RLWE-based Zero-Knowledge Proofs for linear and multiplicative relations *

Ramiro Martínez[1] and Paz Morillo[1]

Universitat Politècnica de Catalunya, Barcelona, Spain**
{ramiro.martinez,paz.morillo}@upc.edu

Abstract. We present efficient Zero-Knowledge Proofs of Knowledge (ZKPoK) for linear and multiplicative relations among secret messages hidden as Ring Learning With Errors (RLWE) samples. Messages are polynomials in $\mathbb{Z}_q[x]/\langle x^n+1\rangle$ and our proposed protocols for a ZKPoK are based on the celebrated paper by Stern on identification schemes using coding problems (Crypto'93). Our 5-move protocol achieves a soundness error slightly above 1/2 and perfect Zero-Knowledge.
As an application we present Zero-Knowledge Proofs of Knowledge of relations between committed messages. The resulting commitment scheme is perfectly binding with overwhelming probability over the choice of the public key, and computationally hiding under the RLWE assumption. Compared with previous Stern-based commitment scheme proofs we decrease computational complexity, improve the size of the parameters and reduce the soundness error of each round.

Keywords: zero-knowledge proofs of knowledge · commitment scheme · ring learning with errors

* The final authenticated version is available online at https://doi.org/10.1007/978-3-030-35199-1_13.

** This work is partially supported by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701) and the Spanish Ministry of Economy and Competitiveness, through Project MTM2016-77213-R.

1 Introduction

The goal of this paper is to present new and more efficient ways of proving linear and multiplicative relations between elements hidden in lattice-based structures, such as commitment schemes, without revealing any additional information about the elements themselves. These kind of proofs play an important role in many applications, from authentication protocols to electronic voting.

Lattice-based cryptography offers a high level of security. Its assumptions rely on the hardness of problems for which there is no known efficient quantum algorithm. This contrasts with classical factorization and discrete logarithm related problems, as they are quantum efficiently solvable by Shor's algorithm [20]. When long term privacy is concerned this is specially important, as public communications could be stored until quantum computers are available. To handle this issue, new protocols whose security is based on post-quantum safe assumptions are required. Code-based and lattice-based cryptography are two families of primitives widely believed to be quantum-resistant, and extensively used in the literature.

In this article we propose improvements on a classical code-based protocol to use it in a lattice context based on the Ring Learning With Errors (RLWE) problem. Then we apply this construction to build exact proofs of knowledge of a valid opening for a commitment, and to prove that messages inside valid openings of different commitments satisfy linear or multiplicative relations.

1.1 Related work

In 1993 Stern proposed one of the first post-quantum protocols in his seminal paper on a new identification scheme based on coding theory [24]. His identification protocol was a Zero-Knowledge Proof of Knowledge (ZKPoK) of a solution of an instance of the Syndrome Decoding problem (SD). The syndrome works as a public key and the user can authenticate himself interacting with a verifier and proving knowledge of a solution (a binary vector with small Hamming weight).

The original proposal by Stern was a 3-move protocol with a soundness error of 2/3, but he also presented alternative variants with 5-moves. One reduced the computational complexity and the other reduced the soundness error to almost 1/2. However, the size of the proof increased and it turned out to be less efficient for practical cases. Many variants and applications have been published since then, addressing this lack of efficiency and providing new features (different signature schemes, possibility of building secrets with integers module q instead of only bits, applications to lattice-based cryptography, commitment schemes, ...). We describe some of them in the following paragraphs.

In 2007 the use of cyclic codes was proposed in [10], later implemented in [6]. It was adapted to lattices in [14] in 2008, preserving a binary secret. Efficiency was improved in 2010 reducing the soundness error in [9]. And many applications have used it [7,8,1,4,21].

Nevertheless we are particularly interested in the contributions of Jain *et al.* in their paper [12] where they build a commitment scheme based on the

Learning Parity with Noise (LPN) problem, proving knowledge of openings, linear and multiplicative relations between committed messages using 3-move and 2/3 soundness error Stern-based protocols. Then in 2013 Ling *et al.* showed in [17] how the original Stern protocol could be run several times in parallel to prove that a solution has small infinity norm (and not only small Hamming weight). Xie *et al.* [26] adapt these techniques to the commitment construction of [12], to be able to prove linear and multiplicative relations between polynomials with coefficients in $\mathbb{Z}_q$. However the size of their proofs require an overhead proportional to $\log^2(q)$. All of them still have a soundness error of 2/3.

In 1997 Véron published a dual version of Stern's identification scheme [25], working with the generator matrix instead of the parity check matrix, and claimed that it was more efficient. We mention it as many subsequent papers were based on this approach. However its proof was flawed and his protocol did not achieve Zero-Knowledge, as two probability distributions for the output were uniformly random but not independent uniformly random as required, and leaked information about the secret, as was pointed out by Jain *et al.* in [12], who correctly used a generator matrix.

In this paper we specially benefit from the adaptation of Stern's protocol to lattices from Ling *et al.* [17], the modification of Cayrel *et al.* [9] for reducing the soundness error increasing the number of rounds and the proposals of Jain *et al.* [12] and Xie *et al.* [26] for proving linear and multiplicative relations, that we further improve.

It is also important to mention the contributions of Benhamouda *et al.* [3] and Baum *et al.* [2], who generalized the commitment idea of [26] without using Stern's approach. They instead use Fiat-Shamir with aborts, a technique that requires relaxing the definition of commitment (so that the set of valid openings is larger than the set of openings generated by an honest prover, with more elements and less tighter bounds for the error terms) obtaining more efficient proofs with the cost of having stronger restrictions that require larger parameters. Therefore if the relaxed ZKPoK are used as a building block in a different protocol (for example for proving that an encryption public key is well formed), then the restrictions on the parameters imposed by the relaxation might have an impact on the efficiency of other parts of the protocol.

Exact Lattice-Based ZKPoK are therefore an active field of research, with very recent efficient constructions for some lattice statements including linear equations with short solutions and matrix-vector relations [27] by Yang *et al.*, new techniques when a cyclotomic polynomial fully splits in linear factors [5] by Bootle *et al.* and new recent Stern-based contributions for proving integer relations [15] and matrix-vector relations [16] by Libert *et al.*

1.2 Our contribution

Our contribution is an improvement over the two Stern-based ZKPoK for linear and multiplicative relations from [12,26]. Our ideas on proving multiplicative relations can be easely adapted to any scenario where messages are encoded as RLWE samples. We show how we are able to prove these relations for messages

commited using a commitment scheme with Benhamouda *et al.* notation, as it is the most natural adaptation of [12] to the RLWE setting, encoding an element as a lattice point and adding a perturbed random point from a different lattice.

We get rid of the relaxations and limitations that were necessary in Benhamouda *et al.* commitment scheme without needing the quadratic logarithm of q overhead from Xie *et al.* For the linear relation case we apply standard improvements to the original Stern protocol, but adding some original modifications to carefully reduce some constants in the communication cost. For the multiplicative relation we construct a new efficient proof. We achieve this by asking the verifier for two challenges in order to get soundness. Honest-Verifier Zero-Knowledge is obtained as we explicitly provide a perfect simulator for each protocol. Notice that simulations can skip the generation of never opened auxiliary commitments, as they can just be computed as commitments to 0, indistinguishable from honestly computed commitments.

Many applications demand to evaluate arbitrary arithmetic circuits on secret elements. Fully Homomorphic Encryption could be a solution (which can be achieved with lattices by means of the Gentry *et al.* scheme [11]). An alternative is to apply our proofs for linear and multiplicative relations to prove knowledge of valid evaluations of the gates. The first lattice-based Attributed Based Signature scheme for unbounded circuits [13] uses this strategy with the ZKPoK from [26]. Directly replacing their construction with our proposal greatly improves the efficiency of the signature scheme.

Our proposal is a 5-move protocol with a soundness error slightly above $1/2$. It allows us to prove exact knowledge of the secret inside a RLWE sample, that is, the secret is a polynomial with coefficients in $\mathbb{Z}_q$. The proposed commitment scheme is perfectly binding with overwhelming probability over the choice of the public key and computationally hiding under the RLWE assumption, widely believe to be post-quantum.

The organization of this paper is as follows. We explain the notation and the basic primitives that we are going to use in Section 2. We present the commitment in Section 3, along with a proof of knowledge of a valid opening in 3.1. We then give proofs of a linear relation and a multiplicative relation in Sections 3.2, 3.3, respectively. We finally end with some conclusions in Section 4.

2 Preliminaries

2.1 Notation

Column vectors are denoted as $\boldsymbol{a}$ and row vectors as $\boldsymbol{a}^\mathsf{T}$. We denote by $\mathbb{1}_n$ the vector of dimension n with all its coordinates equal to 1. Matrices are represented as $\boldsymbol{M}$. Let q be prime, given a vector $\boldsymbol{v} \in \mathbb{Z}_q^n$ we define the infinity norm as $\|\boldsymbol{v}\|_\infty = \max_{1\leq i\leq n} |v_i|$ where v_i are the coordinates of vector $\boldsymbol{v}$ taking $\left[-\left\lfloor \frac{q}{2} \right\rfloor, \ldots, 0, \ldots, \left\lfloor \frac{q}{2} \right\rfloor\right]$ as representatives.

When a is sampled uniformly at random from set A we write $a \xleftarrow{\$} A$, $a \xleftarrow{\$} D$ when a is sampled according to a probability distribution D and $a \xleftarrow{\$} \mathcal{A}$ when a is the output of a probabilistic algorithm $\mathcal{A}$.

PPT denotes the class of Probabilistic Polynomial-Time algorithms.

A function f is *negligible* if $|f(n)| \in \mathcal{O}\left(n^{-c}\right),\ \forall c \in \mathbb{Z}^+$.

A function f is *overwhelming* if $|f(n) - 1| \in \mathcal{O}\left(n^{-c}\right),\ \forall c \in \mathbb{Z}^+$.

When an honest prover should send an element a we denote by $\widetilde{a}$ the element actually disclosed by the (possibly malicious) prover and we call $\widehat{a}$ to the element alleged to play the same role in the simulated conversation.

2.2 Zero-Knowledge Proofs

The goal of this paper is to prove the truthness of an statement without revealing anything else besides what can be efficiently deduced from the fact that the statement is indeed true. To do so we use Public Coin Honest-Verifier Zero-Knowledge Proofs of Knowledge. Let $\mathcal{R} \subset \{0,1\}^* \times \{0,1\}^*$ be a binary relation with one restriction. If $(x, w) \in \mathcal{R}$ satisfies the relation then the size $|w|$ is at most $p(|x|)$ for some fixed polynomial p.

Definition 1 (Zero-Knowledge Proofs of Knowledge).
A $(2n+1)$-move Public Coin Honest-Verifier Zero-Knowledge Proof of Knowledge *is a protocol between a prover* $\mathcal{P}$ *and a verifier* $\mathcal{V}$ *in which, given an* x*,* $\mathcal{P}$ *tries to convince* $\mathcal{V}$ *that he knows a witness* w *such that* $(x, w) \in \mathcal{R}$*. We use the following notation* $ZKP\left[\, w \,\middle|\, (x, w) \in \mathcal{R} \,\right]$*.*

$\mathcal{P}$ *and* $\mathcal{V}$ *engage in an interaction where* $\mathcal{P}$ *consecutively sends a message* a_i *answered by* $\mathcal{V}$ *with a random challenge* b_i *for* i *from* 1 *to* n*. Finally* $\mathcal{P}$ *gives a final answer* z *and* $\mathcal{V}$ *accepts or rejects the proof checking the conversation* $(x, \{a_i\}_i, \{b_i\}_i, z)$*. And has the following properties:*

- ***Completeness****: if an honest prover* $\mathcal{P}$ *knows a valid witness* w *such that* $(x, w) \in \mathcal{R}$ *and follows the protocol, then an honest verifier* $\mathcal{V}$ *always accepts the conversation.*
- k***-Special Soundness****: from* k *accepted conversations* $\left\{\left(x, \{a_{i,j}\}_i, \{b_{i,j}\}_i, z\right)\right\}_{j=1}^{k}$*, and* $\{b_{i,j}\}_i \neq \{b_{i,j'}\}_i$ *for* $j \neq j'$*, it is possible to efficiently extract a witness* w *such that* $(x, w) \in \mathcal{R}$*.*
- ***Honest-Verifier Zero-Knowledge****: there exists a polynomial-time simulator that takes as input* x *and random* $\{b_i\}_i$ *and outputs an accepted conversation* $(x, \{a_i\}_i, \{b_i\}_i, z)$ *with the same probability distribution as conversations between honest* $\mathcal{P}$ *and* $\mathcal{V}$*.*

This is a variant of standard Σ-protocols, as it is also pointed out by of Jain *et al.* [12] and Xie *et al.* [26].

k-Special Soundness means that a prover able to answer k challenges is honest, as in this case a witness could be extracted. If the challenge space is large enough we get soundness in one shot. In Stern's protocol and some of its variants

it is only possible to extract a valid witness from answers to all possible challenges (three in his particular protocol), then the prover could cheat with all but one (and therefore the protocol has 2/3 soundness error). Soundness is achieved repeating the protocol as many times as required until the cheating probability is negligible. In our case, increasing the number of challenges, we prove how to obtain a valid witness from valid answers to approximately one half of the possible challenges, reducing the soundness error and therefore reducing the number of repetitions required.

2.3 Ring Learning With Errors

Considering a ring $R = \mathbb{Z}[x] / \langle f(x) \rangle$ and $R_q = R/qR$, principal ideals $\langle a(x) \rangle \subseteq R_q$ can be identified with lattices generated by structured matrices $\boldsymbol{A}$ that only depend on polynomials $a(x)$ and $f(x)$, called *ideal lattices* [19].

The ideal lattice $\mathcal{L}(\boldsymbol{a})$ generated by a vector of polynomials $\boldsymbol{a} \in R_q^k$ is then $\mathcal{L}(\boldsymbol{a}) = \{\boldsymbol{a}r | r \in R_q\}$. We choose $f(x)$ to be $x^n + 1$, with n a power of 2, and then $R_q = \mathbb{Z}_q[x] / \langle x^n + 1 \rangle$, as it gives nice security reductions.

Definition 2 (Ring Learning With Errors ($\mathsf{RLWE}_{n,q,\chi}$)). *Let χ be a distribution over R (tipically a Gaussian distribution). The decisional* ring learning with errors *assumption states that $\{(a_i, a_i \cdot s + e_i)\}$ is indistinguishable from $\{(a_i, u_i)\}$ for any polynomial number of samples where $a_i \xleftarrow{\$} R_q$, $e_i \xleftarrow{\$} \chi$, $u_i \xleftarrow{\$} R_q$ and $s \in R_q$ is secret.*

The search RLWE *assumption states that no PPT adversary can recover s from a polynomial number of samples with a non-negligible probability.*

Hardness of RLWE. If parameters are chosen properly the RLWE problem becomes as hard as well known hard ideal lattice problems such as the ideal Shortest Vector Problem (SVP) [18]. With a discrete Gaussian error distribution χ where its standard deviation $\sigma \geq \omega(\sqrt{\log n})$, and for any ring, there exists a quantum reduction from the $\gamma(n)$-SVP problem to the RLWE problem to within an approximation factor $\gamma(n) = \mathcal{O}(\sqrt{n} \cdot q/\sigma)$. Additionaly, RLWE becomes no easier to solve even if the secret s is chosen from the error distribution, rather than uniformly [18].

2.4 Stern Identification Scheme

The original Zero-Knowledge interactive identification scheme by Stern allows a prover to convince a verifier that given a parity check matrix $\boldsymbol{H} \in \mathbb{F}_2^{n \times m}$ and a syndrome $\boldsymbol{y} \in \mathbb{F}_2^n$ he knows a binary vector $\boldsymbol{e} \in \mathbb{F}_2^m$ of small fixed Hamming weight $\|\boldsymbol{e}\|_{\mathsf{H}} = w$ such that it has this syndrome $\boldsymbol{y} = \boldsymbol{H}\boldsymbol{e}$.

The original Stern protocol [24] hides $\boldsymbol{e}$ with a masking vector $\boldsymbol{x} \xleftarrow{\$} \mathbb{F}_2^m$, a masking syndrome $\boldsymbol{y}' \in \mathbb{F}_2^n$ (an honest prover will compute $\boldsymbol{y}' = \boldsymbol{H}\boldsymbol{x}$) and a permutation $\pi \xleftarrow{\$} \mathfrak{S}_m$. Notice that $\boldsymbol{x} + \boldsymbol{e}$ reveals no information about $\boldsymbol{e}$, while $\pi(\boldsymbol{e})$ only reveals its Hamming weight, which is already known. Then the prover shows some of the following properties:

(a) the syndrome of $\boldsymbol{x}$ is $\boldsymbol{y}'$
(b) the syndrome of $\boldsymbol{x} + \boldsymbol{e}$ is $\boldsymbol{y}' + \boldsymbol{y}$
(c) the Hamming weight of $\pi(\boldsymbol{e})$ is w

All the properties combined imply that there is an $\boldsymbol{e}$ with Hamming weight w and syndrome $\boldsymbol{y}$.

Many of the subsequent variants turn this scheme into a lattice-based setting by just using a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and a secret $\boldsymbol{e} \in \mathbb{Z}_q^m$ with $m/2$ entries equal to 0 and $m/2$ entries equal to 1, obtaining a special instance of the ISIS problem $\boldsymbol{A}\boldsymbol{e} = \boldsymbol{y}$.

Ling *et al.* [17] propose to use a bounded infinity norm secret. In order to prove this restriction on the norm they show that the secret element has a fixed length binary decomposition. To hide the binary decomposition they extend it so that it has the same number of -1, 0 and 1. Then running the protocol in parallel for each of the vectors of the decomposition allows to prove knowledge of a solution of a general instance of the Inhomogeneous Short Integer Solution (ISIS) problem. We have to adapt their setting to the dual version and prove knowledge of a solution of a RLWE problem.

In order to prove that something has small norm we prove that it can be written with a constant number of bits. An ad-hoc basis could be used, but we prefer to keep notation simple and decompose the elements in binary assuming that the bound is a power of two.

The paper of Cayrel *et al.* [9] combines the secret and the masking element with a random challenge $\alpha \in \mathbb{Z}_q$ to obtain $(\pi(\boldsymbol{x} + \alpha\boldsymbol{e}))$, reducing the communication cost and the soundness error. We extend their approach with more challenges so that we can prove knowledge of linear and multiplicative relations.

3 Commitment scheme

Now we define a lattice-based commitment scheme, for this we can encode a message $m \in R_q$ as the coordinates of a point in an ideal lattice defined by $\boldsymbol{a} \in R_q^k$. To hide this lattice point $\boldsymbol{a}m$ we add a RLWE sample from another lattice $\boldsymbol{b}r + \boldsymbol{e}$, where $\boldsymbol{b} \in R_q^k$ defines this other lattice, the randomness $r \xleftarrow{\$} R_q$ is chosen uniformly at random and the error term $\boldsymbol{e} \xleftarrow{\$} \chi^{nk}$ is chosen from the appropriate bounded discrete Gaussian distribution.

This structure $\boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}$ is used by Benhamouda *et al.* in [3], and it is very similar to the one proposed by Xie *et al.* in [26]. As we use their structure we can use some of the parameters proposed by Benhamouda *et al.*

The degree of the polynomial $n = 2^\kappa$ is a power of two, usually $\kappa = 9$ or $\kappa = 10$. γ is an integer parameter controlling the size of the modulus q, a prime number such that $q \equiv 3 \mod 8$ and $q \geq n^\gamma$. Integer k would be the multiplicative overhead (the length of $\boldsymbol{a}$ as a vector of polynomials). Finally as in their case our errors obtained from χ will have a standard deviation $\sigma \in \mathcal{O}(n^{3/4})$ and will be bounded by $n = 2^\kappa$. We will restrict our coefficients to $[-2^\kappa, \ldots, 2^\kappa)$ but abuse notation and just write $\|\boldsymbol{e}\|_\infty < 2^\kappa$.

While the commitment algorithm Com we present in this paper is the same as the one that was presented in [3] our proofs of openings and relations do not require any relaxation (in our case the set of valid openings is exactly the set of openings obtained following the commitment algorithm). Therefore our proposal is different as a commitment scheme, our verification algorithm Ver is simpler and our parameter conditions required to prove security are less strict.

Proposition 1. *If $n \geq 256$, $\gamma \geq 3$ and $k \geq \frac{8\gamma+4}{2\gamma-5}$ then the following is a secure commitment scheme under the assumption that RLWE is hard.*

- Gen*: the generator algorithm takes a security parameter 1^λ and outputs a public key $pk = (\boldsymbol{a}, \boldsymbol{b}) \in \left(R_q^k\right)^2$, where $R_q = \mathbb{Z}_q[x] / \langle x^n + 1 \rangle$ and k are defined so that the difficulty of solving the RLWE problem is related to 1^λ. In particular the size of n is also related to 1^λ.*
  $(\boldsymbol{a}, \boldsymbol{b}) \xleftarrow{\$} \mathsf{Gen}\left(1^\lambda\right)$
- Com*: the commitment algorithm takes as input a message $m \in R_q$ and a public key $pk = (\boldsymbol{a}, \boldsymbol{b})$ and produces a commitment $\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}$ and an opening $d = (m, r, \boldsymbol{e})$, where $r \xleftarrow{\$} R_q$ and $\boldsymbol{e} \xleftarrow{\$} \chi^{nk}$ conditioned to have infinity norm smaller than $n = 2^\kappa$.*
  $(\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}, d = (m, r, \boldsymbol{e})) \xleftarrow{\$} \mathsf{Com}\left(m; pk = (\boldsymbol{a}, \boldsymbol{b})\right)$
- Ver*: the verification algorithm takes as input a commitment $\boldsymbol{c}$, a message m, an opening $d = (m, r, \boldsymbol{e})$ and a public key $pk = (\boldsymbol{a}, \boldsymbol{b})$ and accepts, 1, if $(\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}) \wedge (\|\boldsymbol{e}\|_\infty < 2^\kappa)$, or rejects, 0, otherwise.*
  $\mathsf{Ver} : \{(\boldsymbol{c}, m, d; pk)\} \to \{0, 1\}$

It satisfies the properties of a secure commitment scheme:

- ***Correctness****: if the commitment has been built correctly and the valid message and opening are published the verifier algorithm always accepts:*

$$\left(pk \xleftarrow{\$} \mathsf{Gen}\left(1^\lambda\right), (\boldsymbol{c}, d) \xleftarrow{\$} \mathsf{Com}\left(m; pk\right)\right) \implies 1 \leftarrow \mathsf{Ver}\left(\boldsymbol{c}, m, d; pk\right).$$

- ***Perfectly Binding****: a commitment can only be opened to one message:*

$$1 \leftarrow \mathsf{Ver}\left(\boldsymbol{c}, m, d; pk\right) \wedge 1 \leftarrow \mathsf{Ver}\left(\boldsymbol{c}, m', d'; pk\right) \implies m = m'.$$

- ***Computationally Hiding****: a well constructed commitment $\boldsymbol{c}$ does not leak any relevant information about the message m. For any PPT adversary $(\mathcal{A}_1, \mathcal{A}_2)$:*

$$\left| \Pr\left[b = b' \;\middle|\; \begin{array}{c} pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda),\ (m_0, m_1, aux) \xleftarrow{\$} \mathcal{A}_1(pk) \\ b \xleftarrow{\$} \{0,1\},\ (\boldsymbol{c}, d) \xleftarrow{\$} \mathsf{Com}(m_b; pk),\ b' \xleftarrow{\$} \mathcal{A}_2(\boldsymbol{c}, aux) \end{array} \right] - \frac{1}{2} \right| \in negl(\lambda).$$

The proof of this proposition is included in appendix A.

3.1 Knowledge of a Valid Opening

We first propose an Interactive Honest-Verifier Zero-Knowledge Proof of Knowledge of a valid opening for the commitment presented before. The difficult part is to prove that the error term is small enough, for which we adapt Stern-based protocols to this particular RLWE based commitment. While SD problem and ISIS problem are very similar, in order to prove that the commitment has been constructed with a RLWE sample we need several auxiliary elements. What we obtain is a 5-move protocol with a soundness error of $\frac{q+1}{2q}$, really close to $1/2$ as q is usually a very large prime.

Let $\boldsymbol{a} = (a_1, \ldots, a_k), \boldsymbol{b} = (b_1, \ldots, b_k) \in R_q^k$, a message $m \in R_q$, a random element r in R_q and $\boldsymbol{e} \in R_q^k$ a vector of polynomials with their coefficients sampled from a discrete Gaussian distribution conditioned to have norm smaller than $n = 2^\kappa$. We want to prove knowledge of a valid opening for the commitment $\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}$.

We identify a polynomial u with a vector $\boldsymbol{u}$ that has as elements the coefficients of the polynomial. For convenience we also identify a vector of polynomials with the concatenation of its associated vectors.

$$\begin{aligned} \varphi : \mathbb{Z}_q^n &\longrightarrow R_q \\ \boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1}) &\longmapsto u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \\ \phi : \mathbb{Z}_q^{nk} &\longrightarrow R_q^k \\ \boldsymbol{u} = (u_0, \ldots, u_{nk-1}) &\longmapsto \boldsymbol{u} = (\varphi(u_0, \ldots, u_{n-1}), \ldots, \varphi(u_{n(k-1)}, \ldots, u_{nk-1})) \end{aligned}$$

Lets consider the vector $\bar{\boldsymbol{e}} = \phi^{-1}(\boldsymbol{e}) + 2^\kappa \mathbb{1}_{nk}$ and its binary decomposition $\bar{\boldsymbol{e}} = \sum_{j=0}^{\kappa} 2^j \bar{\boldsymbol{e}}_j$, $\bar{\boldsymbol{e}}_j \in \{0,1\}^{nk}$ (notice that $\bar{\boldsymbol{e}}$ has only positive representatives because we have added $2^\kappa \mathbb{1}_{nk}$). From now on index j will always belong to $[0, \ldots, \kappa]$. Choose extensions $\boldsymbol{e}'_j = (\bar{\boldsymbol{e}}_j || \boldsymbol{e}''_j) \in \mathcal{B}_{nk}$, where $\mathcal{B}_{nk} \subset \{0,1\}^{2nk}$ are vectors with the same number of 0 and 1's. The extended error term is $\boldsymbol{e}' = \sum_j 2^j \boldsymbol{e}'_j$. Let $\boldsymbol{I}'$ be an nk-identity matrix attached to nk columns of 0's.

Then we have: $\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \phi((\boldsymbol{I}' \sum_j 2^j \boldsymbol{e}'_j) - 2^\kappa \mathbb{1}_{nk})$.

With this notation we can define an interactive protocol to prove knowledge of a valid opening for commitment $\boldsymbol{c}$. This extension is an adaptation of the idea from Ling *et al.* in [17] to the dual ring setting (we also shift the error to only have 0's and 1's, while their protocol also included -1's, this way we only have a factor two overhead instead of a factor three). Notice that each error decomposition element in $\mathcal{B}_{nk}$ with the same number of 0 and 1's can be completely randomized with a permutation, as it was done in the original Stern protocol with fixed Hamming weight vectors.

The complex structure of the commitment scheme requires more subtle details than the original Stern proposal, but the underlying intuition is the same. We want to prove knowledge of some elements $m, r, \boldsymbol{e}$, of some masking elements $\mu, \rho, \boldsymbol{f}$ and a of vector of polynomials $\boldsymbol{y}$ such that:

(a) $\pi_j(\boldsymbol{e}'_j) \in \mathcal{B}_{nk}$
(b) $\boldsymbol{y} = \boldsymbol{a}\mu + \boldsymbol{b}\rho + \boldsymbol{f}$
(c) $\boldsymbol{y} + \boldsymbol{c} = \boldsymbol{a}(\mu + m) + \boldsymbol{b}(\rho + r) + (\boldsymbol{f} + \boldsymbol{e})$, where $\boldsymbol{e} = \phi(\boldsymbol{I}' \sum_j 2^j \boldsymbol{e}'_j - 2^\kappa \mathbb{1}_{nk})$

All three properties imply knowledge of a valid opening for the commitment. In order to improve efficiency we can add one more round where we ask the verifier for an element $\alpha \in \mathbb{Z}_q$ and then prove only these two properties:

(a) $\pi_j(\boldsymbol{e}'_j) \in \mathcal{B}_{nk}$
(b') $\boldsymbol{y} + \alpha\boldsymbol{c} = \boldsymbol{a}(\mu + \alpha m) + \boldsymbol{b}(\rho + \alpha r) + (\boldsymbol{f} + \alpha\boldsymbol{e})$, where $\boldsymbol{e} = \phi(\boldsymbol{I}' \sum_j 2^j \boldsymbol{e}'_j - 2^\kappa \mathbb{1}_{nk})$

Since the relevant elements were commited in the first round (using an auxiliary commitment scheme) before α was chosen we can ensure with high probability that property (b') implies both properties (b) and (c). This is an adaptation of the idea used in [9] and allows us to reduce the soundness error to almost $1/2$.

With this intuition in mind we can provide our protocol (1) for proving knowledge of valid openings. Let $(\mathsf{aCom}, \mathsf{aVer})$ denote an auxiliary commitment scheme that can be instantiated using our construction or a different one.

The prover $\mathcal{P}$ chooses $\kappa + 1$ permutations $\pi_0, \ldots, \pi_\kappa \xleftarrow{\$} \mathfrak{S}_{2nk}$, $\kappa + 1$ random vectors $\boldsymbol{f}_0, \ldots, \boldsymbol{f}_\kappa \xleftarrow{\$} \mathbb{Z}_q^{2nk}$ and 2 random polynomials $\mu, \rho \xleftarrow{\$} R_q$.

Then computes the following commitments:

$$c_1 = \mathsf{aCom}\Big(\{\pi_j\}_j, \boldsymbol{a}\mu + \boldsymbol{b}\rho + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \boldsymbol{f}_j)\Big)$$
$$c_2 = \mathsf{aCom}\Big(\{\pi_j(\boldsymbol{f}_j)\}_j, \{\pi_j(\boldsymbol{e}'_j)\}_j\Big)$$

The prover sends these commitments to the verifier. The verifier $\mathcal{V}$ chooses an integer $\alpha \in \mathbb{Z}_q$ and sends it to the prover. Then the prover computes:

$$\boldsymbol{g}_j = \pi_j(\boldsymbol{f}_j + \alpha \boldsymbol{e}'_j)$$

The prover sends $\{\boldsymbol{g}_j\}_j$ to the verifier. The verifier $\mathcal{V}$ chooses a bit $b \xleftarrow{\$} \{0, 1\}$ and sends it to the prover.

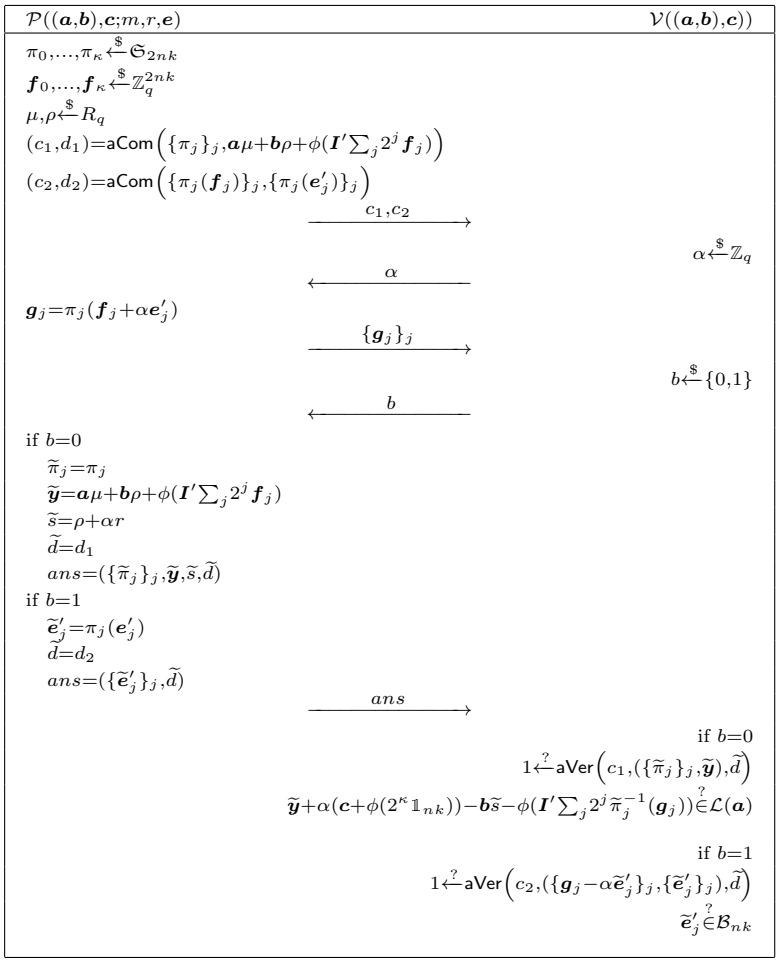
Case $b = 0$.

- $\mathcal{P}$ reveals $\{\widetilde{\pi}_j = \pi_j\}_j$, $\widetilde{\boldsymbol{y}} = \boldsymbol{a}\mu + \boldsymbol{b}\rho + \phi(\boldsymbol{I}' \sum_j 2^j \boldsymbol{f}_j)$, $\widetilde{s} = \rho + \alpha r$ and an opening of commitment c_1 to $(\{\widetilde{\pi}_j\}_j, \widetilde{\boldsymbol{y}})$.
- $\mathcal{V}$ checks c_1.
  He also checks that $\widetilde{\boldsymbol{y}} + \alpha(\boldsymbol{c} + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s} - \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_j^{-1}(\boldsymbol{g}_j)) \in \mathcal{L}(\boldsymbol{a})$ and writes it as $\boldsymbol{a}\widetilde{t}$.

Case $b = 1$.

- $\mathcal{P}$ reveals $\{\widetilde{\boldsymbol{e}}'_j = \pi_j(\boldsymbol{e}'_j)\}_j$ and openings of commitments c_2 to $(\{\boldsymbol{g}_j - \alpha\widetilde{\boldsymbol{e}}'_j\}_j, \{\widetilde{\boldsymbol{e}}'_j\}_j)$.
- $\mathcal{V}$ checks c_2 and that each $\widetilde{\boldsymbol{e}}'_j$ belongs to $\mathcal{B}_{nk}$.

$$\mathrm{ZKP}\left[m, r, \boldsymbol{e} \,\middle|\, \begin{array}{c} \boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e} \\ \|\boldsymbol{e}\|_\infty < 2^\kappa \end{array}\right] \tag{1}$$



Completeness: If $\mathcal{P}$ knows a valid witness and both the prover and the verifier correctly follow the protocol then the verifier always accepts at the end, immediate as all relations hold by construction.

Soundness: If a (possibly malicious) prover $\widetilde{\mathcal{P}}$ is able to provide accepted answers to δ rounds of interaction with an honest verifier $\mathcal{V}$ with probability $(q+1/2q)^\delta+\epsilon$, were ϵ is non-negligible, then he is able to efficiently extract a witness with probability $2(\epsilon/3)^3$. Details on how to find valid answers to the required number of different challenges are skipped here and explained in appendix B.

By the pigeonhole principle we can find commitments c_1, c_2, two α,α' and $\boldsymbol{g}_j,\boldsymbol{g}'_j$ that induce accepted answers. Define $\Delta_\alpha=\alpha-\alpha'\neq 0$. The binding

property of c_1, c_2 ensures that openings to $\widetilde{\pi}_j$, $\widetilde{\boldsymbol{y}}$ and $\widetilde{\boldsymbol{e}}'_j$ are fixed.

$$\begin{aligned}
\boldsymbol{a}\widetilde{t} &= \widetilde{\boldsymbol{y}} + \alpha(\boldsymbol{c} + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s} - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_j^{-1}(\boldsymbol{g}_j)) \\
\boldsymbol{a}\widetilde{t}' &= \widetilde{\boldsymbol{y}} + \alpha'(\boldsymbol{c} + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s}' - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_j^{-1}(\boldsymbol{g}'_j)) \\
\Delta_\alpha \boldsymbol{c} &= \boldsymbol{a}(\widetilde{t} - \widetilde{t}') + \boldsymbol{b}(\widetilde{s} - \widetilde{s}') + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_j^{-1}(\boldsymbol{g}_j - \boldsymbol{g}'_j) - \Delta_\alpha 2^\kappa \mathbb{1}_{nk}) \\
\boldsymbol{c} &= \boldsymbol{a}(\Delta_\alpha^{-1}(\widetilde{t} - \widetilde{t}')) + \boldsymbol{b}(\Delta_\alpha^{-1}(\widetilde{s} - \widetilde{s}')) + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_j^{-1}(\Delta_\alpha^{-1}(\boldsymbol{g}_j - \boldsymbol{g}'_j)) - 2^\kappa \mathbb{1}_{nk}) \\
\boldsymbol{g}_j - \alpha\widetilde{\boldsymbol{e}}'_j &= \boldsymbol{g}'_j - \alpha'\widetilde{\boldsymbol{e}}'_j \\
\widetilde{\boldsymbol{e}}'_j &= \Delta_\alpha^{-1}(\boldsymbol{g}_j - \boldsymbol{g}'_j) \\
\boldsymbol{c} &= \boldsymbol{a}(\Delta_\alpha^{-1}(\widetilde{t} - \widetilde{t}')) + \boldsymbol{b}(\Delta_\alpha^{-1}(\widetilde{s} - \widetilde{s}')) + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_j^{-1}(\widetilde{\boldsymbol{e}}'_j) - 2^\kappa \mathbb{1}_{nk})
\end{aligned}$$

As these elements come from accepted answers we know that $\widetilde{\boldsymbol{e}}'_j \in \mathcal{B}_{nk} \subset \{0,1\}^{2nk}$ and therefore $\phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_j^{-1}(\widetilde{\boldsymbol{e}}'_j) - 2^\kappa \mathbb{1}_{nk})$ has norm smaller than 2^κ. Then $(\Delta_\alpha^{-1}(\widetilde{t} - \widetilde{t}'), \Delta_\alpha^{-1}(\widetilde{s} - \widetilde{s}'), \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_j^{-1}(\widetilde{\boldsymbol{e}}'_j) - 2^\kappa \mathbb{1}_{nk}))$ is a valid opening.

Zero-Knowledge:

Case $b = 0$

$\widehat{t}, \widehat{s} \xleftarrow{\$} R_q, \quad \widehat{\boldsymbol{g}}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \widehat{\pi}_j \xleftarrow{\$} \mathfrak{S}_{2nk}$

$c_1 = \mathsf{aCom}(\{\widehat{\pi}_j\}_j, \boldsymbol{a}\widehat{t} + \boldsymbol{b}\widehat{s}$

$+\phi(\boldsymbol{I}' \sum_j 2^j \widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j)) - \alpha(\boldsymbol{c} + \phi(2^\kappa \mathbb{1}_{nk})))$

$\mathcal{P}$ reveals $\{\widehat{\boldsymbol{g}}_j\}_j$, $\{\widetilde{\pi}_j = \widehat{\pi}_j\}_j$, $\widetilde{\boldsymbol{y}} = \boldsymbol{a}\widehat{t} + \boldsymbol{b}\widehat{s} + \phi(\boldsymbol{I}' \sum_j 2^j \widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j)) - \alpha\boldsymbol{c}$, $\widetilde{s} = \widehat{s}$. Indistinguishable from a real conversation with the same $\pi_j = \widehat{\pi}_j$ and where $\mu = \widehat{t} - \alpha m$, $\rho = \widehat{s} - \alpha r$ and $\boldsymbol{f}_j = \widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j) - \alpha\boldsymbol{e}'_j$.

$$\begin{aligned}
\boldsymbol{g}_j &= \pi_j(\boldsymbol{f}_j + \alpha\boldsymbol{e}'_j) \\
&= \pi_j(\widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j)) + \pi_j(\alpha\boldsymbol{e}'_j - \alpha\boldsymbol{e}'_j) \\
&= \widehat{\boldsymbol{g}}_j \\
\boldsymbol{a}\mu + \boldsymbol{b}\rho + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \boldsymbol{f}_j) &= \\
&= \boldsymbol{a}(\widehat{t} - \alpha m) + \boldsymbol{b}(\widehat{s} - \alpha r) \\
&\quad + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j (\widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j) - \alpha\boldsymbol{e}'_j)) \\
&= \boldsymbol{a}\widehat{t} + \boldsymbol{b}\widehat{s} + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j)) \\
&\quad - \alpha(\boldsymbol{a}m + \boldsymbol{b}r + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \boldsymbol{e}'_j)) \\
&= \boldsymbol{a}\widehat{t} + \boldsymbol{b}\widehat{s} + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widehat{\pi}_j^{-1}(\widehat{\boldsymbol{g}}_j)) \\
&\quad - \alpha(\boldsymbol{c} + \phi(2^\kappa \mathbb{1}_{nk}))
\end{aligned}$$

Case $b = 1$

$\widehat{\boldsymbol{e}}'_j \xleftarrow{\$} \mathcal{B}_{nk}, \quad \widehat{\boldsymbol{f}}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \widehat{\pi}_j \xleftarrow{\$} \mathfrak{S}_{2nk}$

$c_2 = \mathsf{aCom}(\{\widehat{\pi}_j(\widehat{\boldsymbol{f}}_j)\}_j, \{\widehat{\pi}_j(\widehat{\boldsymbol{e}}'_j)\}_j)$

$\widehat{\boldsymbol{g}}_j = \widehat{\pi}_j(\widehat{\boldsymbol{f}}_j + \alpha\widehat{\boldsymbol{e}}'_j)$

$\mathcal{P}$ reveals $\{\widehat{\boldsymbol{g}}_j\}_j$, $\{\widetilde{\boldsymbol{e}}'_j = \widehat{\pi}_j(\widehat{\boldsymbol{e}}'_j)\}_j$. Equivalent to an honest conversation were π_j is such that $\pi_j(\boldsymbol{e}'_j) = \widehat{\pi}_j(\widehat{\boldsymbol{e}}'_j)$ and $\boldsymbol{f}_j = \pi_j^{-1}(\widehat{\pi}_j(\widehat{\boldsymbol{f}}_j))$.

$$\begin{aligned}
\boldsymbol{g}_j &= \pi_j(\boldsymbol{f}_j + \alpha\boldsymbol{e}'_j) \\
&= \pi_j(\pi_j^{-1}(\widehat{\pi}_j(\widehat{\boldsymbol{f}}_j))) + \alpha\widehat{\pi}_j(\widehat{\boldsymbol{e}}'_j) \\
&= \widehat{\pi}_j(\widehat{\boldsymbol{f}}_j + \alpha\widehat{\boldsymbol{e}}'_j) \\
&= \widehat{\boldsymbol{g}}_j
\end{aligned}$$

Notice that in both cases simulated conversations follow the same distribution as honest conversations.

3.2 Linear relation

The analyzed commitment scheme is not homomorphic, since the sum of two commitments may not be a commitment to the sum as the errors may grow. However it is possible to prove knowledge of openings to different commitments proving that the committed messages satisfy a given linear relation. As in the proof for the opening we have $\boldsymbol{a}, \boldsymbol{b} \in R_q^k$, messages $m_1, m_2, m_3 \in R_q$ such that $m_3 = \lambda_1 m_1 + \lambda_2 m_2$ with $\lambda_1, \lambda_2 \in R_q$, random elements r_1, r_2, r_3 in R_q and $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3 \in R_q^k$ vectors of polynomials with their coefficients sampled from a discrete Gaussian distribution conditioned to have norm smaller than $n = 2^\kappa$. We want to prove knowledge of valid openings for the commitments $\boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \boldsymbol{e}_i$ satisfying the relation. From now on index i will belong to $\{1, 2, 3\}$.

Consider the extended error decomposition terms $\boldsymbol{e}'_{ij} \in \mathcal{B}_{nk}$ so that:

$$\boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \phi(\boldsymbol{I}' \sum_j 2^j \boldsymbol{e}'_{ij} - 2^\kappa \mathbb{1}_{nk}).$$

With this notation we can define the interactive protocol (2) to prove knowledge of valid openings for commitments $\boldsymbol{c}_i$ holding the required relation.

This can be done analogously as the previous case, reproducing protocol (1) three times in parallel imposing that the message masking elements hold the same linear relation. μ_3 is computed as $\mu_3 = \lambda_1\mu_1 + \lambda_2\mu_2$ and in case $b = 0$ the verifier needs to check whether $\widetilde{t}_3 = \lambda_1\widetilde{t}_1 + \lambda_2\widetilde{t}_2$.

$$\text{ZKP}\left[m_i, r_i, \boldsymbol{e}_i \;\middle|\; \begin{array}{c} \boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \boldsymbol{e}_i \\ \|\boldsymbol{e}_i\|_\infty < 2^\kappa, \quad m_3 = \lambda_1 m_1 + \lambda_2 m_2 \end{array} \right].$$

Completeness: The relation $\widehat{t}_3 = \lambda_1\widehat{t}_1 + \lambda_2\widehat{t}_2$ is satisfied as $\widehat{t}_i = \mu_i + \alpha m_i$, m_i hold the relation and μ_3 is computed such that it holds the relation too.

Soundness: If a (possibly malicious) prover $\widetilde{\mathcal{P}}$ is able to provide accepted answers to δ rounds of interaction with an honest verifier $\mathcal{V}$ with probability $(q + 1/2q)^\delta + \epsilon$, were ϵ is non-negligible, then he is able to efficiently extract a witness. The same argument for the knowledge of a valid opening applies here and provides us with three valid openings

$$\{(\Delta_\alpha^{-1}(\widetilde{t}_i - \widetilde{t}'_i), \Delta_\alpha^{-1}(\widetilde{s}_i - \widetilde{s}'_i), \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{e}}'_{ij}) - 2^\kappa \mathbb{1}_{nk}))\}_i.$$

We know that $\widetilde{t}_3 = \lambda_1\widetilde{t}_1 + \lambda_2\widetilde{t}_2$ and the same applies to $\widetilde{t}'_3 = \lambda_1\widetilde{t}'_1 + \lambda_2\widetilde{t}'_2$. Therefore we have that the required linear relation holds:

$$\Delta_\alpha^{-1}(\widetilde{t}_3 - \widetilde{t}'_3) = \lambda_1\Delta_\alpha^{-1}(\widetilde{t}_1 - \widetilde{t}'_1) + \lambda_2\Delta_\alpha^{-1}(\widetilde{t}_2 - \widetilde{t}'_2).$$

Zero-Knowledge: The same simulator for protocol 1 works repeated 3 times, with the only exception that in case $b = 0$ we randomly choose $\widehat{t}_1, \widehat{t}_2 \xleftarrow{\$} R_q$ but $\widehat{t}_3$ is computed as $\widehat{t}_3 = \lambda_1\widehat{t}_1 + \lambda_2\widehat{t}_2$.

3.3 Multiplicative relation

In this subsection we present the main contribution of this paper, an efficient proof of knowledge of a multiplicative relation. That is, index i belongs again to $\{1,2,3\}$ and we have $\boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \boldsymbol{e}_i$ three valid commitments where $m_3 = m_1 \cdot m_2$. We want to prove knowledge of valid openings for the commitments $\boldsymbol{c}_i$ satisfying this relation.

If we mask the messages $(m_1+\mu_1)$ and $(m_2+\mu_2)$ with random $\mu_1, \mu_2 \xleftarrow{\$} R_q$, as we did before, and then multiply them, some crossed terms appear: $(m_1+\mu_1)(m_2+\mu_2) = m_3 + (m_1\mu_2 + m_2\mu_1) + \mu_1\mu_2$. Following the notation from [3] we define $m_+ = m_1\mu_2 + m_2\mu_1$ and $m_\times = \mu_1\mu_2$. If we want to get $m_3 = m_1m_2$ we need to prove a similar equality involving two challenges $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$ chosen by the verifier. In [3] they use a challenge to prove the relation, while [9] introduces the challenge to reduce the soundness error of each round as we did in section 3.1. The particular requirements of our proofs, where we try to achieve both goals at the same time, imply that we need a much more involved analysis in order to prove the soundness of this strategy. This efficient interactive protocol to prove knowledge of a valid opening for commitments $\boldsymbol{c}_i$ holding the required relation is the main contribution of this paper.

The prover $\mathcal{P}$ chooses $3(\kappa+1)$ permutations $\pi_{i0}, \ldots, \pi_{i\kappa} \xleftarrow{\$} \mathfrak{S}_{2nk}$, $3(\kappa+1)$ random vectors $\boldsymbol{f}_{i0}, \ldots, \boldsymbol{f}_{i\kappa} \xleftarrow{\$} \mathbb{Z}_q^{2nk}$ and 6 random polynomials $\mu_1, \mu_2, \mu_3, \rho_1, \rho_2, \rho_3 \xleftarrow{\$} R_q$. $\mathcal{P}$ computes $m_\times = \mu_1\mu_2$ and $m_+ = \mu_1 m_2 + \mu_2 m_1$. Then he chooses 2 additional random polynomials $\mu_\times, \mu_+ \xleftarrow{\$} R_q$.

Then computes the following commitments:

$$
\begin{aligned}
c_1 &= \mathsf{aCom}\Big(\{\pi_{ij}\}_{i,j}, \{\boldsymbol{a}\mu_i + \boldsymbol{b}\rho_i + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \boldsymbol{f}_{ij}\}_i)\Big) \\
c_2 &= \mathsf{aCom}\Big(\mu_3, \mu_\times, \mu_+\Big) \\
c_3 &= \mathsf{aCom}\Big(\{\pi_{ij}(\boldsymbol{f}_{ij})\}_{i,j}, \{\pi_{ij}(\boldsymbol{e}'_{ij})\}_{i,j}\Big) \\
c_4 &= \mathsf{aCom}\Big(\mu_\times + m_\times, \mu_+ + m_+\Big)
\end{aligned}
$$

The prover sends these commitments to the verifier. The verifier $\mathcal{V}$ chooses a pair of integers $(\alpha, \beta) \xleftarrow{\$} \mathbb{Z}_q^2$ and sends it to the prover.

Lets define the following auxiliary constants to simplify notation:

$$
\delta_i = \begin{cases} \alpha, & \text{for } i \in \{1,2\} \\ \beta, & \text{for } i \in \{3\} \end{cases}
$$

Now $\mathcal{P}$ computes the following elements and sends them to $\mathcal{V}$:

$$
\begin{aligned}
\boldsymbol{g}_{ij} &= \pi_{ij}(\boldsymbol{f}_{ij} + \delta_i \boldsymbol{e}'_{ij}) \\
c_5 &= \mathsf{aCom}\Big((\beta\mu_\times) + \alpha(\beta\mu_+) + \alpha^2(\mu_3)\Big)
\end{aligned}
$$

The prover sends $\{\boldsymbol{g}_{ij}\}_{i,j}$ and c_5 to the verifier. The verifier $\mathcal{V}$ chooses a bit $b \xleftarrow{\$} \{0,1\}$ and sends it to the prover.

Case $b = 0$.

- $\mathcal{P}$ reveals $\{\widetilde{\pi}_{ij} = \pi_{ij}\}_{i,j}$, $\{\widetilde{\boldsymbol{y}}_i = \boldsymbol{a}\mu_i + \boldsymbol{b}\rho_i + \phi(\boldsymbol{I}' \sum_j 2^j \boldsymbol{f}_{ij})\}_i$, $\widetilde{t}_\times = \mu_\times + m_\times$, $\widetilde{t}_+ = \mu_+ + m_+$, $\{\widetilde{s}_i = \rho_i + \delta_i r_i\}_i$. The prover could also compute $\widetilde{t}_i = \mu_i + \delta_i m_i$, but does not send them as the verifier can compute them as the coordinates of $\widetilde{\boldsymbol{y}}_i + \delta_i(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s}_i - \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij})) \in \mathcal{L}(\boldsymbol{a})$. Then he sends openings of commitments c_1 to $(\{\widetilde{\pi}_{ij}\}_{i,j}, \{\widetilde{\boldsymbol{y}}_i\}_i)$, c_4 to $(\widetilde{t}_\times, \widetilde{t}_+)$ and c_5 to $\beta\widetilde{t}_\times + \alpha\beta\widetilde{t}_+ + \alpha^2\widetilde{t}_3 - \beta\widetilde{t}_1\widetilde{t}_2$.
- $\mathcal{V}$ checks that $\widetilde{\boldsymbol{y}}_i + \delta_i(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s}_i - \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij})) \in \mathcal{L}(\boldsymbol{a})$ and writes them as $\boldsymbol{a}\widetilde{t}_i$. Then $\mathcal{V}$ checks c_1, c_4 and c_5.

Case $b = 1$.

- $\mathcal{P}$ reveals $\{\widetilde{\boldsymbol{e}}'_{ij} = \pi_{ij}(\boldsymbol{e}'_{ij})\}_{i,j}, \widetilde{\mu}_3 = \mu_3, \widetilde{\mu}_\times = \mu_\times, \widetilde{\mu}_+ = \mu_+$ and openings of commitments c_2 to $(\widetilde{\mu}_3, \widetilde{\mu}_\times, \widetilde{\mu}_+)$, c_3 to $(\{\boldsymbol{g}_{ij} - \delta_i \widetilde{\boldsymbol{e}}'_{ij}\}_{i,j}, \{\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j})$ and c_5 to $(\beta\widetilde{\mu}_\times) + \alpha(\beta\widetilde{\mu}_+) + \alpha^2(\widetilde{\mu}_3)$.
- $\mathcal{V}$ checks c_2,c_3,c_5 and that each $\widetilde{\boldsymbol{e}}'_{ij}$ belongs to $\mathcal{B}_{nk}$.

The multiplicative relation protocol (3) can also be seen as parallel executions of protocol (1), this time taking into account the crossed terms.

Completeness: We should check the alternative openings of commitment c_5.

$$\beta\widetilde{t}_\times + \alpha\beta\widetilde{t}_+ + \alpha^2\widetilde{t}_3 - \beta\widetilde{t}_1\widetilde{t}_2 =$$
$$= \beta(\mu_\times + m_\times) + \alpha\beta(\mu_+ + m_+) + \alpha^2(\mu_3 + \beta m_3) - \beta(\mu_1 + \alpha m_1)(\mu_2 + \alpha m_2)$$
$$= \beta(\mu_\times + m_\times - \mu_1\mu_2) + \alpha\beta(\mu_+ + m_+ - \mu_1 m_2 - \mu_2 m_1) + \alpha^2(\mu_3 + \beta(m_3 - m_1 m_2))$$
$$= (\beta\mu_\times) + \alpha(\beta\mu_+) + \alpha^2(\mu_3)$$

Soundness: If a (possibly malicious) prover $\widetilde{\mathcal{P}}$ is able to provide accepted answers to δ rounds of interaction with an honest verifier $\mathcal{V}$ with probability $\left((q^2 + 3q - 2)/(2q^2)\right)^\delta + \epsilon$, were ϵ is non-negligible, then he is able to efficiently extract a witness. If q is such that $\log(q^2/(q^2 + 3q - 2)) \geq -1/9$ (which is true if $q \geq 37$) we should be able to find more than $q^2 + 3q - 2$ accepted answers (by an argument analogous to that of appendix B).

Then the pigeonhole principle ensures that we can find six pairs $(\alpha^{(1)}, \beta^{(1)})$, $(\alpha^{(2)}, \beta^{(2)}), (\alpha^{(3)}, \beta^{(3)}), (\alpha^{(4)}, \beta^{(4)}), (\alpha^{(5)}, \beta^{(5)}), (\alpha^{(6)}, \beta^{(6)})$, with all $\alpha^{(l)}$ different for $l \in \{1,2,3\}$, all $\alpha^{(l)}$ different for $l \in \{4,5,6\}$ and $\beta^{(1)} = \beta^{(2)} = \beta^{(3)} \neq \beta^{(4)} = \beta^{(5)} = \beta^{(6)}$ that induce accepted answers for both $b = 0$ and $b = 1$.

Assume there only exist one β for which there exists at least 3 different $\alpha^{(i)}$ with accepted answers for $b = 0$ and $b = 1$. This particular β belongs to at most $2q$ answers, 2 for each possible α. All other β' contribute each of them with at most $q + 2$, only one b accepted for each possible α except two of them. If we add everything up we get $2q + (q-1)(q+2) = q^2 + 3q - 2$, but we had strictly more valid answers.

$$\mathrm{ZKP}\left[m_i,r_i,\boldsymbol{e}_i \;\middle|\; \begin{matrix}\boldsymbol{c}_i=\boldsymbol{a}m_i+\boldsymbol{b}r_i+\boldsymbol{e}_i\\ \|\boldsymbol{e}_i\|_\infty<2^\kappa,\\ m_3=\lambda_1 m_1+\lambda_2 m_2\end{matrix}\right] \quad (2)$$

$$\mathrm{ZKP}\left[m_i,r_i,\boldsymbol{e}_i \;\middle|\; \begin{matrix}\boldsymbol{c}_i=\boldsymbol{a}m_i+\boldsymbol{b}r_i+\boldsymbol{e}_i\\ \|\boldsymbol{e}_i\|_\infty<2^\kappa, m_3=m_1m_2\end{matrix}\right] \quad (3)$$

$\mathcal{P}((\boldsymbol{a},\boldsymbol{b}),\boldsymbol{c}_i;m_i,r_i,\boldsymbol{e}_i)$ $\qquad$ $\mathcal{V}((\boldsymbol{a},\boldsymbol{b}),\boldsymbol{c}_i))$

$\pi_{i0},\ldots,\pi_{i\kappa}\xleftarrow{\$}\mathfrak{S}_{2nk}$
$\boldsymbol{f}_{i0},\ldots,\boldsymbol{f}_{i\kappa}\xleftarrow{\$}\mathbb{Z}_q^{2nk}$
$\mu_1,\mu_2,\rho_1,\rho_2,\rho_3\xleftarrow{\$}R_q$
$\mu_3=\lambda_1\mu_1+\lambda_2\mu_2$
$(c_1,d_1)=\mathsf{aCom}\Big(\{\pi_{ij}\}_{i,j},\{\boldsymbol{a}\mu_i+\boldsymbol{b}\rho_i+\phi(\boldsymbol{I}'\sum_j 2^j\boldsymbol{f}_{ij})\}_i\Big)$
$(c_2,d_2)=\mathsf{aCom}\Big(\{\pi_{ij}(\boldsymbol{f}_{ij})\}_{i,j},\{\pi_{ij}(\boldsymbol{e}'_{ij})\}_{i,j}\Big)$
$\xrightarrow{\quad c_1,c_2\quad}$
$\alpha\xleftarrow{\$}\mathbb{Z}_q$
$\xleftarrow{\quad\alpha\quad}$
$\boldsymbol{g}_{ij}=\pi_{ij}(\boldsymbol{f}_{ij}+\alpha\boldsymbol{e}'_{ij})$
$\xrightarrow{\quad\{\boldsymbol{g}_{ij}\}_{i,j}\quad}$
$b\xleftarrow{\$}\{0,1\}$
$\xleftarrow{\quad b\quad}$
if b=0
$\widetilde{\pi}_{ij}=\pi_{ij}$
$\widetilde{\boldsymbol{y}}_i=\boldsymbol{a}\mu_i+\boldsymbol{b}\rho_i+\phi(\boldsymbol{I}'\sum_j 2^j\boldsymbol{f}_{ij})$
$\widetilde{s}_i=\rho_i+\alpha r_i$
$\widetilde{d}=d_1$
$ans=(\{\widetilde{\pi}_{ij}\}_{i,j},\{\widetilde{\boldsymbol{y}}_i\}_i,\{\widetilde{s}_i\}_i,\widetilde{d})$
if b=1
$\widetilde{\boldsymbol{e}}'_{ij}=\pi_{ij}(\boldsymbol{e}'_{ij})$
$\widetilde{d}=d_2$
$ans=(\{\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j},\widetilde{d})$
$\xrightarrow{\quad ans\quad}$
if b=0
$1\xleftarrow{?}\mathsf{aVer}\Big(c_1,(\{\widetilde{\pi}_{ij}\}_{i,j},\{\widetilde{\boldsymbol{y}}_i\}_i),\widetilde{d}\Big)$
$\widetilde{\boldsymbol{y}}_i+\alpha(\boldsymbol{c}_i+\phi(2^\kappa\mathbb{1}_{nk}))-\boldsymbol{b}\widetilde{s}_i-\phi(\boldsymbol{I}'\sum_j 2^j\widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}))\overset{?}{\in}\mathcal{L}(\boldsymbol{a})$
$\widetilde{t}_3\overset{?}{=}\lambda_1\widetilde{t}_1+\lambda_2\widetilde{t}_2$
if b=1
$1\xleftarrow{?}\mathsf{aVer}\Big(c_2,(\{\boldsymbol{g}_{ij}-\alpha\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j},\{\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j}),\widetilde{d}\Big)$
$\widetilde{\boldsymbol{e}}'_{ij}\overset{?}{\in}\mathcal{B}_{nk}$

$\mathcal{P}((\boldsymbol{a},\boldsymbol{b}),\boldsymbol{c}_i;m_i,r_i,\boldsymbol{e}_i)$ $\qquad$ $\mathcal{V}((\boldsymbol{a},\boldsymbol{b}),\boldsymbol{c}_i)$

$\pi_{i0},\ldots,\pi_{i\kappa}\xleftarrow{\$}\mathfrak{S}_{2nk}$
$\boldsymbol{f}_{i0},\ldots,\boldsymbol{f}_{i\kappa}\xleftarrow{\$}\mathbb{Z}_q^{2nk}$
$\mu_i,\mu_\times,\mu_+,\rho_i\xleftarrow{\$}R_q$
$m_\times=\mu_1\mu_2,\quad m_+=\mu_1m_2+\mu_2m_1$
$(c_1,d_1)=\mathsf{aCom}\big(\{\pi_{ij}\}_{i,j},\{\boldsymbol{a}\mu_i+\boldsymbol{b}\rho_i+\phi(\boldsymbol{I}'\sum_j 2^j\boldsymbol{f}_{ij})\}_i\big)$
$(c_2,d_2)=\mathsf{aCom}\big(\mu_3,\mu_\times,\mu_+\big)$
$(c_3,d_3)=\mathsf{aCom}\big(\{\pi_{ij}(\boldsymbol{f}_{ij})\}_{i,j},\{\pi_{ij}(\boldsymbol{e}'_{ij})\}_{i,j}\big)$
$(c_4,d_4)=\mathsf{aCom}\big(\mu_\times+m_\times,\mu_++m_+\big)$
$\xrightarrow{\quad c_1,c_2,c_3,c_4\quad}$
$\alpha,\beta\xleftarrow{\$}\mathbb{Z}_q$
$\xleftarrow{\quad\alpha,\beta\quad}$
$\delta_1=\alpha,\quad\delta_2=\alpha,\quad\delta_3=\beta$
$\boldsymbol{g}_{ij}=\pi_{ij}(\boldsymbol{f}_{ij}+\delta_i\boldsymbol{e}'_{ij})$
$(c_5,d_5)=\mathsf{aCom}\big((\beta\mu_\times)+\alpha(\beta\mu_+)+\alpha^2(\mu_3)\big)$
$\xrightarrow{\quad\{\boldsymbol{g}_{ij}\}_{i,j},c_5\quad}$
$b\xleftarrow{\$}\{0,1\}$
$\xleftarrow{\quad b\quad}$
if b=0
$\widetilde{\pi}_{ij}=\pi_{ij}$
$\widetilde{\boldsymbol{y}}_i=\boldsymbol{a}\mu_i+\boldsymbol{b}\rho_i+\phi(\boldsymbol{I}'\sum_j 2^j\boldsymbol{f}_{ij})$
$\widetilde{t}_\times=\mu_\times+m_\times,\quad\widetilde{t}_+=\mu_++m_+,\quad\widetilde{s}_i=\rho_i+\delta_i r_i$
$\widetilde{d}_1=d_1,\quad\widetilde{d}_4=d_4,\quad\widetilde{d}_5=d_5$
$ans=(\{\widetilde{\pi}_{ij}\}_{i,j},\{\widetilde{\boldsymbol{y}}_i\}_i,\widetilde{t}_\times,\widetilde{t}_+,\{\widetilde{s}_i\}_i,\widetilde{d}_1,\widetilde{d}_4,\widetilde{d}_5)$
if b=1
$\widetilde{\boldsymbol{e}}'_{ij}=\pi_{ij}(\boldsymbol{e}'_{ij})$
$\widetilde{\mu}_3=\mu_3,\quad\widetilde{\mu}_\times=\mu_\times,\quad\widetilde{\mu}_+=\mu_+$
$\widetilde{d}_2=d_2,\quad\widetilde{d}_3=d_3,\quad\widetilde{d}_5=d_5$
$ans=(\{\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j},\widetilde{\mu}_3,\widetilde{\mu}_\times,\widetilde{\mu}_+,\widetilde{d}_2,\widetilde{d}_3,\widetilde{d}_5)$
$\xrightarrow{\quad ans\quad}$
if b=0
$1\xleftarrow{?}\mathsf{aVer}\big(c_1,(\{\widetilde{\pi}_{ij}\}_{i,j},\{\widetilde{\boldsymbol{y}}_i\}_i),\widetilde{d}_1\big)$
$1\xleftarrow{?}\mathsf{aVer}\big(c_4,(\widetilde{t}_\times,\widetilde{t}_+),\widetilde{d}_4\big)$
$1\xleftarrow{?}\mathsf{aVer}\big(c_5,\beta\widetilde{t}_\times+\alpha\beta\widetilde{t}_+-\alpha^2\widetilde{t}_3-\beta\widetilde{t}_1\widetilde{t}_2,\widetilde{d}_5\big)$
$\widetilde{\boldsymbol{y}}_i+\delta_i(\boldsymbol{c}_i+\phi(2^\kappa\mathbb{1}_{nk}))-\boldsymbol{b}\widetilde{s}_i-\phi(\boldsymbol{I}'\sum_j 2^j\widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}))\overset{?}{\in}\mathcal{L}(\boldsymbol{a})$
if b=1
$1\xleftarrow{?}\mathsf{aVer}\big(c_2,(\widetilde{\mu}_3,\widetilde{\mu}_\times,\widetilde{\mu}_+),\widetilde{d}_2\big)$
$1\xleftarrow{?}\mathsf{aVer}\big(c_3,(\{\boldsymbol{g}_{ij}-\alpha\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j},\{\widetilde{\boldsymbol{e}}'_{ij}\}_{i,j}),\widetilde{d}_3\big)$
$1\xleftarrow{?}\mathsf{aVer}\big(c_5,(\beta\widetilde{\mu}_\times)+\alpha(\beta\widetilde{\mu}_+)+\alpha^2(\widetilde{\mu}_3),\widetilde{d}_5\big)$
$\widetilde{\boldsymbol{e}}'_{ij}\overset{?}{\in}\mathcal{B}_{nk}$

The binding property of all commitments ensures that openings to the same elements are equal. Therefore we have fixed $\widetilde{\pi}_{ij}$, $\widetilde{\boldsymbol{y}}_i$, $\widetilde{\mu}_3$, $\widetilde{\mu}_\times$, $\widetilde{\mu}_+$, $\widetilde{\boldsymbol{e}}'_{ij}$, $\widetilde{t}_\times$ and $\widetilde{t}_+$. For each pair $(\alpha^{(l)},\beta^{(l)})$ we have $\boldsymbol{g}_{ij}^{(l)}$.

We know that $\widetilde{\boldsymbol{y}}_i + \delta_i^{(l)}(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}_i\widetilde{s}_i^{(l)} - \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l)})) \in \mathcal{L}(\boldsymbol{a})$ and call $\widetilde{t}_i^{(l)}$ to its coordinates. Let l and l' in $\{1,2,3,4,5,6\}$ such that $\Delta_{\delta_i} = \delta_i^{(l)} - \delta_i^{(l')} \neq 0$. Then we will be able to compute valid openings of $\boldsymbol{c}_i$:

$$\begin{aligned}
\boldsymbol{a}\widetilde{t}_i^{(l)} &= \widetilde{\boldsymbol{y}}_i + \delta_i^{(l)}(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s}_i^{(l)} - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l)})) \\
\boldsymbol{a}\widetilde{t}_i^{(l')} &= \widetilde{\boldsymbol{y}}_i + \delta_i^{(l')}(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s}_i^{(l')} - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l')})) \\
\Delta_{\delta_i}\boldsymbol{c}_i &= \boldsymbol{a}(\widetilde{t}_i^{(l)} - \widetilde{t}_i^{(l')}) + \boldsymbol{b}(\widetilde{s}_i^{(l)} - \widetilde{s}_i^{(l')}) + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l)} - \boldsymbol{g}_{ij}^{(l')}) - \Delta_{\delta_i} 2^\kappa \mathbb{1}_{nk}) \\
\boldsymbol{c}_i &= \boldsymbol{a}(\Delta_{\delta_i}^{-1}(\widetilde{t}_i^{(l)} - \widetilde{t}_i^{(l')})) + \boldsymbol{b}(\Delta_{\delta_i}^{-1}(\widetilde{s}_i^{(l)} - \widetilde{s}_i^{(l')})) + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\Delta_{\delta_i}^{-1}(\boldsymbol{g}_{ij}^{(l)} - \boldsymbol{g}_{ij}^{(l')})) - 2^\kappa \mathbb{1}_{nk})
\end{aligned}$$

$$\boldsymbol{g}_{ij}^{(l)} - \delta_i^{(l)}\widetilde{\boldsymbol{e}}'_{ij} = \boldsymbol{g}_{ij}^{(l')} - \delta_i^{(l')}\widetilde{\boldsymbol{e}}'_{ij}$$

$$\begin{aligned}
\widetilde{\boldsymbol{e}}'_{ij} &= \Delta_{\delta_i}^{-1}(\boldsymbol{g}_{ij}^{(l)} - \boldsymbol{g}_{ij}^{(l')}) \\
\boldsymbol{c}_i &= \boldsymbol{a}(\Delta_{\delta_i}^{-1}(\widetilde{t}_i^{(l)} - \widetilde{t}_i^{(l')})) + \boldsymbol{b}(\Delta_{\delta_i}^{-1}(\widetilde{s}_i^{(l)} - \widetilde{s}_i^{(l')})) + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{e}}'_{ij}) - 2^\kappa \mathbb{1}_{nk})
\end{aligned}$$

As these elements come from accepted answers we know that $\widetilde{\boldsymbol{e}}'_{ij} \in \mathcal{B}_{nk} \subset \{0,1\}^{2nk}$ and therefore $\phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{e}}'_{ij}) - 2^\kappa \mathbb{1}_{nk})$ has norm smaller than 2^κ. This implies that $(\Delta_{\delta_i}^{-1}(\widetilde{t}_i^{(l)} - \widetilde{t}_i^{(l')}), \Delta_{\delta_i}^{-1}(\widetilde{s}_i^{(l)} - \widetilde{s}_i^{(l')}), \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{e}}'_{ij}) - 2^\kappa \mathbb{1}_{nk}))$ are valid openings.

We know that these openings do not depend on (l) and (l'), as the commitment scheme is binding. Therefore we can call them $(\overline{m}_i = \Delta_{\delta_i}^{-1}(\widetilde{t}_i^{(l)} - \widetilde{t}_i^{(l')}), \widetilde{r}_i = \Delta_{\delta_i}^{-1}(\widetilde{s}_i^{(l)} - \widetilde{s}_i^{(l')}), \widetilde{\boldsymbol{e}}_i = \phi(\boldsymbol{I}' \sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{e}}'_{ij}) - 2^\kappa \mathbb{1}_{nk}))$. It only remains to prove that $\overline{m}_3 = \overline{m}_1 \overline{m}_2$.

We can define $\overline{\mu}_i^{(l)} = \widetilde{t}_i^{(l)} - \delta_i^{(l)}\overline{m}_i$ and $\widetilde{\rho}_i^{(l)} = \widetilde{s}_i^{(l)} - \delta_i^{(l)}\widetilde{r}_i$.

Claim. This newly defined elements do not depend on l and we can omit the superindex (l) as $\overline{\mu}_i = \overline{\mu}_i^{(l)} = \overline{\mu}_i^{(l')}$ and $\widetilde{\rho}_i = \widetilde{\rho}_i^{(l)} = \widetilde{\rho}_i^{(l')}$ for any pair l and l'.

Proof. Assume that we have l and l' such that $\overline{\mu}_i^{(l)} \neq \overline{\mu}_i^{(l')}$ or $\widetilde{\rho}_i^{(l)} \neq \widetilde{\rho}_i^{(l')}$.

We could rewrite the expression of $\boldsymbol{a}\widetilde{t}_i^{(l)}$ in terms of this new variables.

$$\begin{aligned}
\boldsymbol{a}\widetilde{t}_i^{(l)} &= \widetilde{\boldsymbol{y}}_i + \delta_i^{(l)}(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk})) - \boldsymbol{b}\widetilde{s}_i^{(l)} - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l)})) \\
\boldsymbol{a}(\overline{\mu}_i^{(l)} + \delta_i^{(l)}\overline{m}_i) &= \widetilde{\boldsymbol{y}}_i + \delta_i^{(l)}(\boldsymbol{a}\overline{m}_i + \boldsymbol{b}\widetilde{r}_i + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{e}}'_{ij}))) \\
&\quad - \boldsymbol{b}(\widetilde{\rho}_i^{(l)} + \delta_i^{(l)}\widetilde{r}_i) - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l)})) \\
\boldsymbol{a}\overline{\mu}_i^{(l)} + \boldsymbol{b}\widetilde{\rho}_i^{(l)} &= \widetilde{\boldsymbol{y}}_i - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\boldsymbol{g}_{ij}^{(l)} - \delta_i^{(l)}\widetilde{\boldsymbol{e}}'_{ij}))
\end{aligned}$$

Notice that $\boldsymbol{g}_{ij}^{(l)} - \delta_i^{(l)}\widetilde{\boldsymbol{e}}'_{ij}$ is open to $\widetilde{\boldsymbol{f}}_{ij}$, that was commited before $\alpha^{(l)}$ and $\beta^{(l)}$ were chosen and therefore does not depend on l:

$$\boldsymbol{a}\overline{\mu}_i^{(l)} + \boldsymbol{b}\widetilde{\rho}_i^{(l)} = \widetilde{\boldsymbol{y}}_i - \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widetilde{\pi}_{ij}^{-1}(\widetilde{\boldsymbol{f}}_{ij})).$$

Since the right handside does not depend on l nor l' from two equations we get:

$$\boldsymbol{a}(\overline{\mu}_i^{(l)} - \overline{\mu}_i^{(l')}) + \boldsymbol{b}(\widetilde{\rho}_i^{(l)} - \widetilde{\rho}_i^{(l')}) = 0. \tag{4}$$

We can apply a similar argument as we do in appendix A to prove that the commitment was binding. In this particular case there exist nonzero elements satisfying equation (4) with probability:

$$\Pr_{(\boldsymbol{a},\boldsymbol{b})}\Big[\exists \mu,\rho \text{ (not both 0)}\Big|\boldsymbol{a}\mu+\boldsymbol{b}\rho=0\Big] \leq \frac{q^{2n}}{q^{kn/2}} \in negl(1^{\lambda}).$$

Then both differences have to be 0 and the elements do not depend on l. □

We can also define $\widetilde{m}_{\times} = \widetilde{t}_{\times} - \widetilde{\mu}_{\times}, \widetilde{m}_{+} = \widetilde{t}_{+} - \widetilde{\mu}_{+}$. This time there is no dependence with l as the elements were committed previously. With all these discussions now we are ready to prove the relation $\overline{m}_3 = \overline{m}_1\overline{m}_2$.

$$\begin{aligned}
&{\alpha^{(l)}}^2(\widetilde{\mu}_3) + \alpha^{(l)}(\beta^{(l)}\widetilde{\mu}_{+}) + (\beta^{(l)}\widetilde{\mu}_{\times}) = \beta^{(l)}\widetilde{t}_{\times} + \alpha^{(l)}\beta^{(l)}\widetilde{t}_{+} + {\alpha^{(l)}}^2\widetilde{t}_3 - \beta^{(l)}\widetilde{t}_1\widetilde{t}_2 \\
&= \begin{pmatrix} \beta^{(l)}(\widetilde{\mu}_{\times}+\widetilde{m}_{\times}) + \alpha^{(l)}\beta^{(l)}(\widetilde{\mu}_{+}+\widetilde{m}_{+}) + {\alpha^{(l)}}^2(\overline{\mu}_3+\beta^{(l)}\overline{m}_3) \\ -\beta^{(l)}(\overline{\mu}_1+\alpha^{(l)}\overline{m}_1)(\overline{\mu}_2+\alpha^{(l)}\overline{m}_2) \end{pmatrix} \\
&\begin{pmatrix} {\alpha^{(l)}}^2(\widetilde{\mu}_3-\overline{\mu}_3+\beta^{(l)}(\overline{m}_1\overline{m}_2-\overline{m}_3)) \\ +\alpha^{(l)}(\beta^{(l)}(\overline{\mu}_1\overline{m}_2+\overline{\mu}_2\overline{m}_1-\widetilde{m}_{+})) \\ +(\beta^{(l)}(\overline{\mu}_1\overline{\mu}_2-\widetilde{m}_{\times})) \end{pmatrix} = 0
\end{aligned}$$

If we restrict ourselves to the cases with equal β we can see this expression as a two degree polynomial in α (the coefficients were committed before the challenges were chosen), that is equal to 0 for three evaluations $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$ or $\alpha^{(4)}, \alpha^{(5)}, \alpha^{(6)}$. This implies that it is the 0 polynomial and that all its coefficients are 0, providing us with the equalities $\widetilde{\mu}_3 - \overline{\mu}_3 + \beta^{(l)}(\overline{m}_1\overline{m}_2 - \overline{m}_3) = 0$. Given that this equality is satisfied by two different β we have that $(\beta^{(l)} - \beta^{(l')})(\overline{m}_1\overline{m}_2 - \overline{m}_3) = 0$ and finally $\overline{m}_3 = \overline{m}_1\overline{m}_2$ as we wanted to prove, the relation holds for the extracted witness.

Zero-Knowledge :

Case $b = 0$

$\widehat{t}_i, \widehat{s}_i \xleftarrow{\$} R_q, \quad \widehat{t}_{\times}, \widehat{t}_{+} \xleftarrow{\$} R_q$

$\widehat{\boldsymbol{g}}_{ij} \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \widehat{\pi}_{ij} \xleftarrow{\$} \mathfrak{S}_{2nk}$

$$\begin{aligned}
c_1 = \mathsf{aCom}\Big(\{\widehat{\pi}_{ij}\}_{i,j}, \{\boldsymbol{a}\widehat{t_i} + \boldsymbol{b}\widehat{s_i} \\
+ \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij})) \\
- \delta_i(\boldsymbol{c}_i + \phi(2^{\kappa}\mathbb{1}_{nk}))\}_i\Big)
\end{aligned}$$

$c_4 = \mathsf{aCom}(\widehat{t_{\times}}, \widehat{t_{+}})$

$c_5 = \mathsf{aCom}(\beta\widehat{t_{\times}} + \alpha\beta\widehat{t_{+}} + \alpha^2\widehat{t_3} - \beta\widehat{t_1}\widehat{t_2})$

$\mathcal{P}$ reveals $\{\widehat{\boldsymbol{g}}_{ij}\}_{i,j}, \{\widetilde{\pi}_{ij} = \widehat{\pi}_{ij}\}_{i,j}, \{\widetilde{\boldsymbol{y}}_i = \boldsymbol{a}\widehat{t_i} + \boldsymbol{b}\widehat{s_i} + \phi(\boldsymbol{I}' \sum_j 2^j \widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij})) - \delta_i(\boldsymbol{c}_i + \phi(2^{\kappa}\mathbb{1}_{nk}))\}_i, \widetilde{t}_{\times}, \widetilde{t}_{+}, \{\widetilde{s}_i\}_i$.

Case $b = 1$

$\widehat{\mu}_3, \widehat{\mu}_{\times}, \widehat{\mu}_{+} \xleftarrow{\$} R_q, \quad \widehat{\boldsymbol{e}}'_{ij} \xleftarrow{\$} \mathcal{B}_{nk}$

$\widehat{\boldsymbol{f}}_{ij} \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \widehat{\pi}_{ij} \xleftarrow{\$} \mathfrak{S}_{2nk}$

$c_2 = \mathsf{aCom}(\widehat{\mu}_3, \widehat{\mu}_{\times}, \widehat{\mu}_{+})$

$c_3 = \mathsf{aCom}(\{\widehat{\pi}_{ij}(\widehat{\boldsymbol{f}}_{ij})\}_{i,j}, \{\widehat{\pi}_{ij}(\widehat{\boldsymbol{e}}'_{ij})\}_{i,j})$

$c_5 = \mathsf{aCom}(\beta\widehat{\mu}_{\times} + \alpha\beta\widehat{\mu}_{+} + \alpha^2\widehat{\mu}_3)$

$\widehat{\boldsymbol{g}}_{ij} = \widehat{\pi}_{ij}(\widehat{\boldsymbol{f}}_{ij} + \delta_i\widehat{\boldsymbol{e}}'_{ij})$

$\mathcal{P}$ reveals $\{\widehat{\boldsymbol{g}}_{ij}\}_{i,j}, \{\widetilde{\boldsymbol{e}}'_{ij} = \widehat{\pi}_{ij}(\widehat{\boldsymbol{e}}'_{ij})\}_{i,j}, \widetilde{\mu}_3 = \widehat{\mu}_3, \widetilde{\mu}_{\times} = \widehat{\mu}_{\times}, \widetilde{\mu}_{+} = \widehat{\mu}_{+}$.

Indistinguishable from a real conversation with the same $\pi_{ij} = \widehat{\pi}_{ij}$ and where $\mu_i = \widehat{t}_i - \delta_i m_i$, $\mu_\times = \widehat{t}_\times - m_\times$, $\mu_+ = \widehat{t}_+ - m_+$, $\rho_i = \widehat{s}_i - \delta_i r_i$ and $\boldsymbol{f}_{ij} = \widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij}) - \delta_i \boldsymbol{e}'_{ij}$.

$$
\begin{aligned}
\boldsymbol{g}_{ij} &= \pi_{ij}(\boldsymbol{f}_{ij} + \delta_i \boldsymbol{e}'_{ij}) \\
&= \pi_{ij}(\widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij})) \\
&= \widehat{\boldsymbol{g}}_{ij}
\end{aligned}
$$

$$
\begin{aligned}
&\boldsymbol{a}\mu_i + \boldsymbol{b}\rho_i + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \boldsymbol{f}_{ij}) = \\
&= \boldsymbol{a}(\widehat{t}_i - \delta_i m_i) + \boldsymbol{b}(\widehat{s}_i - \delta_i r_i) \\
&\quad + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j (\widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij}) - \delta_i \boldsymbol{e}'_{ij})) \\
&= \boldsymbol{a}\widehat{t}_i + \boldsymbol{b}\widehat{s}_i + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij})) \\
&\quad - \delta_i(\boldsymbol{a}m_i + \boldsymbol{b}r_i + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \boldsymbol{e}'_{ij})) \\
&= \boldsymbol{a}\widehat{t}_i + \boldsymbol{b}\widehat{s}_i + \phi(\boldsymbol{I}' \textstyle\sum_j 2^j \widehat{\pi}_{ij}^{-1}(\widehat{\boldsymbol{g}}_{ij})) \\
&\quad - \delta_i(\boldsymbol{c}_i + \phi(2^\kappa \mathbb{1}_{nk}))
\end{aligned}
$$

Equivalent to an honest conversation with equal $\mu_3 = \widehat{\mu}_3, \mu_\times = \widehat{\mu}_\times, \mu_+ = \widehat{\mu}_+$ and were π_{ij} is such that $\pi_{ij}(\boldsymbol{e}'_{ij}) = \widehat{\pi}_{ij}(\widehat{\boldsymbol{e}}'_{ij})$ and $\boldsymbol{f}_{ij} = \pi_{ij}^{-1}(\widehat{\pi}_{ij}(\widehat{\boldsymbol{f}}_{ij}))$.

$$
\begin{aligned}
\boldsymbol{g}_{ij} &= \pi_{ij}(\boldsymbol{f}_{ij} + \delta_i \boldsymbol{e}'_{ij}) \\
&= \pi_{ij}(\pi_{ij}^{-1}(\widehat{\pi}_{ij}(\widehat{\boldsymbol{f}}_{ij}))) + \delta_i \widehat{\pi}_{ij}(\widehat{\boldsymbol{e}}'_{ij}) \\
&= \widehat{\pi}_{ij}(\widehat{\boldsymbol{f}}_{ij} + \delta_i \widehat{\boldsymbol{e}}'_{ij}) \\
&= \widehat{\boldsymbol{g}}_{ij}
\end{aligned}
$$

Notice again that simulated conversations follow the proper distributions.

4 Conclusions

To sum up, we have proposed a new protocol for proving linear and multiplicative relations between secret elements hidden inside RLWE samples. The direct applications are new Zero-Knowledge Proofs for proving knowledge of the evaluations of arithmetic circuits with committed inputs.

Xie *et al.* [26] proposed exact Stern-based proofs for lattice-based commitments, but they had a factor $\log(q)^2$ overhead to the messages. We are able to build exact proofs with a constant factor overhead, thus further improving efficiency. Besides that, our scheme is compatible with the techniques that reduce the soundness error to $1/2$, so that it requires less repetitions to achieve the same confidence level. Several constructions using Xie *et al.* Zero-Knowledge Proofs for relations between committed messages (as the recently presented lattice-based Attributed Based Signature scheme for unbounded circuits [13]) could benefit from this improvement directly replacing their proofs with our proposal.

Our scheme can be directly compared to the one proposed by Benhamouda *et al.* [3]. While their proofs do not require repetitions our proposal achieves the same security level with smaller commitments, as we do not generalize the definition of opening of the commitment. It is also more robust and easy to implement, as in our protocol the prover is always able to answer with a valid response, without any abort probability. And finally we require a significantly smaller modulus q for our construction to be sound. This implies that our schemes can still be

used as a building block in larger protocols where it would be much less efficient (or even unfeasible) to increase the modulus q for the whole protocol. That could be the case for electronic voting, where heavy ZKPoK could be performed on some servers but votes have to be encrypted using resource constrained voting devices. More detailed comparisons and cost analysis can be found in appendix C.

We think that these properties represent a major improvement on constructions based on Stern protocol and might be useful in applications that heavily require this kind of proofs, as electronic voting. We think that our ideas are flexible enough to be applied as building blocks for other different constructions besides commitment schemes. We consider that it would be interesting to implement the protocol presented in this paper and leave it as future work.

References

1. Aguilar Melchor, C., Cayrel, P.L., Gaborit, P., Laguillaumie, F.: A new efficient threshold ring signature scheme based on coding theory. IEEE Transactions on Information Theory **57**(7), 4833–4842 (July 2011), DOI: 10.1109/TIT.2011.2145950
2. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More efficient commitments from structured lattice assumptions. In: Catalano, D., De Prisco, R. (eds.) Security and Cryptography for Networks. pp. 368–385. Springer International Publishing, Cham (2018), DOI: 10.1007/978-3-319-98113-0_20
3. Benhamouda, F., Krenn, S., Lyubashevsky, V., Pietrzak, K.: Efficient zero-knowledge proofs for commitments from learning with errors over rings. In: Pernul, G., Ryan, P.Y.A., Weippl, E.R. (eds.) ESORICS 2015, Part I. LNCS, vol. 9326, pp. 305–325. Springer, Heidelberg, Germany, Vienna, Austria (Sep 21–25, 2015), DOI: 10.1007/978-3-319-24174-6_16
4. Bettaieb, S., Schrek, J.: Improved lattice-based threshold ring signature scheme. In: Gaborit, P. (ed.) Post-Quantum Cryptography. pp. 34–51. Springer Berlin Heidelberg, Berlin, Heidelberg (2013), DOI: 10.1007/978-3-642-38616-9_3
5. Bootle, J., Lyubashevsky, V., Seiler, G.: Algebraic techniques for short(er) exact lattice-based zero-knowledge proofs. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part I. LNCS, vol. 11692, pp. 176–202. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019), DOI: 10.1007/978-3-030-26948-7_7
6. Cayrel, P.L., Gaborit, P., Prouff, E.: Secure implementation of the stern authentication and signature schemes for low-resource devices. In: Grimaud, G., Standaert, F.X. (eds.) Smart Card Research and Advanced Applications. pp. 191–205. Springer Berlin Heidelberg, Berlin, Heidelberg (2008), DOI: 10.1007/978-3-540-85893-5_14
7. Cayrel, P.L., Lindner, R., Rückert, M., Silva, R.: Improved zero-knowledge identification with lattices. In: Heng, S.H., Kurosawa, K. (eds.) ProvSec 2010. LNCS, vol. 6402, pp. 1–17. Springer, Heidelberg, Germany, Malacca, Malaysia (Oct 13–15, 2010)
8. Cayrel, P.L., Lindner, R., Rückert, M., Silva, R.: A lattice-based threshold ring signature scheme. In: Abdalla, M., Barreto, P.S.L.M. (eds.) LATINCRYPT 2010. LNCS, vol. 6212, pp. 255–272. Springer, Heidelberg, Germany, Puebla, Mexico (Aug 8–11, 2010)

9. Cayrel, P.L., Véron, P., Alaoui, S.M.E.Y.: A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 171–186. Springer, Heidelberg, Germany, Waterloo, Ontario, Canada (Aug 12–13, 2011), DOI: 10.1007/978-3-642-19574-7_12
10. Gaborit, P., Girault, M.: Lightweight code-based identification and signature. In: 2007 IEEE International Symposium on Information Theory. pp. 191–195 (June 2007), DOI: 10.1109/ISIT.2007.4557225
11. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2013), DOI: 10.1007/978-3-642-40041-4_5
12. Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 663–680. Springer, Heidelberg, Germany, Beijing, China (Dec 2–6, 2012), DOI: 10.1007/978-3-642-34961-4_40
13. Kaafarani, A.E., Katsumata, S.: Attribute-based signatures for unbounded circuits in the ROM and efficient instantiations from lattices. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part II. LNCS, vol. 10770, pp. 89–119. Springer, Heidelberg, Germany, Rio de Janeiro, Brazil (Mar 25–29, 2018), DOI: 10.1007/978-3-319-76581-5_4
14. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 372–389. Springer, Heidelberg, Germany, Melbourne, Australia (Dec 7–11, 2008), DOI: 10.1007/978-3-540-89255-7_23
15. Libert, B., Ling, S., Nguyen, K., Wang, H.: Lattice-based zero-knowledge arguments for integer relations. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part II. LNCS, vol. 10992, pp. 700–732. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2018), DOI: 10.1007/978-3-319-96881-0_24
16. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Zero-knowledge arguments for matrix–vector relations and lattice-based group encryption. Theoretical Computer Science **759**, 72 – 97 (2019), DOI: 10.1016/j.tcs.2019.01.003
17. Ling, S., Nguyen, K., Stehlé, D., Wang, H.: Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 107–124. Springer, Heidelberg, Germany, Nara, Japan (Feb 26 – Mar 1, 2013), DOI: 10.1007/978-3-642-36362-7_8
18. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg, Germany, French Riviera (May 30 – Jun 3, 2010), DOI: 10.1007/978-3-642-13190-5_1
19. Peikert, C., et al.: A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science **10**(4), 283–424 (2016), DOI: 10.1561/0400000074
20. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997), DOI: 10.1137/S0097539795293172
21. Silva, R., Cayrel, P.L., Lindner, R.: A lattice-based batch identification scheme. In: 2011 IEEE Information Theory Workshop. pp. 215–219 (Oct 2011), DOI: 10.1109/ITW.2011.6089381

22. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg, Germany, Tokyo, Japan (Dec 6–10, 2009), DOI: 10.1007/978-3-642-10366-7_36
23. Stern, J.: A new paradigm for public key identification. IEEE Transactions on Information Theory **42**(6), 1757–1768 (Nov 1996), DOI: 10.1109/18.556672
24. Stern, J.: A new identification scheme based on syndrome decoding. In: Stinson, D.R. (ed.) CRYPTO'93. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 22–26, 1994), DOI: 10.1007/3-540-48329-2_2
25. Véron, P.: Improved identification schemes based on error-correcting codes. Applicable Algebra in Engineering, Communication and Computing **8**(1), 57–69 (Jan 1997), DOI: 10.1007/s002000050053
26. Xie, X., Xue, R., Wang, M.: Zero knowledge proofs from ring-LWE. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 13. LNCS, vol. 8257, pp. 57–73. Springer, Heidelberg, Germany, Paraty, Brazil (Nov 20–22, 2013), DOI: 10.1007/978-3-319-02937-5_4
27. Yang, R., Au, M.H., Zhang, Z., Xu, Q., Yu, Z., Whyte, W.: Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part I. LNCS, vol. 11692, pp. 147–175. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2019), DOI: 10.1007/978-3-030-26948-7_6

A Commitment security proof

Proposition 2. *If $n \geq 256$, $\gamma \geq 3$ and $k \geq \frac{8\gamma+4}{2\gamma-5}$ then the following is a secure commitment scheme under the assumption that RLWE is hard.*

- Gen*: the generator algorithm takes a security parameter 1^λ and outputs a public key $pk = (\boldsymbol{a}, \boldsymbol{b}) \in \left(R_q^k\right)^2$, where $R_q = \mathbb{Z}_q[x] / \langle x^n + 1 \rangle$ and k are defined so that the difficulty of solving the RLWE problem is related to 1^λ. In particular the size of n is also related to 1^λ.*
  $(\boldsymbol{a}, \boldsymbol{b}) \xleftarrow{\$} \mathsf{Gen}\left(1^\lambda\right)$
- Com*: the commitment algorithm takes as input a message $m \in R_q$ and a public key $pk = (\boldsymbol{a}, \boldsymbol{b})$ and produces a commitment $\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}$ and an opening $d = (m, r, \boldsymbol{e})$, where $r \xleftarrow{\$} R_q$ and $\boldsymbol{e} \xleftarrow{\$} \chi^{nk}$ conditioned to have infinity norm smaller than $n = 2^\kappa$.*
  $(\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}, d = (m, r, \boldsymbol{e})) \xleftarrow{\$} \mathsf{Com}(m; pk = (\boldsymbol{a}, \boldsymbol{b}))$
- Ver*: the verification algorithm takes as input a commitment $\boldsymbol{c}$, a message m, an opening $d = (m, r, \boldsymbol{e})$ and a public key $pk = (\boldsymbol{a}, \boldsymbol{b})$ and accepts, 1, if $(\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}) \wedge (\|\boldsymbol{e}\|_\infty < 2^\kappa)$, or rejects, 0, otherwise.*
  $\mathsf{Ver} : \{(\boldsymbol{c}, m, d; pk)\} \to \{0, 1\}$

Proof. We can check that all properties are verified.

- **Correctness**: it immediate follows by the definitions of Com and Ver.
- **Binding**: a commitment can only be correctly opened to one message.
  It is perfectly binding with overwhelming probability as:

$$1 \leftarrow \mathsf{Ver}(\boldsymbol{c}, m', d'; pk) \wedge 1 \leftarrow \mathsf{Ver}(\boldsymbol{c}, m'', d''; pk) \implies m' = m''$$

  We redo here the proof from [3] since our simpler verification algorithm implies that we require less restrictions on the parameters.
  Two accepted openings to the same commitment would be:

$$\boldsymbol{c} = \boldsymbol{a}m' + \boldsymbol{b}r' + \boldsymbol{e}'$$
$$\boldsymbol{c} = \boldsymbol{a}m'' + \boldsymbol{b}r'' + \boldsymbol{e}''$$

  Therefore if $m' \neq m''$ we have that $\boldsymbol{a}(m' - m'') + \boldsymbol{b}(r' - r'') + (\boldsymbol{e}' - \boldsymbol{e}'') = 0$. If $q \equiv 3 \mod 8$, with overwhelming probability over the choice of $\boldsymbol{a}$ and $\boldsymbol{b}$, there are no $m, r \in R_q$ and $\boldsymbol{e} \in R_q^k$ small such that $\boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e} = 0$ holds and $m \neq 0$.

  We bound the probability that this solution exists. For a fixed m, r and $\boldsymbol{e}$ we count the proportion of pairs $(\boldsymbol{a}, \boldsymbol{b})$ for which the equality holds. In order to estimate the overall probability of choosing a pair $(\boldsymbol{a}, \boldsymbol{b})$ such that there exists a solution we use a union bound adding up all previous probabilities. We finally see that it is negligible if parameters are carefully selected.

  Fixed m, r and $\boldsymbol{e}$ for each $\boldsymbol{b}$ we have $\boldsymbol{a}m = -\boldsymbol{b}r - \boldsymbol{e}$. In each component $a_j m = -b_j r - e_j$. $q \equiv 3 \mod 8$ implies that $x^n + 1$ splits into two irreducible

polynomials $p_1(x), p_2(x)$ of degree $n/2$ (lemma 3 in [22]). We know that $m \not\equiv 0 \mod x^n + 1$, therefore $m \not\equiv 0 \mod p_1(x)$ or $m \not\equiv 0 \mod p_2(x)$.

In either case we know that $a_j m$ takes at least $q^{n/2}$ different values. There are $q^{n/2}$ equivalence classes $\mod p_i(x)$ and only one of them is $-b_j r - e_j \mod p_i(x)$, therefore at most $1/q^{n/2}$ of the possible a_j hold the equation. As this is independently true for each j we have that the probability of $(\boldsymbol{a}, \boldsymbol{b})$ to fit the equation for these particular m, r and e is at most $1/q^{nk/2}$.

If we want to consider the possibility that there exists a solution we can bound this probability with a union bound. There are q^n possible m, q^n possible r and $(4n)^{nk}$ possible $\boldsymbol{e}$. Therefore if $(\boldsymbol{a}, \boldsymbol{b}) \xleftarrow{\$} \mathrm{Gen}(1^\lambda)$:

$$\Pr_{(\boldsymbol{a},\boldsymbol{b})}\left[\exists m, r, \boldsymbol{e} \middle| \begin{array}{c} \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e} = 0 \\ \wedge \left\|\boldsymbol{e}\right\|_\infty \leq n \end{array}\right] \leq \frac{q^{2n}(4n)^{nk}}{q^{nk/2}} \in negl(1^\lambda).$$

The condition $n \geq 256$ implies $(4n) \leq n^{5/4}$:

$$\begin{aligned} \frac{q^{2n}(4n)^{nk}}{q^{nk/2}} &\leq \frac{q^{2n} n^{5nk/4}}{q^{nk/2}} \\ &\leq \frac{q^{2n} q^{5nk/(4\gamma)}}{q^{nk/2}} \\ &= q^{n(2+5k/(4\gamma)-k/2)} \end{aligned}$$

because $\gamma \geq 3$ and $k \geq \frac{8\gamma+4}{2\gamma-5} \geq \frac{8\gamma}{2\gamma-5}$ we know that $2 + 5k/(4\gamma) - k/2 \leq 0$:

$$q^{n(2+5k/(4\gamma)-k/2)} \leq n^{n\gamma(2+5k/(4\gamma)-k/2)}$$

because $\gamma \geq 3$ and $k \geq \frac{8\gamma+4}{2\gamma-5}$ we know that $\gamma(2 + 5k/(4\gamma) - k/2) \leq -1$:

$$\begin{aligned} n^{n\gamma(2+5k/(4\gamma)-k/2)} &\leq n^{-n} = 2^{-n\kappa} \\ &\leq \frac{1}{2^n} \end{aligned}$$

– **Hiding**: a well constructed commitment $\boldsymbol{c}$ does not leak any relevant information about the message m.

It is computationally hiding as $\boldsymbol{b}r + \boldsymbol{e}$ are k RLWE samples, indistinguishable from independent uniformly random polynomials under the $\mathsf{RLWE}_{n,q,\chi}$ assumption. Any adversary able to break the hiding property would then also be able to solve the decisional $\mathsf{RLWE}_{n,q,\chi}$. Notice that the probability that $\boldsymbol{e} \xleftarrow{\$} \chi^{nk}$ has $\left\|\boldsymbol{e}\right\|_\infty > n$ is negligible and then original and conditioned probability distributions are statistically indistinguishable.

□

B Soundness extractor

Let $\omega \in \Omega$ be the random coins used by the prover in its interaction with the verifier. We call $T(\omega)$ to the execution tree of all possible interactions between $\widetilde{\mathcal{P}}$ and $\mathcal{V}$ depending on the verifier challenges. Many authors [9] that face similar problems simply argue that a probability larger than $\left(\frac{q+1}{2q}\right)^{\delta} + \epsilon$ implies that there is a node with at least $q+2$ accepted answers, meaning that there exist c_1, c_2, two α, α' and $\boldsymbol{g}_j, \boldsymbol{g}'_j$ that induce accepted answers for both $b = 0$ and $b = 1$, from which it is possible to extract a witness.

However, merely proving existence implies that the extractor should explore the whole tree rewinding the prover $\widetilde{\mathcal{P}}$ until he finds this particular node. It is possible to do so in polynomial-time if q is polynomial in the security parameter and the number of nodes in $T(\omega)$ is $\mathcal{O}(q^{\delta})$, but is very inefficient and provides us bounds $\mathcal{O}(q^{\delta}/\epsilon)$ that are far from tight.

We prefer to analyze it as Stern did in an extension of its original paper [23], that gives us a more detailed insight and requires at most an expected number of $\mathcal{O}(1/\epsilon^3)$ attempts to find such a node and extract a witness. For this to be true we have to assume that q is large enough so that $\log\left(\frac{q}{q+1}\right) > -1/9$ (which only implies $q \geq 13$).

We start defining a subset of the possible random coins:

$$X = \left\{ \omega \in \Omega \quad \middle| \quad T(\omega) \text{ has at least } (q+1)^{\delta} + \frac{\epsilon}{2}(2q)^{\delta} \text{ branches at level } \delta \right\}$$

Claim. X has probability at least $\epsilon/2$.

Proof. Assume $\Pr[X] < \frac{\epsilon}{2}$. Then we arrive at a contradiction with the fact that $\widetilde{\mathcal{P}}$ has a success probability of more than $\left(\frac{q+1}{2q}\right)^{\delta} + \epsilon$.

$$\begin{aligned}
\Pr\left[\widetilde{\mathcal{P}}(\omega)\right] &= \Pr\left[\widetilde{\mathcal{P}}(\omega)\middle|\omega \in X\right]\Pr\left[X\right] + \Pr\left[\widetilde{\mathcal{P}}(\omega)\middle|\omega \notin X\right]\Pr\left[\Omega \setminus X\right] \\
&\leq \Pr\left[X\right] + \Pr\left[\widetilde{\mathcal{P}}(\omega)\middle|\omega \notin X\right]
\end{aligned}$$

We are under the assumption of $\Pr[X] < \epsilon/2$:

$$< \frac{\epsilon}{2} + \Pr\left[\widetilde{\mathcal{P}}(\omega)\middle|\omega \notin X\right]$$

If $\omega \notin X$ there are less than $(q+1)^{\delta} + \frac{\epsilon}{2}(2q)^{\delta}$ branches and $(2q)^{\delta}$ possible challenges:

$$\begin{aligned}
&< \frac{\epsilon}{2} + \left(\frac{q+1}{2q}\right)^{\delta} + \frac{\epsilon}{2}\left(\frac{2q}{2q}\right)^{\delta} \\
&= \left(\frac{q+1}{2q}\right)^{\delta} + \epsilon
\end{aligned}$$

And we have found the contradiction. Therefore $\Pr[X] \geq \epsilon/2$. □

From now on consider $T(\omega)$ with $\omega \in X$. For any index $0 \leq d \leq \delta$ we denote by n_d the number of vertices at level d, and for $0 \leq d < \delta$ we define $\gamma_d = n_{d+1}/n_d$.

$$\prod_{d=0}^{\delta-1} \gamma_d \geq (q+1)^\delta + \frac{\epsilon}{2}(2q)^\delta$$

Taking binary logarithms:

$$\begin{aligned}\sum_{d=0}^{\delta-1} \log(\gamma_d) &\geq \log\left((q+1)^\delta + \frac{\epsilon}{2}(2q)^\delta\right) \\ &\geq \log\left(\left(1-\frac{\epsilon}{2}\right)(q+1)^\delta + \frac{\epsilon}{2}(2q)^\delta\right)\end{aligned}$$

By convexity of the log function:

$$\geq \delta\left(\left(1-\frac{\epsilon}{2}\right)\log(q+1) + \frac{\epsilon}{2}\log(2q)\right)$$

This implies that there exists an $0 \leq i \leq \delta - 1$ such that:

$$\begin{aligned}\log(\gamma_i) &\geq \left(1-\frac{\epsilon}{2}\right)\log(q+1) + \frac{\epsilon}{2}\log(2q) \\ &= \log(q+1) + \frac{\epsilon}{2}\left(1 + \log\left(\frac{q}{q+1}\right)\right)\end{aligned}$$

Given that $\log\left(\frac{q}{q+1}\right) \geq -1/9$:

$$\geq \log(q+1) + \frac{4\epsilon}{9}$$

Undoing logarithms:

$$\begin{aligned}\gamma_i &\geq 2^{\log(q+1)+4\epsilon/9} \\ &= (q+1)2^{4\epsilon/9} \\ &\geq (q+1)(1+\frac{4\epsilon}{9}\ln(2)) \\ &\geq (q+1) + \frac{8(q+1)\epsilon}{27} \\ &\geq (q+1) + \frac{8(q-1)\epsilon}{27}\end{aligned}$$

If we define $n_{i,\leq q+1}$ as the number of nodes on level i that have less or equal than $q+1$ children and $n_{i,>q+1}$ as the number of nodes on level i that have more than $q+1$ children we can also bound γ_i:

$$\begin{aligned}\gamma_i &\leq \frac{(q+1)n_{i,\leq q+1} + (2q)n_{i,>q+1}}{n_{i,\leq q+1} + n_{i,>q+1}} \\ &= (q+1) + (q-1)\frac{n_{i,>q+1}}{n_{i,\leq q+1} + n_{i,>q+1}}\end{aligned}$$

Combining all we have:

$$(q+1) + \frac{8(q-1)\epsilon}{27} \leq (q+1) + (q-1)\frac{n_{i,>q+1}}{n_{i,\leq q+1} + n_{i,>q+1}}$$
$$\frac{8\epsilon}{27} \leq \frac{n_{i,>q+1}}{n_{i,\leq q+1} + n_{i,>q+1}}$$

That is, the fraction of nodes with $q+2$ children or more is larger than $8\epsilon/27$.

Therefore, we know that ω belongs to X with probability at least $\epsilon/2$. We know that $T(\omega)$ has at least $(q+1)^\delta + \epsilon/2(2q)^\delta$ branches, that is, the probability of choosing a successful branch is $\left(\frac{q+1}{2q}\right)^\delta + \frac{\epsilon}{2}$. Once we have chosen at random a successful branch, if we look at its level i the probability of finding a node with at least $q+2$ children is at least $8\epsilon/27$. Combining all these probabilities we have that the probability of a success is greater than $(\epsilon/2)(\epsilon/2)(8\epsilon/27) = 2(\epsilon/3)^3$.

C Comparisons with other proposals

In this appendix we compare our proposal of Zero-Knowledge proofs for commitments with those presented by Xie *et al.* [26] and Benhamouda *et al.* [3]. All these commitments are adaptations of the LPN commitment scheme of Jain *et al.* [12] to the RLWE problem.

We first compare the size of the commitments (table 1). Benhamouda *et al.* directly adapt the structure from [12], and we use their same notation for commiting to a polynomial of degree n with coefficients in $\mathbb{Z}_q$. The commitment is a vector of k polynomials. Xie *et al.* do not commit to a single polynomial but to l polynomials of smaller degree d. Their commitment is made of m polynomials of degree d, but as their construction requires m to be linear in l, the size is asymptotically the same.

Table 1: Commitment size

	Xie *et al.*	Benhamouda *et al.*	our proposal
Commitment Size (in bits)	$md \log q$	$kn \log q$	$kn \log q$

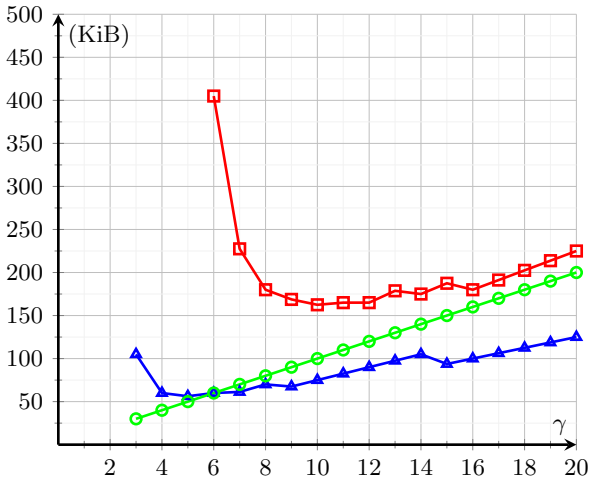
In order to be able to relate these sizes we have to compare the restrictions on the parameters (table 2). Xie *et al.* impose that the overhead factor (the ratio between the size of the commitment and the size of the original message) has to be of the order of the logarithm of the security parameter. We can directly compare our and Benhamouda *et al.* proposal as we both require this ratio k to be greater than a quotient related to a constant γ, where $q \geq n^\gamma$. Our restriction is weaker and we also require a smaller minimum value for γ. This is really important as it allows us to choose the size of q with more flexibility.

Table 2: Parameter restrictions

	Xie *et al.*	Benhamouda *et al.*	our proposal
overhead factor	$m/l \in \omega(\log \lambda)$	$k > \frac{18\gamma}{3\gamma-16}$	$k > \frac{8\gamma+4}{2\gamma-5}$
n and q relation	–	$\gamma \geq 6$	$\gamma \geq 3$

In figure 1, for a fixed value $n = 2^{10}$, we represent the size of the commitment of Xie *et al.*, Benhamouda *et al.* and ours for different values of γ (that is, different values of q since $q \geq n^{\gamma}$).

Fig. 1: Commitment's size of Xie *et al.* (—○—), Benhamouda *et al.* (—□—) and our proposal (—△—)



Finally we can compare the communication cost of the Zero-Knowledge Proofs of multiplicative relations (table 3), as this is the most interesting case and the major contribution of this paper. In table 4 we compare soundness and completeness properties for one round of each protocol.

We separately show what are the initial communication costs (in bits), the cost per round (in bits), the number of auxiliary commitments, the number of openings of these auxiliary commitments and the number of seeds for the pseudorandom generation of the permutations. The last three items depend on the final implementation. Random seeds could be 256 bit strings. If the auxiliary commitment scheme is implemented using a hash function (secure in the random oracle model) then the size of each of these auxiliary commitments could also be 256 bits.

It should be taken into account that the cost per round has to be multiplied by the number of rounds required to achieve soundness, that depends on the desired level of soundness and the soundness error per round exposed in table 4.

In this final table we also include what we call the extracted error gap, that is, the quotient between the bound on the error of the RLWE samples obtained by the extractor and the original bound on the error known by the prover.

Compared with the Stern-based protocol of Xie *et al.* we have a similar commitment size but significantly reduce the cost of the proofs. Notice that md is comparable to kn, therefore we reduce the size of the proof by a factor $\log^2 q$ and we also improve the constants. We also reduce the number of rounds, as our soundness error per round is aproximately $1/2$ instead of $2/3$. Xie *et al.* needed to decompose the original message into bits, while we only need to decompose the error. Then we do not need any initial communication (they had to commit to the decompositions of the messages before starting the rounds), and we also reduce in the same proportion the number of auxiliar commitments, openings of auxiliar commitments and random seeds for the permutations, that are common in all Stern-based protocols.

On the other hand our commitment scheme is smaller than Benhamouda *et al.* for the same value of n and q, but they have a smaller communication cost, as its proof has a smaller cost per round and only needs one round. There is a trade-off between the size of the commitment and the communication cost. The running time of their proofs depends on the secret elements that are used, and that has to be taken into account in an interactive setting to avoid timing attacks. We don't have this issue, which makes the implementation more direct.

We only need the modulus q to be greater than n^3 while they require $q \geq n^6$. Just taking into account the size of the proofs it could still be more efficient to use a larger q and their negligible soundness error technique, however, if these proofs are just part of a different protocol then being forced to use a larger q for the whole protocol might not be compensated by their more efficient commitment proofs and our more flexible scheme could be the best option.

The same applies if the relation proofs are used not just for commitments but for any messages hidden in RLWE samples where the bounds on the size of the error matters (for example in proofs about public keys of encryption schemes). One could increase the size of all parameters in order to take into account the extracted error gap, or one could use our slightly more expensive but exact ZKPoK and avoid modifications on the parameters of the rest of the protocol.

Table 3: Communication cost (in bits)

	Benhamouda *et al.*	Xie *et al.*	our proposal
initial com.	–	$md\log^3 q + 2md\log^2 q$	–
round cost	$(8k+7)n\log q$ $+n/2+16\kappa/3-8$	$(12\kappa+2)md\log^3 q + 8ld\log^3 q$ $+\frac{\kappa^2+2\kappa+3}{3}(14md\log q)$	$(3(\kappa+1)k+1.5k+4)n\log q$ $+6(\kappa+1)kn+2\log q+1$
aux. com.	1	$3(\log^2 q+1)$	5
openings	1	$2(\log^2 q+1)$	3
seeds	–	$2(\kappa\log^2 q+\log^2 q+\kappa)$	$3(\kappa+1)$

Table 4: Soundness and completeness

	Benhamouda *et al.*	Xie *et al.*	our proposal
soundness error	negligible	$\frac{2}{3}$	$\frac{q^2+3q-2}{2q^2}$
extracted error gap	$\mathcal{O}\left(n^{4/3}/2\right)$	1	1

It would be interesting to study the benefits and costs of applying our proofs to other constructions that currently use Fiat-Shamir with aborts, such as the commitment scheme using more structured lattice assumptions (Module-LWE and Module-SIS) from [2], and we left it as future work.