# Improved Zero-Knowledge Proofs of Knowledge for the ISIS Problem, and Applications

San Ling[1], Khoa Nguyen[1], Damien Stehlé[2], and Huaxiong Wang[1]

[1] Division of Mathematical Sciences,
School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore
{lingsan,nguy0106,hxwang}@ntu.edu.sg
[2] ÉNS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL),
46 Allée d'Italie, 69364 Lyon Cedex 07, France
damien.stehle@ens-lyon.fr

**Abstract.** In all existing efficient proofs of knowledge of a solution to the infinity norm Inhomogeneous Small Integer Solution (ISIS$^\infty$) problem, the knowledge extractor outputs a solution vector that is only guaranteed to be $\widetilde{O}(n)$ times longer than the witness possessed by the prover. As a consequence, in many cryptographic schemes that use these proof systems as building blocks, there exists a gap between the hardness of solving the underlying ISIS$^\infty$ problem and the hardness underlying the security reductions. In this paper, we generalize Stern's protocol to obtain two statistical zero-knowledge proofs of knowledge for the ISIS$^\infty$ problem that remove this gap. Our result yields the potential of relying on weaker security assumptions for various lattice-based cryptographic constructions. As applications of our proof system, we introduce a concurrently secure identity-based identification scheme based on the worst-case hardness of the $\mathrm{SIVP}_{\widetilde{O}(n^{1.5})}$ problem (in the $\ell_2$ norm) in general lattices in the random oracle model, and an efficient statistical zero-knowledge proof of plaintext knowledge with small constant gap factor for Regev's encryption scheme.

## 1 Introduction

Zero-knowledge proofs and proofs of knowledge are fundamental notions and powerful tools in cryptography. In a zero-knowledge proof system [GMR89], a prover convinces a verifier that some statement is true while leaking nothing but the validity of the assertion. In a proof of knowledge ([GMR89, BG93]), the prover also convinces the verifier that he indeed knows a satisfying "witness" for the given statement. In the last 25 years, zero-knowledge proofs of knowledge (**ZKPoK**) have been extensively studied ([FFS87, GQ90, FS89, RS92, Mau09],...). These proof systems are the building blocks in many cryptographic constructions (e.g., identification schemes, group signatures, anonymous credential systems, to name just a few). In this work, we focus on **ZKPoK** for an important hard-on-average problem in lattice-based cryptography - the Inhomogeneous

K. Kurosawa and G. Hanaoka (Eds.): PKC 2013, LNCS 7778, pp. 107–124, 2013.

Small Integer Solution (ISIS) problem, that was introduced in [GPV08] and has since then been used extensively ([ABB10a, ABB10b, CHKP10, Boy10],...).

In recent years, lattice-based cryptography has received much attention from the research community because it enjoys a unique combination of attractive features: provable security under worst-case hardness assumptions, conjectured resistance against quantum computers, and asymptotic efficiency. The rapid development of the field yields an interesting challenge of designing and improving proof systems for lattice problems. There exist several proof systems, both interactive and non-interactive ([GG98, MV03, GMR05, PV08]) that exploit the geometric structure of worst-case lattice problems. On the other hand, when designing lattice-based cryptographic protocols, one essentially has to deal with the average-case problems that enjoy worst-case to average-case reductions, such as the SIS and ISIS problems ([Ajt96, MR07, GPV08]) and the Learning With Errors (LWE) problem ([Reg05, Reg09, Pei09]). All existing proofs of knowledge for the ISIS problem ([MV03, Lyu08]) have some limitations, most notably the fact that there is a gap between the norm of the witness vector and the norm of the vector computed by the knowledge extractor: The latter is only guaranteed to be $\widetilde{O}(n)$ larger than the former in the case of the infinity norm, where $n$ denotes the dimension of the corresponding worst-case lattice problem. As a consequence, cryptographic schemes using these proof systems as building blocks rely on a stronger security assumption than the assumed hardness of finding a witness for the ISIS instance, by a $\widetilde{O}(n)$ factor. This hints that the existing **ZKPoK** for the ISIS$^\infty$ problem are sub-optimal: Is it possible to design an efficient **ZKPoK** for ISIS$^\infty$ whose security provably relies on a weaker assumption than the existing ones? In this work, we reply positively, and describe such a **ZKPoK**, for which there is only a constant gap between the norm of the witness vector and the norm of the vector computed by the extractor. We also briefly describe a scheme with no gap (i.e., constant factor 1), but that is less efficient.

Notations. Throughout the paper, we assume that all vectors are column vectors. We denote vectors by bold lower-case letters (e.g., $\mathbf{x}$), and matrices by bold upper-case letters (e.g., $\mathbf{A}$). The Gram-Schmidt norm of a matrix $\mathbf{A}$ is denoted by $\|\widetilde{\mathbf{A}}\|$. We let the Hamming weight of a vector $\mathbf{x} \in \{0,1\}^m$ be denoted by $\mathrm{wt}(\mathbf{x})$. We let $\mathrm{B}_{3m}$ denote the set of all vectors $\mathbf{x} \in \{-1,0,1\}^{3m}$ having exactly $m$ coordinates equal to $-1$; $m$ coordinates equal to 0; and $m$ coordinates equal to 1. The symmetric group of all permutations of $k$ elements is denoted by $\mathcal{S}_k$. We use the notation $y \xleftarrow{\$} \mathrm{D}$ when $y$ is sampled from the distribution D. When S is a finite set, $y \xleftarrow{\$} \mathrm{S}$ means that $y$ is chosen uniformly at random from S. We let $n$ denote the security parameter of our schemes. A function $\epsilon : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is said negligible in $n$ (denoted by $\mathrm{negl}(n)$) if it vanishes faster than the inverse of any polynomial. We say that an event happens with overwhelming probability if it happens with probability $1 - \epsilon(n)$ for some negligible function $\epsilon$. We often use the soft-O notation: We write $f(n) = \widetilde{O}(g(n))$ if $f(n) = O(g(n) \log^c g(n))$ for some constant $c$. The statistical distance between two distributions X and Y over a countable domain D is $\frac{1}{2}\sum_{d \in \mathrm{D}} |\mathrm{X}(d) - \mathrm{Y}(d)|$. We say that X and Y are statistically close (denoted by $\mathrm{X} \approx_s \mathrm{Y}$) if their statistical distance is negligible.

### 1.1 Related Works

We briefly review some of the results related to proofs of knowledge for the ISIS problem. The $\mathrm{ISIS}^{p}_{n,m,q,\beta}$ problem in the $\ell_p$ norm with parameters $(n, m, q, \beta)$ asks to find a vector $\mathbf{x} \in \mathbb{Z}^m$ such that and $\|\mathbf{x}\|_p \leq \beta$ and $\mathbf{Ax} = \mathbf{y} \bmod q$ for a uniformly chosen input matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a uniformly chosen input vector $\mathbf{y} \in \mathbb{Z}_q^n$. The hardness of the $\mathrm{ISIS}^{2}_{n,m,q,\beta}$ problem is established by a worst-case to average-case reduction from standard lattice problems, such as the Shortest Independent Vectors Problem (SIVP).

**Theorem 1 ([GPV08]).** *For any $m$, $\beta = \mathrm{poly}(n)$, and for any integer $q \geq \beta \cdot \omega(\sqrt{n \log n})$, solving a* random *instance of the $\mathrm{ISIS}^{2}_{n,m,q,\beta}$ problem with non-negligible probability is at least as hard as approximating the $\mathrm{SIVP}^{2}_{\gamma}$ problem on* any *lattice of dimension $n$ to within certain $\gamma = \beta \cdot \widetilde{O}(\sqrt{n})$ factors.*

By the relationship between the $\ell_2$ and $\ell_\infty$ norms (i.e., for any vector $\mathbf{x} \in \mathbb{R}^n$, we have $\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\|_2 \leq \sqrt{n} \cdot \|\mathbf{x}\|_\infty$), it follows that the $\mathrm{ISIS}^{\infty}_{n,m,q,\beta}$ problem is at least as hard as $\mathrm{SIVP}^{2}_{\gamma}$ (in the $\ell_2$ norm) for some $\gamma = \beta \cdot \widetilde{O}(n)$. Without loss of generality, throughout this work, we will assume that $\beta$ is a positive *integer*. We define the relation $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$ for this problem as

$$\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}} = \Big\{((\mathbf{A}, \mathbf{y}), \mathbf{x}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \mathbb{Z}^m \colon (\|\mathbf{x}\|_\infty \leq \beta) \wedge (\mathbf{Ax} = \mathbf{y}\,[q])\Big\}.$$

Kawachi et al. [KTX08] adapted Stern's identification scheme [Ste96] to the lattice setting to obtain a **ZKPoK** for a *restricted* version of the $\mathrm{ISIS}^{\infty}$ problem, with respect to the relation

$$\mathrm{R}_{\mathrm{KTX}_{n,m,q,w}} = \Big\{((\mathbf{A}, \mathbf{y}), \mathbf{x}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \{0,1\}^m \colon (\mathrm{wt}(\mathbf{x}) = w) \wedge (\mathbf{Ax} = \mathbf{y}\,[q])\Big\}.$$

This restriction of $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$ does not seem to suffice for a wide range of applications. For some cryptographic schemes that allow many users, such as ID-based identification [Sha85] and group signature [CH91] schemes, the secret keys of the users are typically generated from the public keys by a trusted authority. For such schemes that rely on lattice-based hardness assumptions ([SSTX09, Rüc10a, CNR12, GKV10]), this task is performed by using a secret trapdoor possessed by the trusted authority, consisting in a relatively short basis of a publicly known lattice. As a result, a user secret key $\mathbf{x}$ is a *general* solution to the $\mathrm{ISIS}^{\infty}_{n,m,q,\beta}$ problem, where $\beta$ is typically $\widetilde{O}(\sqrt{n})$. Whenever a user in the scheme wants to identify himself, he must prove that he knows such a vector $\mathbf{x}$. In other words, these schemes require a **PoK** for the relation $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$, for which, up to the best of our knowledge, there exist two options:

- A proof of knowledge for $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$ was introduced by Lyubashevsky [Lyu08]. His protocol is efficient with low communication cost, but suffers from several limitations: It is not proven zero-knowledge (it is only proven to be witness-indistinguishable - a weaker notion than zero-knowledge [FS90]); It has a constant completeness error in each round; And it relies on a relatively strong hardness assumption for the $\mathrm{ISIS}^{\infty}$ problem, with a $\widetilde{O}(n)$ gap factor.

• Another proof system can be obtained by transforming the ISIS instance into a GapCVP instance, and adapting the Micciancio-Vadhan **ZKPoK** for GapCVP [MV03] to the infinity norm. Let $\mathbf{B}$ be any basis of the lattice $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{Ax} = \mathbf{0} \bmod q\}$ and $\mathbf{t}$ be a vector in $\mathbb{Z}^m$ such that $\mathbf{At} = \mathbf{y} \bmod q$. Such $\mathbf{B}$ and $\mathbf{t}$ can be efficiently computed using linear algebra. Then run the Micciancio-Vadhan protocol for $\mathrm{GapCVP}_{\gamma}^{\infty}$ with common input $(\mathbf{B}, \mathbf{t}, \beta)$. The prover's auxiliary input is $\mathbf{e} = \mathbf{t} - \mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A})$. We note that the knowledge extractor in [MV03] is only able to output a vector $\mathbf{e}' \in \Lambda_q^{\perp}(\mathbf{A})$, such that $\|\mathbf{t} - \mathbf{e}'\|_{\infty} \leq g \cdot \beta$ for some $g > 1$. This implies that $\mathbf{x}' = \mathbf{t} - \mathbf{e}'$ is a solution to the $\mathrm{ISIS}_{n,m,q,g\cdot\beta}^{\infty}$ problem with respect to $(\mathbf{A}, \mathbf{y})$. However, in the infinity norm, the smallest $g$ that can be obtained is $\geq \Theta(n/\log n)$ while the bit complexity is relatively high. In more details, the gap factor $g$ depends on some parameter $k$ as follows: $g = m^{1+\Omega(1)}$ for $k = \omega(1)$; $g = \Omega(m)$ for $k = \omega(\log m)$; and $g = \Omega(m/\log m)$ for $k = \mathrm{poly}(m)$ - a sufficiently large polynomial. The communication cost of the protocol depends linearly on $k$. Alternatively, one could apply the ISIS-GapCVP transformation to the Micciancio-Vadhan protocol for the $\ell_2$ norm, and then use the relationship between the $\ell_2$ and $\ell_{\infty}$ norms. However, in this case, the gap is slightly bigger (at least $\Theta(n/\sqrt{\log n})$).

We now shortly review a class of proof systems related to our work: zero-knowledge proofs of plaintext knowledge (**ZKPoPK**) for Regev's LWE-based cryptosystem ([Reg05, Reg09]). All known **ZKPoPK** ([BD10, BDOZ11, AJLA+12, DLA12]) were derived from Secure Multi-Party Computation protocols, via the [IKOS07] transformation from **MPC** to **ZK**. The proof systems are relatively inefficient and rely on the assumption that SIVP is hard for super-polynomial approximation factors (i.e., $\gamma = n^{\omega(1)}$). We observe (in Section 3.2) that a **PoPK** for Regev's cryptosystem can be obtained from a **PoK** for $\mathrm{R}_{\mathrm{ISIS}}$. Thus, a **ZKPoK** for the ISIS problem with lower communication cost and a weaker hardness assumption leads to a significant improvement in this direction.

### 1.2 Our Contributions and Techniques

The discussions above raise the question whether it is possible to design a **ZKPoK** for the *general* ISIS problem that completely removes the gap. Even a **ZKPoK** that has small constant gap factor while maintaining efficiency would be desirable. In this work, we answer this question positively. Specifically, we show that there exists a statistical **ZKPoK** (called **Naive SternExt**) for the relation $\mathrm{R}_{\mathrm{ISIS}_{n,m,q,\beta}^{\infty}}$ whose security relies on the assumed hardness of the $\mathrm{ISIS}_{n,m,q,\beta}^{\infty}$. This scheme achieves optimal gap, as the norm bounds for the witness and the security assumptions are identical. However, its communication cost depends linearly on $\beta$, which may be a significant drawback for large $\beta$. Our main result is a statistical **ZKPoK** called **SternExt** achieving both security and efficiency requirements: it has an almost optimal gap factor ($g \leq 2$), while the communication cost compares favorably to the Micciancio-Vadhan proof system. We believe that our result can be applied to many cryptographic primitives. In particular, we will describe two applications of the **SternExt** proof system:

1. A concurrently secure identity-based identification scheme that relies on worst-case hardness of the $\mathrm{SIVP}_{\widetilde{O}(n^{1.5})}$ problem (in the $\ell_2$ norm) in general lattices. This is the weakest security assumption among contemporary lattice-based ID-based ID schemes ([SSTX09, Rüc10a]).
2. An efficient statistical **ZKPoPK** for Regev's cryptosystem with small constant gap factor between the sizes of a valid plaintext and the output of the knowledge extractor. In comparison with the results of [BD10, BDOZ11, AJLA+12, DLA12], our proof system offers a noticeable improvement in both security and efficiency points of view.

We now sketch our approach. While the [MV03] protocol exploits the geometric aspect of the ISIS problem, our protocol exploits its combinatorial and algebraic aspects. We first look at the scheme from [Ste96, KTX08], and investigate how to loosen the restrictions on the witness $\mathbf{x}$, which are $\mathbf{x} \in \{0,1\}^m$ and $\mathrm{wt}(\mathbf{x}) = w$. Note that these conditions are invariant under all permutations of coordinates: For $\pi \in \mathcal{S}_m$, a vector $\mathbf{x}$ satisfies those restrictions if and only if $\pi(\mathbf{x})$ also does. Thus, a witness $\mathbf{x}$ with such constraints can be verified in zero-knowledge thanks to the randomness of $\pi$. We then notice that the same statement still holds true for $\mathbf{x} \in \mathrm{B}_{3m}$, namely: for $\pi \in \mathcal{S}_{3m}$, $\mathbf{x} \in \mathrm{B}_{3m} \Leftrightarrow \pi(\mathbf{x}) \in \mathrm{B}_{3m}$. This basic fact allows us to generalize the proof system from [Ste96, KTX08]. Our generalization consists of two steps:

**Step 1.** *Removing the restriction on the Hamming weight.* Specifically, we observe that a **ZKPoK** for the relation

$$\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,1}} = \left\{((\mathbf{A},\mathbf{y}),\mathbf{x}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \{-1,0,1\}^m \colon \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q\right\}$$

can be derived from Stern's scheme by the following *extensions*: For any vector $\mathbf{x} \in \{-1,0,1\}^m$, append $2m$ coordinates from the set $\{-1,0,1\}$ to $\mathbf{x}$ to obtain $\mathbf{x}' \in \mathrm{B}_{3m}$. Next, append $2m$ zero-columns to matrix $\mathbf{A}$ to get $\mathbf{A}' \in \mathbb{Z}_q^{n\times 3m}$. We then have:

$$\mathbf{x}' \in \mathrm{B}_{3m} \Leftrightarrow \mathbf{x} \in \{-1,0,1\}^m,$$
$$\mathbf{A}'\mathbf{x}' = \mathbf{y} \bmod q \Leftrightarrow \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q.$$

In other words, if a verifier is convinced that $\mathbf{x}' \in \mathrm{B}_{3m}$ and $\mathbf{A}'\mathbf{x}' = \mathbf{y} \bmod q$, then he is also convinced that $\mathbf{x}$ is a valid witness for the relation $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,1}}$.

**Step 2.** *Increasing the $\ell_\infty$ bound to $\beta$, for any $\beta > 0$.* The principle of **Step 1** can be generalized in a naive manner. For any $\mathbf{x} \in \{-\beta,\ldots,0,\ldots,\beta\}^m$, one can append $2\beta m$ coordinates to $\mathbf{x}$ to obtain an $\mathbf{x}^* \in \{-\beta,\ldots,0,\ldots,\beta\}^{(2\beta+1)m}$ that has exactly $m$ coordinates equal to $d$ for each $d \in \{-\beta,\ldots,0,\ldots,\beta\}$. The extended matrix $\mathbf{A}^* \in \mathbb{Z}_q^{n\times(2\beta+1)m}$ is obtained by appending $2\beta m$ zero-columns to matrix $\mathbf{A}$. Then $\mathbf{A}^*\mathbf{x}^* = \mathbf{A}\mathbf{x} \bmod q$. Moreover, the constraints of $\mathbf{x}^*$ can be verified in zero-knowledge by using a uniform $\pi \in \mathcal{S}_{(2\beta+1)m}$. Therefore, we obtain a **ZKPoK** for $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$, that we call **Naive SternExt**, where the extraction gap factor is completely removed. However, as mentioned earlier, the proof is inefficient for large $\beta$ as its communication cost is $\beta \cdot \widetilde{O}(n \lg q)$.

A much more efficient method to achieve our goal is based on the idea of representing any vector $\mathbf{x} \in \{-\beta, \ldots, 0, \ldots, \beta\}^m$ by $k = \lfloor \lg \beta \rfloor + 1$ vectors $\tilde{\mathbf{u}}_0, \ldots, \tilde{\mathbf{u}}_{k-1}$ in $\{-1, 0, 1\}^m$ via a binary decomposition, namely: $\mathbf{x} = \sum_{j=0}^{k-1} 2^j \cdot \tilde{\mathbf{u}}_j$. Next we apply the extension of **Step 1**: Extend each $\tilde{\mathbf{u}}_j$ to $\mathbf{u}_j \in \mathrm{B}_{3m}$, and extend $\mathbf{A}$ to $\mathbf{A}' \in \mathbb{Z}_q^{n \times 3m}$. We then have:

$$\mathbf{A}'\big(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{u}_j\big) = \mathbf{y} \bmod q \Leftrightarrow \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q.$$

This allows us to combine $k$ proofs for $\mathrm{R}_{\mathrm{ISIS}^\infty_{n,m,q,1}}$ into one proof $\mathrm{R}_{\mathrm{ISIS}^\infty_{n,m,q,\beta}}$.[1] We thus obtain a statistical **ZKPoK** for the *general* $\mathrm{ISIS}^\infty$ problem, that we call **SternExt**, with the following properties:

- The knowledge extractor obtains an $\mathbf{x}'$ with $\|\mathbf{x}'\|_\infty \leq \beta'$, where $\beta \leq \beta' \leq 2\beta - 1$ (depending on the binary representation of $\beta$). Hence, the extraction gap factor satisfies $g < 2$.
- The communication cost is $\lg \beta \cdot \widetilde{O}(n \lg q)$. In particular, in most cryptographic applications $q$ is $\mathrm{poly}(n)$, and we then have $\lg \beta \leq \lg q = \widetilde{O}(1)$.

Overall, **SternExt** provides a better proof system for $\mathrm{R}_{\mathrm{ISIS}^\infty_{n,m,q,\beta}}$ in both security and efficiency aspects than the one derived from the Micciancio-Vadhan protocol. We summarize the comparison among the **PoK** for $\mathrm{R}_{\mathrm{ISIS}^\infty_{n,m,q,\beta}}$ in Table 1. The comparison data are for one round of protocol, in which case all the considered proof systems admit a constant soundness error.

**Table 1.** Comparison among the proofs of knowledge for $\mathrm{R}_{\mathrm{ISIS}^\infty_{n,m,q,\beta}}$. See discussion in Section 1.1 for other security/efficiency trade-offs for the [MV03] scheme.

| Schemes | [Lyu08] | [MV03] | **Naive SternExt** | **SternExt** |
|---|---|---|---|---|
| Zero-knowledge? | ✗(WI) | ✓ | ✓ | ✓ |
| Perfect completeness? | ✗ | ✓ | ✓ | ✓ |
| Norm bound in the ISIS hardness assumption | $\beta \cdot \widetilde{O}(n)$ | $\beta \cdot \widetilde{O}(n)$ | $\beta$ | $\leq 2\beta - 1$ |
| Communication cost | $\widetilde{O}(n \lg q)$ | $\widetilde{O}(n \lg q)$ | $\beta \cdot \widetilde{O}(n \lg q)$ | $\lg \beta \cdot \widetilde{O}(n \lg q)$ |

Outline. The rest of the paper is organized as follows: In Section 2, we present the **SternExt** proof system; and in Section 3, we describe two cryptographic applications. We refer the reader to [Gol04, Chap. 4] and [GPV08] for standard definitions of zero-knowledge proof systems and lattice problems, respectively. In the appendix, we adapt **SternExt** to the relation $\mathrm{R}_{\mathrm{SIS}^\infty}$ associated to the SIS problem: $\mathrm{R}_{\mathrm{SIS}^\infty}$ corresponds to setting $\mathbf{y} = \mathbf{0}$ and imposing $\mathbf{x} \neq \mathbf{0}$ in $\mathrm{R}_{\mathrm{ISIS}^\infty}$.

[1] This packing of proofs is akin to Jain et al.'s recent work on the Learning Parity with Noise problem [JKPT12, Section 4.2].

## 2 A Zero-Knowledge Proof of Knowledge for ISIS

Our scheme extends Stern's **ZKPoK** [Ste96] for the Syndrome Decoding Problem (SDP). Stern's proof system is a 3-move interactive protocol: the prover $P$ computes three commitments and sends them to the verifier $V$; verifier $V$ sends a uniformly random challenge to $P$; prover $P$ reveals two of the three commitments according to the challenge. Kawachi et al. [KTX08] adapted Stern's scheme to the lattice setting, exploiting the similarity between the SDP and ISIS problems. Their construction makes use of a string commitment scheme that is statistically hiding and computationally binding.

**Definition 1.** *A statistically hiding, computationally binding string commitment scheme is a* PPT *algorithm* $\mathrm{COM}(s, \rho)$ *satisfying:*

- *For all* $s_0, s_1 \in \{0,1\}^*$*, we have (over the random coins of* COM*):*
$$\mathrm{COM}(s_0; \cdot) \approx_s \mathrm{COM}(s_1; \cdot),$$
- *For all* PPT *algorithm* $\mathcal{A}$ *returning* $(s_0, \rho_0); (s_1, \rho_1)$*, where* $s_0 \neq s_1$*, we have (over the random coins of* $\mathcal{A}$*):*
$$\Pr[\mathrm{COM}(s_0; \rho_0) = \mathrm{COM}(s_1; \rho_1)] = \mathrm{negl}(n).$$

### 2.1 Setup

For a security parameter $n$, let $q$ be a positive integer. Let $\beta$ be some positive integer, and $k = \lfloor \lg \beta \rfloor + 1$. Let COM be a statistically hiding and computationally binding string commitment scheme. It was shown in [KTX08] that such a scheme can be constructed based on the hardness of the $\mathrm{ISIS}^{\infty}_{n,m,q,\widetilde{O}(1)}$ problem. For simplicity, in the interactive protocol, we will not explicitly write the randomness $\rho$ of the commitment scheme COM.

The common input is a pair $(\mathbf{A}, \mathbf{y})$ such that $\mathbf{y}$ belongs to the image of $\mathbf{A}$, and the prover's auxiliary input is vector $\mathbf{x}$. Prior to the interaction, both $P$ and $V$ form the extended matrix $\mathbf{A}' \in \mathbb{Z}_q^{n \times 3m}$ by appending $2m$ zero-columns to matrix $\mathbf{A}$. In addition, prover $P$ performs the following preparation steps:

1. Decomposition. The goal is to represent vector $\mathbf{x} = (x_1, x_2, \ldots, x_m)$ by $k$ vectors in $\{-1, 0, 1\}^m$. For each $1 \leq i \leq m$, consider a binary representation of coordinate $x_i$, that is: $x_i = b_{i,0} \cdot 2^0 + b_{i,1} \cdot 2^1 + \ldots + b_{i,k-1} \cdot 2^{k-1}$, where $b_{i,j} \in \{-1, 0, 1\}$, for all $j = 0, \ldots, k-1$. Now for each index $j$, let $\tilde{\mathbf{u}}_j = (b_{1,j}, b_{2,j}, \ldots, b_{m,j}) \in \{-1, 0, 1\}^m$. We observe that $\mathbf{x} = \sum_{j=0}^{k-1} 2^j \cdot \tilde{\mathbf{u}}_j$.
2. Extension. For each index $j = 0, \ldots, k-1$, extend $\tilde{\mathbf{u}}_j$ to a vector $\mathbf{u}_j \in \mathrm{B}_{3m}$ as follows: If the numbers of coordinates $-1$, 0, and 1 in vectors $\tilde{\mathbf{u}}_j$ are $\lambda_j^{(-1)}$, $\lambda_j^{(0)}$ and $\lambda_j^{(1)}$ respectively, then choose a random vector $\mathbf{t}_j \in \{-1, 0, 1\}^{2m}$ that has exactly $(m - \lambda_j^{(-1)})$ coordinates $-1$, $(m - \lambda_j^{(0)})$ coordinates 0, and

$(m - \lambda_j^{(1)})$ coordinates 1; and append $\mathbf{t}_j$ to $\tilde{\mathbf{u}}_j$, i.e., set $\mathbf{u}_j = (\tilde{\mathbf{u}}_j \| \mathbf{t}_j)$. Since the last $2m$ columns of matrix $\mathbf{A}'$ are zero-columns, we have:

$$\mathbf{A}'\big(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{u}_j\big) = \mathbf{y} \bmod q \Leftrightarrow \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q.$$

### 2.2 The Interactive Proof System

The prover $P$ and the verifier $V$ interact as described in Figure 1.

1. **Commitment.** Prover $P$ samples $k$ vectors $\mathbf{r}_0, \ldots, \mathbf{r}_{k-1} \xleftarrow{\$} \mathbb{Z}_q^{3m}$; $k$ permutations $\pi_0, \ldots, \pi_{k-1} \xleftarrow{\$} \mathcal{S}_{3m}$, and sends the commitment $\mathrm{CMT} := (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = \mathrm{COM}(\pi_0, \ldots, \pi_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{r}_j) \bmod q) \\ \mathbf{c}_2 = \mathrm{COM}(\pi_0(\mathbf{r}_0), \ldots, \pi_{k-1}(\mathbf{r}_{k-1})) \\ \mathbf{c}_3 = \mathrm{COM}(\pi_0(\mathbf{u}_0 + \mathbf{r}_0), \ldots, \pi_{k-1}(\mathbf{u}_{k-1} + \mathbf{r}_{k-1})) \end{cases}$$

2. **Challenge.** Receiving CMT, verifer $V$ sends a challenge $Ch \xleftarrow{\$} \{1, 2, 3\}$ to $P$.
3. **Response.** Prover $P$ replies as follows:
   - If $Ch = 1$, then reveal $\mathbf{c}_2$ and $\mathbf{c}_3$. For each $j$, let $\mathbf{v}_j = \pi_j(\mathbf{u}_j)$, and $\mathbf{w}_j = \pi_j(\mathbf{r}_j)$. Send $\mathrm{RSP} := (\mathbf{v}_0, \ldots, \mathbf{v}_{k-1}, \mathbf{w}_0, \ldots, \mathbf{w}_{k-1})$.
   - If $Ch = 2$, then reveal $\mathbf{c}_1$ and $\mathbf{c}_3$. For each $j$, let $\phi_j = \pi_j$, and $\mathbf{z}_j = \mathbf{u}_j + \mathbf{r}_j$. Send $\mathrm{RSP} := (\phi_0, \ldots, \phi_{k-1}, \mathbf{z}_0, \ldots, \mathbf{z}_{k-1})$.
   - If $Ch = 3$, then reveal $\mathbf{c}_1$ and $\mathbf{c}_2$. For each $j$, let $\psi_j = \pi_j$, and $\mathbf{s}_j = \mathbf{r}_j$. Send $\mathrm{RSP} := (\psi_0, \ldots, \psi_{k-1}, \mathbf{s}_0, \ldots, \mathbf{s}_{k-1})$.

**Verification.** Receiving the response RSP, verifier $V$ performs the following checks:

- If $Ch = 1$: Check that $\mathbf{v}_j \in \mathrm{B}_{3m}$ for all $j = 0, \ldots, k-1$, and

$$\begin{cases} \mathbf{c}_2 = \mathrm{COM}(\mathbf{w}_0, \ldots, \mathbf{w}_{k-1}) \\ \mathbf{c}_3 = \mathrm{COM}(\mathbf{v}_0 + \mathbf{w}_0, \ldots, \mathbf{v}_{k-1} + \mathbf{w}_{k-1}) \end{cases}$$

- If $Ch = 2$: Check that

$$\begin{cases} \mathbf{c}_1 = \mathrm{COM}(\phi_0, \ldots, \phi_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{z}_j) - \mathbf{y} \bmod q) \\ \mathbf{c}_3 = \mathrm{COM}(\phi_0(\mathbf{z}_0), \ldots, \phi_{k-1}(\mathbf{z}_{k-1})) \end{cases}$$

- If $Ch = 3$: Check that

$$\begin{cases} \mathbf{c}_1 = \mathrm{COM}(\psi_0, \ldots, \psi_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{s}_j) \bmod q) \\ \mathbf{c}_2 = \mathrm{COM}(\psi_0(\mathbf{s}_0), \ldots, \psi_{k-1}(\mathbf{s}_{k-1})) \end{cases}$$

In each case, verifier $V$ outputs the decision $d = 1$ (Accept) if and only if all the conditions hold. Otherwise, he outputs $d = 0$ (Reject).

**Fig. 1.** The **SternExt** proof system

**Completeness.** We observe that if prover $P$ has a valid witness $\mathbf{x}$ for the relation $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$ and follows the protocol, then he always gets accepted by $V$. Therefore, the proof system has perfect completeness.

**Communication Cost.** The size of the commitment scheme from [KTX08] is $\widetilde{O}(n \lg q)$. If $Ch = 1$, then the size of RSP is $3km + 3km \lg q$. If $Ch = 2$ or $Ch = 3$, then RSP consists of $k$ vectors in $\mathbb{Z}_q^{3m}$ and $k$ permutations. Note that in practice, instead of sending the permutations and vectors, one would send the *random seed* of the PRNG used to generate these data, and thus significantly reduce the communication cost. Overall, the total communication cost of the protocol is $\lg \beta \cdot \widetilde{O}(n \lg q)$.

### 2.3 Statistical Zero-Knowledge

We now prove that the proof system **SternExt** is statistically zero-knowledge, by exhibiting a transcript simulator.

**Theorem 2.** *If* COM *is a statistically hiding string commitment scheme, then the proof system* ***SternExt*** *from Figure 1 is statistically zero-knowledge.*

*Proof.* Adapting the techniques of [Ste96] and [KTX08], we construct a simulator $\mathcal{S}$ which has black-box access to a (possibly cheating) verifier $\widehat{V}$, such that on input the public parameters $\mathbf{A}$ (and implicitly its extension $\mathbf{A}'$) and $\mathbf{y}$, outputs with probability 2/3 a successful transcript (i.e., an accepted interaction), and the view of $\widehat{V}$ in the simulation is statistically close to that in the real interaction. The simulator $\mathcal{S}$ begins by selecting a random $\overline{Ch} \in \{1, 2, 3\}$ (a prediction of the challenge value that $\widehat{V}$ will *not* choose), and a random tape $r'$ of $\widehat{V}$. We note that in all the cases we consider below, by the assumption on the commitment scheme COM, the distributions of $\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3$ are statistically close to the distributions of the commitments in the real interaction, and thus, the distributions of the challenge $Ch$ from $\widehat{V}$ is also statistically close to that in the real interactions.

**Case** $\overline{Ch} = 1$: The simulator $\mathcal{S}$ computes $\mathbf{x}' \in \mathbb{Z}_q^m$ such that $\mathbf{A}\mathbf{x}' = \mathbf{y} \bmod q$ using linear algebra. It picks $k-1$ random vectors $\widetilde{\mathbf{u}}'_1, \ldots, \widetilde{\mathbf{u}}'_{k-1} \xleftarrow{\$} \mathbb{Z}_q^m$ and sets:

$$\widetilde{\mathbf{u}}'_0 := \mathbf{x}' - \sum_{j=1}^{k-1} 2^j \cdot \widetilde{\mathbf{u}}'_j \bmod q.$$

In other words, we have $\mathbf{x}' = \sum_{j=0}^{k-1} 2^j \cdot \widetilde{\mathbf{u}}'_j \bmod q$. Now for each $j$, the simulator extends $\widetilde{\mathbf{u}}'_j$ to $\mathbf{u}'_j \in \mathbb{Z}_q^{3m}$ by appending $2m$ random coordinates. It then picks $k$ vectors $\mathbf{r}'_0, \ldots, \mathbf{r}'_{k-1} \xleftarrow{\$} \mathbb{Z}_q^{3m}$; $k$ permutations $\pi'_0, \ldots, \pi'_{k-1} \xleftarrow{\$} \mathcal{S}_{3m}$; and uniformly random strings $\rho'_1, \rho'_2, \rho'_3$. It sends the following commitments to $\widehat{V}$:

$$\begin{cases} \mathbf{c}'_1 = \mathrm{COM}(\pi'_0, \ldots, \pi'_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{r}'_j) \bmod q; \rho'_1) \\ \mathbf{c}'_2 = \mathrm{COM}(\pi'_0(\mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{r}'_{k-1}); \rho'_2) \\ \mathbf{c}'_3 = \mathrm{COM}(\pi'_0(\mathbf{u}'_0 + \mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{u}'_{k-1} + \mathbf{r}'_{k-1}); \rho'_3). \end{cases}$$

Receiving a challenge $Ch$ from $\widehat{V}$, simulator $\mathcal{S}$ provides a transcript as follows:

- If $Ch = 1$: Output $\perp$ and halt.
- If $Ch = 2$: Output

$$\Big(r', (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3), 2, (\pi'_0, \pi'_1, \ldots, \pi'_{k-1}, \mathbf{u}'_0 + \mathbf{r}'_0, \ldots, \mathbf{u}'_{k-1} + \mathbf{r}'_{k-1}); \rho'_1, \rho'_3\Big).$$

- If $Ch = 3$: Output $\Big(r', (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3), 3, (\pi'_0, \ldots, \pi'_{k-1}, \mathbf{r}'_0, \ldots, \mathbf{r}'_{k-1}); \rho'_1, \rho'_2\Big)$.

**Case** $\overline{Ch} = 2$: The simulator $\mathcal{S}$ picks $\mathbf{r}'_0, \ldots, \mathbf{r}'_{k-1} \xleftarrow{\$} \mathbb{Z}_q^{3m}$; $\mathbf{u}'_0, \ldots, \mathbf{u}'_{k-1} \xleftarrow{\$} \mathrm{B}_{3m}$; permutations $\pi'_0, \ldots, \pi'_{k-1} \xleftarrow{\$} \mathcal{S}_{3m}$; and uniformly random strings $\rho'_1, \rho'_2, \rho'_3$. It sends to $\widehat{V}$ the commitments:

$$\begin{cases} \mathbf{c}'_1 = \mathrm{COM}(\pi'_0, \ldots, \pi'_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{r}'_j) \bmod q; \rho'_1) \\ \mathbf{c}'_2 = \mathrm{COM}(\pi'_0(\mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{r}'_{k-1}); \rho'_2) \\ \mathbf{c}'_3 = \mathrm{COM}(\pi'_0(\mathbf{u}'_0 + \mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{u}'_{k-1} + \mathbf{r}'_{k-1}); \rho'_3). \end{cases}$$

Receiving a challenge $Ch$ from $\widehat{V}$, simulator $\mathcal{S}$ computes the following transcript:

- If $Ch = 1$: Output

$$\Big(r', (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3), 1, (\pi'_0(\mathbf{u}'_0), \ldots, \pi'_{k-1}(\mathbf{u}'_{k-1}), \pi'_0(\mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{r}'_{k-1})); \rho'_2, \rho'_3\Big).$$

- If $Ch = 2$: Output $\perp$ and halt.
- If $Ch = 3$: Output $\Big(r', (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3), 3, (\pi'_0, \ldots, \pi'_{k-1}, \mathbf{r}'_0, \ldots, \mathbf{r}'_{k-1}); \rho'_1, \rho'_2\Big)$.

**Case** $\overline{Ch} = 3$: The simulator picks the uniformly random vectors, permutations, and strings exactly as in the case $\overline{Ch} = 2$ above, but sends the following:

$$\begin{cases} \mathbf{c}'_1 = \mathrm{COM}(\pi'_0, \ldots, \pi'_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot (\mathbf{u}'_j + \mathbf{r}'_j)) - \mathbf{y} \bmod q; \rho'_1) \\ \mathbf{c}'_2 = \mathrm{COM}(\pi'_0(\mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{r}'_{k-1}); \rho'_2) \\ \mathbf{c}'_3 = \mathrm{COM}(\pi'_0(\mathbf{u}'_0 + \mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{u}'_{k-1} + \mathbf{r}'_{k-1}); \rho'_3). \end{cases}$$

Receiving a challenge $Ch$ from $\widehat{V}$, simulator $\mathcal{S}$ computes a transcript as follows:

- If $Ch = 1$: Output

$$\Big(r', (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3), 1, (\pi'_0(\mathbf{u}'_0), \ldots, \pi'_{k-1}(\mathbf{u}'_{k-1}), \pi'_0(\mathbf{r}'_0), \ldots, \pi'_{k-1}(\mathbf{r}'_{k-1})); \rho'_2, \rho'_3\Big).$$

- If $Ch = 2$: Output

$$\Big(r', (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3), 2, (\pi'_0, \ldots, \pi'_{k-1}, \mathbf{u}'_0 + \mathbf{r}'_0, \ldots, \mathbf{u}'_{k-1} + \mathbf{r}'_{k-1}); \rho'_1, \rho'_3\Big).$$

- If $Ch = 3$: Output $\perp$ and halt.

We observe that the probability that the simulator outputs $\perp$ is negligibly close to 1/3. Moreover, one can check that whenever $\mathcal{S}$ does not halt, it will provide a successful transcript, and the distribution of the transcript is statistically close to that of the prover in the real interaction. Hence, we have constructed a simulator that can successfully impersonate the honest prover with probability 2/3, and completed the proof.

### 2.4 Proof of Knowledge

The fact that anyone can run the simulator to convince the verifier with probability 2/3 implies that the **SternExt** proof system has soundness error $\geq 2/3$. In the following, we prove that it is indeed a proof of knowledge for the relation $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$ with knowledge error $\kappa = 2/3$.

**Theorem 3.** *Assume that* COM *is a computationally binding string commitment scheme. Then there exists a knowledge extractor $\mathcal{K}$ such that the following holds. If $\mathcal{K}$ has access to a cheating prover who convinces the verifier on input $(\mathbf{A}, \mathbf{y})$ with probability $2/3 + \epsilon$ for some $\epsilon > 0$ and in time $T$, then $\mathcal{K}$ outputs an $\mathbf{x}$ such that $((\mathbf{A}, \mathbf{y}); \mathbf{x}) \in \mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,2\beta-1}}$ with overwhelming probability and runtime $T \cdot \mathrm{poly}(n, m, \lg q, 1/\epsilon)$.*

As a corollary, **SternExt** is sound for uniform $(\mathbf{A}, \mathbf{y})$ under the assumption that the $\mathrm{ISIS}^{\infty}_{n,m,q,2\beta-1}$ problem is hard.

*Proof.* We apply the technique of [Vér96] relying on trees to model the probability space corresponding to the protocol execution. Suppose a cheating prover $\widehat{P}$ can convince the verifier with probability $2/3 + \epsilon$. Then by rewinding $\widehat{P}$ a number of times polynomial in $1/\epsilon$, the knowledge extractor $\mathcal{K}$ can find with overwhelming probability a node with 3 sons in the tree associated with the protocol between $\widehat{P}$ and the verifier. This node corresponds to the reception of all 3 values of the challenge. In other words, $\widehat{P}$ is able to answer correctly to all challenges for the same commitment. Therefore, $\mathcal{K}$ can get the following relations:

$$\mathrm{COM}(\phi_0, \ldots, \phi_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{z}_j) - \mathbf{y}) = \mathrm{COM}(\psi_0, \ldots, \psi_{k-1}, \mathbf{A}'(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{s}_j))$$
$$\mathrm{COM}(\mathbf{w}_0, \ldots, \mathbf{w}_{k-1}) = \mathrm{COM}(\psi_0(\mathbf{s}_0), \ldots, \psi_{k-1}(\mathbf{s}_{k-1}))$$
$$\mathrm{COM}(\phi_0(\mathbf{z}_0), \ldots, \phi_{k-1}(\mathbf{z}_{k-1})) = \mathrm{COM}(\mathbf{v}_0 + \mathbf{w}_0, \ldots, \mathbf{v}_{k-1} + \mathbf{w}_{k-1}),$$

and $\mathbf{v}_j \in \mathrm{B}_{3m}$ for all $j = 0, \ldots, k-1$. Since COM is computationally binding, it follows that:

$$\mathbf{A}'\Big(\sum_{j=0}^{k-1} 2^j \cdot (\mathbf{z}_j - \mathbf{s}_j)\Big) = \mathbf{y} \bmod q,$$

and for all $j$, we have $\phi_j = \psi_j; \mathbf{w}_j = \psi_j(\mathbf{s}_j); \mathbf{v}_j + \mathbf{w}_j = \phi_j(\mathbf{z}_j); \mathbf{v}_j \in \mathrm{B}_{3m}$. This implies that $\phi_j(\mathbf{z}_j - \mathbf{s}_j) = \mathbf{v}_j \in \mathrm{B}_{3m}$. Let $\mathbf{v}'_j := \mathbf{z}_j - \mathbf{s}_j = \phi_j^{-1}(\mathbf{v_j})$, then we obtain that $\mathbf{A}'\Big(\sum_{j=0}^{k-1} 2^j \cdot \mathbf{v}'_j\Big) = \mathbf{y} \bmod q$ and $\mathbf{v}'_j \in \mathrm{B}_{3m}$. Then for each $\mathbf{v}'_j$, we drop the last $2m$ coordinates to obtain $\widetilde{\mathbf{v}'_j} \in \{-1, 0, 1\}^m$. Now we have $\mathbf{A}\Big(\sum_{j=0}^{k-1} 2^j \cdot \widetilde{\mathbf{v}'_j}\Big) = \mathbf{y} \bmod q$. Let $\mathbf{x}' = \sum_{j=0}^{k-1} 2^j \cdot \widetilde{\mathbf{v}'_j}$. Then $\mathbf{A}\mathbf{x}' = \mathbf{y} \bmod q$, and

$$\|\mathbf{x}'\|_\infty \leq \sum_{j=0}^{k-1} 2^j \cdot \|\widetilde{\mathbf{v}'_j}\|_\infty \leq \sum_{j=0}^{k-1} 2^j = \sum_{j=0}^{\lfloor \lg \beta \rfloor} 2^j = 2^{\lfloor \lg \beta \rfloor + 1} - 1 \leq 2\beta - 1.$$

The knowledge extractor outputs $\mathbf{x}'$, which satisfies $((\mathbf{A}, \mathbf{y}; \mathbf{x}') \in \mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,2\beta-1}}$.

### 2.5 A Scheme Variant with No Gap

In a personal communication, D. Micciancio indicated to the authors a modification of the **SternExt** proof system that removes the extraction gap entirely. Instead of relying on powers of 2, one can use the following sequence of integers: $b_1 = \lceil \beta/2 \rceil$, $b_2 = \lceil (\beta - b_1)/2 \rceil$, $b_3 = \lceil (\beta - b_1 - b_2)/2 \rceil$, ... , and 1. One obtains a sequence of numbers of length $k = \lfloor \lg \beta \rfloor + 1$, whose subset sums are precisely the numbers between 0 and $\beta$. Finally, any integer in this interval can be efficiently expressed as a subset sum of the integers in the sequence.

## 3 Applications

Our results described in Section 2 yield the potential of enabling weaker security assumptions and lower complexities for various lattice-based cryptographic constructions. In this section, we will describe two applications of the **SternExt** proof system: an improved ID-based identification scheme and a new **ZKPoPK** for Regev's encryption scheme [Reg05, Reg09].

### 3.1 Identity-Based Identification

**Definition 2 ([BNN09]).** *An* identity-based identification (IBI) scheme *is a tuple of four* PPT *algorithms* $(\mathrm{MKg}, \mathrm{UKg}, \overline{\mathrm{P}}, \overline{\mathrm{V}})$*:*

- $\mathrm{MKg}(1^n)$*: On input* $1^n$*, output a master public and master secret key pair* $(mpk, msk)$.
- $\mathrm{UKg}(msk, id)$*: On input* $msk$ *and a user identity* $id \in \{0,1\}^*$*, output a secret key* $sk_{id}$ *for this user.*
- $\langle \overline{\mathrm{P}}, \overline{\mathrm{V}} \rangle$ *is an interactive protocol. The prover* $\overline{\mathrm{P}}$ *takes* $(mpk, id, sk_{id})$ *as input, the verifier* $\overline{\mathrm{V}}$ *takes* $(mpk, id)$ *as input. At the end of the protocol,* $\overline{\mathrm{V}}$ *outputs* 1 *(accept) or* 0 *(reject).*

The completeness requirement for an IBI scheme is as follows: For any $mpk$ generated by $\mathrm{MKg}(1^n)$, and $sk_{id}$ extracted by $\mathrm{UKg}(msk, id)$, the decision of $\overline{\mathrm{V}}$ after interacting with $\overline{\mathrm{P}}$ is always 1. We refer the reader to [BNN09] for formal definitions of security notions for IBI schemes.

A common strategy in constructing IBI schemes consists in combining a signature scheme and a **PoK** in the following way: The trusted authority generates $(mpk, msk)$ as a verification key - signing key pair of a signature scheme; whenever a user $id$ queries for his secret key, the authority returns $sk_{id}$ as a signature on $id$; for identification, the user plays the role of the prover, and runs a **PoK** to prove the possession of $sk_{id}$. If the signature scheme is strongly secure against existential forgery under chosen message attacks, and the **PoK** is at least witness-indistinguishable, then the resulting IBI scheme is secure against impersonation under concurrent attacks [BNN09]. This strategy is widely used for lattice-based IBI schemes. Stehlé et al. [SSTX09] combined the GPV signature scheme [GPV08], and the Micciancio-Vadhan [MV03] **PoK** to obtain an

IBI scheme based on the hardness of the $\mathrm{SIVP}_{\widetilde{O}(n^2)}$ problem (in the $\ell_2$ norm). Rückert [Rüc10a] combined the Bonsai tree signature scheme [CHKP10] and Lyubashevsky's **PoK** [Lyu08] for ideal lattices to produce an IBI scheme based on the hardness of the restriction of $\mathrm{SVP}_{\widetilde{O}(n^{3.5})}$ to ideal lattices (in the $\ell_\infty$ norm).

Following the same approach, the **SternExt** proof system allows us to achieve better in terms of security assumption. Since **SternExt** is zero-knowledge, it has the witness-indistinguishability (**WI**) property. As **WI** is preserved under parallel composition [FS90], we can repeat the protocol $\omega(\log n)$ times in parallel to obtain a **WIPoK** with negligible soundness error. Combining with the GPV signature scheme, we obtain a secure IBI scheme in the random oracle model with hardness assumption $\mathrm{SIVP}_{\widetilde{O}(n^{1.5})}$. At first, we review the trapdoor generation and preimage sampling algorithms used in [GPV08], which will essentially serve as the $\mathrm{MKg}(1^n)$ and $\mathrm{UKg}(msk, id)$ algorithms in our IBI scheme. The following trapdoor generation algorithm was introduced in [Ajt99], improved in [AP11], and recently simplified in [MP12].

**Lemma 1 ([AP11, MP12]).** *Let $q \geq 2$ and $m \geq 6n \lg q$. There is a* PPT *algorithm* $\mathrm{TrapGen}(n, m, q)$ *that outputs a matrix $\mathbf{A}$ statistically close to uniform in $\mathbb{Z}_q^{n\times m}$, and a basis $\mathbf{T_A} \in \mathbb{Z}^{m\times m}$ for $\Lambda_q^\perp(\mathbf{A})$ satisfying $\|\widetilde{\mathbf{T_A}}\| \leq O(\sqrt{n \lg q})$.*

Given an integer lattice $\mathbf{L}$, the discrete Gaussian distribution $\mathrm{D}_{\mathbf{L},\sigma,\mathbf{c}}$ with parameter $\sigma$ is the $m$-dimensional Gaussian distribution centered at $\mathbf{c}$, with support restricted to the lattice $\mathbf{L}$. Given a basis $\mathbf{B}$ for $\mathbf{L}$, the distribution $\mathrm{D}_{\mathbf{L},\sigma,\mathbf{c}}$ can be sampled efficiently for $\sigma \geq \|\widetilde{\mathbf{B}}\|\omega(\sqrt{\log m})$.

**Lemma 2 ([GPV08]).** *Let $q \geq 2$ and $m \geq n$. Let $\mathbf{A}$ be a matrix in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{T_A}$ be a basis for $\Lambda_q^\perp(\mathbf{A})$. Then for $\mathbf{y}$ in the image of $\mathbf{A}$ and $\sigma \geq \|\widetilde{\mathbf{T_A}}\|\omega(\sqrt{\log m})$, there is a* PPT *algorithm* $\mathrm{SampleISIS}(\mathbf{A}, \mathbf{T_A}, \mathbf{y}, \sigma)$ *that outputs $\mathbf{x} \in \mathbb{Z}^m$ sampled from the distribution $\mathrm{D}_{\mathbb{Z}^m,\sigma,\mathbf{0}}$, conditioned on the event that $\mathbf{Ax} = \mathbf{y} \bmod q$.*

Let $\mathbf{x}$ be the output of $\mathrm{SampleISIS}(\mathbf{A}, \mathbf{T_A}, \mathbf{y}, \sigma)$. Gentry et al. [GPV08] noted that for any fixed function $t(m) \geq \omega(\sqrt{\log m})$, one has $\|\mathbf{x}\|_\infty \leq \sigma \cdot t$ with overwhelming probability. If $\mathbf{T_A}$ is a basis generated by $\mathrm{TrapGen}(n, m, q)$, then we can take $\sigma = O(\sqrt{n \lg q}) \cdot \omega(\sqrt{\log m})$. In this case, let $\beta = \lceil \sigma \cdot t \rceil = \widetilde{O}(\sqrt{n})$. Now let $\mathrm{H} : \{0,1\}^* \to \mathbb{Z}_q^n$ be the random oracle used in the GPV signature. For parameters $(m, q, \beta, \sigma)$ as described above, we obtain the following IBI scheme:

- $\mathrm{MKg}(1^n)$: Run algorithm $\mathrm{TrapGen}(n, m, q)$ to output a master public key $mpk = \mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a master secret key $msk = \mathbf{T_A} \in \mathbb{Z}^{m\times m}$.
- $\mathrm{UKg}(msk, id)$: For $id \in \{0,1\}^*$, let $sk_{id} = \mathrm{SampleISIS}(\mathbf{A}, \mathbf{T_A}, \mathrm{H}(id), \sigma)$. If $\|sk_{id}\|_\infty > \beta$ (which happens with negligible probability) then restart. Otherwise, output $sk_{id}$ as the secret key for identity $id$. We note that $sk_{id}$ is the GPV signature for the message $id$, and is a solution to the $\mathrm{ISIS}^\infty_{n,m,q,\beta}$ instance $(\mathbf{A}, \mathrm{H}(id))$.
- $\langle \overline{\mathrm{P}}, \overline{\mathrm{V}} \rangle$: The common input is the pair $(\mathbf{A}, \mathrm{H}(id))$. The auxiliary input of $\overline{P}$ is $sk_{id}$. Then $\overline{P}$ and $\overline{V}$ play the roles of the prover and the verifier in the **SternExt** protocol. The protocol is repeated $l = \omega(\log n)$ times in parallel to make the soundness error negligibly small.

The completeness of the obtained IBI scheme follows from the perfect completeness of **SternExt**. Since the GPV signature scheme is strongly secure against existential forgery under chosen message attacks [GPV08], and the **SternExt** protocol is a **WIPoK**, the obtained IBI scheme is secure against impersonation under concurrent attacks. The scheme relies on the assumed hardness of the $\mathrm{ISIS}^{\infty}_{n,m,q,2\beta-1}$ problem, where $\beta = \widetilde{O}(\sqrt{n})$. It follows from Theorem 1 that solving the $\mathrm{ISIS}^{\infty}_{n,m,q,2\beta-1}$ problem is at least as hard as solving $\mathrm{SIVP}^{2}_{\gamma}$ (in the $\ell_2$ norm) with $\gamma = (2\beta-1)\cdot\widetilde{O}(n) = \widetilde{O}(n^{1.5})$.

**Theorem 4.** *The obtained* IBI *scheme is concurrently secure in the random oracle model if the* $\mathrm{SIVP}_{\widetilde{O}(n^{1.5})}$ *problem is hard (in the worst-case).*

Similarly, combining the **SternExt** proof system with lattice-based signature schemes that are secure in the standard model (e.g., [CHKP10, Boy10, MP12]) we can obtain secure lattice-based IBI schemes in the standard model, with weaker security assumptions than in the contemporary schemes.

### 3.2 Proof of Plaintext Knowledge for Regev's Cryptosystem

Regev's LWE-based encryption scheme is as follows:

- **Parameters:** Integers $n, m, q$, an integer $p \ll q$ and a real $\alpha > 0$.
- **Private key:** The private key is $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$.
- **Public key:** Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and $\mathbf{e} \xleftarrow{\$} (\overline{\Psi}_\alpha(q))^m$ , where $\overline{\Psi}_\alpha(q)$ is the LWE error distribution [Reg05, Reg09]. The public key is
$$(\mathbf{A}, \mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m.$$
- **Encryption:** The message space is $\{0, \ldots, p-1\}$. Given a message $M$, and the public key $(\mathbf{A}, \mathbf{b})$, choose a uniformly random[2] integer vector $\mathbf{r} \xleftarrow{\$} \{0, \ldots, p-1\}^m$, and output the ciphertext
$$(\mathbf{u}, c) = (\mathbf{A}\mathbf{r}, \mathbf{b}^T\mathbf{r} + M \cdot \lfloor q/p \rfloor) \in \mathbb{Z}_q^n \times \mathbb{Z}_q.$$
- **Decryption:** Given the ciphertext $(\mathbf{u}, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, and the private key $\mathbf{s} \in \mathbb{Z}_q^n$, output $M = \lfloor (c - \mathbf{s}^T\mathbf{u}) \cdot p/q \rceil$.

For the correctness, security, and parameters selection of this cryptosystem we refer to [Reg09]. We now show how to derive a **PoPK** for this encryption scheme from a **PoK** for the relation $\mathrm{R}_{\mathrm{ISIS}^\infty}$. A **PoPK** for Regev's cryptosystem is a **PoK** for the following relation:

$$\mathrm{R}_{\mathrm{Regev}} = \Big\{((\mathbf{A}, \mathbf{b}), (\mathbf{u}, c), \mathbf{r} \| M) \in (\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m) \times (\mathbb{Z}_q^n \times \mathbb{Z}_q) \times \{0, \ldots, p-1\}^{m+1} : (\mathbf{u} = \mathbf{A}\mathbf{r}) \wedge (c = \mathbf{b}^T\mathbf{r} + M \cdot \lfloor q/p \rfloor)\Big\}.$$

[2] In fact, the proof system can be adapted to any nonce distribution, as long as $\|\mathbf{r}\|_\infty$ is bounded by some $B$ sufficiently smaller than $q$.

We form the following matrix:

$$\mathbf{A}' = \left[\begin{array}{c|c} \multirow{2}{*}{$\mathbf{A}$} & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline \mathbf{b}^{\mathrm{T}} & \lfloor q/p \rceil \end{array}\right] \in \mathbb{Z}_q^{(n+1)\times(m+1)},$$

and let $\mathbf{y} = (\mathbf{u} \| c) \in \mathbb{Z}_q^{n+1}$. Let $\mathbf{x} = (\mathbf{r} \| M)$ be any witness of the relation $\mathrm{R}_{\mathrm{Regev}}$. Then we have $\mathbf{x} \in \mathbb{Z}^{m+1}$, and $\|\mathbf{x}\|_\infty \leq p-1$. Moreover, we observe that $\mathbf{A}'\mathbf{x} = \mathbf{y} \bmod q$. Therefore, vector $\mathbf{x}$ is a solution to the $\mathrm{ISIS}^\infty$ problem with parameters $(n+1, m+1, q, p-1)$ defined by $(\mathbf{A}', \mathbf{y})$. In other words, we have shown that the relation $\mathrm{R}_{\mathrm{Regev}}$ can be embedded into the relation $\mathrm{R}_{\mathrm{ISIS}^\infty_{n+1,m+1,q,p-1}}$. We then run the **SternExt** protocol for the relation $\mathrm{R}_{\mathrm{ISIS}^\infty_{n+1,m+1,q,p-1}}$ to obtain an efficient **ZKPoPK** for Regev's encryption scheme.

If a cheating prover succeeds in proving the knowledge of a plaintext $\mathbf{x} = (\mathbf{r} \| M)$, then we use the knowledge extractor to output a vector $\mathbf{x}' = (\mathbf{r}' \| M') \in \mathbb{Z}^{m+1}$ such that $\|\mathbf{x}'\|_\infty \leq 2 \cdot (p-1) - 1 = 2p-3$. In particular, we obtain $\mathbf{r}' \in \mathbb{Z}^m$ such that $\|\mathbf{r}'\|_\infty \leq 2p-3$ and $\mathbf{A}\mathbf{r}' = \mathbf{u} \bmod q$. Since $\mathbf{A}$ is chosen uniformly at random in $\mathbb{Z}_q^{n\times m}$, and the distribution of $\mathbf{u}$ is statistically close to uniform over $\mathbb{Z}_q^n$ (see [Reg09, Section 5]), the vector $\mathbf{r}'$ is a solution to the random $\mathrm{ISIS}^\infty_{n,m,q,2p-3}$ instance $(\mathbf{A}, \mathbf{u})$. This implies that the security of our **ZKPoPK** for Regev's encryption scheme relies on the assumed hardness of $\mathrm{SIVP}_{p\cdot\widetilde{O}(n)}$ (in the $\ell_2$ norm).

**Acknowledgements.** The authors would like to thank D. Micciancio and the anonymous reviewers for their helpful comments. This work was supported by the LaBaCry MERLION grant. The research of S. Ling and H. Wang is also supported by the National Research Foundation Singapore under the Competitive Research Programme (NRF-CRP2-2007-03). Part of this research was undertaken while S. Ling was visiting ÉNS de Lyon as an invited professor. D. Stehlé was partly supported by the Australian Research Council Discovery Grant DP110100628.

## References

[ABB10a] Agrawal, S., Boneh, D., Boyen, X.: Efficient Lattice (H)IBE in the Standard Model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010)

[ABB10b] Agrawal, S., Boneh, D., Boyen, X.: Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 98–115. Springer, Heidelberg (2010)

[AJLA+12] Asharov, G., Jain, A., López-Alt, A., Tromer, E., Vaikuntanathan, V., Wichs, D.: Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 483–501. Springer, Heidelberg (2012)

[Ajt96] Ajtai, M.: Generating Hard Instances of Lattice Problems (Extended Abstract). In: Proc. of STOC 1996, pp. 99–108. ACM (1996)

[Ajt99] Ajtai, M.: Generating Hard Instances of the Short Basis Problem. In: Wiedermann, J., Van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol. 1644, pp. 1–9. Springer, Heidelberg (1999)

[AP11] Alwen, J., Peikert, C.: Generating Shorter Bases for Hard Random Lattices. Theory of Computing Systems 48(3), 535–553 (2011)

[BD10] Bendlin, R., Damgård, I.: Threshold Decryption and Zero-Knowledge Proofs for Lattice-Based Cryptosystems. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 201–218. Springer, Heidelberg (2010)

[BDOZ11] Bendlin, R., Damgård, I., Orlandi, C., Zakarias, S.: Semi-homomorphic Encryption and Multiparty Computation. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 169–188. Springer, Heidelberg (2011)

[BG93] Bellare, M., Goldreich, O.: On Defining Proofs of Knowledge. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 390–420. Springer, Heidelberg (1993)

[BNN09] Bellare, M., Namprempre, C., Neven, G.: Security Proofs for Identity-Based Identification and Signature Schemes. Journal of Cryptology 22(1), 1–61 (2009)

[Boy10] Boyen, X.: Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 499–517. Springer, Heidelberg (2010)

[CH91] Chaum, D., van Heyst, E.: Group Signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)

[CHKP10] Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai Trees, or How to Delegate a Lattice Basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010)

[CNR12] Camenisch, J., Neven, G., Rückert, M.: Fully Anonymous Attribute Tokens from Lattices. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 57–75. Springer, Heidelberg (2012)

[DLA12] Damgård, I., López-Alt, A.: Zero-Knowledge Proofs with Low Amortized Communication from Lattice Assumptions. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 38–56. Springer, Heidelberg (2012)

[FFS87] Fiege, U., Fiat, A., Shamir, A.: Zero Knowledge Proofs of Identity. In: Proc. of STOC 1987, pp. 210–217. ACM (1987)

[FS89] Feige, U., Shamir, A.: Zero Knowledge Proofs of Knowledge in Two Rounds. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 526–544. Springer, Heidelberg (1990)

[FS90] Feige, U., Shamir, A.: Witness Indistinguishable and Witness Hiding Protocols. In: Proc. of STOC 1990, pp. 416–426. ACM (1990)

[GG98] Goldreich, O., Goldwasser, S.: On the Limits of Non-Approximability of Lattice Problems. In: Proc. of STOC 1998, pp. 1–9. ACM (1998)

[GKV10] Gordon, S.D., Katz, J., Vaikuntanathan, V.: A Group Signature Scheme from Lattice Assumptions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 395–412. Springer, Heidelberg (2010)

[GMR89] Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems. SIAM J. Comput. 18(1), 186–208 (1989)

[GMR05] Guruswami, V., Micciancio, D., Regev, O.: The Complexity of the Covering Radius Problem. Computational Complexity 14(2), 90–121 (2005)

[Gol04] Goldreich, O.: The Foundations of Cryptography. Basic Techniques, vol. 1. Cambridge University Press (2004)

[GPV08] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for Hard Lattices and New Cryptographic Constructions. In: Proc. of STOC 2008, pp. 197–206. ACM (2008)

[GQ90] Guillou, L.C., Quisquater, J.-J.: A "Paradoxical" Identity-Based Signature Scheme Resulting from Zero-Knowledge. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 216–231. Springer, Heidelberg (1990)

[IKOS07] Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-Knowledge from Secure Multiparty Computation. In: Proc. of STOC 2007, pp. 21–30. ACM (2007)

[JKPT12] Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 663–680. Springer, Heidelberg (2012)

[KTX08] Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 372–389. Springer, Heidelberg (2008)

[Lyu08] Lyubashevsky, V.: Lattice-Based Identification Schemes Secure Under Active Attacks. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 162–179. Springer, Heidelberg (2008)

[Mau09] Maurer, U.: Unifying Zero-Knowledge Proofs of Knowledge. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 272–286. Springer, Heidelberg (2009)

[MP12] Micciancio, D., Peikert, C.: Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012)

[MR07] Micciancio, D., Regev, O.: Worst-case to Average-case Reductions based on Gaussian Measures. SIAM J. Comput. 37(1), 267–302 (2007)

[MR09] Micciancio, D., Regev, O.: Lattice-Based Cryptography. In: Post-Quantum Cryptography, pp. 147–191. Springer (2009)

[MV03] Micciancio, D., Vadhan, S.P.: Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 282–298. Springer, Heidelberg (2003)

[Pei09] Peikert, C.: Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem: Extended Abstract. In: Proc. of STOC 2009, pp. 333–342. ACM (2009)

[PV08] Peikert, C., Vaikuntanathan, V.: Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 536–553. Springer, Heidelberg (2008)

[Reg05] Regev, O.: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In: Proc. of STOC 2005, pp. 84–93. ACM (2005)

[Reg09] Regev, O.: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. J. ACM 56(6) (2009)

[RS92] Rackoff, C., Simon, D.R.: Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992)

[Rüc10a] Rückert, M.: Adaptively Secure Identity-Based Identification from Lattices without Random Oracles. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 345–362. Springer, Heidelberg (2010)

[Rüc10b] Rückert, M.: Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS, vol. 6061, pp. 182–200. Springer, Heidelberg (2010)

[Sha85] Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

[SSTX09] Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient Public Key Encryption Based on Ideal Lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (2009)

[Ste96] Stern, J.: A New Paradigm for Public Key Identification. IEEE Transactions on Information Theory 42(6), 1757–1768 (1996)

[Vér96] Véron, P.: Improved Identification Schemes based on Error-Correcting Codes. Appl. Algebra Eng. Commun. Comput. 8(1), 57–69 (1996)

## A A Zero-Knowledge Proof of Knowledge for SIS

We consider the relation associated to the $\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ problem:

$$\mathrm{R}_{\mathrm{SIS}^{\infty}_{n,m,q,\beta}} = \left\{(\mathbf{A},\mathbf{x}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^m \colon (0 < \|\mathbf{x}\|_\infty \leq \beta) \wedge (\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q)\right\}.$$

We now show how to modify the **SternExt** proof system for $\mathrm{R}_{\mathrm{ISIS}^{\infty}_{n,m,q,\beta}}$ in Section 2 to handle the additional requirement on the witness, i.e., $\mathbf{x} \neq \mathbf{0}$. In particular, the protocol must prevent a cheating prover using $\mathbf{x} = \mathbf{0}$ from passing the verification step. We look at the binary decomposition of $\mathbf{x}$, i.e., $\mathbf{x} = \sum_{j=0}^{k-1} 2^j \cdot \tilde{\mathbf{u}}_j$, and observe that $\mathbf{x} = \mathbf{0}$ is equivalent to $\forall j : \tilde{\mathbf{u}}_j = \mathbf{0}$. Our idea is to constrain the prover to prove in zero-knowledge that (at least) one of his $\tilde{\mathbf{u}}_j$'s is non-zero.

Now, observe that if $\mathbf{x} = (x_1, \ldots, x_m)$ is a valid witness for $\mathrm{R}_{\mathrm{SIS}^{\infty}_{n,m,q,\beta}}$, and $2^l$ is the highest power of 2 dividing $\gcd(x_1, \ldots, x_m)$, then $\mathbf{x}^* = (x_1/2^l, \ldots, x_m/2^l)$ is also a valid witness for $\mathrm{R}_{\mathrm{SIS}^{\infty}_{n,m,q,\beta}}$. Applying the binary decomposition to the vector $\mathbf{x}^*$, we note that the vector $\tilde{\mathbf{u}}_0^*$, whose coordinates are the least significant bits of $x_1/2^l, \ldots, x_m/2^l$, must be non-zero. To prove the knowledge of such a vector $\tilde{\mathbf{u}}_0^*$, the prover can use the extension trick, but in dimension $3m-1$ instead of dimension $3m$. More precisely, the prover appends $2m-1$ coordinates to $\tilde{\mathbf{u}}_0^*$ to get a vector $\mathbf{u}_0^*$ that has exactly $m$ coordinates equal to 1; $m$ coordinates equal to $-1$; and $m-1$ coordinates equal to 0. Seeing a permutation of $\mathbf{u}_0^*$ that has these constraints, the verifier will be convinced that the original vector $\tilde{\mathbf{u}}_0^*$ must have *at least* one coordinate equal to 1 or $-1$, and thus it must be non-zero.

In summary, the modified **SternExt** proof system for $\mathrm{R}_{\mathrm{SIS}^{\infty}_{n,m,q,\beta}}$ works as follows: The common input is a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. The auxiliary input of the prover is $\mathbf{x}$. Prior to the interaction, both parties append $2m-1$ and $2m$ zero-columns to the matrix $\mathbf{A}$ to get a matrix $\mathbf{A}^*$, and a matrix $\mathbf{A}'$, respectively. In addition, the prover performs the following preparation steps:

- Shifting: Map $\mathbf{x}$ to $\mathbf{x}^*$, as described above.
- Binary decomposition: Write $\mathbf{x}^* = \sum_{j=0}^{k-1} 2^j \cdot \tilde{\mathbf{u}}_j^*$.
- Extensions: Append $(2m-1)$ coordinates to $\tilde{\mathbf{u}}_0^*$ as described above, and perform the usual extension to dimension $3m$ for the other vectors $\tilde{\mathbf{u}}_1^*, \ldots, \tilde{\mathbf{u}}_{k-1}^*$.

We note that $\mathbf{A}^*\mathbf{u}_0^* + \mathbf{A}'(\sum_{j=1}^{k-1} 2^j \cdot \mathbf{u}_j^*) = \mathbf{0} \bmod q$ is equivalent to $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$. Therefore, we can now apply the **SternExt** proof with a small tweak: The constraints of $\mathbf{u}_0^*$ are verified using a random permutation of $3m-1$ elements. This leads to a **ZKPoK** for the $\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ problem.