Aalto University
School of Science

Master’s Programme in Security and Cloud Computing

Cryptographic Primitives from the Lattice Isomorphism Problems

Huan Pham

Master’s Thesis
2025

Aalto University
School of Science

Author Huan Pham

Title Cryptographic Primitives from the Lattice Isomorphism Problems

Degree programme Security and Cloud Computing

Major Security and Cloud Computing

Supervisor Prof. Russell W. F. Lai (Aalto University) and Prof. Antonio Faonio (EURECOM)

Advisor Prof. Russell W. F. Lai

Date 31 Aug 2025 **Number of pages** 75 **Language** English

Abstract

The Lattice Isomorphism Problem (LIP) is an emerging foundation for post-quantum cryptography thanks to the pioneering work of Ducas and van Woerden (EUROCRYPT ’22). That work lays the foundation for LIP in cryptography with a zero-knowledge proof of knowledge (ZKPoK), a key-encapsulation mechanism, and a digital signature scheme which is further developed into the efficient signature Hawk (ASIACRYPT ’22) using structured lattices. However, as compared to the development of lattice-based cryptography from the Short Integer Solution (SIS) and Learning with Errors (LWE) problems, LIP-based cryptography is yet to cover a rich variety of functionalities beyond the two basic ones: encrypting and digitally signing messages. This work is an effort to extend the landscape of LIP-based cryptography from the above basic primitives to more advanced ones by adapting techniques used in SIS-based and LWE-based primitives to LIP. We provide a public-key encryption (PKE) which encrypts plaintexts of integral vectors, and it comes with a zero-knowledge proof of plaintext knowledge. We use this PKE as a commitment scheme in the construction of a ZKPoK for quadratic relations, so this ZKPoK has a straightline extractor naturally. Using the same ZKPoK in non-interactive mode by Fiat-Shamir transformation, we introduce the first LIP-based blind signature scheme which is the blinded version of the digital signatures of Ducas and van Woerden. The security of our scheme stems from a new one-more Close Vector Problem (omCVP) assumption. This assumption is arguably an analogue of the one-more-SIS assumption by Agrawal et al. (CCS ’22) and the one-more Short Vector Problem in Hawk signatures. To ensure confidence in omCVP, we provide a cryptanalysis attempt and convince that our parameter choice is in the safe zone.

Keywords Lattice-based Cryptography, Post-Quantum Cryptography, Lattice Isomorphism Problems, Public-Key Encryption, Blind Signatures, Zero-Knowledge Proofs

Preface

Firstly, I want to thank Professor Russell W. F. Lai and Professor Antonio Faonio for their supervision. Secondly, I want to express my gratitude to the European Union for funding my Master's studies via the Erasmus Mundus scholarship grant. Last but not least, I would like to give thanks to Dr. Michael Klooß for discussions on Zero-Knowledge Proofs, Fiat-Shamir transformation, and Fischlin transformation, Michał Osadnik for helping me to understand Lattice-based Zero-Knowledge Proofs, and all other members of the Aalto Cryptography group for their encouragement and support during this thesis.

Espoo, 31 August 2025

Huan Pham

Co-funded by
the European Union

Contents

Symbols and abbreviations

Symbols

$\mathbf{B}$	matrix
$\mathbf{v}$	vector
$\mathbb{R}$	set of real numbers
$\mathbb{Z}$	set of integers
$\mathbb{N}$	set of natural numbers
$\mathbb{Z}_q$	balancedly represented set of integers modulo q, $(-q/2, q/2] \cap \mathbb{Z}$
$\mathbb{T}_q$	balancedly represented discretised torus $(-1/2, 1/2] \cap \frac{1}{q} \cdot \mathbb{Z}$
$[n]$	set of integers from 1 to n for $n \in \mathbb{N}$ and $n > 0$, $\{1, \ldots, n\}$

Operators

$\mathbf{B}^{\mathsf{T}}$	transpose of a matrix or a vector
$\mathbf{B}^{\mathsf{GS}}$	Gram-Schmidt orthogonalisation of a matrix
$\lVert\mathbf{v}\rVert$	Euclidean norm of a vector
$\lVert\mathbf{x}\rVert_{\mathbf{Q}}$	Norm of a vector w.r.t. to a Gram matrix $\mathbf{Q}$

Abbreviations

PKE	Public-Key Encryption
LIP	Lattice Isomorphism Problem
LWE	Learning with Errors
SIS	Short Integer Solutions
SIVP	Shortest Independent Vectors Problem
SVP	Shortest Vector Problem
GL	General Linear
omCVP	One-more Close Vector Problem
omSIS	One-more Short Integer Solution
ZKPoK	Zero-Knowledge Proof of Knowledge
NIZKPoK	Non-Interactive Zero-Knowledge Proof of Knowledge

1 Introduction

Classical public-key cryptosystems which we are using to secure our private data on the Internet are under a significant threat of quantum computing. The security of such cryptosystems relies on the hardness of computational problems such as factoring integers and finding discrete logarithms. In the 1990s, Peter Shor developed quantum algorithms [Sho99] to solve these computational problems in polynomial-time with a large enough quantum computer. Recently, Regev has made an improve [Reg25] to those algorithms, and for the advances in building quantum computers in the last decade, the quantum threat against the classical public-key cryptosystems is more imminent than ever before. In order to protect our information systems against the quantum threat, there have been a vast amount of effort to develop new cryptosystems which are resistant to both classical and quantum attacks. This marked the beginning of the field of post-quantum cryptography. Lattice-based cryptosystems stand out among the leading candidates for post-quantum cryptography.

Lattices are discrete subgroups of a multidimensional space $\mathbb{R}^n$. The security of lattice-based cryptography relies on the assumption that computational problems on lattices are hard. Some notable examples of these problems are the shortest vector problem (SVP) and the shortest independent vectors problem (SIVP). In 1996, Ajtai [Ajt96] brought these problems to cryptographic applications, laying the foundation stone of lattice-based cryptography. He proposed the Short Integer Solution (SIS) problem and proved that it is at least as hard as SIVP under certain parameters. The (SIS) problem askes one to find a short solution (preimage) $\mathbf{x}$ to the linear equations $\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$, given an integer q and a public random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. Later in 2005, Regev introduced another fundamental problem in lattice-based cryptography, the Learning with Errors (LWE) problem [Reg09]. The search variant of LWE askes one to recover a secret vector $\mathbf{s} \in \mathbb{Z}_q^m$ given the evaluation of noisy linear function $\mathbf{b}^\top = \mathbf{s}^\top\mathbf{A} + \mathbf{e}^\top \bmod q$ where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is a public random matrix and $\mathbf{e} \in \mathbb{Z}_q^m$ is an noise vector of short coefficients (i.e., the errors). Its decisional variant askes to distinguish such vector $\mathbf{b}$ from a uniformly random one from $\mathbb{Z}_p^m$.

Throughout more than a decade of lattice-based cryptography research, SIS and LWE assumptions have enabled cryptographer to construct not only standard primitives such as digital signatures [GPV08, Lyu12] and public-key encryption [Reg09] but also advanced ones such as fully-homomorphic encryption (FHE) [Gen09, BGV12, GSW13]. FHE is a powerful cryptographic notion allowing an untrusted party to perform arbitrary computations on encrypted data without learning anything about those data. Until the first candidate construction by Gentry in 2009 [Gen09] from lattices, FHE was an open question for three decades. Recent lines of works explore structural variations of SIS and LWE which utilise algebraic lattices to build more efficient primitives [LPR13] and hinted variations (i.e., providing some hints for solving SIS and LWE) to realise primitives with interesting functionalities such as blind signatures [AKSY22], broadcast encryption [Wee22], and succint non-interactive argument of knowledge systems [ACL+22]. The central idea of lattice-based cryptography is that the secret key is a "good" lattice basis comprising particularly short and as orthogonal as possible vectors while the public key is a random "bad" basis of the same lattice.

This "bad" basis contains long and non-orthogonal vectors. It is easy for one with the "good" basis to decrypt or sign a message while it is computationally hard for one with the "bad" one to do the same.

The Lattice Isomorphism Problem (LIP) has emerged to add a new flavour to lattice-based cryptography by suggesting to use remarkable lattices with special geometric properties in building cryptosystems. LIP, in the search variant, askes to compute an isometry (if any) between two given lattices Λ_1 and Λ_2. Therefore, to set up public-key cryptography from LIP, the public key is a random rotation of a lattice with some good geometric feature, and the secret key is the rotation information. The work of Haviv and Regev [HR14] is the first to study the worst-case hardness of LIP, and their proposed algorithm remains the best algorithm to solve LIP. Ducas and van Woerden [DvW22] later provide a worst-case-to-average-case reduction for LIP and introduce it into cryptography with an identification scheme, a key encapsulation mechanism, and a hash-then-sign signature scheme. Subsequently, the practical Hawk signature scheme based on the module variant of LIP is introduced [DPPvW22], and it achieves better performance than Falcon [FHK+20], one of the standardised lattice-based signature schemes. Meanwhile, in an independent work, Bennett et al. [BGPSD23] studied LIP restricting to the integer lattice $\mathbb{Z}^n$ and its rotations, and they propose a public-key encryption (PKE). This scheme was then generalised to random lattices in [ARLW24]. Starting with such standard primitives, one may ask whether we could extend the current landscape of LIP-based cryptography to realise more advanced primitives by adapting the techniques of those based on SIS and LWE.

From a signature scheme, we can attempt to design it to a blind signature scheme. Blind signatures were first introduced by Chaum for e-cash [Cha83], and it was found useful in other applications including e-voting [IKSA03] and cryptocurrencies [HBG16]. A blind signature scheme is an interactive protocol between a signer holding a secret key and a user holding a public key to jointly produce a signature to a message such that this message is oblivious to the signer during the issuance time (blindness) while no additional signatures can be made without the signer (unforgeability). In blind signatures, the signing usually takes multi rounds of interaction, which is susceptible to failures due to network disruption. To achieve round-optimality, one can use the Fischlin construction [Fis06] to build a blind signature scheme from a standard signature scheme, a PKE, and a general-purpose non-interactive zero-knowledge proof of knowledge (NIZKPoK). Among constructions using lattices, Agrawal et al. [AKSY22] adapts the instantiation of Fischlin construction on GPV signatures [GPV08] to one using the more efficient lattice-based NIZKPoK for linear relations instead of a general-purpose NIZKPoK, and the security of this adaptation is based on the one-more-SIS (omSIS) assumption. For the LIP-based signature is an analogue to the GPV signature, we can take the omSIS-based blind signature scheme as an inspiration to design a blind signature scheme from LIP. However, this entails non-trivial work to construct a zero-knowledge proof system to prove knowledge of LIP-based signature and to adapt LIP-based primitives for better composability. The motivation for LIP-based blind signatures stems from the fact that the Hawk signatures from module-LIP is more efficient than the standardised SIS-based Falcon signatures. For Hawk is the practical adaptation of the DvW signatures [DvW22], constructing a blind signature scheme from the DvW signatures may implies a practical blind signature scheme built upon Hawk, and this scheme might be more efficient than blind signatures built upon Falcon such as the omSIS-based scheme [AKSY22]. Our blind signatures also serve as a candidate post-quantum blind signature scheme in the event that there is a cryptanalytic advance (though unlikely) against SIS or other post-quantum assumptions.

This thesis aims to extend the capabilities of LIP to build more advanced primitives. Though the main goal of this work is to design a LIP-based blind signature, we believe the technical toolkit we provide here is useful for future expansion of LIP-based cryptography.

1.1 Our Contributions

There are two lines of research on LIP-based cryptography. The first line started from [DvW22] exploits lattices with special geometric properties to build cryptographic primitives and uses the hardness of the distinguish variant of LIP to argue their security. As mentioned above, the works of this line gives a zero-knowledge proof of lattice isomorphism, public-key encryption [DvW22, BGPSD23, ARLW24], digital signatures [DvW22, DPPvW22], and recently fully-homomorphic encryption [BMM25, LRvW25]. The second line studies the lattice isomorphism as a cryptographic group action [BBCDK24] and constructs LIP-based primitives using the group action frameworks. So far, we have a commitment scheme [JWL+25] from this approach. While there are group action frameworks to construct various primitives, they are not applicable to LIP since it does not satisfies certain properties as a group action [BBCDK24].

Our work expands the first line with a blind signature scheme. Though it sounds limited, the framework we choose to build our scheme requires an NIZKPoK which allows a user, after interacting with the signer, to prove that he knows the "unblinded" signature of his message, and this proof serves as the "blind" signature. More specifically, we need an NIZKPoK for proving that the prover knows a lattice vector which is close to a non-lattice vector given as a target. Furthermore, this NIZKPoK must come with a straightline extractor to keep the unforgeability proof tight. Our contributions can be summarised as follows:

- We generalise the PKE by Ackermann et al. [ARLW24] from encrypting bits to encrypting vectors in $\mathbb{Z}_p^n$. Our PKE in Section 3 is naturally additively homomorphic, so it implies an additively-homomorphic commitment scheme. Furthermore, we provide a zero-knowledge proof of plaintext knowledge to accommodate the design of verifable-PKE-based NIZKPoK. The witness vector is encrypted, and the proof of plaintext knowledge together with the proof of that the witness vector is close a given target form a non-interactive proof. For any valid proof, the decryptor acts as a straightline extractor.

- We adapt techniques of zero-knowledge proofs for SIS relation to construct a zero-knowledge proof system to prove knowledge of a lattice point whose distance to a given target is short in Section 5. We believe that such zero-knowledge proof is essential in the constructions of not only blind signatures but also other types of advanced signatures based on LIP. We first consider a Schnorr-like-with-Abort protocol adapted from the Lyubashevsky's identification scheme [Lyu12]. Though this ZKPoK is simple to implemnent, it suffers from high soundness error and the soundness slack. While it is trivial to reduce the soundness error by parallel repetitions, it is more challening to compensate the soundness slack (i.e. the knowledge extractor can only extract a witness that is slightly farther from the given target than in the original relation). In the second attempt, we reduce the knowledge of a close vector to a set of quadratic relations and build a ZKPoK for proving these quadratic relations by adapting the technique in [YAZ+19, LNP22a]. This ZKPoK is more complicated but has tight soundness, and it uses the PKE above to commit to the witness, so there is a straightline extractor for free. We then use it (via the Fiat-Shamir transformation) as the NIZKPoK in our blind signatures.

- We give a construction of a blind signature scheme whose security relies on a new *one-more Close Vector Problem* (omCVP) assumption. omCVP can be seen as a LIP analogue of the omSIS [AKSY22] and the one-more-RSA-inversion assumption [BNPS03], both of which are for building blind signatures from SIS and RSA assumptions, respectively. Both our blind signature scheme and the omCVP assumption are direct translations from the lattice-based blind signature scheme and the omSIS assumption in the work of Agrawal et al. [AKSY22]. We also provide a cryptanalysis of our omCVP to identify in which parameter regime that the assumption is prone to polynomial-time attacks and ensure that our parameter regime is within the safe zone.

1.2 Related Works

LIP as a Cryptographic Group Action. Since LIP primitives use quadratic forms (the Gram matrix of the lattice basis) to denote lattices, LIP can be modelled as a cryptographic group action, which opens the door to apply methods of the group action framework formalised in the work of Alamati et al. [ADFMP20] to build various primitives from lattice isomorphism group actions (LIGA). Benčina et al.[BBCDK24] study the properties of LIGA and unfortunately find that LIGA only have one-wayness, while building primitives from the group action framework requires the group action to satisfy weak-unpredictability and weak-pseudorandomness. Duong et al. propose a generic construction of blind signatures from non-communicative group actions [DKQ+25] of which LIGA is one, and Khuc et al. propose a LIGA-based linkable ring signature [KTS+24], but Budroni, Chi-Domínguez and Franch [BCDF25] point out that reusing the isometry transformation (i.e., the LIP secret) twice as in [KTS+24, DKQ+25] breaks the LIP assumption. On the bright side, the Tanuki framework of Hanzlik et al. [HLM+25] for post-quantum group actions such isogenies implies a LIP-based blind signature, though this framework for blind signatures is not round-optimal, and they leave the implementation from LIGA and its module version introduced in Hawk [DPPvW22] for future work. Another group-action-based framework for commitment schemes by Jiang et al. [JWL+25] introduces a LIP-based commitment scheme which is also dual-mode and enhanced linkable. This is followed by the realisation of Module-LIP-based commitments [LJPW25]. Though having a dedicated commitment scheme may be a gateway to privacy-preserving primitives including zero-knowledge proofs, this LIP-based commitment scheme does not work natively with Ducas-van-Woerden LIP-based cryptosystem, e.g., a LIP signature is an integral vector in $\mathbb{Z}^n$ while Jiang et al. commitment commits to a fixed-length bit-string. Given the limitations of LIGA [BBCDK24], it is unlikely we can construct a wide variety of primitives as other group actions such as isogenies. Furthermore, for the fact that the primitives built from LIGA only make use of the lattice isometry for their security while Ducas-van-Woerden primitives utlise both the isometry and the geometric features of remarkable lattices, one can be doubtful about their composability for any advanced constructions.

LIP-based Homomorphic Encryption. Branco, Malavolta and Maradni [BMM25] propose the first FHE from LIP. Their base encryption scheme can be seen as a dual to our scheme such that our scheme has the secret vector sampled by the encryptor while their scheme has the receiver holds the secret vector as part of his secret key. Leporati, Rovida and van Woerden [LRvW25] give a general lattice framework for homomorphic encryption (HE) by examining the current the homomorphic LWE-based cryptosystems under a geometric point of view, and they consider a LIP instantiation but provides no security proof.

Lattice-based Blind Signatures. Constructions from lattices have a dominant place in post-quantum blind signatures literature. Rückert proposes the first lattice-based blind signature scheme [Rüc10] using Lyubashevsky's SIS-based identification scheme [Lyu12]. This line of research follows with a more efficient construction by [AAEBB20]. Hauck et al. [HKLN20] identify flaws in security proofs of those constructions and propose a blind signature construction with provable security based on standard SIS assumption, but this scheme has large signature size (7.73 MB) and is limited to 7 signatures per public key. Lyubashevsky et al. [LNP22b] propose another construction from one-time signatures and OR-proofs and achieve lower signature size of 150 KB despite still allowing only bounded number of signatures. On the constructions based on hash-then-sign paradigm, del Pino and Katsumata [dPK22] introduce the first lattice-based round-optimal blind signature scheme which supports unbounded signing sessions and is secure under standard assumptions. Agrawal et al.[AKSY22] then improves with a more efficient construction with the one-more-SIS assumption which inspires us to translate their framework to LIP. Recently, Beullens et al.[BLNS23] modify the scheme of Agrawal et al. to achieve security under standard assumptions and a shorter signature size, but their blind signature sacrifices the efficiency of the signing session by requiring a general-purpose NIZKPoK to prove knowledge of hash preimage. Lately, the further optimisation by Jeudy and Sanders [JS24] circumvents the use of the inefficient general-purpose NIZKPoK while keep the standard security by their entropy recycling strategy.

1.3 Thesis Organisation

We provide in Section 2 the preliminaries including definitions regarding lattices, LIP, discrete Gaussian distribution, rejection sampling technique, and relevant cryptographic primitives. In Section 3, we present our LIP-based public key encryption which also implies a commitment scheme, and we construct a zero-knowledge proof to prove the ciphertext wellformedness (or commitment opening). We introduce the omCVP assumption in Section 4 and our cryptanalysis attempt which is an adaptation of the cryptanalysis of omSIS in [AKSY22]. In Section 5, we build non-interactive zero-knowledge proofs which are straightline-extractable to prove knowledge of a vector close to a given target. We need such an NIZKPoK for our blind signature scheme, and we describe two choices of such NIZKPoK. The first one is the Fiat-Shamir transformation [FS87] of an approximate ZKPoK of a close vector accompanied with the encryption of the witness using the PKE in Section 3 and the ZKPoK of the ciphertext wellformedness. Using the decryption, we have a straightline extractor to get the witness from an accepted proof. The second one is the Fiat-Shamir transformation of a ZKPoK for a set of quadratic relations to which we reduce the knowledge of a close vector. This ZKPoK has the advantage of having standard soundness while the approximate ZKPoK mentioned above has relaxed soundness. We use the PKE in Section 3 to commit the witness in the second NIZKPoK construction, so we can use the decryption as a straightline extractor. Finally, we introduce the omCVP-based blind signature scheme in Section 6. This blind signature scheme is built upon the LIP-based signature scheme of Ducas and van Woerden [DvW22].

1.4 Open Problems

Instantiating with Module-LIP. For Hawk is the implementation of the DvW LIP-based signatures in Module-LIP, it is natural to raise the question whether we could realise our schemes in Module-LIP. The realisation of Hawk employs the fact that the rank-2 module lattice R^2 for the cyclotomic ring $R = \mathbb{Z}[X]/(X^n+1)$ is isomorphic to the integral lattice $\mathbb{Z}^{2n}$ which has an efficient Gaussian sampler. However, it is unknown whether there are any remarkably decodable lattices which are also structured lattice. Without those, we cannot instantiate our public-key encryption and ZKPoK using Module-LIP.

Efficient sampling algorithm for $\mathcal{D}_{s,\mu}([Q])$ and the cryptanalysis of our conjectured average-case LIP assumptions. In Section 2.3, we introduce a new parameter μ to the average-case distribution $\mathcal{D}_s([\mathbf{Q}])$ introduced by Ducas and van Woerden [DvW22] on an equivalence class. An equivalent form $\mathbf{Q}'$ sampled $\mathcal{D}_{s,\mu}([\mathbf{Q}])$ has its minimum eigenvalue $\nu_{\min}(\mathbf{Q}') \geq \mu$. The benefit of this lower bound is that we can upper bound the Euclidean norm of the coefficient vector $\mathbf{x}$ by its quadratic-form-induced norm $\|\mathbf{x}\|_{\mathbf{Q}'}$ and μ via Lemma 2.4, which makes it easier to prove the knowledge of such $\mathbf{x}$ in the commit-and-prove protocol described in Section 5.2. A trivial approach to sample from $\mathcal{D}_{s,\mu}([\mathbf{Q}])$ is to sample from $\mathcal{D}_s([\mathbf{Q}])$ first and reject until there is an equivalent form whose minimum eigenvalue $\nu_{\min}(\mathbf{Q}') \geq \mu$. Unfortunately, we did not succeed to give a proof on the expected running-time of this sampling approach. Furthermore, to use equivalent forms sampled from $\mathcal{D}_{s,\mu}([\mathbf{Q}])$ in our blind signature scheme, we conjecture that the LIP problems instantiated with the new average-case distribution, $\mathsf{ac\text{-}sLIP}^{\mathbf{Q}}_{s,\mu}$ and $\mathsf{ac\text{-}\Delta LIP}^{\mathbf{Q}_0,\mathbf{Q}_1}_{s,\mu}$, are at least as hard as $\mathsf{ac\text{-}sLIP}^{\mathbf{Q}}_{s}$ and $\mathsf{ac\text{-}\Delta LIP}^{\mathbf{Q}_0,\mathbf{Q}_1}_{s}$ introduced in [DvW22] since none of existing attacks against LIP exploit the parameter μ. Therefore, it is crucial for the concrete instantiation of our blind signature scheme in the future to find an efficient sampler for $\mathcal{D}_{s,\mu}([\mathbf{Q}])$ and study the hardness of the above conjectured assumptions.

Cryptanalysis of omCVP. Same as other "one-more" type assumptions, we are unable to reduce omCVP to standard assumptions. Meanwhile, we provide two strategies of attacks from which we determine the insecure parameter range allowing to solve omCVP in polynomial time. Our cryptanalysis of omCVP assumption is inspired from the cryptanalysis of the related omSIS assumption by Agrawal et al. [AKSY22]. One of the attack strategies is to find a short basis of the given lattice and use it to sample close vectors to any targets. The adversary can achieve the shortest basis at the cost of calling the shortest vector problem solvers which run in exponential time. Thus, improving the algorithm for the shortest vector problem will improve the cryptanalysis of omCVP.

2 Preliminaries

Let $\lambda \in \mathbb{N}$ be the security parameter. Vectors are denoted by bold lowercase letters $\mathbf{v}$ and are intepreted as column vectors. Matrices are denoted by bold uppercase letters $\mathbf{B}$ and are intepreted as a set of column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The general linear group $\mathsf{GL}_n(\mathbb{Z})$ is the set of $n \times n$ invertible integer matrices. For a matrix $\mathbf{B}$, $\mathbf{B}^\mathsf{T}$ is its transpose, and $\mathbf{B}^{\mathsf{GS}}$ is its Gram-Schmidt orthogonalisation. The Euclidean norm of a vector $\mathbf{v}$ is denoted by $\|\mathbf{v}\|$. The norm of a matrix $\mathbf{B}$ is defined by $\|\mathbf{B}\| := \max_i \|\mathbf{b}_i\|$, i.e., the length of its longest column vector. The discretised torus $\mathbb{T}_q := \frac{1}{q}\mathbb{Z}/\mathbb{Z}$ is identified as $(-1/2, 1/2] \cap \frac{1}{q} \cdot \mathbb{Z}$ where q is odd. Let $[n] = \{1, \ldots, n\}$ for a positive integer n.

2.1 Lattices and Lattice Isomorphism Problem

A full-rank n-dimensional lattice Λ is a discrete subgroup of $\mathbb{R}^n$ given by a basis $\mathbf{B} \in \mathbb{R}^{n\times n}$ such that $\Lambda(\mathbf{B}) := \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}$. Two bases $\mathbf{B}$ and $\mathbf{B}'$ generate the same lattice if there exists a unimodular matrix $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ such that $\mathbf{B}' = \mathbf{BU}$. Two lattices Λ and Λ' are isomorphic if there exists an orthogonal transformation $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\Lambda' = \mathbf{O} \cdot \Lambda$.

Definition 2.1 (LIP). *Given two isomorphic lattices Λ and Λ', find an orthogonal transformation $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathbf{O} \cdot \Lambda = \{\mathbf{Ov} : \mathbf{v} \in \Lambda\} = \Lambda'$.*

Given that two lattices Λ and Λ' are generated by bases $\mathbf{B}$ and $\mathbf{B}'$ respectively, they are isomorphic if there exists an orthogonal transformation $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ and a unimodular matrix $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ such that $\mathbf{B}' = \mathbf{OBU}$. To avoid the real-valued orthogonal transformation, we denote lattices by quadratic forms. A quadratic form is a positive definite real symmetric matrix $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, and for a lattice basis $\mathbf{B}$, the Gram matrix $\mathbf{Q} = \mathbf{B}^\mathsf{T}\mathbf{B}$ is a quadratic form. On the other hand, given any quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, Cholesky decomposition finds a unique upper triangular lattice basis $\mathbf{B_Q}$ such that $\mathbf{B_Q}^\mathsf{T}\mathbf{B_Q} = \mathbf{Q}$. Now, for two isomorphic lattice bases $\mathbf{B}$ and $\mathbf{B}' = \mathbf{OBU}$ we have:

$$\mathbf{Q}' = (\mathbf{B}')^\mathsf{T}(\mathbf{B}') = \mathbf{U}^\mathsf{T}\mathbf{B}^\mathsf{T}\mathbf{O}^\mathsf{T}\mathbf{OBU} = \mathbf{U}^\mathsf{T}\mathbf{B}^\mathsf{T}\mathbf{BU} = \mathbf{U}^\mathsf{T}\mathbf{QU}$$

Then, we call $\mathbf{Q}$ and $\mathbf{Q}'$ are equivalent if such a unimodular matrix $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ exists. The equivalence class is denoted by:

$$[\mathbf{Q}] := \left\{\mathbf{U}^\mathsf{T}\mathbf{QU} : \mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})\right\}$$

The search variant of LIP in Definition 2.1 can now be restated.

Definition 2.2 ($\mathsf{sLIP}^{\mathbf{Q}}$). *For a quadratic form $\mathbf{Q}$, given any equivalent quadratic form $\mathbf{Q}' \in [\mathbf{Q}]$, find a unimodular matrix $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ such that $\mathbf{Q}' = \mathbf{U}^\mathsf{T}\mathbf{QU}$.*

Apart from the search variant, we also consider the distinguish variant $\Delta\mathsf{LIP}$.

Definition 2.3 ($\Delta\mathsf{LIP}^{\mathbf{Q}_0,\mathbf{Q}_1}$)**.** *For two quadratic forms $\mathbf{Q}_0, \mathbf{Q}_1$, given an equivalent form $\mathbf{Q}' \in [\mathbf{Q}_b]$ where $b \in \{0, 1\}$, find b.*

In the quadratic form setting, lattice points $\mathbf{Bx} \in \mathbb{R}^n$ are denoted by their integral coefficients $\mathbf{x} \in \mathbb{Z}^n$. The inner product of two vectors $\mathbf{x}$ and $\mathbf{y}$ with respect to a quadratic form $\mathbf{Q}$ is given by $\langle \mathbf{x}, \mathbf{y} \rangle_{\mathbf{Q}} \coloneqq \mathbf{x}^{\mathsf{T}}\mathbf{Q}\mathbf{y}$, and the norm of a vector $\mathbf{x}$ is given by $\|\mathbf{x}\|_{\mathbf{Q}}^2 \coloneqq \mathbf{x}^{\mathsf{T}}\mathbf{Q}\mathbf{x}$. The first minimum $\lambda_1(\mathbf{Q})$ is defined as:

$$\lambda_1(\mathbf{Q}) \coloneqq \underset{\mathbf{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}}{min} \|\mathbf{x}\|_{\mathbf{Q}}$$

and the i-th minimal distance $\lambda_i(\mathbf{Q})$ is the smallest r such that the ball of radius r, $\left\{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\|_{\mathbf{Q}} \le r\right\}$ spans a space of at least i dimensions. These successive minima are invariant within an equivalence class $[\mathbf{Q}]$, so we also denote $\lambda_i([\mathbf{Q}])$.

For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$ and a coefficient vector $\mathbf{v} \in \mathbb{R}^n$, we abuse the notation to denote the coset $\Lambda\left(\mathbf{B}_{\mathbf{Q}}\right) + \mathbf{B}_{\mathbf{Q}}\mathbf{v}$ as $\mathbf{Q} + \mathbf{v}$. A point in the coset $\mathbf{Q} + \mathbf{v}$ is represented as its coefficients w.r.t. $\mathbf{Q}$.

Since an integral coefficient vector $\mathbf{x}$, representing a point in $\mathbf{Q}$, is of an infinite set $\mathbb{Z}^n$, we use the following lemma to bound its ℓ_2-norm of $\|\mathbf{x}\|$ given its $\mathbf{Q}$-norm $\|\mathbf{x}\|_{\mathbf{Q}}$.

Lemma 2.4 ([Kam23, adapted from Theorem 2])**.** *Let $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$ be a quadratic form representing a full-rank n-dimensional lattice and $\mathbf{x} \in \mathbb{R}^n$. The Euclidean norm of $\mathbf{x}$ can be upper bounded according to its norm with respect to $\mathbf{Q}$ as*

$$\|\mathbf{x}\| \le \frac{\|\mathbf{x}\|_{\mathbf{Q}}}{\sqrt{v_{\min}(\mathbf{Q})}}$$

where $v_{\min}(\mathbf{Q})$ is the minimum eigenvalue of the matrix $\mathbf{Q}$.

Proof. Since $\mathbf{Q}$ is a symmetric positive definite matrix of rank n, $\mathbf{Q}$ has n positive eigenvalues $0 < v_{\min}(\mathbf{Q}) = v_1 \le v_2 \le \ldots \le v_n$. Let $\mathbf{u}_1, \ldots, \mathbf{u}_n$ be the corresponding normalised eigenvectors. $\forall i \in [n]$, $\mathbf{Q}\mathbf{u}_i = v_i \cdot \mathbf{u}_i$ and $\|\mathbf{u}_i\| = 1$. Additionally, these eigenvectors are mutually orthogonal, so any vector $\mathbf{x} \in \mathbb{R}^n$ can be expressed as:

$$\mathbf{x} = \sum_{i\in[n]} \left(\mathbf{u}_i^{\mathsf{T}}\mathbf{x}\right)\mathbf{u}_i, \text{ and } \|\mathbf{x}\|^2 = \sum_{i\in[n]} \left(\mathbf{u}_i^{\mathsf{T}}\mathbf{x}\right)^2$$

Then, we have:

$$\mathbf{Q}\mathbf{x} = \sum_{i\in[n]} v_i \cdot \left(\mathbf{u}_i^{\mathsf{T}}\mathbf{x}\right)\mathbf{u}_i$$

Next,

$$\|\mathbf{x}\|_{\mathbf{Q}}^2 = \mathbf{x}^{\mathsf{T}}\mathbf{Q}\mathbf{x} = \sum_{i\in[n]} v_i \cdot \left(\mathbf{u}_i^{\mathsf{T}}\mathbf{x}\right)^2$$

Because $v_{\min}(\mathbf{Q})$ is the minumum eigenvalue of $\mathbf{Q}$, we have:

$$\|\mathbf{x}\|_{\mathbf{Q}}^2 \geq v_{\min}(\mathbf{Q}) \sum_{i \in [n]} \left(\mathbf{u}_i^\mathsf{T} \mathbf{x}\right)^2 = v_{\min}(\mathbf{Q}) \|\mathbf{x}\|^2, \text{ or}$$

$$\|\mathbf{x}\| \leq \frac{\|\mathbf{x}\|_{\mathbf{Q}}}{\sqrt{v_{\min}(\mathbf{Q})}}$$

□

2.2 Discrete Gaussian Distribution

Discrete Gaussian sampling has been foundational to the development of lattice-based cryptography. It is the key for worst-case to average-case reductions of lattice problems [MR07]. Sampling from a discrete Gaussian distribution enables us to obtain short or nearby lattice vectors without leaking information about the secret key [GPV08]. The seminal work of Ducas and van Woerden [DvW22] rephrases the relevant definitions and lemmas in the quadratic form setting, and we recall them here.

Definition 2.5 (Continuous Gaussian Distribution [DvW22])**.** *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, the continuous Gaussian distribution over $\mathbb{R}^n$ with a parameter $s > 0$ and a centre $\mathbf{c} \in \mathbb{R}^n$ is defined as:*

$$\forall \mathbf{x} \in \mathbb{R}^n : \rho_{\mathbf{Q},s,\mathbf{c}}(\mathbf{x}) := \exp\left(-\pi \|\mathbf{x} - \mathbf{c}\|_{\mathbf{Q}}^2 / s^2\right)$$

We have the discrete Gaussian distribution by restricting the continuous Gaussian distribution to a discrete lattice. In the quadratic form setting, that lattice is always the integral lattice $\mathbb{Z}^n$, while the quadratic form induces the geometry.

Definition 2.6 (Discrete Gaussian Distribution [DvW22])**.** *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, the discrete Gaussian distribution $\mathcal{D}_{\mathbf{Q},s,\mathbf{c}}$ with a parameter $s > 0$ and a centre $\mathbf{c} \in \mathbb{R}^n$ is defined as:*

$$\Pr_{X \sim \mathcal{D}_{\mathbf{Q},s,\mathbf{c}}}[X = \mathbf{x}] := \frac{\rho_{\mathbf{Q},s,\mathbf{c}}(\mathbf{x})}{\rho_{\mathbf{Q},s,\mathbf{c}}(\mathbb{Z}^n)} \textit{ if } \mathbf{x} \in \mathbb{Z}^n, \textit{ and } 0 \textit{ otherwise,}$$

where $\rho_{\mathbf{Q},s,\mathbf{c}}(\mathbb{Z}^n) = \sum_{\mathbf{x} \in \mathbb{Z}^n} \rho_{\mathbf{Q},s,\mathbf{c}}(\mathbf{x})$. The centre $\mathbf{c}$ is omitted if $\mathbf{c} = \mathbf{0}$.

Micciancio and Regev [MR07] define an important *smoothing parameter* of a lattice. The smoothing parameter shows how large the standard deviation parameter s should be so that the discrete $\mathcal{D}_{\mathbf{Q},s,\mathbf{c}}$ behaves like continuous one.

Definition 2.7 (Smoothing Parameter [DvW22, Definition 2.4])**.** *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$ and $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\mathbf{Q})$ is the minimal $s > 0$ such that $\rho_{\mathbf{Q}^{-1},1/s}(\mathbb{Z}^n) \leq \epsilon$.*

The smoothing parameter $\eta_\epsilon(\mathbf{Q})$ is an invariant property of an equivalence class $[\mathbf{Q}]$, so we also denote $\eta_\epsilon([\mathbf{Q}])$ for an equivalence class.

We recall some facts regarding the discrete Gaussian distribution that apply when the parameter s is at least as large as the smoothing parameter of the lattice.

Lemma 2.8 ([GPV08, adapted from Lemma 2.4])**.** *For a quadratic form* $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$*,* $\epsilon \in (0,1)$*, a parameter* $s \geq \eta_\epsilon(\mathbf{Q})$*, and a centre* $c \in \mathbb{R}^n$*, we have:*

$$\rho_{\mathbf{Q},s,\mathbf{c}}(\mathbb{Z}^n) \in \left[\frac{1-\epsilon}{1+\epsilon}, 1\right] \rho_{\mathbf{Q},s}(\mathbb{Z}^n)$$

Lemma 2.9 ([GPV07, Corollary 2.8])**.** *Let* Λ *and* Λ' *be n-dimensional lattices such that* $\Lambda' \subseteq \Lambda$*. For all* $\epsilon \in \left(0, \frac{1}{2}\right)$*,* $s \geq \eta_\epsilon(\Lambda')$*, and* $\mathbf{c} \in \mathbb{R}^n$*, the statistical distance between the distribution of* $\left(\mathcal{D}_{\Lambda,s,\mathbf{c}} \bmod \Lambda'\right)$ *and the uniform distribution over* $(\Lambda \bmod \Lambda')$ *is at most* 2ϵ*.*

Corollary 2.9.1. *For a quadratic form* $\mathbf{Q} = \mathbf{B}_\mathbf{Q}^\mathsf{T}\mathbf{B}_\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{Z})$*, any integer* $q > 2$*, any* $\epsilon \in \left(0, \frac{1}{2}\right)$*,* $s \geq \eta_\epsilon(\mathbf{Q})$*, and* $\mathbf{c} \in \mathbb{R}^n$*, the statistical distance between the distribution* $\left(\frac{1}{q}\mathcal{D}_{\mathbf{Q},qs,\mathbf{c}q} \bmod \mathbb{Z}^n\right)$ *and the uniform distribution over* $\mathbb{T}_q^n$ *is at most* 2ϵ*.*

Proof. Let $\Lambda(\mathbf{B}_\mathbf{Q})$ be the lattice generated by the basis $\mathbf{B}_\mathbf{Q}$. A vector $\mathbf{x}$ distributed as $\frac{1}{q}\mathcal{D}_{\mathbf{Q},qs,\mathbf{c}q}$ in the quadratic form setting is equivalent to the vector $\mathbf{B}_\mathbf{Q}\mathbf{x}$ distributed as $\mathcal{D}_{\frac{1}{q}\Lambda(\mathbf{B}_\mathbf{Q}),s,\mathbf{B}_\mathbf{Q}\mathbf{c}}$. Hence, the vector $\mathbf{a} := \mathbf{x} \bmod \mathbb{Z}^n$ distributed as $\left(\frac{1}{q}\mathcal{D}_{\mathbf{Q},qs,\mathbf{c}q} \bmod \mathbb{Z}^n\right)$ in the quadratic form setting is equivalent to the vector $\mathbf{B}_\mathbf{Q}\mathbf{a} := \mathbf{B}_\mathbf{Q}\mathbf{x} \bmod \Lambda(\mathbf{B}_\mathbf{Q})$ distributed as $\left(\mathcal{D}_{\frac{1}{q}\Lambda(\mathbf{B}_\mathbf{Q}),s,\mathbf{B}_\mathbf{Q}\mathbf{c}} \bmod \Lambda(\mathbf{B}_\mathbf{Q})\right)$. Additionally, the set $\frac{1}{q}\Lambda(\mathbf{B}_\mathbf{Q})/\Lambda(\mathbf{B}_\mathbf{Q})$ is equivalent to the set $\mathbb{T}_q^n$ in the quadratic form setting, and $\Lambda(\mathbf{B}_\mathbf{Q}) \subseteq \frac{1}{q}\Lambda(\mathbf{B}_\mathbf{Q})$. Therefore, for $s \geq \eta_\epsilon(\mathbf{Q})$, we have the statistical distance between the distribution $\left(\frac{1}{q}\mathcal{D}_{\mathbf{Q},qs,\mathbf{c}q} \bmod \mathbb{Z}^n\right)$ and the uniform distribution over $\mathbb{T}_q^n$ is at most 2ϵ by Lemma 2.9. □

Corollary 2.9.2. *For a quadratic form* $\mathbf{Q} = \mathbf{B}_\mathbf{Q}^\mathsf{T}\mathbf{B}_\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{Z})$*, some integer* $q > 2$*, a prime* p*, any* $\epsilon \in \left(0, \frac{1}{2}\right)$*,* $s \geq \eta_\epsilon(p^2\mathbf{Q}) = p \cdot \eta_\epsilon(\mathbf{Q})$*, and* $\mathbf{c} \in \mathbb{R}^n$*, the statistical distance between the distribution* $\left(\mathcal{D}_{\mathbf{Q},s,c} \bmod p\right)$ *and the uniform distribution over* $\mathbb{Z}_p^n$ *is at most* 2ϵ*.*

For practical purposes, we need to sample the discrete Gaussian distribution efficiently. Given a lattice basis, one can sample exactly from the discrete Gaussian distribution with an adequately large parameter s using the sampling algorithm by Brakerski et al. [BLP+13b, Section 5].

Lemma 2.10 ([DvW22, Lemma 2.9] rephrased from [BLP+13a, Lemma 2.3])**.** *For a quadratic form* $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$*, a parameter* $s \geq \left\|\mathbf{B}_\mathbf{Q}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$*, and a centre* $\mathbf{c} \in \mathbb{R}^n$*, there exists a polynomial-time algorithm* $\mathsf{DiscreteSample}(\mathbf{Q}, s, \mathbf{c})$ *returns a sample* $\mathbf{x} \in \mathbb{Z}^n$ *distributed as* $\mathcal{D}_{\mathbf{Q},s,\mathbf{c}}$*.*

The following lemma enables us to expect that a lattice vector sampled from a discrete Gaussian distribution is either short or close to a specified target.

Lemma 2.11 ([DvW22, Lemma 2.7]). *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, $\epsilon \in (0,1)$, a parameter $s \geq \eta_\epsilon(\mathbf{Q})$, and a centre $c \in \mathbb{R}^n$, we have:*

$$\Pr_{\mathbf{x} \sim \mathcal{D}_{\mathbf{Q},s,\mathbf{c}}}\left[\|\mathbf{x}-\mathbf{c}\|_{\mathbf{Q}} > s\sqrt{n}\right] \leq \frac{1-\epsilon}{1+\epsilon} \cdot 2^{-n}$$

Using the discrete Gaussian distribution, Ducas and van Woerden define an average-case distribution on an equivalence class $[\mathbf{Q}]$. This average-case distribution is fundamental to their reduction from worst-case to average-case LIP. Firstly, we recall the linear algebra step that, given a quadratic form and a set of short and linearly-independent vectors, returns a well-reduced equivalent form.

Lemma 2.12 ([DvW22, Lemma 3.1] adapted from [MG02, Lemma 7.1]). *Given a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$ and a matrix $\mathbf{Y} = (\mathbf{y}_1, \ldots, \mathbf{y}_m) \in \mathbb{Z}^{n \times m}$ such that $\mathbf{Y}$ is of rank n, there exists a polynomial-time algorithm $\mathsf{Extract}(\mathbf{Q}, \mathbf{Y})$ outputs a unimodular transformation $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ and a quadratic form $\mathbf{R} = \mathbf{U}^\mathsf{T}\mathbf{Q}\mathbf{U} \in [\mathbf{Q}]$ such that $\left\|\mathbf{B}_\mathbf{R}^{\mathsf{GS}}\right\| = \max_i \|\mathbf{y}_i\|_\mathbf{Q}$ and $\|\mathbf{B}_\mathbf{R}\| \leq \max_i \|\mathbf{y}_i\|_\mathbf{Q} \sqrt{n}/2$.*

Then, for $s > 0$, we have the following definition of the average-case distribution over the equivalence form $\mathbf{Q}$.

Definition 2.13 ([DvW21, Definition 3.3]). *Given a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, the Gaussian distribution $\mathcal{D}_s([\mathbf{Q}])$ over $[\mathbf{Q}]$ with a parameter $s > 0$ is algorithmically defined in Fig. 1.*

$\mathcal{D}_s([\mathbf{Q}])$
$C := 1 - (1 + e^{-\pi})^{-1}$
$m := \left\lceil \frac{2n}{C} \right\rceil$
do
for $i = 1, \ldots, m$ **do**
$\mathbf{y}_i \leftarrow\$ \mathcal{D}_{\mathbf{Q},s}$
$\mathbf{Y} := (\mathbf{y}_i, \ldots, \mathbf{y}_m)$
while $\mathsf{rank}(\mathbf{Y}) < n$
$(\mathbf{R}, \mathbf{U}) \leftarrow \mathsf{Extract}(\mathbf{Q}, \mathbf{Y})$
return R

Figure 1: The Gaussian distribution over $[\mathbf{Q}]$.

Finally, using the efficient sampling algorithm for discrete Gaussian distribution and the above algorithmic distribution $\mathcal{D}_s([\mathbf{Q}])$, Ducas and van Woerden describe an efficient sampler for $\mathcal{D}_s([\mathbf{Q}])$.

Lemma 2.14 ([DvW21, Algorithm 1 and Lemma 3.4]). *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{Z})$ and $s \geq \max\left\{\lambda_n(\mathbf{Q}), \left\|\mathbf{B}_{\mathbf{Q}}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$, there exists an expected polynomial-time (EPT) algorithm* $\mathsf{QFS}(\mathbf{Q}, s)$ *returns a quadratic form $\mathbf{Q}'$ distributed as $\mathcal{D}_s([\mathbf{Q}])$ with a unimodular transformation $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ such that $\mathbf{Q}' = \mathbf{U}^{\mathsf{T}}\mathbf{Q}\mathbf{U}$.*

For an equivalent form sampled from the above algorithm, we have this lemma about the shortness of the Gram-Schmidt orthogonalisation of its basis.

Lemma 2.15 ([DvW21, Lemma 3.6]). *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, a parameter $\epsilon \in (0,1)$, and $s \geq \max\{\lambda_n(\mathbf{Q}), \eta_\epsilon(\mathbf{Q})\}$, we have:*

$$\Pr_{\mathbf{Q}' \sim \mathcal{D}_s([\mathbf{Q}])}\left[\left\|\mathbf{B}_{\mathbf{Q}'}^{\mathsf{GS}}\right\| > s\sqrt{n}\right] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 100n \cdot 2^{-n}$$

2.3 Average-case LIP Variants

Using the Gaussian distribution $\mathcal{D}_s([\mathbf{Q}])$ parametrised by a width parameter s over an equivalence class $[\mathbf{Q}]$, Ducas and van Woerden [DvW21] lay the foundation for LIP-based cryptography by reducing the worst-case LIP to the following average-case problems.

Definition 2.16 (ac-sLIP$_s^{\mathbf{Q}}$ [DvW22, Definition 3.7]). *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$ and $s > 0$, given a quadratic form $\mathbf{Q}' \leftarrow\!\!\$\ \mathcal{D}_s([\mathbf{Q}])$, find a unimodular transformation $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ such that $\mathbf{Q}' = \mathbf{U}^{\mathsf{T}}\mathbf{Q}\mathbf{U}$.*

Definition 2.17 (ac-ΔLIP$_s^{\mathbf{Q}_0,\mathbf{Q}_1}$ [DvW22, Definition 3.8]). *For two quadratic forms $\mathbf{Q}_0, \mathbf{Q}_1 \in \mathcal{S}_n^{>0}(\mathbb{R})$ and $s > 0$, given a quadratic form $\mathbf{Q}' \leftarrow\!\!\$\ \mathcal{D}_s([\mathbf{Q}_b])$ where $b \in \{0,1\}$, find b.*

In order to make use of Lemma 2.4, we further make stronger assumptions such that the form $\mathbf{Q}'$ sampled from the Gaussian distribution over a class in the above two definitions has its smallest eigenvalue $\nu_{\min}(\mathbf{Q}')$ be at least μ where μ is a small real number. To sample such quadratic form from $\mathcal{D}_s([\mathbf{Q}])$, we define an algorithmic distribution $\mathcal{D}_{s,\mu}([\mathbf{Q}])$ such that it uses rejection sampling on $\mathcal{D}_s([\mathbf{Q}])$ until there is a quadratic form $\mathbf{Q}'$ such that $\nu_{\min}(\mathbf{Q}) \geq \mu$. We redefine the average-case LIP variants in Definition 2.16 and Definition 2.17 as ac-sLIP$_{s,\mu}^{\mathbf{Q}}$ and ac-ΔLIP$_{s,\mu}^{\mathbf{Q}_0,\mathbf{Q}_1}$ respectively by adding the lower bound μ on the minimum eigenvalue of the sampled quadratic form to the Gaussian distribution over an equivalence class $\mathcal{D}_{s,\mu}([\mathbf{Q}])$. We conjecture that there exists an EPT algorithm to sample from $\mathcal{D}_{s,\mu}([\mathbf{Q}])$.

Conjecture 2.18 (EPT algorithm for $\mathcal{D}_{s,\mu}([\mathbf{Q}])$). *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{Z})$, $s \geq \max\left\{\lambda_n(\mathbf{Q}), \left\|\mathbf{B}_{\mathbf{Q}}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$ and some small real $\mu > 0$, there exists an EPT algorithm* $\mathsf{QFS}(\mathbf{Q}, s, \mu)$ *returns a quadratic form $\mathbf{Q}'$ distributed as $\mathcal{D}_{s,\mu}([\mathbf{Q}])$ with a unimodular transformation $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ such that $\mathbf{Q}' = \mathbf{U}^{\mathsf{T}}\mathbf{Q}\mathbf{U}$ and $\nu_{\min}(\mathbf{Q}') \geq \mu$.*

Definition 2.19 (ac-sLIP$^{\mathbf{Q}}_{s,\mu}$)**.** *For a quadratic form* $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$*,* $s > 0$*, and* $\mu > 0$*, given a quadratic form* $\mathbf{Q}' \leftarrow\$ \mathcal{D}_{s,\mu}([\mathbf{Q}])$*, find a unimodular transformation* $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ *such that* $\mathbf{Q}' = \mathbf{U}^\mathsf{T}\mathbf{Q}\mathbf{U}$.

Definition 2.20 (ac-ΔLIP$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s,\mu}$)**.** *For two quadratic forms* $\mathbf{Q}_0, \mathbf{Q}_1 \in \mathcal{S}_n^{>0}(\mathbb{R})$*,* $s > 0$*, and* $\mu > 0$*, given a quadratic form* $\mathbf{Q}' \leftarrow\$ \mathcal{D}_{s,\mu}([\mathbf{Q}_b])$ *where* $b \in \{0,1\}$*, find* b.

Since all quadratic forms are symmetric positive-definite matrices, their eigenvalues are real and positive, so for any sampled form $\mathbf{Q}' \leftarrow\$ \mathcal{D}_s([\mathbf{Q}])$, $\nu_{\min}(\mathbf{Q}') > 0$. Thus, for $\mu = 0$, ac-sLIP$^{\mathbf{Q}}_{s,\mu}$ and ac-ΔLIP$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s,\mu}$ are at least as hard as ac-sLIP$^{\mathbf{Q}}_{s}$ and ac-ΔLIP$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s}$, respectively. In the cryptographic applications of LIP, we start with a quadratic form $\mathbf{Q}$ whose basis $\mathbf{B}_\mathbf{Q}$ is short and as orthogonal as possible and use an equivalent form $\mathbf{Q}' \in [\mathbf{Q}]$ as the public key and the corresponding unimodular transformation $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ as the trapdoor to exploit some remarkable geometric feature of $\mathbf{Q}$. For $\mathbf{Q}'$ is random, its basis $\mathbf{B}'_\mathbf{Q}$ is arbitrarily long and non-orthogonal. In the average case LIP problems, the Gaussian parameter s can be seen as the "lower-bound" of the non-orthogonality of $\mathbf{Q}'$ while it allows one to sample $\mathbf{Q}'$ efficiently. The introduction of the parameter μ which is lower bound of the minimum eigenvalue of $\mathbf{Q}'$ sets the "upper-bound" of the non-orthogonality of $\mathbf{Q}'$. For the best algorithm to solve LIP at the moment [HR14, DvW22] does not exploit the non-orthogonality $\mathbf{Q}'$ to find its isometry with $\mathbf{Q}$, so we conjecture that ac-sLIP$^{\mathbf{Q}}_{s,\mu}$ and ac-ΔLIP$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s,\mu}$ for $\mu > 0$ are at least as hard as ac-sLIP$^{\mathbf{Q}}_{s}$ and ac-ΔLIP$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s}$, respectively.

Conjecture 2.21 (Hardness of ac-sLIP$^{\mathbf{Q}}_{s,\mu}$)**.** *For any quadratic form* $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$*,* $s > 0$ *and* $\mu > 0$*, ac-sLIP*$^{\mathbf{Q}}_{s,\mu}$ *is* $2^{\Theta(n)}$*-hard.*

Conjecture 2.22 (Hardness of ac-ΔLIP$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s,\mu}$)**.** *For any two quadratic forms* $\mathbf{Q}_0, \mathbf{Q}_1 \in \mathcal{S}_n^{>0}(\mathbb{R})$*,* $s > 0$ *and* $\mu > 0$*, ac-ΔLIP*$^{\mathbf{Q}_0,\mathbf{Q}_1}_{s,\mu}$ *is* $2^{\Theta(n)}$*-hard.*

2.4 Rejection Sampling

We uses rejection sampling technique [Lyu12] in our zero-knowledge proof protocol to hide the secrets. Otherwise, an adversary can learn a secret if it sees sufficiently many proofs for that secret. Theorem 2.26 is the main rejection sampling theorem which is adapted to the quadratic form setting from Theorem 4.6 in [Lyu11]. To prove Theorem 2.26, we recall the general rejection sampling lemma (Lemma 2.25), and extend Lemmas 4.3 and 4.5 in [Lyu11] to Lemma 2.23 and Lemma 2.24, respectively, to include non-zero centres in the discrete Gaussian distribution and allow the rejection sampling parameter M to be either constant or polynomial. In the latter case, we can choose to sacrifice the runtime of the proof protocol for shorter Gaussian parameter.

Lemma 2.23 ([Lyu11, extended from Lemma 4.3])**.** *For a quadratic form* $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$*, any vector* $\mathbf{v}, \mathbf{u} \in \mathbb{R}^n$*, and any* $s, r > 0$*,*

$$\Pr\left[\mathbf{z} \leftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}} : \left|\langle \mathbf{z} - \mathbf{u}, \mathbf{v}\rangle_\mathbf{Q}\right| > r\right] \leq 2\exp\left(-\frac{\pi r^2}{s^2\|\mathbf{v}\|_\mathbf{Q}^2}\right)$$

Proof. For any $\alpha > 0$, we have:

$$\begin{aligned}
&E\left[\exp\left(\frac{2\pi t}{s^2}\langle \mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}}\right)\right] \\
&= \sum_{\mathbf{z}\in\mathbb{Z}^n} \Pr[\mathbf{z}] \exp\left(\frac{2\pi}{s^2}\langle \mathbf{z}-\mathbf{u}, t\mathbf{v}\rangle_{\mathbf{Q}}\right) \\
&= \frac{1}{\rho_{\mathbf{Q},s,\mathbf{u}}(\mathbb{Z}^n)} \sum_{\mathbf{z}\in\mathbb{Z}^n} \exp\left(-\frac{\pi\|\mathbf{z}-\mathbf{u}\|_{\mathbf{Q}}^2}{s^2}\right)\exp\left(\frac{2\pi\langle \mathbf{z}-\mathbf{u}, t\mathbf{v}\rangle_{\mathbf{Q}}}{s^2}\right) \\
&= \frac{1}{\rho_{\mathbf{Q},s,\mathbf{u}}(\mathbb{Z}^n)} \sum_{\mathbf{z}\in\mathbb{Z}^n} \exp\left(-\frac{\pi\|\mathbf{z}-\mathbf{u}-t\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right)\exp\left(\frac{\pi t^2\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right) \\
&= \frac{\rho_{\mathbf{Q},s,\mathbf{u}+t\mathbf{v}}(\mathbb{Z}^n)}{\rho_{\mathbf{Q},s,\mathbf{u}}(\mathbb{Z}^n)} \exp\left(\frac{\pi t^2\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right) \le \exp\left(\frac{\pi t^2\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right)
\end{aligned}$$

Applying Markov's chain inequality, we have for any $t > 0$:

$$\begin{aligned}
\Pr\left[\langle \mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}} > r\right] &= \Pr\left[\exp\left(\frac{2\pi t}{s^2}\langle \mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}}\right) > \exp\left(\frac{2\pi t r}{s^2}\right)\right] \\
&\le \frac{E\left[\exp\left(\frac{2\pi t}{s^2}\langle \mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}}\right)\right]}{\exp\left(\frac{2\pi t r}{s^2}\right)} \\
&\le \exp\left(\frac{\pi t^2\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2} - \frac{2\pi t r}{s^2}\right) \\
&\le \exp\left(-\frac{\pi r^2}{s^2\|\mathbf{v}\|_{\mathbf{Q}}^2}\right)
\end{aligned}$$

where the last inequality is due to setting optimally $t = \frac{r}{\|\mathbf{v}\|_{\mathbf{Q}}^2}$. Because the distribution of $\mathbf{z}$ is symmetric around $\mathbf{u}$, we also have $\Pr\left[\langle \mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}} < -r\right] \le \exp\left(-\frac{\pi r^2}{s^2\|\mathbf{v}\|_{\mathbf{Q}}^2}\right)$, so applying both inequality, we have the claim made in the lemma. □

Lemma 2.24 ([Lyu11, extended from Lemma 4.5])**.** *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$, any vector $\mathbf{v} \in \mathbb{R}^n$, and any centre $\mathbf{u} \in \mathbb{R}^n$, if:*

- $s = \Theta(\|\mathbf{v}\|_{\mathbf{Q}}/\sqrt{\ln n})$*, then:*

$$\Pr\left[\mathbf{z} \leftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}} : \frac{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}}(\mathbf{z})}{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}(\mathbf{z})} = \mathsf{poly}(n)\right] = 1 - 2^{-\Theta(\ln n)}$$

- $s = \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}\sqrt{\ln n}\right)$*, then:*

$$\Pr\left[\mathbf{z} \leftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}} : \frac{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}}(\mathbf{z})}{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}(\mathbf{z})} = O(1)\right] = 1 - 2^{-\Theta(\ln n)}$$

Proof. By Definition 2.6, we have:

$$\frac{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}}(\mathbf{z})}{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}(\mathbf{z})} = \frac{\rho_{\mathbf{Q},s,\mathbf{u}}(\mathbf{z})}{\rho_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}(\mathbf{z})} = \frac{\exp(-\pi\|\mathbf{z}-\mathbf{u}\|_{\mathbf{Q}}^2/s^2)}{\exp(-\pi\|\mathbf{z}-\mathbf{u}-\mathbf{v}\|_{\mathbf{Q}}^2/s^2)}$$
$$= \exp\left(\pi\frac{-2\langle\mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}} + \|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right)$$

By Lemma 2.23, we have $\left|\langle\mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}}\right|$ is smaller than $r = \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}} s\sqrt{\ln n}\right)$ with probability:

$$\Pr\left[\mathbf{z} \hookleftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}} : \left|\langle\mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}}\right| < \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}} s\sqrt{\ln n}\right)\right] > 1 - 2e^{-\pi\Theta(\ln n)}$$
$$= 1 - 2^{-\Theta(\ln n)}$$

Thus, with probability at least $1 - 2^{-\Theta(\ln n)}$, we have:

$$\exp\left(\pi\frac{-2\langle\mathbf{z}-\mathbf{u},\mathbf{v}\rangle_{\mathbf{Q}} + \|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right) < \exp\left(\pi\frac{\Theta(\|\mathbf{v}\|_{\mathbf{Q}} s\sqrt{\ln n}) + \|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right)$$

Then, when $s = \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}/\sqrt{\ln n}\right)$, we have:

$$\exp\left(\pi\frac{\Theta(\|\mathbf{v}\|_{\mathbf{Q}} s\sqrt{\ln n}) + \|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right) = \mathsf{poly}(n),$$

and when $s = \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}\sqrt{\ln n}\right)$, we have:

$$\exp\left(\pi\frac{\Theta(\|\mathbf{v}\|_{\mathbf{Q}} s\sqrt{\ln n}) + \|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right) = O(1)$$

□

Lemma 2.25 (Rejection Sampling [DFPS22, adapted from Lemma 1])**.** *Let $f : \mathbb{Z}^n \to \mathbb{R}$ and $g : \mathbb{Z}^n \to \mathbb{R}$ be probability distribution with the property that:*

$$\exists M \in \mathbb{R}, \epsilon \in \left[0, \frac{1}{2}\right] : \Pr[z \hookleftarrow\$ f : Mg(z) \geq f(z)] \geq 1 - \epsilon$$

then the statistical distance between the outputs of two algorithms $\mathcal{A}$ sampling a value from g and outputting that value with probability $\min\left(1, \frac{f(z)}{Mg(z)}\right)$ and $\mathcal{B}$ sampling a value from z and outputting that value with probability $\frac{1}{M}$ is at most $\frac{\epsilon}{M}$ and the probability that $\mathcal{A}$ outputs something is at least $\frac{1-\epsilon}{M}$.

Theorem 2.26 ([Lyu11, adapted from Theorem 4.6])**.** *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{Z})$, a subset $V \subset \mathbb{Z}^n$ such that $V = \left\{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v}\|_{\mathbf{Q}} < \beta\right\}$, $\mathbf{u} \in \mathbb{R}^n$, and $s \in \mathbb{R}$ if:*

- $s = \Theta(\beta/\sqrt{\ln n})$, *there exists a polynomial* $M = \mathsf{poly}(n)$, *or*

- $s = \Theta(\beta\sqrt{\ln n})$, *there exists a constant* $M = O(1)$,

the statistical distance between distributions of the following algorithms $\mathcal{A}$ *taking a vector* $\mathbf{v} \in V$ *as the input and* $\mathcal{B}$ *is at most* $\frac{2^{-\Theta(\ln n)}}{M}$, *and* $\mathcal{A}$ *outputs something with probability at least* $\frac{1-2^{-\Theta(\ln n)}}{M}$.

$\mathcal{A}(\mathbf{v})$	$\mathcal{B}$
$\mathbf{z} \leftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}$	$\mathbf{z} \leftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}}$
return z *with probability* $\min\left(1, \frac{\mathcal{D}_{\mathbf{Q},s,\mathbf{u}}(\mathbf{z})}{M\mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}(\mathbf{z})}\right)$	**return z** *with probability* $\frac{1}{M}$

Proof. By Lemma 2.24, we have for $M = \mathsf{poly}(n)$ or $M = O(1)$:

$$\forall \mathbf{v} \in V, \Pr\left[\mathbf{z} \leftarrow\$ \mathcal{D}_{\mathbf{Q},s,\mathbf{u}} : M\mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}(\mathbf{z}) \geq \mathcal{D}_{\mathbf{Q},s,\mathbf{u}}(\mathbf{z})\right] \geq 1 - 2^{-\Theta(\ln n)}$$

Applying Lemma 2.25 with f set as $\mathcal{D}_{\mathbf{Q},s,\mathbf{u}}$, and g set as $\mathcal{D}_{\mathbf{Q},s,\mathbf{u}+\mathbf{v}}$, we have the statistical distance between the outputs of $\mathcal{A}$ and $\mathcal{B}$ is at most $\frac{2^{-\Theta(\ln n)}}{M}$, and the probability that $\mathcal{A}$ outputs something is at least $\frac{1-2^{-\Theta(\ln n)}}{M}$. □

2.5 Cryptographic Primitives

In this section, we recall the definitions of cryptographic primitives relevant to this work: public-key encryption, commitments, zero-knowledge proofs, and blind signatures.

2.5.1 Public-Key Encryption

Public-key encryption, also known as asymmetric encryption, uses a pair of public and secret keys to encrypt and decrypt messages. Each user has a key pair which is assumed to be honestly generated by a trusted third party. To send an encrypted message, the *Sender* uses the *Receiver*'s public key to encrypt the message. After receiving the encrypted message, the *Receiver* uses his secret key which is only known to him (apart from the trusted third party) to decrypt for the message. The basic security requirement for a public-key encryption is that its ciphertexts are indistinguishable under chosen-plaintext attack (IND-CPA), i.e., a ciphertext reveals almost no information about the plaintext it encrypts.

Definition 2.27. *A public key encryption scheme for encyrpting any messages* $m \in \mathcal{M}$ *is a tuple of three PPT algorithms* PKE = (Setup, KGen, Enc, Dec) *such that for any security parameter* λ*:*

- pp ← Setup (1^λ)*: chooses the public parameters* pp.

- (pk, sk) ← KGen (pp)*: generates a pair of public key* pk *and secret key* sk.

- $\mathsf{ctxt} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$*: encrypts a message* $m \in \mathcal{M}$ *using the public key* pk.
- $m \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt})$*: decrypts a ciphertext* ctxt *for the plaintext* m *using the secret key* sk.

Definition 2.28 (Correctness)**.** $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is correct if for any messages* $m \in \mathcal{M}$ *and any security parameter* λ*:*

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt}) = m \;\middle|\; \begin{array}{r} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp}) \\ m \leftarrow\$ \mathcal{M} \\ \mathsf{ctxt} \leftarrow \mathsf{Enc}(\mathsf{pk}, m) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda)$$

Definition 2.29 (IND-CPA Security)**.** $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *is indistinguishable under chosen plaintext attack or* IND-CPA*-secure if for any PPT adversary* $\mathcal{A}$*, the advantage that* $\mathcal{A}$ *has in the* IND-CPA *experiment described in Fig. 2 is:*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}}\left(1^{\lambda}\right) &= \left|\Pr\left[\mathsf{IND\text{-}CPA}^{0}_{\mathsf{PKE},\mathcal{A}}\left(1^{\lambda}\right) = 1\right] - \Pr\left[\mathsf{IND\text{-}CPA}^{1}_{\mathsf{PKE},\mathcal{A}}\left(1^{\lambda}\right) = 1\right]\right| \\ &\leq \mathsf{negl}(\lambda)\end{aligned}$$

$$\boxed{\begin{array}{l} \underline{\mathsf{IND\text{-}CPA}^{b}_{\mathsf{PKE},\mathcal{A}}\left(1^{\lambda}\right)} \\ \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp}) \\ (m_0, m_1, \mathsf{st}) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \mathsf{ctxt}_b \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b) \\ b' \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{ctxt}_b, \mathsf{st}) \\ \textbf{return } b = b' \end{array}}$$

Figure 2: IND-CPA experiment

2.5.2 Commitments

A commitment scheme allows one party *Sender* to commit to value while keeping it unknown (Hiding) to the other party *Receiver*. Once sending the commitment, the *Sender* cannot modify the committed value (Binding). At a later stage, the *Sender* can choose to reveal the committed value to the *Receiver*. Commitment schemes have useful applications in advanced cryptographic protocols such as zero-knowledge proof and secure multi-party computation.

Definition 2.30 (Commitment Scheme)**.** *A commitment scheme for a message space* $\mathcal{M}$ *is a tuple of three PPT algorithms* $\mathsf{Com} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Commit}, \mathsf{Open})$ *such that:*

- $\mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right)$*: takes the security parameter* 1^{λ} *and outputs the public parameters* pp.

- $\mathsf{ck} \leftarrow \mathsf{KGen}\left(\mathsf{pp}\right)$*: takes the public parameters* pp *and outputs a commitment key* ck.

- $(\mathsf{com}, r) \leftarrow \mathsf{Commit}\left(\mathsf{ck}, m\right)$*: uses the commitment key* ck *and generates a randomness* r *to make a commitment* com *to a message* $m \in \mathcal{M}$.

- $\{0, 1\} \leftarrow \mathsf{Open}\left(\mathsf{ck}, \mathsf{com}, m, r\right)$*: takes the commitment key* ck*, a message* $m \in \mathcal{M}$*, values* com *and* r *as inputs and outputs a bit* $b \in \{0, 1\}$.

Definition 2.31 (Hiding)**.** $\mathsf{Com} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Commit}, \mathsf{Open})$ *is hiding if for any adversary* $\mathcal{A}$ *which generates two messages* m_0 *and* m_1 *and receives a commitment* $\mathsf{com}_b \leftarrow \mathsf{Commit}(m_b, r)$ *for* $b \in \{0, 1\}$*, the advantage that* $\mathcal{A}$ *has in determining* b *is negligible.*

$$\left| \Pr\left[b = b' \;\middle|\; \begin{array}{r} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ \mathsf{ck} \leftarrow \mathsf{KGen}\left(\mathsf{pp}\right) \\ (m_0, m_1, \mathsf{st}) \leftarrow \mathcal{A}\left(\mathsf{ck}\right) \\ b \leftarrow\!\!\$\; \{0, 1\} \\ (\mathsf{com}_b, r) \leftarrow \mathsf{Commit}\left(\mathsf{ck}, m_b\right) \\ b' \leftarrow \mathcal{A}\left(\mathsf{ck}, \mathsf{com}_b, \mathsf{st}\right) \end{array} \right] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

If the adversaries $\mathcal{A}$ are limited to PPT algorithms, the scheme is *computationally* hiding. Otherwise, it is *statistically* hiding if we allow for arbitrarily-powerful adversaries.

Definition 2.32 (Binding)**.** $\mathsf{Com} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Commit}, \mathsf{Open})$ *is binding if for any adversary* $\mathcal{A}$*, the probability that* $\mathcal{A}$ *can make a commitment that opens to two distinct messages is negligible.*

$$\Pr\left[\begin{array}{l} m_0 \neq m_1 \wedge \\ \mathsf{Open}(\mathsf{ck}, \mathsf{com}, m_0, r_0) = 1 \wedge \\ \mathsf{Open}(\mathsf{ck}, \mathsf{com}, m_1, r_1) = 1 \end{array} \;\middle|\; \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ \mathsf{ck} \leftarrow \mathsf{KGen}\left(\mathsf{pp}\right) \\ (\mathsf{com}, m_0, m_1, r_0, r_1) \leftarrow \mathcal{A}\left(\mathsf{ck}\right) \end{array} \right] \leq \mathsf{negl}(\lambda)$$

Likewise, if we restrict the adversaries $\mathcal{A}$ PPT algorithms, the scheme is *computationally* biding. Otherwise, it is *statistically* biding if there is no restriction on the running-time of $\mathcal{A}$.

2.5.3 Zero-Knowledge Proof of Knowledge

Let $R \subseteq \{0, 1\}^* \times \{0, 1\}^*$ be a relation. R is a collection of tuples $(\mathsf{stmt}, \mathsf{wit})$ where stmt is a statement and wit is a witness for stmt. A statmement admitting a witness is called a true statement, and the set of true statements is denoted as $L_R = \{\mathsf{stmt} : \exists \mathsf{wit}, (\mathsf{stmt}, \mathsf{wit}) \in R\}$. R is said to be an NP relation if it takes time polynomial in the size $|\mathsf{stmt}|$ to verify the validity of a witness wit for stmt. A proof system for the relation R is a protocol where a prover $\mathcal{P}$ convince a verifier $\mathcal{V}$ that $\mathcal{P}$ knows a witness wit for a statement stmt. This protocol is zero-knowledge if the $\mathcal{V}$ learns nothing more than the fact that the statement stmt admits a witness.

Definition 2.33 (Interactive Proof)**.** *An interactive proof* Π *for an NP relation* R *consists of a PPT algorithm* Setup *and a pair of PPT interactive algorithms* $(\mathcal{P}, \mathcal{V})$ *such that:*

- $\mathsf{pp} \leftarrow \mathsf{Setup}\left(1^\lambda\right)$*: generates public parameters of* Π.
- $(\mathsf{tx}, b) \leftarrow \langle \mathcal{P}(\mathsf{pp}, \mathsf{stmt}, \mathsf{wit}), \mathcal{V}(\mathsf{pp}, \mathsf{stmt}) \rangle$*: The prover takes as inputs the public parameters, a statement* stmt*, and a witness* wit*, and the verifier takes as inputs the public parameters, and the same statement* stmt*. Their interaction produces a transcript* tx*, which is the concatenation of all messages between the prover and the verifier, and the verifier finally outputs a bit* $b \in \{0, 1\}$ *indicating whether the transcript* tx *is* accepting *or* rejecting.

An interactive proof Π *is said to be* $(2\mu + 1)$*-move (for some positive integer* $\mu \geq 1$*) if the transcript* tx *contains* $(2\mu + 1)$ *messages.*

Definition 2.34 (Completeness)**.** $\Pi = (\mathsf{Setup}, \mathcal{P}, \mathcal{V})$ *is complete for the relation* R *if for any* $(\mathsf{stmt}, \mathsf{wit}) \in R$*:*

$$\Pr\left[b = 1 \;\middle|\; \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^\lambda\right) \\ (\mathsf{tx}, b) \leftarrow \langle \mathcal{P}(\mathsf{pp}, \mathsf{stmt}, \mathsf{wit}), \mathcal{V}(\mathsf{pp}, \mathsf{stmt}) \rangle \end{array} \right] \geq 1 - \mathsf{negl}(\lambda)$$

An interactive proof Π is said to be knowledge-sound for the relation R if any prover which convinces the verifier of knowing a witness for a statement stmt with sufficiently large probability can efficiently extract a witness wit.

Definition 2.35 ($(k_1, \ldots, k_\mu)$-Special-Soundness)**.** *Let* $\Pi = (\mathsf{Setup}, \mathcal{P}, \mathcal{V})$ *be a* $(2\mu + 1)$*-move proof. A* $\left(k_1, \ldots, k_\mu\right)$*-tree of accepting transcripts of* Π *on* $(\mathsf{pp}, \mathsf{stmt})$ *is a set of* $K = \prod_{i=1}^{\mu} k_i$ *transcripts in a tree format with the following properties:*

- *Each node corresponds to a prover's message.*
- *Each edge corresponds to a verifier's challenge.*
- *For* $i \in [\mu]$*, every node at depth* i *has* k_i *children, and the edges connecting to these children correspond to* k_i *pairwise distinct verifier's challenges.*
- *The path from the root node to a leaf node forms an accepting transcript for* $(\mathsf{pp}, \mathsf{stmt})$.

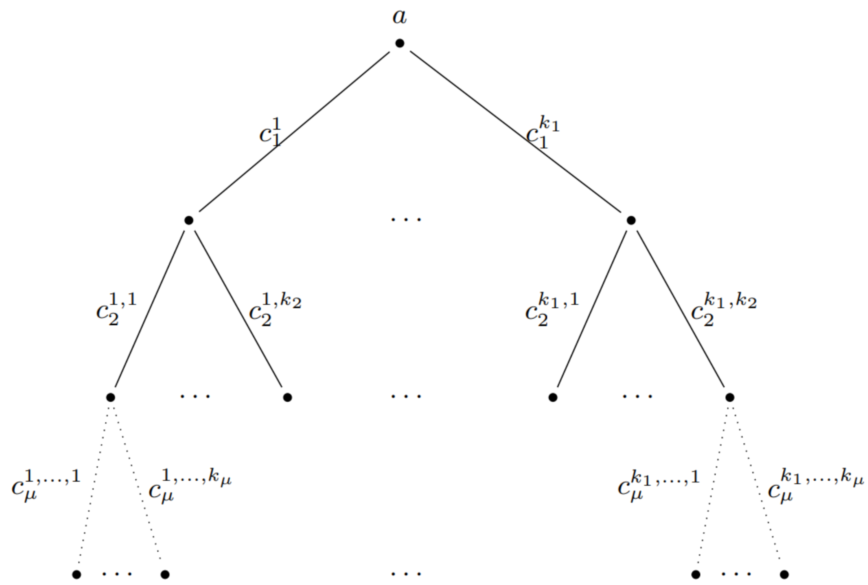

Figure 3: A $(k_1, \dots, k_\mu)$-tree of accepting transcripts of a $(2\mu + 1)$-move interactive proof [ACK21, Figure 1]

Π is said to be $(k_1, \dots, k_\mu)$-special-sound for the relation R if there exists a PPT extractor $\mathcal{E}$ which takes a $(k_1, \dots, k_\mu)$-tree of accepting transcripts of Π on $(\mathsf{pp}, \mathsf{stmt})$ as inputs and outputs a witness wit such that $(\mathsf{stmt}, \mathsf{wit}) \in R$. If Π is 3-move and 2-special-sound, then it is said to be special-sound.

Theorem 2.36 ([ACK21, Theorem 1])**.** *Let $\Pi = (\mathsf{Setup}, \mathcal{P}, \mathcal{V})$ be a $(2\mu + 1)$-move proof where the verifier samples each challenge c_i from a set of cardinality N_i for $i \in [\mu]$. If Π is $(k_1, \dots, k_\mu)$-special-sound, then it is knowledge-sound with knowledge error κ.*

$$\kappa = 1 - \prod_{i=1}^{\mu} \left(1 - \frac{k_i - 1}{N_i}\right)$$

Definition 2.37 (Special Honest-Verifier Zero-Knowledge (SHVZK))**.** *An interactive proof Π is SHVZK for the relation R if there exists a PPT simulator $\mathcal{S}$ upon the statement stmt and a uniformly random challenge value ch outputs an accepting transcript tx which is statistically indistinguishable from the transcripts of honest executions of Π on the same statement.*

An interactive proof Π is said to be public-coin if all of the verifier's challenges are randomly sample from public distributions independent of the prover's messages. Any $(2\mu + 1)$-move proof can be transformed into a non-interactive one (i.e., 1-move proof) in the random oracle model by the Fiat-Shamir transformation [FS87].

Definition 2.38 (Non-Interactive Zero Knowledge Proof of Knowledge (NIZKPoK))**.** *An NIZKPoK system Π for an NP relation R has three probabilistic polynomial-time*

(PPT) algorithms $\left(\mathsf{Setup}, \mathcal{P}^{\mathcal{O}}, \mathcal{V}^{\mathcal{O}}\right)$*, in which* $\mathcal{P}^{\mathcal{O}}$ *and* $\mathcal{V}^{\mathcal{O}}$ *have access to a random oracle* $\mathcal{O}$*, defined as follows:*

- $\mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right)$*: takes the security parameter* λ *and generates public parameters* pp.
- $\pi \leftarrow \mathcal{P}^{\mathcal{O}}\left(\mathsf{stmt}, \mathsf{wit}\right)$*: takes the public parameters* pp*, and a pair of a statement* stmt *and a witness* wit *such that* $(\mathsf{stmt}, \mathsf{wit}) \in R$ *and outputs a proof* π.
- $\{0, 1\} \leftarrow \mathcal{V}^{\mathcal{O}}\left(\mathsf{stmt}, \pi\right)$*: takes the public parameters* pp*, a statement* stmt*, and a proof* π *and outputs a bit indicating whether the proof is valid* (1) *or invalid* (0).

Definition 2.39 (Completeness)**.** $\Pi = \left(\mathsf{Setup}, \mathcal{P}^{\mathcal{O}}, \mathcal{V}^{\mathcal{O}}\right)$ *is complete if there exists a negligible function* negl *such that for any* pp*,* $(\mathsf{stmt}, \mathsf{wit}) \in R$*, and any oracle* $\mathcal{O}$*, we have:*

$$\Pr\left[\mathcal{V}^{\mathcal{O}}\left(\mathsf{stmt}, \pi\right) = 1 \;\middle|\; \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ \pi \leftarrow \mathcal{P}^{\mathcal{O}}\left(\mathsf{stmt}, \mathsf{wit}\right) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda)$$

Definition 2.40 (Straightline Extractability [Fis05, *Online Extractor* in Definition 2])**.** $\Pi = \left(\mathsf{Setup}, \mathcal{P}^{\mathcal{O}}, \mathcal{V}^{\mathcal{O}}\right)$ *is straightline extractable if for any PPT malicious prover* $\mathcal{A}$*, there exists a PPT extractor* $\mathcal{E}$ *such that the following holds. Let* $Q_{\mathcal{O}}(\mathcal{A})$ *be the sequence of* $\mathcal{A}$*'s queries to* $\mathcal{O}$ *and* $\mathcal{O}$*'s answers.*

$$\Pr\left[(\mathsf{stmt}, \mathsf{wit}) \notin R \wedge \mathcal{V}^{\mathcal{O}}\left(\mathsf{stmt}, \pi\right) = 1 \;\middle|\; \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ (\mathsf{stmt}, \pi) \leftarrow \mathcal{A}^{\mathcal{O}}\left(\mathsf{pp}\right) \\ \mathsf{wit} \leftarrow \mathcal{E}\left(\mathsf{stmt}, \pi, Q_{\mathcal{O}}\left(\mathcal{A}\right)\right) \end{array}\right] \leq \mathsf{negl}(\lambda)$$

Definition 2.41 (Zero Knowledge [Fis05, *Zero-Knowledge* in Definition 2])**.** $\Pi = \left(\mathsf{Setup}, \mathcal{P}^{\mathcal{O}}, \mathcal{V}^{\mathcal{O}}\right)$ *is zero-knowledge if there exists a pair of PPT algorithms (simulators)* $\mathcal{S} = (\mathcal{S}_0, \mathcal{S}_1)$*, such that for any pair of PPT algorithms (distinguishers)* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$*, the advantage* $\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A}}(\lambda)$ *is negligible:*

$$\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A}}(\lambda) = \left|\Pr^{\mathsf{ZK}}_{\Pi,\mathcal{A}}(\lambda) - \Pr^{\mathsf{ZK}}_{\mathcal{S},\mathcal{A}}(\lambda)\right| \leq \mathsf{negl}(\lambda), \textit{ where}$$

$$\Pr_{\Pi,\mathcal{A}}^{\mathsf{ZK}}(\lambda) = \Pr\left[\mathcal{A}_1^{\mathcal{O}}(\pi, \mathsf{st}) = 1 \;\middle|\; \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ (\mathsf{stmt}, \mathsf{wit}, \mathsf{st}) \leftarrow \mathcal{A}_0^{\mathcal{O}}(\mathsf{pp}) \\ \pi \leftarrow \begin{cases} \mathcal{P}^{\mathcal{O}}(\mathsf{stmt}, \mathsf{wit}), & \textit{if } (\mathsf{stmt}, \mathsf{wit}) \in R \\ \bot, & \textit{otherwise} \end{cases} \end{array}\right]$$

$$\Pr_{\mathcal{S},\mathcal{A}}^{\mathsf{ZK}}(\lambda) = \Pr\left[\mathcal{A}_1^{\mathcal{O}_1}(\pi, \mathsf{st}) = 1 \;\middle|\; \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right) \\ (\mathcal{O}_0, \mathsf{ch}) \leftarrow \mathcal{S}_0(\mathsf{pp}) \\ (\mathsf{stmt}, \mathsf{wit}, \mathsf{st}) \leftarrow \mathcal{A}_0^{\mathcal{O}_0}(\mathsf{pp}) \\ (\mathcal{O}_1, \pi) \leftarrow \begin{cases} \mathcal{S}_1(\mathsf{stmt}, \mathsf{ch}, 1), \textit{if } (\mathsf{stmt}, \mathsf{wit}) \in R \\ \mathcal{S}_1(\mathsf{stmt}, \mathsf{ch}, 0), \textit{otherwise} \end{cases} \end{array}\right]$$

2.5.4 Blind Signatures

A blind signature scheme is an interactive protocol where a user $\mathcal{U}$ requests a signature from a signer $\mathcal{S}$ for a message m such that:

- The signer $\mathcal{S}$ cannot link a message-signature pair to any protocol executions.
- The user $\mathcal{U}$ is not able to forge signatures after several interactions with the signer $\mathcal{S}$.

In this work, we consider only round-optimal blind signatures where it takes two moves between the user and the signer for the user to obtain a signature.

Definition 2.42 (Blind Signatures [BLNS23, Section 2.2])**.** *A blind signature scheme* BSig *has PPT algorithms* Setup, KGen, Verify, *and 3 stateful PPT algorithms for the signing protocol in the following order:* Blind, $\mathsf{BlindSign}$, *and* Derive*; such that for any* λ*:*

- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^{\lambda})$*: takes the security parameter* λ *and chooses the public parameters* pp.
- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp})$*: generates a public key* pk *and a secret key* sk *from the public parameters* pp.
- $(t, \mathsf{st}) \leftarrow \mathsf{Blind}(\mathsf{pk}, m)$*: the first move of the signing protocol between a user* $\mathcal{U}$ *and a signer* $\mathcal{S}$*, in which the user takes the public key* pk *and a message* $m \in \{0,1\}^*$ *then generates a blinded message* t *to send to the signer, and a state* st.
- $\sigma \leftarrow \mathsf{BlindSign}(\mathsf{sk}, t)$*: the second move of the signing protocol in which the signer takes the secret key* sk *to provide a standard signature for the blinded message* t*.*

- $\sigma^* \leftarrow \mathsf{Derive}(\mathsf{pk}, \sigma, \mathsf{st})$*: the final move of the signing protocol in which the user takes the public key* pk*, the signature for* t *from the signer* σ*, and the state* st *and outputs a signature for the message* m*.*

- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{pk}, m, \sigma^*)$*: takes the public key* pk*, a message* m*, and a signature* σ^* *and outputs a bit indicating whether the signature is valid* (1) *or invalid* (0).

Definition 2.43 (Correctness [BLNS23, Definition 2.1])**.** *A blind signature scheme* $\mathsf{BSig} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Blind}, \mathsf{BlindSign}, \mathsf{Derive}, \mathsf{Verify})$ *is correct if there exists a negligible function* negl *such that for any message* $m \in \{0,1\}^*$*, we have:*

$$\Pr\left[\mathsf{Verify}(\mathsf{pk}, m, \sigma^*) = 1 \;\middle|\; \begin{array}{r}\mathsf{pp} \leftarrow \mathsf{Setup}\left(1^\lambda\right)\\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp})\\ (t, \mathsf{st}) \leftarrow \mathsf{Blind}(\mathsf{pk}, m)\\ \sigma \leftarrow \mathsf{BlindSign}(\mathsf{sk}, t)\\ \sigma^* \leftarrow \mathsf{Derive}(\mathsf{pk}, \sigma, \mathsf{st})\end{array}\right] \geq 1 - \mathsf{negl}(\lambda)$$

Definition 2.44 (One-More Unforgeability [BLNS23, Definition 2.3])**.** *A blind signature scheme* $\mathsf{BSig} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Blind}, \mathsf{BlindSign}, \mathsf{Derive}, \mathsf{Verify})$ *is one-more unforgeable if for any polynomial* $\ell = \mathsf{poly}(n)$*, and any PPT algorithm* $\mathcal{A}$ *acting as a user, the probability that* $\mathcal{A}$ *succeeds in the experiment* $\mathsf{ExpForge}^{\mathsf{BSig},\mathcal{A}}(\lambda)$ *(as in Fig. 4) is negligible.*

$$\Pr\left[\mathsf{ExpForge}^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] \leq \mathsf{negl}(\lambda)$$

$\mathsf{ExpForge}^{\mathsf{BSig},\mathcal{A}}(\lambda)$	$\mathsf{BlindSign}\mathcal{O}(\mathsf{sk}, t)$
$\mathsf{pp} \leftarrow \mathsf{Setup}\left(1^\lambda\right)$	**if** $c = \ell$ **then**
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp})$	**return** $\perp$
$c := 0$	$c \leftarrow c + 1$
$\{(m_i, \sigma_i)\}_{i \in [\ell+1]} \leftarrow \mathcal{A}^{\mathsf{BlindSign}\mathcal{O}(\mathsf{sk},.)}(\mathsf{pk})$	**return** $\mathsf{BlindSign}(\mathsf{sk}, t)$
if $(\forall i \in [\ell+1] : \mathsf{Verify}(\mathsf{pk}, m_i, \sigma_i) = 1) \wedge$	
$\left(\forall 1 \leq i < j \leq \ell + 1 : m_i \neq m_j\right)$ **then**	
return 1	
return 0	

Figure 4: One-more unforgeability experiment.

Definition 2.45 (Honest-Signer Blindness [BLNS23, Definition 2.2])**.** *A blind signature scheme* $\mathsf{BSig} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Blind}, \mathsf{BlindSign}, \mathsf{Derive}, \mathsf{Verify})$ *is fulfills the* *honest-signer blindness requirement if for any PPT algorithm $\mathcal{A}$ acting as the signer, the advantage of $\mathcal{A}$ in the experiment* $\mathsf{ExpBlind}^{\mathsf{BSig},\mathcal{A}}(\lambda)$ *(as in Fig. 5) is negligible.*

$$\mathsf{Adv}^{\mathsf{ExpBlind}}_{\mathsf{BSig},\mathcal{A}}(\lambda) = \left|\Pr\left[\mathsf{ExpBlind}^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \leq \mathsf{negl}(\lambda)$$

$\mathsf{ExpBlind}^{\mathsf{BSig},\mathcal{A}}(\lambda)$
$\mathsf{pp} \leftarrow \mathsf{Setup}\left(1^{\lambda}\right)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp})$
$m_0, m_1 \leftarrow \mathcal{A}(\mathsf{sk})$
$b \leftarrow\$ \{0, 1\}$
$((t_b, \mathsf{st}_b), (t_{1-b}, \mathsf{st}_{1-b})) \leftarrow (\mathsf{Blind}(\mathsf{pk}, m_b), \mathsf{Blind}(\mathsf{pk}, m_{1-b}))$
$(\sigma_b, \sigma_{1-b}) \leftarrow (\mathcal{A}.\mathsf{BlindSign}(\mathsf{sk}, t_b), \mathcal{A}.\mathsf{BlindSign}(\mathsf{sk}, t_{1-b}))$
$\left(\sigma_b^*, \sigma_{1-b}^*\right) \leftarrow (\mathsf{Derive}(\mathsf{pk}, \sigma_b, \mathsf{st}_b), \mathsf{Derive}(\mathsf{pk}, \sigma_{1-b}, \mathsf{st}_{1-b}))$
if $\sigma_b^* = \perp$ **or** $\sigma_{1-b}^* = \perp$ **then**
$\left(\sigma_b^*, \sigma_{1-b}^*\right) = (\perp, \perp)$
$b^* \leftarrow \mathcal{A}\left(\mathsf{sk}, \sigma_b^*, \sigma_{1-b}^*\right)$
if $b = b^*$ **then return** 1
return 0

Figure 5: Honest-signer blindness experiment.

3 Public-Key Encryption from Distinguish-LIP

In this section, we construct a public-key encryption whose security relies on the hardness of the average-case ΔLIP. Our construction take inspirations from the key-encapsulation mechanism in [DvW22] and the public-key encryption in [ARLW24]. First, we begin a quadratic form $\mathbf{S}$ which has an efficient decoder up to radius $\rho < \lambda_1(\mathbf{S})/2$. The public key is an equivalent form $\mathbf{P} \leftarrow\!\!\$\ \mathcal{D}_s([\mathbf{S}])$, and the secret key is a unimodular transformation $\mathbf{U}$ such that $\mathbf{P} = \mathbf{U}^\mathsf{T}\mathbf{S}\mathbf{U}$. To encrypt a message $\mathbf{m} \in \mathbb{Z}_p^n$ for some modulo p, the sender first samples a random error $\mathbf{e} \in \frac{1}{q}$ such that $\|\mathbf{e}\|_\mathbf{P} \leq \rho$, and he then splits $\mathbf{e}$ into a fractional vector $\mathbf{d}_1 \in \mathbb{T}_q^n$ and an integral vector $\mathbf{x} \in \mathbb{Z}^n$ and uses $\mathbf{x}$ to "one-time pad" $\mathbf{m}$, $\mathbf{d}_2 := \mathbf{x} + \mathbf{m} \bmod p$. The ciphertext is a tuple $(\mathbf{d}_1, \mathbf{d}_2)$. Knowing the unimodular transformation $\mathbf{U}$, the receiver can decode $\mathbf{d}_1$ for $\mathbf{x}$ via $\mathbf{S}$ due to $\mathbf{d}_1 = \mathbf{e} + \mathbf{x}$ and $\|\mathbf{e}\|_\mathbf{P} < \lambda_1(\mathbf{S})/2$, and he can then decrypt for $\mathbf{m}$. For the security proof, it is assumed to be computationally hard to distinguish $\mathbf{P} \leftarrow\!\!\$\ \mathcal{D}_s([\mathbf{S}])$ and a form $\mathbf{R} \leftarrow\!\!\$\ \mathcal{D}_s([\mathbf{Q}])$ for a quadratic form $\mathbf{Q}$ having significantly small smoothing bound $\eta_{2^{-\Theta(n)}}([Q]) \leq \frac{\rho}{kp\sqrt{n}}$. Thus, by replacing $\mathbf{P}$ by $\mathbf{R}$, the ciphertext $(\mathbf{d}_1, \mathbf{d}_2)$ is statistically close to uniformly random.

Our PKE can be used as a commitment scheme which is statistically binding, computationally hiding by the hardness of ac-$\Delta\mathsf{LIP}_s^{\mathbf{S},\mathbf{Q}}$, additively-homomorphic, and extractable by the decryption using the secret key. The extractability of this commitment scheme is important to achieve straightline-extractability in NIZKPoK in Section 5. Additionally, we construct a ZKPoK of a ciphertext wellformedness (or a commitment opening if one uses PKE as a commitment scheme).

3.1 Construction

Let $\mathbf{S} := \mathbf{B}_\mathbf{S}^\mathsf{T}\mathbf{B}_\mathbf{S} \in \mathcal{S}_n^{>0}(\mathbb{Z})$ be a quadratic form being decodable with radius $\rho < \lambda_1(\mathbf{S})/2$. Given $\mathbf{S}, n, \rho$, and other public parameters s, p, q, k, σ parametrised by λ, we construct a public-key encryption scheme $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ for any messages $\mathbf{m} \in \mathbb{Z}_p^n$ in Fig. 6.

$\mathsf{Setup}(1^\lambda)$

$\mathsf{pp} := (\mathbf{S}, s, n, p, q, k, \rho, \sigma)$
return pp

$\mathsf{KGen}(\mathsf{pp})$

$(\mathbf{P}, \mathbf{U}) \leftarrow\!\!\$\ \mathcal{D}_s([\mathbf{S}])$
$\mathsf{pk} := \mathbf{P}$
$\mathsf{sk} := \mathbf{U}$
return $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Enc}\left(\mathsf{pk}, \mathbf{m} \in \mathbb{Z}_p^n\right)$

$\mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},\sigma}$
$\mathbf{d}_1 := \mathbf{e} \bmod \mathbb{Z}^n$
$\mathbf{x} := \mathbf{d}_1 - \mathbf{e}$
$\mathbf{d}_2 := \mathbf{x} + \mathbf{m} \bmod p$
$\mathsf{ctxt} := (\mathbf{d}_1, \mathbf{d}_2)$
return ctxt

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt})$

$\mathbf{u} \leftarrow \mathsf{Decode}(\mathbf{S}, \mathbf{U}\mathbf{d}_1)$
if $\|\mathbf{u} - \mathbf{U}\mathbf{d}_1\|_\mathbf{S} > \rho$ **then**
  return $\perp$
$\mathbf{m}' := \mathbf{d}_2 - \mathbf{U}^{-1}\mathbf{u} \bmod p$
$\mathsf{msg} := \mathbf{m}'$
return msg

Figure 6: LIP-based public-key encryption

Theorem 3.1 (Correctness). *For* $s \geq \max\left\{\lambda_n(\mathbf{S}), \|\mathbf{B}^*_{\mathbf{S}}\| \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$, *and* $q = \frac{ksn}{\rho}\sqrt{\frac{\ln(2n+4)}{\pi}}$, $\sigma = s\sqrt{n}\sqrt{\frac{\ln(2n+4)}{\pi}}$, *and some integers* k *and* $p \geq 2$, PKE *is correct.*

Proof. By Lemma 2.14, one can sample efficiently a quadratic form $\mathbf{P}$ distributed as $\mathcal{D}_s([\mathbf{S}])$ and a unimodular $\mathbf{U}$ for $s \geq \max\left\{\lambda_n(\mathbf{S}), \|\mathbf{B}^*_{\mathbf{S}}\| \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$, such that $\mathbf{P} = \mathbf{U}^{\mathsf{T}}\mathbf{S}\mathbf{U}$.

Since $\sigma = s\sqrt{n}\sqrt{\frac{\ln(2n+4)}{\pi}} \geq \|\mathbf{B}^{\mathsf{GS}}_{\mathbf{P}}\| \sqrt{\frac{\ln(2n+4)}{\pi}}$ with non-negligible probability by Lemma 2.15, it is efficient, by Lemma 2.10, to sample $\mathbf{e} \leftarrow\$ \frac{1}{q}\mathcal{D}_{\mathbf{P},\sigma} \in \frac{1}{q}\mathbb{Z}^n$. By Lemma 2.11, we have $\mathbf{e}$ to be short with non-negligible probability.

$$\|\mathbf{e}\|_{\mathbf{P}} \leq \frac{\sigma\sqrt{n}}{q} = \rho/k < \lambda_1([\mathbf{S}])/2$$

For $\mathbf{d}_1 := \mathbf{e} \bmod \mathbb{Z}^n$ $\|\mathbf{e}\|_{\mathbf{P}} < \lambda_n([\mathbf{S}])/2$, there is a $\mathbf{x} := \mathbf{d}_1 - \mathbf{e} \in \mathbb{Z}^n$ which is a unique and the closest lattice vector to $\mathbf{d}_1$ in $\mathbf{P}$. Therefore, $\mathbf{U}\mathbf{x}$ is the unique and closest vector to $\mathbf{U}\mathbf{d}_1$ in the lattice $\mathbf{S}$. In the decryption, one can decode $\mathbf{U}\mathbf{d}_1$ in $\mathbf{S}$ for a unique vector $\mathbf{u}$ such that $\|\mathbf{u} - \mathbf{U}\mathbf{d}_1\|_{\mathbf{S}} \leq \rho$, so we have $\mathbf{u} = \mathbf{U}\mathbf{x}$. Hence, $\mathbf{m}' = \mathbf{d}_2 - \mathbf{U}^{-1}\mathbf{u} = \mathbf{m} \bmod p$. □

Theorem 3.2 (IND-CPA Security). *Let* $\mathbf{S}$ *and* $\mathbf{Q}$ *be two quadratic forms such that* $\mathbf{S}$ *has an efficient decoding algorithm for distance* $\rho < \lambda_1([\mathbf{S}])/2$, *and* $\sigma/q \geq p\eta_{2^{-\Theta(n)}}([\mathbf{Q}])$ *for* $\sigma/q = \rho/k\sqrt{n}$ *and positive integers* k *and* $p \geq 2$. *If* ac-ΔLIP$_s^{\mathbf{S},\mathbf{Q}}$ *is hard,* PKE *is* IND-CPA*-secure.*

Proof. The proof comprises a set of hybrid experiments.

- Hyb_0: Identical to $\mathsf{IND\text{-}CPA}^0_{\mathsf{PKE},\mathcal{A}}(1^\lambda)$.
- Hyb_1: Identical to Hyb_0, except that the key pair $(\mathbf{P}, \mathbf{U})$ is sampled from the distribution $\mathcal{D}_s([\mathbf{Q}])$ instead of $\mathcal{D}_s([\mathbf{S}])$.
- Hyb_2: Identical to Hyb_1, except that we choose uniformly $\mathbf{d}_1 \leftarrow\$ \mathbb{T}^n_q$ and $\mathbf{d}_2 \leftarrow\$ \mathbb{Z}^n_p$.
- Hyb_3: Identical to Hyb_1, except that $\mathbf{m}_1$ is chosen for encryption.
- Hyb_4: Identical to $\mathsf{IND\text{-}CPA}^1_{\mathsf{PKE},\mathcal{A}}(1^\lambda)$.

Due to the hardness of ac-ΔLIP$_s^{\mathbf{S},\mathbf{Q}}$, Hyb_0 and Hyb_1 are computationally indistinguishable.

$$\left|\Pr\left[\mathsf{Hyb}_0 = 1\right] - \Pr[\mathsf{Hyb}_1 = 1]\right| \leq \mathsf{negl}(\lambda)$$

Likewise, Hyb_3 and Hyb_4 are also computationally indistinguishable.

$$\left|\Pr\left[\mathsf{Hyb}_3 = 1\right] - \Pr[\mathsf{Hyb}_4 = 1]\right| \leq \mathsf{negl}(\lambda)$$

In Hyb_1 and Hyb_3, $\mathbf{P}$ is generated from $\mathbf{Q}$ and

$$\sigma/q \geq p\eta_{2^{-\Theta(n)}}([\mathbf{Q}]) = \eta_{2^{-\Theta(n)}}\left(\left[p^2\mathbf{P}\right]\right) > \eta_{2^{-\Theta(n)}}([\mathbf{P}])$$

By Corollary 2.9.1, the distribution of $\mathbf{d}_1$ in Hyb_1 and Hyb_3 is statistical close to the uniform distribution over $\mathbb{T}_q^n$, and the conditional distribution of $\mathbf{x}$ is $\mathcal{D}_{\mathbf{P},\sigma/q,\mathbf{d}_1}$ given $\mathbf{d}_1 \in \mathbb{T}_q^n$.

$$\left\{(\mathbf{d}_1,\mathbf{x}) \;\middle|\; \begin{array}{l} \mathbf{e} \leftarrow\$ \frac{1}{q}\mathcal{D}_{\mathbf{P},\sigma} \\ \mathbf{d}_1 := \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{x} := \mathbf{d}_1 - \mathbf{e} \end{array}\right\} \approx_s \left\{(\mathbf{d}_1,\mathbf{x}) \;\middle|\; \begin{array}{l} \mathbf{d}_1 \leftarrow\$ \mathbb{T}_q^n \\ \mathbf{x} \leftarrow\$ \mathcal{D}_{\mathbf{P},\sigma/q,\mathbf{d}_1} \end{array}\right\}$$

Then, by Corollary 2.9.2, the conditional distribution of $\left(\mathcal{D}_{\mathbf{P},\sigma/q,\mathbf{d}_1} \bmod p\right)$ given $\mathbf{d}_1 \in \mathbb{T}_q^n$ is statistically close to the uniform distribution over $\mathbb{Z}_p^n$.

$$\begin{aligned} \left\{(\mathbf{d}_1,\mathbf{d}_2) \;\middle|\; \begin{array}{l} \mathbf{e} \leftarrow\$ \frac{1}{q}\mathcal{D}_{\mathbf{P},\sigma} \\ \mathbf{d}_1 := \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{x} := \mathbf{d}_1 - \mathbf{e} \\ \mathbf{d}_2 := \mathbf{x} \bmod p \end{array}\right\} &\approx_s \left\{(\mathbf{d}_1,\mathbf{d}_2) \;\middle|\; \begin{array}{l} \mathbf{d}_1 \leftarrow\$ \mathbb{T}_q^n \\ \mathbf{x} \leftarrow\$ \mathcal{D}_{\mathbf{P},\sigma/q,\mathbf{d}_1} \\ \mathbf{d}_2 := \mathbf{x} \bmod p \end{array}\right\} \\ &\approx_s \left\{(\mathbf{d}_1,\mathbf{d}_2) \;\middle|\; \begin{array}{l} \mathbf{d}_1 \leftarrow\$ \mathbb{T}_q^n \\ \mathbf{d}_2 \leftarrow\$ \mathbb{Z}_p^n \end{array}\right\} \end{aligned}$$

Hence, the distribution of $\mathbf{d}_2 := \mathbf{x} + \mathbf{m} \bmod p$ where $\mathbf{m} \leftarrow\$ \mathbb{Z}_p^n$ is statistical close to the uniform distribution over $\mathbb{Z}_p^n$.

$$\left\{(\mathbf{d}_1,\mathbf{d}_2) \;\middle|\; \begin{array}{l} \mathbf{m} \leftarrow\$ \mathbb{Z}_p^n \\ \mathbf{e} \leftarrow\$ \frac{1}{q}\mathcal{D}_{\mathbf{P},\sigma} \\ \mathbf{d}_1 := \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{x} := \mathbf{d}_1 - \mathbf{e} \\ \mathbf{d}_2 := \mathbf{x} + \mathbf{m} \bmod p \end{array}\right\} \approx_s \left\{(\mathbf{d}_1,\mathbf{d}_2) \;\middle|\; \begin{array}{l} \mathbf{d}_1 \leftarrow\$ \mathbb{T}_q^n \\ \mathbf{d}_2 \leftarrow\$ \mathbb{Z}_p^n \end{array}\right\}$$

Therefore, Hyb_1 is statistically indistinguishable from Hyb_2, and Hyb_2 is statistically indistinguishable from Hyb_3.

$$\begin{aligned} |\Pr[\mathsf{Hyb}_1 = 1] - \Pr[\mathsf{Hyb}_2 = 1]| &\leq \mathsf{negl}(\lambda) \\ \left|\Pr[\mathsf{Hyb}_2 = 1] - \Pr\left[\mathsf{Hyb}_3 = 1\right]\right| &\leq \mathsf{negl}(\lambda) \end{aligned}$$

Hence, we have:

$$\begin{aligned} \mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}}\left(1^\lambda\right) &= \left|\Pr\left[\mathsf{IND\text{-}CPA}^0_{\mathsf{PKE},\mathcal{A}}\left(1^\lambda\right) = 1\right] - \Pr\left[\mathsf{IND\text{-}CPA}^1_{\mathsf{PKE},\mathcal{A}}\left(1^\lambda\right) = 1\right]\right| \\ &= \left|\Pr\left[\mathsf{Hyb}_0 = 1\right] - \Pr[\mathsf{Hyb}_4 = 1]\right| \\ &= \left|\sum_{i=1}^{4} \Pr\left[\mathsf{Hyb}_{i-1} = 1\right] - \Pr\left[\mathsf{Hyb}_i = 1\right]\right| \\ &\leq \sum_{i=1}^{4}\left|\Pr\left[\mathsf{Hyb}_{i-1} = 1\right] - \Pr\left[\mathsf{Hyb}_i = 1\right]\right| \leq \mathsf{negl}(\lambda) \end{aligned}$$

□

If we instantiate PKE with parameters $\sigma = s\sqrt{n}\sqrt{\frac{\ln(2n+4)}{\pi}}$ and $q = \frac{ksn}{\rho}\sqrt{\frac{\ln(2n+4)}{\pi}}$ for an integer $k \geq 2$ while keeping $\rho \leq \lambda_1([\mathbf{S}])/2$, PKE is additively homomorphic. As long as the summed error vector $\|\mathbf{e}\|_{\mathbf{P}} \leq \rho$, the associated ciphertexts can be correctly decrypted. A ciphertext $(\mathbf{d}_1, \mathbf{d}_2) \leftarrow \mathsf{Enc}(\mathbf{P}, \mathbf{m})$ can be multiplied by an integer $t \in [-k, k]$ and be decrypted to $t\mathbf{m}$.

Theorem 3.3 (Additively Homomorphic). *For some positive integer $k \geq 2$, $\sigma = s\sqrt{n}\sqrt{\frac{\ln(2n+4)}{\pi}}$ and $q = \frac{ksn}{\rho}\sqrt{\frac{\ln(2n+4)}{\pi}}$, it holds for $(\mathbf{d}_{1,1}, \mathbf{d}_{1,2}) \leftarrow \mathsf{Enc}(\mathbf{P}, \mathbf{m}_1)$ and $(\mathbf{d}_{2,1}, \mathbf{d}_{2,2}) \leftarrow \mathsf{Enc}(\mathbf{P}, \mathbf{m}_2)$ that:*

$$\mathbf{m}_1 + \mathbf{m}_2 \bmod p \leftarrow \mathsf{Dec}\left(\mathbf{S}, \left(\mathbf{d}'_1, \mathbf{d}'_2\right)\right)$$

where $\mathbf{d}'_1 = \mathbf{d}_{1,1} + \mathbf{d}_{2,1} \bmod \mathbb{Z}^n$ *and* $\mathbf{d}'_2 = \mathbf{d}_{1,2} + \mathbf{d}_{2,2} \bmod p$

Proof. Let $\mathbf{e}_1$ and $\mathbf{e}_2$ be the error vectors sampled when encrypting $\mathbf{m}_1$ and $\mathbf{m}_2$, respectively and $\mathbf{e}' = \mathbf{e}_1 + \mathbf{e}_2 \in \frac{1}{q}\mathbb{Z}^n$. We have that:

$$\begin{aligned}
\mathbf{d}'_1 &= \mathbf{d}_{1,1} + \mathbf{d}_{2,1} = \mathbf{e}_1 + \mathbf{e}_2 \bmod \mathbb{Z}^n = \mathbf{e}' \bmod \mathbb{Z}^n \\
\mathbf{d}'_2 &= \mathbf{d}_{1,2} + \mathbf{d}_{2,2} \\
&= \left(\mathbf{d}_{1,1} - \mathbf{e}_1\right) + \left(\mathbf{d}_{2,1} - \mathbf{e}_2\right) + \mathbf{m}_1 + \mathbf{m}_2 \bmod p \\
&= \left(\mathbf{d}'_1 - \mathbf{e}'\right) + \mathbf{m}_1 + \mathbf{m}_2 \bmod p
\end{aligned}$$

Let $\mathbf{x} = \mathbf{d}'_1 - \mathbf{e}' \in \mathbb{Z}^n$. Since $\|\mathbf{e}'\|_{\mathbf{P}} \leq \|\mathbf{e}_1\|\mathbf{P} + \|\mathbf{e}_2\|\mathbf{P} \leq 2\rho/k \leq \lambda_1([\mathbf{S}])/2$, $\mathbf{x}$ is the unique and closest vector of $\mathbf{P}$ to $\mathbf{d}'_1$. Hence, the decryption can decode $\mathbf{U}\mathbf{d}'_1$ to $\mathbf{U}\mathbf{x}$ in $\mathbf{S}$ and then decrypt for $\mathbf{m}' = \mathbf{d}'_2 - \mathbf{x} = \mathbf{m}_1 + \mathbf{m}_2 \bmod p$. □

3.2 Usage as a Commitment Scheme

Any IND-CPA-secure public key encryption implies a commitment scheme that is computationally hiding and statistically binding. One can use our LIP-based PKE as a commitment scheme $\mathsf{Com} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Commit}, \mathsf{Open})$ on the same public parameters $\mathsf{pp} := (\mathbf{S}, s, n, p, q, k, \rho, \sigma)$ such that:

- $\mathsf{ck} \leftarrow \mathsf{KGen}(\mathsf{pp})$: runs $\mathsf{PKE.KGen}(1^\lambda)$ to get $(\mathsf{pk}, \mathsf{sk}) = (\mathbf{P}, \mathbf{U})$, discard sk, set $\mathsf{ck} := \mathbf{P}$ and return ck.

- $(\mathsf{com}, r) \leftarrow \mathsf{Commit}\left(\mathsf{ck}, \mathbf{m} \in \mathbb{Z}_p^n\right)$: runs $\mathsf{PKE.Enc}(\mathsf{ck}, \mathbf{m})$ but gets the ciphertext $(\mathbf{d}_1, \mathbf{d}_2)$ together with the error vector $\mathbf{e} \leftarrow\$ \frac{1}{q}\mathcal{D}_{\mathbf{P},\sigma}$, and outputs the commitment $\mathsf{com} := (\mathbf{d}_1, \mathbf{d}_2)$ and the randomness $r := \mathbf{e}$.

- $\{0, 1\} \leftarrow \mathsf{Open}(\mathsf{ck}, \mathsf{com}, \mathbf{m}, r, f)$: takes the commitment key ck, commitment $\mathsf{com} = (\mathbf{d}_1, \mathbf{d}_2)$, message $\mathbf{m}$, randomness $r = \mathbf{e}$ and an integer $f \in \left[\left\lceil -\frac{k}{2} \right\rceil, \left\lfloor \frac{k}{2} \right\rfloor\right] \setminus \{0\}$ and checks whether

  $$f\mathbf{d}_1 = \mathbf{e} \bmod \mathbb{Z}^n \wedge f\mathbf{d}_2 = \mathbf{x} + f\mathbf{m} \bmod p$$

  where $\mathbf{x} = (f\mathbf{d}_1 - \mathbf{e})$ (without modulo p)

The proof that Com is hiding follows the proof that PKE is $\mathsf{IND\text{-}CPA}$-secure based on the hardness of $\mathsf{ac\text{-}\Delta LIP}_s^{\mathbf{S},\mathbf{Q}}$ for $\mathbf{S}$ and $\mathbf{Q}$ be two quadratic forms such that there exists an efficient decoding algorithm for distance $\rho < \lambda_1([\mathbf{S}])/2$ in $[\mathbf{S}]$, and $\sigma/q \geq p\eta_{2^{-\Theta(n)}}([\mathbf{Q}])$ for $\sigma/q = \rho/k\sqrt{n}$, and positive integers k and $p \geq 2$.

Similar to the well-known lattice-based BDLOP commitment scheme [BDL+18], our commitment admits a relaxed opening including not only the message $\mathbf{m}$ and randomness $\mathbf{e}$ but also a scalar $f \in \left[\left\lceil -\frac{k}{2} \right\rceil, \left\lfloor \frac{k}{2} \right\rfloor\right] \setminus \{0\}$. We are unable to build efficient zero-knowledge proofs (in Fig. 7) to prove the knowledge of $\mathbf{m}$ and $\mathbf{r}$ satisfying the original commitment/encryption relation such that its extractor cannot guarantee to extract exactly $f = 1$ from the prover. For this weaker zero-knowledge proof, the commitment scheme must still be binding with a relaxed opening.

For PKE is additively homomorphic, Com of course inherits this properties, so we can construct fairly simple zero-knowledge proofs of linear relations over the committed messages.

Theorem 3.4 (Computationally Hiding)**.** *If $\mathsf{ac\text{-}\Delta LIP}_s^{\mathbf{S},\mathbf{Q}}$ is hard for two quadratic forms $\mathbf{S}$ and $\mathbf{Q}$ such that $\mathbf{S}$ has an efficient decoding algorithm for distance $\rho < \lambda_1([\mathbf{S}])/2$, and $\sigma/q \geq p\eta_{2^{-\Theta(n)}}([\mathbf{Q}])$ for $\sigma/q = \rho/k\sqrt{n}$ and positive integers k and $p \geq 2$, Com is computationally hiding.*

Proof. This proof follows the proof to Theorem 3.2 that PKE is $\mathsf{IND\text{-}CPA}$-secure if $\mathsf{ac\text{-}\Delta LIP}_s^{\mathbf{S},\mathbf{Q}}$ is hard. □

Theorem 3.5 (Statistically Binding)**.** *For $\sigma = s\sqrt{n}\sqrt{\frac{\ln(2n+4)}{\pi}}$, $q = \frac{ksn}{\rho}\sqrt{\ln\left(\frac{2n+4}{\pi}\right)}$, $f \in \left[\left\lceil -\frac{k}{2} \right\rceil, \left\lfloor \frac{k}{2} \right\rfloor\right] \setminus \{0\}$, a positive integer $k \geq 2$, and a prime p, Com is statistically binding.*

Proof. Assume that there exists an adversary $\mathcal{A}$ given the quadratic form $\mathbf{P}$ is capable of outputting a commitment $(\mathbf{d}_1, \mathbf{d}_2)$ and valid openings $(\mathbf{m}, \mathbf{e}, f)$ and $(\mathbf{m}', \mathbf{e}', f')$ with $\mathbf{m} \neq \mathbf{m}'$ such that:

$$\begin{aligned}
f\mathbf{d}_1 &= \mathbf{e} \bmod \mathbb{Z}^n \\
f\mathbf{d}_2 &= (f\mathbf{d}_1 - \mathbf{e}) + f\mathbf{m} \bmod p \\
f'\mathbf{d}_1 &= \mathbf{e}' \bmod \mathbb{Z}^n \\
f'\mathbf{d}_2 &= (f'\mathbf{d}_1 - \mathbf{e}') + f'\mathbf{m}' \bmod p
\end{aligned}$$

Multiplying f' to the first two equations and f to the other twos then subtracting, we have that:

$$\begin{aligned}
f'\mathbf{e} - f\mathbf{e}' &= \mathbf{0}^n \bmod \mathbb{Z}^n \\
(f'\mathbf{e} - f\mathbf{e}') + ff'(\mathbf{m}' - \mathbf{m}) &= \mathbf{0}^n \bmod p
\end{aligned}$$

For p is prime, f and f' are invertible in $\mathbb{Z}_p$, and $\mathbf{m}' \neq \mathbf{m}$, so $ff'(\mathbf{m}' - \mathbf{m})$ is non-zero. This therefore implies that $\mathbf{x} := (f'\mathbf{e} - f\mathbf{e}') \in \mathbb{Z}^n$ is a non-zero lattice vector in $\mathbf{P}$. For

$f, f' \in \left[\left\lceil -\frac{k}{2} \right\rceil, \left\lfloor \frac{k}{2} \right\rfloor\right] \setminus \{0\}$, $k \geq 2$, the **P**-norm of $\mathbf{x} \in \mathbb{Z}^n$ is shorter than $\lambda_1([\mathbf{S}])/2$

$$\|\mathbf{x}\|_{\mathbf{P}} \leq (|f| + |f'|) \frac{\rho}{k} < \rho \leq \lambda_1([\mathbf{S}])/2 = \lambda_1([\mathbf{P}])/2$$

This is impossible for any lattice vector of **P** since the shortest vector **P** is of length $\lambda_1([\mathbf{P}])$. Therefore, $\mathcal{A}$ cannot break the binding of Com. □

3.3 Zero-Knowledge Proof of Plaintext Knowledge (Commitment Opening)

We show a zero-knowledge proof protocol to prove the wellformedness of ciphertexts produced by PKE or the knowledge of a valid opening of Com. To convince a verifier that a ciphertext $(\mathbf{d}_1, \mathbf{d}_2)$ is correctly constructed, the prover must provide a proof that it knows a short vector $\mathbf{e} \in \frac{1}{q}\mathbb{Z}^n$ and the plaintext $\mathbf{m} \in \mathbb{Z}_q^n$ which satisfy $\mathbf{d}_1 = \mathbf{e} \bmod \mathbb{Z}^n$ and $\mathbf{d}_2 = (\mathbf{d}_1 - \mathbf{e}) + \mathbf{m} \bmod p$. We observe that one can uniquely determine the message $\mathbf{m}$ given the ciphertext $(\mathbf{d}_1, \mathbf{d}_2)$ and the short error vector $\mathbf{e}$. Thus, the zero-knowledge proof only needs to prove the knowledge of $\mathbf{e}$ without $\mathbf{m}$.

Our proof employs a technique which is similar to that of the Lyubashevsky's identification scheme [Lyu12] and the zero-knowledge proof for the opening of a BDLOP commitment [BDL+18]. The prover samples a mask $\mathbf{r}$ which is short but large enough to mask $\mathbf{e}$ and outputs $\mathbf{a} := \mathbf{r} \bmod \mathbb{Z}^n$. For a challenge $c \in [-g, g]$ where g is a small positive element of $\mathbb{Z}_p$, the prover outputs $\mathbf{z} = \mathbf{r} + c\mathbf{e}$ (for some challenge c) with rejection sampling, so that $\mathbf{z}$ does not leak information about $\mathbf{e}$. Then, the verifier can check if $\mathbf{z}$ is short and $\mathbf{a} + c\mathbf{d}_1 = \mathbf{z} \bmod \mathbb{Z}^n$. We can obtain, by rewinding, another equation $\mathbf{a} + c'\mathbf{d}_1 = \mathbf{z}' \bmod \mathbb{Z}^n$ for $c \neq c'$, and by subtracting the two, we have

$$\mathbf{z}' - \mathbf{z} = (c' - c)\,\mathbf{d}_1 \bmod \mathbb{Z}^n$$

Since the term $(c' - c)$ is not invertible in the above equation and not necessarily equal to 1, we can only extract $\mathbf{e}^* = \mathbf{z}' - \mathbf{z}$ which is short if $(c' - c)$ is relatively small. Particularly, by construction of our proof, $\|\mathbf{e}^*\|_{\mathbf{P}} \leq 2\left(\sigma\sqrt{n} + g\beta\right)$ where β is the upper bound of the **P**-norm of $\mathbf{e}$ held by the honest prover and σ is the Gaussian parameter used in sampling the mask $\mathbf{r}$. For $\mathbf{r}$ to hide $\mathbf{e}$ with rejection sampling, we require $\sigma = \Theta\left(g\beta\sqrt{\ln n}\right)$, and we have $\beta = \rho/k$. Then, for convincing the verifier with the extracted $\mathbf{e}^*$, it is required that $\|\mathbf{e}^*\|_{\mathbf{P}} \leq \rho$, so we can obtain the lower bound of k when instantiate PKE (or Com):

$$\rho \geq 2\Theta\left(g\beta\sqrt{n \ln n}\right) + 2g\beta, \text{ or}$$
$$k = \Omega\left(g\sqrt{n \ln n}\right)$$

Having $\mathbf{e}^* = \mathbf{z}' - \mathbf{z} = f\mathbf{d}_1$ where $f = c' - c$, one can extract $\mathbf{m}^* = f\mathbf{d}_2 - f^{-1}\mathbf{x}^*$ where $\mathbf{x}^* := f\mathbf{d}_1 - \mathbf{e}^*$ (without modulo p). For a prime p, f is invertible in $\mathbb{Z}_p$. Hence, another weakpoint of our proof is that it can only convince the verifier about the wellformedness of the ciphertext (or a opening to the commitment) $(f\mathbf{d}_1, f\mathbf{d}_2)$

for some relaxing factor $f = c' - c \in [-2g, 2g - 1] \setminus \{0\}$. However, as long as the extracted $\mathbf{e}^*$ has $\mathbf{P}$-norm shorter than $\lambda_1(\mathbf{P})/2$ and for PKE is additively homomorphic (or Com is still binding while accepting relaxed openings), our proof can sufficiently convince the verifier about the knowledge of $\mathbf{e}$ and $\mathbf{m}$.

Let $\mathsf{pp} := (n, p, q, k, \beta, \sigma, M)$ be parametrised by λ. The zero-knowledge proof of plaintext knowledge for PKE (or commitment opening for Com) described in Fig. 7 is a proof of knowledge for the following relation:

$$R^{\mathsf{PKE}}_{\mathsf{pp},\beta} = \left\{ (\mathsf{stmt}, \mathsf{wit}) \;\middle|\; \begin{array}{l} \mathsf{stmt} := (\mathbf{P}, \mathbf{d}_1, \mathbf{d}_2) \in \mathcal{S}_n^{>0}(\mathbb{Z}) \times \mathbb{T}_q^n \times \mathbb{Z}_p^n \\ \quad \mathsf{wit} := (\mathbf{e}, \mathbf{m}, f) \in \frac{1}{q}\mathbb{Z}^n \times \mathbb{Z}_p^n \times \bar{C} \\ \|\mathbf{e}\|_{\mathbf{P}} \leq \beta \\ f\mathbf{d}_1 = \mathbf{e} \bmod \mathbb{Z}^n \\ f\mathbf{d}_2 = (f\mathbf{d}_1 - \mathbf{e}) + f\mathbf{m} \bmod p \end{array} \right\}$$

where $\bar{C} = \{c' - c : \forall c, c' \in [-g, g], c \neq c'\}$

Protocol Σ^{PKE}

$$\begin{array}{lcl}
\underline{\mathcal{P}((\mathbf{P}, \mathbf{d}_1, \mathbf{d}_2), (\mathbf{e}, \mathbf{m}))} & & \underline{\mathcal{V}((\mathbf{P}, \mathbf{d}_1, \mathbf{d}_2))} \\
\mathbf{r} \leftarrow\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma} & & \\
\mathbf{a} := \mathbf{r} \bmod \mathbb{Z}^n & & \\
 & \xrightarrow{\quad\mathbf{a}\quad} & \\
 & & c \leftarrow\!\$\ [-g, g] \\
 & \xleftarrow{\quad c\quad} & \\
\mathbf{z} := \mathbf{r} + c\mathbf{e} & & \\
\text{Abort with probability} & & \\
\quad 1 - \min\left(1, \dfrac{\mathcal{D}_{\mathbf{P},q\sigma}(q\mathbf{z})}{M\mathcal{D}_{\mathbf{P},q\sigma,qc\mathbf{e}}(q\mathbf{z}_1)}\right) & & \\
 & \xrightarrow{\quad\mathbf{z}\quad} & \\
 & & \text{Accept iff:} \\
 & & \quad \mathbf{z} \in \frac{1}{q}\mathbb{Z}^n, \\
 & & \quad \|\mathbf{z}\|_{\mathbf{P}} \leq \sigma\sqrt{n} + g\beta, \text{ and} \\
 & & \quad \mathbf{z} = \mathbf{a} + c\mathbf{d}_1 \bmod \mathbb{Z}^n
\end{array}$$

Figure 7: Protocol Σ^{PKE} for proving plaintext knowledge for PKE

Theorem 3.6. *For $q\sigma \geq \left\|\mathbf{B}_{\mathbf{P}}^{\mathsf{GS}}\right\|\sqrt{\frac{\ln(2n+4)}{\pi}}$, $\sigma = \Theta\left(g\beta\sqrt{\ln n}\right)$, $k = \Omega\left(g\sqrt{n\ln n}\right)$, p is prime, and $M = O(1)$, Σ^{PKE} is complete for $R^{\mathsf{PKE}}_{\mathsf{pp},\beta}$, special-sound for $R^{\mathsf{PKE}}_{\mathsf{pp},2\left(\sigma\sqrt{n}+g\beta\right)}$, and SHVZK for $R^{\mathsf{PKE}}_{\mathsf{pp},2\left(\sigma\sqrt{n}+g\beta\right)}$.*

Proof. **Completeness**. Given $q\sigma \geq \left\|\mathbf{B}_{\mathbf{P}}^{\mathsf{GS}}\right\|\sqrt{\frac{\ln(2n+4)}{\pi}}$, it is efficient to sample $\mathbf{r} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma}$ by Lemma 2.10, and by Lemma 2.11, we have that $\|\mathbf{r}\|_{\mathbf{P}} \leq \sigma\sqrt{n}$. Since both $\mathbf{r}, \mathbf{e} \in \frac{1}{q}\mathbb{Z}^n$, $\mathbf{z} = \mathbf{r} + c\mathbf{e} \in \frac{1}{q}\mathbb{Z}^n$, so condition b_0 is satisfied. By the triangular inequality and for $c \in [-g, g]$, we have the condition b_1 satisfied.

$$\|\mathbf{z}\|_{\mathbf{P}} \leq \|\mathbf{r}\|_{\mathbf{P}} + \|c\mathbf{e}\|_{\mathbf{P}} \leq \sigma\sqrt{n} + g\|\mathbf{e}\|_{\mathbf{P}} \leq \sigma\sqrt{n} + g\beta$$

Finally, by construction, the condition b_2 is satisfied.

$$\begin{aligned}\mathbf{a} + c\mathbf{d}_1 &= \mathbf{r} + c\mathbf{e} \bmod \mathbb{Z}^n\\ &= \mathbf{z} \bmod \mathbb{Z}^n\end{aligned}$$

Special Soundness. With two accepting transcripts $(\mathbf{a}, c, \mathbf{z})$ and $(\mathbf{a}, c', \mathbf{z}')$, we can extract a witness $(\mathbf{e}^*, \mathbf{m}^*, f)$:

$$\begin{aligned}\mathbf{e}^* &:= \mathbf{z}' - \mathbf{z} \in \frac{1}{q}\mathbb{Z}^n\\ f &:= c' - c \in \bar{C}\\ \mathbf{m}^* &:= \mathbf{d}_2 - f^{-1}\mathbf{x}^* \bmod p \in \mathbb{Z}_p^n\end{aligned}$$

where $\mathbf{x}^* = f\mathbf{d}_1 - \mathbf{e}^*$ (without $\bmod p$). For p is prime, c', c and f are invertible in $\mathbb{Z}_p$.

By construction, we have that:

$$\begin{aligned}\|\mathbf{e}^*\|_{\mathbf{P}} &= \|\mathbf{z}' - \mathbf{z}\|_{\mathbf{P}}\\ &\leq \|\mathbf{z}'\|_{\mathbf{P}} + \|\mathbf{z}\|_{\mathbf{P}}\\ &\leq 2\left(\sigma\sqrt{n} + g\beta\right) \leq \rho, \text{ and}\end{aligned}$$

$$\begin{aligned}\mathbf{e}^* &= \mathbf{z}' - \mathbf{z}\\ &= \mathbf{a} + c'\mathbf{d}_1 - \mathbf{a} - c\mathbf{d}_1\\ &= f\mathbf{d}_1 \bmod \mathbb{Z}^n, \text{ and}\end{aligned}$$

$$\begin{aligned}(f\mathbf{d}_1 - \mathbf{e}^*) + f\mathbf{m}^* &= \mathbf{x}^* + f\mathbf{d}_2 - \mathbf{x}^* \bmod p\\ &= f\mathbf{d}_2 \bmod p\end{aligned}$$

Hence, $(\mathbf{e}^*, \mathbf{m}^*, f)$ is a valid witness.

Lemma 3.7 (adapted from Lemma 2.24)**.** *For a quadratic form $\mathbf{Q} \in \mathcal{S}_n^{>0}(\mathbb{R})$ and any vector $\mathbf{v} \in \mathbb{R}^n$, if $s = \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}\sqrt{\ln n}\right)$, then:*

$$\Pr\left[\mathbf{z} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{Q},qs} : \frac{\mathcal{D}_{\mathbf{Q},qs}(q\mathbf{z})}{\mathcal{D}_{\mathbf{Q},qs,q\mathbf{v}}(q\mathbf{z})} = O(1)\right] \geq 1 - 2^{-\Theta(\ln n)}.$$

Proof. By Definition 2.6, we have:

$$\frac{\mathcal{D}_{\mathbf{Q},qs}(q\mathbf{z})}{\mathcal{D}_{\mathbf{Q},qs,q\mathbf{v}}(q\mathbf{z})} = \frac{\rho_{\mathbf{Q},qs}(q\mathbf{z})}{\rho_{\mathbf{Q},qs,q\mathbf{v}}(q\mathbf{z})} = \frac{\exp(-\pi\|q\mathbf{z}\|_{\mathbf{Q}}^2/q^2s^2)}{\exp(-\pi\|q\mathbf{z}-q\mathbf{v}\|_{\mathbf{Q}}^2/q^2s^2)}$$
$$= \exp\left(\pi\frac{-2\langle\mathbf{z},\mathbf{v}\rangle_{\mathbf{Q}}+\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right)$$

By Lemma 2.23, we have $\left|\langle\mathbf{z},\mathbf{v}\rangle_{\mathbf{Q}}\right|$ is at most $r=\Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}s\sqrt{\ln n}\right)$ with probability:

$$\Pr\left[\mathbf{z}\leftarrow_\$ \frac{1}{q}\mathcal{D}_{\mathbf{Q},qs} : \left|\langle\mathbf{z},\mathbf{v}\rangle_{\mathbf{Q}}\right| \le \Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}s\sqrt{\ln n}\right)\right] \ge 1-2e^{-\pi\Theta(\ln n)}$$
$$= 1-2^{-\Theta(\ln n)}$$

Thus, with probability at least $1-2^{-\Theta(\ln n)}$, we have:

$$\exp\left(\pi\frac{-2\langle\mathbf{z},\mathbf{v}\rangle_{\mathbf{Q}}+\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right) \le \exp\left(\pi\frac{\Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}s\sqrt{\ln n}\right)+\|\mathbf{v}\|_{\mathbf{Q}}^2}{s^2}\right)$$
$$= O(1)$$

where the last equality uses $s=\Theta\left(\|\mathbf{v}\|_{\mathbf{Q}}\sqrt{\ln n}\right)$. □

Theorem 3.8 (adapted from Theorem 2.26)**.** *For a quadratic form $\mathbf{Q}\in\mathcal{S}_n^{>0}(\mathbb{R})$, a subset $V\subset\mathbb{R}^n$ such that $V=\left\{\mathbf{v}\in\mathbb{R}^n : \|\mathbf{v}\|_{\mathbf{Q}}<\beta\right\}$ for some positive $\beta\in\mathbb{R}$, and $s=\Theta\left(\beta\sqrt{\ln n}\right)$, there exists a constant $M=O(1)$ such that the statistical distance between distributions of the following algorithms $\mathcal{A}$ taking a vector $\mathbf{v}\in V$ as the input and $\mathcal{B}$ is at most $\frac{2^{-\Theta(\ln n)}}{M}$, and $\mathcal{A}$ outputs something with probability at least $\frac{1-2^{-\Theta(\ln n)}}{M}$.*

$\mathcal{A}(\mathbf{v})$	$\mathcal{B}$
$\mathbf{z}\leftarrow_\$ \frac{1}{q}\mathcal{D}_{\mathbf{Q},qs,q\mathbf{v}}$	$\mathbf{z}\leftarrow_\$ \frac{1}{q}\mathcal{D}_{\mathbf{Q},qs}$
return z *with probability* $\min\left(1,\frac{\mathcal{D}_{\mathbf{Q},qs}(q\mathbf{z})}{M\mathcal{D}_{\mathbf{Q},qs,q\mathbf{v}}(q\mathbf{z})}\right)$	**return z** *with probability* $\frac{1}{M}$

Proof. By Lemma 3.7, we have for $M=O(1)$:

$$\forall\mathbf{v}\in V, \Pr\left[\mathbf{z}\leftarrow_\$ \frac{1}{q}\mathcal{D}_{\mathbf{Q},qs} : M\mathcal{D}_{\mathbf{Q},qs,\mathbf{v}}(q\mathbf{z}) \ge \mathcal{D}_{\mathbf{Q},qs}(q\mathbf{z})\right] \ge 1-2^{-\Theta(\ln n)}$$

Applying Lemma 2.25 with f set as $\mathcal{D}_{\mathbf{Q},qs}$, and g set as $\mathcal{D}_{\mathbf{Q},qs,q\mathbf{v}}$, we have the statistical distance between the outputs of $\mathcal{A}$ and $\mathcal{B}$ is at most $\frac{2^{-\Theta(\ln n)}}{M}$, and the probability that $\mathcal{A}$ outputs something is at least $\frac{1-2^{-\Theta(\ln n)}}{M}$. □

$$
\begin{array}{|l|}
\hline
\mathcal{S}\left((\mathbf{P}, \mathbf{d}_1, \mathbf{d}_2), c\right) \\
\hline
\mathbf{z} \leftarrow\!\!\$ \ \frac{1}{q}\mathcal{D}_{\mathbf{P}, q\sigma} \in \frac{1}{q}\mathbb{Z}^n \\
\mathbf{a} := \mathbf{z} - c\mathbf{d}_1 \bmod \mathbb{Z}^n \in \mathbb{T}_q^n \\
\text{with probability } 1 - \frac{1}{M}: \\
\quad \textbf{abort} \\
\textbf{return } (\mathbf{a}, c, \mathbf{z}) \\
\hline
\end{array}
$$

Figure 8: The simulator of Σ^{PKE}

SHVZK. Given a challenge $c \in [-g, g]$, we define a simulator $\mathcal{S}$ in Fig. 8 that gives an accepting conversation.

By Lemma 2.10, we have with overwhelming probability that:

$$
\begin{aligned}
\|q\mathbf{z}\|_{\mathbf{P}} &\leq q\sigma\sqrt{n}, \text{ or} \\
\|\mathbf{z}\|_{\mathbf{P}} &\leq \sigma\sqrt{n} < \sigma\sqrt{n} + g\beta
\end{aligned}
$$

By construction, we have $\mathbf{z} \in \frac{1}{q}\mathbb{Z}^n$ and $\mathbf{a} = \mathbf{z} - c\mathbf{d}_1 \bmod \mathbb{Z}^n \in \mathbb{T}_q^n$, so $\mathbf{z} = \mathbf{a} + c\mathbf{d}_1 \bmod \mathbb{Z}^n$. Thus, $\mathcal{S}\left((\mathbf{P}, \mathbf{d}_1, \mathbf{d}_2), c\right)$ yields an accepting conversation $(\mathbf{a}, c, \mathbf{z})$. We continue the proof using the following games:

- Game_0: Same as an honest prover.
- Game_1: Same as Game_0 except that $\mathbf{a} := \mathbf{z} - c\mathbf{d}_1 \bmod \mathbb{Z}^n$.
- Game_2: Same as Game_1 except that $\mathbf{z} \leftarrow\!\!\$ \ \frac{1}{q}\mathcal{D}_{\mathbf{P}, q\sigma}$, and it aborts with probability $1 - 1/M$.

From the completeness proof of Σ^{PKE}, we see that Game_0 and Game_1 are identical and therefore indistinguishable. Applying Theorem 3.8 with $V = \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v}\|_{\mathbf{P}} \leq g\beta\}$, $s = \sigma$ and $\mathbf{u} = \mathbf{0}$, we have for $\mathbf{v} = c\mathbf{e} \in V$ and $\sigma = \Theta\left(g\beta\sqrt{\ln n}\right)$, there exists a constant $M = O(1)$ such that the distribution of $\mathbf{z}$ in Game_1 is within statistical distance of $\frac{2^{-\Theta(\ln n)}}{M}$ to the distribution of $\mathbf{z}$ in Game_2. Hence, Game_1 and Game_2 are statistically indistinguishable. For Game_2 is identical to $\mathcal{S}$, the simulator $\mathcal{S}$ outputs an accepting conversation $(\mathbf{a}, c, \mathbf{z})$ distributed statistically close to that of an honest execution of Σ^{PKE}. □

4 One More Close Vector Problem Assumption

In this section, we introduce the one more close vector problem (omCVP) assumption. The hardness of omCVP implies the one-more unforgeability of our blind signature scheme in Section 6. In the LIP-based signature scheme proposed by Ducas and van Woerden [DvW22], there is a quadratic form $\mathbf{S}$ which has an efficient Gaussian sampler for a small parameter $\rho/\sqrt{n} \geq \eta_{2^{-\Theta(n)}}([\mathbf{S}])$, and the public key is an equivalent form $\mathbf{P} \leftarrow\$ \mathcal{D}_s([\mathbf{S}])$, and the secret key is the unimodular transformation $\mathbf{U}$ such that $\mathbf{P} = \mathbf{U}^\mathsf{T}\mathbf{S}\mathbf{U}$. The signature to target $\mathbf{t} = H(m) \in \mathbb{T}_q^n$ is a vector $\mathbf{x}$ distributed as $\mathcal{D}_{\mathbf{P},\rho/\sqrt{n},\mathbf{t}}$ achieved via Gaussian sampling in $\mathbf{S}$ with the unimodular transformation $\mathbf{U}$. Hence, $\mathbf{x}$ is a close vector to $\mathbf{t}$, $\|\mathbf{x}-\mathbf{t}\|_\mathbf{P} \leq \rho$. Similar to other one-more type assumption such as omSIS [AKSY22], we informally define the omCVP assumption as it is computationally hard for a PPT adversary to come up with $\ell+1$ valid LIP-based signatures after knowing ℓ valid ones for $\ell = \mathsf{poly}(\lambda)$.

An adversary in the omCVP experiment is given access to two oracles Gaussian$\mathcal{O}$ and Target$\mathcal{O}$. A query to the Target$\mathcal{O}$ oracle is answered with a random vector $\mathbf{t} \in \mathbb{T}_q^n$, and we use this oracle to model the random oracle $H : \{0,1\}^* \to \mathbb{T}_q^n$ in the security proof of our blind signatures. The Gaussian$\mathcal{O}$ oracle, upon a query for a target $\mathbf{t}' \in \mathbb{T}_q^n$, responses with a vector $\mathbf{x} \in \mathbb{Z}^n$ which is close to $\mathbf{t}'$ (i.e., $\|\mathbf{x}-\mathbf{t}'\|_\mathbf{P} \leq \rho$), but an adversary can only make at most ℓ queries to Gaussian$\mathcal{O}$. The adversary wins the omCVP experiment if it outputs $\ell+1$ tuples $\{(\mathbf{t}_i,\mathbf{x}_i)\}_{i\in[\ell+1]}$ such that for all $i \in [\ell+1]$ $\mathbf{t}_i$ is a respond of Target$\mathcal{O}$, and $\mathbf{x}_i \in \mathbb{Z}^n$ is close to $\mathbf{t}_i$, $\|\mathbf{x}_i - \mathbf{t}_i\|_\mathbf{P} \leq \delta$. We may allow a relaxed closeness $\delta \geq \rho$ between $\mathbf{x}_i$ and $\mathbf{t}_i$, but we stress that the larger δ is, the easier it takes to solve omCVP.

We later present polynomial-time attacks to omCVP for some range of δ with respect to ρ. Our attacks are the adaptation of the attacks against omSIS in [AKSY22]. Same as other assumtptions of the same one-more type, we are unable to reduce the omCVP to standard assumptions, but we would like convince via our cryptanalysis attempt that our parameter choice for the blind signatures is safe from polynomial-time attacks.

4.1 Definition

Definition 4.1 (omCVP Assumption)**.** *Let $\mathbf{S}, n, s, \mu, \rho, q, \ell, \delta$ be functions of λ where $\mathbf{S} \in \mathcal{S}_n^{>0}(\mathbb{Z})$ is a quadratic form and*

$$s \geq \max\left\{\lambda_n(\mathbf{S}), \left\|\mathbf{B}_\mathbf{S}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$$

$$\rho/\sqrt{n} \geq \eta_{2^{-\Theta(n)}}([\mathbf{S}])$$

$$q := \left\lceil \frac{s\cdot n}{\rho} \cdot \sqrt{\frac{\ln(2n+4)}{\pi}} \right\rceil$$

The omCVP$_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$ *assumption states that for all PPT adversary* $\mathcal{A}$*, the probability that* $\mathcal{A}$ *wins the* omCVP$^{\mathcal{A}}_{\mathbf{S},n,s,\rho,q,\ell,\delta}$ *experiment as in Fig. 9 is negligible.*

$$\Pr\left[\mathsf{omCVP}^{\mathcal{A}}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}(\lambda) = 1\right] \leq \mathsf{negl}(\lambda)$$

$\mathsf{omCVP}^{\mathcal{A}}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}(\lambda)$

$T := \emptyset$

$c := 0$

$\mathbf{P} \leftarrow\!\!\$\ \mathcal{D}_{s,\mu}([\mathbf{S}])$

$\{(\mathbf{t}_i, \mathbf{x}_i)\}_{i \in [\ell+1]} \leftarrow \mathcal{A}^{\mathsf{Target}\mathcal{O}, \mathsf{Gaussian}\mathcal{O}(.)}(\mathbf{P})$

if $\forall i \in [\ell+1], \mathbf{x}_i \in \mathbb{Z}^n \wedge \|\mathbf{x}_i - \mathbf{t}_i\|_{\mathbf{P}} \leq \delta \wedge \mathbf{t}_i \in T$ **then**

  return 1

return 0

$\mathsf{Gaussian}\mathcal{O}(\mathbf{t}')$

$c := c + 1$

if $c > \ell$ **then**

  return $\perp$

$\mathbf{x} \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{P},\rho/\sqrt{n},\mathbf{t}'}$

return $\mathbf{x}$

$\mathsf{Target}\mathcal{O}$

$\mathbf{t} \leftarrow\!\!\$\ \mathbb{T}_q^n$

$T \leftarrow T \cup \{\mathbf{t}\}$

return $\mathbf{t}$

Figure 9: omCVP assumption.

4.2 Cryptanalysis

This cryptanalysis is to argue that the new computational problem omCVP is hard. Though we are not able to obtain a reduction from a standard and well-studied problem to omCVP, we expect that this problem is hard for polynomial-time adversaries for the parameter ranges specified in our blind signature construction in Section 6.1. The hardness of omCVP primarily depends on the relation between δ, the upper bound of the distance between the vectors $\mathbf{x}_i$'s that the adversaries must output and their corresponding targets $\mathbf{t}_i$'s, ρ, the distance between the queried target and the vector answered by the Gaussian oracle, and the dimension n of the quadratic forms $\mathbf{P}$ and $\mathbf{S}$.

We first consider the trivial case for which omCVP can be solved without queries to the Gaussian oracles. By Lemma 2.14 and Lemma 2.10, it is efficient to sample from the quadratic form $\mathbf{P} \leftarrow\!\!\$\ \mathcal{D}_{s,\mu}([S])$ with Gaussian parameter larger than or equal to $s\sqrt{n}\sqrt{\frac{\ln(2n+4)}{\pi}}$ due to $\left\|\mathbf{B}_{\mathbf{P}}^{\mathsf{GS}}\right\| \leq s\sqrt{n}$. Therefore, for any target $\mathbf{t}$, any adversaries can efficiently sample a close vector $\mathbf{x}$ such that $\|\mathbf{x} - \mathbf{t}\|_{\mathbf{P}} \leq sn\sqrt{\frac{\ln(2n+4)}{\pi}}$, so we have the omCVP assumption trivially broken with $\delta = \Theta\left(sn\sqrt{\ln n}\right)$.

Then, we provide two techniques to attack omCVP: combinatorial and lattice-based. These two are the adaptation of the attack strategies against omSIS [AKSY22]. By these attacks, we explicitly describe the parameter ranges for which omCVP can be solved in polynomial-time and for which it is exponentially hard to the best of our knowledge.

In the combinatorial attack, the adversary begins with a set of elementary vectors such that any target $\mathbf{t} \in \mathbb{T}_q^n$ can be presented by a sum of at most n elementary vectors. For each elementary vector, the adversary makes a $\mathsf{Gaussian}O$ queries for a close vector. Then, for each target $\mathbf{t}$, the adversary decomposes it to at most n elementary vectors and combine the close vectors to these elementary vectors to achieve a close vector to $\mathbf{t}$, and it is at most $\rho \cdot n$ in distance.

In the lattice-based attack, the adversary makes several $\mathsf{Gaussian}O$ queries on targets $\mathbf{0}$ and obtain a set of short vectors. Then, it can create a quadratic form $\mathbf{P}' = \mathbf{U}'^{\mathsf{T}}\mathbf{P}\mathbf{U}'$ which is slight worse than $\mathbf{S}$ but better than $\mathbf{P}$ in the sense it is efficient to do Gaussian sampling from $\mathbf{P}'$ with a parameter $\Theta\left(\rho\sqrt{\ln n}\right)$. Therefore, knowing $\mathbf{P}'$ and $\mathbf{U}'$, the adversary can find a close vector to any target $\mathbf{t}$, and it is at most $\Theta\left(\rho\sqrt{n \ln n}\right)$ in distance.

To sum up, our best polynomial-time attack gives solution to the $\mathsf{omCVP}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$ for $\delta = \Theta\left(\rho\sqrt{n \ln n}\right)$ and $\ell = \Theta(n)$. Meanwhile, the security of our blind signatures assumes that the $\mathsf{omCVP}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$ is hard for $\delta = \Theta(\rho)$, and for such small δ, we know only exponential-time attacks.

4.2.1 Combinatorial Attack

Consider the set of vectors

$$A = \left\{\mathbf{v}_i \cdot t : \forall i \in [n], t \in \mathbb{T}_q\right\}, \text{ where } \begin{pmatrix}\mathbf{v}_1 & \cdots & \mathbf{v}_n\end{pmatrix} = \mathbf{I}_n$$

There are $q \cdot n$ vectors in the set A, and it is clear that A is a subset of $\mathbb{T}_q^n$ such that any target $\mathbf{t} \in \mathbb{T}_q^n$ can be a sum of at most n vectors from A (one for each dimension). The adversary $\mathcal{A}$ (described in Fig. 10) first makes $\mathsf{Gaussian}O$ queries for all vectors in A and acquires vectors $\mathbf{x}'$. Thus, for each vector $\mathbf{a} \in A$, $\mathcal{A}$ knows a vector $\mathbf{x}' \in \mathbb{Z}^n$ such that $\|\mathbf{x}' - \mathbf{a}\|_{\mathbf{P}} \leq \rho$ with overwhelming probability. Leveraging this knowledge, $\mathcal{A}$ decomposes a target $\mathbf{t} \in \mathbb{T}_q^n$ as a sum of at most n vectors from A and sum all the corresponding $\mathbf{x}'$'s to obtain $\mathbf{x} \in \mathbb{Z}^n$ whose distance to $\mathbf{t} \in \mathbb{T}_q^n$ in $\mathbf{P}$ is at most $\rho \cdot n$ to win the omCVP experiment for $\delta = \Theta(\rho \cdot n)$ and $\ell = \Theta(q \cdot n)$.

$$\|\mathbf{x} - \mathbf{t}\|_{\mathbf{P}} = \left\|\sum_{k \in [n]} \mathbf{x}'_k - \sum_{k \in [n]} \mathbf{a}_k\right\|_{\mathbf{P}} = \sum_{k \in [n]} \left\|\mathbf{x}'_k - \mathbf{a}_k\right\| \leq \rho \cdot n$$

$\mathcal{A}^{\mathsf{Gaussian}O(.),\mathsf{Target}O}(\mathbf{P})$

$A := \left\{\mathbf{a} := \mathbf{v}_i \cdot t : \forall i \in [n], t \in \mathbb{T}_q\right\}$
$X := \emptyset$
for $i \in [q \cdot n]$ **do**
  $\mathbf{x}_i' \leftarrow \mathsf{Gaussian}O(\mathbf{a}_i)$
  $X[\mathbf{a}_i] := \mathbf{x}_i'$
for $j \in [\ell + 1]$ **do**
  $\mathbf{t}_j \leftarrow \mathsf{Target}O$
  Decompose $\mathbf{t}_j$ into $\{\mathbf{a}_k\}_{k\in[n]}$ s.t. $\mathbf{t}_j = \sum_{k=1}^{n} \mathbf{a}_k \wedge \{\mathbf{a}_k\}_{k\in[n]} \subset A$
  $\mathbf{x}_j = \sum_{k=1}^{n} X[\mathbf{a}_k]$
return $\left\{(\mathbf{t}_j, \mathbf{x}_j)\right\}_{j\in[\ell+1]}$

Figure 10: The combinatorial attack against $\mathsf{omCVP}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$.

4.2.2 Lattice-based Attack

As described in Fig. 11, one can construct an EPT attack $\mathcal{A}$ (similar to the definition of $s, \mu([\mathbf{Q}])$ in Definition 2.13) against the omCVP assumption if $\delta = \Theta\left(\rho\sqrt{n \ln n}\right)$. Firstly, $\mathcal{A}$ queries the discrete Gaussian oracle $\mathsf{Gaussian}O$ for a set of short vectors $\mathbf{V} = (\mathbf{v}_i)_{i\in[\ell]}$ such that $\mathbf{v}_i \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{P},\rho/\sqrt{n}}$ then uses the algorithm $\mathsf{Extract}(\mathbf{P}, \mathbf{V})$ to get another quadratic form $\mathbf{P}'$ and unimodular transformation $\mathbf{U}'$ such that $\mathbf{P}' = \mathbf{U}'^{\mathsf{T}}\mathbf{P}\mathbf{U}'$. By Lemma 2.11 and Lemma 2.12, $\left\|\mathbf{B}_{\mathbf{P}'}^{\mathsf{GS}}\right\| = \max_i \|\mathbf{v}_i\|_{\mathbf{Q}} \leq \rho$, so it is efficient to sample from the discrete Gaussian distribution $\mathcal{D}_{\mathbf{P}',\rho\sqrt{\frac{\ln(2n+4)}{\pi}}}$. Having $\mathbf{P}'$ and the transformation $\mathbf{U}'$, $\mathcal{A}$ can sample short vectors $\mathbf{x}_i$ for each of $\ell + 1$ targets $\mathbf{t}_i$ queried from the $\mathsf{Target}O$ such that $\|\mathbf{x}_i - \mathbf{t}_i\|_{\mathbf{P}} \leq \rho\sqrt{\frac{n\ln(2n+4)}{\pi}}$ to win the omCVP experiment for $\delta = \Theta\left(\rho\sqrt{n \ln n}\right)$ and $\ell = \Theta(n)$.

We can obtain an attack for a shorter bound on δ at higher cost by:

1. Calling the closest vector problem algorithm on the quadratic form $\mathbf{P}$ and the targets $\mathbf{t}_i$'s.

2. Generating a quadratic form (equivalent to $\mathbf{P}$) that has an efficient Gaussian sampler for shorter standard deviation parameter than that of the Gaussian oracle by calling the shortest vector problem algorithm on the quadratic form $\mathbf{P}$.

In the former case, we can obtain vectors $\mathbf{x}_i$'s such that for $i \in [\ell]$, $\|\mathbf{x}_i - \mathbf{t}_i\|_{\mathbf{P}} \leq \lambda_1(\mathbf{P})$. In the latter case, we first obtain an equivalent form $\mathbf{P}'$ such that $\left\|\mathbf{B}_{\mathbf{P}'}^{\mathsf{GS}}\right\| = \lambda_1(\mathbf{P})$, so by using the same technique in Fig. 11, we can obtain vectors $\mathbf{x}_i$'s such that for

$\mathcal{A}^{\mathsf{Gaussian}O(.),\mathsf{Target}O}(\mathbf{P})$

$C := 1 - (1 + e^{-\pi})^{-1}$
$\ell := \lceil 2n/C \rceil$
do
  for $i = 1, \ldots, \ell$ **do**
    $\mathbf{v}_i \leftarrow \mathsf{Gaussian}O(\mathbf{0})$
  $\mathbf{V} := (\mathbf{v}_i)_{i \in [\ell]}$
while $\mathsf{rank}(\mathbf{V}) < n$
$(\mathbf{P}', \mathbf{U}') \leftarrow \mathsf{Extract}(\mathbf{P}, \mathbf{V})$
for $i = 1, \ldots, \ell + 1$ **do**
  $\mathbf{t}_i \leftarrow \mathsf{Target}O$
  $\mathbf{x}_i \leftarrow\!\!\$\ \mathbf{U}'\mathcal{D}_{\mathbf{P}',\rho\sqrt{\ln(2n+4)/\pi},\mathbf{U}'^{-1}\mathbf{t}_i}$
return $\{(\mathbf{t}_i, \sigma_i)\}_{i \in [\ell+1]}$

Figure 11: The lattice-based attack against $\mathsf{omCVP}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$.

$i \in [\ell]$, $\|\mathbf{x}_i - \mathbf{t}_i\|_{\mathbf{P}} \leq \lambda_1(\mathbf{P}) \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$. The fastest known algorithms to solve the shortest and closest vector problems run in time $2^{\Theta(n)}$ [MV10, ADRSD15]. These exponential attacks allow us to solve the omCVP for $\delta = \Theta(\lambda_1(\mathbf{P}))$. This bound on δ is obviously even smaller than ρ.

5 NIZKPoK of Close Vectors

To construct blind signature scheme from the omCVP assumption, we need an NIZKPoK system with straightline extractability for LIP signatures, i.e., to prove the knowledge of a lattice vector $\mathbf{x} \in \mathbb{Z}^n$ that is close to a target $\mathbf{h} \in \mathbb{T}_q^n$.

$$\|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}} \leq \beta$$

We first starts with a relatively simple 3-move ZKPoK Σ^{CV} which encloses $\mathbf{x}$ in a vector $\mathbf{z} \in \mathbb{Z}^n$ which is slightly farther to $\mathbf{h}$ and uses rejection sampling [Lyu12] to prevent $\mathbf{z}$ to leak any information regarding $\mathbf{x}$. The main two drawbacks of this protocol are that

- It takes a small challenge set $\{0, 1\}$, so we requires λ parallel repetitions to have it reach soundness error of $2^{-\lambda}$.
- Its knowledge extractor can only extract witnesses $\mathbf{x}^*$ whose distance to the target $\mathbf{h}$ is larger than that of the original witness. This is called *soundness slack* in lattice-based ZKPoK [ACK21].

$$\|\mathbf{x}^* - \mathbf{h}\|_{\mathbf{P}} \leq \beta', \text{ where } \beta' > \beta$$

We can make this protocol non-interactive in the random oracle by the Fiat-Shamir transformation, and to achieve straightline extractability, we encrypt the witness $\mathbf{x}$ by the public-key encryption PKE in Section 3.1 given that $\mathbf{x}$ falls in the plaintext space $\mathbb{Z}_p^n$, and we use the Fiat-Shamir transformation of the ZKPoK in Section 3.3 to prove that the ciphertext correctly encrypt $\mathbf{x}$. Our combined non-interactive protocol Π^{CV} proves the knowledge of $\mathbf{x}$ that is close to $\mathbf{h}$ and correctly encrypted by PKE. With the secret key of PKE, we can use the decryption of the ciphertext in the proof as a straightline extractor. Since we only need to decrypt the ciphertext in the security proof, this technique for straightline extractability is called "encryption to the sky". However, due to the soundness slack issue in Σ^{CV}, a proof π from combined NIZKPoK Π^{CV} for the statement $(\mathbf{P}, \mathbf{h})$ can only convince a verifier that the witness $\mathbf{x}^*$ extracted from π satisfies $\|\mathbf{x}^* - \mathbf{h}\|_{\mathbf{P}} \leq \beta'$.

To overcome the high soundness error and the soundness slack issue in the above protocol, we introduce the second ZKPoK which is for proving simultaneously many quadratic relations. The technique in this proof is similar to the lattice-based ZKPoKs which circumvent the soundness slack issue [YAZ+19, LNP22a]. Without harming the zero-knowledge property, the prover can prove the knowledge of $\mathbf{x}$ such that $\|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}} = B$ for some $B \leq \beta$. Then, we reduce this $\mathbf{P}$-norm equation to a set of $N = 2n + 1$ quadratic equations of the form $\mathbf{w}^\mathsf{T}\mathbf{A}_i\mathbf{w} + \mathbf{b}_i^\mathsf{T}\mathbf{w} = d_i$ (for $i \in [N]$) over a witness $\mathbf{w}$ which is a binary vector. We employ the commitment scheme based on PKE in Section 3.2 and construct a commit-and-prove ZKPoK. For the commitment scheme works on vectors in the ring $\mathbb{Z}_p$ for some prime p, we only prove that $\mathbf{w}^\mathsf{T}\mathbf{A}_i\mathbf{w} + \mathbf{b}_i^\mathsf{T}\mathbf{w} = d_i \bmod p$. Therefore, p is required to be large enough, so that there is no wraparound in all N quadratic equations. To prove N quadratic relations simultaneously, we linearly combine these relations into one quadratic relation, and then the prover can provide an amortised ZKPoK Π^*. This ZKPoK is free from the soundness slack issue and has smaller soundness error than the previous Π^{CV}. Again, it is trivial to convert Π^* into a non-interactive proof by the Fiat-Shamir transformation. A commitment to the witness is included in this proof, so we have a straightline extractor for free, i.e., the decryptor of PKE.

5.1 Approximate ZKPoK of a Close Vector

In the blind signatures from omCVP in Section 6.1, the signature $\mathbf{x} \in \mathbb{Z}^n$ is of distance at most β from the hash of the message $\mathbf{h} = H(m) \in \mathbb{T}_q^n$. To achieve blindness, we need a zero-knowledge proof of knowledge of such vector $\mathbf{x}$.

Let $\mathsf{pp} := (n, q, \beta, \sigma, M)$ be parametrised by λ. For a quadratic form $\mathbf{P} = \mathbf{B}_\mathbf{P}^\mathsf{T}\mathbf{B}_\mathbf{P} \in \mathcal{S}_n^{>0}(\mathbb{Z})$, a target $\mathbf{h} \in \mathbb{T}_q^n$, and a vector $\mathbf{x} \in \mathbb{Z}^n$ satisfying $\|\mathbf{x} - \mathbf{h}\|_\mathbf{P} \le \beta$, we have the relation $R_{\mathsf{pp},\beta}$:

$$R_{\mathsf{pp},\beta} = \left\{ (\mathsf{stmt}, \mathsf{wit}) \,\middle|\, \begin{array}{l} \mathsf{stmt} := (\mathbf{P}, \mathbf{h}) \in \mathcal{S}_n^{>0}(\mathbb{Z}) \times \mathbb{T}_q^n \\ \mathsf{wit} := \mathbf{x} \in \mathbb{Z}^n \\ \|\mathbf{x} - \mathbf{h}\|_\mathbf{P} \le \beta \end{array} \right\}$$

Then, we construct a protocol Σ^{CV} which is a ZKPoK system for the relation $R_{\mathsf{pp},\beta}$ in Fig. 12.

Theorem 5.1. *For $q\sigma \ge \left\|\mathbf{B}_\mathbf{P}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$, the protocol Σ^{CV} is complete for the relation $R_{\mathsf{pp},\beta}$.*

Proof. For $q\sigma \ge \left\|\mathbf{B}_\mathbf{P}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$, by Lemma 2.10, it is efficient to sample an error $\mathbf{e} \leftarrow\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma} \in \frac{1}{q}\mathbb{Z}^n$, and by Lemma 2.11, we have $\|\mathbf{e}\|_\mathbf{P} \le \sigma\sqrt{n}$ with overwhelming probability. With $\mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \in \mathbb{T}_q^n$, we have $\mathbf{a} - \mathbf{e} \in \mathbb{Z}^n$, and with $c\mathbf{x} \in \mathbb{Z}^n$, we have $\mathbf{z} := \mathbf{a} - \mathbf{e} + c\mathbf{x} \in \mathbb{Z}^n$. Thus, when the prover $\mathcal{P}$ executes the protocol honestly, we have:

$$\begin{aligned} &\mathbf{z} \in \mathbb{Z}^n, \text{ and} \\ \|\mathbf{z} - c\mathbf{h} - \mathbf{a}\|_\mathbf{P} &= \|\mathbf{a} - \mathbf{e} + c\mathbf{x} - c\mathbf{h} - \mathbf{a}\|_\mathbf{P} \\ &= \|c(\mathbf{x} - \mathbf{h}) - \mathbf{e}\|_\mathbf{P} \\ &\le \sigma\sqrt{n} + c\beta \end{aligned}$$

Thus, the verifier accepts with overwhelming probability. □

Theorem 5.2. *The protocol Σ^{CV} is special-sound for the relation $R_{\mathsf{pp},2\sigma\sqrt{n}+\beta}$.*

Proof. Suppose there are two accepting conversations $(\mathbf{a}, 0, \mathbf{z})$ and $(\mathbf{a}, 1, \mathbf{z}')$ of Σ^{CV} where the first message $\mathbf{a}$ is identical. The acceptance implies that:

$$\begin{aligned} \|\mathbf{z} - \mathbf{a}\|_\mathbf{P} &\le \sigma\sqrt{n} \\ \|\mathbf{z}' - \mathbf{h} - \mathbf{a}\|_\mathbf{P} &\le \sigma\sqrt{n} + \beta \end{aligned}$$

	Protocol Σ^{CV}	
$\underline{\mathcal{P}\left((\mathbf{P},\mathbf{h}),\mathbf{x}\right)}$		$\underline{\mathcal{V}\left((\mathbf{P},\mathbf{h})\right)}$
$\mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma}$		
$\mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n$		
	$\xrightarrow{\mathbf{a}}$	
		$c \leftarrow\!\!\$\ \{0,1\}$
	$\xleftarrow{c}$	
$\mathbf{z} := \mathbf{a} - \mathbf{e} + c\mathbf{x}$		
Abort with probability		
$1 - \min\left\{1, \frac{\mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+c\mathbf{h}}(\mathbf{z})}{M\mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+c\mathbf{x}}(\mathbf{z})}\right\}$		
	$\xrightarrow{\mathbf{z}}$	
		Accept iff:
		$\mathbf{z} \in \mathbb{Z}^n$ and
		$\|\mathbf{z} - c\mathbf{h} - \mathbf{a}\|_{\mathbf{P}} \leq \sigma\sqrt{n} + c\beta$

Figure 12: Protocol Σ^{CV} for knowledge of a close vector

Thus, we have:

$$\begin{aligned} \|\mathbf{z}' - \mathbf{h} - \mathbf{a} - \mathbf{z} + \mathbf{a}\|_{\mathbf{P}} &\leq \|\mathbf{z}' - \mathbf{h} - \mathbf{a}\|_{\mathbf{P}} + \|\mathbf{z} - \mathbf{a}\|_{\mathbf{P}} \\ \|\mathbf{z}' - \mathbf{z} - \mathbf{h}\|_{\mathbf{P}} &\leq \sigma\sqrt{n} + \beta + \sigma\sqrt{n} \\ \|(\mathbf{z}' - \mathbf{z}) - \mathbf{h}\|_{\mathbf{P}} &\leq 2\sigma\sqrt{n} + \beta \end{aligned}$$

Thus, $\mathbf{x}^* := \mathbf{z}' - \mathbf{z} \in \mathbb{Z}^n$ is a witness for the relation $R_{\mathsf{pp},2\sigma\sqrt{n}+\beta}$. □

Theorem 5.3. *For $M = \mathsf{poly}(n)$ and $\sigma = \Theta\left(\beta\sqrt{\frac{1}{\ln n}}\right)$, or $M = O(1)$ and $\sigma = \Theta\left(\beta\sqrt{\ln n}\right)$, and $\sigma \geq \eta_{2^{-\Theta(n)}}([\mathbf{P}])$, the protocol Σ^{CV} is SHVZK for the relation $R_{\mathsf{pp},2\sigma\sqrt{n}+\beta}$.*

Proof. Given a challenge $c \in \{0,1\}$, we define a simulator $\mathcal{S}$ in Fig. 13 that gives an accepting conversation.

In the case of $c = 0$, $\mathcal{S}$ computes the three vectors $\mathbf{e}$, $\mathbf{a}$, and $\mathbf{z}$ in the same manner as an honest execution of Σ^{CV}. Therefore, the conversation $(\mathbf{a}, 0, \mathbf{z})$ yielded by $\mathcal{S}$ is accepting and has, by construction, the same distribution as an honest execution of Σ^{CV}.

$$\begin{array}{|l|}\hline \mathcal{S}((\mathbf{P},\mathbf{h}),c) \\ \hline \mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma,-qc\mathbf{h}} \in \frac{1}{q}\mathbb{Z}^n \\ \mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \in \mathbb{T}_q^n \\ \mathbf{z} := \mathbf{a} - \mathbf{e} \in \mathbb{Z}^n \\ \textbf{return}\ \ (\mathbf{a}, 1, \mathbf{z})\ \text{ with probability } \frac{1}{M} \\ \hline \end{array}$$

Figure 13: The simulator of Σ^{CV}

In the case of $c = 1$, by Lemma 2.10, we have with overwhelming probability that:

$$\begin{aligned} \|\mathbf{e}q + \mathbf{h}q\|_{\mathbf{P}} &\le q\sigma\sqrt{n}, \text{ or} \\ \|\mathbf{e} + \mathbf{h}\|_{\mathbf{P}} &\le \sigma\sqrt{n}. \end{aligned}$$

By construction, we have $\mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \in \mathbb{T}_q^n$ and $\mathbf{z} := \mathbf{a} - \mathbf{e} \in \mathbb{Z}^n$. Therefore,

$$\begin{aligned} \|\mathbf{z} - \mathbf{h} - \mathbf{a}\|_{\mathbf{P}} &= \|\mathbf{a} - \mathbf{e} - \mathbf{h} - \mathbf{a}\|_{\mathbf{P}} \\ &= \|-\mathbf{e} - \mathbf{h}\|_{\mathbf{P}} \le \sigma\sqrt{n} < \sigma\sqrt{n} + \beta \end{aligned}$$

Thus, $\mathcal{S}((\mathbf{P}, \mathbf{h}), c = 1)$ yields an accepting conversation $(\mathbf{a}, 1, \mathbf{z})$. We continue the proof using two following simulators:

- $\mathcal{S}_1$: samples a commitment $\mathbf{a} \leftarrow\!\!\$\ \mathbb{T}_q^n$ uniformly, then samples a response $\mathbf{z} \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{x}}$ and outputs $\mathbf{z}$ with probability $\min\left\{1, \frac{\mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{h}}(\mathbf{z})}{M\mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{x}}(\mathbf{z})}\right\}$.
- $\mathcal{S}_2$: samples a commitment $\mathbf{a} \leftarrow\!\!\$\ \mathbb{T}_q^n$ uniformly, then samples a response $\mathbf{z} \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{h}}$ and outputs $\mathbf{z}$ with probability $\frac{1}{M}$.

For $\sigma \ge \eta_{2^{-\Theta(n)}}([\mathbf{P}])$, we have by Corollary 2.9.1 that these two distributions are statistically close:

$$\left\{(\mathbf{a},\mathbf{e}) \;\middle|\; \begin{array}{l} \mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma} \\ \mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \end{array}\right\} \approx_s \left\{(\mathbf{a},\mathbf{e}) \;\middle|\; \begin{array}{l} \mathbf{a} \leftarrow\!\!\$\ \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma} : \mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n \end{array}\right\}$$

Note that restricting $\mathbf{e} \in \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma}$ to satisfy $\mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n$ simply means restricting the support to the coset $\mathbf{P} + \mathbf{a}$. Thus, the distribution of $\mathbf{e}$ is equivalent to $\mathcal{D}_{\mathbf{P}+\mathbf{a},\sigma}$ or $\left(\mathbf{a} + \mathcal{D}_{\mathbf{P},\sigma,-\mathbf{a}}\right)$. Substituting, we have:

$$\begin{aligned} \left\{(\mathbf{a},\mathbf{e}) \;\middle|\; \begin{array}{l} \mathbf{a} \leftarrow\!\!\$\ \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma} : \mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n \end{array}\right\} &= \left\{(\mathbf{a},\mathbf{e}) \;\middle|\; \begin{array}{l} \mathbf{a} \leftarrow\!\!\$\ \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{P}+\mathbf{a},\sigma} \end{array}\right\} \\ &= \left\{(\mathbf{a},\mathbf{e}) \;\middle|\; \begin{array}{l} \mathbf{a} \leftarrow\!\!\$\ \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{P},\sigma,-\mathbf{a}} + \mathbf{a} \end{array}\right\} \end{aligned}$$

Consequently, for $\mathbf{z} := \mathbf{a} - \mathbf{e} + \mathbf{x}$, the two following distributions are statistically close:

$$\left\{ (\mathbf{a}, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\$\; \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma} : \mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{z} := \mathbf{a} - \mathbf{e} + \mathbf{x} \end{array} \right\} = \left\{ (\mathbf{a}, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{z} \leftarrow\!\$\; \mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{x}}. \end{array} \right\}$$

where the last equality is due to

$$\mathbf{a} - (\mathcal{D}_{\mathbf{P},\sigma,-\mathbf{a}} + \mathbf{a}) + \mathbf{x} = \mathcal{D}_{\mathbf{P}+\mathbf{x},\sigma,\mathbf{a}+\mathbf{x}}$$

and $\mathbf{P} + \mathbf{x} = \mathbf{P}$ (for $\mathbf{x} \in \mathbb{Z}^n$ is a lattice vector of $\mathbf{P}$). We conclude that:

$$\left\{ (\mathbf{a}, 1, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{e} \leftarrow\!\$\; \mathcal{D}_{\mathbf{P},\sigma} \\ \mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{z} := \mathbf{a} - \mathbf{e} + \mathbf{x} \end{array} \right\} \approx_s \left\{ (\mathbf{a}, 1, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{z} \leftarrow\!\$\; \mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{x}} \end{array} \right\}$$

Therefore, an honest execution of Σ^{CV} conditioned on the challenge $c = 1$ is statistically indistinguishable from $\mathcal{S}_1$.

Likewise, we use the same series of arguments to prove the closeness of $\mathcal{S}_2$ and $\mathcal{S}$. For $\sigma \geq \eta_{2^{-\Theta(n)}}([\mathbf{P}])$, we have by Corollary 2.9.1 that these two distributions are statistically close:

$$\left\{ (\mathbf{a}, \mathbf{e}) \,\middle|\, \begin{array}{l} \mathbf{e} \leftarrow\!\$\; \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma,-q\mathbf{h}} \\ \mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \end{array} \right\} \approx_s \left\{ (\mathbf{a}, \mathbf{e}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\$\; \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma,-q\mathbf{h}} : \mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n \end{array} \right\}$$

Restricting $\mathbf{e} \in \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma,-q\mathbf{h}}$ to satisfy $\mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n$ simply means restricting the support to the coset $\mathbf{P} + \mathbf{a}$. Thus, the distribution of $\mathbf{e}$ is equivalent to $\mathcal{D}_{\mathbf{P}+\mathbf{a},\sigma,-\mathbf{h}}$ or $\left(\mathbf{a} + \mathcal{D}_{\mathbf{P},\sigma,-\mathbf{a}-\mathbf{h}}\right)$. Substituting, we have:

$$\begin{aligned} \left\{ (\mathbf{a}, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{e} \leftarrow\!\$\; \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma,-q\mathbf{h}} : \mathbf{a} = \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{z} := \mathbf{a} - \mathbf{e} \end{array} \right\} &= \left\{ (\mathbf{a}, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{z} \leftarrow\!\$\; \mathbf{a} - (\mathcal{D}_{\mathbf{P},\sigma,-\mathbf{a}-\mathbf{h}} + \mathbf{a}) \end{array} \right\} \\ &= \left\{ (\mathbf{a}, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{z} \leftarrow\!\$\; \mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{h}} \end{array} \right\} \end{aligned}$$

Hence, we conclude that:

$$\left\{ (\mathbf{a}, 1, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{e} \leftarrow\!\$\; \frac{1}{q}\mathcal{D}_{\mathbf{P},q\sigma,-q\mathbf{h}} \\ \mathbf{a} := \mathbf{e} \bmod \mathbb{Z}^n \\ \mathbf{z} := \mathbf{a} - \mathbf{e} \end{array} \right\} \approx_s \left\{ (\mathbf{a}, 1, \mathbf{z}) \,\middle|\, \begin{array}{l} \mathbf{a} \leftarrow\!\$\; \mathbb{T}_q^n \\ \mathbf{z} \leftarrow\!\$\; \mathcal{D}_{\mathbf{P},\sigma,\mathbf{a}+\mathbf{h}} \end{array} \right\}$$

Thus, $\mathcal{S}_2$ is statistically indistinguishable from an execution $\mathcal{S}$ conditioned on the challenge $c = 1$.

Applying Theorem 2.26 with $V = \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v}\|_{\mathbf{P}} \leq \beta\}$, $s = \sigma$, $\mathbf{c} = \mathbf{a} + \mathbf{h}$, we have for $\mathbf{v} = \mathbf{x} - \mathbf{h} \in V$, there exists a polynomial $M = \mathsf{poly}(n)$ if $\sigma = \Theta\left(\beta\sqrt{\frac{1}{\ln n}}\right)$ or a constant $M = O(1)$ if $\sigma = \Theta\left(\beta\sqrt{\ln n}\right)$ such that for a fixed $\mathbf{a} \in \mathbb{T}_q^n$, the conditional distribution of $\mathbf{z}$ conditioned on $\mathbf{a}$ in $\mathcal{S}_1$ is within statistical distance of $\frac{2^{-\Theta(\ln n)}}{M}$ to the conditional distribution of $\mathbf{z}$ conditioned on $\mathbf{a}$ in $\mathcal{S}_2$. Therefore, $\mathcal{S}_1$ and $\mathcal{S}_2$ are statistically indistinguishable, so the simulator $\mathcal{S}$ outputs an accepting conversation $(\mathbf{a}, c, \mathbf{z})$ distributed statistically close to an honest execution of Σ^{CV} conditioned on challenge $c = 1$. □

5.2 ZKPoK for Quadratic Relations

To provide the exact $\mathbf{P}$-norm proof of $\mathbf{x} - \mathbf{h}$, we can disclose $\|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}} = B$ $(B \leq \beta)$ as a constraint on $\mathbf{x}$ prove that we know such $\mathbf{x}$. By definition, we have that:

$$\|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}}^2 = (\mathbf{x} - \mathbf{h})^{\mathsf{T}} \mathbf{P} (\mathbf{x} - \mathbf{h}) = B^2, \text{ or}$$
$$\|\mathbf{y}\|_{\mathbf{P}}^2 = q (\mathbf{x} - \mathbf{h})^{\mathsf{T}} \mathbf{P} (\mathbf{x} - \mathbf{h}) q = q^2 B^2$$

where $\mathbf{y} = q(\mathbf{x} - \mathbf{h})$ is an integral vector.

Knowing that the quadratic form $\mathbf{P}$ is a sample of $\mathcal{D}_{s,\mu}([\mathbf{S}])$ for some quadratic form $\mathbf{S}$, a positive $s \geq \max\left\{\lambda_n(\mathbf{S}), \|\mathbf{B}_{\mathbf{S}}^{\mathsf{GS}}\|\sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$ and a small positive μ, we assure that the minimum eigenvalue of $\mathbf{P}$, $\nu_{\min}(\mathbf{P}) \geq \mu$, so by Lemma 2.4, we have the ℓ_2-norms of $\mathbf{x}$ and $\mathbf{y}$ upper-bounded.

$$\begin{aligned}
\|\mathbf{y}\| &\leq \frac{1}{\sqrt{\mu}}\|q(\mathbf{x} - \mathbf{h})\|_{\mathbf{P}} \leq \frac{1}{\sqrt{\mu}} q\beta \\
\|\mathbf{x}\| &\leq \frac{1}{\sqrt{\mu}}\|\mathbf{x}\|_{\mathbf{P}} \\
&\leq \frac{1}{\sqrt{\mu}}(\beta + \|\mathbf{h}\|_{\mathbf{P}}) \leq \frac{1}{\sqrt{\mu}}(\beta + \|\mathbf{B_P h}\|) \leq \frac{1}{\sqrt{\mu}}\left(\beta + \frac{sn^2}{4}\right)
\end{aligned}$$

where the last inequality is because $\|\mathbf{B_P h}\| \leq \frac{n}{2}\|\mathbf{B_P}\|$ for $\mathbf{h} \in \mathbb{T}_q^n$, and $\|\mathbf{B_P}\| \leq \frac{sn}{2}$ due to Lemma 2.12 and Lemma 2.11.

Let $S = \max\left\{\frac{1}{\sqrt{\mu}}q\beta, \frac{1}{\sqrt{\mu}}\left(\beta + \frac{sn^2}{4}\right)\right\}$, then we can say $\mathbf{x}, \mathbf{y} \in [-S, S]^n$. For $\ell = \lceil \log_2(S+1) \rceil + 1$, we can decompose each element of $\mathbf{x}$ and $\mathbf{y}$ to ℓ bits. Let $\mathbf{w}_1, \mathbf{w}_2 \in \{0,1\}^{n\ell}$ be the binary decompositions of $\mathbf{x}$ and $\mathbf{y}$ respectively. We have that $\mathbf{x} = \mathbf{G}\mathbf{w}_1$ and $\mathbf{y} = \mathbf{G}\mathbf{w}_2$ where the gadget matrix $\mathbf{G} := \mathbf{I}_n \otimes \begin{pmatrix} 1 & 2 & 4 \ldots 2^{\ell-2} & -2^{\ell-1} \end{pmatrix}$. With $\mathbf{w} = \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \in \{0,1\}^{2n\ell}$ as the witness, we can rewrite the statements $\|\mathbf{y}\|_{\mathbf{P}}^2 = q^2 B^2$ and $\mathbf{y} = q(\mathbf{x} - \mathbf{h})$ as:

$$\mathbf{w}^{\mathsf{T}}\mathbf{D}\mathbf{w} = \mathbf{w}^{\mathsf{T}} \begin{pmatrix} \mathbf{0}^{n\ell \times n\ell} & \\ & \mathbf{G}^{\mathsf{T}}\mathbf{P}\mathbf{G} \end{pmatrix} \mathbf{w} = q^2 B^2$$
$$\mathbf{E}\mathbf{w} = \begin{pmatrix} q\mathbf{G} & -\mathbf{G} \end{pmatrix} \mathbf{w} = q\mathbf{h}$$

Additionally, to prove that $\mathbf{w}$ is binary, we have to prove that $\mathbf{w} \odot (\mathbf{w} - \mathbf{1}) = 0$ where $\odot$ denotes the element-wise product and $\mathbf{1}$ is a vector of all 1's. These three relations on $\mathbf{w}$ can be reduced to a set of quadratic equation of the form

$$\mathbf{w}^{\mathsf{T}}\mathbf{A}\mathbf{w} + \mathbf{b}^{\mathsf{T}}\mathbf{w} = d$$

The equation $\mathbf{w}^\top \mathbf{D}\mathbf{w} = q^2B^2$ is equivalent to $\mathbf{w}^\top \mathbf{D}\mathbf{w} + \mathbf{0}^\top \mathbf{w} = q^2B^2$ where $\mathbf{0}$ is a vector of 0's. The linear equations $\mathbf{E}\mathbf{w} = q\mathbf{h}$ is equivalent to n equations $\mathbf{w}^\top \mathbf{A}\mathbf{w} + \mathbf{e}_i^\top \mathbf{w} = qh_i$ where $\mathbf{A}$ is an $2n\ell$-by-$2n\ell$ matrix of 0's, $\mathbf{e}_i^\top$ is the i-th row vector of $\mathbf{E}$, and h_i is the i-th element of $\mathbf{h}$ for $i \in [n]$. Let $\mathbf{F}_i$ is an $2n\ell$-by-$2n\ell$ matrix of 0's except that the element at the i-th column and the i-th row is 1, and $\mathbf{f}_i$ is a vector of size $2n\ell$ such that it has all 0's except that the i-th element is 1. For $i \in [n]$, the product $\mathbf{w} \odot (\mathbf{w} - \mathbf{1}) = 0$ is equivalent to n quadratic equations $\mathbf{w}^\top \mathbf{F}_i \mathbf{w} - \mathbf{f}_i^\top \mathbf{w} = 0$. The three equations which $\mathbf{w}$ must satisfy are reduced to $2n+1$ quadratic equations $\mathbf{w}^\top \mathbf{A}_i \mathbf{w} + \mathbf{b}_i^\top \mathbf{w} = d_i$ for $i \in [2n+1]$.

We now construct a zero-knowledge proof for multiple quadratic relations over a vector $\mathbf{w}$. For the public parameters $\mathsf{pp}^* := (N, m, \mathbf{R}, \sigma, p, q_0, k, \rho_0, \sigma_1, \sigma_2, M)$ parametrised by λ, we define a new relation $R^*_{\mathsf{pp}^*}$

$$R^*_{\mathsf{pp}^*} = \left\{ (\mathsf{stmt}, \mathsf{wit}) \left| \begin{array}{l} \mathsf{stmt} := \{\mathbf{A}_i, \mathbf{b}_i, d_i\}_{i \in [N]} \\ \mathsf{wit} := \mathbf{w} \in \mathbb{Z}_p^m \\ \forall i \in [N], \mathbf{w}^\top \mathbf{A}_i \mathbf{w} + \mathbf{b}_i^\top \mathbf{w} = d_i \end{array} \right. \right\}$$

Our zero-knowledge proof for $R^*_{\mathsf{pp}^*}$ uses the commitment scheme described in Section 3.2. Among the public parameters, $\mathbf{R}$ is the commitment key which is assumed to be honestly generated by sampling from $\mathcal{D}_\sigma([\mathbf{Q}])$ for $\mathbf{Q}$ is a quadratic form with an efficient decoder for radius $\rho_0 \leq \lambda_1([\mathbf{Q}])/2$ and $\sigma \geq \max\left\{\lambda_m(\mathbf{Q}), \left\|\mathbf{B}_{\mathbf{Q}}^{\mathsf{GS}}\right\| \sqrt{\frac{\ln(2m+4)}{\pi}}\right\}$. We use the commitment scheme to commit the message space $\mathbb{Z}_p^m$.

To prove the knowledge of $\mathbf{w}$ satisfying a quadratic equation $\mathbf{w}^\top \mathbf{A}\mathbf{w} + \mathbf{b}^\top \mathbf{w} = d$, the prover chooses a mask $\bar{\mathbf{w}}$ and sends $\hat{\mathbf{w}} = \bar{\mathbf{w}} + c\mathbf{w}$ upon a challenge c. We observe that:

$$\begin{aligned} \hat{\mathbf{w}}^\top \mathbf{A}\hat{\mathbf{w}} + c\mathbf{b}^\top \hat{\mathbf{w}} &= \bar{\mathbf{w}}^\top \mathbf{A}\bar{\mathbf{w}} + \left(2\bar{\mathbf{w}}^\top \mathbf{A}\mathbf{w} + \mathbf{b}^\top \bar{\mathbf{w}}\right) c + \left(\mathbf{w}^\top \mathbf{A}\mathbf{w} + \mathbf{b}^\top \mathbf{w}\right) c^2 \\ &= \alpha + c\gamma + c^2 d \end{aligned}$$

where $\alpha = \bar{\mathbf{w}}^\top \mathbf{A}\bar{\mathbf{w}}$ and $\gamma = 2\bar{\mathbf{w}}^\top \mathbf{A}\mathbf{w} + \mathbf{b}^\top \bar{\mathbf{w}}$. Therefore, the prover sends to the verifier two commitments $\mathsf{Commit}(\mathbf{w}, \mathbf{r})$ and $\mathsf{Commit}(\bar{\mathbf{w}}, \bar{\mathbf{r}})$ and two terms α, γ in the clear. Upon a challenge c, the prover sends a masked opening $\hat{\mathbf{w}} = \bar{\mathbf{w}} + c\mathbf{w}$ and $\hat{\mathbf{r}} = \bar{\mathbf{r}} + c\mathbf{r}$. It is required that $\hat{\mathbf{r}}$ remains short for the binding of the commitments, so we choose the challenge set $[-g, g]$ for g is a small element of $\mathbb{Z}_p$. For the commitment scheme is additively homomorphic, the verifier can check whether $\mathsf{Commit}(\hat{\mathbf{w}}, \hat{\mathbf{r}}) = \mathsf{Commit}(\bar{\mathbf{w}}, \bar{\mathbf{r}}) + c \cdot \mathsf{Commit}(\mathbf{w}, \mathbf{r})$. Finally, it verifies if

$$\hat{\mathbf{w}}^\top \mathbf{A}\hat{\mathbf{w}} + c\mathbf{b}^\top \hat{\mathbf{w}} = \alpha + c\gamma + c^2 d$$

In the case of proving N quadratic relations altogether, instead of proving each relation simultaneously, we linearly combine all N quadratic relations into one and prove that relation using the technique described above. Specifically, suppose that we want to prove that we know $\mathbf{w}$ satisfying

$$\forall i \in [N], \mathbf{w}^\top \mathbf{A}_i \mathbf{w} + \mathbf{b}_i^\top \mathbf{w} = d_i$$

In the first step, the prover sends two commitments of the witness $\mathbf{w}$ and the random mask $\hat{\mathbf{w}}$. Secondly, the verifier then chooses and a set of N challenges $c_1, \ldots, c_N \in \mathbb{Z}_p$. Both the prover and verifier can now agree on one combined quadratic relation

$$\mathbf{w}^\mathsf{T}\mathbf{A}\mathbf{w} + \mathbf{b}^\mathsf{T}\mathbf{w} = d$$

where

$$\mathbf{A} = \sum_{i=1}^{n} c_i \mathbf{A}_i, \mathbf{b} = \sum_{i=1}^{n} c_i \mathbf{b}_i, \text{ and } d = \sum_{i=1}^{n} c_i d_i$$

Afterwards, the protocol follows as in the case of proving one quadratic relation. Given the linearly-combined quadratic relation satisfies, the probability that one of N quadratic relations does not satisfy is $1/p$. So far, our proof can prove the relation $\mathbf{w}^\mathsf{T}\mathbf{A}\mathbf{w} + \mathbf{b}^\mathsf{T}\mathbf{w} = d \bmod p$, so to convince the verifier, we need p to be sufficiently large such that there is no "wraparound" in all N quadratic relations, $p \geq 2(q^2\beta^2 + 2^\ell qn\ell)$.

We describe the zero-knowledge proof protocol Π^* for the relation $R^*_{\mathsf{pp}^*}$ in Fig. 14.

Theorem 5.4. *For $\sigma_1 = \sigma\sqrt{m}\sqrt{\frac{\ln(2m+4)}{\pi}}$, $\sigma_2 = \Theta\left(g\sigma_1\sqrt{m \ln m}\right)$, $k = \Omega\left(g^2\sqrt{m \ln m}\right)$, $q_0 = \frac{k\sigma m}{\rho_0}\sqrt{\frac{\ln(2m+4)}{\pi}}$, $M = O(1)$, a prime p, and that the assumption $\mathsf{ac}\text{-}\Delta\mathsf{LIP}^{\mathbf{Q},\mathbf{Q}'}_{\sigma}$ is hard for two quadratic forms $\mathbf{Q}$ and $\mathbf{Q}'$ such that $\mathbf{Q}$ has an efficient decoding algorithm for distance $\rho_0 < \lambda_1([\mathbf{Q}])/2$, and $\sigma_1/q_0 \geq p\eta_{2^{-\Theta(m)}}([\mathbf{Q}'])$ for $\sigma_1/q_0 = \rho/k\sqrt{n}$, the protocol Π^* is complete, $(2,3)$-special-sound and SHVZK for the relation $R^*_{\mathsf{pp}^*}$.*

Proof. **Completeness**. Because $\mathbf{R} \leftarrow\$ \mathcal{D}_\sigma([\mathbf{Q}])$, we have by Lemma 2.15 that $\sigma\sqrt{m} \geq \left\|\mathbf{B}^{\mathsf{GS}}_{\mathbf{R}}\right\|$ with overwhelming probability. Consequently, we have $\sigma_1 = \sigma\sqrt{m}\sqrt{\frac{\ln(2m+4)}{\pi}} \geq \left\|\mathbf{B}^{\mathsf{GS}}_{\mathbf{R}}\right\|\sqrt{\frac{\ln(2m+4)}{\pi}}$ except with negligible probability, and $\sigma_2 > \sigma_1$, so it is efficient to sample $\mathbf{r} \leftarrow\$ \frac{1}{q_0}\mathcal{D}_{\mathbf{R},\sigma_1}$ and $\bar{\mathbf{r}} \leftarrow\$ \frac{1}{q_0}\mathcal{D}_{\mathbf{R},\sigma_2}$. By Lemma 2.11, we have that

$$\begin{aligned}
\|\hat{\mathbf{r}}\|_{\mathbf{R}} &\leq \|\bar{\mathbf{r}}\|_{\mathbf{R}} + \|c\mathbf{r}\|_{\mathbf{R}} \\
&\leq \frac{1}{q_0}\sigma_2\sqrt{m} + \frac{g}{q_0}\sigma_1\sqrt{m} \\
&\leq \frac{1}{q_0}\left(\sigma_2 + g\sigma_1\right)\sqrt{m}
\end{aligned}$$

By the additive homomorphism of the commitment scheme,

$$\begin{aligned}
\bar{\mathbf{d}}_1 + c\mathbf{d}_1 &= \bar{\mathbf{r}} + c\mathbf{r} \bmod \mathbb{Z}^m \\
&= \hat{\mathbf{r}} \bmod \mathbb{Z}^m, \text{ and} \\
\hat{\mathbf{u}} &= \bar{\mathbf{d}}_1 + c\mathbf{d}_1 - \hat{\mathbf{r}} \\
&= \bar{\mathbf{d}}_1 - \bar{\mathbf{r}} + c\left(\mathbf{d}_1 - \mathbf{r}\right) \\
&= \bar{\mathbf{u}} + c\mathbf{u}, \text{ and} \\
\bar{\mathbf{d}}_2 + c\mathbf{d}_2 &= \bar{\mathbf{u}} + \bar{\mathbf{w}} + c\left(\mathbf{u} + \mathbf{w}\right) \bmod p \\
&= \hat{\mathbf{u}} + \hat{\mathbf{w}} \bmod p
\end{aligned}$$

Protocol Π^*

$$
\begin{array}{lcl}
\underline{\mathcal{P}\left(\{\mathbf{A}_i,\mathbf{b}_i,d_i\}_{i\in[N]},\mathbf{w}\right)} & & \underline{\mathcal{V}\left(\{\mathbf{A}_i,\mathbf{b}_i,d_i\}_{i\in[N]}\right)} \\
\bar{\mathbf{w}} \leftarrow\!\!\$\; \mathbb{Z}_p^m & & \\
\mathbf{r} \leftarrow\!\!\$\; \frac{1}{q_0}\mathcal{D}_{\mathbf{R},\sigma_1}, \bar{\mathbf{r}} \leftarrow\!\!\$\; \frac{1}{q_0}\mathcal{D}_{\mathbf{R},\sigma_2} & & \\
\mathbf{d}_1 := \mathbf{r} \bmod \mathbb{Z}^m, \bar{\mathbf{d}}_1 := \bar{\mathbf{r}} \bmod \mathbb{Z}^m & & \\
\mathbf{u} := \mathbf{d}_1 - \mathbf{r} \in \mathbb{Z}^m, \bar{\mathbf{u}} := \bar{\mathbf{d}}_1 - \bar{\mathbf{r}} \in \mathbb{Z}^m & & \\
\mathbf{d}_2 := \mathbf{u} + \mathbf{w} \bmod p, \bar{\mathbf{d}}_2 := \bar{\mathbf{u}} + \bar{\mathbf{w}} \bmod p & & \\
& \xrightarrow{\mathbf{d}_1,\mathbf{d}_2,\bar{\mathbf{d}}_1,\bar{\mathbf{d}}_2} & \\
& & c_1,\ldots,c_N \leftarrow\!\!\$\; \mathbb{Z}_p \\
& \xleftarrow{c_1,\ldots,c_N} & \\
\alpha := \sum_{i=1}^N c_i\left(\bar{\mathbf{w}}^\top\mathbf{A}_i\bar{\mathbf{w}}\right) \bmod p & & \mathbf{A} := \sum_{i=1}^N c_i\mathbf{A}_i, \mathbf{b} := \sum_{i=1}^N c_i\mathbf{b}_i \\
\gamma := \sum_{i=1}^N c_i\left(2\bar{\mathbf{w}}^\top\mathbf{A}_i\mathbf{w} + \mathbf{b}_i^\top\bar{\mathbf{w}}\right) \bmod p & & d := \sum_{i=1}^N c_i d_i \\
& \xrightarrow{\alpha,\gamma} & \\
& & c \leftarrow\!\!\$\; [-g,g] \\
& \xleftarrow{c} & \\
\hat{\mathbf{w}} := \bar{\mathbf{w}} + c\mathbf{w} \bmod p & & \\
\hat{\mathbf{r}} := \bar{\mathbf{r}} + c\mathbf{r} & & \\
\text{Abort with probability} & & \\
\quad 1 - \min\left\{1, \frac{\mathcal{D}_{\mathbf{R},\sigma_2}(q_0\cdot\hat{\mathbf{r}})}{M\mathcal{D}_{\mathbf{R},\sigma_2,q_0\cdot c\cdot\mathbf{r}}(q_0\cdot\hat{\mathbf{r}})}\right\} & & \\
& \xrightarrow{\hat{\mathbf{w}},\hat{\mathbf{r}}} & \\
& & \hat{\mathbf{u}} := \bar{\mathbf{d}}_1 + c\mathbf{d}_1 - \hat{\mathbf{r}} \\
& & \text{Accept iff:} \\
& & \quad \|\hat{\mathbf{r}}\|_{\mathbf{R}} \le (\sigma_2 + g\sigma_1)\sqrt{m}/q_0, \\
& & \quad \hat{\mathbf{r}} = \bar{\mathbf{d}}_1 + c\mathbf{d}_1 \bmod \mathbb{Z}^m, \\
& & \quad \hat{\mathbf{u}} + \hat{\mathbf{w}} = \bar{\mathbf{d}}_2 + c\mathbf{d}_2 \bmod p, \text{ and} \\
& & \quad \hat{\mathbf{w}}^\top\mathbf{A}\hat{\mathbf{w}} + c\mathbf{b}^\top\hat{\mathbf{w}} \\
& & \qquad = \alpha + c\gamma + c^2 d \bmod p
\end{array}
$$

Figure 14: Protocol Π^* for proving many quadratic relations $R^*_{\mathsf{pp}^*}$

If $\mathbf{w}$ satisfies N quadratic equations $\mathbf{w}^\top \mathbf{A}_i \mathbf{w} + \mathbf{b}_i^\top \mathbf{w} = d_i$, then it satisfies the linearly-combined quadratic equation $\mathbf{w}^\top \mathbf{A} \mathbf{w} + \mathbf{b}^\top \mathbf{w} = d$ where $\mathbf{A} = \sum_{i=1}^N c_i \mathbf{A}_i$, $\mathbf{b} = \sum_{i=1}^N c_i \mathbf{b}_i$ and $d = \sum_{i=1}^N c_i d_i$. Therefore, it follows that

$$\hat{\mathbf{w}}^\top \mathbf{A} \hat{\mathbf{w}} + c\mathbf{b}^\top \hat{\mathbf{w}} = \alpha + c\gamma + c^2 d$$

where $\alpha = \sum_{i=1}^N c_i \left(\bar{\mathbf{w}}^\top \mathbf{A}_i \bar{\mathbf{w}}\right)$ and $\gamma = \sum_{i=1}^N c_i \left(2\bar{\mathbf{w}}^\top \mathbf{A}_i \mathbf{w} + \mathbf{b}_i^\top \bar{\mathbf{w}}\right)$.

SHVZK. Upon $\{\mathbf{A}_i, \mathbf{b}_i, d_i\}_{i\in[N]}$, $c \in [-g, g]$, and $(c_1, \ldots, c_N) \in \mathbb{Z}_p$, let $\mathcal{S}$ be a simulator described in Fig. 15.

$\mathcal{S}\left(\{\mathbf{A}_i, \mathbf{b}_i, d_i\}_{i\in[N]}, c, (c_1, \ldots, c_N)\right)$
$\mathbf{A} := \sum_{i=1}^N c_i \mathbf{A}_i, \mathbf{b} := \sum_{i=1}^N c_i \mathbf{b}_i, d := \sum_{i=1}^N c_i d_i$
$\hat{\mathbf{w}} \leftarrow\$ \mathbb{Z}_p^m, \hat{\mathbf{r}} \leftarrow\$ \frac{1}{q_0}\mathcal{D}_{\mathbf{R},\sigma_2}$
$\mathbf{d}_1 \leftarrow\$ \mathbb{T}_{q_0}^m$
$\bar{\mathbf{d}}_1 := \hat{\mathbf{r}} - c\mathbf{d}_1 \bmod \mathbb{Z}^m$
$\hat{\mathbf{u}} := \bar{\mathbf{d}}_1 + c\mathbf{d}_1 - \hat{\mathbf{r}}$
$\mathbf{d}_2 \leftarrow\$ \mathbb{Z}_p^m$
$\bar{\mathbf{d}}_2 := \hat{\mathbf{u}} + \hat{\mathbf{w}} - c\mathbf{d}_2 \bmod p$
$\gamma \leftarrow\$ \mathbb{Z}_p$
$\alpha := \hat{\mathbf{w}}^\top \mathbf{A} \hat{\mathbf{w}} + c\mathbf{b}^\top \hat{\mathbf{w}} - c^2 d - c\gamma \bmod p$
return $\left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, c, (c_1, \ldots, c_N), \hat{\mathbf{w}}, \hat{\mathbf{r}}, \alpha, \gamma\right)$ with probability $1/M$

Figure 15: The simulator of Π^*

By construction, the output of $\mathcal{S}$ is accepted by the verifier due to

$$\|\hat{\mathbf{r}}\|_{\mathbf{R}} \leq \frac{1}{q_0}\sigma_2\sqrt{m} < \frac{1}{q_0}(\sigma_2 + g\sigma_1)\sqrt{m}, \text{ and}$$

$$\bar{\mathbf{d}}_1 + c\mathbf{d}_1 = \hat{\mathbf{r}} \bmod \mathbb{Z}^m, \text{ and}$$

$$\bar{\mathbf{d}}_2 + c\mathbf{d}_2 = \hat{\mathbf{u}} + \hat{\mathbf{w}} \bmod p, \text{ where } \hat{\mathbf{u}} = \bar{\mathbf{d}}_1 + c\mathbf{d}_1 - \hat{\mathbf{r}}, \text{ and}$$

$$\hat{\mathbf{w}}^\top \mathbf{A} \hat{\mathbf{w}} + c\mathbf{b}^\top \hat{\mathbf{w}} = \alpha + c\gamma + c^2 d$$

Next, we show that the output of $\mathcal{S}$ is computationally indistinguishable from the output of an honest prover when interacting with an honest verifier conditioned on the verifier's challenge c and $(c_1, \ldots, c_N)$ via the following games.

- Game_0: Same as an honest prover.
- Game_1: Same as Game_0 except that $\bar{\mathbf{d}}_1 := \hat{\mathbf{r}} - c\mathbf{d}_1 \bmod \mathbb{Z}^m$, $\hat{\mathbf{u}} := \bar{\mathbf{d}}_1 + c\mathbf{d}_1 - \hat{\mathbf{r}}$, $\bar{\mathbf{d}}_2 := \hat{\mathbf{u}} + \hat{\mathbf{w}} - c\mathbf{d}_2 \bmod p$, $\alpha := \hat{\mathbf{w}}^{\mathsf{T}}\mathbf{A}\hat{\mathbf{w}} + c\mathbf{b}^{\mathsf{T}}\hat{\mathbf{w}} - c^2 d - c\gamma \bmod p$.
- Game_2: Same as Game_1 except that $\hat{\mathbf{r}} \leftarrow\$ \frac{1}{q_0}\mathcal{D}_{\mathbf{R},\sigma_2}$ and abort with probability $1 - 1/M$.
- Game_3: Same as Game_2 except that $\mathbf{d}_1 \leftarrow\$ \mathbb{T}_{q_0}^m$ and $\mathbf{d}_2 \leftarrow\$ \mathbb{Z}_p^m$.
- Game_4: Same as Game_3 except that $\gamma \leftarrow\$ \mathbb{Z}_p$.
- Game_5: Same as Game_4 except that $\hat{\mathbf{w}} \leftarrow\$ \mathbb{Z}_p^m$.

Game_0 and Game_1 are identical as shown in the completeness proof. Game_1 and Game_2 is statistically indistinguishable due to the rejection sampling on $\hat{\mathbf{r}}$ according to Theorem 3.8 (for the quadratic form $\mathbf{R}$, $\sigma_2 = \Theta\left(g\sigma_1\sqrt{m \ln m}\right)$, and $M = O(1)$). Since the commitment scheme is computationally hiding due to the hardness of $\mathsf{ac}\text{-}\Delta\mathsf{LIP}_{\sigma}^{\mathbf{Q},\mathbf{Q}'}$, we have $\mathbf{d}_1$ and $\mathbf{d}_2$ in Game_2 are computationally indistinguishable from uniformly random $\mathbf{d}_1 \leftarrow\$ \mathbb{T}_{q_0}^m$ and $\mathbf{d}_2 \leftarrow\$ \mathbb{Z}_p^m$ (refer to the proof to Theorem 3.2). Thus, Game_2 and Game_3 are computationally indistinguishable. For $\bar{\mathbf{w}}$ is uniformly random, γ in Game_3 is uniformly random, so Game_3 and Game_4 are statistically indistinguishable. In Game_4, only $\hat{\mathbf{w}}$ is calculated using the witness $\mathbf{w}$. Because the mask $\bar{\mathbf{w}}$ is uniformly random, $\hat{\mathbf{w}}$ is also uniformly random, so Game_4 and Game_5 are statistically indistinguishable. We have Game_5 to be identical to $\mathcal{S}$, so the output of $\mathcal{S}$ is computationally indistinguishable from the output of the honest prover conditioned on an honest verifier output c and $(c_1, \ldots, c_N)$.

$(2,3)$**-Special Soundness**. Suppose by rewinding, we find three accepting transcripts with the same $\left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, \alpha, \gamma\right)$ and $(c_1, \ldots, c_N)$.

$$\begin{cases} \left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, c_1, \ldots, c_N, \alpha, \gamma, c^{(1)}, \hat{\mathbf{w}}^{(1)}, \hat{\mathbf{r}}^{(1)}\right) \\ \left\|\hat{\mathbf{r}}^{(1)}\right\|_{\mathbf{R}} \leq \dfrac{1}{q_0}\left(\sigma_2 + g\sigma_1\right)\sqrt{m} \\ \hat{\mathbf{r}}^{(1)} = \bar{\mathbf{d}}_1 + c^{(1)}\mathbf{d}_1 \bmod \mathbb{Z}^m \\ \left(\bar{\mathbf{d}}_1 + c^{(1)}\mathbf{d}_1 - \hat{\mathbf{r}}^{(1)}\right) + \hat{\mathbf{w}}^{(1)} = \bar{\mathbf{d}}_2 + c^{(1)}\mathbf{d}_2 \bmod p \\ \hat{\mathbf{w}}^{(1)^{\mathsf{T}}}\mathbf{A}\hat{\mathbf{w}}^{(1)} + c^{(1)}\mathbf{b}^{\mathsf{T}}\hat{\mathbf{w}}^{(1)} = \alpha + c^{(1)}\gamma + c^{(1)^2}d \end{cases}$$

$$\begin{cases} \left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, c_1, \ldots, c_N, \alpha, \gamma, c^{(2)}, \hat{\mathbf{w}}^{(2)}, \hat{\mathbf{r}}^{(2)}\right) \\ \left\|\hat{\mathbf{r}}^{(2)}\right\|_{\mathbf{R}} \leq \dfrac{1}{q_0}\left(\sigma_2 + g\sigma_1\right)\sqrt{m} \\ \hat{\mathbf{r}}^{(2)} = \bar{\mathbf{d}}_1 + c^{(2)}\mathbf{d}_1 \bmod \mathbb{Z}^m \\ \left(\bar{\mathbf{d}}_1 + c^{(2)}\mathbf{d}_1 - \hat{\mathbf{r}}^{(2)}\right) + \hat{\mathbf{w}}^{(2)} = \bar{\mathbf{d}}_2 + c^{(2)}\mathbf{d}_2 \bmod p \\ \hat{\mathbf{w}}^{(2)^{\mathsf{T}}}\mathbf{A}\hat{\mathbf{w}}^{(2)} + c^{(2)}\mathbf{b}^{\mathsf{T}}\hat{\mathbf{w}}^{(2)} = \alpha + c^{(2)}\gamma + c^{(2)^2}d \end{cases}$$

$$\begin{cases} \left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, c_1, \ldots, c_N, \alpha, \gamma, c^{(3)}, \hat{\mathbf{w}}^{(3)}, \hat{\mathbf{r}}^{(3)}\right) \\ \left\|\hat{\mathbf{r}}^{(3)}\right\|_{\mathbf{R}} \leq \frac{1}{q_0} \left(\sigma_2 + g\sigma_1\right) \sqrt{m} \\ \hat{\mathbf{r}}^{(3)} = \bar{\mathbf{d}}_1 + c^{(3)}\mathbf{d}_1 \bmod \mathbb{Z}^m \\ \left(\bar{\mathbf{d}}_1 + c^{(3)}\mathbf{d}_1 - \hat{\mathbf{r}}^{(3)}\right) + \hat{\mathbf{w}}^{(3)} = \bar{\mathbf{d}}_2 + c^{(3)}\mathbf{d}_2 \bmod p \\ \hat{\mathbf{w}}^{(3)^{\mathsf{T}}} \mathbf{A} \hat{\mathbf{w}}^{(3)} + c^{(3)} \mathbf{b}^{\mathsf{T}} \hat{\mathbf{w}}^{(3)} = \alpha + c^{(3)}\gamma + {c^{(3)}}^2 d \end{cases}$$

where $\mathbf{A} = \sum_{i=1}^{N} c_i \mathbf{A}_i$, $\mathbf{b} = \sum_{i=1}^{N} c_i \mathbf{b}_i$, and $d = \sum_{i=1}^{N} c_i d_i$

Let $f_1 = c^{(2)} - c^{(1)}$, $f_2 = c^{(3)} - c^{(1)}$. For p is prime and $f_1, f_2 \neq 0$, f_1 and f_2 are invertible in $\mathbb{Z}_p$. We now prove that we can extract $\mathbf{w}^* := f_1^{-1} \left(\hat{\mathbf{w}}^{(2)} - \hat{\mathbf{w}}^{(1)}\right)$ satisfying the linearly-combined quadratic relation specified by $(c_1, \ldots, c_N)$. Let $\mathbf{r}_1^* := \hat{\mathbf{r}}^{(2)} - \hat{\mathbf{r}}^{(1)}$ and $\mathbf{r}_2^* := \hat{\mathbf{r}}^{(3)} - \hat{\mathbf{r}}^{(1)}$. We have, by subtracting, that:

$$f_2 \mathbf{r}_1^* = f_2 \left(c^{(2)} - c^{(1)}\right) \mathbf{d}_1 = f_1 f_2 \mathbf{d}_1 \bmod \mathbb{Z}^m, \text{ and}$$
$$f_1 \mathbf{r}_2^* = f_1 \left(c^{(3)} - c^{(1)}\right) \mathbf{d}_1 = f_1 f_2 \mathbf{d}_1 \bmod \mathbb{Z}^m$$

Hence, we get $\left(f_2 \mathbf{r}_1^* - f_1 \mathbf{r}_2^*\right) \in \mathbb{Z}^m$ such that

$$\left\|f_2 \mathbf{r}_1^* - f_1 \mathbf{r}_2^*\right\|_{\mathbf{R}} \leq \frac{4g}{q_0} \left(\sigma_2 + g\sigma_1\right) \sqrt{m}$$

Due to $\sigma_2 = \Theta\left(g\sigma_1 \sqrt{m \ln m}\right)$, $\sigma_1 = \sigma\sqrt{m}\sqrt{\frac{\ln(2m+4)}{\pi}}$, $k = \Omega\left(g^2 \sqrt{m \ln m}\right)$ and $q_0 = \frac{k\sigma m}{\rho_0}\sqrt{\frac{\ln(2m+4)}{\pi}}$, it implies that:

$$\begin{aligned} \left\|f_2 \mathbf{r}_1^* - f_1 \mathbf{r}_2^*\right\|_{\mathbf{R}} &\leq \frac{\Theta\left(g^2 \rho_0 \sqrt{m \ln m}\right)}{\Omega\left(g^2 \sqrt{m \ln m}\right)} \\ &\leq \rho_0 \\ &\leq \lambda_1\left([\mathbf{Q}]\right)/2 = \lambda_1\left([\mathbf{R}]\right)/2 \end{aligned}$$

For it is impossible that $\left(f_2 \mathbf{r}_1^* - f_1 \mathbf{r}_2^*\right) \in \mathbb{Z}^m$ is non-zero and shorter than the shortest vector in $\mathbf{R}$, $\left(f_2 \mathbf{r}_1^* - f_1 \mathbf{r}_2^*\right) = \mathbf{0}^m$.

Similarly, by subtracting, we have that:

$$\left(f_1 \mathbf{d}_1 - \mathbf{r}_1^*\right) + \left(\hat{\mathbf{w}}^{(2)} - \hat{\mathbf{w}}^{(1)}\right) = f_1 \mathbf{d}_2 \bmod p$$
$$\left(f_2 \mathbf{d}_1 - \mathbf{r}_2^*\right) + \left(\hat{\mathbf{w}}^{(3)} - \hat{\mathbf{w}}^{(1)}\right) = f_2 \mathbf{d}_2 \bmod p$$

Multiplying the former by f_2 and the latter by f_1,

$$\left(f_1 f_2 \mathbf{d}_1 - f_2 \mathbf{r}_1^*\right) + f_2 \left(\hat{\mathbf{w}}^{(2)} - \hat{\mathbf{w}}^{(1)}\right) = f_1 f_2 \mathbf{d}_2 \bmod p$$
$$\left(f_1 f_2 \mathbf{d}_1 - f_1 \mathbf{r}_2^*\right) + f_1 \left(\hat{\mathbf{w}}^{(3)} - \hat{\mathbf{w}}^{(1)}\right) = f_1 f_2 \mathbf{d}_2 \bmod p$$

Subtracting one from another, it implies that

$$\left(f_2\mathbf{r}_1^* - f_1\mathbf{r}_2^*\right) + f_1\left(\hat{\mathbf{w}}^{(3)} - \hat{\mathbf{w}}^{(1)}\right) - f_2\left(\hat{\mathbf{w}}^{(2)} - \hat{\mathbf{w}}^{(1)}\right) = \mathbf{0}^m \bmod p$$

For $\left(f_2\mathbf{r}_1^* - f_1\mathbf{r}_2^*\right) = \mathbf{0}^m$, $f_1\left(\hat{\mathbf{w}}^{(3)} - \hat{\mathbf{w}}^{(1)}\right) = f_2\left(\hat{\mathbf{w}}^{(2)} - \hat{\mathbf{w}}^{(1)}\right)$, or

$$\mathbf{w}^* = f_2^{-1}\left(\hat{\mathbf{w}}^{(3)} - \hat{\mathbf{w}}^{(1)}\right) \bmod p$$

Next, by subtracting the quadratic equations, we have

$$\hat{\mathbf{w}}^{(2)^\top}\mathbf{A}\hat{\mathbf{w}}^{(2)} - \hat{\mathbf{w}}^{(1)^\top}\mathbf{A}\hat{\mathbf{w}}^{(1)} + c^{(2)}\mathbf{b}^\top\hat{\mathbf{w}}^{(2)} - c^{(1)}\mathbf{b}^\top\hat{\mathbf{w}}^{(1)} = f_1\gamma + \left(c^{(2)^2} - c^{(1)^2}\right)d$$
$$\hat{\mathbf{w}}^{(3)^\top}\mathbf{A}\hat{\mathbf{w}}^{(3)} - \hat{\mathbf{w}}^{(1)^\top}\mathbf{A}\hat{\mathbf{w}}^{(1)} + c^{(3)}\mathbf{b}^\top\hat{\mathbf{w}}^{(3)} - c^{(1)}\mathbf{b}^\top\hat{\mathbf{w}}^{(1)} = f_2\gamma + \left(c^{(3)^2} - c^{(1)^2}\right)d$$

Substituting $\hat{\mathbf{w}}^{(2)} = f_1\mathbf{w}^* + \hat{\mathbf{w}}^{(1)}$ and $\hat{\mathbf{w}}^{(3)} = f_2\mathbf{w}^* + \hat{\mathbf{w}}^{(1)}$,

$$f_1\mathbf{w}^{*\top}\mathbf{A}\mathbf{w}^* + c^{(2)}\mathbf{b}^\top\mathbf{w}^* - c^{(2)}d = \gamma + c^{(1)}d - 2\mathbf{w}^{*\top}\mathbf{A}\hat{\mathbf{w}}^{(1)} - \mathbf{b}^\top\hat{\mathbf{w}}^{(1)}$$
$$f_2\mathbf{w}^{*\top}\mathbf{A}\mathbf{w}^* + c^{(3)}\mathbf{b}^\top\mathbf{w}^* - c^{(3)}d = \gamma + c^{(1)}d - 2\mathbf{w}^{*\top}\mathbf{A}\hat{\mathbf{w}}^{(1)} - \mathbf{b}^\top\hat{\mathbf{w}}^{(1)}$$

Then, we get

$$\left(c^{(3)} - c^{(2)}\right)\left(\mathbf{w}^{*\top}\mathbf{A}\mathbf{w}^* + \mathbf{b}^\top\mathbf{w}^* - d\right) = 0$$

For $c^{(3)} \neq c^{(2)}$ and $\left|c^{(3)} - c^{(2)}\right| \leq 2g < p$, we have $\mathbf{w}^*$ satisfying $\mathbf{w}^{*\top}\mathbf{A}\mathbf{w}^* + \mathbf{b}^\top\mathbf{w}^* = d$. Additionally, we also have $\left(\mathbf{r}_1^*, \mathbf{w}^*, f_1\right)$ to be a valid opening to the commitment $(\mathbf{d}_1, \mathbf{d}_2)$ because

$$\mathbf{r}_1^* = \hat{\mathbf{r}}^{(2)} - \hat{\mathbf{r}}^{(1)} = f_1\mathbf{d}_1 \bmod \mathbb{Z}^m,$$
$$\left\|\mathbf{r}_1^*\right\|_{\mathbf{R}} \leq \frac{2}{q_0}\left(\sigma_2 + g\sigma_1\right)\sqrt{m} \leq \rho_0, \text{ and}$$
$$\left(f_1\mathbf{d}_1 - \mathbf{r}_1^*\right) + f_1\mathbf{w}^* = f_1\mathbf{d}_2 \bmod p$$

Similarly, suppose by rewinding, we have another three accepting transcripts

$$\left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, \tilde{c}_1, \ldots, \tilde{c}_N, \tilde{\alpha}, \tilde{\gamma}, c^{(4)}, \hat{\mathbf{w}}^{(4)}, \hat{\mathbf{r}}^{(4)}\right)$$
$$\left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, \tilde{c}_1, \ldots, \tilde{c}_N, \tilde{\alpha}, \tilde{\gamma}, c^{(5)}, \hat{\mathbf{w}}^{(5)}, \hat{\mathbf{r}}^{(5)}\right)$$
$$\left(\mathbf{d}_1, \mathbf{d}_2, \bar{\mathbf{d}}_1, \bar{\mathbf{d}}_2, \tilde{c}_1, \ldots, \tilde{c}_N, \tilde{\alpha}, \tilde{\gamma}, c^{(6)}, \hat{\mathbf{w}}^{(6)}, \hat{\mathbf{r}}^{(6)}\right)$$

where $(c_1, \ldots, c_N) \neq (\tilde{c}_1, \ldots, \tilde{c}_N)$ and $(\alpha, \gamma) \neq (\tilde{\alpha}, \tilde{\gamma})$.

By the same set of arguments, we can extract $\tilde{\mathbf{w}}^* := \tilde{f}_1^{-1}\left(\hat{\mathbf{w}}^{(5)} - \hat{\mathbf{w}}^{(4)}\right)$, $\tilde{\mathbf{r}}_1^* := \hat{\mathbf{r}}^{(5)} - \hat{\mathbf{r}}^{(4)}$ where $\tilde{f}_1 := c^{(5)} - c^{(4)}$ such that $\left(\tilde{\mathbf{r}}_1^*, \tilde{\mathbf{w}}^*, \tilde{f}_1\right)$ is a valid opening to the commitment $(\mathbf{d}_1, \mathbf{d}_2)$ and $\tilde{\mathbf{w}}^*$ satisfies $\tilde{\mathbf{w}}^{*\mathsf{T}}\tilde{\mathbf{A}}\tilde{\mathbf{w}}^* + \tilde{\mathbf{b}}^{\mathsf{T}}\tilde{\mathbf{w}}^* = \tilde{d}$ where $\tilde{\mathbf{A}} = \sum_{i=1}^{N} \tilde{c}_i \mathbf{A}_i$, $\tilde{\mathbf{b}} = \sum_{i=1}^{N} \tilde{c}_i \mathbf{b}_i$, and $\tilde{d} = \sum_{i=1}^{N} \tilde{c}_i d_i$.

By the binding property of the commitment $(\mathbf{d}_1, \mathbf{d}_2)$, it must be the case that $\tilde{\mathbf{w}}^* = \mathbf{w}^*$. So far, we can extract $\mathbf{w}^*$ which satisfies

$$\sum_{i}^{N} c_i \left(\mathbf{w}^{*\mathsf{T}}\mathbf{A}_i\mathbf{w}^* + \mathbf{b}_i^{\mathsf{T}}\mathbf{w}^* - d_i\right) = 0 \bmod p, \text{ and}$$
$$\sum_{i}^{N} \tilde{c}_i \left(\mathbf{w}^{*\mathsf{T}}\mathbf{A}_i\mathbf{w}^* + \mathbf{b}_i^{\mathsf{T}}\mathbf{w}^* - d_i\right) = 0 \bmod p$$

There are two cases on $\mathbf{w}^*$:

1. $\forall i \in [N]$, $\mathbf{w}^{*\mathsf{T}}\mathbf{A}_i\mathbf{w}^* + \mathbf{b}_i^{\mathsf{T}}\mathbf{w}^* = d_i$

2. $\exists i \in [N]$, $\mathbf{w}^{*\mathsf{T}}\mathbf{A}_i\mathbf{w}^* + \mathbf{b}_i^{\mathsf{T}}\mathbf{w}^* \neq d_i$

The probability that at least one of quadratic equations does not satisfy while the linearly-combined quadratic equation satisfies is at most $1/p$ which is negligible. Therefore, $\mathbf{w}^*$ is a valid witness of $R^*_{\mathsf{pp}^*}$. □

5.3 Towards Straightline-Extractable NIZKPoK of a Close Vector

As mentioned in the beginning of this section, there are two choices for the NIZKPoK with a straightline extractor for proving the knowledge of a vector $\mathbf{x}$ to a given statement $(\mathbf{P}, \mathbf{h})$ such that $\|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}} \leq \beta$.

Encryption-to-the-sky and Approximate ZKPoK. Besides proving that $\mathbf{x}$ is close $\mathbf{h}$, we also encrypt $\mathbf{x}$ using the LIP-based scheme PKE in Section 3.1 and give a combined proof including the approximate proof by Σ^{CV}, the ciphertext, and the proof by Σ^{PKE} in Section 3.3 that the ciphertext is wellformed. Then, the straightline extractor of this combined ZKPoK is the PKE decryptor. In order to encrypt $\mathbf{x} \in \mathbb{Z}^n$, we need it to live in the plaintext space $\mathbb{Z}_p^n$. Since the quadratic form $\mathbf{P}$ is sample from $\mathcal{D}_{s,\mu}([\mathbf{S}])$, we have the ℓ_2-norm of $\mathbf{x}$ (as shown in Section 5.2) by Lemma 2.4 that

$$\|\mathbf{x}\| \leq \frac{1}{\sqrt{\mu}}\left(\beta + \frac{sn^2}{4}\right)$$

Then, it is enough to encrypt $\mathbf{x}$ using PKE instantiated with a prime $p \geq \frac{2}{\sqrt{\mu}}\left(\beta + \frac{sn^2}{4}\right)$. For Σ^{CV} takes a bit challenge set and Σ^{PKE} admits a polynomial-size challenge set $[-g, g]$, the soundness error of the combined ZKPoK is $t = \frac{1}{2(2g+1)}$, and it needs $\frac{\lambda}{\log(2(2g+1))}$ to achieve the soundness error of $2^{-\lambda}$. We then use the Fiat-Shamir transformation to get a NIZKPoK in the random oracle model. Let this NIZKPoK called NIZK_1. Unfortunately, for Σ^{CV} is special-sound for $R_{\mathsf{pp},2\sigma\sqrt{n}+\beta}$ where $\sigma = \Theta\left(\beta\sqrt{\frac{1}{\ln n}}\right)$, the verifier can only be convinced on an extracted witness of NIZK_1 for $(\mathbf{P}, \mathbf{h})$ that

$\|\mathbf{x}-\mathbf{h}\| \leq \Theta\left(\beta\sqrt{\frac{n}{\ln n}}\right)$. This causes the problem when we use NIZK_1 in the blind signatures. In such scenario, $\beta = 2\rho$, and we know from Section 4.2 that there is polynomial-time attack to the omCVP when the distance between $\mathbf{x}$ and $\mathbf{h}$ is $\delta = \Omega\left(\rho\sqrt{n}\ln n\right)$. Thus, the blind signatures instantiated with NIZK_1 is at very close gap $\Theta(\ln n)$ to being forgeable.

Extractable Commitment and ZKPoK for Quadratic Relations. We can circumvent the soundness slack issue in the above ZKPoK by the more complicated ZKPoK for quadratic relations in Section 5.2. We have shown to reduce the relation $R_{\mathsf{pp},\beta}$ to the relation $R^*_{\mathsf{pp}^*}$ of multiple quadratic equations, so if the protocol Σ^* is sound for $R^*_{\mathsf{pp}^*}$, its proof can convince the verifier on the knowledge of $\mathbf{x}$ such that $\|\mathbf{x}-\mathbf{h}\| \leq \Theta(\beta)$. We also have a straightline extractor for free as we have in the proof a PKE commitment to $\mathbf{x}$ which can be extracted for $\mathbf{x}$ by the decryption of PKE. The soundness error of Σ^* is $\frac{1}{p^N} + \frac{1}{2g+1}$, so it needs $t = \frac{\lambda}{\log \frac{p^N(2g+1)}{p^N+2g+1}}$ parallel repetitions for getting negligible soundness error of $2^{-\lambda}$. Finally, this ZKPoK is trivially converted into NIZKPoK in the random oracle by the Fiat-Shamir transformation, NIZK_2.

Theorem 5.5. *Let* NIZK_2 *be the Fiat-Shamir transformation of the protocol* Π^* *repeated in* $t = \frac{\lambda}{\log \frac{p^N(2g+1)}{p^N+2g+1}}$ *times.* NIZK_2 *is complete, sound with a straightline knowledge extractor and zero-knowledge for the relation* $R_{\mathsf{pp},\beta}$.

Proof. The protocol Π^* is complete, $(2,3)$-special-sound and SHVZK for the relation $R^*_{\mathsf{pp}^*}$ by Theorem 5.4, and there is a reduction of the relation $R_{\mathsf{pp},\beta}$ to $R^*_{\mathsf{pp}^*}$ as shown in Section 5.2. Hence, NIZK_2 is complete, sound and zero-knowledge for $R_{\mathsf{pp},\beta}$. Since Π^* use PKE to commit to the witness as in Section 3.2, the decryptor of PKE acts as a straightline extractor for Π^*, and it does the same for NIZK_2. □

6 Blind Signatures from One-More-CVP

In the section, we give the construction of the blind signature scheme based on the omCVP assumption. Our scheme is the adaptation of the Agrawal et al. omSIS-based scheme [AKSY22] which is built upon the hash-then-sign GPV signatures [GPV08] to the LIP-based DvW signatures[DvW22]. In the hash-then-sign DvW signatures, the signer signs upon the hash of the message $\mathbf{h} \leftarrow H(m) \in \mathbb{T}_q^n$ where H is modelled as a random oracle. Then, in the blind signature setup, the user requesting a signature on a message m should mask $H(m)$ before sending a request to the signer, so that the signer does not learn anything about $H(m)$ or m. A simple way to do that is to sample a mask $\mathbf{r}$ which is sampled from a distribution which is indistinguishable from uniform in the hash space $\mathbb{T}_q^n$ and use it to "one-time pad" $\mathbf{t} := \mathbf{r} + \mathbf{h} \bmod \mathbb{Z}^n$. The signer then gives a DvW signature for $\mathbf{t}$ which is a vector $\boldsymbol{\sigma} \in \mathbb{Z}^n$ that is close to $\mathbf{t}$. The user can then derive a vector $\mathbf{x} \in \mathbb{Z}^n$ which is close to $\mathbf{h}$. Even though $\mathbf{x}$ looks like a LIP-based signature for m, disclosing $\mathbf{x}$ trivially allows the signer to link it to one of the signer's complete signing sessions and thus breaks the blindness property. Therefore, it is required to employ an NIZKPoK to prove that the user knows $\mathbf{x}$ which is close $\mathbf{h}$.

In the unforgeability proof, we resort to the omCVP assumption which allows a natural reduction proof. Relying on "one-more" type assumptions is a common technique to achieve round-optimal blind signatures in the literature [BNPS03, AKSY22].

For instantiating the NIZKPoK protocol NIZK_2 in Section 5.3, the witness $\mathbf{x} \in \mathbb{Z}^n$ must be put into a finite integral vector space. In this blind signature scheme, the public key being the quadratic form $\mathbf{P}$ is sampled from the distribution $\mathcal{D}_{s,\mu}([\mathbf{S}])$ mentioned in Section 2.3, so that we have the ℓ_2-norm of $\mathbf{x}$ bounded as in Lemma 2.4.

6.1 Construction

Let $H : \{0,1\}^* \to \mathbb{T}_q^n$ be a full-domain hash function, and $\mathsf{NIZK} = (\mathcal{P}^G, \mathcal{V}^G)$, where G is a random oracle, be a NIZKPoK system for LIP signatures which is the protocol NIZK_2 defined in Section 5.3. Given a quadratic form $\mathbf{S} \in \mathcal{S}_n^{>0}(\mathbb{Z})$ and public parameters s, μ, n, ρ, q which are parametrised by λ, we define a blind signature scheme $\mathsf{BSig}(1^\lambda) = (\mathsf{Setup}, \mathsf{KGen}, \langle \mathcal{U}, \mathcal{S} \rangle, \mathsf{Verify})$ in Fig. 16.

Theorem 6.1 (Correctness)**.** *For* $s \geq \max\left\{\lambda_n(\mathbf{S}), \left\|\mathbf{B}_\mathbf{S}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$ *and* $q \leq \frac{s \cdot n}{\rho} \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$, BSig *is correct.*

Proof. By Lemma 2.14, sampling $(\mathbf{P}, \mathbf{U})$ using $\mathsf{QFS}(\mathbf{S}, s)$ is efficient with a parameter $s \geq \max\left\{\lambda_n(\mathbf{S}), \left\|\mathbf{B}_\mathbf{S}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}\right\}$. By Lemma 2.15, we have with overwhelming probability that $q\rho/\sqrt{n} \geq s\sqrt{n} \cdot \sqrt{\frac{\ln(2n+4)}{\pi}} \geq \left\|\mathbf{B}_\mathbf{P}^{\mathsf{GS}}\right\| \cdot \sqrt{\frac{\ln(2n+4)}{\pi}}$, so by Lemma 2.10, it is efficient to sample an error $\mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\rho/\sqrt{n}} \in \frac{1}{q}\mathbb{Z}^n$, and by Lemma 2.11, we have $\|\mathbf{e}\|_\mathbf{P} \leq \rho$ with overwhelming probability. Then, $\mathbf{t} := \mathbf{e} + \mathbf{h} \bmod \mathbb{Z}^n$, so $\mathbf{v} := \mathbf{t} - \mathbf{e} - \mathbf{h} \in \mathbb{Z}^n$. From the correctness of $\mathsf{DiscreteSample}$ in Lemma 2.10, $\boldsymbol{\sigma} \in \mathbb{Z}^n$, Blind Signatures BSig

$\underline{\mathsf{Setup}\left(1^{\lambda}\right)}$

$\mathsf{pp}_{\mathsf{Sig}} := (\mathbf{S}, s, \mu, n, \rho, q)$

$\mathsf{pp}_{\mathsf{NIZK}} := \mathsf{NIZK.Setup}\left(1^{\lambda}\right)$

$\mathsf{pp} := \left(\mathsf{pp}_{\mathsf{Sig}}, \mathsf{pp}_{\mathsf{NIZK}}\right)$

return pp

$\underline{\mathsf{KGen}\left(\mathsf{pp}\right)}$

$(\mathbf{P}, \mathbf{U}) \leftarrow\!\!\$\ \mathcal{D}_{s,\mu}\left([\mathbf{S}]\right)$

$\mathsf{pk} := \mathbf{P}$

$\mathsf{sk} := \mathbf{U}$

return $(\mathsf{pk}, \mathsf{sk})$

Signing Protocol

$\underline{\mathcal{U}\left(\mathsf{pk}, m\right)}$ $\qquad\qquad$ $\underline{\mathcal{S}\left(\mathsf{sk}\right)}$

$\mathbf{h} \leftarrow H\left(m\right)$

$\mathbf{e} \leftarrow\!\!\$\ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\rho/\sqrt{n}}$

$\mathbf{t} := \mathbf{e} + \mathbf{h} \bmod \mathbb{Z}^n$

$\mathbf{v} := \mathbf{t} - \mathbf{e} - \mathbf{h}$

$\xrightarrow{\quad \mathbf{t} \quad}$

$\boldsymbol{\sigma}' \leftarrow\!\!\$\ \mathcal{D}_{\mathbf{S},\rho/\sqrt{n},\mathbf{Ut}}$

$\boldsymbol{\sigma} := \mathbf{U}^{-1}\boldsymbol{\sigma}'$

$\xleftarrow{\quad \boldsymbol{\sigma} \quad}$

if $(\boldsymbol{\sigma} \notin \mathbb{Z}^n \vee \|\boldsymbol{\sigma} - \mathbf{t}\|_{\mathbf{P}} > \rho)$ **then**

  abort

$\mathbf{x} := \boldsymbol{\sigma} - \mathbf{v}$

$\pi \leftarrow \mathsf{NIZK}.\mathcal{P}^{G}\left(\mathsf{pp}_{\mathsf{NIZK}}, (\mathbf{P}, \mathbf{h}), \mathbf{x}\right)$

return π

$\underline{\mathsf{Verify}\left(\mathsf{pk}, m, \pi\right)}$

$\mathbf{h} \leftarrow H\left(m\right)$

$b \leftarrow \mathsf{NIZK}.\mathcal{V}^{G}\left(\mathsf{pp}_{\mathsf{NIZK}}, (\mathbf{P}, \mathbf{h}), \pi\right)$

return b

Figure 16: The blind signatures from omCVP.

so $\mathbf{x} := \boldsymbol{\sigma} - \mathbf{v} \in \mathbb{Z}^n$. Since $\mathbf{P} = \mathbf{U}^{\mathsf{T}}\mathbf{S}\mathbf{U}$, we have:

$$\|\boldsymbol{\sigma} - \mathbf{t}\|_{\mathbf{P}} = \|\mathbf{U}(\boldsymbol{\sigma} - \mathbf{t})\|_{\mathbf{S}} = \|\boldsymbol{\sigma}' - \mathbf{Ut}\|_{\mathbf{S}}$$

and from Lemma 2.11, $\|\boldsymbol{\sigma} - \mathbf{t}\|_{\mathbf{P}} = \|\boldsymbol{\sigma}' - \mathbf{Ut}\|_{\mathbf{S}} \leq \rho/\sqrt{n} \cdot \sqrt{n} = \rho$ with overwhelming probability. This gives us:

$$\begin{aligned}\|\mathbf{x} - \mathbf{h} - \mathbf{e}\|_{\mathbf{P}} &= \|\sigma - \mathbf{v} - \mathbf{e} - \mathbf{h}\|_{\mathbf{P}} \\ &= \|\sigma - \mathbf{t}\|_{\mathbf{P}} \leq \rho\end{aligned}$$

Thus, we have with overwhelming probability that:

$$\begin{aligned}\|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}} &= \|\mathbf{x} - \mathbf{h} - \mathbf{e} + \mathbf{e}\|_{\mathbf{P}} \\ &\leq \|\mathbf{x} - \mathbf{h} - \mathbf{e}\|_{\mathbf{P}} + \|\mathbf{e}\|_{\mathbf{P}} \\ &\leq 2\rho\end{aligned}$$

Therefore, the proof π for the statement

$$\mathbf{x} \in \mathbb{Z}^n \wedge \|\mathbf{x} - \mathbf{h}\|_{\mathbf{P}} \leq 2\rho$$

is accepted due to the completeness of NIZK. □

Theorem 6.2 (One-More Unforgeability)**.** *For* NIZK *is straightline extractable and sound for the relation* $R_{\mathsf{pp}_{\mathsf{NIZK}},2\rho}$*,* BSig *is one-more unforgeable if* $\mathsf{omCVP}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$ *(with* $\delta = 2\rho$*) is hard.*

Proof. We construct the proof using the following hybrids.

- Hyb_1: This is the same as the one-more unforgeability experiment in Definition 2.44.
- Hyb_2: For all signatures π_i output by the adversary $\mathcal{A}$ for all $i \in [\ell+1]$, the challenger uses the straightline extractor of NIZK to get $\mathbf{x}_i$ and stores $\{\mathbf{x}_i\}_{i\in[\ell+1]}$.

The differences between Hyb_1 and Hyb_2 are only within the inner computations and not in the interactions with the adversary, so these two hybrids are identical in the view of the adversary. Thus, we have:

$$\Pr\left[\mathsf{Forge}^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] = \Pr\left[\mathsf{Hyb}_1^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] = \Pr\left[\mathsf{Hyb}_2^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right]$$

There exists a reduction $\mathcal{R}$ as a PPT omCVP adversary using the adversary $\mathcal{A}$ in the hybrid Hyb_2 as in Fig. 17.

For NIZK is straightline extractable and sound, the probability that $\mathcal{E}_{\mathsf{NIZK}}$ extracts a false witness for a statement with a valid proof is negligible, and it holds that for all $i \in [\ell+1]$:

$$\mathbf{x}_i \in \mathbb{Z}^n \wedge \|\mathbf{x}_i - H[m_i]\|_{\mathbf{P}} \leq 2\rho$$

Due to the way that hashing queries are answered by $\mathcal{R}$, $H[m_i]$ is one of the targets returned by $\mathsf{Target}\mathcal{O}$. Define $\mathbf{t}_i = H[m_i]$. Then, we have for all $i \in [\ell+1]$:

$$\mathbf{t}_i \in T \wedge \mathbf{x}_i \in \mathbb{Z}^n \wedge \|\mathbf{x}_i - \mathbf{t}_i\|_{\mathbf{P}} \leq 2\rho$$

$\mathcal{R}(\mathbf{P})$	$\mathcal{R}.\mathsf{Sign}O(\mathbf{t})$
$H := \emptyset$	$\boldsymbol{\sigma} \leftarrow \mathsf{Gaussian}O(\mathbf{t})$
$\mathsf{pk} := \mathbf{P}$	**return** $\boldsymbol{\sigma}$
for $i \in [\ell]$ **do**	
$\quad \mathbf{t}_i \leftarrow \mathcal{A}^{\mathsf{Hash}O}(\mathsf{pk})$	$\mathcal{R}.\mathsf{Hash}O(m)$
$\quad \boldsymbol{\sigma}_i \leftarrow \mathsf{Sign}O(\mathbf{t}_i)$	**if** $H[m] = \perp$ **then**
$\{(m_i, \pi_i)\}_{i\in[\ell+1]} \leftarrow \mathcal{A}^{\mathsf{Hash}O,G}\left(\mathsf{pk}, \{\boldsymbol{\sigma}_i\}_{i\in[\ell]}\right)$	$\quad \mathbf{h} \leftarrow \mathsf{Target}O$
	$\quad H[m] := \mathbf{h}$
for $i \in [\ell+1]$ **do**	**return** $H[m]$
$\quad \mathbf{x}_i \leftarrow \mathcal{E}_{\mathsf{NIZK}}\left((\mathbf{P}, H[m_i]), \pi_i, Q_G(\mathcal{A})\right)$	
$b_1 := (\forall i \in [\ell+1], \mathsf{Verify}(\mathsf{pk}, m_i, \pi_i) = 1)$	
$b_2 := \left(\forall 1 \le i < j \le \ell+1, m_i \ne m_j\right)$	
if $(b_1 \wedge b_2) = 0$ **then return** $\perp$	
return $\{(H[m_i], \mathbf{x}_i)\}_{i\in[\ell+1]}$	

Figure 17: The reduction to omCVP.

Since $\mathcal{A}$ can make at most ℓ signing queries, $\mathcal{R}$ also makes at most ℓ Gaussian queries in the omCVP experiment. Thus, $\mathcal{R}$ is a valid omCVP adversary, and it is assumed that $\mathsf{omCVP}^{\mathcal{R}}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}$ is hard for $\delta = 2\rho = o\left(\rho\sqrt{n}\ln(n)\right)$, so we have:

$$\Pr\left[\mathsf{omCVP}^{\mathcal{R}}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}(\lambda) = 1\right] \ge \Pr\left[\mathsf{Hyb}_2^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] - (\ell+1)\,\mathsf{negl}(\lambda)$$

$$\Pr\left[\mathsf{Forge}^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] \le \Pr\left[\mathsf{omCVP}^{\mathcal{R}}_{\mathbf{S},n,s,\mu,\rho,q,\ell,\delta}(\lambda) = 1\right] + \mathsf{negl}(\lambda)$$

$$\Pr\left[\mathsf{Forge}^{\mathsf{BSig},\mathcal{A}}(\lambda) = 1\right] \le \mathsf{negl}(\lambda)$$

□

Theorem 6.3 (Honest-Signer Blindness)**.** *For $\rho/\sqrt{n} \ge \eta_{2^{-\Theta(n)}}([\mathbf{S}])$ and* NIZK *is zero-knowledge,* BSig *is honest-signer blind in the random oracle model.*

Proof. We construct the proof using the following hybrids.

- Hyb_1: This is the same as the blindness experiment in Definition 2.45.
- Hyb_2: The NIZK proofs π_0 and π_1 are simulated without using the witnesses.
- Hyb_3: The vectors $\mathbf{t}_0$ and $\mathbf{t}_1$ are computed differently. Instead of sampling $\mathbf{e}_0, \mathbf{e}_1 \leftarrow\$ \frac{1}{q}\mathcal{D}_{\mathbf{P},q\rho/\sqrt{n}}$ and setting $\mathbf{t}_0 := \mathbf{e}_0 + H(m_b) \bmod \mathbb{Z}^n$ and $\mathbf{t}_1 := \mathbf{e}_1 + H(m_{\bar{b}}) \bmod \mathbb{Z}^n$, we have $\mathbf{t}_0 := \mathbf{r}_0 + H(m_b) \bmod \mathbb{Z}^n$ and $\mathbf{t}_1 := \mathbf{r}_1 + H(m_{\bar{b}}) \bmod \mathbb{Z}^n$ where $\mathbf{r}_0$ and $\mathbf{r}_1$ are uniformly sampled from $\mathbb{T}_q^n$

The difference between Hyb_1 and Hyb_2 is in the way π_0 and π_1 are computed, so these two hybrids are indistinguishable due to the zero-knowledge property of the NIZK. Therefore,

$$\mathsf{Adv}^{\mathsf{ZK}}_{\mathsf{NIZK},\mathcal{A}}(\lambda) = \left|\mathsf{Adv}^{\mathsf{Hyb}_1}_{\mathsf{BSig},\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hyb}_2}_{\mathsf{BSig},\mathcal{A}}(\lambda)\right| \leq \mathsf{negl}(\lambda)$$
$$\left|\mathsf{Adv}^{\mathsf{ExpBlind}}_{\mathsf{BSig},\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hyb}_2}_{\mathsf{BSig},\mathcal{A}}(\lambda)\right| \leq \mathsf{negl}(\lambda)$$

The difference between Hyb_2 and Hyb_3 is in the choice of blinding term for $H(m)$. Since $\rho/\sqrt{n} \geq \eta_{2^{-\Theta(n)}}([\mathbf{S}]) = \eta_{2^{-\Theta(n)}}([\mathbf{P}])$, we have by Corollary 2.9.1 that the two vectors ($\mathbf{e}_0 \bmod \mathbb{Z}^n$) and ($\mathbf{e}_1 \bmod \mathbb{Z}^n$) are statistically indistinguishable from uniform $\mathbf{r}_0$ and $\mathbf{r}_1$, respectively. Thus, Hyb_3 and Hyb_4 are indistinguishable, so:

$$\left|\mathsf{Adv}^{\mathsf{Hyb}_3}_{\mathsf{BSig},\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{Hyb}_2}_{\mathsf{BSig},\mathcal{A}}(\lambda)\right| \leq \mathsf{negl}(\lambda)$$

Furthermore, the adversary $\mathcal{A}$ has no advantage in Hyb_3 in determining the bit b since it is information-theoretically hidden. Thus,

$$\mathsf{Adv}^{\mathsf{Hyb}_2}_{\mathsf{BSig},\mathcal{A}}(\lambda) \leq \mathsf{negl}(\lambda), \text{ so}$$
$$\mathsf{Adv}^{\mathsf{ExpBlind}}_{\mathsf{BSig},\mathcal{A}}(\lambda) \leq \mathsf{negl}(\lambda)$$

□

7 Conclusion

In this work, we introduce a public-key encryption based on $\Delta\mathsf{LIP}$, and this scheme can be seen as an extension of the key-encapsulation mechanism by Ducas and van Woerden [DvW22] and the bit encryption by Ackermann et al. [ARLW24] to encrypt vector in the ring $\mathbb{Z}_p^n$. We also provide a zero-knowledge proof of plaintext knowledge, so that our PKE can be further extend to a verifiable encryption. As a public-key encryption implies an extractable commitment scheme, our PKE also shows its usefulness as a commitment scheme in our zero-knowledge proof for quadratic relations which we employ to prove the knowledge of a vector that is close to a given target. By committing to the witness by PKE, this ZKPoK naturally has a straightline extractor which is the decryptor of PKE. Finally, we present the first LIP-based blind signature scheme. This scheme is based on the LIP-based digital signatures [DvW22]. For a LIP signature is a vector close to the message's hash, we apply the above ZKPoK to prove the knowledge of such vector to achieve the blindness property. The one-more unforgeability proof of our blind signatures relies on a newly-stated one-more close vector problem (omCVP) assumption. Similar to other assumptions of the "one-more" family for building round-optimal blind signatures such as one-more SIS [AKSY22] and one-more-RSA-inversion assumptions, we are unable to reduce the omCVP assumption to a standard one, for example approximate-CVP or $\Delta\mathsf{LIP}$. However, we show a cryptanalysis details and are confident that our parameter choice for the blind signatures is within the secure range. Though the main focus of this work is to provide a round-optimal blind signature scheme from a LIP-based digital signature scheme, we also expand the technical toolkit of LIP-based cryptography with an additively-homomorphic public-key encryption accompanied with a zero-knowledge proof of ciphertext wellformedness, so that one may use it as a commitment scheme in zero-knowledge proofs for proving linear and quadratic relations.

References

[AAEBB20] Nabil Alkeilani Alkadri, Rachid El Bansarkhani, and Johannes Buchmann. Blaze: Practical lattice-based blind signatures for privacy-preserving applications. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020 , Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers*, page 484–502, Berlin, Heidelberg, 2020. Springer-Verlag.

[ACK21] Thomas Attema, Ronald Cramer, and Lisa Kohl. A compressed Σ-protocol theory for lattices. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 549–579, Cham, 2021. Springer International Publishing.

[ACL+22] Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri AravindaKrishnan Thyagarajan. Lattice-based snarks: Publicly verifiable, preprocessing, and recursively composable. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 102–132, Cham, 2022. Springer Nature Switzerland.

[ADFMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 411–439, Cham, 2020. Springer International Publishing.

[ADRSD15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2n time using discrete gaussian sampling: Extended abstract. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '15, page 733–742, New York, NY, USA, 2015. Association for Computing Machinery.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 99–108, New York, NY, USA, 1996. Association for Computing Machinery.

[AKSY22] Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav. Practical, round-optimal lattice-based blind signatures. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 39–53, New York, NY, USA, 2022. Association for Computing Machinery.

[ARLW24] Léo Ackermann, Adeline Roux-Langlois, and Alexandre Wallet. Public-Key Encryption from the Lattice Isomorphism Problem. In *WCC 2024 - The Thirteenth International Workshop on Coding and Cryptography*, pages 1–11, Perugia, Italy, June 2024.

[BBCDK24] Benjamin Benčina, Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Mukul Kulkarni. Properties of lattice isomorphism as a cryptographic group action. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography*, pages 170–201, Cham, 2024. Springer Nature Switzerland.

[BCDF25] Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Ermes Franch. Don't use it twice: Reloaded! on the lattice isomorphism group action. Cryptology ePrint Archive, Paper 2025/516, 2025.

[BDL+18] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks*, pages 368–385, Cham, 2018. Springer International Publishing.

[BGPSD23] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 252–281, Cham, 2023. Springer Nature Switzerland.

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, page 309–325, New York, NY, USA, 2012. Association for Computing Machinery.

[BLNS23] Ward Beullens, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. Lattice-based blind signatures: Short, efficient, and round-optimal. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 16–29, New York, NY, USA, 2023. Association for Computing Machinery.

[BLP+13a] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, page 575–584, New York, NY, USA, 2013. Association for Computing Machinery.

[BLP+13b] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors, 2013.

[BMM25] Pedro Branco, Giulio Malavolta, and Zayd Maradni. Fully-homomorphic encryption from lattice isomorphism. Cryptology ePrint Archive, Paper 2025/993, 2025.

[BNPS03] Bellare, Namprempre, Pointcheval, and Semanko. The one-more-rsa-inversion problems and the security of chaum's blind signature scheme. *Journal of Cryptology*, 16(3):185–215, Jun 2003.

[Cha83] David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology*, pages 199–203, Boston, MA, 1983. Springer US.

[DFPS22] Julien Devevey, Omar Fawzi, Alain Passelègue, and Damien Stehlé. On rejection sampling in lyubashevsky's signature scheme. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 34–64, Cham, 2022. Springer Nature Switzerland.

[DKQ+25] Dung Hoang Duong, Xuan Thanh Khuc, Youming Qiao, Willy Susilo, and Chuanqi Zhang. Blind signatures from cryptographic group actions. Cryptology ePrint Archive, Paper 2025/397, 2025.

[dPK22] Rafael del Pino and Shuichi Katsumata. A new framework for more efficient round-optimal lattice-based (partially) blind signature via trapdoor sampling. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, page 306–336, Berlin, Heidelberg, 2022. Springer-Verlag.

[DPPvW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: Module lip makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 65–94, Cham, 2022. Springer Nature Switzerland.

[DvW21] Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. Cryptology ePrint Archive, Paper 2021/1332, 2021.

[DvW22] Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 643–673, Cham, 2022. Springer International Publishing.

[FHK+20] 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, 2020.

[Fis05] Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In Victor Shoup, editor, *Advances in*

Cryptology – CRYPTO 2005, pages 152–168, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[Fis06] Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, pages 60–77, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology — CRYPTO' 86*, pages 186–194, Berlin, Heidelberg, 1987. Springer Berlin Heidelberg.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery.

[GPV07] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Paper 2007/432, 2007.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 197–206, New York, NY, USA, 2008. Association for Computing Machinery.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, pages 75–92, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[HBG16] Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, and Kurt Rohloff, editors, *Financial Cryptography and Data Security*, pages 43–60, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[HKLN20] Eduard Hauck, Eike Kiltz, Julian Loss, and Ngoc Khanh Nguyen. Lattice-based blind signatures, revisited. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 500–529, Cham, 2020. Springer International Publishing.

[HLM+25] Lucjan Hanzlik, Yi-Fu Lai, Marzio Mula, Eugenio Paracucchi, Daniel Slamanig, and Gang Tang. Tanuki: New frameworks for (concurrently secure) blind signatures from post-quantum groups actions. Cryptology ePrint Archive, Paper 2025/1100, 2025.

[HR14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '14, page 391–404, USA, 2014. Society for Industrial and Applied Mathematics.

[IKSA03] S. Ibrahim, M. Kamat, M. Salleh, and S.R.A. Aziz. Secure e-voting with blind signature. In *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.*, pages 193–197, 2003.

[JS24] Corentin Jeudy and Olivier Sanders. Improved lattice blind signatures from recycled entropy. Cryptology ePrint Archive, Paper 2024/1289, 2024.

[JWL+25] Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Gang Tang, Yanbin Pan, and Xiaoyun Wang. Re-randomize and extract: A novel commitment construction framework based on group actions. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 124–153, Cham, 2025. Springer Nature Switzerland.

[Kam23] Masahiro Kaminaga. Upper bound for the coefficients of the shortest vector of random lattice. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E106.A(12):1585–1588, 2023.

[KTS+24] Xuan Thanh Khuc, Anh The Ta, Willy Susilo, Dung Hoang Duong, Fuchun Guo, Kazuhide Fukushima, and Shinsaku Kiyomoto. Logarithmic-size (linkable) ring signatures from lattice isomorphism problems. In Francesco Regazzoni, Bodhisatwa Mazumdar, and Sri Parameswaran, editors, *Security, Privacy, and Applied Cryptography Engineering*, pages 214–241, Cham, 2024. Springer Nature Switzerland.

[LJPW25] Hengyi Luo, Kaijie Jiang, Yanbin Pan, and Anyu Wang. Commitment schemes based on module-LIP. Cryptology ePrint Archive, Paper 2025/431, 2025.

[LNP22a] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, page 71–101, Berlin, Heidelberg, 2022. Springer-Verlag.

[LNP22b] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon. Efficient lattice-based blind signatures via gaussian one-time signatures.

In *Public-Key Cryptography – PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II*, page 498–527, Berlin, Heidelberg, 2022. Springer-Verlag.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6), November 2013.

[LRvW25] Alberto Leporati, Lorenzo Rovida, and Wessel van Woerden. Beyond LWE: a lattice framework for homomorphic encryption. Cryptology ePrint Archive, Paper 2025/1171, 2025.

[Lyu11] Vadim Lyubashevsky. Lattice signatures without trapdoors. Cryptology ePrint Archive, Paper 2011/537, 2011.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 738–755, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[MG02] Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, STOC '10, page 351–358, New York, NY, USA, 2010. Association for Computing Machinery.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), September 2009.

[Reg25] Oded Regev. An efficient quantum factoring algorithm. *J. ACM*, 72(1), January 2025.

[Rüc10] Markus Rückert. Lattice-based blind signatures. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010*, pages 413–430, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.

[Wee22] Hoeteck Wee. Optimal broadcast encryption and cp-abe from evasive lattice assumptions. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 217–241, Cham, 2022. Springer International Publishing.

[YAZ+19] Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu, and William Whyte. Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In *Advances in Cryptology – CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I*, page 147–175, Berlin, Heidelberg, 2019. Springer-Verlag.