQXT, OXT and ConjFilter and shows 10× faster performance than IEX-2Lev. To validate this, we follow a similar experimental setup as shown in [TPM23]. We consider a three-keyword query of the form $q = (\mathsf{a}_1 \wedge \mathsf{a}_2) \wedge \mathsf{v}$, where $\mathsf{a}_1, \mathsf{a}_2$ and v are three keywords from **DB**. Without loss of generality, we consider the first term of q (or a_1 here) to be the

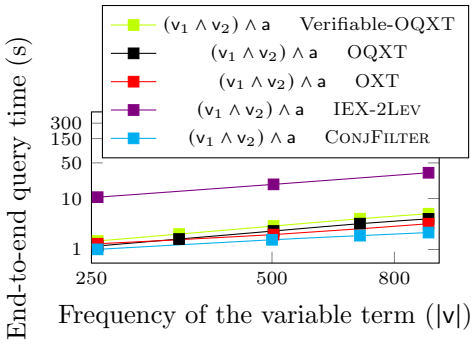

Figure 6: End-to-End Search latency with variable frequency of the least frequent term (both axes are in log scale)

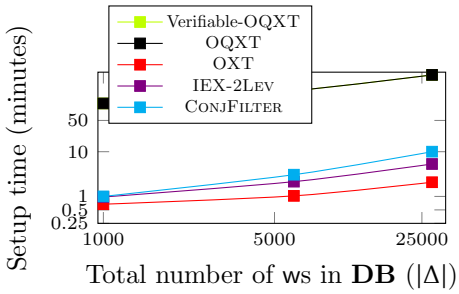

Figure 7: Setup time (minutes) (both axes are in log scale)

least frequent keyword. We vary the frequency of v (referred to as the variable term) with different queries where as the frequency of a is kept constant (constant term). Figure 5 shows a constant time overhead for conjunctive queries of this form with Verifiable-OQXT which scales linearly with OQXT.

Another set of experiments is carried out on queries of the form $q = (\mathsf{v}_1 \wedge \mathsf{v}_2) \wedge \mathsf{a}$ (Figure 6) similarly as done in [TPM23]. This time we vary the frequency of least frequent keyword a_1 with different queries and the frequency of v is kept constant (since we *vary* the least frequent keyword, we denote this variable term as $(\mathsf{v}_1 \wedge \mathsf{v}_2)$ and the constant term as a in Figure 6). The search time of Verifiable-OQXT shows the same linear growth as OQXT and hence compares with the rest of the schemes in the similar fashion.

The verification overhead of appending Protocol 3 with the OQXT SSE scheme incurs an extra overhead of 0.0023 seconds, which exhibits insignificant affect on the overall search time complexity of Verifiable-OQXT.

Setup Time of Verifiable-OQXT. In Figure 7 we show a comparison of the Setup time of Verifiable-OQXT with OQXT. We state that since verification is only performed after a search query execution, there is no direct consequence of Protocol 3 on the Setup time of Verifiable-OQXT.

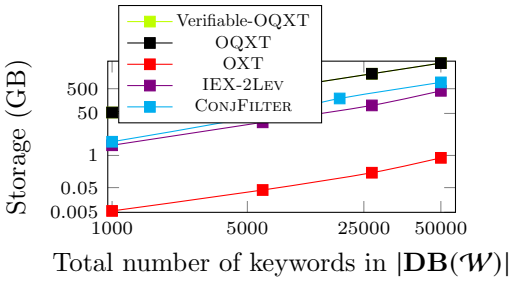

Figure 8: Server Storage (both axes are in log scale)

Storage Overhead of Verifiable-OQXT. The storage overhead of OQXT as shown in [TPM23] is the amount of server storage required to perform an encrypted conjunctive search correctly on the server. The verification step incorporated in Verifiable-OQXT requires no extra storage of information at the server. The commitments and proofs are dynamically computed during a call to the verification routine. Therefore, there is no explicit increase in server storage overhead for Verifiable-OQXT when compared to the original scheme (as shown in Figure 8).

Comparison with state-of-the-art SSE. The Verifiable-OQXT framework proposed in this work scales linearly in terms of search latency with the other three schemes, namely, OQXT, OXT, and ConjFilter, while significantly improving over IEX-2Lev. Verifiable-OQXT builds on the post-quantum secure construction of OQXT and provides verification guarantees via an efficient zero-knowledge based Σ_2 protocol. Therefore, by design, Verifiable-OQXT is inherently post-quantum secure. As a result, a straightforward advantage of Verifiable-OQXT over the state-of-the-art classical searchable encryption schemes (OXT, ConjFilter, IEX-2Lev) is that it offers a post-quantum secure SSE construction based on the hardness of the Learning with Rounding (LWR) assumption. Furthermore, it supersedes all of these SSE schemes along with OQXT by providing a zero-knowledge based verification of the correctness of the scheme by an efficient Σ_2 protocol based on a lightweight commitment scheme. All other SSE constructions do not support verification of the correctness of the search result returned by the server. As such, they consider a threat model where the server is semi-honest. In Verifiable-OQXT we elevate the threat model to a malicious server setting, which is a weaker security assumption, hence providing a more robust security guarantee. Our framework efficiently proves the correctness of the search result returned by a malicious server in zero-knowledge to the client in a single round of communication. The overall search latency of the Verifiable-OQXT scheme due to the additional verification step is negligible (0.0023 seconds), and hence it scales with the search latency of other existing SSE schemes that do not support verification of their search results.

6 Conclusion

In this paper we presented an RLWR based commitment scheme and companion Σ_2 protocol and improved upon the RLWE based commitment scheme proposed in [BKLP14]. Our

proposed commitment scheme reduces the proof size by 4×, and eliminates the requirement for explicit error sampling, thereby ensuring tighter parametrization, that in turn improves efficiency. As an exemplary application, we incorporate our pre-image proofs for proving linear relations into a quantum-safe SSE scheme and devise an efficient verifiable quantum-safe conjunctive SSE scheme, we call it, Verifiable-OQXT. To the best of our knowledge our proposed commitment scheme and ZK-PoK based on RLWR problem is the first in literature, that achieves negligible knowledge error and a short proof size. Additionally, the Verifiable-OQXT construction is conjectured to be the first zero-knowledge proof-based verifiable SSE scheme, capable of proving correctness of a conjunctive search with an additional overhead of less than 0.0023 seconds.

References

[ABPS24] Shahla Atapoor, Karim Baghery, Hilder VL Pereira, and Jannik Spiessens. Verifiable fhe via lattice-based snarks. *Cryptology ePrint Archive*, 2024.

[AGT24] Omar Ahmed, Charles Gouert, and Nektarios Georgios Tsoutsos. Peev: Parse encrypt execute verify-a verifiable fhe framework. *IEEE Access*, 2024.

[AHIV23] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: lightweight sublinear arguments without a trusted setup. *Des. Codes Cryptogr.*, 2023.

[AJL+12] Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. Multiparty computation with low communication, computation and interaction via threshold FHE. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2012. Proceedings*, 2012.

[ASW00] N. Asokan, Victor Shoup, and Michael Waidner. Optimistic fair exchange of digital signatures. *IEEE J. Sel. Areas Commun.*, 2000.

[BBB+18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Gregory Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings*, 2018.

[BCC+15] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit. Short accountable ring signatures based on DDH. In *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, 2015. Proceedings, Part I*, 2015.

[BCC+16] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2016. Proceedings, Part II*, 2016.

[BCK+14] Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, 2014. Proceedings, Part I*, 2014.

[BCR+19] Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza, and Nicholas P. Ward. Aurora: Transparent succinct arguments for R1CS. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2019. Proceedings, Part I*, 2019.

[BDL+18] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks - 11th International Conference, SCN 2018. Proceedings*, 2018.

[BDP00] Joan Boyar, Ivan Damgård, and René Peralta. Short non-interactive cryptographic proofs. *J. Cryptol.*, 2000.

[BF11] Dan Boneh and David Mandell Freeman. Homomorphic signatures for polynomial functions. In *Advances in Cryptology–EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings 30*, pages 149–168. Springer, 2011.

[BFP16] Raphael Bost, Pierre-Alain Fouque, and David Pointcheval. Verifiable dynamic symmetric searchable encryption: Optimality and forward security. *IACR Cryptol. ePrint Arch.*, 2016.

[BKLP14] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. Cryptology ePrint Archive, Paper 2014/889, 2014.

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 1983.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 719–737. Springer, 2012.

[CD09] Ronald Cramer and Ivan Damgård. On the amortized complexity of zero-knowledge protocols. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, 2009. Proceedings*, 2009.

[CDK14] Ronald Cramer, Ivan Damgård, and Marcel Keller. On the amortized complexity of zero-knowledge protocols. *J. Cryptol.*, 2014.

[CDP12] Ronald Cramer, Ivan Damgård, and Valerio Pastro. On the amortized complexity of zero knowledge protocols for multiplicative relations. In Adam D. Smith, editor, *Information Theoretic Security - 6th International Conference, ICITS 2012. Proceedings*, 2012.

[CFSY96] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-autority secret-ballot elections with linear work. In *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, 1996, Proceeding*, 1996.

[CGKO06a] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In *ACM CCS*, 2006.

[CGKO06b] Reza Curtmola, Juan A. Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In *ACM CCS 2006*, 2006.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 1985.

[CJJ+13a] David Cash, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel-Cătălin Roşu, and Michael Steiner. Highly-scalable searchable symmetric encryption with support for boolean queries. In *CRYPTO*, 2013.

[CJJ+13b] David Cash, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Highly-scalable searchable symmetric encryption with support for boolean queries. In *CRYPTO 2013*, 2013.

[CJJ+14] David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Dynamic searchable encryption in very-large databases: Data structures and implementation. In *NDSS 2014*, 2014.

[CK10] Melissa Chase and Seny Kamara. Structured encryption and controlled disclosure. In *ASIACRYPT 2010*, 2010.

[COS20] Alessandro Chiesa, Dev Ojha, and Nicholas Spooner. Fractal: Post-quantum and transparent recursive proofs from holography. In *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2020. Proceedings, Part I*, 2020.

[CT14] David Cash and Stefano Tessaro. The locality of searchable symmetric encryption. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2014. Proceedings*, 2014.

[CYG+15] Rong Cheng, Jingbo Yan, Chaowen Guan, Fangguo Zhang, and Kui Ren. Verifiable searchable symmetric encryption from indistinguishability obfuscation. In *Proceedings of the 10th ACM symposium on information, computer and communications security*, 2015.

[DF89] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, 1989, Proceedings*, 1989.

[ESLL19] Muhammed F. Esgin, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu. Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications. In *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, 2019. Proceedings, Part I*, 2019.

[GK15] Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2015. Proceedings, Part II*, 2015.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *ACM STOC 2008*, pages 197–206, 2008.

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, 2007*, 2007.

[IKOS09] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge proofs from secure multiparty computation. *SIAM J. Comput.*, 2009.

[JKPT12] Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *Advances in Cryptology - ASIACRYPT 2012. Proceedings*, 2012.

[JLZL25] Licheng Ji, Jiguo Li, Yicheng Zhang, and Yang Lu. Verifiable searchable symmetric encryption over additive homomorphism. *IEEE Transactions on Information Forensics and Security*, 2025.

[Kil92] Joe Kilian. A note on efficient zero-knowledge proofs and arguments (extended abstract). In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, 1992.

[KM17] Seny Kamara and Tarik Moataz. Boolean searchable symmetric encryption with worst-case sub-linear complexity. In *EUROCRYPT 2017*, pages 94–124, 2017.

[KO12] Kaoru Kurosawa and Yasuhiro Ohtaki. Uc-secure searchable symmetric encryption. In *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers 16*, 2012.

[KVMGH23] Christian Knabenhans, Alexander Viand, Antonio Merino-Gallardo, and Anwar Hithnawi. vfhe: Verifiable fully homomorphic encryption. In *Proceedings of the 12th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, pages 11–22, 2023.

[LLNW23] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. *J. Cryptol.*, 2023.

[LM06] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006. Proceedings, Part II*, 2006.

[LN17] Vadim Lyubashevsky and Gregory Neven. One-shot verifiable encryption from lattices. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017. Proceedings, Part I*, 2017.

[LNP22] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. In *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022. Proceedings, Part II*, 2022.

[LNSW13] San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In *Public-Key Cryptography - PKC 2013. Proceedings*, 2013.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 2013.

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 2015.

[Lyu09] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, 2009. Proceedings*, 2009.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2012. Proceedings*, 2012.

[Mic94] Silvio Micali. CS proofs (extended abstracts). In *35th Annual Symposium on Foundations of Computer Science*, 1994.

[Mic07] Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complex.*, 2007.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 700–718. Springer, 2012.

[MRAS15] Rachel Player Martin R. Albrecht and Sam Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology. Volume 9, Issue 3, Pages 169–203, ISSN (Online) 1862-2984,ISSN (Print) 1862-2976 DOI: 10.1515/jmc-2015-0016, October*, 2015.

[ON26] Lukasz Olejnik and Bartosz Naskrecki. AI grinding for fun and cryptanalysis. *CoRR*, abs/2608.21986, 2026.

[PFH+17] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. 2017.

[PM21] Sikhar Patranabis and Debdeep Mukhopadhyay. Forward and backward private conjunctive searchable symmetric encryption. In *NDSS 2021*, 2021.

[PPSY21] Sarvar Patel, Giuseppe Persiano, Joon Young Seo, and Kevin Yeo. Efficient boolean search over encrypted data with reduced leakage. In *ASIACRYPT 2021*, 2021.

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006. Proceedings*, 2006.

[RCPT19] Kim Ramchen, Chris Culnane, Olivier Pereira, and Vanessa Teague. Universally verifiable mpc and irv ballot counting. In *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*, pages 301–319. Springer, 2019.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, 2001, Proceedings*, 2001.

[Sch91] Claus-Peter Schnorr. Efficient signature generation by smart cards. *J. Cryptol.*, 1991.

[Ste96] Jacques Stern. A new paradigm for public key identification. *IEEE Trans. Inf. Theory*, 1996.

[SWP00] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *Proceeding 2000 IEEE symposium on security and privacy. S&P 2000*, 2000.

[TPM23] Debadrita Talapatra, Sikhar Patranabis, and Debdeep Mukhopadhyay. Conjunctive searchable symmetric encryption from hard lattices. In *8th IEEE European Symposium on Security and Privacy, EuroS&P*, 2023.

[TZ21] Akira Takahashi and Greg Zaverucha. Verifiable encryption from mpc-in-the-head. *Cryptology ePrint Archive*, 2021.

[VKH23] Alexander Viand, Christian Knabenhans, and Anwar Hithnawi. Verifiable fully homomorphic encryption. *arXiv preprint arXiv:2301.07041*, 2023.

[XXW13] Xiang Xie, Rui Xue, and Minqian Wang. Zero knowledge proofs from ring-lwe. In *Cryptology and Network Security - 12th International Conference, CANS 2013. Proceedings*, 2013.