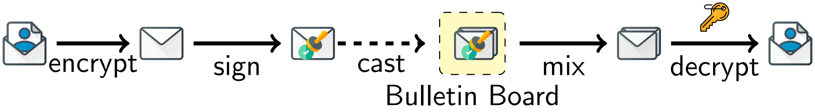
Shorter Lattice-based Zero-Knowledge Proofs for the Correctness of a Shuffle

Javier Herranz **Ramiro Martínez** Manuel Sánchez

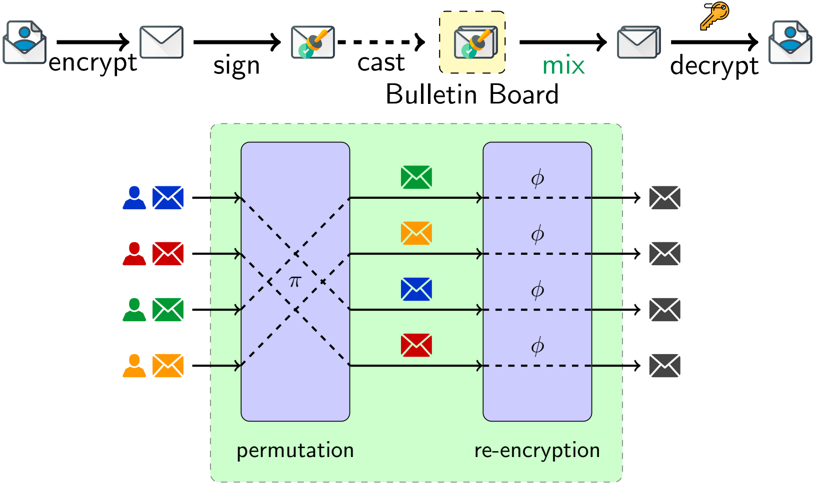
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

e-Voting


encrypt
sign
cast
mix
decrypt
Bulletin Board

π
ϕ
ϕ
ϕ
ϕ
permutation
re-encryption

e-Voting


encrypt
sign
cast
Bulletin Board
mix
decrypt
π
ϕ
ϕ
ϕ
ϕ
permutation
re-encryption

Zero-Knowledge Proofs of Knowledge

Definition

A *Zero-Knowledge Proof* has the following properties:

- **Completeness**: if an honest $\mathcal{P}$ knows a valid witness and both follow the protocol then in the last step $\mathcal{V}$ accepts.
- **Soundness**: a malicious prover can not convince a verifier of a false statement.
- **Zero-Knowledge**: the conversation does not leak any relevant information besides what it is intended to prove.

Zero-Knowledge Proofs of Knowledge

Definition

A *Zero-Knowledge Proof* has the following properties:

- **Completeness**: if an honest $\mathcal{P}$ knows a valid witness and both follow the protocol then in the last step $\mathcal{V}$ accepts.
- **Soundness**: a malicious prover can not convince a verifier of a false statement.
- **Zero-Knowledge**: the conversation does not leak any relevant information besides what it is intended to prove.

Zero-Knowledge Proofs of Knowledge

Definition

A *Zero-Knowledge Proof* has the following properties:

- **Completeness**: if an honest $\mathcal{P}$ knows a valid witness and both follow the protocol then in the last step $\mathcal{V}$ accepts.
- **Soundness**: a malicious prover can not convince a verifier of a false statement.
- **Zero-Knowledge**: the conversation does not leak any relevant information besides what it is intended to prove.

Zero-Knowledge Proofs of Knowledge

Definition

A *Zero-Knowledge Proof* has the following properties:

- **Completeness**: if an honest $\mathcal{P}$ knows a valid witness and both follow the protocol then in the last step $\mathcal{V}$ accepts.
- **Soundness**: a malicious prover can not convince a verifier of a false statement.
- **Zero-Knowledge**: the conversation does not leak any relevant information besides what it is intended to prove.

Ring-Learning With Errors

Let $s(x)$ be a secret polynomial in $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ and χ a probability distribution over $\mathcal{R}_q$. Choose $a_i \leftarrow_R \mathcal{R}_q$ and $e_i \leftarrow_R \chi$ and compute

$$a_i \cdot s + e_i.$$

Definition (Decisional-RLWE)

Distinguish samples $\{(a_i, a_i \cdot s + e_i) \mid a_i \leftarrow_R \mathcal{R}_q,\ e_i \leftarrow_R \chi\}$ from uniformly random $\{(a_i, b_i) \mid a_i, b_i \leftarrow_R \mathcal{R}_q\}$.

Definition (Search-RLWE)

Find s given polynomially many RLWE samples $\{(a_i, a_i \cdot s + e_i)\}$.

Ring-Learning With Errors

Let $s(x)$ be a secret polynomial in $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ and χ a probability distribution over $\mathcal{R}_q$. Choose $a_i \leftarrow_R \mathcal{R}_q$ and $e_i \leftarrow_R \chi$ and compute

$$a_i \cdot s + e_i.$$

Definition (Decisional-RLWE)

Distinguish samples $\{(a_i, a_i \cdot s + e_i) \mid a_i \leftarrow_R \mathcal{R}_q,\ e_i \leftarrow_R \chi\}$ from uniformly random $\{(a_i, b_i) \mid a_i, b_i \leftarrow_R \mathcal{R}_q\}$.

Definition (Search-RLWE)

Find s given polynomially many RLWE samples $\{(a_i, a_i \cdot s + e_i)\}$.

Ring-Learning With Errors

Let $s(x)$ be a secret polynomial in $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ and χ a probability distribution over $\mathcal{R}_q$. Choose $a_i \leftarrow_R \mathcal{R}_q$ and $e_i \leftarrow_R \chi$ and compute

$$a_i \cdot s + e_i.$$

Definition (Decisional-RLWE)

Distinguish samples $\{(a_i, a_i \cdot s + e_i) \mid a_i \leftarrow_R \mathcal{R}_q,\ e_i \leftarrow_R \chi\}$ from uniformly random $\{(a_i, b_i) \mid a_i, b_i \leftarrow_R \mathcal{R}_q\}$.

Definition (Search-RLWE)

Find s given polynomially many RLWE samples $\{(a_i, a_i \cdot s + e_i)\}$.

LPR encryption scheme

- **Key Generation**: given $a \leftarrow_R \mathcal{R}_q$ and $s, e \leftarrow_R \chi$, output the **secret key** s and the **public key** $(a, b = a \cdot s + e)$.
- **Encryption**: given an n-bit message $z \in \{0, 1\}^n$, choose $r, e_u, e_v \leftarrow_R \chi$. Output:

$$(u, v) = (a \cdot r + e_u, b \cdot r + e_v + \left\lfloor \frac{q}{2} \right\rceil z) \in \mathcal{R}_q \times \mathcal{R}_q$$

- **Decryption**:

$$v - u \cdot s = (r \cdot e - s \cdot e_u + e_v) + \left\lfloor \frac{q}{2} \right\rceil \cdot z$$

LPR encryption scheme

- **Key Generation**: given $a \leftarrow_R \mathcal{R}_q$ and $s, e \leftarrow_R \chi$, output the **secret key** s and the **public key** $(a, b = a \cdot s + e)$.
- **Encryption**: given an n-bit message $z \in \{0,1\}^n$, choose $r, e_u, e_v \leftarrow_R \chi$. Output:

$$(u, v) = (a \cdot r + e_u, b \cdot r + e_v + \left\lfloor \frac{q}{2} \right\rceil z) \in \mathcal{R}_q \times \mathcal{R}_q$$

- **Decryption**:

$$v - u \cdot s = (r \cdot e - s \cdot e_u + e_v) + \left\lfloor \frac{q}{2} \right\rceil \cdot z$$

LPR encryption scheme

- **Key Generation**: given $a \leftarrow_R \mathcal{R}_q$ and $s, e \leftarrow_R \chi$, output the **secret key** s and the **public key** $(a, b = a \cdot s + e)$.
- **Encryption**: given an n-bit message $z \in \{0,1\}^n$, choose $r, e_u, e_v \leftarrow_R \chi$. Output:

$$(u, v) = (a \cdot r + e_u, b \cdot r + e_v + \left\lfloor \frac{q}{2} \right\rceil z) \in \mathcal{R}_q \times \mathcal{R}_q$$

- **Decryption**:

$$v - u \cdot s = (r \cdot e - s \cdot e_u + e_v) + \left\lfloor \frac{q}{2} \right\rceil \cdot z$$

Towards efficient ZKPoK for a lattice shuffle

Existing techniques

- Existing proposals require linear space [CMM17; Str19; CMM19].
- Efficient arguments of knowledge exist for circuit satisfiability with sublinear size [Bau+18].

▶ Re-encryption as a circuit

Re-encryption can be done adding an encryption of 0, that is, it only requires multiplications and additions in $\mathcal{R}_q$:

$$(u', v') = (u, v) + \mathrm{Enc}(pk, 0, r', e'_u, e'_v)$$

Small elements

- The main issue is to prove that something is small.
- We prove $(r'_i + B) \dots (r'_i + 1) r'_i (r'_i - 1) \dots (r'_i - B) = 0$.
- Analogously for $e'_{u,i}$ and $e'_{v,i}$.

Re-encryption as a circuit

Re-encryption can be done adding an encryption of 0, that is, it only requires multiplications and additions in $\mathcal{R}_q$:

$$(u', v') = (u, v) + \mathsf{Enc}(pk, 0, r', e'_u, e'_v)$$

Small elements

- The main issue is to prove that something is small.
- We prove $(r'_i + B) \dots (r'_i + 1) r'_i (r'_i - 1) \dots (r'_i - B) = 0$.
- Analogously for $e'_{u,i}$ and $e'_{v,i}$.

▶ Permutation as a circuit

Figure: Switch off ($b = 0$)

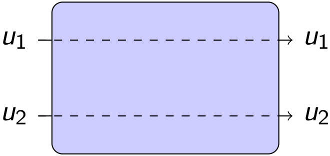
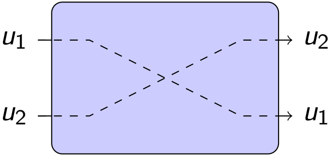
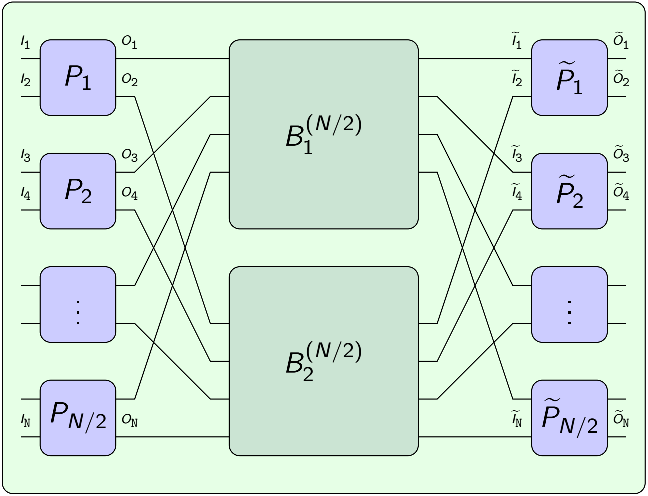


Figure: Switch on ($b = 1$)



$$\overline{u}_1 = (1 - b) \cdot u_1 + b \cdot u_2$$
$$\overline{u}_2 = (1 - b) \cdot u_2 + b \cdot u_1$$

Figure: Beneš Network $B^{(N)}$



Shorter Lattice-based Zero-Knowledge Proofs for the Correctness of a Shuffle

- Circuit size of $M \in \mathcal{O}\left(N \cdot \left(n\hat{k}\sigma + n^{\log_2 3} + n\log(N)\right) \right)$ gates.
- Communication complexity: proof of size $\mathcal{O}(\sqrt{M\log^3(M)}\log(Q))$.

Attention

Before the rounding step of the decryption

$$v - u \cdot s = (\sum r \cdot e - s \cdot \sum e_u + \sum e_v) + \left\lfloor \frac{q}{2} \right\rceil \cdot z$$

the result depends on the secret key s and the error terms $\sum e_u$ and $\sum e_v$.
This has to be considered to avoid any leakage of information.

Shorter Lattice-based Zero-Knowledge Proofs for the Correctness of a Shuffle

Javier Herranz **Ramiro Martínez** Manuel Sánchez

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Bibliography I

[Bau+18] Carsten Baum et al. "Sub-linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits". In: *CRYPTO 2018, Part II*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10992. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, Aug. 2018, pp. 669–699. DOI: 10.1007/978-3-319-96881-0_23.

[CMM17] Nuria Costa, Ramiro Martínez, and Paz Morillo. "Proof of a Shuffle for Lattice-Based Cryptography". In: *Secure IT Systems*. Ed. by Helger Lipmaa, Aikaterini Mitrokotsa, and Raimundas Matulevičius. Cham: Springer International Publishing, 2017, pp. 280–296. ISBN: 978-3-319-70290-2.

Bibliography II

[CMM19] Núria Costa, Ramiro Martínez, and Paz Morillo. "Lattice-Based Proof of a Shuffle". In: *FC 2019 Workshops*. Ed. by Andrea Bracciali et al. Vol. 11599. LNCS. Frigate Bay, St. Kitts and Nevis: Springer, Heidelberg, Germany, Feb. 2019, pp. 330–346. DOI: 10.1007/978-3-030-43725-1_23.

[Str19] Martin Strand. "A Verifiable Shuffle for the GSW Cryptosystem". In: *FC 2018 Workshops*. Ed. by Aviv Zohar et al. Vol. 10958. LNCS. Nieuwpoort, Curaçao: Springer, Heidelberg, Germany, Mar. 2019, pp. 165–180. DOI: 10.1007/978-3-662-58820-8_12.