

Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications

Rupeng Yang^{1,2}, Man Ho Au^{2 *}, Zhenfei Zhang³, Qiuliang Xu^{4 *}, Zuoxia Yu², and William Whyte⁵

¹ School of Computer Science and Technology, Shandong University, Jinan, 250101, China
orbbyrp@gmail.com

² Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong
csallen@comp.polyu.edu.hk, zuoxia.yu@gmail.com

³ Algorand, USA

zhenfei@algorand.com

⁴ School of Software, Shandong University, Jinan, 250101, China
xql@sdu.edu.cn

⁵ Qualcomm Technologies Incorporated, USA
wwhyte@qti.qualcomm.com

Abstract. We provide new zero-knowledge argument of knowledge systems that work directly for a wide class of language, namely, ones involving the satisfiability of matrix-vector relations and integer relations commonly found in constructions of lattice-based cryptography. Prior to this work, practical arguments for lattice-based relations either have a constant soundness error ($2/3$), or consider a weaker form of soundness, namely, extraction only guarantees that the prover is in possession of a witness that “approximates” the actual witness. Our systems do not suffer from these limitations.

The core of our new argument systems is an efficient zero-knowledge argument of knowledge of a solution to a system of linear equations, where variables of this solution satisfy a set of quadratic constraints. This argument enjoys standard soundness, a small soundness error ($1/poly$), and a complexity linear in the size of the solution. Using our core argument system, we construct highly efficient argument systems for a variety of statements relevant to lattices, including linear equations with short solutions and matrix-vector relations with hidden matrices.

Based on our argument systems, we present several new constructions of common privacy-preserving primitives in the *standard lattice* setting, including a group signature, a ring signature, an electronic cash system, and a range proof protocol. Our new constructions are one to three orders of magnitude more efficient than the state of the art (in standard lattice). This illustrates the efficiency and expressiveness of our argument system.

* Corresponding author.

1 Introduction

Traditional cryptographic schemes based on number theoretic assumptions are at risk due to possible attacks from quantum computers. Among all alternatives, the lattice-based ones appear to be the most promising. To date, we have good candidates to fundamental cryptographic primitives such as public key encryption schemes (e.g., [3, 10, 11, 29]) and signature schemes (e.g., [9, 18, 21, 46]). However, lattice-based privacy-preserving primitives, such as group signatures [16], ring signatures [56], electronic cash (E-cash) [15], etc., are still significantly less efficient than their traditional counterparts, partially due to the lack of suitable lattice-based zero-knowledge proofs. Specifically, current zero-knowledge proofs for lattice-based relations either have a poor efficiency or have great restrictions when employed in constructing advanced applications.

The study of lattice-based zero-knowledge proofs is initialized by Goldreich and Goldwasser in [23]. Goldreich and Goldwasser’s proof system, as well as proof systems developed in subsequent works [2, 28, 50, 54], are mainly of theoretical interest. While one can construct applications such as verifiable encryption [25] and group signature [14, 26] from these protocols, their lack of efficiency prevents them from being employed in practice.

For practical lattice-based zero-knowledge proofs, there are two main approaches in current literature.

Stern-type Protocol. One approach, which follows techniques in [31, 57], is proposed by Ling et al. in [40]. They construct an efficient zero-knowledge argument of knowledge (ZKAoK) for the basic Inhomogeneous Short Integer Solution (ISIS) relation $\mathcal{R}_{ISIS} = \{(\mathbf{A}, \mathbf{y}), \mathbf{x} : \mathbf{A} \cdot \mathbf{x} = \mathbf{y} \wedge \|\mathbf{x}\| \leq \beta\}$. Focusing on arguing additional relations over witnesses, ZKAoKs for a wider class of lattice-based relations are constructed in subsequent works. This gives rise to various applications, such as verifiable encryption [40], group signature [33, 34, 36, 41, 43], ring signature [36], group encryption [35] and E-cash [37].

The major issue for Stern-type protocols is their inherent *large soundness error*. More precisely, a single round Stern-type protocol has a soundness error of $2/3$, i.e., a cheating prover is able to convince an honest verifier with probability $2/3$ even if it does not possess any valid witness. Thus, to achieve a negligible soundness error, the protocol is required to repeat for many (e.g., 219) times, and the final proof consists of proofs generated in all iterations. Consequently, its proof size is usually on the order of tens of megabytes to terabytes.

Fiat-Shamir with Abort. Another line of research follows the identification schemes from [44–46]. Early works in this direction [32, 51] consider ZKAoK protocols with binary challenges, which leads to a soundness error of $1/2$ for a single iteration. Thus, multiple (e.g., 128) repetitions are needed to achieve a negligible soundness error. Subsequently, ZKAoKs with larger challenge spaces are adopted to reduce the number of rounds required. This results in one-round protocols with inverse-polynomial/negligible soundness error. Thus, we only need

to run them a few (e.g., 10 or even 1) time(s) to achieve a negligible soundness error. Consequently, the proof size is usually a few megabytes or less.

We have seen some applications, such as verifiable encryption [7, 47], group signature [12, 13, 17] and ring signature [19] from Fiat-Shamir with abort (FSwA) protocols (with large challenge space). However, it is a complex task to design cryptographic protocols using FSwA. This is mainly due to the so-called *soundness gap*. For instance, for the ISIS relation \mathcal{R}_{ISIS} , the FSwA proof only attests the fact that the prover knows a witness for $\mathcal{R}'_{ISIS} = \{(\mathbf{A}, \mathbf{y}), \mathbf{x} : \mathbf{A} \cdot \mathbf{x} = c \cdot \mathbf{y} \wedge \|\mathbf{x}\| \leq \beta'\}$, where $\beta' > \beta$ and $c > 1$. Thus, to construct advanced applications from them, we have to use cryptographic primitives that are compatible with such relaxed soundness, e.g., encryption schemes with a relaxed decryption [7, 47], commitment schemes with a relaxed opening [6, 8] and signature schemes with a relaxed verification [13]. Unfortunately, it is usually hard or even impossible to construct primitives with such property. Meanwhile, general frameworks in the literature for advanced applications may not work when we use relaxed versions as building blocks. Thus, the construction and security analysis has to be conducted from scratch. Additionally, we do not have a simple manner to prove the relations over witnesses using Fiat-Shamir with abort protocols. Ad-hoc techniques are used to circumvent this requirement, which introduce additional complexity.

To summarize, we have some “user-friendly” lattice-based ZKAoKs that are less efficient; and some efficient ZKAoKs that are very complicated for advanced applications. The goal of this paper is, therefore, to construct ZKAoKs that are both efficient and easy to use.

On the Difficulty of Achieving Standard Soundness and Small Soundness Error. Before presenting our main results, we would like to discuss why previous works cannot achieve the standard soundness and a small soundness error simultaneously. First, for most (if not all) lattice-based relations, we need to prove that (parts of) the witnesses are small integers. This can be done in two approaches,

1. In a Stern-type protocol, a short integer is decomposed into a binary vector of bounded length. Then the prover proves that the decomposition outputs are correct via a standard Stern protocol, which asks the prover to open 2 out of 3 commitments in the challenge phase. Therefore, the soundness error $2/3$ is inherent for a Stern-type protocol.
2. In a Fiat-Shamir with abort protocol, the prover and the verifier run a Schnorr-type protocol with some tweaks for arguing shortness of the witness. However, the standard extraction procedure for the Schnorr protocol does not work here. This is because the extracted witnesses will be scaled by some large number (more accurately, the inverse of the difference of two challenges) and may be large. To circumvent this problem, the extraction procedure avoids multiplication of inverses. Correspondingly, the definition of soundness is relaxed in the sense that the extracted witness does not necessarily satisfy the original relation.

1.1 Our Results

In this work, we present a new approach for constructing efficient zero-knowledge arguments of knowledge for a large class of lattice-based relations. The core component of our methodology is an efficient ZKAoK for linear equations with additional quadratic constraints over the witnesses.

More concretely, let m , n , and ℓ be positive integers, and q be a large enough integer that is a *power-of-prime*. The ZKAoK protocol proves the following relation \mathcal{R}^* in Eq.(1)¹:

$$\mathcal{R}^* = \{(\mathbf{A}, \mathbf{y}, \mathcal{M}), (\mathbf{x}) \in (\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m \times ([1, n]^3)^\ell) \times (\mathbb{Z}_q^n) : \mathbf{A} \cdot \mathbf{x} = \mathbf{y} \wedge \forall (h, i, j) \in \mathcal{M}, \mathbf{x}[h] = \mathbf{x}[i] \cdot \mathbf{x}[j]\} \quad (1)$$

where \mathcal{M} is a set of ℓ triples that defines quadratic constraints over \mathbf{x} . Usually, ℓ will be linear in n and in any case, we have $\ell \leq n^3$.

Building upon our main protocol, we present a variety of ZKAoKs for some concrete lattice-based relations. The constructed ZKAoKs have standard soundness, yet achieving an inverse polynomial soundness error. We summarize the differences between our approaches and previous results in Table 1.

Table 1: Comparison of Approaches for Lattice-Based ZKAoKs.

	Standard Soundness	Soundness Error
Stern-Style	✓	2/3
FSwA	✗	1/poly or negl
This work	✓	1/poly

To further demonstrate the usefulness of our methodology, we develop several privacy-preserving primitives from these ZKAoKs. We illustrate the roadmap to these applications in Figure 1.

In addition, we also examine the concrete efficiency (particularly, communication cost) of our applications. We highlight some of the results in Table 2. For more details, see the full version of this work.

We remark that the applications (and the performance data thereof) are to illustrate the usefulness of our framework. They are by no means exhaustive nor optimal. One may extend our results to other privacy-preserving primitives such as anonymous credential, decentralized anonymous credential, group encryption, traceable signature, linkable ring signature, CryptoNote protocol (and thus Monero), k -times anonymous authentication, blacklistable anonymous credential, Zerocoin, etc. Also, one can improve the results of this work via utilizing structured lattices (such as ideal lattices or NTRU lattices) and application-specific optimizations. Those extensions and optimizations are beyond the scope of this paper.

¹ In this paper, operations over group elements in \mathbb{Z}_q are modulo q unless otherwise specified.

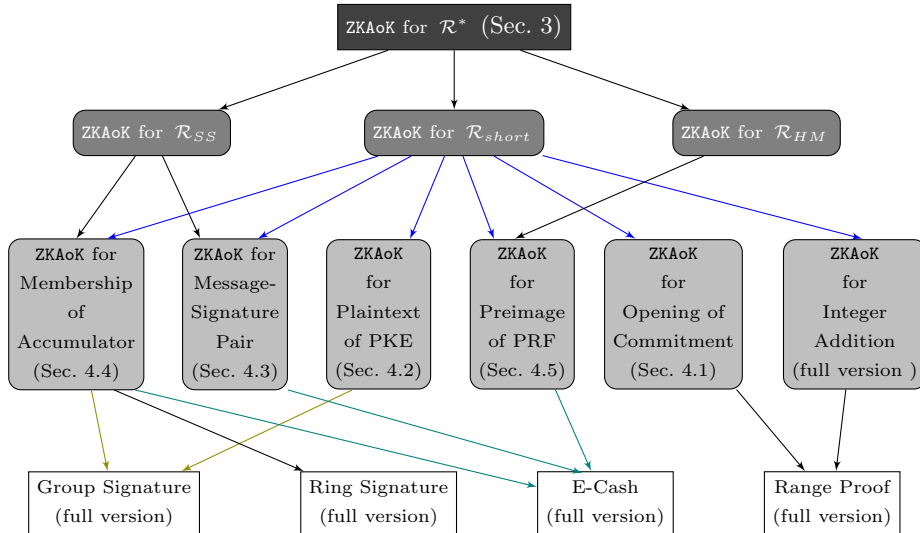


Fig. 1 The Roadmap for our ZKAoKs and their Applications. The starting point is our core ZKAoK for \mathcal{R}^* . It is then used to construct ZKAoKs for some elementary relations, namely, \mathcal{R}_{short} , \mathcal{R}_{SS} , and \mathcal{R}_{HM} (we define these elementary relations and explain how to develop ZKAoKs for them in Sec. 1.2). Based on these elementary ZKAoKs, we further construct ZKAoKs for cryptographic schemes. Finally, we construct privacy-preserving primitives from these ZKAoKs.

Comparisons. Next, we give a brief comparison between the communication cost of applications in this work and that of previous results. Our examples in this section target 80 bits security unless otherwise specified.

We summarize the results in Table 2. Generally, for applications where solutions were only available through Stern-type protocols, our constructions are (much) more efficient than the state of the art. For applications where solutions were also available through Fiat-Shamir with abort protocols, our constructions are less efficient. Note that constructions utilizing Fiat-Shamir with abort are designed from scratch and these state-of-the-art constructions are optimized through the use of structured lattices (ideal lattices); while our solutions are built on standard lattices, which are believed to offer better security.

We stress again that the main advantage of our framework is that it provides a fairly good efficiency yet keeping its user-friendliness. Optimizing toward individual application, as stated earlier, is beyond the scope of this paper.

Ring Signatures. Following the framework of [36], a ring signature scheme can be obtained with our ZKAoK. The signature size of [36] is estimated by [19] at 47.3 MB, for a ring of 2^{10} users. In contrast, the signature size of our ring signature scheme is 4.24 MB in the same setting.

To the best of our knowledge, the most efficient ring signature scheme is from [19], using Fiat-Shamir with abort protocols. For the same number (i.e., 2^{10})

Table 2: Comparison of Communication Cost for Applications from Different ZKAoKs.

Application	This paper	Stern-type	FSwA (ideal lattice)
Ring Signature	4.24MB	47.3MB [36]	1.41MB [19]
Group Signature	6.94MB	61.5MB [36]	0.58MB [17]
Range Proof	1.21MB	3.54MB [38]	N/A
Electronic Cash	262MB	\approx 720TB [37]	N/A

of users, its signature size is about 1.41 MB at 100 bits security level. Using a similar parameter setting, the signature size of our solution is 3.05 MB.²

Group Signatures. A group signature can also be obtained following a similar approach in [36] using our ZKAoK. The signature size of [36] is 61.5 MB for a group of 2^{10} users. In contrast, the signature size of our solution is 6.94 MB in the same setting.

The most efficient group signature scheme to date is from [17], achieving a signature size of less than 1 MB. Nonetheless, our approach can achieve additional features. For example, one can convert our group signature scheme into a fully dynamic one via the techniques in [42], without increasing its signature size.

Electronic Cash. To the best of our knowledge, the only lattice-based (compact) electronic cash system is from [37], but no concrete estimation of its performance is provided. In the full version of this work, we provide a rough estimation for the communication cost of their spend protocol, for a wallet of 2^{10} coins. The estimation shows that the communication cost of their spend protocol is at least several terabytes while our spend protocol can achieve a communication cost of 262 MB in the same setting.

There is no E-cash system from Fiat-Shamir with abort protocols in the literature. This is due to the following technical barriers. First, in an E-cash system, we need an argument of correct evaluation for pseudorandom function (PRF). This requires an argument for the learning with rounding (LWR) relation, i.e., proving the (rounded) error terms lie *exactly* in an interval. Due to the aforementioned soundness gap, it is not known how this proof can be done from Fiat-Shamir with abort protocols. Moreover, we also need an adaptively secure signature scheme and an argument of knowledge of a valid message/signature pair for it. To date, signature schemes that admit an argument from Fiat-Shamir with abort protocols can only achieve selective security. Complexity leveraging trick that converts a selectively secure scheme into an adaptively secure one does not work here either, since the message space, which contains all possible PRF keys, are exponentially large.

² In [19], parameters are set in a slightly mild way, so, the signature size is smaller if we use their criterion to select parameters.

Range Proof. Prior to our work, the most efficient lattice-based range proof is from [38]. When arguing knowledge of a 1000-bits committed value in a given range, its proof size is 3.54 MB. In contrast, the proof led by our solution is only 1.21 MB in the same setting.

1.2 Technical Overview

Warm-Up: An Argument for \mathcal{R}_{ISIS} . Before explaining the idea of our approach, we would like to give a simple intuition on how one can argue the ISIS relation, with standard soundness and small soundness error simultaneously. Our solution can be viewed as a somewhat mix of the Stern-type protocol and the Fiat-Shamir with abort protocol. In particular, we will first use the bit-decomposition technique to deal with small integers. Then we prove that the decomposition outputs are binary via proving some quadratic constraint over them (i.e., arguing $x = x^2$ for each bit x of the output). As shown in [27] (and its lattice variant [19]), this can be proved via arguing linear relations over commitments and thus can be instantiated with known commitment with a relaxed opening and Fiat-Shamir with abort protocols. Since we do not argue shortness of witnesses explicitly in the latter argument, soundness gap is not introduced.³ Surprisingly, this simple strategy can produce much more than merely arguing shortness of witnesses. We elaborate this next.

Building ZKAoK for \mathcal{R}^* . We start with a protocol that proves

$$\mathcal{R}_0 = \{(\mathbf{A}, \mathbf{y}), (\mathbf{x}) \in (\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m) \times (\mathbb{Z}_q^n) : \mathbf{A} \cdot \mathbf{x} = \mathbf{y}\} \quad (2)$$

which is the linear equation part of \mathcal{R}^* . The protocol can be viewed as an extension of the Schnorr protocol to the linear algebra setting. It proceeds as follows:

1. The prover samples a vector $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^n$ and sends $\mathbf{t} = \mathbf{A} \cdot \mathbf{r}$ to the verifier.
2. The verifier samples a challenge $\alpha \in \mathcal{C}$ and sends it to the prover. Here $\mathcal{C} \subset \mathbb{Z}$ is the challenge space of the protocol and will be specified later.
3. The prover sends $\mathbf{z} = \alpha \cdot \mathbf{x} + \mathbf{r}$ to the verifier.
4. The verifier accepts the proof iff $\mathbf{A} \cdot \mathbf{z} = \alpha \cdot \mathbf{y} + \mathbf{t}$.

Given two valid transcripts with distinct challenges, i.e., $(\mathbf{t}, \alpha, \mathbf{z})$ and $(\mathbf{t}, \alpha', \mathbf{z}')$, one can extract a vector $\bar{\mathbf{x}} = (\alpha - \alpha')^{-1} \cdot (\mathbf{z} - \mathbf{z}')$ that satisfies Eq. (2). In the meantime, a cheating prover cannot pass the verification unless it successfully guesses the challenge α . Thus, the protocol achieves a soundness error of $1/|\mathcal{C}|$. Hence, we can obtain an inverse-polynomial soundness error if \mathcal{C} contains polynomial many distinct challenges.

In the remaining part of this section, we explain how to additionally prove the quadratic constraints over the witnesses.

³ There exists a soundness gap in the proof, but it will not affect the proved argument due to the commitment with a relaxed opening.

Let (h, i, j) be an item in \mathcal{M} , our goal is to prove that $\mathbf{x}[h] = \mathbf{x}[i] \cdot \mathbf{x}[j]$. First, from the response $\mathbf{z} = \alpha \cdot \mathbf{x} + \mathbf{r}$, the verifier can compute

$$\begin{aligned} d &= \alpha \cdot \mathbf{z}[h] - \mathbf{z}[i] \cdot \mathbf{z}[j] \\ &= (\mathbf{x}[h] - \mathbf{x}[i] \cdot \mathbf{x}[j]) \cdot \alpha^2 + (\mathbf{r}[h] - \mathbf{r}[i] \cdot \mathbf{x}[j] - \mathbf{r}[j] \cdot \mathbf{x}[i]) \cdot \alpha - \mathbf{r}[i] \cdot \mathbf{r}[j] \\ &:= (\mathbf{x}[h] - \mathbf{x}[i] \cdot \mathbf{x}[j]) \cdot \alpha^2 + a \cdot \alpha - b \end{aligned}$$

where $a = \mathbf{r}[h] - \mathbf{r}[i] \cdot \mathbf{x}[j] - \mathbf{r}[j] \cdot \mathbf{x}[i]$ and $b = \mathbf{r}[i] \cdot \mathbf{r}[j]$. Note that $\mathbf{x}[h] = \mathbf{x}[i] \cdot \mathbf{x}[j]$ iff d is linear in α . Therefore, the main task is reduced to proving that the quadratic polynomial d is indeed linear in α , or alternatively $d - a \cdot \alpha + b$ is a *zero polynomial*.

To prove this, we can ask the prover to additionally send a and b in Step 1. Correspondingly, in Step 4, the verifier computes d and further checks if $d = a \cdot \alpha - b$. Since the prover does not know α in advance, a and b must be independent from α . Therefore, if the verification is successful, d is linear in α .

However, sending a and b in plaintext may leak information about the witness. To solve this problem, we adopt a homomorphic commitment scheme $\text{Commit}(m; r) \mapsto c$ that commits a message m to a commitment c using randomness r . More precisely, in Step 1, the prover generates $C_a = \text{Commit}(a; s_a)$ and $C_b = \text{Commit}(b; s_b)$ for some s_a and s_b , and send them to the verifier. In Step 3, the prover also computes $s = \alpha \cdot s_a - s_b$ and send s to the verifier. The verifier then checks if $\text{Commit}(d; s) = \alpha \cdot C_a - C_b$.

Remark 1.1. In this work, we will use the commitment scheme in [6], which is both additive homomorphic and supports multiplication by small constants. Therefore, we require the challenge space \mathcal{C} to be a set of polynomially-many small integers. The commitment scheme also requires the randomness to be drawn from some distributions with bounded norm. Here, we instantiate it with the Gaussian distribution.

Since new variables C_a, C_b and s are introduced in the proof, we also need to make sure that they will not compromise the privacy of a and b . First, C_b is determined by α, d, s and C_a , thus, we only need to consider s and C_a in the analysis. Recall that both s_a and s_b are drawn from the Gaussian distributions. According to the rejection sampling lemma [46], we can use s_b to mask $\alpha \cdot s_a$, and enforce the output s to follow a specific distribution that is independent from s_a . Then, by the hiding property of the commitment scheme, C_a reveals nothing about a . As a result, the commitments C_a, C_b and the randomness s do not leak additional information to the verifier.

There is an additional subtlety that we need to deal with. Note that in the aforementioned protocol, we try to argue that the quadratic polynomial $d - a \cdot \alpha - b$ is a zero polynomial. Thus, in the proof for soundness, we need three valid transcripts with distinct challenges after rewinding (note that a quadratic polynomial with three distinct roots must be a zero polynomial). So, to fix the extracted witnesses from these transcripts, the prover should also commit the witness \mathbf{x} and proves that the witness is properly committed (using a Fiat-Shamir with abort protocol).

In summary, our ZKAoK protocol contains three parts.

1. A Schnorr-type protocol that proves possession of a witness for \mathcal{R}_0 .
2. A commitment of witness \mathbf{x} and a Fiat-Shamir with abort protocol proving that the committed value is actually \mathbf{x} .
3. A proof for the quadratic constraints over the witnesses.

Building ZKAoK for More Relations. Next, we show how to develop ZKAoKs for relations relevant to lattice-based cryptographic schemes. As we illustrated in Figure 1, such relations can be viewed as combinations of some elementary relations, namely, linear equations with short solutions (\mathcal{R}_{short}), subset sum of linear equations (\mathcal{R}_{SS}), and linear equations with hidden matrices (\mathcal{R}_{HM}). Thus, here we focus on how to deal with these elementary relations.⁴

Linear Equation with Short Solution. This is a primary lattice-based relation and appears in (almost) all applications. Concretely, let m , n , and k be positive integers, q be a large enough power-of-prime, and $\beta = 2^k - 1$. The relation \mathcal{R}_{short} is given as

$$\mathcal{R}_{short} = \{(\mathbf{P}, \mathbf{v}), (\mathbf{w}) \in (\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m) \times ([0, \beta]^n) : \mathbf{P} \cdot \mathbf{w} = \mathbf{v}\}$$

The reduction from \mathcal{R}_{short} to \mathcal{R}^* takes the following steps:

- set a new witness \mathbf{x} as the binary decomposition of the original witness \mathbf{w} , i.e., each element w in \mathbf{w} is decomposed into k bits x_1, \dots, x_k such that $w = \sum_{i=1}^k x_i \cdot 2^{i-1}$ (note that a positive integer can be decomposed into k bits iff it is in $[0, 2^k - 1]$);
- set $\mathbf{A} = \mathbf{P} \cdot \mathbf{G}$ where the gadget matrix $\mathbf{G} := \mathbf{I}_n \otimes (1 \ 2 \ 4 \dots 2^{k-1})$ (thus, we have $\mathbf{G} \cdot \mathbf{x} = \mathbf{w}$);
- set $\mathbf{y} = \mathbf{v}$;
- set $\mathcal{M} = \{(i, i, i)\}_{i \in [1, nk]}$;

In doing so, we obtain a new relation in the form of \mathcal{R}^* where both the length of witness and the size of \mathcal{M} are nk .

Note that since q is a power-of-prime, for any $x \in \mathbb{Z}_q$, $x^2 = x$ iff $x = 0$ or $x = 1$. Thus, the new relation is equivalent to the original relation \mathcal{R}_{short} .

There are two common variants to \mathcal{R}_{short} . First, for simplicity, we have set $\beta + 1$ to be a power-of-2. The first variant removes this unnecessary constraint and deals with arbitrary positive integer β . This is achieved by applying the refined decomposition technique proposed in [40] and the length of the decomposed witness is $n \cdot (\lceil \log \beta \rceil + 1)$.

The second variant is to argue knowledge of a witness $\mathbf{w} \in [-\beta, \beta]^n$ that satisfies a linear equation. This can be reduced to the relation \mathcal{R}_{short} via adding β to each element of \mathbf{w} . Note that the linear equation will also need to be modified accordingly.

⁴ Detailed constructions of ZKAoKs for elementary relations can be found in Sec. 4, e.g. the ZKAoK for lattice-based PKE is in fact a ZKAoK for a variant of \mathcal{R}_{short} .

Optimized arguments for Linear Equation with Short Solution. In some cases, it is desirable to prove a relation \mathcal{R}_{short} with a large n , which makes it inefficient to decompose all elements in \mathbf{x} . We propose an alternative relation, given by Eq. (3), to argue equations with short solutions more efficiently in this case, at a cost of re-introducing some soundness gap for the argument. More precisely, to argue a linear equation $\mathbf{P}\mathbf{w} = \mathbf{v}$ with β -bounded solution \mathbf{w} , the argument can only guarantee that the prover possesses a $n \cdot \beta$ -bounded solution \mathbf{w}' that satisfies $\mathbf{P}\mathbf{w}' = \mathbf{v}$.

$$\begin{aligned} \mathcal{R}'_{short} = \{ & (\mathbf{P}, \mathbf{v}, \mathbf{H}, \mathbf{c}), (\mathbf{w}, \mathbf{u}, \mathbf{r}) \in \\ & (\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m \times [0, 1]^{\lambda \times n} \times \mathbf{C}) \times (\mathbb{Z}_q^n \times [0, n \cdot \beta]^\lambda \times \mathbf{R}) : \\ & \mathbf{P} \cdot \mathbf{w} = \mathbf{v} \wedge \mathbf{H} \cdot \mathbf{w} - \mathbf{u} = 0 \wedge \mathbf{c} = \text{Commit}(\mathbf{w}; \mathbf{r}) \} \end{aligned} \quad (3)$$

where

- **Commit** is a commitment scheme and $\mathbf{c} = \text{Commit}(\mathbf{w}; \mathbf{r})$ is the commitment;
- **C** and **R** are the output space and the randomness space of **Commit**;
- $\mathbf{H} \leftarrow H(\mathbf{c}) \in [0, 1]^{\lambda \times n}$, where λ is the security parameter and H is modeled as a random oracle.

To see why \mathcal{R}'_{short} could guarantee that all elements in \mathbf{w} are in $[0, n \cdot \beta]$, assume there exists $i \in [n]$ such that $|\mathbf{w}[i]| > n \cdot \beta$. Let \mathbf{h}_1 and \mathbf{h}_2 be two n -dimension binary vectors that are identical in all positions except that $\mathbf{h}_1[i] \neq \mathbf{h}_2[i]$. Then we have $|\mathbf{h}_1^\top \cdot \mathbf{w} - \mathbf{h}_2^\top \cdot \mathbf{w}| = |\mathbf{w}[i]| > n \cdot \beta$. Thus, either $\mathbf{h}_1^\top \cdot \mathbf{w}$ or $\mathbf{h}_2^\top \cdot \mathbf{w}$ must be outside the interval $[0, n \cdot \beta]$. Therefore, for a vector \mathbf{h} sampled uniformly from $[0, 1]^n$, with a probability of at least $1/2$, $\mathbf{h}^\top \cdot \mathbf{w} > n \cdot \beta$. Therefore, the probability that all elements in $\mathbf{H} \cdot \mathbf{w}$ are in $[0, n \cdot \beta]$ is negligible.

It remains to show how to argue the relation \mathcal{R}'_{short} . Our strategy is to reduce the relation to an instance of relation \mathcal{R}^* and then argue the instance via our main protocol. Looking ahead, in our main protocol, the prover also generates a commitment of the witness in the first step and will argue that the witness is properly committed during the proof. In addition, the commitment scheme allows one to commit part of the witness first, and then commit the remaining part later, where the partial commitment generated in the first stage is also included in the complete commitment. Consequently, the commitment and the argument for the opening of the commitment are free⁵. The remaining part of relation \mathcal{R}'_{short} are equations with short solutions, and thus can be straightforwardly reduced to \mathcal{R}^* .

In more detail, to argue \mathcal{R}'_{short} , the prover first generates the commitment $\mathbf{c} = \text{Commit}(\mathbf{w})$ and computes the matrix $\mathbf{H} = H(\mathbf{c})$ and $\mathbf{u} = \mathbf{H}\mathbf{w}$. Then, it commits \mathbf{u} and appends the commitment to \mathbf{c} . Finally, it runs the remaining part of our main protocol, arguing that there exists a small vector \mathbf{u} and a vector \mathbf{w} that satisfies $\mathbf{u} = H(\mathbf{c})\mathbf{w}$ and $\mathbf{v} = \mathbf{P}\mathbf{w}$.

⁵ In fact, we only obtain a relaxed argument for the opening of the commitment. This is sufficient for our purpose.

To summarize, we can prove equations with short solutions via our main protocol on \mathcal{R}^* , where the length of the witness is $n + \lambda \cdot (\lfloor \log(n \cdot \beta) \rfloor + 1)$ and the size of \mathcal{M} is $\lambda \cdot (\lfloor \log(n \cdot \beta) \rfloor + 1)$.

Subset Sum of Linear Equations. Let m , n and l be positive integers and q be a large power-of-prime. The relation is given as

$$\mathcal{R}_{SS} = \{(\{\mathbf{P}_i\}_{i \in [1, l]}, \mathbf{v}), (\{\mathbf{w}\}_{i \in [1, l]}, \{b_i\}_{i \in [1, l]}) \in ((\mathbb{Z}_q^{m \times n})^l \times \mathbb{Z}_q^m) \times ((\mathbb{Z}_q^n)^l \times \{0, 1\}^l) : \sum_{i=1}^l b_i \cdot \mathbf{P}_i \cdot \mathbf{w}_i = \mathbf{v}\}$$

To reduce \mathcal{R}_{SS} to \mathcal{R}^* , we first compute $\mathbf{v}_i = \mathbf{P}_i \cdot \mathbf{w}_i$ and $\mathbf{v}'_i = b_i \cdot \mathbf{v}_i$ for $i \in [1, l]$. Then we set the new witness vector $\mathbf{x} = (b_1, \dots, b_l, \mathbf{v}'_1, \dots, \mathbf{v}'_l, \mathbf{v}_1, \dots, \mathbf{v}_l, \mathbf{w}_1, \dots, \mathbf{w}_l)$ and set

$$\mathbf{A} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & -\mathbf{I}_{ml} & \mathbf{P} \\ \mathbf{0} & \mathbf{J} & \mathbf{0} & \mathbf{0} \end{pmatrix} \text{ and } \mathbf{y} = \begin{pmatrix} \mathbf{0} \\ \mathbf{v} \end{pmatrix}$$

where

$$\mathbf{P} = \begin{pmatrix} \mathbf{P}_1 & & & \\ & \mathbf{P}_2 & & \\ & & \ddots & \\ & & & \mathbf{P}_l \end{pmatrix} \text{ and } \mathbf{J} = (\mathbf{I}_m \quad \mathbf{I}_m \quad \dots \quad \mathbf{I}_m).$$

Here, the first part of the equation $\mathbf{A}\mathbf{x} = \mathbf{y}$ (specified by the first ‘‘row’’ of \mathbf{A}) indicates that $\mathbf{v}_i = \mathbf{P}_i \cdot \mathbf{w}_i$ for $i \in [1, l]$ and its second part indicates that the sum of all \mathbf{v}'_i are \mathbf{v} .

Finally, we set

$$\mathcal{M} = \{(i, i, i)\}_{i \in [1, l]} \cup \{(l + m \cdot (i - 1) + j, l + ml + m \cdot (i - 1) + j, i)\}_{i \in [1, l], j \in [1, m]}$$

where $\{(i, i, i)\}_{i \in [1, l]}$ indicates that b_i is binary and the rest indicates that $\mathbf{v}'_i = b_i \cdot \mathbf{v}_i$. This gives us an \mathcal{R}^* statement where the length of witness becomes $(nl + 2ml + l)$ and the size of \mathcal{M} is $ml + l$.

Linear Equation with Hidden Matrix. Let m and n be positive integers and q be a large power-of-prime, the relation is defined as follows:

$$\mathcal{R}_{HM} = \{(\mathbf{v}), (\mathbf{P}, \mathbf{w}) \in (\mathbb{Z}_q^m) \times (\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^n) : \mathbf{P} \cdot \mathbf{w} = \mathbf{v}\}$$

To reduce \mathcal{R}_{HM} to \mathcal{R}^* , we first obtain a new witness vector $\mathbf{x} = (\mathbf{x}_0, \dots, \mathbf{x}_{2m})$ as follows:

- $\mathbf{x}_0 = \mathbf{w}$;
- for $i \in [1, m]$, \mathbf{x}_i is the i -th row of \mathbf{P} ;
- for $i \in [1, m]$, \mathbf{x}_{m+i} is the Hadamard product between the i -th row of \mathbf{P} and \mathbf{w} (i.e., $\mathbf{x}_{m+i}[j] = \mathbf{x}_i[j] \cdot \mathbf{w}[j]$).

Then we set $\mathbf{A} = \begin{pmatrix} \mathbf{0}^{m \times n} & \mathbf{0}^{m \times mn} & \mathbf{M} \end{pmatrix}$ and $\mathbf{y} = \mathbf{v}$ where $\mathbf{M} = \mathbf{I}_m \otimes (\mathbf{1} \ \mathbf{1} \ \dots \ \mathbf{1}) \in \mathbb{Z}_q^{m \times mn}$.

Finally, we set $\mathcal{M} = \{((m+i) \cdot n + j, i \cdot n + j, j)\}_{i \in [1, m], j \in [1, n]}$, which indicates that $\mathbf{x}_{m+i}[j] = \mathbf{x}_i[j] \cdot \mathbf{w}[j]$. In this way, we obtain a new relation in the form of \mathcal{R}^* , where the length of witness is $(2m+1) \cdot n$ and the size of \mathcal{M} is mn .

2 Preliminaries

Notations. In this paper, we will use bold lower-case letters (e.g., \mathbf{v}) to denote vectors, and use bold upper-case letters (e.g., \mathbf{A}) to denote matrices. All elements in vectors and matrices are integers unless otherwise specified. For a vector \mathbf{v} of length n , we use $\mathbf{v}[i]$ to denote the i th element of \mathbf{v} for $i \in [1, n]$ and for an m -by- n matrix \mathbf{A} , we use $\mathbf{A}[i, j]$ to denote the element on the i -th row and the j -th column of \mathbf{A} for $i \in [1, m]$ and $j \in [1, n]$. For a vector \mathbf{v} , we use $\mathbf{bin}(\mathbf{v})$ to denote the binary decomposition of \mathbf{v} , i.e., $\mathbf{v}[i] = \sum_{j=1}^k 2^{j-1} \cdot \bar{\mathbf{v}}[(i-1) \cdot k + j]$, where $\bar{\mathbf{v}} = \mathbf{bin}(\mathbf{v})$ and $k = \lceil \log(\|\mathbf{v}\|_\infty) \rceil$. We use \mathbf{I}_n to denote an n -by- n identity matrix. We use \otimes to denote the Kronecker product of two matrices.

For a string a , we use $\|a\|$ to denote the length of a . For a finite set \mathcal{S} , we use $\|\mathcal{S}\|$ to denote the size of \mathcal{S} and use $s \stackrel{\$}{\leftarrow} \mathcal{S}$ to denote sampling an element s uniformly from set \mathcal{S} . For a distribution \mathcal{D} , we use $d \leftarrow \mathcal{D}$ to denote sampling d according to \mathcal{D} .

For integers $a \leq b$, we write $[a, b]$ to denote all integers from a to b . We write $\mathit{negl}(\cdot)$ to denote a negligible function and write $\mathit{poly}(\cdot)$ to denote a polynomial.

2.1 Discrete Gaussian Distribution

We recall the discrete Gaussian distribution and some results from [46].

Definition 2.1 (Discrete Gaussian Distribution). *The continuous Gaussian distribution over \mathbb{R}^m centered at $\mathbf{v} \in \mathbb{R}^m$ with standard deviation σ is defined by the function $\rho_{\mathbf{v}, \sigma}^m(\mathbf{x}) = \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^m e^{-\frac{\|\mathbf{x}-\mathbf{v}\|^2}{2\sigma^2}}$.*

The discrete Gaussian distribution over \mathbb{Z}^m centered at $\mathbf{v} \in \mathbb{Z}^m$ with standard deviation σ is defined as $D_{\mathbf{v}, \sigma}^m(\mathbf{x}) = \rho_{\mathbf{v}, \sigma}^m(\mathbf{x}) / \rho_\sigma^m(\mathbb{Z}^m)$, where $\rho_\sigma^m(\mathbb{Z}^m) = \sum_{\mathbf{x} \in \mathbb{Z}^m} \rho_\sigma^m(\mathbf{x})$.

We write $D_\sigma^m(\mathbf{x}) = D_{\mathbf{0}, \sigma}^m(\mathbf{x})$ for short.

Lemma 2.1 ([46, Full Version, Lemma 4.4]).

1. For any $k > 0$, $\Pr[\|\mathbf{z}\| > k\sigma : \mathbf{z} \leftarrow D_\sigma^1] \leq 2e^{-\frac{k^2}{2}}$.
2. For any $\mathbf{z} \in \mathbb{Z}^m$, and $\sigma \geq 3/\sqrt{2\pi}$, $D_\sigma^m(\mathbf{z}) \leq 2^{-m}$.
3. For any $k > 1$, $\Pr[\|\mathbf{z}\| > k\sigma\sqrt{m} : \mathbf{z} \leftarrow D_\sigma^m] < k^m e^{-\frac{m}{2}(1-k^2)}$.

2.2 Rejection Sampling

In this work, we will also use the celebrated “rejection sampling lemma” from [45, 46] to argue the zero-knowledge property of our protocol.

Lemma 2.2 ([46, Full Version, Theorem 4.6]). *Let \mathcal{V} be a subset of \mathbb{Z}^m in which all elements have norms less than T . Let h be a probability distribution over \mathcal{V} . Let σ be a real number that $\sigma = \omega(T\sqrt{\log m})$. Then there exists a constant M such that the distribution of the following algorithm \mathcal{A} and that of the following algorithm \mathcal{F} are within statistical distance $\frac{2^{-\omega(\log m)}}{M}$.*

\mathcal{A} :

1. $\mathbf{v} \leftarrow h$
2. $\mathbf{z} \leftarrow D_{\mathbf{v}, \sigma}^m$
3. Output (\mathbf{v}, \mathbf{z}) with probability $\min(1, \frac{D_{\mathbf{v}, \sigma}^m(\mathbf{z})}{MD_{\mathbf{v}, \sigma}^m(\mathbf{z})})$

\mathcal{F} :

1. $\mathbf{v} \leftarrow h$
2. $\mathbf{z} \leftarrow D_{\sigma}^m$
3. Output (\mathbf{v}, \mathbf{z}) with probability $\frac{1}{M}$

Moreover, the probability that \mathcal{A} outputs something is at least $\frac{1-2^{-\omega(\log m)}}{M}$.

As a concrete example (suggested in [30]), if $\sigma = \alpha T$ for some positive α , then $M = e^{13.3/\alpha+1/(2\alpha^2)}$, the output of algorithm \mathcal{A} is within statistical distance $\frac{2^{-128}}{M}$ of the output of \mathcal{F} , and the probability that \mathcal{A} outputs something is at least $\frac{1-2^{-128}}{M}$.

2.3 Hardness Assumptions

The security of our main protocol relies on the short integer solution (SIS) assumption and the learning with errors (LWE) assumption. For both assumptions, we will use the normal form (as defined in [53]).

Definition 2.2 (SIS $_{n,m,q,\beta}$, Normal Form). *Given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times (m-n)}$, find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m$ such that $\|\mathbf{z}\| \leq \beta$ and $[\mathbf{I}_n \mid \mathbf{A}] \cdot \mathbf{z} = 0$.*

As hardness of the SIS assumption usually depends only on n, q, β (assuming m is large enough), in this work, we write SIS $_{n,m,q,\beta}$ as SIS $_{n,q,\beta}$ for short.

Lemma 2.3 ([1, 22, 48, 49, 53]). *For any $m = \text{poly}(n)$, any $\beta > 0$, and any sufficiently large $q \geq \beta \cdot \tilde{O}(\sqrt{n})$, solving (normal form) SIS $_{n,m,q,\beta}$ with non-negligible probability is at least as hard as solving the decisional approximate shortest vector problem GapSVP $_{\gamma}$ and the approximate shortest independent vectors problems SIVP $_{\gamma}$ (among others) on arbitrary n -dimensional lattices (i.e., in the worst case) with overwhelming probability, for some $\gamma = \beta \cdot \tilde{O}(\sqrt{n})$.*

Definition 2.3 (Decision-LWE $_{n,m,q,\chi}$, Normal Form). *Given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{(m-n) \times n}$, and a vector $\mathbf{b} \in \mathbb{Z}_q^{m-n}$, where \mathbf{b} is generated according to either of the following two cases:*

1. $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$, where $\mathbf{s} \leftarrow \chi^n$ and $\mathbf{e} \leftarrow \chi^{m-n}$

2. $\mathbf{b} \xleftarrow{\$} \mathbb{Z}_q^{m-n}$

distinguish which is the case with non-negligible advantage.

If χ is a discrete Gaussian distribution with standard deviation σ , we write the problem as $LWE_{n,m,q,\alpha}$ where $\alpha = \sigma \cdot \sqrt{2\pi}/q$. Also, as the hardness of the LWE assumption usually depends only on n, q, α (assuming m is large enough), in this work, we write $LWE_{n,m,q,\alpha}$ as $LWE_{n,q,\alpha}$ for short.

Lemma 2.4 ([4, 53, 55]). *For any $m = \text{poly}(n)$, any modulus $q \leq 2^{\text{poly}(n)}$, and any (discrete) Gaussian error distribution χ with standard deviation σ (i.e., $\chi = D_\sigma$), where $\sigma = \alpha q / \sqrt{2\pi} \geq \sqrt{2n/\pi}$ and $0 < \alpha < 1$, solving the (normal form) decision-LWE $_{n,m,q,\chi}$ problem is at least as hard as (quantumly) solving GapSVP $_\gamma$ and SIVP $_\gamma$ on arbitrary n -dimensional lattices, for some $\gamma = \tilde{O}(n/\alpha)$.*

2.4 Zero-Knowledge Arguments of Knowledge

In a zero-knowledge argument of knowledge system [24], a prover proves to a verifier that he possesses the witness for a statement without revealing any additional information.

More formally, let $\mathbf{R} = \{(x, w)\} \in \{0, 1\}^* \times \{0, 1\}^*$ be a statements-witnesses set for an NP relation. The ZKAoK for \mathbf{R} is an interactive protocol $\langle \mathcal{P}, \mathcal{V} \rangle$ run between a prover \mathcal{P} and a verifier \mathcal{V} that satisfies:

- **Completeness.** For any $(x, w) \in \mathbf{R}$, $\Pr[\langle \mathcal{P}(x, w), \mathcal{V}(x) \rangle \neq 1] \leq \delta_c$.
- **Proof of Knowledge.** There exists an extractor \mathcal{E} that for any x , for any probabilistic polynomial time (PPT) cheating prover $\hat{\mathcal{P}}$, if $\Pr[\langle \hat{\mathcal{P}}, \mathcal{V}(x) \rangle = 1] > \delta_s + \epsilon$ for some non-negligible ϵ , then \mathcal{E} can extract in polynomial time a witness w such that $(x, w) \in \mathbf{R}$ via accessing $\hat{\mathcal{P}}$ in a black-box manner.
- **(Honest-Verifier) Zero-Knowledge.** There exists a simulator \mathcal{S} that for any $(x, w) \in \mathbf{R}$, the two distributions are computationally indistinguishable:
 1. The view of an honest verifier \mathcal{V} in an interaction $\langle \mathcal{P}(x, w), \mathcal{V}(x) \rangle$.
 2. The output of $\mathcal{S}(x)$.

where δ_c is the completeness error and δ_s is the soundness error.

In this work, we also consider non-interactive ZKAoKs (NIZKAoK). They can be obtained by applying the Fiat-Shamir heuristic [20] to public coin ZKAoKs. One advantage led by the Fiat-Shamir transform is that the transformed NIZKAoKs additionally admit a message as input, thus it is also called signature proof of knowledge (SPK), and is usually written as $SPK\{(x, w) : (x, w) \in \mathbf{R}\}[m]$, where m is the additional message.

2.5 Commitment with A Relaxed Opening

In our main construction, we will employ the commitment scheme presented in [6]⁶, which admits a relaxed opening.

⁶ In fact, we will use its variant in the standard lattice setting. For completeness, we will restate its security in the security proof of our main construction.

Let λ be the security parameter. Let l_1 and l_2 be positive integers that are polynomials in the security parameter λ . Let σ be a small positive integer that satisfies $\sigma \geq \sqrt{2l_2/\pi}$. Also, let n be the length of the committed vector. The public parameter of the commitment scheme is a matrix $\mathbf{B} \in \mathbb{Z}_q^{(l_1+n) \times (l_1+n+l_2)}$ defined as follows:

$$\mathbf{B} = \left(\begin{array}{c|cc} \mathbf{I}_{l_1} & & \mathbf{B}_1 \\ \hline 0^{n \times l_1} & \mathbf{I}_n & \mathbf{B}_2 \end{array} \right)$$

where \mathbf{B}_1 and \mathbf{B}_2 are random matrices sampled from $\mathbb{Z}_q^{l_1 \times (l_2+n)}$ and $\mathbb{Z}_q^{n \times l_2}$ respectively.

To commit to a message $\mathbf{m} \in \{0,1\}^n$, the commit algorithm first samples $\mathbf{s} \in D_\sigma^{l_1+n+l_2}$. Then it outputs a commitment $\mathbf{c} = \mathbf{B} \cdot \mathbf{s} + (\mathbf{0}^\top \parallel \mathbf{m}^\top)^\top$ and the opening \mathbf{s} .

The open algorithm outputs 1 on input $\mathbf{B}, \mathbf{m}, \mathbf{c}, \mathbf{s}$ iff $\mathbf{c} = \mathbf{B} \cdot \mathbf{s} + (\mathbf{0}^\top \parallel \mathbf{m}^\top)^\top$ and \mathbf{s} is small. Besides, it admits a relaxed opening, where the input of the algorithm includes $\mathbf{B}, \mathbf{m}, \mathbf{c}, \mathbf{s}$ and a small integer f , and the algorithm outputs 1 iff $f \cdot \mathbf{c} = \mathbf{B} \cdot \mathbf{s} + f \cdot (\mathbf{0}^\top \parallel \mathbf{m}^\top)^\top$ and \mathbf{s}, f are small.

3 Main Construction

In this section, we present our main construction, namely, an efficient zero-knowledge argument of knowledge for linear equations with quadratic constraints over the witness.

More concretely, let m, n, ℓ be positive integers, q be a large enough integer that is a *power-of-prime*, i.e., $q = q_0^e$ for some prime q_0 and some positive integer e . Also, let \mathbf{A} be a matrix in $\mathbb{Z}_q^{m \times n}$, \mathbf{x} and \mathbf{y} be vectors in \mathbb{Z}_q^n and \mathbb{Z}_q^m respectively, and \mathcal{M} be a set of ℓ 3-tuples, each of which consists of 3 integers in $[1, n]$. We will construct a ZKAoK for the following relation:

$$\mathcal{R}^* = \{(\mathbf{A}, \mathbf{y}, \mathcal{M}), (\mathbf{x}) : \mathbf{A} \cdot \mathbf{x} = \mathbf{y} \wedge \forall (h, i, j) \in \mathcal{M}, \mathbf{x}[h] = \mathbf{x}[i] \cdot \mathbf{x}[j]\} \quad (4)$$

Specifically, in Sec. 3.1, we give a basic version of the ZKAoK protocol for \mathcal{R}^* as defined in Eq. (4). This protocol achieves an inverse polynomial soundness error and a constant completeness error. Then, in Sec. 3.2, we transform the basic protocol into a NIZKAoK with negligible soundness error and completeness error.

3.1 The Basic Protocol

Let `aCommit` be an auxiliary bit commitment scheme with randomness space $\{0,1\}^\kappa$ and a suitable message space. As no additional requirement is desired for `aCommit`, we can safely assume it to be a random oracle G , i.e., given an input x and a random string ρ as randomness, the commitment is $G(x \parallel \rho)$. Nonetheless, `aCommit` can be instantiated by any secure commitment scheme.

Let λ be the security parameter. Let l_1 and l_2 be positive integers that are polynomials in the security parameter λ . Let $\mathbf{B}_{1,1}, \mathbf{B}_{1,2}, \mathbf{B}_{2,1}$ and $\mathbf{B}_{2,2}$

be random matrices sampled from $\mathbb{Z}_q^{l_1 \times (l_2+n)}$, $\mathbb{Z}_q^{n \times l_2}$, $\mathbb{Z}_q^{l_1 \times (l_2+\ell)}$ and $\mathbb{Z}_q^{\ell \times l_2}$ respectively. Also let

$$\mathbf{B}_1 = \left(\begin{array}{c|c} \mathbf{I}_{l_1} & \mathbf{B}_{1,1} \\ \hline 0^{n \times l_1} & \mathbf{I}_n \mathbf{B}_{1,2} \end{array} \right), \quad \mathbf{B}_2 = \left(\begin{array}{c|c} \mathbf{I}_{l_1} & \mathbf{B}_{2,1} \\ \hline 0^{\ell \times l_1} & \mathbf{I}_\ell \mathbf{B}_{2,2} \end{array} \right)$$

Here \mathbf{B}_1 and \mathbf{B}_2 are public parameters of the underlying homomorphic commitment scheme, and we assume that they are honestly generated (via some public coin) and are shared by all parties in the protocol.

Let σ_1 be small positive integer that satisfies $\sigma_1 \geq \sqrt{2l_2/\pi}$. Let p be small positive integer that is polynomial in λ . Let $l = 2l_1 + 2l_2 + n + \ell$. Let $\sigma_2 = 2p \cdot \sqrt{l} \cdot \log l \cdot \sigma_1$. Let $M = e^{13.3/\log l + 1/(2 \log^2 l)}$. For any l -dimension vectors \mathbf{v} and \mathbf{z} , let $\mathfrak{p}(\mathbf{v}, \mathbf{z}) = \min(1, \frac{D_{\sigma_2}^l(\mathbf{z})}{MD_{\mathbf{v}, \sigma_2}^l(\mathbf{z})})$.

The basic protocol P_1 for \mathcal{R}^* is described in Figure 2.

Theorem 3.1. *Assume the worst-case hardness of GapSVP_γ (or SIVP_γ) for some polynomial γ , if $q \geq 16p \cdot \max(\sqrt{l_1 + l_2 + n}, \sqrt{l_1 + l_2 + \ell}) \cdot (\sigma_2 + p \cdot \sigma_1) \cdot \tilde{O}(\sqrt{l_1})$, q/σ_1 is a polynomial, $q_0 > 2p$, and aCommit is a secure bit commitment scheme, then the protocol P_1 , which is described in Figure 2, is a secure zero-knowledge argument of knowledge with completeness error $1 - 1/M$ and soundness error $2/(2p + 1)$.*

We give the detailed proof for Theorem 3.1 in the full version.

3.2 NIZKAoK for \mathcal{R}^*

In this section, we show how to transform our basic protocol in Sec. 3.1 into a non-interactive zero-knowledge arguments of knowledge with negligible soundness error and completeness error. Generally, this can be done via some standard techniques such as repetition and Fiat-Shamir transform. Nonetheless, we will employ a few tricks (developed in previous works) to reduce the efficiency loss in the transformations. In particular, to minimize the number of repetitions, we will employ the tweaks in [19] when repeating the basic protocol. In a nutshell, it applies one rejection sampling on all (repeated) instances simultaneously, which avoids completeness error increasing caused by repetition.

The Construction. Let aCommit , λ , l_1 , l_2 , $\mathbf{B}_{1,1}$, $\mathbf{B}_{1,2}$, $\mathbf{B}_{2,1}$ and $\mathbf{B}_{2,2}$, σ_1 , p , l and M be identical to those of P_1 . We highlight the differences.

In the new scheme, a proof is generated by repeating the basic protocol $N = \lambda/\log p$ times. Then we set $\sigma_2 = 2p \cdot \sqrt{N \cdot l} \cdot \log(N \cdot l) \cdot \sigma_1$, and for any $N \cdot l$ -dimension vectors \mathbf{v} and \mathbf{z} , we set $\mathfrak{p}(\mathbf{v}, \mathbf{z}) = \min(1, \frac{D_{\sigma_2}^{N \cdot l}(\mathbf{z})}{MD_{\mathbf{v}, \sigma_2}^{N \cdot l}(\mathbf{z})})$. We will additionally use a hash function H with output space $[-p, p]^N$, which is modelled as a random oracle. Also, let AUX be some application-dependent auxiliary information (e.g., the signed message in a group signature) that is specified as an input to H .

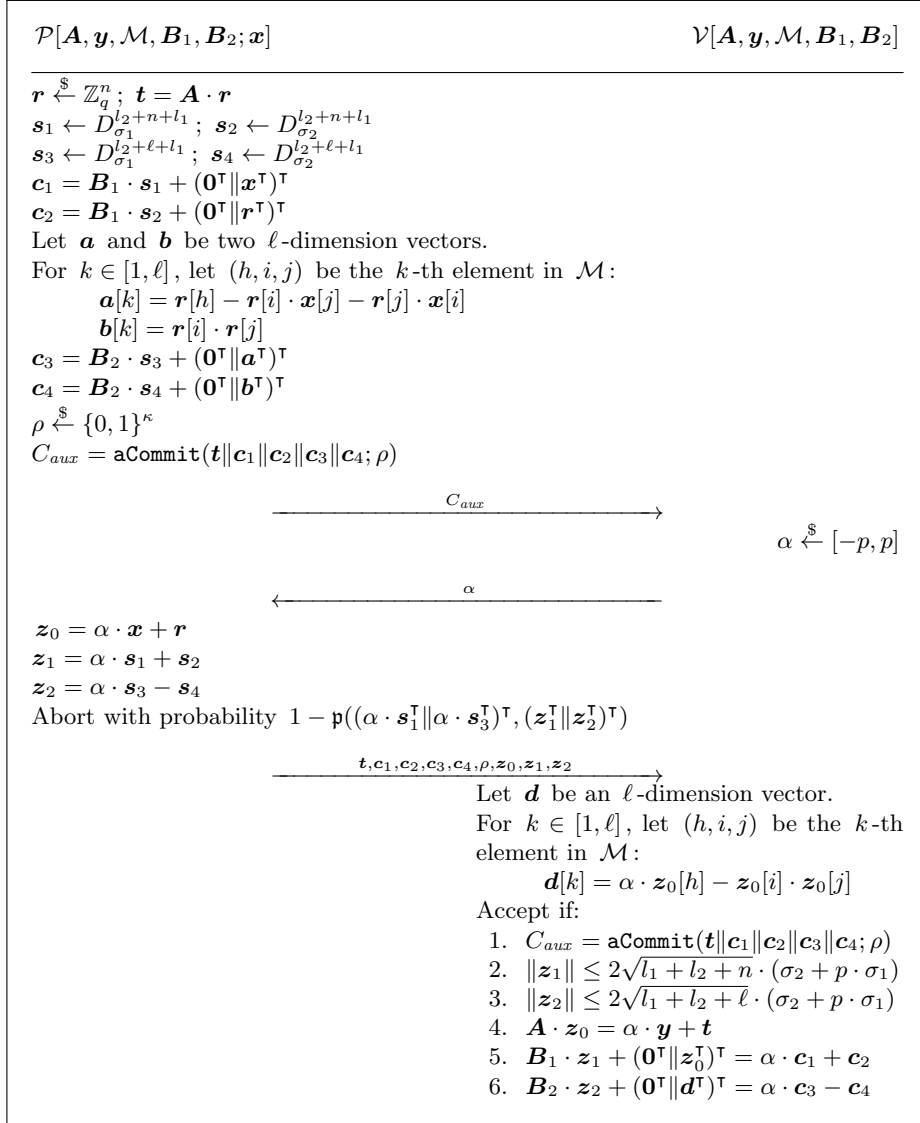


Fig. 2 The Basic Protocol \mathcal{P}_1 : A Zero-Knowledge Arguments of Knowledge for \mathcal{R}^* with Inverse Polynomial Soundness Error and Constant Completeness Error.

The prove algorithm and the verify algorithm of the NIZKAoK \mathcal{P}_2 for \mathcal{R}^* is described in Figure 3 and 4 respectively.

Theorem 3.2. Assume the worst-case hardness of GapSVP_γ (or SIVP_γ) for some polynomial γ , if $q \geq 16p \cdot \max(\sqrt{l_1 + l_2 + n}, \sqrt{l_1 + l_2 + \ell}) \cdot (\sigma_2 + p \cdot \sigma_1) \cdot \tilde{O}(\sqrt{l_1})$, q/σ_1 is a polynomial, $q_0 > 2p$, $\mathbf{aCommit}$ is a secure bit commitment

Prove($\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathcal{M}, \mathbf{B}_1, \mathbf{B}_2, AUX$):

For $j \in [1, \lambda]$:

1. $\mathbf{s}_1 \leftarrow D_{\sigma_1}^{l_2+n+l_1}$, $\mathbf{c}_1 = \mathbf{B}_1 \cdot \mathbf{s}_1 + (\mathbf{0}^\top \|\mathbf{x}^\top)^\top$
2. For $i \in [1, N]$:
 - (a) $\mathbf{r}_i \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{t}_i = \mathbf{A} \cdot \mathbf{r}_i$
 - (b) $\mathbf{s}_{2,i} \leftarrow D_{\sigma_2}^{l_2+n+l_1}$, $\mathbf{s}_{3,i} \leftarrow D_{\sigma_1}^{l_2+l+l_1}$, $\mathbf{s}_{4,i} \leftarrow D_{\sigma_2}^{l_2+l+l_1}$
 - (c) $\mathbf{c}_{2,i} = \mathbf{B}_1 \cdot \mathbf{s}_{2,i} + (\mathbf{0}^\top \|\mathbf{r}_i^\top)^\top$
 - (d) Let \mathbf{a}_i and \mathbf{b}_i be two ℓ -dimension vectors and for $k \in [1, \ell]$, let (h, i, j) be the k -th element in \mathcal{M} :
 - i. $\mathbf{a}_i[k] = \mathbf{r}_i[h] - \mathbf{r}_i[i] \cdot \mathbf{x}[j] - \mathbf{r}_i[j] \cdot \mathbf{x}[i]$
 - ii. $\mathbf{b}_i[k] = \mathbf{r}_i[i] \cdot \mathbf{r}_i[j]$
 - (e) $\mathbf{c}_{3,i} = \mathbf{B}_2 \cdot \mathbf{s}_{3,i} + (\mathbf{0}^\top \|\mathbf{a}_i^\top)^\top$, $\mathbf{c}_{4,i} = \mathbf{B}_2 \cdot \mathbf{s}_{4,i} + (\mathbf{0}^\top \|\mathbf{b}_i^\top)^\top$
 - (f) $\rho_i \xleftarrow{\$} \{0, 1\}^\kappa$
 - (g) $C_{aux,i} = \mathbf{aCommit}(\mathbf{t}_i \|\mathbf{c}_1 \|\mathbf{c}_{2,i} \|\mathbf{c}_{3,i} \|\mathbf{c}_{4,i}; \rho_i)$
3. $\{\alpha_i\}_{i \in [1, N]} = H(\mathbf{A}, \mathbf{y}, \mathcal{M}, \{C_{aux,i}\}_{i \in [1, N]}, AUX)$
4. For $i \in [1, N]$:
 - (a) $\mathbf{z}_{0,i} = \alpha_i \cdot \mathbf{x} + \mathbf{r}_i$, $\mathbf{z}_{1,i} = \alpha_i \cdot \mathbf{s}_1 + \mathbf{s}_{2,i}$, $\mathbf{z}_{2,i} = \alpha_i \cdot \mathbf{s}_{3,i} - \mathbf{s}_{4,i}$
5. Sample a real number $\tau \xleftarrow{\$} [0, 1]$ (Here, we use $[0, 1]$ to denote all real numbers between 0 and 1)
6. If $\tau < \mathbf{p}((\alpha_1 \cdot \mathbf{s}_1^\top \|\dots \|\alpha_N \cdot \mathbf{s}_1^\top \|\alpha_1 \cdot \mathbf{s}_{3,1}^\top \|\dots \|\alpha_N \cdot \mathbf{s}_{3,N}^\top)^\top, (\mathbf{z}_{1,1}^\top \|\dots \|\mathbf{z}_{1,N}^\top \|\mathbf{z}_{2,1}^\top \|\dots \|\mathbf{z}_{2,N}^\top)^\top)$:
 - (a) Abort the algorithm with output $\pi = (\mathbf{c}_1, \{\alpha_i, \rho_i, \mathbf{c}_{3,i}, \mathbf{z}_{0,i}, \mathbf{z}_{1,i}, \mathbf{z}_{2,i}\}_{i \in [1, N]})$

Output \perp if the algorithm does not abort in the loop above.

Fig. 3 The Prove Algorithm of P_2 .

Verify($\mathbf{A}, \mathbf{y}, \mathcal{M}, \mathbf{B}_1, \mathbf{B}_2, AUX, \pi = (\mathbf{c}_1, \{\alpha_i, \rho_i, \mathbf{c}_{3,i}, \mathbf{z}_{0,i}, \mathbf{z}_{1,i}, \mathbf{z}_{2,i}\}_{i \in [1, N]})$):

For $i \in [1, N]$:

1. Let \mathbf{d}_i be an ℓ -dimension vector and for $k \in [1, \ell]$, let (h, i, j) be the k -th element in \mathcal{M} :
 - (a) $\mathbf{d}_i[k] = \alpha_i \cdot \mathbf{z}_{0,i}[h] - \mathbf{z}_{0,i}[i] \cdot \mathbf{z}_{0,i}[j]$
2. $\mathbf{t}_i = \mathbf{A} \cdot \mathbf{z}_{0,i} - \alpha_i \cdot \mathbf{y}$
3. $\mathbf{c}_{2,i} = \mathbf{B}_1 \cdot \mathbf{z}_{1,i} + (\mathbf{0}^\top \|\mathbf{z}_{0,i}^\top)^\top - \alpha_i \cdot \mathbf{c}_1$
4. $\mathbf{c}_{4,i} = \alpha_i \cdot \mathbf{c}_{3,i} - \mathbf{B}_2 \cdot \mathbf{z}_{2,i} - (\mathbf{0}^\top \|\mathbf{d}_i^\top)^\top$
5. $C_{aux,i} = \mathbf{aCommit}(\mathbf{t}_i \|\mathbf{c}_1 \|\mathbf{c}_{2,i} \|\mathbf{c}_{3,i} \|\mathbf{c}_{4,i}; \rho_i)$
6. If $\|\mathbf{z}_{1,i}\| > 2\sqrt{l_1 + l_2 + n} \cdot (\sigma_2 + p \cdot \sigma_1) \vee \|\mathbf{z}_{2,i}\| > 2\sqrt{l_1 + l_2 + \ell} \cdot (\sigma_2 + p \cdot \sigma_1)$:
 - (a) Abort the algorithm with output “Reject”

Output “Accept” if $\{\alpha_i\}_{i \in [1, N]} = H(\mathbf{A}, \mathbf{y}, \mathcal{M}, \{C_{aux,i}\}_{i \in [1, N]}, AUX)$:

Fig. 4 The Verify Algorithm of P_2 .

scheme, and H is modelled as a random oracle, then the scheme P_2 is a secure

non-interactive zero-knowledge argument of knowledge with negligible completeness error and soundness error.

Proof of Theorem 3.2 follows proof of Theorem 3.1 and well-known results, we omit the details here.

Efficiency. In P_2 , a proof π contains a commitment and a set of N elements, where each element consists of a challenge, a κ -bit string, a commitment and three vectors. Thus, we have

$$\|\pi\| = (\log(2p+1) + \kappa + (3l_1 + 2l_2 + 2n + 2\ell) \cdot \log q) \cdot N + (l_1 + n) \cdot \log q$$

4 ZKAoKs for Various Cryptographic Schemes

In this section, we build several tools that are useful for constructing privacy-preserving primitives. This includes an argument of knowledge of committed value, an argument of knowledge of plaintext, an argument of knowledge of signature, an argument for cryptographic accumulator and an argument for pseudorandom function.

4.1 ZKAoK of Committed Value

We start with an argument of knowledge of the committed value for the commitment scheme in [31].

Let l_1, l_2, L be positive integers and q be a power-of-prime. We propose a ZKAoK for the following relation:

$$\mathcal{R}_{com} = \{(\mathbf{B}_1, \mathbf{B}_2, \mathbf{c}), (\mathbf{r}, \mathbf{w}) \in (\mathbb{Z}_q^{l_1 \times l_2} \times \mathbb{Z}_q^{l_1 \times L} \times \mathbb{Z}_q^{l_1}) \times (\{0, 1\}^{l_2} \times \{0, 1\}^L) : \mathbf{B}_1 \cdot \mathbf{r} + \mathbf{B}_2 \cdot \mathbf{w} = \mathbf{c}\}$$

\mathcal{R}_{com} contains linear equations with binary witness. We construct the argument via reducing \mathcal{R}_{com} to an instance of \mathcal{R}^* through the following steps:

1. Set the new witness $\mathbf{x} = (\mathbf{r}^\top \parallel \mathbf{w}^\top)^\top$;
2. Set $\mathbf{A} = (\mathbf{B}_1 \parallel \mathbf{B}_2)$ and $\mathbf{y} = \mathbf{c}$;
3. Set $\mathcal{M} = (i, i, i)_{i \in [1, l_2 + L]}$.

Note that since q is a power of prime, for any $x \in \mathbb{Z}_q$, $x^2 = x$ iff $x = 0$ or $x = 1$. Thus, the new relation \mathcal{R}^* over $(\mathbf{A}, \mathbf{y}, \mathcal{M}), (\mathbf{x})$ is equivalent to the original relation \mathcal{R}_{com} . Also, both $\|\mathbf{x}\|$ and $\|\mathcal{M}\|$ are $l_2 + L$ for \mathcal{R}^* .

4.2 ZKAoK of Plaintext

Next, we give an argument of knowledge of the plaintext for the encryption scheme proposed in [39].

More precisely, let l_1, l_2, L and β be positive integers and q be a power-of-prime, we propose a ZKAoK for the following relation:

$$\begin{aligned}
\mathcal{R}_{enc} = \{ & (\mathbf{B}_1, \mathbf{B}_2, \mathbf{c}_1, \mathbf{c}_2), (\mathbf{r}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{w}) \in \\
& (\mathbb{Z}_q^{l_1 \times l_2} \times \mathbb{Z}_q^{L \times l_2} \times \mathbb{Z}_q^{l_1} \times \mathbb{Z}_q^L) \times (\mathbb{Z}_q^{l_2} \times \mathbb{Z}_q^{l_1} \times \mathbb{Z}_q^L \times \{0, 1\}^L) : \\
& \|\mathbf{r}\|_\infty \leq \beta \wedge \|\mathbf{e}_1\|_\infty \leq \beta \wedge \|\mathbf{e}_2\|_\infty \leq \beta \wedge \\
& \mathbf{B}_1 \cdot \mathbf{r} + \mathbf{e}_1 = \mathbf{c}_1 \wedge \mathbf{B}_2 \cdot \mathbf{r} + \mathbf{e}_2 + \lfloor \frac{q}{2} \rfloor \cdot \mathbf{w} = \mathbf{c}_2 \}
\end{aligned}$$

We construct the argument via reducing the relation \mathcal{R}_{enc} , which contains linear equations with short solutions, to an instance of the relation \mathcal{R}^* .

First, we define vectors $\beta_1 = (\beta \ \beta \dots \beta)^\top \in \mathbb{Z}_q^{l_2}$, $\beta_2 = (\beta \ \beta \dots \beta)^\top \in \mathbb{Z}_q^{l_1}$, $\beta_3 = (\beta \ \beta \dots \beta)^\top \in \mathbb{Z}_q^L$ and define $\mathbf{r}' = \mathbf{r} + \beta_1$, $\mathbf{e}'_1 = \mathbf{e}_1 + \beta_2$ and $\mathbf{e}'_2 = \mathbf{e}_2 + \beta_3$.

Then, we decompose vectors \mathbf{r}' , \mathbf{e}'_1 and \mathbf{e}'_2 into binary vectors $\bar{\mathbf{r}}$, $\bar{\mathbf{e}}_1$ and $\bar{\mathbf{e}}_2$ using the decomposition technique proposed in [40]. More precisely, let $k = \lfloor \log 2\beta \rfloor + 1$ and let $\mathbf{g} = (\lfloor (2\beta + 1)/2 \rfloor \lfloor (2\beta + 2)/4 \rfloor \dots \lfloor (2\beta + 2^{i-1})/2^i \rfloor \dots \lfloor (2\beta + 2^{k-1})/2^k \rfloor)$ be a row vector. It is claimed in [40] that 1) an integer $a \in [0, 2\beta]$ iff there exists a binary vector $\mathbf{a} \in \{0, 1\}^k$ that $\mathbf{g} \cdot \mathbf{a} = a$; 2) one can decompose the integer $a \in [0, 2\beta]$ into the k -dimension binary vector \mathbf{a} efficiently.

Next, we define the gadget matrix $\mathbf{G}_1 = \mathbf{I}_{l_2} \otimes \mathbf{g}$, $\mathbf{G}_2 = \mathbf{I}_{l_1} \otimes \mathbf{g}$, $\mathbf{G}_3 = \mathbf{I}_L \otimes \mathbf{g}$ and they satisfy that $\mathbf{G}_1 \cdot \bar{\mathbf{r}} = \mathbf{r}'$, $\mathbf{G}_2 \cdot \bar{\mathbf{e}}_1 = \mathbf{e}'_1$ and $\mathbf{G}_3 \cdot \bar{\mathbf{e}}_2 = \mathbf{e}'_2$.

Finally, we set

$$\mathbf{A} = \begin{pmatrix} \mathbf{B}_1 \cdot \mathbf{G}_1 & \mathbf{G}_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{B}_2 \cdot \mathbf{G}_1 & \mathbf{0} & \mathbf{G}_3 & \lfloor \frac{q}{2} \rfloor \cdot \mathbf{I}_L \end{pmatrix}$$

$$\mathbf{x} = (\bar{\mathbf{r}}^\top \quad \bar{\mathbf{e}}_1^\top \quad \bar{\mathbf{e}}_2^\top \quad \mathbf{w}^\top)^\top, \quad \mathbf{y} = \begin{pmatrix} \mathbf{c}_1 + \mathbf{B}_1 \cdot \beta_1 + \beta_2 \\ \mathbf{c}_2 + \mathbf{B}_2 \cdot \beta_1 + \beta_3 \end{pmatrix}$$

and set $\mathcal{M} = (i, i, i)_{i \in [1, (l_1 + l_2 + L) \cdot k + L]}$. Here, both $\|\mathbf{x}\|$ and $\|\mathcal{M}\|$ are $(l_1 + l_2 + L) \cdot k + L$.

One common variant of the encryption scheme in [39] is to use binary secrets and errors rather than sampling them from β bounded distributions. To generate arguments of knowledge of plaintexts for this variant, we can use an almost identical construction as above, except that we do not need to decompose the vectors \mathbf{r} , \mathbf{e}_1 and \mathbf{e}_2 . Thus, when reducing the relation to \mathcal{R}^* in this case, both $\|\mathbf{x}\|$ and $\|\mathcal{M}\|$ will be $l_1 + l_2 + 2L$.

4.3 ZKAoK of Message-Signature Pair

Next, we give an argument of knowledge of a valid message/signature pair for the signature scheme proposed in [37].

Let l_1 , l_2 , l_3 , L , and β be positive integers and q be a power-of-prime. Also let $k_q = \lceil \log q \rceil$. We propose a ZKAoK that proves knowledge of

$$\begin{cases} \{\tau_i\}_{i \in [1, l_3]} \in \{0, 1\}^{l_3}; \mathbf{v}_1 \in \mathbb{Z}_q^{l_2}; \mathbf{v}_2 \in \mathbb{Z}_q^{l_2}; \\ \mathbf{w} \in \{0, 1\}^{k_q l_1}; \mathbf{s} \in \mathbb{Z}_q^{2l_2}; \mathbf{m} \in \{0, 1\}^L \end{cases}$$

that satisfies

$$\begin{cases} \mathbf{B} \cdot \mathbf{v}_1 + (\mathbf{B}_0 + \sum_{i=1}^{l_3} \tau_i \cdot \mathbf{B}_i) \cdot \mathbf{v}_2 = \mathbf{u} + \mathbf{D} \cdot \mathbf{w} \\ \mathbf{H} \cdot \mathbf{w} = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot \mathbf{m} \\ \|\mathbf{v}_1\|_\infty \leq \beta; \|\mathbf{v}_2\|_\infty \leq \beta; \|\mathbf{s}\|_\infty \leq \beta \end{cases}$$

for public

$$\begin{cases} \mathbf{B} \in \mathbb{Z}_q^{l_1 \times l_2}; \{\mathbf{B}_i\}_{i \in [0, l_3]} \in (\mathbb{Z}_q^{l_1 \times l_2})^{l_3+1}; \mathbf{u} \in \mathbb{Z}_q^{l_1} \\ \mathbf{D} \in \mathbb{Z}_q^{l_1 \times k_q l_1}; \mathbf{D}_0 \in \mathbb{Z}_q^{l_1 \times 2l_2}; \mathbf{D}_1 \in \mathbb{Z}_q^{l_1 \times L} \end{cases}$$

where $\mathbf{H} = \mathbf{I}_{l_1} \otimes (1 \ 2 \ 4 \dots 2^{k_q-1})$.

Again, we construct the argument via reducing the relation, which contains a subset sum of linear equations and linear equations with short solutions, to an instance of the relation \mathcal{R}^* .

First, we define vectors $\beta_1 = (\beta \ \beta \dots \beta)^\top \in \mathbb{Z}_q^{l_2}$, $\beta_2 = (\beta \ \beta \dots \beta)^\top \in \mathbb{Z}_q^{2l_2}$, and define $\mathbf{v}'_1 = \mathbf{v}_1 + \beta_1$, $\mathbf{v}'_2 = \mathbf{v}_2 + \beta_2$ and $\mathbf{s}' = \mathbf{s} + \beta_2$.

Then, we decompose vectors \mathbf{v}'_1 , \mathbf{v}'_2 and \mathbf{s}' into binary vectors $\bar{\mathbf{v}}_1$, $\bar{\mathbf{v}}_2$, and $\bar{\mathbf{s}}$ using the decomposition technique proposed in [40]. Let $k = \lceil \log 2\beta \rceil + 1$, then the vectors $\bar{\mathbf{v}}_1$, $\bar{\mathbf{v}}_2$ and $\bar{\mathbf{s}}$ are of length kl_2 , kl_2 and $2kl_2$ respectively.

Also, let $\mathbf{g} = (\lfloor (2\beta + 1)/2 \rfloor \dots \lfloor (2\beta + 2^{i-1})/2^i \rfloor \dots \lfloor (2\beta + 2^{k-1})/2^k \rfloor)$ be a row vector. Then, we define the gadget matrix $\mathbf{G}_1 = \mathbf{I}_{l_2} \otimes \mathbf{g}$, $\mathbf{G}_2 = \mathbf{I}_{2l_2} \otimes \mathbf{g}$, and they satisfy that $\mathbf{G}_1 \cdot \bar{\mathbf{v}}_1 = \mathbf{v}'_1$, $\mathbf{G}_1 \cdot \bar{\mathbf{v}}_2 = \mathbf{v}'_2$ and $\mathbf{G}_2 \cdot \bar{\mathbf{s}} = \mathbf{s}'$.

Next, for $i \in [1, l_3]$, let $\mathbf{u}_i = \mathbf{B}_i \cdot \mathbf{v}_2$ and let $\mathbf{u}'_i = \tau_i \cdot \mathbf{u}_i$. Also, we define $\hat{\mathbf{u}} = (\mathbf{u}_1^\top \|\mathbf{u}_2^\top \|\dots \|\mathbf{u}_{l_3}^\top)^\top$ and $\hat{\mathbf{u}}' = (\mathbf{u}'_1^\top \|\mathbf{u}'_2^\top \|\dots \|\mathbf{u}'_{l_3}^\top)^\top$. Moreover, define $\boldsymbol{\tau} = (\tau_1 \ \tau_2 \dots \tau_{l_3})^\top$.

Finally, we set

$$\mathbf{A} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & -\mathbf{I}_{l_1 l_3} & \bar{\mathbf{B}} \cdot \mathbf{G}_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{J} & \mathbf{0} & \mathbf{B}_0 \cdot \mathbf{G}_1 & \mathbf{B} \cdot \mathbf{G}_1 & -\mathbf{D} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & -\mathbf{H} & \mathbf{D}_0 \cdot \mathbf{G}_2 & \mathbf{D}_1 \end{pmatrix}$$

$$\mathbf{x} = (\boldsymbol{\tau}^\top \ \hat{\mathbf{u}}'^\top \ \hat{\mathbf{u}}^\top \ \bar{\mathbf{v}}_2^\top \ \bar{\mathbf{v}}_1^\top \ \mathbf{w}^\top \ \bar{\mathbf{s}}^\top \ \mathbf{m}^\top)^\top, \quad \mathbf{y} = \begin{pmatrix} \bar{\mathbf{B}} \cdot \beta_1 \\ \mathbf{u} + \mathbf{B}_0 \cdot \beta_1 + \mathbf{B} \cdot \beta_1 \\ \mathbf{D}_0 \cdot \beta_2 \end{pmatrix}$$

where

$$\bar{\mathbf{B}} = \begin{pmatrix} \mathbf{B}_1 \\ \vdots \\ \mathbf{B}_{l_3} \end{pmatrix}, \quad \mathbf{J} = (\mathbf{I}_{l_1} \quad \mathbf{I}_{l_1} \quad \dots \quad \mathbf{I}_{l_1})$$

Besides, let $N = l_3 + 2l_1l_3 + 2kl_2 + k_ql_1 + 2kl_2 + L$, we define

$$\begin{cases} \mathcal{M}_1 = \{(i, i, i)\}_{i \in [1, l_3]} \\ \mathcal{M}_2 = \{(i, i, i)\}_{i \in [l_3 + 2l_1l_3 + 1, N]} \\ \mathcal{M}_3 = \{(l_3 + l_1 \cdot (i-1) + j, i, l_3 + l_1l_3 + l_1 \cdot (i-1) + j)\}_{i \in [1, l_3], j \in [1, l_1]} \end{cases}$$

where \mathcal{M}_1 indicates that each τ_i is binary, \mathcal{M}_2 indicates that $\bar{\mathbf{v}}_2, \bar{\mathbf{v}}_1, \mathbf{w}, \bar{\mathbf{s}}, \mathbf{m}$ are binary vectors, and \mathcal{M}_3 indicates that $\mathbf{u}'_i = \tau_i \cdot \mathbf{u}_i$ for $i \in [1, l_3]$. Then we set $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$. In the new relation, the length of the witness is N and the size of \mathcal{M} is $N - l_1l_3$.

We can also use the fast mode (mentioned in Sec. 1.2) to argue that $\mathbf{v}_1, \mathbf{v}_2$ and \mathbf{s} are short. This will lead to an instance of \mathcal{R}^* , where the length of the witness is $l_3 + 2l_1l_3 + 4l_2 + k_ql_1 + L + \lambda \cdot (\lceil \log(2 \cdot 4l_2 \cdot \beta) \rceil + 1)$, and the size of \mathcal{M} is $l_3 + l_1l_3 + k_ql_1 + L + \lambda \cdot (\lceil \log(2 \cdot 4l_2 \cdot \beta) \rceil + 1)$.

4.4 ZKAoK of Accumulated Value

In this section, we give an argument of knowledge of an accumulated value for the accumulator scheme presented in [36].

More precisely, let l_1, L be positive integers and q be a power-of-prime. Also, let $k_q = \lceil \log q \rceil$ and $l_2 = l_1k_q$. We propose a zero knowledge argument of knowledge that proves knowledge of

$$\{\{\tau_i\}_{i \in [1, L]} \in \{0, 1\}^L; \{\mathbf{v}_i\}_{i \in [1, L]} \in ([0, 1]^{l_2})^L; \{\mathbf{w}_i\}_{i \in [1, L]} \in ([0, 1]^{l_2})^L\}$$

that satisfies

$$\begin{cases} \mathbf{B}_{1+\tau_1} \cdot \mathbf{v}_1 + \mathbf{B}_{2-\tau_1} \cdot \mathbf{w}_1 = \mathbf{H} \cdot \mathbf{u} \\ \forall i \in [2, L], \mathbf{B}_{1+\tau_i} \cdot \mathbf{v}_i + \mathbf{B}_{2-\tau_i} \cdot \mathbf{w}_i = \mathbf{H} \cdot \mathbf{v}_{i-1} \end{cases}$$

for public

$$\{\mathbf{B}_1 \in \mathbb{Z}_q^{l_1 \times l_2}; \mathbf{B}_2 \in \mathbb{Z}_q^{l_1 \times l_2}; \mathbf{u} \in [0, 1]^{l_1k_q}\}$$

where $\mathbf{H} = \mathbf{I}_{l_1} \otimes (1 \ 2 \ 4 \dots 2^{k_q-1})$.

We construct the argument via reducing the relation to an instance of the relation \mathcal{R}^* . Note that the relation contains L parts, each of which is a disjunction of two equations, namely, $\mathbf{B}_1 \cdot \mathbf{v}_i + \mathbf{B}_2 \cdot \mathbf{w}_i = \mathbf{H} \cdot \mathbf{v}_{i-1}$ and $\mathbf{B}_1 \cdot \mathbf{w}_i + \mathbf{B}_2 \cdot \mathbf{v}_i = \mathbf{H} \cdot \mathbf{v}_{i-1}$ (here, we define $\mathbf{v}_0 = \mathbf{u}$). As shown in [36], each part can be transformed into a subset sum of these two equations via setting the coefficients as $(1 - \tau_i, \tau_i)$. Next, we describe the reduction in more details.

First, for $i \in [2, L]$, we define $\mathbf{z}_{i,0} = \mathbf{B}_1 \cdot \mathbf{v}_i + \mathbf{B}_2 \cdot \mathbf{w}_i - \mathbf{H} \cdot \mathbf{v}_{i-1}$, $\mathbf{z}_{i,1} = \mathbf{B}_1 \cdot \mathbf{w}_i + \mathbf{B}_2 \cdot \mathbf{v}_i - \mathbf{H} \cdot \mathbf{v}_{i-1}$, $\mathbf{z}'_{i,0} = (1 - \tau_i) \cdot \mathbf{z}_{i,0}$ and $\mathbf{z}'_{i,1} = \tau_i \cdot \mathbf{z}_{i,1}$. Moreover,

More precisely, let l_1, l_2 be positive integers, q_0 be a prime and $p = q_0^{e_1}$, $q = q_0^{e_2}$, where $1 \leq e_1 < e_2$, we propose a ZKAoK for the following relation:

$$\mathcal{R}_{PRF} = \{(\mathbf{c}), (\mathbf{B}, \mathbf{k}) \in (\mathbb{Z}_p^{l_1}) \times (\mathbb{Z}_q^{l_1 \times l_2} \times \mathbb{Z}_q^{l_2}) : \mathbf{c} = \lfloor \mathbf{B} \cdot \mathbf{k} \rfloor_p \pmod{p}\}$$

We construct the argument via reducing the relation \mathcal{R}_{PRF} to an instance of the relation \mathcal{R}^* . First, we rewrite the equation $\mathbf{c} = \lfloor \mathbf{B} \cdot \mathbf{k} \rfloor_p \pmod{p}$ as follows:

$$\begin{cases} \mathbf{B} \cdot \mathbf{k} = \mathbf{u} \pmod{q} \\ \lfloor \frac{p}{q} \cdot \mathbf{u} \rfloor = \mathbf{c} \pmod{p} \end{cases}$$

The first equation is a linear equation with hidden matrix. The second equation, as shown in [37, 58], holds iff each element of the vector $\mathbf{u} - \frac{q}{p}\mathbf{c}$ is in $[0, \frac{q}{p})$, and thus can be transformed into a linear equation with short solution. Next, we describe the reduction in more details. We remark that in the remaining part of this section, all arithmetic operations are under the modulus q , so we omit the moduli in the remaining part of this section.

First, for $i \in [1, l_1]$, we define \mathbf{b}_i as the i -th row of \mathbf{B} and define \mathbf{v}_i as the Hadamard product between \mathbf{b}_i and \mathbf{k} , i.e., $\mathbf{v}_i[j] = \mathbf{b}_i[j] \cdot \mathbf{k}[j]$ for $j \in [1, l_2]$.

Let $\mathbf{e} = \mathbf{u} - \frac{q}{p}\mathbf{c}$, then we decompose the vector \mathbf{e} into a binary vector $\bar{\mathbf{e}}$ using the decomposition technique proposed in [40]. Let $\gamma = \frac{q}{p} - 1$ and $k = \lfloor \log \gamma \rfloor + 1$, then the length of $\bar{\mathbf{e}}$ is $k \cdot l_1$.

Also, let $\mathbf{g} = (\lfloor (\gamma + 1)/2 \rfloor \parallel \dots \parallel \lfloor (\gamma + 2^{i-1})/2^i \rfloor \parallel \dots \parallel \lfloor (\gamma + 2^{k-1})/2^k \rfloor)$ be a row vector. Then, we define the gadget matrix $\mathbf{G} = \mathbf{I}_{l_1} \otimes \mathbf{g}$, and it satisfies that $\mathbf{G} \cdot \bar{\mathbf{e}} = \mathbf{e}$.

Next, we define $\mathbf{b} = (\mathbf{b}_1^\top \parallel \dots \parallel \mathbf{b}_{l_1}^\top)^\top \in \mathbb{Z}_q^{l_1 \cdot l_2}$ and define $\mathbf{v} = (\mathbf{v}_1^\top \parallel \dots \parallel \mathbf{v}_{l_1}^\top)^\top \in \mathbb{Z}_q^{l_1 \cdot l_2}$.

Finally, we set

$$\mathbf{A} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{M} & -\mathbf{I}_{l_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_l & -\mathbf{G} \end{pmatrix}$$

$$\mathbf{x} = (\mathbf{k}^\top \quad \mathbf{b}^\top \quad \mathbf{v}^\top \quad \mathbf{u}^\top \quad \bar{\mathbf{e}}^\top)^\top, \quad \mathbf{y} = \left(\mathbf{0} \quad \frac{q}{p} \cdot \mathbf{c}^\top \right)^\top$$

where $\mathbf{M} = \mathbf{I}_{l_1} \otimes (1 \ 1 \ \dots \ 1) \in \mathbb{Z}_q^{l_1 \times l_1 \cdot l_2}$.

Besides, we define

$$\begin{cases} \mathcal{M}_1 = \{(i, i, i)\}_{i \in [l_2 + 2l_1l_2 + l_1 + 1, l_2 + 2l_1l_2 + l_1 + kl_1]} \\ \mathcal{M}_2 = \{(l_2 + l_1l_2 + (i-1) \cdot l_2 + j, l_2 + (i-1) \cdot l_2 + j, j)\}_{i \in [1, l_1], j \in [1, l_2]} \end{cases}$$

where \mathcal{M}_1 indicates that $\bar{\mathbf{e}}$ is a binary vector and \mathcal{M}_2 indicates that \mathbf{v}_i is the Hadamard product between \mathbf{b}_i and \mathbf{k} . Then we set $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$. In the new relation, the length of the witness is $l_2 + 2l_1l_2 + l_1 + kl_1$, and the size of \mathcal{M} is $kl_1 + l_1l_2$.

Remark 4.1. We remark that besides privacy-preserving primitives, our ZKAoK for weak PRF also implies a lattice-based verifiable random function (VRF) with trusted uniqueness (as formally defined in [52]).

More precisely, let λ be the security parameter. Let m, n, p, q be positive integers that are polynomial in λ , where $m \geq n(\log q + 1)/(\log p - 1)$. Let \mathbf{A} be a random matrix in $\mathbb{Z}_q^{m \times n}$ and serves as a public parameter. The secret key of the VRF is a random vector $\mathbf{s} \in \mathbb{Z}_q^n$ and the public key is a vector $\mathbf{b} = \lfloor \mathbf{A} \cdot \mathbf{s} \rfloor_p \bmod p$. The evaluation algorithm outputs $\mathbf{y} = \lfloor H(x) \cdot \mathbf{s} \rfloor_p \bmod p$ on input a bitstring x , where H is a hash function that maps an arbitrary-length bitstrings onto a matrix in $\mathbb{Z}_q^{m \times n}$ and is modeled as a random oracle. The proof for the correct evaluation of the VRF on an input x is a ZKAoK that argues knowledge of a secret key \mathbf{s} s.t. $\mathbf{b} = \lfloor \mathbf{A} \cdot \mathbf{s} \rfloor_p \wedge \mathbf{y} = \lfloor \mathbf{B} \cdot \mathbf{s} \rfloor_p$, where $\mathbf{B} = H(x)$ (Note that, we do not need to hide the matrices in this argument.).

First, as proved in [58], with all but negligible probability over the choice of \mathbf{A} , the secret key and the public key are bijective. Then the trusted uniqueness of the VRF follows directly from the soundness of the underlying arguments.

Acknowledgement. We appreciate the anonymous reviewers for their valuable suggestions. Part of this work was supported by the National Natural Science Foundation of China (Grant No. 61602396, 61572294, 61632020), Early Career Scheme research grant (ECS Grant No. 25206317) from the Research Grant Council of Hong Kong, the Innovation and Technology Support Programme of Innovation and Technology Fund of Hong Kong (Grant No. ITS/356/17), and the MonashU-PolyU-Collinstar Capital Joint Lab on Blockchain.

References

- [1] Miklós Ajtai. Generating hard instances of lattice problems. In *STOC*, pages 99–108. ACM, 1996.
- [2] Navid Alamati, Chris Peikert, and Noah Stephens-Davidowitz. New (and old) proof systems for lattice problems. In *PKC*, pages 619–643. Springer, 2018.
- [3] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange—a new hope. In *USENIX Security Symposium*, volume 2016, 2016.
- [4] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *CRYPTO*, pages 595–618. Springer, 2009.
- [5] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *EUROCRYPT*, pages 719–737. Springer, 2012.
- [6] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In *SCN*, pages 368–385. Springer, 2018.

- [7] 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 *ASIACRYPT*, pages 551–572. Springer, 2014.
- [8] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In *ESORICS*, pages 305–325. Springer, 2015.
- [9] Nina Bindel, Sedat Akeylek, Erdem Alkim, Paulo SLM Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Julaine Kramer, Patrick Longa, Harun Polat, et al. qtesla. submission to the nist’s post-quantum cryptography standardization process.(2018), 2018.
- [10] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. In *CCS*, pages 1006–1018. ACM, 2016.
- [11] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: a cca-secure module-lattice-based kem. In *EuroS&P*, pages 353–367. IEEE, 2018.
- [12] Cecilia Boschini, Jan Camenisch, and Gregory Neven. Floppy-sized group signatures from lattices. In *ACNS*, pages 163–182. Springer, 2018.
- [13] Cecilia Boschini, Jan Camenisch, and Gregory Neven. Relaxed lattice-based signatures with short zero-knowledge proofs. In *ISC*, pages 3–22. Springer, 2018.
- [14] Jan Camenisch, Gregory Neven, and Markus Rückert. Fully anonymous attribute tokens from lattices. In *SCN*, pages 57–75. Springer, 2012.
- [15] David Chaum. Blind signatures for untraceable payments. In *CRYPTO*, pages 199–203. Springer, 1982.
- [16] David Chaum and Eugène Van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265. Springer, 1991.
- [17] Rafael del Pino, Vadim Lyubashevsky, and Gregor Seiler. Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In *CCS*, pages 574–591. ACM, 2018.
- [18] Léo Ducas, Alain Durmus, Tancrede Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *CRYPTO*, pages 40–56. Springer, 2013.
- [19] Muhammed F. Esgin, Ron Steinfeld, Amin Sakzad, Joseph K. Liu, and Dongxi Liu. Short lattice-based one-out-of-many proofs and applications to ring signatures. Cryptology ePrint Archive, Report 2018/773, 2018. <https://eprint.iacr.org/2018/773>.
- [20] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO*, pages 186–194. Springer, 1986.
- [21] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William

- Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. submission to the nist's post-quantum cryptography standardization process.(2018), 2018.
- [22] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206. ACM, 2008.
- [23] Oded Goldreich and Shafi Goldwasser. On the limits of non-approximability of lattice problems. In *STOC*, pages 1–9. ACM, 1998.
- [24] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *STOC*, pages 291–304. ACM, 1985.
- [25] Shafi Goldwasser and Dmitriy Kharchenko. Proof of plaintext knowledge for the ajtai-dwork cryptosystem. In *TCC*, pages 529–555. Springer, 2005.
- [26] S Dov Gordon, Jonathan Katz, and Vinod Vaikuntanathan. A group signature scheme from lattice assumptions. In *ASIACRYPT*, pages 395–412. Springer, 2010.
- [27] Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In *EUROCRYPT*, pages 253–280. Springer, 2015.
- [28] Venkatesan Guruswami, Daniele Micciancio, and Oded Regev. The complexity of the covering radius problem. *Computational Complexity*, 14(2):90–121, 2005.
- [29] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer, 1998.
- [30] Jeffrey Hoffstein, Jill Pipher, William Whyte, and Zhenfei Zhang. A signature scheme from learning with truncation. Cryptology ePrint Archive, Report 2017/995, 2017. <https://eprint.iacr.org/2017/995>.
- [31] Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *ASIACRYPT*, pages 372–389. Springer, 2008.
- [32] Fabien Laguillaumie, Adeline Langlois, Benoît Libert, and Damien Stehlé. Lattice-based group signatures with logarithmic signature size. In *ASIACRYPT*, pages 41–61. Springer, 2013.
- [33] Adeline Langlois, San Ling, Khoa Nguyen, and Huaxiong Wang. Lattice-based group signature scheme with verifier-local revocation. In *PKC*, pages 345–361. Springer, 2014.
- [34] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In *ASIACRYPT*, pages 373–403. Springer, 2016.
- [35] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. In *ASIACRYPT*, pages 101–131. Springer, 2016.
- [36] 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. In *EUCRYPT*, pages 1–31. Springer, 2016.

- [37] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based PRFs and applications to E-cash. In *ASIACRYPT*, pages 304–335. Springer, 2017.
- [38] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Lattice-based zero-knowledge arguments for integer relations. In *CRYPTO*, pages 700–732. Springer, 2018.
- [39] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *CT-RSA*, pages 319–339. Springer, 2011.
- [40] San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang. Improved zero-knowledge proofs of knowledge for the isis problem, and applications. In *PKC*, pages 107–124. Springer, 2013.
- [41] San Ling, Khoa Nguyen, and Huaxiong Wang. Group signatures from lattices: simpler, tighter, shorter, ring-based. In *PKC*, pages 427–449. Springer, 2015.
- [42] San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu. Lattice-based group signatures: Achieving full dynamicity with ease. In *ACNS*, pages 293–312. Springer, 2017.
- [43] San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu. Constant-size group signatures from lattices. In *PKC*, pages 58–88. Springer, 2018.
- [44] Vadim Lyubashevsky. Lattice-based identification schemes secure under active attacks. In *PKC*, pages 162–179. Springer, 2008.
- [45] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *ASIACRYPT*, pages 598–616. Springer, 2009.
- [46] Vadim Lyubashevsky. Lattice signatures without trapdoors. In *EUROCRYPT*, pages 738–755. Springer, 2012.
- [47] Vadim Lyubashevsky and Gregory Neven. One-shot verifiable encryption from lattices. In *EUROCRYPT*, pages 293–323. Springer, 2017.
- [48] D Micciancio and O Regev. Worst-case to average-case reductions based on gaussian measures. In *FOCS*, pages 372–381. IEEE, 2004.
- [49] Daniele Micciancio and Chris Peikert. Hardness of SIS and LWE with small parameters. In *CRYPTO*, pages 21–39. Springer, 2013.
- [50] Daniele Micciancio and Salil P Vadhan. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. In *CRYPTO*, pages 282–298. Springer, 2003.
- [51] Phong Q Nguyen, Jiang Zhang, and Zhenfeng Zhang. Simpler efficient group signatures from lattices. In *PKC*, pages 401–426. Springer, 2015.
- [52] Dimitrios Papadopoulos, Duane Wessels, Shumon Huque, Moni Naor, Jan Včelák, Leonid Reyzin, and Sharon Goldberg. Making NSEC5 practical for DNSSEC. Cryptology ePrint Archive, Report 2017/099, 2017. <https://eprint.iacr.org/2017/099>.
- [53] Chris Peikert. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016.
- [54] Chris Peikert and Vinod Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In *CRYPTO*, pages 536–553. Springer, 2008.

- [55] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93. ACM, 2005.
- [56] Ronald L Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *ASIACRYPT*, pages 552–565. Springer, 2001.
- [57] Jacques Stern. A new identification scheme based on syndrome decoding. In *CRYPTO*, pages 13–21. Springer, 1993.
- [58] Rupeng Yang, Man Ho Au, Junzuo Lai, Qiuliang Xu, and Zuoxia Yu. Lattice-based techniques for accountable anonymity: Composition of abstract sterns protocols and weak PRF with efficient protocols from LWR. Cryptology ePrint Archive, Report 2017/781, 2017. <http://eprint.iacr.org/2017/781>.