Improved Lattice-Based Mix-Nets for Electronic Voting

Valeh Farzaliyev[1,2,3], Jan Willemson[1][0000−0002−6290−2099], and Jaan Kristjan Kaasik[1,3]

[1] Cybernetica AS, Narva mnt 20, 51009 Tartu, Estonia
[2] STACC OÜ, Narva mnt 20, 51009 Tartu, Estonia
[3] Tartu University, Narva mnt 18, 51009 Tartu, Estonia

Abstract. Mix-networks were first proposed by Chaum in the late 1970s – early 1980s [10] as a general tool for building anonymous communication systems. Classical mix-net implementations rely on standard public key primitives (e.g. ElGamal encryption) that will become vulnerable when a sufficiently powerful quantum computer will be built. Thus, there is a need to develop quantum-resistant mix-nets. This paper focuses on the application case of electronic voting where the number of votes to be mixed may reach hundreds of thousands or even millions. We propose an improved architecture for lattice-based post-quantum mix-nets featuring more efficient zero-knowledge proofs while maintaining established security assumptions. Our current implementation scales up to 100000 votes, still leaving a lot of room for future optimisation.

Keywords: Lattice-based post-quantum cryptography, mix-nets, zero-knowledge proofs, electronic voting, implementation

1 Introduction

Voting is the main mechanism of public opinion polling utilised e.g. in the context of general elections. Traditionally, voting has happened in a controlled location (polling station) to ease electoral management and reduce potential fraud.

However, by the beginning of the 21st century, people have become more mobile than ever before, so taking all the electorate into one place for a short period of time has become increasingly challenging. This challenge has been amplified by the recent COVID-19 outburst that has brought along the need to avoid gathering people in small spaces.

Thus, the need for the methods of remote voting has increased significantly. E.g. during the 2020 U.S. presidential elections, more than 65 million votes were sent in by post. Even though there seems to be little evidence of direct fraud, the extent of postal voting still caused a lot of controversy and discussion.

Indeed, the unreliability of postal services may raise questions about what to do with late votes, voter identification of postal votes is not particularly strong, and due to voting in an uncontrolled environment, it is hard to guarantee voting privacy and coercion-resistance.

Such problems motivate a search for alternatives, with remote electronic (Internet) voting being one of the prime candidates.

The votes stored on and transmitted via digital media are, contrary to paper votes, not directly perceivable by humans. Thus, the central problem of remote electronic voting is the independent verifiability of all the actions. In this paper, we are going to focus on a particular method of ensuring verifiability of the central voting system, since this is potentially the most critical point of failure.

What makes central server-side verification challenging is the need to also maintain the privacy of the votes. There are two main approaches used to implement privacy-preserving verifiable electronic voting systems – homomorphic tallying and mixing the votes before decryption [7]. There are a number of implementations known for both of these approaches, typically relying on some form of homomorphic encryption, e.g. Paillier or ElGamal scheme [24].

However, the classical asymmetric algorithms used in these implementations are known to become weak due to Shor's algorithm once a sufficiently capable quantum computer will be built [26]. Thus, looking for post-quantum alternatives is a necessity.

In recent years, both post-quantum homomorphic tallying [11, 25] and mixing [12, 27, 13] have been studied. In this paper, we will concentrate on quantum-resistant mix-nets, aiming at improving their efficiency in terms of the number of votes they are able to shuffle in a given time period.

As the most expensive part of a cryptographic mix-net is the generation and verification of zero-knowledge proofs of correct operation, we concentrate on improving these proofs. Technically, we build upon the recently proposed protocol by Costa *et al.* [13], implementing amortization techniques described by Attema *et al.* [4] and using a commitment scheme by Baum *et al.* [5].

As a result, we design a purely lattice-based zero-knowledge proof of a shuffle for lattice-based mixing scheme that can be scaled up to about 100000 votes. We instantiate the protocol with specific parameters such that the protocol achieves 128-bit soundness and 180-bit post-quantum encryption security level. Finally, we provide a proof-of-concept implementation of the proposed scheme and benchmark its practical performance.

The structure of this paper is as follows. In Section 2 we specify notation and Preliminaries used in the construction of the protocol and its security proof. The protocol itself is presented in Section 3. Implementation and experimental results are presented in Section 4. Finally, Section 5 draws some conclusions and sets directions for future work. Details of the proofs can be found in the Appendices.

2 Preliminaries

2.1 Notation

For a prime q, let $\mathbb{Z}_q$ be the ring of integers modulo q, with its elements considered in the interval $\left[-\frac{q-1}{2}, \frac{q-1}{2}\right]$, and let $\mathbb{Z}_n^\times$ denote the group of invertible elements modulo n. $\lfloor x \rceil$ represents the closest integer to x in $\mathbb{Z}_q$. Vectors over $\mathbb{Z}_q$ are denoted as $\overrightarrow{v} \in \mathbb{Z}_q^m$ and matrices over $\mathbb{Z}_q$ are denoted by regular capital letters (e.g. A) unless explicitly stated otherwise. Letting d be a power of two, we consider the rings $\mathcal{R} = \mathbb{Z}[X]/(X^d + 1)$ and $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^d + 1)$. Elements of these rings are written in bold lower-case letters (e.g. $\boldsymbol{p}$), and vectors with elements from these rings will naturally be denoted as $\overrightarrow{\boldsymbol{b}}$. Matrices over $\mathcal{R}$ or $\mathcal{R}_q$ are bold upper-case letters, e.g. $\boldsymbol{B}$. By default, all vectors and their concatenations are column vectors. More precisely, an element $\boldsymbol{a} \in \mathcal{R}_q$ can be written as column vector $\mathcal{V}_{\boldsymbol{a}} = |a_0, a_1, \ldots, a_{d-1}|^T$ where $\boldsymbol{a} = \sum_{i=0}^{d-1} a_i X^i$ and $a_i \in \mathbb{Z}_q$. Especially for ring $\mathcal{R}_q$, the same element can be represented as a matrix in $\mathbb{Z}_q$ when it is a multiplicand:

$$\mathcal{M}_{\boldsymbol{a}} = \begin{vmatrix} a_0 & -a_{d-1} & -a_{d-2} & \cdots & -a_1 \\ a_1 & a_0 & -a_{d-1} & \cdots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{d-1} & a_{d-2} & a_{d-3} & \cdots & a_0 \end{vmatrix} .$$

l_2 and l_∞ norms are defined as usual:

$$\|\boldsymbol{a}\|_\infty = \max_i |a_i| \text{ and } \|\boldsymbol{a}\|_2 = \sqrt{|a_0|^2 + \cdots + |a_{d-1}|^2} .$$

These norms can naturally be extended to vectors over $\mathcal{R}_q$. For $\overrightarrow{\boldsymbol{w}} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k\} \in \mathcal{R}_q^k$, we have

$$\|\overrightarrow{\boldsymbol{w}}\|_\infty = \max_i \|\boldsymbol{w}_i\| \text{ and } \|\overrightarrow{\boldsymbol{w}}\|_2 = \sqrt{\|\boldsymbol{w}_1\|_2^2 + \cdots + \|\boldsymbol{w}_k\|_2^2} .$$

Polynomials and vectors with short norms will simply be referred to as short.

2.2 Splitting Rings

In this work, we set $q - 1 \equiv 2l \bmod 4l$, so that $X^d + 1$ splits into l irreducible polynomials of degree d/l, i.e

$$X^d + 1 = \prod_{i \in \mathbb{Z}_{2l}^\times} (X^{d/l} - \zeta^i) \bmod q = \prod_{i=1}^{l} \boldsymbol{\varphi_i} \bmod q ,$$

where ζ is primitive $2l$-th root of unity in $\mathbb{Z}_q$ and $\boldsymbol{\varphi_i} = X^{d/l} - \zeta^{2i-1}$. Thus, the ring $\mathcal{R}_q$ is isomorphic to the product of the corresponding residue fields:

$$\mathcal{R}_q \cong \mathbb{Z}_q[X]/(\boldsymbol{\varphi}_1) \times \cdots \times \mathbb{Z}_q[X]/(\boldsymbol{\varphi}_l) .$$

We call a ring fully splitting when $l = d$.

The Number Theoretic Transform (NTT) of a polynomial $\boldsymbol{p} \in \mathcal{R}_q$ is defined as

$$\mathbf{NTT}(\boldsymbol{p}) = \begin{bmatrix} \hat{\boldsymbol{p}}_0 \\ \vdots \\ \hat{\boldsymbol{p}}_{l-1} \end{bmatrix} \text{ where } \hat{\boldsymbol{p}}_{i-1} = \boldsymbol{p} \bmod \boldsymbol{\varphi}_i.$$

By Chinese Remainder Theorem, there exists a unique inverse transformation – Inverse NTT – such that, $\mathbf{INTT}(\mathbf{NTT}(\boldsymbol{p})) = \boldsymbol{p}$. Also, NTT allows the computing of the product of two polynomials faster and saves time in other operations.

$$\begin{aligned} \boldsymbol{ab} &= \mathbf{INTT}(\mathbf{NTT}(\boldsymbol{a}) \circ \mathbf{NTT}(\boldsymbol{b})) \\ \mathbf{NTT}(\boldsymbol{a} + \boldsymbol{b}) &= \mathbf{NTT}(\boldsymbol{a}) + \mathbf{NTT}(\boldsymbol{b}) \end{aligned}$$

Here $\circ$ is the component-wise multiplication operation.

2.3 Ring-LWE Encryption, Module SIS/LWE

In our constructions, we will rely on hardness of Ring-LWE (RLWE) [21] and Module-LWE (MLWE)/ Module-SIS (MSIS) [14, 23] problems.

Definition 1 ($RLWE_\chi$)**.** *In the decisional Ring-LWE problem with an error distribution χ over $\mathcal{R}$, the probabilistic polynomial time (PPT) adversary $\mathcal{A}$ is asked to distinguish $(\boldsymbol{a}, \boldsymbol{b}) \overset{\$}{\leftarrow} \mathcal{R}_q \times \mathcal{R}_q$ from $(\boldsymbol{a}, \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e})$ for $\boldsymbol{a} \overset{\$}{\leftarrow} \mathcal{R}_q$ and $\boldsymbol{s}, \boldsymbol{e} \leftarrow \chi$.*

The corresponding *search*-RLWE problem asks to find $\boldsymbol{s}$ from several $(\boldsymbol{a}, \boldsymbol{b})$ RLWE samples. RLWE assumption is that *search*-RLWE and/or *decisional*-RLWE problem is hard for any PPT adversaries.

We implement the encryption scheme described in [21]. Let χ_1 be error distribution over $\mathcal{R}$ where each coefficient is sampled from $\{-1, 0, 1\}$.

- *KeyGen*: Given $\boldsymbol{a}$ uniformly sampled in $\mathcal{R}_q$, a secret $\boldsymbol{s} \leftarrow \chi_1$ and an error $\boldsymbol{e} \leftarrow \chi_1$, the public key is defined as $pk = (\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{a}, \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e})$ and private key as $\boldsymbol{s}$.
- *Encryption*: To encrypt a message $\boldsymbol{z} \in \mathcal{R}_2$, sample new randomness $\boldsymbol{r}$ and error terms $\boldsymbol{e}_1, \boldsymbol{e}_2$ from error distribution χ_1. Then the ciphertext is a pair of polynomials $(\boldsymbol{u}, \boldsymbol{v})$ such that

$$\begin{aligned} \boldsymbol{u} &= \boldsymbol{a} \cdot \boldsymbol{r} + \boldsymbol{e}_1 \ , \\ \boldsymbol{v} &= \boldsymbol{b} \cdot \boldsymbol{r} + \boldsymbol{e}_2 + \left\lfloor \frac{q}{2} \right\rceil \boldsymbol{z} \ . \end{aligned}$$

- *Decryption*: Given ciphertext $(\boldsymbol{u}, \boldsymbol{v})$, compute

$$\boldsymbol{v} - \boldsymbol{u} \cdot \boldsymbol{s} = (\boldsymbol{r} \cdot \boldsymbol{e} - \boldsymbol{e}_1 \cdot \boldsymbol{s} + \boldsymbol{e}_2) + \left\lfloor \frac{q}{2} \right\rceil \boldsymbol{z} \ .$$

  If each coefficient of the resulting polynomial is close to 0, set the respective coefficient of the decrypted message to 0. Otherwise, set the decrypted message as 1.

The RLWE encryption scheme defined as above is semantically secure under RLWE_{χ_1} assumption. To see this, just observe that the ciphertext consists of two RLWE samples, which by the RLWE_{χ_1} assumption are indistinguishable from uniformly random elements. Thus, unless one can solve the *decisional*-RLWE problem, all ciphertexts look uniform and no information can be extracted about the plaintext.

Definition 2 ($MLWE_{n,m,\chi}$)**.** *In the Module-LWE problem with parameters $n, m > 0$ and an error distribution χ over $\mathcal{R}$, the PPT adversary $\mathcal{A}$ is asked to distinguish $(\boldsymbol{A}, \overrightarrow{\boldsymbol{t}}) \xleftarrow{\$} \mathcal{R}_q^{m\times n} \times \mathcal{R}_q^m$ from $(\boldsymbol{A}, \boldsymbol{A}\overrightarrow{\boldsymbol{s}} + \overrightarrow{\boldsymbol{e}})$ for $\boldsymbol{A} \xleftarrow{\$} \mathcal{R}_q^{m\times n}$, a secret vector $\overrightarrow{\boldsymbol{s}} \leftarrow \chi^n$, and an error vector $\overrightarrow{\boldsymbol{e}} \leftarrow \chi^m$.*

Definition 3 ($MSIS_{m,n,\beta}$)**.** *The goal in the Module-SIS problem with parameters $n, m > 0$ and $0 < \beta < q$ is to find $\overrightarrow{\boldsymbol{x}} \in \mathcal{R}_q^m$ for a given matrix $\boldsymbol{A} \xleftarrow{\$} \mathcal{R}_q^{n\times m}$ such that $\boldsymbol{A}\overrightarrow{\boldsymbol{x}} = \overrightarrow{\boldsymbol{0}} \bmod q$ and $0 < \|\overrightarrow{\boldsymbol{x}}\|_\infty < \beta$.*

In practical security estimations, the parameter m in Definitions 2 and 3 does not play a crucial role, therefore we simply omit it and use the notations $\mathsf{MLWE}_{n,\chi}$ and $\mathsf{MSIS}_{n,\beta}$. Furthermore, we let the parameters μ and λ denote the module ranks for MSIS and MLWE, respectively.

2.4 Challenge space

Elements of the ring $\mathcal{R}_q$ are not always invertible. In fact, Lyubashevsky *et al.* proved a relation between the probability of invertibility in this ring and the number of residue fields it splits into [22, Corollary 1.2]. Their claim is that generally short non-zero polynomials are invertible. In lattice-based zero-knowledge proofs, the verifier often samples from a challenge set such that the difference between any two elements in that set is invertible. However, constructing such a set and uniformly sampling from it is not a trivial task.

Therefore, Lyubashevsky *et al.* proposed another method where they relaxed the invertiblity requirement. They defined the challenge space as the set of ternary polynomials $\mathcal{C} = \{-1, 0, 1\}^d \subset \mathcal{R}$. Coefficients of a challenge $\boldsymbol{c} \in \mathcal{C}$ are identically and independently distributed where 0 has probability $1/2$ and ± 1 both have probability $1/4$. In [4, Lemma 3.3], it is shown that if $\boldsymbol{c} \leftarrow \mathcal{C}$, the distribution of coefficients of $\boldsymbol{c} \mod (X^{d/l} - \zeta)$ is almost uniform and the maximum probability of coefficients over $\mathbb{Z}_q$ is bounded. Denote this bound with p. For example, in [4] it is estimated that $p = 2^{-31.44}$ for $l = d = 128$, $q \approx 2^{32}$. An element $\boldsymbol{c}$ in splitting ring $\mathcal{R}_q$ is non-invertible when $\boldsymbol{c} \mod \boldsymbol{\varphi}_i = 0$ for any $i = 1, \ldots, l$. Then the difference betwwen any two challenges $\bar{\boldsymbol{c}} = \boldsymbol{c} - \boldsymbol{c}'$ is non-invertible with probability at most $p^{d/l}$.

2.5 Error distribution and Rejection Sampling

Security of RLWE and MLWE problems depends on the error distribution. The original security proofs [21, 14] assumed the errors from discrete spherical Gaussian distribution. However, in literature we can find different choices such as centered binomial distribution [1, 16] or uniform distribution in a small interval [9]. We use the former for sampling randomness in MLWE and the latter for randomness and error terms in RLWE.

Rejection sampling. It is a common practice to hide secret commitment randomness $\overrightarrow{\boldsymbol{r}} \in \mathcal{R}_q^\kappa$ in another vector $\overrightarrow{\boldsymbol{z}}$ without leaking any information about

$\overrightarrow{\boldsymbol{r}}$. For this purpose, we use uniform rejection sampling technique from [16]. In the protocol the prover samples a "masking" vector $\overrightarrow{\boldsymbol{y}}$ using uniform distribution in $[-\delta+1, \delta]$. Upon receiving the challenge $\boldsymbol{c} \xleftarrow{\$} \mathcal{C}$ by the verifier, the prover responds with $\overrightarrow{\boldsymbol{z}} = \overrightarrow{\boldsymbol{y}} + \boldsymbol{c}\overrightarrow{\boldsymbol{r}}$. The dependency of $\overrightarrow{\boldsymbol{z}}$ on $\overrightarrow{\boldsymbol{r}}$ is removed if $\|\overrightarrow{\boldsymbol{z}}\|_\infty < \delta - \beta$ where $\|\boldsymbol{c}\overrightarrow{\boldsymbol{r}}\|_\infty \leq \beta$. Otherwise, the prover rejects the masked vector and aborts the protocol to start over again.

The expected number of repetitions M required by rejection sampling can be estimated by

$$1/M = \Big(\frac{2(\delta-\beta)-1}{2\delta-1}\Big)^{\kappa d} \approx e^{-\kappa d\beta/\delta} .$$

For more details see [16]. The parameter δ is typically chosen so that the expected value of M is small (say, 2 or 3).

2.6 Commitment scheme

In this work, we will be using a variant of BDLOP commitment scheme [5]. Let, $\boldsymbol{B}_0 \in \mathcal{R}_q^{\mu\times(\mu+\lambda+1)}$, $\overrightarrow{\boldsymbol{b}}_1 \in \mathcal{R}_q^{\mu+\lambda+1}$ and $\overrightarrow{\boldsymbol{r}} \leftarrow \chi_2^{(\mu+\lambda+1)d}$. The commitment of a single message $\boldsymbol{m} \in \mathcal{R}_q$ is a pair $(\overrightarrow{\boldsymbol{t}}_0, \boldsymbol{t}_1)$ where

$$\overrightarrow{\boldsymbol{t}}_0 = \boldsymbol{B}_0\overrightarrow{\boldsymbol{r}} ,$$
$$\boldsymbol{t}_1 = \langle \overrightarrow{\boldsymbol{b}}_1, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{m} .$$

It is easy to see that the commitment scheme is binding and hiding due to MSIS_μ and MLWE_λ assumptions, respectively.

Definition 4. *A weak opening for the commitment* $\overrightarrow{\boldsymbol{t}} = \overrightarrow{\boldsymbol{t}}_0 \| \boldsymbol{t}_1$ *consists of* l *polynomials* $\bar{\boldsymbol{c}}_i \in \mathcal{R}_q$*, randomness vector* $\overrightarrow{\boldsymbol{r}}^\star$ *over* $\mathcal{R}_q$ *and a message* $\boldsymbol{m}^\star \in \mathcal{R}_q$ *such that*

$$\|\bar{\boldsymbol{c}}_i\|_1 \leq 2d \textit{ and } \bar{\boldsymbol{c}}_i \bmod \boldsymbol{\varphi}_i \neq 0 \textit{ for all } 1 \leq i \leq l ,$$
$$\|\bar{\boldsymbol{c}}_i \overrightarrow{\boldsymbol{r}}^\star\|_\infty \leq 2\beta \textit{ for all } 1 \leq i \leq l ,$$
$$\boldsymbol{B}_0 \overrightarrow{\boldsymbol{r}}^\star = \overrightarrow{\boldsymbol{t}}_0 ,$$
$$\langle \overrightarrow{\boldsymbol{b}}_1, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}^\star = \boldsymbol{t}_1 .$$

The BDLOP commitment scheme is proven to be binding also with respect to the weak opening in [4, Lemma 4.3].

2.7 Generalized Schwartz-Zippel lemma

The generalized Schwartz-Zippel lemma is stated as follows [13, Appendix A].

Lemma 1. *Let* $p \in R[x_1, x_2, \ldots, x_n]$ *be a non-zero polynomial of total degree* $d \geq 0$ *over a commutative ring* R*. Let* S *be a finite subset of* R *such that none of the differences between two elements of* S *is a divisor of 0 and let* $r_1, r_2, \ldots, r_n$ *be selected at random independently and uniformly from* S*. Then* $Pr[p(r_1, r_2, \ldots, r_n) = 0] \leq d/|S|$.

In general, it is not trivial to construct the set S. A polynomial in $\mathcal{R}_q$ is a zero divisor when at least one of its NTT coefficients is zero. Thus, the difference between two elements is not a divisor of zero when they do not have a common NTT coefficient. There can be at most q pairwise different modulo degree 1 prime ideals for fully splitting rings. This strictly reduces soundness. However, for partially splitting rings, this number increases to $q^{d/l}$. For any random polynomial, one can find $q^{d/l}-1$ other polynomials which do not have common NTT coefficients and construct the set S. We fix this set to be $\mathcal{S} = \{\boldsymbol{f} \in \mathcal{R}_q \mid \deg \boldsymbol{f} < d/l\}$.

2.8 Mix-node security

Costa *et al.* [13] proposed a stronger security definition for a mix-node. Assume that **MixVotes** is a generic mixing algorithm such that, given input ciphertexts and a permutation vector, produces shuffled and re-encrypted ciphertexts. Moreover, let $z^{(i_{\mathcal{A}})}$ and $z^{\pi(j_{\mathcal{A}})}$ be the message before and after running the algorithm.

Definition 5. *Let J be a uniform random variable taking values in $[1,\dots,N]$. A mix-node given by algorithm **MixVotes** is said to be secure if the advantage of any PPT adversary $\mathcal{A}$ over random guess is negligible in the security parameter. That is, $\forall c$, $\exists \kappa_0$ s.t if $\kappa > \kappa_0$:*

$$\boldsymbol{Adv}_{\mathcal{A}}^{sec} = \left|\Pr\left[z^{(i_{\mathcal{A}})} = z^{\pi(j_{\mathcal{A}})}\right] - \Pr\left[z^{(i_{\mathcal{A}})} = z^{\pi(J)}\right]\right| < \frac{1}{\kappa^c} .$$

3 Improved mix-node

Our proof of shuffle protocol is based on Costa *et al.'s* work [13]. Assume that there are N RLWE ciphertexts $(\boldsymbol{u}_i, \boldsymbol{v}_i)$ encrypted with public key $(pk.\boldsymbol{a}, pk.\boldsymbol{b})$ to be shuffled. A mixing node will generate secret random zero encryption ciphertexts $(\boldsymbol{u}_{i,0}, \boldsymbol{v}_{i,0})$ and permutation π, and output $(\boldsymbol{u}'_i, \boldsymbol{v}'_i)$ such that

$$\begin{aligned}(\boldsymbol{u}_{i,0}, \boldsymbol{v}_{i,0}) &= (pk.\boldsymbol{a}\cdot \boldsymbol{r}_{E,i} + \boldsymbol{e}_{u,i}, pk.\boldsymbol{b}\cdot \boldsymbol{r}_{E,i} + \boldsymbol{e}_{v,i} + 0)\\ (\boldsymbol{u}'_i, \boldsymbol{v}'_i) &= (\boldsymbol{u}_{\pi(i)} + \boldsymbol{u}_{i,0}, \boldsymbol{v}_{\pi(i)} + \boldsymbol{v}_{i,0})\end{aligned}$$

where $\boldsymbol{r}_{E,i}, \boldsymbol{e}_{u,i}, \boldsymbol{e}_{v,i} \leftarrow \chi_1$ for all $i = 1,\dots,N$. We extend the proof in [13] for any spllitting rings in the full version of the paper [17] to show that if π is a valid permutation, then for any $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathcal{S}$ the equation

$$\prod_{i=1}^{N}(\boldsymbol{\beta} i + \boldsymbol{\alpha}^i - \boldsymbol{\gamma}) = \prod_{i=1}^{N}(\boldsymbol{\beta}\pi(i) + \boldsymbol{\alpha}^{\pi(i)} - \boldsymbol{\gamma}) \tag{1}$$

holds due to generalized Schwartz-Zippel lemma with small cheating probability. Furthermore,

$$\sum_{i=1}^{N}\boldsymbol{\alpha}^i \boldsymbol{u}_i = \sum_{i=1}^{N}\boldsymbol{\alpha}^{\pi(i)}(\boldsymbol{u}'_i - \boldsymbol{u}_{i,0}) \ , \tag{2}$$

$$\sum_{i=1}^{N} \boldsymbol{\alpha}^i \boldsymbol{v}_i = \sum_{i=1}^{N} \boldsymbol{\alpha}^{\pi(i)} (\boldsymbol{v}'_i - \boldsymbol{v}_{i,0}) \ . \tag{3}$$

One can think of (2) and (3) as two polynomials with coefficients in $\mathcal{R}_q$ evaluated at the same point $\boldsymbol{\alpha}$. Again, due to generalized Schwartz-Zippel lemma, if equality holds, then both polynomials are equal to each other, thus their coefficients are the same. Moreover, the relations (1), (2) and (3) along with proof of correct encryption are shown in [13] to be enough to argue for the correctness of shuffle.

The protocol in [13] uses a commitment scheme from [6] to prove the aforementioned arguments mainly due to the existence of zero-knowledge proofs for linear and multiplicative relations for the commitment scheme. We recap the protocol briefly below.

First, the prover $\mathcal{P}$ commits to zero encryption ciphertexts $(\boldsymbol{u}_{i,0}, \boldsymbol{v}_{i,0})$, sends them to the verifier $\mathcal{V}$ and runs amortized zero-knowledge proof of knowledge of small secret elements that those commitments are indeed commitments to encryptions of zero with valid error parameters. Next, $\mathcal{P}$ commits to the permutation vector π and sends the commitment to the verifier again. Committing to permutation vector means committing to $\pi(1), \ldots, \pi(N)$. Then, $\mathcal{V}$ samples a polynomial $\boldsymbol{\alpha}$ from the challenge set and sends it back to the prover. Following to that, $\mathcal{P}$ calculates commitments to $\boldsymbol{\alpha}^{\pi(1)}, \ldots, \boldsymbol{\alpha}^{\pi(N)}$. To show that the permutation vector is chosen before challenges and is a valid permutation, the prover runs linear and multiplicative relation proofs several times and calculates the product in (1) using the committed values. Next, again by the relation proofs, it proves the remaining two equalities to show shuffling is correct. During the verification phase, the verifier has to verify zero-knowledge proofs of knowledge of small secret elements and relations (1), (2) and (3).

Costa *et al.* [13] mention that it is possible to use amortization techniques described in [25] to reduce the complexity and total cost of the protocol. Unfortunately, they have not explicitly shown how to do that, nor have they instantiated the parameters to evaluate the performance and concrete security level of the protocol.

We solve both issues by replacing the commitment scheme with a variant of the Module SIS/LWE based commitment scheme from [5]. This allows us to use more efficient zero-knowledge arguments for proving linear and product relations between committed messages [4, 20]. Those protocols are short, efficient, and have no extra cost when amortized over many relations. Besides, there is no need to repeat the protocol several times to get desired soundness properties. Nevertheless, as we change the mathematical setting, there is a need for additional careful analysis of security.

For example, another change we introduce is regarding challenge sets. Previously, prime modulus q was required to satisfy $q \equiv 3 \bmod 8$, which implies that the ring $\mathcal{R}_q$ splits only into two residue fields. This condition is required to define a concrete sufficiently large set of challenge polynomials of which any of the differences between two elements in this set is invertible. Now, we relax this restriction and allow q to split into more than 2 residue fields.

Now we proceed to describe our protocol.

First, let μ and λ be rank of secure MSIS and MLWE instances, respectively, $q - 1 \equiv 2l \bmod 4l$ be such that $\mathcal{R}_q$ is a partially splitting ring and $\boldsymbol{B}_0 \in \mathcal{R}_q^{\mu \times (\mu+\lambda+9N+1)}$, $\overrightarrow{\boldsymbol{b}}_1, \overrightarrow{\boldsymbol{b}}_2, \ldots \overrightarrow{\boldsymbol{b}}_{9N+1} \in \mathcal{R}_q^{\mu+\lambda+9N+1}$. Furthermore, set $q^{d/l} \approx 2^{256}$ and $\beta_i' = \delta_i - \beta_i - 1$ for $i = 1, 2$.

Theorem 1. *The protocol in Figure 1 is statistically complete, computationally honest verifier zero-knowledge under the Module-LWE assumption, computationally special-sound under the Module-SIS assumption, and is a computationally secure mix-node under* RLWE_{χ_1} *and* $\mathrm{MSIS}_{\mu,8d\beta_2'}$ *assumptions. That is, if p is the maximum probability over $\mathbb{Z}_q$ of the coefficients of $\boldsymbol{c} \mod X^{d/l} - \zeta$, then*

- *for completeness, in case of non-aborting transcript due to rejection sampling, the honest verifier $\mathcal{V}$ is always convinced.*
- *For zero-knowledge, there exists a simulator Sim that, without access to secret information, outputs a simulation of accepting the transcript of the protocol. Any adversary capable of distinguishing an actual transcript from a simulated one with an advantage ϵ also has an advantage ϵ in distinguishing* $\mathrm{MLWE}_{\lambda,\chi_2}$ *within the same running time.*
- *For soundness, there is an extractor $\mathcal{E}$ with rewindable black-box access to a deterministic prover $\mathcal{P}^\star$ that convinces $\mathcal{V}$ with probability $\epsilon \geq (3p)^k$, either outputting a weak opening for commitment*

$$\overrightarrow{\boldsymbol{t}} = \overrightarrow{\boldsymbol{t}}_0 \| \boldsymbol{t}_{u_0^{(i)}} \| \boldsymbol{t}_{v_0^{(i)}} \| \boldsymbol{t}_{\pi(i)} \| \boldsymbol{t}_{\boldsymbol{\alpha}^{\pi(i)}} \| \boldsymbol{t}_{4N+1} \| \ldots \| \boldsymbol{t}_{9N+1}$$

  such that extracted messages satisfy equations (1), (2) and (3), or being able to solve $\mathrm{MSIS}_{\mu,8d\beta_1'}$

- *And finally, an adversary with advantage ϵ over random guessing has also advantage over* $\mathrm{MSIS}_{\mu,8d\beta_2'}$ *and/or* RLWE_{χ_1} *problems with probability at least ϵ.*

Prover $\mathcal{P}$ | Verifier $\mathcal{V}$

$\boldsymbol{u}_i, \boldsymbol{u}_{i,0}, \boldsymbol{u}'_i \in \mathcal{R}_q$ | $\boldsymbol{u}_i, \boldsymbol{u}'_i$
$\boldsymbol{v}_i, \boldsymbol{v}_{i,0}, \boldsymbol{v}'_i \in \mathcal{R}_q$ | $\boldsymbol{v}_i, \boldsymbol{v}'_i$
$\kappa = \mu + \lambda + 9N + 1$
$\boldsymbol{B}_0 \in \mathcal{R}_q^{\mu\times\kappa};\ \overrightarrow{\boldsymbol{b}}_0, \overrightarrow{\boldsymbol{b}}_1, \dots, \overrightarrow{\boldsymbol{b}}_{9N+1} \in \mathcal{R}_q^{\kappa}$ | $\boldsymbol{B}_0, \overrightarrow{\boldsymbol{b}}_1, \dots, \overrightarrow{\boldsymbol{b}}_{9N+1}$
$\pi = \mathrm{Perm}(N)$

$\overrightarrow{\boldsymbol{r}} \in \chi_2^{\kappa d};$
$\overrightarrow{\boldsymbol{t}}_0 = \boldsymbol{B_0}\overrightarrow{\boldsymbol{r}}$
For $i = 1, \dots, N$
$\boldsymbol{t}_{u_{i,0}} = \langle \overrightarrow{\boldsymbol{b}}_i, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{u}_{i,0}$
$\boldsymbol{t}_{v_{i,0}} = \langle \overrightarrow{\boldsymbol{b}}_{N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{v}_{i,0}$
$\boldsymbol{t}_{\pi(i)} = \langle \overrightarrow{\boldsymbol{b}}_{2N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \pi(i)$
Shortness proof Σ_1

$\xrightarrow{\overrightarrow{t}_0, t_{\pi(i)}, t_{u_{i,0}}, t_{v_{i,0}}, \Sigma_1}$ $\boldsymbol{\alpha}\ \in \mathcal{S}$
$\xleftarrow{\boldsymbol{\alpha}}$

for $i = 1, \dots, N$:
$\boldsymbol{t}_{\boldsymbol{\alpha}^{\pi(i)}} = \langle \overrightarrow{\boldsymbol{b}}_{3N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{\alpha}^{\pi(i)}$
$\boldsymbol{t}_{4N+i} = \langle \overrightarrow{\boldsymbol{b}}_{4N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{\alpha}^{\pi(i)}\boldsymbol{u}_{i,0}$
$\boldsymbol{t}_{5N+i} = \langle \overrightarrow{\boldsymbol{b}}_{5N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{\alpha}^{\pi(i)}\boldsymbol{v}_{i,0}$

$\xrightarrow{t_{\boldsymbol{\alpha}^{\pi(i)}}, t_{4N+i}, t_{5N+i}}$ $\boldsymbol{\beta}, \boldsymbol{\gamma}\ \in \mathcal{S}$
$\xleftarrow{\boldsymbol{\beta}, \boldsymbol{\gamma}}$

$\boldsymbol{\Pi} = 1$
for $i = 1, \dots, N$:
$\boldsymbol{t}_{6N+i} = \langle \overrightarrow{\boldsymbol{b}}_{6N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{\beta}\pi(i) + \boldsymbol{\alpha}^{\pi(i)} - \boldsymbol{\gamma}$
$\boldsymbol{t}_{7N+i} = \langle \overrightarrow{\boldsymbol{b}}_{7N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{\Pi}$
$\boldsymbol{t}_{8N+i} = \langle \overrightarrow{\boldsymbol{b}}_{8N+i}, \overrightarrow{\boldsymbol{r}} \rangle + \boldsymbol{\Pi}(\boldsymbol{\beta}\pi(i) + \boldsymbol{\alpha}^{\pi(i)} - \boldsymbol{\gamma})$
$\boldsymbol{\Pi} = \boldsymbol{\Pi} \cdot (\boldsymbol{\beta}\pi(i) + \boldsymbol{\alpha}^{\pi(i)} - \boldsymbol{\gamma})$

$\xrightarrow{t_{6N+i}, t_{7N+i}, t_{8N+i}}$

$\overrightarrow{\boldsymbol{y}} \overset{\$}{\leftarrow} [-\delta_1 + 1, \delta_1]^{\kappa d}$
$\overrightarrow{\boldsymbol{w}} = \boldsymbol{B}_0\overrightarrow{\boldsymbol{y}}$

$\xrightarrow{\overrightarrow{w}}$
$\xleftarrow{\boldsymbol{\epsilon}}$ $\boldsymbol{\epsilon}_1, \boldsymbol{\epsilon}_2, \dots, \boldsymbol{\epsilon}_{(4N+4)} \in \mathcal{R}_q$

$\boldsymbol{v}_1 = \sum_{j=1}^{N} \boldsymbol{\epsilon}_j \Big(\boldsymbol{\beta}\langle \overrightarrow{\boldsymbol{b}}_{2N+j}, \overrightarrow{\boldsymbol{y}} \rangle + \langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}} \rangle - \langle \overrightarrow{\boldsymbol{b}}_{6N+j}, \overrightarrow{\boldsymbol{y}} \rangle\Big)$
$\boldsymbol{v}_2 = \langle \overrightarrow{\boldsymbol{b}}_{9N+1}, \overrightarrow{\boldsymbol{y}}_0 \rangle + \sum_{j=1}^{N} \boldsymbol{\epsilon}_{N+j}(\langle \overrightarrow{\boldsymbol{b}}_{6N+j}, \overrightarrow{\boldsymbol{y}} \rangle\langle \overrightarrow{\boldsymbol{b}}_{7N+j}, \overrightarrow{\boldsymbol{y}} \rangle)+$
$+\sum_{i=0}^{k-1}\sum_{j=1}^{N} \boldsymbol{\epsilon}_{2N+j}(\langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}} \rangle\langle \overrightarrow{\boldsymbol{b}}_{j}, \overrightarrow{\boldsymbol{y}} \rangle)+$
$+\sum_{j=1}^{N} \boldsymbol{\epsilon}_{3N+j}(\langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}} \rangle\langle \overrightarrow{\boldsymbol{b}}_{N+j}, \overrightarrow{\boldsymbol{y}} \rangle)$

$\boldsymbol{t}_{9N+1} = \langle \overrightarrow{\boldsymbol{b}}_{9N+1}, \overrightarrow{\boldsymbol{r}} \rangle + \sum_{j=1}^{N} \boldsymbol{\epsilon}_{N+j}\big(\langle \overrightarrow{\boldsymbol{b}}_{8N+j}, \overrightarrow{\boldsymbol{y}} \rangle-$
$-\Pi\langle \overrightarrow{\boldsymbol{b}}_{6N+j}, \overrightarrow{\boldsymbol{y}} \rangle - (\boldsymbol{\beta}\pi(j) + \boldsymbol{\alpha}^{\pi(j)} - \boldsymbol{\gamma})\langle \overrightarrow{\boldsymbol{b}}_{7N+j}, \overrightarrow{\boldsymbol{y}} \rangle\big)+$
$+\sum_{j=1}^{N} \boldsymbol{\epsilon}_{2N+j}\big(\langle \overrightarrow{\boldsymbol{b}}_{4N+j}, \overrightarrow{\boldsymbol{y}} \rangle - \boldsymbol{\alpha}^{\pi(j)}\langle \overrightarrow{\boldsymbol{b}}_{j}, \overrightarrow{\boldsymbol{y}} \rangle - \boldsymbol{u}_{j,0}\langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}}_i \rangle\big)+$
$+\sum_{j=1}^{N} \boldsymbol{\epsilon}_{3N+j}\big(\langle \overrightarrow{\boldsymbol{b}}_{5N+j}, \overrightarrow{\boldsymbol{y}} \rangle - \boldsymbol{\alpha}^{\pi(j)}\langle \overrightarrow{\boldsymbol{b}}_{N+j}, \overrightarrow{\boldsymbol{y}} \rangle - \boldsymbol{v}_{j,0}\langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}} \rangle\big)$

$\boldsymbol{v}_3 = \boldsymbol{\epsilon}_{4N+1}\big(\sum_{j=1}^{N} \boldsymbol{u}'_j\langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}} \rangle - \sum_{j=1}^{N}\langle \overrightarrow{\boldsymbol{b}}_{4N+j}, \overrightarrow{\boldsymbol{y}} \rangle\big)+$
$+\boldsymbol{\epsilon}_{4Nk+2}\big(\sum_{j=1}^{N} \boldsymbol{v}'_j\langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}} \rangle - \sum_{j=1}^{N}\langle \overrightarrow{\boldsymbol{b}}_{5N+j}, \overrightarrow{\boldsymbol{y}} \rangle\big)$
$\boldsymbol{v}_4 = \boldsymbol{\epsilon}_{4N+3}(\langle \overrightarrow{\boldsymbol{b}}_{9N}, \overrightarrow{\boldsymbol{y}} \rangle) + \boldsymbol{\epsilon}_{4N+4}(\langle \overrightarrow{\boldsymbol{b}}_{7N+1}, \overrightarrow{\boldsymbol{y}} \rangle)$

$\xrightarrow{v_1, v_2, v_3, v_4, t_{9N+1}}$
$\xleftarrow{c}$ $\boldsymbol{c} \overset{\$}{\leftarrow} C$

$\overrightarrow{\boldsymbol{z}} = \overrightarrow{\boldsymbol{y}} + \boldsymbol{c}\overrightarrow{\mathbf{r}}$
If $\|\overrightarrow{\boldsymbol{z}}\|_\infty \geq \delta_1 - \beta_1$, abort $\xrightarrow{\overrightarrow{z}}$ **Verify**

Fig. 1. ZK-proof of shuffle

Verify

Verify Shortness proof Σ_1

$$||\overrightarrow{\boldsymbol{z}}||_\infty \overset{?}{<} \delta_1 - \beta_1$$
$$\boldsymbol{B}_0 \overrightarrow{\boldsymbol{z}} \overset{?}{=} \overrightarrow{\boldsymbol{w}} + \boldsymbol{c}\, \overrightarrow{\boldsymbol{t}}_0$$

For $j = 1, \dots N$:

$$\begin{aligned}
\boldsymbol{f}^{u_0^{(j)}} &= \langle \overrightarrow{\boldsymbol{b}}_j, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{u_{j,0}} \\
\boldsymbol{f}^{v_0^{(i)}} &= \langle \overrightarrow{\boldsymbol{b}}_{N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{v_{j,0}} \\
\boldsymbol{f}^{\pi(j)} &= \langle \overrightarrow{\boldsymbol{b}}_{2N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{\pi(j)} \\
\boldsymbol{f}^{\boldsymbol{\alpha}^{\pi(j)}} &= \langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{\boldsymbol{\alpha}^{\pi(j)}} \\
\boldsymbol{f}^{4N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{4N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{4N+j} \\
\boldsymbol{f}^{5N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{5N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{5N+j} \\
\boldsymbol{f}^{6N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{6N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{6N+j} \\
\boldsymbol{f}^{7N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{7N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{7N+j} \\
\boldsymbol{f}^{8N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{8N+j}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{8N+j}
\end{aligned}$$

$$\boldsymbol{f}_{9N+1} = \langle \overrightarrow{\boldsymbol{b}}_{9N+1}, \overrightarrow{\boldsymbol{z}} \rangle - \boldsymbol{c}\boldsymbol{t}_{9N+1}$$

$$\textstyle\sum_{j=1}^N \boldsymbol{\epsilon}_j \Big(\boldsymbol{\beta}\boldsymbol{f}^{\pi(j)} + \boldsymbol{f}^{\boldsymbol{\alpha}^{\pi(j)}} - \boldsymbol{f}^{6N+j} + \boldsymbol{c}\boldsymbol{\gamma} \Big) \overset{?}{=} \boldsymbol{v}_1$$

$$\begin{aligned}
&\textstyle\sum_{j=1}^N \boldsymbol{\epsilon}_{N+j}(\boldsymbol{f}^{6N+j}\boldsymbol{f}^{7N+j} + \boldsymbol{c}\boldsymbol{f}^{8N+j})+ \\
&\qquad + \textstyle\sum_{j=1}^N \boldsymbol{\epsilon}_{2N+j}(\boldsymbol{f}^{\boldsymbol{\alpha}^{\pi(j)}}\boldsymbol{f}^{u_0^{(j)}} + \boldsymbol{c}\boldsymbol{f}^{4N+j})+ \\
&\qquad + \textstyle\sum_{j=1}^N \boldsymbol{\epsilon}_{3N+j}(\boldsymbol{f}^{\boldsymbol{\alpha}^{\pi(j)}}\boldsymbol{f}^{v_0^{(j)}} + \boldsymbol{c}\boldsymbol{f}^{5N+j}) + \boldsymbol{f}_{9N+1} \overset{?}{=} \boldsymbol{v}_2
\end{aligned}$$

$$\begin{aligned}
&M_1 = \textstyle\sum_{i=1}^N \boldsymbol{\alpha}^i \boldsymbol{u}_i \quad M_2 = \textstyle\sum_{i=1}^N \boldsymbol{\alpha}^i \boldsymbol{v}_i \\
&\boldsymbol{\epsilon}_{4N+1}\big(\textstyle\sum_{j=1}^N \boldsymbol{u}'_j \boldsymbol{f}^{\boldsymbol{\alpha}^{\pi(j)}} - \textstyle\sum_{j=1}^N \boldsymbol{f}^{4N+j} + \boldsymbol{c}M_1 \big)+ \\
&\qquad +\boldsymbol{\epsilon}_{4N+2}\big(\textstyle\sum_{j=1}^N \boldsymbol{v}'_j \boldsymbol{f}^{\boldsymbol{\alpha}^{\pi(j)}} - \textstyle\sum_{j=1}^N \boldsymbol{f}^{5N+j} + \boldsymbol{c}M_2 \big) \overset{?}{=} \boldsymbol{v}_3
\end{aligned}$$

$$\begin{aligned}
&\mathit{\Pi} = \textstyle\prod_{j=1}^N (\boldsymbol{\beta}j + \boldsymbol{\alpha}^j - \boldsymbol{\gamma}) \\
&\boldsymbol{\epsilon}_{4N+3}(\boldsymbol{f}^{9N} + \boldsymbol{c}\mathit{\Pi}) + \boldsymbol{\epsilon}_{4N+4}(\boldsymbol{f}^{7N+1} + \boldsymbol{c}) \overset{?}{=} \boldsymbol{v}_4
\end{aligned}$$

Fig. 2. Verification equations

Proof. Completeness. Observe that in a non-aborting transcript vector $\overrightarrow{\boldsymbol{z}}$ is bounded by $\delta_1 - \beta_1$. The remaining four verification equations in Figure 2 regarding $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ and $\boldsymbol{v}_4$ are straightforward to verify. Similarly, proof of shortness protocol is complete.

Zero-knowledge. Zero-knowledge property of proof of shortness protocol is given in [20]. Indeed, following the same steps, it is possible to simulate this protocol as well. First, sample $\overrightarrow{\boldsymbol{z}} \xleftarrow{\$} [-(\delta_1 - \beta_1) + 1, \delta_1 - \beta_1 - 1]^{\kappa d}$, which is the distribution of $\overrightarrow{\boldsymbol{z}}$ in non-aborting transcript. Next, due to rejection sampling step, $\boldsymbol{c}\overrightarrow{\boldsymbol{r}}$ is independent of $\overrightarrow{\boldsymbol{z}}$ and thus the simulator chooses $\boldsymbol{c} \xleftarrow{\$} C$, $\overrightarrow{\boldsymbol{r}} \in \chi_2^{ld}$ like an honest prover. Now, the simulator can calculate $\overrightarrow{\boldsymbol{w}}$ which is uniquely determined by previous variables. Other challenges $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathcal{S}$ are independent of each other, thus they can also be randomly chosen. Straightforwardly, the simulator computes $\overrightarrow{\boldsymbol{t}}_0$. The rest of commitments can be uniformly sampled from $\mathcal{R}_q$ as by the MLWE assumption they will be indistinguishable from real MLWE samples. Finally, remaining equations of $\boldsymbol{v}_i$ are deterministic functions of $\overrightarrow{\boldsymbol{t}}$, $\overrightarrow{\boldsymbol{z}}$ and $\boldsymbol{c}$.

Soundness. The soundness relation for proof of shortness protocol is described in detail in [20] and is similar to the proof for a protocol in Figure 1. Consider the extractor given in [4] which can extract weak openings after rewinding the protocol l times and get $\overrightarrow{\boldsymbol{r}}^\star$ and $\overrightarrow{\boldsymbol{y}}^\star$, or finds $\mathsf{MSIS}_{8d\beta_1}$ solution for $\boldsymbol{B}_0$. It can also extract messages simply from commitment relations.

$$\begin{aligned}
\boldsymbol{t}_{u_{i,0}} &= \langle \overrightarrow{\boldsymbol{b}}_i, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_0^{(i)\star} \\
\boldsymbol{t}_{v_{i,0}} &= \langle \overrightarrow{\boldsymbol{b}}_{N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_1^{(i)\star} \\
\boldsymbol{t}_{\pi(i)} &= \langle \overrightarrow{\boldsymbol{b}}_{2N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_2^{(i)\star} \\
\boldsymbol{t}_{\boldsymbol{\alpha}^{\pi(i)}} &= \langle \overrightarrow{\boldsymbol{b}}_{3N+i}, \overrightarrow{\boldsymbol{r}}\star \rangle + \boldsymbol{m}_3^{(i)\star} \\
\boldsymbol{t}_{4N+i} &= \langle \overrightarrow{\boldsymbol{b}}_{4N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_4^{(i)\star} \\
\boldsymbol{t}_{5N+i} &= \langle \overrightarrow{\boldsymbol{b}}_{5N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_5^{(i)\star} \\
\boldsymbol{t}_{6N+i} &= \langle \overrightarrow{\boldsymbol{b}}_{6N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_6^{(i)\star} \\
\boldsymbol{t}_{7N+i} &= \langle \overrightarrow{\boldsymbol{b}}_{7N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_7^{(i)\star} \\
\boldsymbol{t}_{8N+i} &= \langle \overrightarrow{\boldsymbol{b}}_{8N+i}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_8^{(i)\star} \\
\boldsymbol{t}_{9N+1} &= \langle \overrightarrow{\boldsymbol{b}}_{9N+1}, \overrightarrow{\boldsymbol{r}}^\star \rangle + \boldsymbol{m}_9^\star
\end{aligned}$$

Setting $\overrightarrow{\boldsymbol{z}}^\star = \overrightarrow{\boldsymbol{y}}^\star + \boldsymbol{c}\overrightarrow{\boldsymbol{r}}^\star$, masked openings are defined below.

$$
\begin{aligned}
\boldsymbol{f}^{u_{j,0}} &= \langle \overrightarrow{\boldsymbol{b}}_j, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_0^{(j)\star} \\
\boldsymbol{f}^{v_{j,0}} &= \langle \overrightarrow{\boldsymbol{b}}_{N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_1^{(j)\star} \\
\boldsymbol{f}^{\pi(j)} &= \langle \overrightarrow{\boldsymbol{b}}_{2N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_2^{(j)\star} \\
\boldsymbol{f}^{\alpha_0^{\pi(j)}} &= \langle \overrightarrow{\boldsymbol{b}}_{3N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_3^{(j)\star} \\
\boldsymbol{f}^{4N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{4N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_4^{(j)\star} \\
\boldsymbol{f}^{5N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{5N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_5^{(j)\star} \\
\boldsymbol{f}^{6N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{6N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_6^{(j)\star} \\
\boldsymbol{f}^{7N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{7N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_7^{(j)\star} \\
\boldsymbol{f}^{8N+j} &= \langle \overrightarrow{\boldsymbol{b}}_{8N+j}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_8^{(j)\star} \\
\boldsymbol{f}^{9N+1} &= \langle \overrightarrow{\boldsymbol{b}}_{9N+1}, \overrightarrow{\boldsymbol{y}}^{\star} \rangle - \boldsymbol{c}\boldsymbol{m}_9^{(j)\star}
\end{aligned}
$$

Now, let's substitute those terms to their respective places in verification equations. After simplifications (see the full version of the paper [17]) and following the argument in [4, Theorem 5.1], for some j, $\Pr[\boldsymbol{\beta}\boldsymbol{m}_2^{(j)\star} + \boldsymbol{m}_3^{(j)\star} - \boldsymbol{m}_6^{(j)\star} + \boldsymbol{\gamma} \neq 0] = \epsilon < (3p)^k$. Similarly, with the same probability bound, we get $\boldsymbol{m}_0^{(j)\star}\boldsymbol{m}_3^{(j)\star} - \boldsymbol{m}_4^{(j)\star} \neq 0$; $\boldsymbol{m}_1^{(j)\star}\boldsymbol{m}_3^{(j)\star} - \boldsymbol{m}_5^{(j)\star} \neq 0$ and $\boldsymbol{m}_6^{(j)\star}\boldsymbol{m}_7^{(j)\star} - \boldsymbol{m}_8^{(j)\star} \neq 0$ altogether, or $\sum_{j=1}^N \boldsymbol{u}'_j\boldsymbol{m}_3^{(j)\star} - \sum_{j=1}^N \boldsymbol{m}_4^{(j)\star} - M_1 \neq 0$ and $\sum_{j=1}^N \boldsymbol{v}'_j\boldsymbol{m}_3^{(j)\star} - \sum_{j=1}^N \boldsymbol{m}_5^{(j)\star} - M_2 \neq 0$; and $\boldsymbol{m}_8^{(N)\star} - \mathit{\Pi} \neq 0$.

Combining all extracted relations we obtain

$$
\begin{aligned}
\prod_{j}^{N}(\boldsymbol{\beta}\boldsymbol{m}_2^{(j)\star} + \boldsymbol{m}_3^{(j)\star} - \boldsymbol{\gamma}) = \mathit{\Pi} = \prod_{j}^{N}(\boldsymbol{\beta}j + \boldsymbol{\alpha}^j - \boldsymbol{\gamma}) \ , \\
\sum_{j}^{N} \boldsymbol{m}_3^{(j)\star}(\boldsymbol{u}'_j - \boldsymbol{m}_0^{(j)\star}) = M_1 = \sum_{i=1}^{N} \boldsymbol{\alpha}^i \boldsymbol{u}_i \ , \\
\sum_{j}^{N} \boldsymbol{m}_3^{(j)\star}(\boldsymbol{v}'_j - \boldsymbol{m}_1^{(j)\star}) = M_2 = \sum_{i=1}^{N} \boldsymbol{\alpha}^i \boldsymbol{v}_i \ .
\end{aligned}
$$

Mix-Node Security. Once more, we refer to [13] where mix-node security is proved using a game-based approach. By following exactly the same steps, and only replacing statistical closeness of Game 0 and Game 1 with computational closeness under $\mathsf{MLWE}_{8d\beta_2}$ assumption guaranteeing shortness error terms in RLWE encryptions, it is possible to show that the advantage of an adversary over random guessing is bounded by

$$\epsilon = \mathbf{Adv}_{\mathcal{A}}^{sec}(\kappa) \leq \epsilon_{MLWE} + \epsilon_{RLWE} \ .$$

3.1 Non-interactivity and proof size

The protocol in Figure 1 can be made non-interactive with the help of Fiat-Shamir transformation. In other words, challenges are computed by the prover by hashing all previous messages and public information. Furthermore, instead of sending $\overrightarrow{\boldsymbol{w}}, \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4$ which are used as inputs to the hash function to generate challenges, the standard technique is to send the hash output and let the verifier recompute those values from verification equations and check that the hashes of the computed input terms match with the prover's hash. Thus, it is enough to send the commitment $\overrightarrow{\boldsymbol{t}}_0 \| \boldsymbol{t}_1 \| \cdots \| \boldsymbol{t}_{9N}$, garbage term $\boldsymbol{t}_{9N+1}$ and vector $\overrightarrow{\boldsymbol{z}}$. A polynomial in $\mathcal{R}_q$ consists of d coefficients less than q, so it takes $d\lfloor \log q \rfloor$ bits at most. $\overrightarrow{\boldsymbol{t}}_0$ and $\overrightarrow{\boldsymbol{z}}$ consist of μ and $\lambda + \mu + 9N + 1$ polynomials, respectively. The full cost of shortness proof is analysed in the full version of the paper [17]. Combining all of these, the size of accepting transcript for our protocol is

$$\begin{aligned}
&(\mu + 9N + 1)d\lfloor \log q \rfloor + (\lambda + \mu + 9N + 1)d\lfloor \log q \rfloor + 256+ \\
&+ (2\lambda + 10N)\frac{d^2}{l}\lfloor \log q \rfloor + (\lambda + 2\mu + 7)d\lfloor \log q \rfloor + 256 = \\
&= \left(18 + \frac{10d}{l}\right) Nd\lfloor \log q \rfloor + (2\lambda(1 + d/l) + 4\mu + 9)d\lfloor \log q \rfloor + 512 \; .
\end{aligned}$$

Overall, the size of the proof of shuffle protocol is linearly dependent on the number of ciphertexts (i.e. votes in the voting scenario). However, the number of public variables, such as commitment keys, is increasing quadratically. A possible optimization method is to choose a common shared seed and derive all the public polynomials using that seed.

Another possible place for optimization is to choose public variables in a specific format such as $\boldsymbol{B}_0 = [\mathbf{I}_\mu | \boldsymbol{B}_0']$ where $\boldsymbol{B}_0' \in \mathcal{R}_q^{\mu \times (\lambda + 9N + 1)}$ and vectors $\overrightarrow{\boldsymbol{b}}_i = \overrightarrow{\mathbf{0}}_\mu \| \overrightarrow{\boldsymbol{e}}_i \| \overrightarrow{\boldsymbol{b}}_i'$ where $\overrightarrow{\boldsymbol{e}}_i$ is the i-th standard basis vector of length $9N + 1$ and $\overrightarrow{\boldsymbol{b}}_i' \in \mathcal{R}_q^\lambda$ as suggested in [20], so that total number of uniform polynomials will be linear in N. (This optimization is already taken into account in the size of shortness proof transcript, see the full version of the paper [17].)

4 Implementation and benchmarks

We want to instantiate the protocol parameters in a way that the protocol achieves 128 bit classical soundness, and post-quantum encryption security of RLWE is at least that much. For Module SIS security, $8d(\delta_1 - \beta_1 - 1) = 8d\beta_1' < q$ and $8d(\delta_2 - \beta_2 - 1) = 8d\beta_2' < q$. Coefficients of secret key and error terms used in RLWE encryption are sampled uniformly in $\{-1, 0, 1\}$, i.e $\chi_1 = \mathcal{U}(\{-1, 0, 1\}^d)$. Similarly, distribution C and χ_2 are defined on the same set: $Pr(x = 1) = Pr(x = -1)$ and $Pr(x = 0) = 1/2$ in C and $Pr(x = 0) = 6/16$ in χ_2. We find that for $q \approx 2^{32}$, mixing node is secure up to 10 voters which is insufficient. For this reason and in order to easily represent coefficients with primary data types, we choose $q \approx 2^{63}$. Then, using LWE and SIS security estimator script[4] we get that for $\beta_1 = \beta_2 = d = 4096, \lambda = 1, \mu = 1$ and $\delta_1 = \delta_2 = 2^{45}$ ($M \leq 2$ for $N < 10^5$ voters) Hermite factor for $\mathsf{MLWE}_{\lambda,\chi_2}$ with ternary noise is 1.0029 and $\mathsf{MSIS}_{8d\beta'_{1,2}}$ has root Hermite factor 1.003. Finally, by Lemma 3 in [4], $p \approx 2^{-62}$, which implies that $d/l = 2$ is enough for the desired soundness level. However, following the analysis in the full version of the paper [17], we set $d/l = 4$.

We can estimate the performance of proof of shuffle protocol in terms of expensive operations. Sampling challenges uniformly random from $\mathcal{C}$, χ_1 or in interval $[-\delta_1+1, \delta_1]$ is not complex. Thus, the only expensive operation is polynomial multiplication in $\mathcal{R}_q$. When the ring is fully splitting, multiplication can be handled in NTT domain in a linear number of steps. But, due to the large soundness error, we avoid using such rings. In [22], authors show the performance of NTT-based polynomial multiplication in partially splitting rings. We believe that their optimized implementation can further reduce overall protocol performance. In Figure 1, we see that the protocol uses $O(N^2)$ multiplication operations due to $18N$ inner products between vectors of length $\lambda+\mu+9N+1$. However, applying the optimization trick in Section 3.1, this dependency becomes linear in N. Because the complexity of polynomial multiplication depends only on the ring structure, it can be assumed to be constant. Thus, the time complexity of the protocol becomes linear in the number of voters.

As a proof of concept, the proposed scheme is implemented in C language and made publicly available.[5] The polynomial operations are borrowed from Kyber/Dilithium reference implementations and modified afterward for chosen parameters. SHAKE128 is used as a hash function while generating challenges. In Table 1, the average runtime to generate and verify the proof of shuffle protocol is given. Tests are run on Intel Haswell CPUs with 2.2 GHz clock speed and 64GB RAM.

Table 1. Performance table of our implementation of the protocol in Figure 1

.

	Shortness proof generation/verification	Shuffle proof generation/verification	Whole proof generation/verification	Proof size
Per voter	1.5s/1.48s	20ms /13ms	1.52s/1.49s	15 MB

Relying on the numbers shown in Table 1, in case the number of voters is 100000, we can expect the proofs to take about 150000 seconds (approximately 41.7 hours) and the proof size to be about 1.4 TB, which is still manageable. We note that our implementation has not been heavily optimised. In order to go beyond the 100000 order of magnitude, further optimisations are needed.

[4] https://github.com/pq-crystals/security-estimates

[5] https://github.com/Valeh2012/ilmx

In the existing literature, a few other lattice-based e-voting protocols are proposed aiming at practical performance. EVOLVE [25] performs about 10 times faster than our implementation using a highly optimized mathematical library. Correctness, privacy, and consistency of EVOLVE scheme are based on only hardness of MLWE and MSIS problems which is also the case for our protocol. However, EVOLVE is a homomorphic tally-based protocol, limiting its potential usage scenarios. The decryption mix-net-based voting solution by Boyen *et al.* [8] avoids using Non-Interactive Zero-knowledge proofs and bases security claims on trusted public audits. As a result, their proposed system achieves very fast results, but they need to trust the auditors is a significant restriction. To the best of our knowledge, the fastest fully lattice-based proof of correct shuffle is presented in [3] where the authors use the shuffle of known values technique. The problem here is that the shuffle server can break the privacy of voters if the ballot box, decrypted ballots, and shuffle proofs are made public. The proposed verifiable shuffle protocol is 5 times faster (33ms per voter) than EVOLVE scheme benchmarked on an almost two times more powerful CPU. Our protocol, while being slower in the current implementation by about an order of magnitude, does not allow the shuffle server to break vote privacy.

Post-quantum security of Fiat-Shamir transform has not been fully proven in the quantum random oracle model (QROM) yet. Several works in this research area restricted definitions for security properties. For example, computationally binding commitment schemes can be insecure against quantum attacks, as shown in [2]. Collapse-binding is a stronger security property that allows to the construction of a quantum argument of knowledge [29]. The BDLOP commitment scheme used in our protocol has not been shown to satisfy the collapse-binding property. But because SIS hash functions are collapse-binding [19], hopefully one can prove for Module-SIS based BDLOP commitments as well. Another main challenge is to prove the security of mutli-round Fiat-Shamir[15] in QROM. Until these problems are solved, unfortunately, we cannot claim full post-quantum security of non-interactive protocol described in 3.1. An alternative solution is Unruh transform [28], but applying it will result in reduced performance.

However, the interactive protocol in Figure 1 will be *potentially* post-quantum secure. In the online voting context, election auditors can be assumed to be honest verifiers. They can be restricted to have access to the powerful quantum device during the mixing procedure in order to prevent them obtain the secret permutation vector. After the successfully verified mixing phase is over, RLWE ciphertexts can be publicly shared at no risk due to the post-quantum security level of chosen parameters.

5 Conclusions and further work

In this work, we have presented an improved lattice-based proof of shuffle protocol for secure mix-nets. The resulting scheme has linear memory cost and time complexity. As a result, we can potentially handle mixing up to 100000 values.

This is a significant landmark considering our motivating example case of mixing electronic votes.

The performance of the protocol can be improved even further with the help of parallel programming approaches. For example with OpenMP SIMD [18] computations can be distributed to multiple processors, and at each of them, 8 polynomial coefficients can be processed at a time on 512-bit wide registers using AVX512 instruction set. Another approach is to use GPUs as they are much faster than CPUs in matrix calculations [14]. We expect the effect of such optimisations to be approximately one or two orders of magnitude, but establishing the exact amount will remain the subject for future work.

Acknowledgements This paper has been supported by the Estonian Research Council under the grant number PRG920 and European Regional Development Fund through the grant number EU48684.

References

1. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange – a new hope. IACR Cryptol. ePrint Arch. **2015**, 1092 (2015)
2. Ambainis, A., Rosmanis, A., Unruh, D.: Quantum attacks on classical proof systems: The hardness of quantum rewinding. In: 55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014. pp. 474–483. IEEE Computer Society (2014). https://doi.org/10.1109/FOCS.2014.57, https://doi.org/10.1109/FOCS.2014.57
3. Aranha, D.F., Baum, C., Gjøsteen, K., Silde, T., Tunge, T.: Lattice-Based Proof of Shuffle and Applications to Electronic Voting. In: Paterson, K.G. (ed.) Topics in Cryptology - CT-RSA 2021 - Cryptographers' Track at the RSA Conference 2021, Virtual Event, May 17-20, 2021, Proceedings. Lecture Notes in Computer Science, vol. 12704, pp. 227–251. Springer (2021). https://doi.org/10.1007/978-3-030-75539-3_10, https://doi.org/10.1007/978-3-030-75539-3_10
4. Attema, T., Lyubashevsky, V., Seiler, G.: Practical Product Proofs for Lattice Commitments. In: Micciancio, D., Ristenpart, T. (eds.) Proceedings of CRYPTO 2020, Part II. LNCS, vol. 12171, pp. 470–499. Springer (2020)
5. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More Efficient Commitments from Structured Lattice Assumptions. In: Catalano, D., Prisco, R.D. (eds.) Proceedings of SCN 2018. LNCS, vol. 11035, pp. 368–385. Springer (2018)
6. 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.) Proceedings ESORICS 2015 Part I. LNCS, vol. 9326, pp. 305–325. Springer (2015)
7. del Blanco, D.Y.M., Alonso, L.P., Alonso, J.A.H.: Review of Cryptographic Schemes applied to Remote Electronic Voting systems: remaining challenges and the upcoming post-quantum paradigm. Open Mathematics **16**(1), 95–112 (2018)
8. Boyen, X., Haines, T., Müller, J.: A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing. In: Chen, L., Li, N., Liang, K., Schneider, S.A. (eds.) Computer Security - ESORICS 2020 - 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol.

12309, pp. 336–356. Springer (2020). https://doi.org/10.1007/978-3-030-59013-0_17, https://doi.org/10.1007/978-3-030-59013-0_17

9. Cabarcas, D., Göpfert, F., Weiden, P.: Provably secure LWE encryption with smallish uniform noise and secret. In: Emura, K., Hanaoka, G., Zhao, Y. (eds.) Proceedings of ASIAPKC'14. pp. 33–42. ACM (2014)
10. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commun. ACM **24**(2), 84–88 (1981)
11. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: A Homomorphic LWE Based E-voting Scheme. In: Takagi, T. (ed.) Proceedings of PQCrypto 2016. LNCS, vol. 9606, pp. 245–265. Springer (2016)
12. Costa, N., Martínez, R., Morillo, P.: Proof of a Shuffle for Lattice-Based Cryptography. In: Lipmaa, H., Mitrokotsa, A., Matulevicius, R. (eds.) Proceedings of NordSec 2017. LNCS, vol. 10674, pp. 280–296. Springer (2017)
13. Costa, N., Martínez, R., Morillo, P.: Lattice-Based Proof of a Shuffle. In: Bracciali, A., Clark, J., Pintore, F., Rønne, P.B., Sala, M. (eds.) Proceedings of Financial Cryptography and Data Security - FC 2019. LNCS, vol. 11599, pp. 330–346. Springer (2019)
14. Dai, W., Sunar, B.: cuHE: A Homomorphic Encryption Accelerator Library. In: Pasalic, E., Knudsen, L.R. (eds.) Proceedings of BalkanCryptSec 2015. LNCS, vol. 9540, pp. 169–186. Springer (2015)
15. Don, J., Fehr, S., Majenz, C.: The measure-and-reprogram technique 2.0: Multiround fiat-shamir and more. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12172, pp. 602–631. Springer (2020). https://doi.org/10.1007/978-3-030-56877-1_21, https://doi.org/10.1007/978-3-030-56877-1_21
16. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - Dilithium: Digital Signatures from Module Lattices. IACR Cryptol. ePrint Arch. **2017**, 633 (2017)
17. Farzaliyev, V., Willemson, J., Kaasik, J.K.: Improved Lattice-Based Mix-Nets for Electronic Voting. Cryptology ePrint Archive, Report 2021/1499 (2021), https://ia.cr/2021/1499
18. Fortin, P., Fleury, A., Lemaire, F., Monagan, M.: High performance SIMD modular arithmetic for polynomial evaluation (Apr 2020), https://hal.archives-ouvertes.fr/hal-02552673, working paper or preprint
19. Liu, Q., Zhandry, M.: Revisiting post-quantum fiat-shamir. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 326–355. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_12, https://doi.org/10.1007/978-3-030-26951-7_12
20. Lyubashevsky, V., Nguyen, N.K., Seiler, G.: Practical Lattice-Based Zero-Knowledge Proofs for Integer Relations. In: Ligatti, J., Ou, X., Katz, J., Vigna, G. (eds.) Proceedings of ACM CCS 2020 0. pp. 1051–1070. ACM (2020)
21. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors over Rings. J. ACM **60**(6), 43:1–43:35 (2013)
22. Lyubashevsky, V., Seiler, G.: Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In: Nielsen, J.B., Rijmen, V. (eds.) Proceedings of EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 204–224. Springer (2018)

23. Peikert, C., Rosen, A.: Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices. Electron. Colloquium Comput. Complex. (158) (2005)
24. Peng, K., Aditya, R., Boyd, C., Dawson, E., Lee, B.: Multiplicative Homomorphic E-Voting. In: Canteaut, A., Viswanathan, K. (eds.) Proceedings of INDOCRYPT 2004. LNCS, vol. 3348, pp. 61–72. Springer (2004)
25. del Pino, R., Lyubashevsky, V., Neven, G., Seiler, G.: Practical Quantum-Safe Voting from Lattices. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) Proceedings of ACM CCS 2017. pp. 1565–1581. ACM (2017)
26. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Rev. **41**(2), 303–332 (1999)
27. Strand, M.: A Verifiable Shuffle for the GSW Cryptosystem. In: Zohar, A., Eyal, I., Teague, V., Clark, J., Bracciali, A., Pintore, F., Sala, M. (eds.) Financial Cryptography and Data Security 2018, Revised Selected Papers. LNCS, vol. 10958, pp. 165–180. Springer (2018)
28. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9057, pp. 755–784. Springer (2015). https://doi.org/10.1007/978-3-662-46803-6_25, https://doi.org/10.1007/978-3-662-46803-6_25
29. Unruh, D.: Computationally binding quantum commitments. In: Fischlin, M., Coron, J. (eds.) Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9666, pp. 497–527. Springer (2016). https://doi.org/10.1007/978-3-662-49896-5_18, https://doi.org/10.1007/978-3-662-49896-5_18