# Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings

Fabrice Benhamouda[1], Stephan Krenn[2(✉)], Vadim Lyubashevsky[3], and Krzysztof Pietrzak[4]

[1] ENS, CNRS, INRIA, and PSL, Paris, France
fabrice.ben.hamouda@ens.fr
[2] AIT Austrian Institute of Technology GmbH, Vienna, Austria
stephan.krenn@ait.ac.at
[3] ENS, INRIA, Paris, France
lyubash@di.ens.fr
[4] IST Austria, Klosterneuburg, Austria
pietrzak@ist.ac.at

**Abstract.** We extend a commitment scheme based on the learning with errors over rings (RLWE) problem, and present efficient companion zero-knowledge proofs of knowledge. Our scheme maps elements from the ring (or equivalently, $n$ elements from $\mathbb{F}_q$) to a small constant number of ring elements. We then construct $\Sigma$-protocols for proving, in a zero-knowledge manner, knowledge of the message contained in a commitment. We are able to further extend our basic protocol to allow us to prove additive and multiplicative relations among committed values.

Our protocols have a communication complexity of $\mathcal{O}(Mn \log q)$ and achieve a negligible knowledge error in one run. Here $M$ is the constant from a rejection sampling technique that we employ, and can be set close to 1 by adjusting other parameters. Previously known $\Sigma$-protocols for LWE-related languages only achieved a noticeable or even constant knowledge error (thus requiring many repetitions of the protocol), or relied on "smudging" out the error (which necessitates working over large fields, resulting in poor efficiency).

**Keywords:** Commitment schemes · Ring learning with errors · Zero-Knowledge Proofs of Knowledge

## 1 Introduction

*Commitment schemes* are among the most widely used cryptographic primitives. They allow one party, the committer, to *commit* to a message $m$ to another

This work was done while the second author was at IBM Research – Zurich. This work was partly funded by the ERC Grants 321310–PERCY and 259668–PSPC, and by the French ANR-13-JS02-0003 JCJC Project CLE.


G. Pernul et al. (Eds.): ESORICS 2015, Part I, LNCS 9326, pp. 305–325, 2015.
DOI: 10.1007/978-3-319-24174-6_16

party. At a later point in time, the committer may reveal $m$ by *opening* the commitment $c$. The scheme is said to be secure if it is *binding* and *hiding*. The former property says that the committer cannot open $c$ to a message different from $m$, and the latter ensures that only knowing $c$ gives no information about $m$ to the receiver.

In higher-level protocols, commitments are often used to link different building blocks, e.g., encryption-, signature-, and revocation schemes in constructions of group signatures or anonymous credentials [CKL+14]. In such situations, it is often necessary to prove properties of a message $m$ contained in a commitment, without revealing any additional information about $m$. This is done via so-called *zero-knowledge proofs of knowledge* (ZK-PoK). These are two-party protocols which allow a *prover* to convince a *verifier* that it knows some secret piece of information, without revealing anything else than what is already revealed by the claim itself [GMR85]. As the efficiency of ZK-PoKs of commitments directly affects the efficiency of many higher-level systems, generic constructions such as [GMW86, GMR85] are too inefficient for practical use. A large amount of research effort has therefore been expended in improving the efficiency of such protocols for concrete proof goals. We continue this direction by presenting the so far most efficient ZK-PoKs for lattice-based commitment schemes.

Our constructions are proved secure under the *learning with errors over rings* (RLWE) assumption. Informally, it says that tuples $(a, a.s + e) \in R_q^2$ are computationally indistinguishable from $(a, u) \in R_q^2$, where $a, s, u$ are uniformly random in $R_q$ and $e$ is drawn according to some low-weight distribution $\chi$. We use $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, which as a vector space is isomorphic to $\mathbb{Z}_q^n$ (one can identify $a = a_1 + a_2 x + \cdots + a_n x^{n-1} \in R_q$ with $(a_1, \ldots, a_n) \in \mathbb{Z}_q^n$). For appropriately chosen parameters there exists a quantum reduction from certain worst-case problems on ideal lattices to the RLWE-problem [LPR10].

### 1.1 Our Contributions

In this paper is to construct efficient commitments and zero-knowledge proofs from the RLWE-assumption. To the best of our knowledge, our protocols are the first to achieve a negligible knowledge error in one run for lattice-based crypto systems.

In detail, our contributions are as follows:

- **Efficient Commitment Schemes from RLWE.** We first construct a perfectly binding and computationally hiding string commitment scheme. Committing to a message is done as in Xie et al. [XXW13], but we relax requirements on valid openings to be able to realize better ZK proofs while still preserving the binding property of the scheme.
- **Efficient ZK-PoK for Committed Values.** We then give a simple and efficient zero-knowledge protocol for proving knowledge of committed values. The protocol differs substantially from previous protocols for RLWE, and improves over them in the following ways: On the one hand, our protocol

already achieves a negligible knowledge error in a single run. Previous protocols only achieved a noticeable knowledge error, e.g., Ling et al. [LNSW13] or Xie et al. [XXW13], and thus many repetitions are required to get meaningful security, resulting in a low efficiency. On the other hand, we only require that the modulus is polynomially larger than the error in the RLWE problem. The construction of Asharov et al. [AJLA+12], which achieves a knowledge error of 1/2, relied on "smudging out" (or "drowning") the error, which required stronger assumptions as the modulus-error ratio had to be super-polynomial. Our protocols can be turned into concurrently zero-knowledge arguments of knowledge without any additional computational costs.

– **Efficient ZK-PoK for Relations.** Starting from our basic ZK-PoK we then construct protocols for proving that committed values $m_1, m_2, m_3 \in R_q$ satisfy $m_3 = m_1 + m_2$ as well as $m_3 = m_1 m_2$.

### 1.2 Related Work

At Asiacrypt'12, Jain et al. [JKPT12] presented a commitment scheme whose hiding property relies on the learning parity with noise (LPN) assumption, which is defined like LWE but over bits, i.e., for $q = 2$. Similar to our work, they give a $\Sigma$-protocol to prove any relation among committed values. A single run of their preimage proof requires $\mathcal{O}(n \log n)$ bits of communication, where each committed message is from $\{0,1\}^n$. However, their protocols only achieve a knowledge error of 2/3, and thus reaching a success probability of a malicious prover negligible in $k$, requires $\mathcal{O}(kn \log n)$ bits of communication. The main open problem of [JKPT12] was to find a commitment scheme and protocols whose security is based on LPN or a related problem, and which avoids the dependency on $k$.

Xie et al. [XXW13] generalized the commitment scheme from Jain et al. [JKPT12] from LPN to RLWE, and gave companion protocols for their scheme. However, their zero-knowledge proofs still require Stern-like techniques [Ste93], and therefore only achieve a knowledge error of 2/3. Our commitment scheme is closely related to theirs and may be seen as a generalization as we relax the requirements on valid openings. In their construction, a commitment $\boldsymbol{c}$ to a message $m$ can be opened by revealing $r$ and a short $\boldsymbol{e}$ such that $\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e}$, where $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{e} \in R_q^k$ and $m, r \in R_q$. Getting a bit ahead, we relax the openings such that we also accept openings of the form $\boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + f^{-1}\boldsymbol{e}$, where $f \in R_q$ is an additional small polynomial. We will prove that commitments are still binding, and show that this relaxation allows us to overcome the constant knowledge-error "barrier" for the commitment scheme by employing rejection sampling techniques introduced by Lyubashevsky [Lyu09,Lyu12].

Recently, Benhamouda et al. [BCK+14] improved the efficiency of ZK-PoKs for RLWE-based encryption schemes. As encryption schemes can also be seen as commitment schemes, it is worthwhile comparing their result to ours. They give a protocol for proving relations of the form $y = as + e$ (for $y, a, s, e \in R_q$ and $s, e$ short) that has a knowledge error of $1/(2n)$, where $n$ is the dimension of the ring, and thus also overcomes the above barrier. However, their protocol has a soundness gap in the sense that it only proves that the prover knows a valid

representation of $2y$, not of $y$ itself, which is still sufficient for many applications as illustrated in their work. We improve over their results by reaching a negligible knowledge error already in one run of the protocol (compared to $1/(2n)$) and by not having such a soundness gap. On the other hand, our protocol requires the ring $R_q$ to have a large subring that is a field, whereas the protocol in [BCK+14] does not require such a property.

Asharov et al. [AJLA+12] constructed $\Sigma$-protocols for several specific languages related to the standard LWE-problem. However, they do not give (efficient, i.e., direct) constructions for proving relations among LWE-secrets. Furthermore, their protocols have a super-polynomial knowledge-gap, i.e., the norm of the error known to a potentially malicious prover can only be guaranteed to be super-polynomially larger than that known to an honest party, while this gap is only polynomial in our case. This allows us to prove the security of our scheme under weaker assumptions, and to use a smaller modulus in the RLWE-problem, giving better efficiency.

Apart from these very closely related works, a large number of cryptographic applications based on the LWE-assumption has been proposed, starting with the work of Regev [Reg05]. This includes (fully homomorphic) encryption [BV11a, Gen09, LP11, LPR10, Reg05], signature schemes [DDLL13, GPV08, Lyu09, Lyu12, Rüc10], pseudorandom functions [BPR12] and hash functions [KV09, PR06]. Similarly, efficient (non-)interactive zero-knowledge proofs and arguments have been a vivid topic of research, see, e.g., [AJLA+12, BDP00, CD97, CD98, CD09, DPSZ12, GS08, IKOS07, KR06, KMO90, KP98] and the references therein. Finally, starting with a different motivation, the idea of committing to the first message in a $\Sigma$-protocol was also used by Damgård [Dam00], where it was shown how to obtain concurrent zero-knowledge for any $\Sigma$-protocol. We commit to the first message to get zero-knowledge in the first place, and we will discuss how the concurrency results also apply to our constructions in Sect. 4.1.

### 1.3 Roadmap

In Sect. 2 we recap some basic definitions on ZK proofs and LWE. Then, in Sect. 3 we present our commitment scheme, and give protocols for proving knowledge of, and relations among, the contents of commitments in Sect. 4. We finally briefly conclude in Sect. 5.

## 2 Preliminaries

We denote vectors by bold lower-case letters ($\boldsymbol{a}, \boldsymbol{b}, \dots$) and algorithms by sans-serif letters ($\mathsf{A}, \mathsf{B}, \dots$). We write $a \xleftarrow{\$} A$ for a set $A$ if $a$ was uniformly drawn from $A$, $a \xleftarrow{\$} D$ for a distribution $D$ if $a$ was drawn according to $D$, and $a \xleftarrow{\$} \mathsf{A}$ if $\boldsymbol{a}$ is the output of a randomized algorithm $\mathsf{A}$.

For two distributions $D, E$, we write $D \overset{c}{\sim} E$, if $D$ and $E$ are computationally indistinguishable. Furthermore, we use the notation $\mathsf{Pr}[\mathcal{E} : \Omega]$ to denote the

probability of event $\mathcal{E}$ over the probability space $\Omega$. For instance, $\mathsf{Pr}[x = y : x, y \xleftarrow{\$} D]$ denotes the probability that $x = y$ if $x, y$ were drawn according to a distribution $D$.

The language induced by a binary relation $\mathcal{R}$ is defined as

$$\mathcal{L}(\mathcal{R}) = \{c : \exists w \text{ such that } (c, w) \in \mathcal{R}\}.$$

We finally assume that elements of $\mathbb{Z}_q$ ($q$ odd) are represented by elements from $\left\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\right\}$.

### 2.1 Commitment Schemes

We now formally define commitment schemes.

**Definition 2.1.** *A* commitment scheme *consists of three algorithms* ($\mathsf{KGen}$, $\mathsf{Com}$, $\mathsf{Ver}$) *such that:*

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

A commitment scheme has to satisfy the following security requirements:

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

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

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

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

  On the other hand, a scheme is said to be *computationally binding* if no PPT adversary can come up with a commitment and two different openings, i.e., for every PPT adversary $\mathsf{A}$ there exists a negligible function $\mathsf{negl}$ such that:

$$\mathsf{Pr}\Big[\mathsf{Ver}(pk, m, c, d) = \mathsf{Ver}(pk, m', c, d') : pk \xleftarrow{\$} \mathsf{KGen}(1^\ell), \\ (c, m, d, m', d') \xleftarrow{\$} \mathsf{A}(pk)\Big] \leq \mathsf{negl}(n).$$

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

$$\mathsf{Pr}\left[b = b' : \begin{array}{c} pk \xleftarrow{\$} \mathsf{KGen}(1^\ell), (m_0, m_1, \mathsf{aux}) \xleftarrow{\$} \mathsf{A}_1(pk), \\ b \xleftarrow{\$} \{0,1\}, (c,d) = \mathsf{Com}(m_b, pk), b' \xleftarrow{\$} \mathsf{A}_2(c, \mathsf{aux}) \end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

A scheme is called a *trapdoor commitment scheme*, if $\mathsf{KGen}$ additionally outputs a trapdoor $td$ for the public key, such that there exists an efficient algorithm taking $(c,d) = \mathsf{Com}(m, pk)$, $m$, $td$ and $m' \in \mathcal{M}$ as inputs, that outputs $d'$ such that $\mathsf{Ver}(pk, m', c, d') = \mathsf{accept}$. Note that trapdoor commitment schemes can only be computationally binding. See, e.g., Fischlin [Fis01] for a detailed discussion of such schemes.

For the sake of simplicity, we will not state $pk$ explicitly as an input in the following.

### 2.2 Zero-Knowledge Proofs and $\Sigma$-Protocols

Informally, a zero-knowledge proof of knowledge is a two party protocol between a prover and a verifier, which allows the former to convince the latter that it knows some secret piece of information, without revealing anything about the secret apart from what the claim itself already reveals. For a formal definition we refer to Bellare and Goldreich [BG93]. The ZK proofs constructed in this paper will be instantiations of the following definition, which is a straightforward generalization of the standard notion of $\Sigma$-protocols [Cra97, Dam10]:

**Definition 2.2.** *Let* $(\mathsf{P}, \mathsf{V})$ *be a two-party protocol, where* $\mathsf{V}$ *is PPT, and let* $\mathcal{R}, \mathcal{R}'$ *be a binary relation such that* $\mathcal{R} \subseteq \mathcal{R}'$*. Then* $(\mathsf{P}, \mathsf{V})$ *is called a* $\Sigma'_m$-protocol *for* $\mathcal{R}, \mathcal{R}'$ *with challenge set* $\mathcal{C}$*, public input* $c$ *and private input* $w$*, if and only if it satisfies the following conditions:*

– **3-move form:** *The protocol is of the following form:*
  - *The prover* $\mathsf{P}$ *computes a commitment* $t$ *and sends it to* $\mathsf{V}$*.*
  - *The verifier* $\mathsf{V}$ *draws a challenge* $d \xleftarrow{\$} \mathcal{C}$ *and sends it to* $\mathsf{P}$*.*
  - *The prover sends a response* $s$ *to the verifier.*
  - *Depending on the protocol transcript* $(t, d, s)$*, the verifier accepts or rejects the proof.*

  *The protocol transcript* $(t, d, s)$ *is called* accepting*, if the verifier accepts the protocol run.*
– **Completeness:** *Whenever* $(c, w) \in \mathcal{R}$*, the verifier* $\mathsf{V}$ *accepts with probability at least* $1 - \alpha$*.*
– **Special soundness:** *There exists a PPT algorithm* $\mathsf{E}$ *(the* knowledge extractor*) which takes* $m$ *accepting transcripts* $(t, d_1, s_1), \ldots, (t, d_m, s_m)$ *satisfying* $d_i \neq d_j$ *for* $i \neq j$ *as inputs, and outputs* $w'$ *such that* $(c, w') \in \mathcal{R}'$*.*
– **Special honest-verifier zero-knowledge:** *There exists a PPT algorithm* $\mathsf{S}$ *(the* simulator*) taking* $c \in \mathcal{L}(\mathcal{R})$ *and* $d \in \mathcal{C}$ *as inputs, that outputs triples* $(t, d, s)$ *whose distribution is (computationally) indistinguishable from accepting protocol transcripts generated by real protocol runs.*

We now discuss some additional points regarding Definition 2.2. First, the standard definition for $\Sigma$-protocols found in the literature considers the case where $m = 2$, $\mathcal{R} = \mathcal{R}'$ and $\alpha = 0$. In this case, it is well known that the protocol is also a proof of knowledge for the same relation $\mathcal{R}$ with knowledge error $1/|\mathcal{C}|$ [Dam10]. However, it can be seen that the proof given there also generalizes to other constants $m$ with a knowledge error of $(m-1)/|\mathcal{C}|$ if $1 - \alpha > (m-1)/|\mathcal{C}|$, and special cases of this result were already used implicitly in previous work, e.g., [JKPT12, Ste93]. Second, the modification that $\mathcal{R} \subseteq \mathcal{R}'$ means that the protocol is honest-verifier zero-knowledge and complete whenever the prover uses a secret witness $w$ such that $(c, w) \in \mathcal{R}$, but the verifier is only assured that the prover supplied a witness $w'$ such that $(c, w') \in \mathcal{R}'$. For many interesting relations this gap allows for much more efficient protocols, e.g., Fujisaki et al. [FO97, DF02] or Benhamouda et al. [BCK+14]. If this gap is reasonably small, as is the case in the protocols we present, one still obtains sufficient security guarantees from the protocol. Finally, the above definition only guarantees privacy to the prover against honest-but-curious verifiers, i.e., verifiers not deviating from the protocol. This issue can be solved generically using techniques of, e.g., Damgård et al. [DGOW95] or Fiat and Shamir [FS87]; furthermore, for our concrete protocols it can be solved without any extra costs, cf. Lemma 4.3.

### 2.3 Learning with Errors

The learning with errors (LWE) problems was first introduced by Regev [Reg05]. Informally, it asks to distinguish slightly perturbed random linear equations from truly random ones. LWE has been shown to be as hard as certain worst-case problems on lattices, and has served as a basis for a large variety of cryptographic schemes. Unfortunately, schemes built upon LWE are inherently inefficient due to a large overhead in the use of the problem. This drawback has been resolved by Lyubashevsky et al. [LPR10] by introducing the ring learning with noise problem, which still enjoys strong hardness guarantees. The following formulation is a special case of the problem restricted to the ring $\mathbb{Z}[x]/\langle x^n + 1\rangle$, with $n$ a power of two:

**Definition 2.3.** *Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $R_q = R/qR$, and let $\chi$ be a distribution over $R$.*

*The (decisional)* ring learning with errors *assumption (denoted by* $\mathsf{RLWE}_{q,\chi}$*) states that:*

$$\{(a_i, a_i \cdot s + e_i)\} \overset{c}{\sim} \{(a_i, u_i)\},$$

*for any polynomial number of samples, where $a_i \xleftarrow{\$} R_q$, $e_i \xleftarrow{\$} \chi$, $u_i \xleftarrow{\$} R_q$, and $s \xleftarrow{\$} R_q$ is secret.*

We further recapitulate the definition of Normal distributions:

**Definition 2.4.** *The* continuous Normal distribution *on* $\mathbb{R}^m$ *centered at* $\boldsymbol{v}$ *with standard deviation* $\sigma$ *is defined by the density function*

$$\rho^m_{\boldsymbol{v},\sigma}(\boldsymbol{x}) = \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^m e^{-\frac{\|x-v\|^2}{2\sigma^2}}.$$

*We avoid the subscript* $\boldsymbol{v}$ *if* $\boldsymbol{v} = 0^m$.

*The* discrete Normal distribution *on* $\mathbb{Z}^m$ *centered at* $\boldsymbol{v}$ *with standard deviation* $\sigma$ *is defined by the density function* $D^m_{\boldsymbol{v},\sigma}(\boldsymbol{x}) = \rho^m_{\boldsymbol{v},\sigma}(\boldsymbol{x})/\rho_\sigma(\mathbb{Z}^m)$, *where* $\rho_\sigma(\mathbb{Z}^m) = \sum_{\boldsymbol{z}\in\mathbb{Z}^m} \rho^m_\sigma(\boldsymbol{z})$ *is the scaling factor required to obtain a probability distribution.*

For convenience, sampling the normal distribution over a ring $R$, we will still write $D_{\boldsymbol{v},\sigma}$ even though it is not a 1-dimensional distribution. Lyubashevsky et al. [LPR10] showed the search and the decisional version of $\mathsf{RLWE}_{q,\chi}$ are polynomially related, and that there exists a quantum reduction from the worst-case approximate shortest vector problem on ideal lattices to $\mathsf{RLWE}_{q,\chi}$.[1]

### 2.4 Rejection Sampling

For proving the zero-knowledge property of our protocol, it is essential that all the responses of the prover can be simulated without knowing the secret key. We thus need that the response elements are from a distribution which is *independent* of the secret key. In our protocol, however, all the potential responses will be from a shifted distribution $D^\ell_{\boldsymbol{v},\sigma}$ for $\ell = kn$ and some vector $\boldsymbol{v}$ depending on the secret key. To correct for this, we employ rejection sampling [Lyu09, Lyu12], where a potential response is only output with a certain probability, and otherwise the protocol is aborted.

Informally, the following theorem states that if $\sigma \in \tilde{\Theta}(\|\boldsymbol{v}\|)$, then the rejection sampling procedure will result in a distribution statistically close to $D^\ell_\sigma$, which is independent of $\boldsymbol{v}$ as required. The technique only requires a constant number of iterations before a value is output, and furthermore the output is also statistically close for every $\boldsymbol{v}'$ with norm at most $\|\boldsymbol{v}\|$. For concrete parameters we refer to the original work of Lyubashevsky [Lyu12].

**Theorem 2.5** ([Lyu12])**.** *Let* $V$ *be a subset of* $\mathbb{Z}^\ell$ *in which all elements have norms less than* $T$, *and let* $h$ *be a probability distribution over* $V$. *Then, for any constant* $M$, *there exists a* $\sigma = \tilde{\Theta}(T)$ *such that the output distributions of the following algorithms* $\mathsf{A}, \mathsf{F}$ *are statistically close:*

$\mathsf{A}$*:*
$\boldsymbol{v} \xleftarrow{\$} h$; $\boldsymbol{z} \xleftarrow{\$} D^\ell_{\boldsymbol{v},\sigma}$;
*output* $(\boldsymbol{z}, \boldsymbol{v})$ *with probability* $\min\left(\exp\left(\frac{-2\langle \boldsymbol{z},\boldsymbol{v}\rangle + \|\boldsymbol{v}\|^2}{2\sigma^2}\right), 1\right)$

$\mathsf{F}$*:*
$\boldsymbol{v} \xleftarrow{\$} h$; $\boldsymbol{z} \xleftarrow{\$} D^\ell_\sigma$;
*output* $(\boldsymbol{z}, \boldsymbol{v})$ *with probability* $\frac{1}{M}$

*Moreover, the probability that* $\mathsf{A}$ *outputs something is exponentially close to that of* $\mathsf{F}$, *i.e.,* $1/M$.

[1] The work of [LPR10] showed the hardness for decisional $\mathsf{RLWE}$ only for rings where $x^n + 1$ splits completely modulo $q$. Employing the modulus switching technique from [BV11b], it was shown in [BLP+13] that the problem remains hard for any $q$.

In [Lyu12], it is also shown that if $\sigma = \alpha T$ for a positive $\alpha$, then $M = e^{12/\alpha+1/(2\alpha^2)}$, the output of $\mathsf{A}$ is within a statistical distance of $\frac{2^{-100}}{M}$ of the output of $\mathsf{F}$, and the probability that $\mathsf{A}$ outputs something is at least $\frac{1-2^{-100}}{M}$.

## 3 Commitments from Ring-LWE

In the following we describe our commitment scheme. Table 1 lists the parameters being used and the requirements we pose on them.

- $\mathsf{KGen}$: The public commitment key $pk = (\boldsymbol{a}, \boldsymbol{b})$ is computed as $\boldsymbol{a}, \boldsymbol{b} \xleftarrow{\$} (\mathbb{Z}_q[x]/\langle x^n + 1\rangle)^k$, where $q \equiv 3 \bmod 8$ is prime, and $n$ is a power of 2.
- $\mathsf{Com}$: To commit to a message $m \in \mathbb{Z}_q[x]/\langle x^n+1\rangle$, the commitment algorithm draws $r \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ and $\boldsymbol{e} \xleftarrow{\$} D^k_{\sigma_e}$ conditioned on $\|\boldsymbol{e}\|_\infty \leq n$, and outputs

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

  and the opening information for $\boldsymbol{c}$ is given by $(m, r, \boldsymbol{e}, 1)$.
- $\mathsf{Ver}$: Given a commitment $\boldsymbol{c}$, a message $m'$, a randomness $r'$, as well as $\boldsymbol{e}'$ and $f'$, the verifier accepts, if and only if

$$\boldsymbol{a}m' + \boldsymbol{b}r' + f'^{-1}\boldsymbol{e}' = \boldsymbol{c} \wedge \|\boldsymbol{e}'\|_\infty < \left\lfloor \frac{n^{4/3}}{2} \right\rfloor \wedge \|f'\|_\infty \leq 1 \wedge \deg f' < \frac{n}{2}.$$

The scheme above is a generalization of that by Xie et al. [XXW13], as we allow for the additional small polynomial $f$ in valid openings. While an honest party can always set $f = 1$ when opening $\boldsymbol{c}$ and therefore the completeness property is not affected by this relaxation, the immediate question arises whether the given construction is still binding, i.e., whether a malicious user still cannot

**Table 1.** Overview of parameters used in this document.

| Parameter | Semantics/Restrictions |
|---|---|
| $n$ | degree of polynomial, power of 2, typical values are $2^9$ or $2^{10}$ |
| $\gamma$ | integer parameter controlling the size of the modulus |
| $q$ | prime number, $\equiv 3 \bmod 8$ and $\geq n^\gamma$ |
| $k$ | multiplicative overhead of commitment size |
| $\sigma_e$ | standard deviation of the error in the commitment scheme; $\tilde{\mathcal{O}}(n^{3/4})$ |
| $\kappa$ | integer, where $1/\lvert\mathcal{C}\rvert = 1/\binom{n/2}{\kappa}$ bounds the knowledge error of our proofs; for instance, $n = 2^9$, $\kappa = 21$ or $n = 2^{10}$, $\kappa = 17$ give a knowledge error of less than $2^{-100}$ |
| $\mathcal{C}$ | domain of challenges; $\mathcal{C} = \{d \in \{0,1\}^n : \|d\|_1 \leq \kappa \wedge \deg d < n/2\}$ |
| $\sigma_\eta$ | standard deviation of the randomness for $\boldsymbol{e}$ in the protocols; $\tilde{\mathcal{O}}(n^{5/4})$ |

open a commitment to two different messages. We give a formal security proof in the following.

We want to stress that the above modification will be at the heart for the construction of efficient zero-knowledge proofs of the contained message in Sect. 4.

**Theorem 3.1.** *Let $\gamma > 6$ and $q, k$ be polynomial in $n$ such that the following is satisfied:*

$$q \geq n^{\gamma} \geq n^6 \quad \text{and} \quad k > \frac{18\gamma}{3\gamma - 16}. \tag{1}$$

*Then, under the* RLWE*-assumption, the above scheme is a computationally hiding and perfectly binding commitment scheme with overwhelming probability over the choices of the public commitment key.*

*Proof.* Correctness is trivial to see.

*Computational Hiding.* First note that by, e.g., [Lyu12, Lemma 4.4], the probability that $\boldsymbol{e} \xleftarrow{\$} D_{\sigma_e}^k$ has $\|\boldsymbol{e}\|_\infty > n$ is negligible, and thus the conditional distribution of $\boldsymbol{e}$ in $\mathsf{Com}$ is statistically close to a discrete Normal distribution. Now, by the RLWE-assumption, $\boldsymbol{b}r + \boldsymbol{e}$ is pseudorandom, and thus so is $\boldsymbol{c}$.

*Binding.* For the binding property, we have to show that

$$\boldsymbol{c} = \boldsymbol{a}m' + \boldsymbol{b}r' + f'^{-1}\boldsymbol{e}' = \boldsymbol{a}m'' + \boldsymbol{b}r'' + f''^{-1}\boldsymbol{e}''$$

implies that $m' = m''$, if $\|\boldsymbol{e}'\|_\infty, \|\boldsymbol{e}''\|_\infty < n^{4/3}/2$, $\|f'\|_\infty, \|f''\|_\infty \leq 1$, and $\deg f', \deg f'' < n/2$, or, alternatively, that

$$\boldsymbol{a}m + \boldsymbol{b}r = f'^{-1}\boldsymbol{e}' - f''^{-1}\boldsymbol{e}''$$

implies that $m = 0$ with overwhelming probability over the choices of $\boldsymbol{a}, \boldsymbol{b}$.

Assume by contradiction that this holds for some fixed $m, r, e', e'', f', f''$ with $m \neq 0$ and $e', e'', f', f''$ being sufficiently small. Because of the assumption on $n$ and $q$, we have that $x^n + 1$ splits into two irreducible factors $\alpha(x), \beta(x)$ [SSTX09, Lemma 3]. Now, since $m \neq 0 \bmod (x^n + 1)$, we also have that $m \neq 0 \bmod \alpha(x)$ or $m \neq 0 \bmod \beta(x)$, and thus $\boldsymbol{a}_i m$ takes at least $q^{n/2}$ different values. We then have that

$$\mathsf{Pr}\left[\begin{pmatrix} \boldsymbol{a}_1 m + \boldsymbol{b}_1 r \\ \vdots \\ \boldsymbol{a}_k m + \boldsymbol{b}_k r \end{pmatrix} = \begin{pmatrix} f'^{-1}\boldsymbol{e}'_1 - f''^{-1}\boldsymbol{e}''_1 \\ \vdots \\ f'^{-1}\boldsymbol{e}'_k - f''^{-1}\boldsymbol{e}''_k \end{pmatrix} : \boldsymbol{a}, \boldsymbol{b} \xleftarrow{\$} (\mathbb{Z}_q[x]/\langle x^n + 1\rangle)^k\right] \leq \frac{1}{q^{kn/2}}.$$

Now, taking a union bound over all $m, r, e', e'', f', f''$ we get that the overall probability that there exists such an $m \neq 0$ is at most

$$\frac{q^{2n}(n^{4/3})^{2kn}3^{2n/2}}{q^{kn/2}} \leq \frac{q^{2n}(q^{4/(3\gamma)})^{2kn}3^{2n/2}}{q^{kn/2}} = 3^n q^{(2+(\frac{8}{3\gamma}-\frac{1}{2})k)n}.$$

This is negligible in $n$ if $3q^{2+(8/(3\gamma)-1/2)k} \leq 1/2$, which holds if the requirements from (1) are satisfied. □

## 4 Zero-Knowledge of Proofs of Knowledge

In this section we first present a protocol for proving knowledge of valid openings of commitments as defined in the previous section. We then give protocols which allow one to prove that the messages $m_1, m_2, m_3$ contained in commitments $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ satisfy $m_3 = m_1 + m_2$ or $m_3 = m_1 m_2$, respectively. Together this allows one to prove knowledge of arbitrary algebraic circuits.

In this entire section we let $(\mathsf{aKGen}, \mathsf{aCom}, \mathsf{aVer})$ be an arbitrary auxiliary string commitment scheme. For simplicity, the reader may think of it as the scheme from Sect. 3, or as well just as a random oracle. We write $(c_{\mathsf{aux}}, d_{\mathsf{aux}}) = \mathsf{aCom}(s)$, where $c_{\mathsf{aux}}$ is the commitment and $d_{\mathsf{aux}}$ is the opening of $c_{\mathsf{aux}}$.

### 4.1 Preimage Proofs

Protocol 4.1 is a $\Sigma_2'$-protocol for showing knowledge of a valid opening for a single commitment. It is honest-verifier zero-knowledge whenever the commitment was honestly computed, and is sound with respect to valid openings. In particular, whenever a potentially malicious prover can make the verifier accept with more than negligible probability, it must know a valid opening of $\boldsymbol{c}$. We stress that this gap between the zero-knowledge and the soundness property is in line with previous protocols, e.g., for discrete logarithms in groups of hidden order [DF02], where the prover is also guaranteed security only for a subset of valid openings. However, this gap is meaningful, as our commitment scheme is still perfectly binding also for the larger set of valid openings, and so the proof still guarantees knowledge of the *unique* valid opening of $\boldsymbol{c}$.

**Theorem 4.2.** *If the auxiliary commitment scheme is perfectly binding, then Protocol 4.1 is an honest-verifier zero-knowledge proof of knowledge with knowledge error* $1/\binom{n/2}{\kappa}$ *for the following relations:*

$$\mathcal{R}_{LWE} = \{((\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}), (m, r, \boldsymbol{e})) : \boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + \boldsymbol{e} \ \wedge \ \|\boldsymbol{e}\|_\infty \leq n\} \quad \textit{and}$$

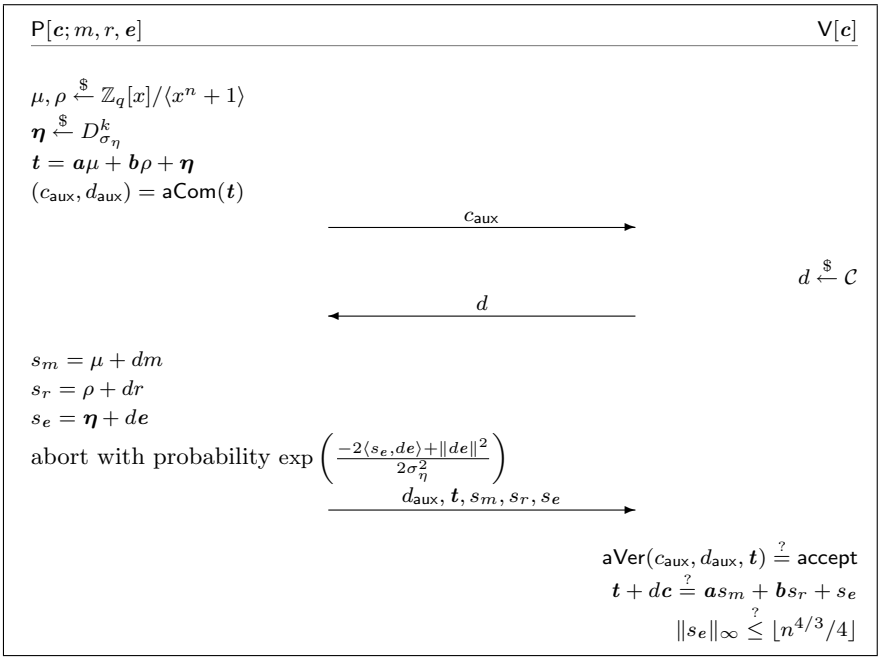
$$\mathcal{R}'_{LWE} = \Big\{ ((\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}), (m, r, \boldsymbol{e}, f)) : \boldsymbol{c} = \boldsymbol{a}m + \boldsymbol{b}r + f^{-1}\boldsymbol{e} \ \wedge \ \|\boldsymbol{e}\|_\infty \leq \lfloor n^{4/3}/2 \rfloor, \\ \|f\|_\infty \leq 1, \deg f < \frac{n}{2} \Big\}.$$

*Proof.* The theorem is proved by showing that the protocol is a $\Sigma_2'$-protocol for the given relation. The claim then follows directly from the discussion in Sect. 2.2.

The 3-move-form is obvious.

*Completeness.* An honest prover responses with a probability close to $\frac{1}{M}$. In this case we get:

$$\begin{aligned} \boldsymbol{t} + d\boldsymbol{c} &= \boldsymbol{a}\mu + \boldsymbol{b}\rho + \boldsymbol{\eta} + d\boldsymbol{a}m + d\boldsymbol{b}r + d\boldsymbol{e} \\ &= \boldsymbol{a}(\mu + dm) + \boldsymbol{b}(\rho + dr) + (\boldsymbol{\eta} + d\boldsymbol{e}) = \boldsymbol{a}s_m + \boldsymbol{b}s_r + s_{\boldsymbol{e}}. \end{aligned}$$




**Protocol 4.1:** Simple preimage proof. The verifier accepts, iff all conditions marked with "?" are satisfied.

Furthermore, we have that with overwhelming probability

$$\|s_{\boldsymbol{e}}\|_\infty = \|\boldsymbol{\eta} + d\boldsymbol{e}\|_\infty \leq \|\boldsymbol{\eta}\|_\infty + \kappa\|\boldsymbol{e}\|_\infty \leq \lfloor n^{4/3}/4 \rfloor,$$

as the standard deviations of $D_{\sigma_e}, D_{\sigma_\eta}$ are significantly smaller than $n^{4/3}$.

*Special Soundness.* Let the extractor $\mathsf{E}$ be given two accepting protocol transcripts $(c_{\mathsf{aux}}, d', (d'_{\mathsf{aux}}, \boldsymbol{t}', s'_m, s'_r, s'_{\boldsymbol{e}}))$ and $(c_{\mathsf{aux}}, d'', (d''_{\mathsf{aux}}, \boldsymbol{t}'', s''_m, s''_r, s''_{\boldsymbol{e}}))$, where $d' \neq d''$. By the perfect binding property of $\mathsf{aCom}$ we get that $\boldsymbol{t}' = \boldsymbol{t}'' = \boldsymbol{t}$. By subtracting the verification equations performed by the verifier we then obtain:

$$\Delta_d \boldsymbol{c} = \boldsymbol{a}\Delta_m + \boldsymbol{b}\Delta_r + \Delta_{\boldsymbol{e}},$$

where we set $\Delta_d = d' - d''$, $\Delta_m = s'_m - s''_m$, $\Delta_r = s'_r - s''_r$ and $\Delta_{\boldsymbol{e}} = s'_{\boldsymbol{e}} - s''_{\boldsymbol{e}}$. As $\deg \Delta_d < n/2$, we also have that $\Delta_d$ is invertible in $R_q$. We get the witness $(\Delta_d^{-1}\Delta_m, \Delta_d^{-1}\Delta_r, \Delta_d, \Delta_{\boldsymbol{e}})$, where $\|\Delta_d\|_\infty \leq 1$ and $\|\Delta_{\boldsymbol{e}}\| \leq \lfloor n^{4/3}/2 \rfloor$.

*Honest-Verifier Zero-Knowledge.* Taking a challenge $d$ as an input, the simulator first draws uniformly random elements $s'_m, s'_r \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, and $s'_{\boldsymbol{e}}$ to be $\perp$ with probability $1 - 1/M$ and distributed according to $D_{\sigma_\eta}$ with probability $1/M$. If $s'_{\boldsymbol{e}} \neq \perp$, it computes $(c'_{\mathsf{aux}}, d'_{\mathsf{aux}}) = \mathsf{aCom}(\boldsymbol{t}' = \boldsymbol{a}s'_m + \boldsymbol{b}s'_r + s'_{\boldsymbol{e}} - d\boldsymbol{c})$ and

outputs $(c'_{\mathsf{aux}}, d, (d'_{\mathsf{aux}}, \boldsymbol{t}', s'_m, s'_r, s'_{\boldsymbol{e}}))$. (Note that $s'_i$ and $d$ uniquely determine $\boldsymbol{t}'$ in the protocol and in the simulation.) Otherwise the simulator sets $(c'_{\mathsf{aux}}, d'_{\mathsf{aux}}) = \mathsf{aCom}(0)$ and outputs $(c'_{\mathsf{aux}}, d, \perp)$.

It follows from Theorem 2.5 that the distribution conditioned on the prover not outputting $\perp$ is indistinguishable from real protocol runs. From the same theorem, it follows that aborts occur with probability $1 - 1/M$ for every value of $d\boldsymbol{e}$. In case of an abort, the indistinguishability follows from the hiding property of $\mathsf{aCom}$ and the fact that for every $d$, there is an equal chance of an abort happening. □

**Lemma 4.3.** *If the auxiliary commitment scheme is a trapdoor commitment scheme, then Protocol 4.1 is a concurrently secure zero-knowledge argument of knowledge with knowledge error* $1/\binom{n/2}{\kappa}$ *for the relation specified in Theorem 4.2.*

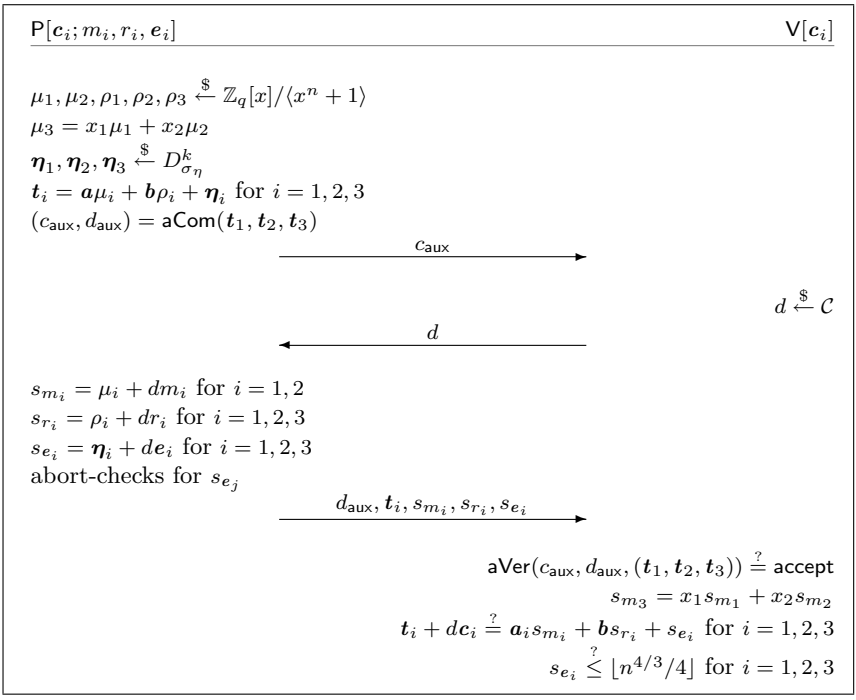
The proof is similar to Damgård [Dam00] who gives a generic construction to achieve concurrent ZK for any $\Sigma$-protocol. However, our technique had a slightly different origin as our protocols are inherently based on the auxiliary commitment scheme to achieve honest-verifier zero-knowledge. The lemma literally also applies for the subsequent protocols.

*On the Abort Probability.* From Theorem 2.5 and [Lyu12] it follows that the probability that the prover does not abort is exponentially close to $\frac{1}{M}$, where $M \in \mathcal{O}(\exp(\frac{\|d\boldsymbol{e}\|}{\sigma_\eta}))$. Thus, on average $M$ repetitions of the protocol are required. By choosing $\sigma_\eta$ sufficiently large, $M$ can be made arbitrarily small at the cost of requiring larger parameters, see also Lyubashevsky [Lyu12].

*Number of Rounds.* By nesting the executions, the expected number of rounds until a successful protocol run is about $2M$. Alternatively, when only aiming for *arguments* of knowledge, one can also use the idea of Damgård et al. [DPSZ12], who compute many independent first messages and send a Merkle-tree commitment of those in the first step. While on average requiring more computation on the prover side, this approach gives a constant 3-round protocol.

### 4.2 Proving Linear Relations

Protocol 4.4 allows one to prove knowledge of messages $m_1, m_2, m_3$ contained in $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$, where the $m_i$ additionally satisfy a linear relation of the form $m_3 = x_1 m_1 + x_2 m_2$ for arbitrary public $x_i \in \mathbb{Z}_q[x]/\langle x^n + 1\rangle$. The construction uses a standard technique: Three instances of Protocol 4.1 are run in parallel for $m_1, m_2, m_3$ using the same challenge, but instead of choosing the randomness $\mu_3$ for $m_3$ in the prover's first step at random, it is computed such that $\mu_1, \mu_2, \mu_3$ satisfy the claimed linear relation. Verifying now whether the $s_{m_i}$ also satisfy that linear relation is enough for the verifier to be guaranteed that the supplied messages have the correct form.




**Protocol 4.4:** Proving linear relations. The abort-checks are as in Protocol 4.1 and Theorem 2.5.

**Theorem 4.5.** *If the auxiliary commitment scheme is perfectly binding, then Protocol 4.4 is an honest-verifier zero-knowledge proof of knowledge with knowledge error* $1/\binom{n/2}{\kappa}$ *for the following relations:*

$$\mathcal{R}_{LLWE} = \left\{ ((\boldsymbol{a}, \boldsymbol{b}, x_1, x_2, \boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3), (m_1, m_2, m_3, r_1, r_2, r_3, \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)) : \right.$$
$$\left. \bigwedge_{i=1}^{3} (\boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \boldsymbol{e}_i \ \wedge \ \|\boldsymbol{e}_i\|_\infty \leq n) \ \wedge \ m_3 = x_1 m_1 + x_2 m_2 \right\},$$

*and* $\mathcal{R}'_{LLWE}$ *is defined accordingly.*

*Proving Inhomogeneous Relations.* As for, e.g., DLOG based protocols, inhomogeneous relations like $m_3 = x_1 m_1 + x_2 m_2 + x_3$ can be proved by first removing the inhomogeneity: If $\boldsymbol{c}_i$ is a commitment to $m_i$, both parties first compute $\boldsymbol{c}'_3 = \boldsymbol{c}_3 - \boldsymbol{a}x_3$, and the prover sets $m'_3 = m_3 - x_3$. The parties then perform Protocol 4.4 for $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}'_3$ and $m_1, m_2, m'_3$ and the homogeneous linear relation $m'_3 = x_1 m_1 + x_2 m_2$.

### 4.3 Proving Multiplicative Relations

In this section we show how one can prove knowledge of $m_i, r_i, \boldsymbol{e}_i$, $i = 1, 2, 3$ such that $\boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \boldsymbol{e}_i$, and additionally $m_3 = m_1 \cdot m_2$. We begin by giving the intuition behind the protocol.

(i) The prover first proves knowledge of the contents of $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ by running 3 instances of Protocol 4.1 in parallel.

(ii) Similar to Protocol 4.4, the verifier will check the multiplicative relation by combining the responses for $m_1, m_2, m_3$ accordingly. Unfortunately, in contrast to linear proofs where we have $s_{m_1} + s_{m_2} = s_{m_3}$ for an honest prover, we have that $s_{m_1} s_{m_2} \neq s_{m_3}$. We tackle this problem by letting the prover commit to the arising cross-terms $\mu_1 m_2 + \mu_2 m_1$ and $\mu_1 \mu_2$ in a second part. The according commitments are denoted by $\boldsymbol{c}_+$ and $\boldsymbol{c}_\times$. Again using two instances of Protocol 4.1, the prover now proves that it knows the openings of those two commitments.

(iii) The third part of the proof now establishes the multiplicative relation. It is based on the following observation: from $(i)$ and $(ii)$ it follows that:

$$\begin{aligned}\tilde{\boldsymbol{c}} &= \boldsymbol{a}s_{m_1}s_{m_2} - d^2\boldsymbol{c}_3 - \boldsymbol{c}_\times - d\boldsymbol{c}_+ \\ &= \quad \boldsymbol{a}\left(\mu_1\mu_2 - m_\times + d(\mu_1 m_2 + \mu_2 m_1 - m_+) + d^2(m_1 m_2 - m_3)\right) \\ &\quad + \boldsymbol{b}(-d^2 r_3 - r_\times - d r_+) + (-d^2\boldsymbol{e}_3 - \boldsymbol{e}_\times - d\boldsymbol{e}_+),\end{aligned}$$

for some $m_\times, m_+$. Note here that the error term $(-d^2\boldsymbol{e}_3 - \boldsymbol{e}_\times - d\boldsymbol{e}_+)$ of $\tilde{\boldsymbol{c}}$ has small norm, because $\boldsymbol{e}_3, \boldsymbol{e}_\times, \boldsymbol{e}_+$ have small norm and $\|d\|_1 \leq \kappa$.
Now, for an honest prover it can easily be seen that $\tilde{\boldsymbol{c}} = \boldsymbol{b}\tilde{r} + \tilde{\boldsymbol{e}}$ for $\tilde{r}$ and $\tilde{\boldsymbol{e}}$ as defined in the protocol, i.e., $\tilde{\boldsymbol{c}}$ is a commitment to 0. On the other hand, if a prover can prove that for at least three different challenges $d$, the multiplicative relation follows. This can be seen as follows. If

$$\mu_1\mu_2 - m_\times + d(\mu_1 m_2 + \mu_2 m_1 - m_+) + d^2(m_1 m_2 - m_3) = 0,$$

for three different values of $d$, this coefficient must be the zero-polynomial (in the indeterminate $d$), and thus $m_3 = m_1 m_2$. This is because a quadratic polynomial in $R_q$ can only have at most two distinct roots in $\mathcal{C}$. The proof of this claim is straightforward and thus omitted.

**Theorem 4.6.** *If the auxiliary commitment scheme is perfectly binding, then Protocol 4.7 is an honest-verifier zero-knowledge proof of knowledge with knowledge error* $2/\binom{n/2}{\kappa}$ *for the following relations:*

$$\mathcal{R}_{MLWE} = \left\{ ((\boldsymbol{a}, \boldsymbol{b}, x_1, x_2, \boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3), (m_1, m_2, m_3, r_1, r_2, r_3, \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)) : \right.$$
$$\left. \bigwedge_{i=1}^{3} (\boldsymbol{c}_i = \boldsymbol{a}m_i + \boldsymbol{b}r_i + \boldsymbol{e}_i \ \wedge \ \|\boldsymbol{e}_i\|_\infty \leq n) \ \wedge \ m_3 = m_1 m_2 \right\},$$

*and* $\mathcal{R}'_{MLWE}$ *is defined accordingly.*

$\mathsf{P}[\boldsymbol{c}_i; m_i, r_i, \boldsymbol{e}_i]$ $\qquad$ $\mathsf{V}[\boldsymbol{c}_i]$

$(i)$ $\quad \mu_1, \mu_2, \mu_3, \rho_1, \rho_2, \rho_3 \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$
$\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \boldsymbol{\eta}_3 \xleftarrow{\$} D^k_{\sigma_\eta}$
$\boldsymbol{t}_i = \boldsymbol{a}\mu_i + \boldsymbol{b}\rho_i + \boldsymbol{\eta}_i$ for $i = 1, 2, 3$

$(ii)$ $\quad m_+ = \mu_1 m_2 + \mu_2 m_1$
$m_\times = \mu_1 \mu_2$
$r_+, r_\times \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$
$\boldsymbol{e}_+, \boldsymbol{e}_\times \xleftarrow{\$} D^k_{\sigma_e}$
$\boldsymbol{c}_+ = \boldsymbol{a}m_+ + \boldsymbol{b}r_+ + \boldsymbol{e}_+$
$\boldsymbol{c}_\times = \boldsymbol{a}m_\times + \boldsymbol{b}r_\times + \boldsymbol{e}_\times$
$\mu_+, \mu_\times, \rho_+, \rho_\times \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$
$\boldsymbol{\eta}_+, \boldsymbol{\eta}_\times \xleftarrow{\$} D^k_{\sigma_\eta}$
$\boldsymbol{t}_+ = \boldsymbol{a}\mu_+ + \boldsymbol{b}\rho_+ + \boldsymbol{\eta}_+$
$\boldsymbol{t}_\times = \boldsymbol{a}\mu_\times + \boldsymbol{b}\rho_\times + \boldsymbol{\eta}_\times$

$(iii)$ $\tilde{\rho} \xleftarrow{\$} \mathbb{Z}_q[x]/\langle x^n + 1\rangle$
$\tilde{\boldsymbol{\eta}} \xleftarrow{\$} D^k_{\sigma_\eta}$
$\tilde{\boldsymbol{t}} = \boldsymbol{b}\tilde{\rho} + \tilde{\boldsymbol{\eta}}$
$(c_{\mathsf{aux}}, d_{\mathsf{aux}}) = \mathsf{aCom}(\boldsymbol{t}_+, \boldsymbol{t}_\times, \boldsymbol{t}_i, \tilde{\boldsymbol{t}}, \boldsymbol{c}_+, \boldsymbol{c}_\times)$

$\xrightarrow{\quad c_{\mathsf{aux}} \quad}$

$d \xleftarrow{\$} \mathcal{C}$

$\xleftarrow{\quad d \quad}$

$(i) + (ii)$ $s_{m_i} = \mu_i + d m_i$ for $i = 1, 2, 3, +, \times$
$s_{r_i} = \rho_i + d r_i$ for $i = 1, 2, 3, +, \times$
$s_{e_i} = \boldsymbol{\eta}_i + d\boldsymbol{e}_i$ for $i = 1, 2, 3, +, \times$

$(iii)$ $\quad s_{\tilde{r}} = \tilde{\rho} + d\tilde{r}$
$\tilde{\boldsymbol{e}} = -d^2 \boldsymbol{e}_3 - \boldsymbol{e}_\times - d\boldsymbol{e}_+$
$\tilde{r} = -d^2 r_3 - r_\times - d r_+$
$s_{\tilde{\boldsymbol{e}}} = \tilde{\boldsymbol{\eta}} + d\tilde{\boldsymbol{e}}$

abort-checks for $s_{\tilde{\boldsymbol{e}}}, s_{\boldsymbol{e}_j}$
$d_{\mathsf{aux}}, \boldsymbol{t}_+, \boldsymbol{t}_\times, \boldsymbol{t}_i, \tilde{\boldsymbol{t}}, \boldsymbol{c}_+, \boldsymbol{c}_\times, s_{m_i}, s_{r_i}, s_{\boldsymbol{e}_i}, s_{\tilde{r}}, s_{\tilde{\boldsymbol{e}}}$

$\xrightarrow{\qquad\qquad}$

$\mathsf{aVer}(c_{\mathsf{aux}}, d_{\mathsf{aux}}, (\boldsymbol{t}_+, \boldsymbol{t}_\times, \boldsymbol{t}_i, \tilde{\boldsymbol{t}}, \boldsymbol{c}_+, \boldsymbol{c}_\times)) \stackrel{?}{=} \mathsf{accept}$
$(i) + (ii)$ $\boldsymbol{t}_i + d\boldsymbol{c}_i \stackrel{?}{=} \boldsymbol{a}_i s_{m_i} + \boldsymbol{b} s_{r_i} + s_{\boldsymbol{e}_i}$ for $i = 1, 2, 3, +, \times$
$s_{\boldsymbol{e}_i} \stackrel{?}{\leq} \lfloor n^{4/3}/4 \rfloor$ for $i = 1, 2, 3, +, \times$
$(iii)$ $\tilde{\boldsymbol{c}} = \boldsymbol{a} s_{m_1} s_{m_2} - d^2 \boldsymbol{c}_3 - \boldsymbol{c}_\times - d\boldsymbol{c}_+$
$\tilde{\boldsymbol{t}} + d\tilde{\boldsymbol{c}} \stackrel{?}{=} \boldsymbol{b} s_{\tilde{r}} + s_{\tilde{\boldsymbol{e}}}$
$s_{\tilde{\boldsymbol{e}}} \stackrel{?}{\leq} \lfloor n^{4/3}/4 \rfloor$

**Protocol 4.7:** Proving multiplicative relations. The abort-checks are as in Protocol 4.1 and Theorem 2.5

## 5 Conclusion

We presented a simple and efficient string commitment scheme whose security is based on the hardness of the RLWE-problem, or, equivalently, on the hardness of solving certain problems on ideal lattices. Additionally we gave constructions for zero-knowledge proofs of knowledge of valid openings of such commitments, and for proving arbitrary relations among such messages. By achieving a negligible knowledge error in our protocols, we solve an open problem stated in previous work, e.g., Jain et al. [JKPT12].

## A Proofs

### A.1 Proofs of Theorem 4.5

The theorem is proved by showing that the protocol is a $\Sigma'_2$-protocol for the given relation. The claim then follows directly from the discussion in Sect. 2.2.

The proof is essentially a straightforward adaption of that of Theorem 4.2.

*Completeness.* This follows directly from the completeness of Protocol 4.1 and:

$$\begin{aligned} x_1 s_{m_1} + x_2 s_{m_2} &= x_1(\mu_1 + dm_1) + x_2(\mu_2 + dm_2) \\ &= (x_1\mu_1 + x_2\mu_2) + d(x_1 m_1 + x_2 m_2) = \mu_3 + dm_3 = s_{m_3}, \end{aligned}$$

*Special Soundness.* Given two accepting transcripts, we can extract witnesses $(\Delta_{m_i}, \Delta_{r_i}, \Delta_d, \Delta_{\boldsymbol{e}_i})$ for $\boldsymbol{c}_i$ $(i = 1, 2, 3)$ analogously to Theorem 4.2. The only thing that remains to show is that the linear relation $\Delta_{m_3} = x_1\Delta_{m_1} + x_2\Delta_{m_2}$ is indeed satisfied. This can be seen as follows:

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

*Special Honest-Verifier Zero-Knowledge.* The simulator is essentially given by three independent instances of that for Protocol 4.1, except that $s'_{m_3} = x_1 s'_{m_1} + x_2 s'_{m_2}$. The correctness of this simulation is shown by a standard argument, cf., e.g., [BGK+09, JKPT12].

### A.2 Proofs of Theorem 4.6

The theorem is proved by showing that the protocol is a $\Sigma'_3$-protocol for the given relation. The claim then follows directly from the discussion in Sect. 2.2.

*Completeness.* It is easy to see that V accepts with overwhelming probability when P does not abort.

*Special Soundness.* This follows from the soundness of Protocol 4.1 and 4.4 and the above considerations.

*Special Honest-Verifier Zero-Knowledge.* The intuition is the following: By the hiding property of our commitment scheme, $\boldsymbol{c}_+$ and $\boldsymbol{c}_\times$ computationally do not reveal any information about the secrets. Furthermore, as Protocol 4.1 is zero-knowledge, $s_{m_1}, s_{m_2}$ and consequently $\tilde{\boldsymbol{c}}$ do not reveal anything to the verifier either. The claim then follows from the proof of Theorem 4.2.

More formally, the simulator first computes $\tilde{\boldsymbol{c}}'$ as a commitment to 0, and similarly for $\boldsymbol{c}'_+$. It then runs the simulator for $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ and, assuming that no aborts happened, computes $\boldsymbol{c}'_\times = \tilde{\boldsymbol{c}}' + d^2\boldsymbol{c}_3 - \boldsymbol{a}s'_{m_1}s'_{m_2} + d\boldsymbol{c}_+$. It now runs the simulator for $\boldsymbol{c}'_\times, \boldsymbol{c}'_+, \tilde{\boldsymbol{c}}'$, and, again assuming no aborts, computes an auxiliary commitment, and outputs a transcript by appropriately arranging the messages. If in any step an abort occurred, it sets $(c'_{\mathsf{aux}}, d'_{\mathsf{aux}}) = \mathsf{aCom}(0)$ and returns $(c'_{\mathsf{aux}}, d, \perp)$. It can now be shown that the simulator outputs transcripts that are computationally indistinguishable from real protocol runs. Note therefore that even though the error distributions of $\tilde{\boldsymbol{c}}'$ and $\tilde{\boldsymbol{c}}$ (and of $\boldsymbol{c}'_\times$ and $\boldsymbol{c}_\times$, respectively) are not identical, the resulting commitments cannot be distinguished under the RLWE-assumption.

## References


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

[BCK+14] Benhamouda, F., Camenisch, J., Krenn, S., Lyubashevsky, V., Neven, G.: Better zero-knowledge proofs for lattice encryption and their application to group signatures. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 551–572. Springer, Heidelberg (2014)

[BDP00] Boyar, J., Damgård, I., Peralta, R.: Short non-interactive cryptographic proofs. J. Cryptology **13**(4), 449–472 (2000)

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

[BGK+09] Bangerter, E., Ghadafi, E., Krenn, S., Sadeghi, A.-R., Schneider, T., Smart, N.P., Tsay, J.-K., Warinschi, B.: Final Report on Unified Theoretical Framework of Efficient Zero-Knowledge Proofs of Knowledge. CACE Project Deliverable (2009)

[BLP+13] Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical Hardness of Learning with Errors. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) STOC 2009, pp. 575–584. ACM (2013)

[BPR12] Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 719–737. Springer, Heidelberg (2012)

[BV11a] Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011)

[BV11b] Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: FOCS (2011)

[CD97] Cramer, R., Damgård, I.: Linear zero-knowledge - a note on efficient zero-knowledge proofs and arguments. In: Leighton, F.T., Shor, P.W. (eds.) STOC 97, pp. 436–445. ACM (1997)

[CD98] Cramer, R., Damgård, I.B.: Zero-knowledge proofs for finite field arithmetic or: can zero-knowledge be for free? In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 424–441. Springer, Heidelberg (1998)

[CD09] Cramer, R., Damgård, I.: On the amortized complexity of zero-knowledge protocols. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 177–191. Springer, Heidelberg (2009)

[CKL+14] Camenisch, J., Krenn, S., Lehmann, A., Mikkelsen, G.L., Neven, G., Pedersen, M.Ø.: Formal treatment of privacy-enhancing credential systems. Cryptology ePrint Archive, Report 2014/708 (2014). http://eprint.iacr.org/

[Cra97] Cramer, R.: Modular Design of Secure yet Practical Cryptographic Protocols. Ph.D. thesis, CWI and University of Amsterdam (1997)

[Dam00] Damgård, I.B.: Efficient concurrent zero-knowledge in the auxiliary string model. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 418–430. Springer, Heidelberg (2000)

[Dam10] Damgård, I.: On $\Sigma$-Protocols, Lecture on Cryptologic Protocol Theory, Faculty of Science. University of Aarhus (2010)

[DPSZ12] Damgård, I., Pastro, V., Smart, N., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 643–662. Springer, Heidelberg (2012)

[DDLL13] Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal gaussians. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 40–56. Springer, Heidelberg (2013)

[DF02] Damgård, I.B., Fujisaki, E.: A statistically-hiding integer commitment scheme based on groups with hidden order. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 125–142. Springer, Heidelberg (2002)

[DGOW95] Damgård, I.B., Goldreich, O., Okamoto, T., Wigderson, A.: Honest verifier vs dishonest verifier in public coin zero-knowledge proofs. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 325–338. Springer, Heidelberg (1995)

[Fis01] Fischlin, M.: Trapdoor Commitment Schemes and Their Applications. Ph.D. thesis, Johann Wolfgang Goethe-Universität Frankfurt am Main (2001)

[FO97] Fujisaki, E., Okamoto, T.: Statistical zero knowledge protocols to prove modular polynomial relations. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 16–30. Springer, Heidelberg (1997)

[FS87] Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)

[Gen09] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Mitzenmacher, M. (eds.) STOC 2009, pp. 169–178. ACM (2009)

[GMR85] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems (extended abstract). In: STOC, pp. 291–304 (1985)

[GMW86] Goldreich, O., Micali, S., Wigderson, A.: How to prove all NP-statements in zero-knowledge and a methodology of cryptographic protocol design. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 171–185. Springer, Heidelberg (1987)

[GPV08] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (eds.) STOC 2008, pp. 197–206. ACM (2008)

[GS08] Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)

[IKOS07] Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-knowledge from secure multiparty computation. In: Johnson, D.S., Feige, U. (eds.) STOC 2007, pp. 21–30. ACM (2007)

[JKPT12] Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 663–680. Springer, Heidelberg (2012)

[KMO90] Kilian, J., Micali, S., Ostrovsky, R.: Minimum resource zero-knowledge proofs. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 545–546. Springer, Heidelberg (1990)

[KP98] Kilian, J., Petrank, E.: An efficient noninteractive zero-knowledge proof system for NP with general assumptions. J. Cryptology **11**(1), 1–27 (1998)

[KR06] Kalai, Y.T., Raz, R.: Succinct non-interactive zero-knowledge proofs with preprocessing for LOGSNP. In: FOCS 2006, pp. 355–366. IEEE Computer Society (2006)

[KV09] Katz, J., Vaikuntanathan, V.: Smooth projective hashing and password-based authenticated key exchange from lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 636–652. Springer, Heidelberg (2009)

[LNSW13] 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 (2013)

[LP11] Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 319–339. Springer, Heidelberg (2011)

[LPR10] 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 (2010)

[Lyu09] Lyubashevsky, V.: Fiat-shamir with aborts: applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 598–616. Springer, Heidelberg (2009)

[Lyu12] Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (2012)

[PR06] Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 145–166. Springer, Heidelberg (2006)

[Reg05] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005, pp. 84–93. ACM (2005)

[Rüc10] Rückert, M.: Lattice-based blind signatures. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 413–430. Springer, Heidelberg (2010)

[SSTX09] Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (2009)

[Ste93] Stern, J.: A new identification scheme based on syndrome decoding. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg (1994)

[XXW13] Xie, X., Xue, R., Wang, M.: Zero knowledge proofs from Ring-LWE. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 57–73. Springer, Heidelberg (2013)