Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE

Duhyeong Kim
Intel Labs

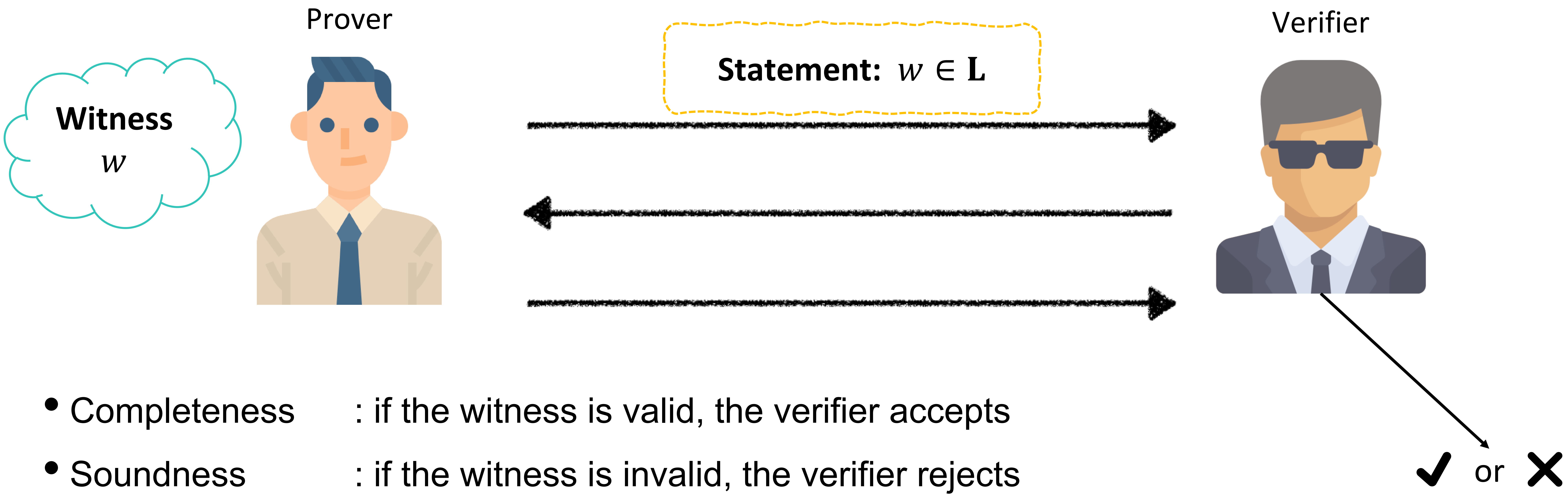
Dongwon Lee, Jinyeong Seo, Yongsoo Song
Seoul National University

CRYPTO 2023
Aug 23, 2023

Background

Background

Proof of Knowledge (PoK)



- Completeness : if the witness is valid, the verifier accepts
- Soundness : if the witness is invalid, the verifier rejects
- **Zero-knowledge** : the verifier **does not learn anything** about the witness
  - There exists a simulator that simulates the transcript

Background

Lattice-based PoK for linear relation

- High-Level Description
  - Public: $\mathbf{B} \in R_q^{k\times\ell}$, $\mathbf{c} \in R_q^k$ for $k < \ell$ (R: polynomial ring)
  - We want to prove the knowledge of $\mathbf{r} \in R^\ell$ and $\mathbf{m} \in \mathcal{M}(\subset R_q^k)$ s.t.

$$\boxed{\mathbf{c} = \mathbf{B}\mathbf{r} + \mathbf{m} \pmod{q} \quad \text{and} \quad \|\mathbf{r}\|_2 \leq \beta.}$$

Background

Lattice-based PoK for linear relation

- BFV encryption
  - Parameters : Ciphertext modulus q, plaintext modulus $t \mid q$, error distribution χ.
  - Public key : $\mathbf{p} = (p_0, p_1)^T \in R_q^2$
  - Ciphertext : For a message $m \in R_t$, the encryption algorithm samples $\mathbf{r} = (r_0, r_1, r_2) \leftarrow \chi^3$ and return

$$\mathbf{c} = r_2 \cdot \mathbf{p} + \left(r_0 + (q/t) \cdot m,\ r_1\right)^T \pmod{q}$$

  - The BFV ciphertext can also be expressed as

$$\mathbf{c} = \mathbf{Br} + \mathbf{m} \pmod{q}$$

  where $\mathbf{B} = [\,\mathbf{I_2} \mid \mathbf{p}\,] \in R_q^{2\times 3}$ and $\mathbf{m} = \left((q/t) \cdot m,\ 0\right)^T$.

- **Proof of Plaintext Knowledge (PPK)** for BFV encryption:

  To prove the knowledge of the **message $\mathbf{m}$** and the **encryption randomness $\mathbf{r}$** for given ciphertext $\mathbf{c}$

[Bra12] Zvika Brakerski. “Fully homomorphic encryption without modulus switching from classical GapSVP”, *CRYPTO 2012.*
[FV12] Junfeng Fan and Frederik Vercauteren. “Somewhat practical fully homomorphic encryption”, *ePrint 2012/144*.

Background

Lattice-based PoK for linear relation

- BDLOP commitment
  - Parameters : Modulus q, error distribution χ.
  - Commitment key : $\mathbf{B} = \mathbf{R} \cdot [\, \mathbf{I}_k \mid \mathbf{A} \,] \in R_q^{k \times \ell}$ for $\mathbf{A} \in R_q^{k \times (k-\ell)}$ and invertible $\mathbf{R} \in R_q^{k \times k}$
  - Commitment : For a message $m \in R_q$, the commitment algorithm samples $\mathbf{r} \leftarrow \chi^{\ell}$ and return

$$\mathbf{c} = \mathbf{Br} + \mathbf{m} \pmod q$$

  where $\mathbf{m} = \begin{bmatrix} \mathbf{0} \\ m \end{bmatrix}$.

- **Proof of Opening Knowledge (POK)** for BDLOP commitment:

  To prove the knowledge of the **message $\mathbf{m}$** and the **commitment randomness $\mathbf{r}$** for given commitment $\mathbf{c}$

[BDLOP18] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. "More efficient commitments from structured lattice assumptions“, *SCN 2018*.

Motivation

Motivation

Zero-Knowledge “Overkill”

- Conventional goal of Zero-knowledge:

Zero-knowledge w.r.t. **both** message $\mathbf{m}$ and randomness $\mathbf{r}$

- **BUT!** Zero-knowledge of **randomness can be an overkill** for many of PoK applications

- Then, the natural question would be:
  - How about **refining the goal** of zero-knowledge as following?

    Zero-knowledge w.r.t. **only** message $\mathbf{m}$

  - Can we still achieve **zero-knowledge of $\mathbf{m}$** while **allowing the leakage of $\mathbf{r}$** information?

Motivation

Previous Approaches

- Σ-protocol Framework:

$$\mathbf{c} = \mathbf{B}\mathbf{r} + \mathbf{m} \pmod{q}$$

$\mathbf{m}, \mathbf{r}$

Prover

1) Commitment: $\mathbf{d}_i = \mathbf{B}\mathbf{y}_\mathbf{i} + \mathbf{u}_\mathbf{i} \pmod{q}$ for $1 \le i \le \ell$

2) Challenge: $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$

3) Response: $(\mathbf{v}_\mathbf{i}, \mathbf{z}_i) = (\mathbf{u}_\mathbf{i}, \mathbf{y}_i) + \gamma_i \cdot (\mathbf{m}, \mathbf{r})$ for $1 \le i \le \ell$

Verifier

Generate random elements:
$\mathbf{u}_i \leftarrow \mathcal{M}, \mathbf{y}_i \leftarrow D_{rnd}$
for $1 \le i \le \ell$

Generate random challenges:
$\gamma_i \leftarrow \mathcal{C}$ for $1 \le i \le \ell$

4) Verification:

$$\mathbf{B}\mathbf{z}_\mathbf{i} + \mathbf{v}_\mathbf{i} \stackrel{?}{=} \mathbf{d}_i + \gamma_i \cdot \mathbf{c},$$
$$\| \mathbf{z}_i \| \stackrel{?}{<} B,$$
for $1 \le i \le \ell$

Motivation

Previous Approaches: Noise Flooding

- For the zero-knowledge proof, previous work adopted statistical methods.

$$\mathbf{c} = \mathbf{Br} + \mathbf{m} \pmod{q}$$

Prover

$\mathbf{m}, \mathbf{r}$

Verifier

1) Commitment: $\mathbf{d}_i = \mathbf{B}\mathbf{y}_\mathbf{i} + \mathbf{u}_\mathbf{i} \pmod{q}$ for $1 \le i \le \ell$ →

2) Challenge: $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$ ←

3) Response: $(\mathbf{v}_\mathbf{i}, \mathbf{z}_i) = \boxed{(\mathbf{u}_\mathbf{i}, \mathbf{y}_i) + \gamma_i \cdot (\mathbf{m}, \mathbf{r})}$ for $1 \le i \le \ell$ →

Generate random elements:
$\mathbf{u}_i \leftarrow \mathcal{M}, \mathbf{y}_i \leftarrow D_{rnd}$
for $1 \le i \le \ell$

Noise Flooding
Set $\|(\mathbf{u}_i, \mathbf{y}_i)\| \gg \|\gamma_i \cdot (\mathbf{m}, \mathbf{r})\|$
to make $(\mathbf{v}_i, \mathbf{z}_i)$ **statistically independent** to $(\mathbf{m}, \mathbf{r})$

Generate random challenges:
$\gamma_i \leftarrow \mathcal{C}$ for $1 \le i \le \ell$

4) Verification:
$\mathbf{B}\mathbf{z}_\mathbf{i} + \mathbf{v}_\mathbf{i} \stackrel{?}{=} \mathbf{d}_i + \gamma_i \cdot \mathbf{c}$,
$\| \mathbf{z}_i \| \stackrel{?}{<} B$,
for $1 \le i \le \ell$

Motivation

Previous Approaches: Noise Flooding

- For the zero-knowledge proof, previous work adopted statistical methods.

$$\mathbf{c} = \mathbf{B}\mathbf{r} + \mathbf{m} \pmod{q}$$

Prover

$\mathbf{m}, \mathbf{r}$

Verifier

1) Commitment: $\mathbf{d}_i = \mathbf{B}\mathbf{y}_\mathbf{i} + \mathbf{u}_\mathbf{i} \pmod{q}$ for $1 \leq i \leq \ell$ →

2) Challenge: $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$ ←

3) Response: $(\mathbf{v}_\mathbf{i}, \mathbf{z}_i) = \boxed{(\mathbf{u}_\mathbf{i}, \mathbf{y}_i) + \gamma_i \cdot (\mathbf{m}, \mathbf{r})}$ for $1 \leq i \leq \ell$ →

Generate random elements:
$\mathbf{u}_i \leftarrow \mathcal{M}, \mathbf{y}_i \leftarrow D_{rnd}$
for $1 \leq i \leq \ell$

Noise Flooding
Set $\|(\mathbf{u}_i, \mathbf{y}_i)\| \gg \|\gamma_i \cdot (\mathbf{m}, \mathbf{r})\|$
to make $(\mathbf{v}_i, \mathbf{z}_i)$ **statistically independent** to $(\mathbf{m}, \mathbf{r})$

Generate random challenges:
$\gamma_i \leftarrow \mathcal{C}$ for $1 \leq i \leq \ell$

4) Verification:
$\mathbf{B}\mathbf{z}_\mathbf{i} + \mathbf{v}_\mathbf{i} \stackrel{?}{=} \mathbf{d}_i + \gamma_i \cdot \mathbf{c}$,
$\| \mathbf{z}_i \| \stackrel{?}{<} B$,
for $1 \leq i \leq \ell$

✓ Distribution-independent Solution
✓ Exponential Overhead

Motivation

Previous Approaches: Rejection Sampling

- For the zero-knowledge proof, previous work adopted statistical methods.

$$\mathbf{c} = \mathbf{Br} + \mathbf{m} \pmod{q}$$

$\mathbf{m}, \mathbf{r}$

Prover

Generate random elements:
$\mathbf{u}_i \leftarrow \mathcal{M}, \mathbf{y}_i \leftarrow D_{rnd}$
for $1 \le i \le \ell$

1) Commitment: $\mathbf{d}_i = \mathbf{B}\mathbf{y}_\mathbf{i} + \mathbf{u}_\mathbf{i} \pmod{q}$ for $1 \le i \le \ell$

2) Challenge: $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$

3) Response: $(\mathbf{v}_\mathbf{i}, \mathbf{z}_i) = (\mathbf{u}_\mathbf{i}, \mathbf{y}_i) + \gamma_i \cdot (\mathbf{m}, \mathbf{r})$ for $1 \le i \le \ell$

Rejection Sampling
Reject and re-run the steps with certain probability
to make $(\mathbf{v}_i, \mathbf{z}_i)$ **statistically independent** to $(\mathbf{m}, \mathbf{r})$

Verifier

Generate random challenges:
$\gamma_i \leftarrow \mathcal{C}$ for $1 \le i \le \ell$

4) Verification:
$\mathbf{B}\mathbf{z}_\mathbf{i} + \mathbf{v}_\mathbf{i} \stackrel{?}{=} \mathbf{d}_i + \gamma_i \cdot \mathbf{c}$,
$\| \mathbf{z}_i \| \stackrel{?}{<} B$,
for $1 \le i \le \ell$

Motivation

Previous Approaches: Rejection Sampling

- For the zero-knowledge proof, previous work adopted statistical methods.

$\mathbf{c} = \mathbf{B}\mathbf{r} + \mathbf{m} \pmod{q}$

Prover

$\mathbf{m}, \mathbf{r}$

Verifier

1) Commitment: $\mathbf{d}_i = \mathbf{B}\mathbf{y_i} + \mathbf{u_i} \pmod{q}$ for $1 \le i \le \ell$

2) Challenge: $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$

3) Response: $(\mathbf{v_i}, \mathbf{z}_i) = (\mathbf{u_i}, \mathbf{y}_i) + \gamma_i \cdot (\mathbf{m}, \mathbf{r})$ for $1 \le i \le \ell$

Generate random elements:
$\mathbf{u}_i \leftarrow \mathcal{M}, \mathbf{y}_i \leftarrow D_{rnd}$
for $1 \le i \le \ell$

Rejection Sampling
Reject and re-run the steps with certain probability
to mak $\mathbf{z}_i)$ **statistically independent** to $(\mathbf{m}, \mathbf{r})$

Generate random challenges:
$\gamma_i \leftarrow \mathcal{C}$ for $1 \le i \le \ell$

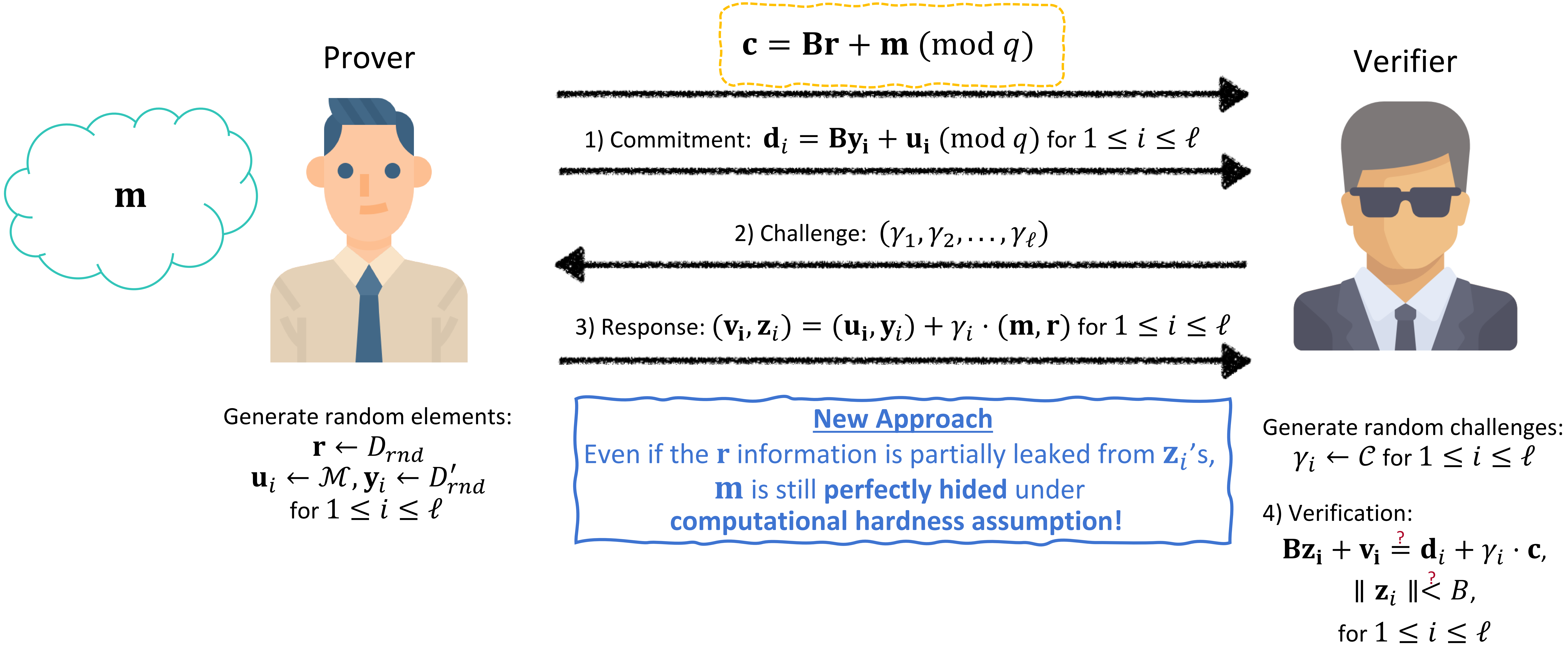
4) Verification:
$\mathbf{B}\mathbf{z_i} + \mathbf{v_i} \stackrel{?}{=} \mathbf{d}_i + \gamma_i \cdot \mathbf{c}$,
$\| \mathbf{z}_i \| \stackrel{?}{<} B$,
for $1 \le i \le \ell$

- ✓ Polynomial/Constant Overhead
- ✓ Multiple iterations (exponential in multi-prover case)
- ✓ Side-channel attack vulnerability

Motivation

New Framework

- **"Refined"** zero-knowledge proof based on **computational hardness assumption!**



Our Work

Our Work

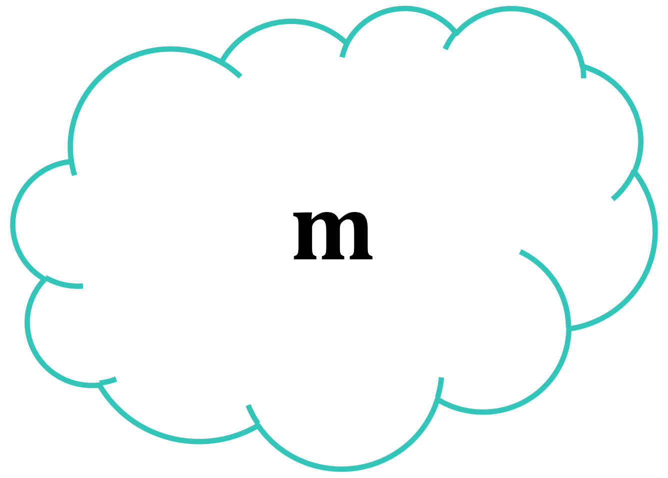
A New Framework on Lattice-based PoK with "refined" Zero-Knowledge

- We **first** propose secure lattice-based PoK protocols **w/o noise flooding or rejection sampling**
  - Zero-knowledge w.r.t. message holds under the **"Hint-MLWE"** assumption**.**
  - *v.s.* noise flooding : exponential → **polynomial/constant** overhead
  - *v.s.* rejection sampling : $\boldsymbol{O}(\sqrt{\boldsymbol{dim}})$ **smaller** soundness slack, no repetition required
- Instantiation on the following primitives:
  - Proof of Plaintext Knowledge (PPK) for BFV encryption
  - Proof of Opening Knowledge (POK) for BDLOP commitment
    - Naturally extendable to various BDLOP-based ZKP applications
- **Tight Reduction** from **MLWE to Hint-MLWE** under discrete Gaussian setting
    - LWE→Hint-LWE & RLWE→Hint-RLWE also hold

Proof Sketch

Zero-Knowledge w.r.t. Message

- Need to show the transcript $(\mathbf{c}, (\mathbf{d}_i, \gamma_i, \mathbf{v}_i, \mathbf{z}_i)_{\mathrm{i}})$ is **simulatable** without the message $\mathbf{m}$



Prover

$\boxed{\mathbf{c} = \mathbf{Br} + \mathbf{m} \pmod{q}}$

1) Commitment: $\boxed{\mathbf{d}_i = \mathbf{B}\mathbf{y}_{\mathrm{i}} + \mathbf{u}_{\mathrm{i}} \pmod{q}}$ for $1 \le i \le \ell$

2) Challenge: $\boxed{(\gamma_1, \gamma_2, \ldots, \gamma_\ell)}$

3) Response: $\boxed{(\mathbf{v}_{\mathrm{i}}, \mathbf{z}_i) = (\mathbf{u}_{\mathrm{i}}, \mathbf{y}_i) + \gamma_i \cdot (\mathbf{m}, \mathbf{r})}$ for $1 \le i \le \ell$

Verifier

Generate random elements:
$\mathbf{r} \leftarrow D_{rnd}$
$\mathbf{u}_i \leftarrow \mathcal{M}, \mathbf{y}_i \leftarrow D'_{rnd}$
for $1 \le i \le \ell$

Our Approach
Even if the $\mathbf{r}$ information is partially leaked from $\mathbf{z}_i$'s, $\mathbf{m}$ is still **perfectly hided** under **computational hardness assumption!**

Generate random challenges:
$\gamma_i \leftarrow \mathcal{C}$ for $1 \le i \le \ell$

4) Verification:
$\mathbf{B}\mathbf{z}_{\mathrm{i}} + \mathbf{v}_{\mathrm{i}} \stackrel{?}{=} \mathbf{d}_i + \gamma_i \cdot \mathbf{c},$
$\| \mathbf{z}_i \| \stackrel{?}{<} B,$
for $1 \le i \le \ell$

Proof Sketch

Zero-Knowledge w.r.t. Message

- **Observation 1:** Trivially-simulatable components of the transcript $(\mathbf{c}, (\mathbf{d}_i, \gamma_i, \mathbf{v}_i, \mathbf{z}_i)_\mathrm{i})$:
  1. $\mathbf{d}_i$ can be generated by the other components and the public key $\mathbf{B}$
     - $\mathbf{d}_i = \mathbf{B}\mathbf{y}_i + \mathbf{u}_i = \mathbf{B}(\mathbf{z}_i - \gamma_i \cdot \mathbf{r}) + (\mathbf{v}_i - \gamma_i \cdot \mathbf{m}) = \mathbf{B}\mathbf{z}_i + \mathbf{v}_i - \gamma_i \cdot \mathbf{c}$
  2. $\mathbf{v}_i$ is also trivially simulatable for each case as following:
     - PPK of BFV encryption : $\mathbf{v}_i = \mathbf{u}_i + \gamma_i \cdot \mathbf{m} \pmod{t}$ is uniform modulo t
     - POK of BDLOP commitment : $\mathbf{u}_i = \mathbf{0}$ & Do not send $\mathbf{v}_i$ to the verifier

- Now, it **suffices to simulate** $(\mathbf{c}, (\mathbf{z}_i)_i)$ for public key $\mathbf{B}$ and challenges $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$

Proof Sketch

Zero-Knowledge w.r.t. Message

- **Observation 2**: The tuple $(\mathbf{B}, \mathbf{c}, \mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_\ell)$ can be expressed as

$$(\mathbf{B}, \mathbf{Br} + \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \ldots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

- Since $\mathbf{B} = \mathbf{R} \cdot [\mathbf{I} \mid \mathbf{A}]$ for a public invertible matrix $\mathbf{R}$**,** it is equivalent to simulate

$$(\mathbf{A}, [\mathbf{I} \mid \mathbf{A}]\mathbf{r} + \mathbf{R}^{-1} \cdot \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \ldots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

Proof Sketch

Zero-Knowledge w.r.t. Message

- **Observation 2**: The tuple $(\mathbf{B}, \mathbf{c}, \mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_\ell)$ can be expressed as

$$(\mathbf{B}, \mathbf{Br} + \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

- Since $\mathbf{B} = \mathbf{R} \cdot [\mathbf{I} \mid \mathbf{A}]$ for a public invertible matrix $\mathbf{R}$**,** it is equivalent to simulate

$$(\boxed{\mathbf{A}, [\mathbf{I} \mid \mathbf{A}]\mathbf{r}} + \mathbf{R}^{-1} \cdot \mathbf{m}, \boxed{\gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell})$$

MLWE Instance over the secret $\mathbf{r}$

Hints on the secret $\mathbf{r}$

Proof Sketch

Zero-Knowledge w.r.t. Message

- **Observation 2**: The tuple $(\mathbf{B}, \mathbf{c}, \mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_\ell)$ can be expressed as

$$(\mathbf{B}, \mathbf{Br} + \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

- Since $\mathbf{B} = \mathbf{R} \cdot [\mathbf{I} \mid \mathbf{A}]$ for a public invertible matrix $\mathbf{R}$, it is equivalent to simulate

$$(\mathbf{A}, [\mathbf{I} \mid \mathbf{A}]\mathbf{r} + \mathbf{R}^{-1} \cdot \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

$$\overset{?}{\approx}$$

$$(\mathbf{A}, \quad uniform \quad , \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

Proof Sketch

Zero-Knowledge w.r.t. Message

- **Observation 2**: The tuple $(\mathbf{B}, \mathbf{c}, \mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_\ell)$ can be expressed as

$$(\mathbf{B}, \mathbf{Br} + \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

- Since $\mathbf{B} = \mathbf{R} \cdot [\mathbf{I} \mid \mathbf{A}]$ for a public invertible matrix $\mathbf{R}$, it is equivalent to simulate

$$(\mathbf{A}, [\mathbf{I} \mid \mathbf{A}]\mathbf{r} + \mathbf{R}^{-1} \cdot \mathbf{m}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

$$? \wr$$

$$\underline{(\mathbf{A}, \quad uniform \quad , \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)}$$

Simulatable!

Hint-MLWE

Definition

- $\mathbf{MLWE}_{R,d,m,q,\sigma}$ **Assumption:**

$$(\mathbf{A}, [\mathbf{I}\ |\mathbf{A}]\mathbf{r})$$

$$\wr_{c}$$

$$(\mathbf{A}, \quad \mathbf{b} \quad)$$

for $\mathbf{A} \xleftarrow{\$} R_q^{m\times d}, \mathbf{b} \xleftarrow{\$} R_q^{m}, \mathbf{r} \xleftarrow{\$} D_\sigma^{m+d}$ (discrete Gaussian)

[LS15] Adeline Langlois, and Damien Stehlé. "Worst-case to average-case reductions for module lattices." *Designs, Codes and Cryptography*, 2015.

Hint-MLWE

Definition

- $\textbf{Hint-MLWE}_{R,d,m,q,\sigma_1}^{\ell,\sigma_2,\mathcal{C}}$ **Assumption:**

$$(\mathbf{A}, [\mathbf{I}\ |\mathbf{A}]\mathbf{r}, \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

$$\approx_c$$

$$(\mathbf{A}, \quad \mathbf{b} \quad , \gamma_1 \cdot \mathbf{r} + \mathbf{y}_1, \gamma_2 \cdot \mathbf{r} + \mathbf{y}_2, \dots, \gamma_\ell \cdot \mathbf{r} + \mathbf{y}_\ell)$$

for $\mathbf{A} \xleftarrow{\$} R_q^{m\times d}, \mathbf{b} \xleftarrow{\$} R_q^m, \mathbf{r} \xleftarrow{\$} D_{\sigma_1}^{m+d}, \mathbf{y}_i \xleftarrow{\$} D_{\sigma_2}^{m+d}$ (discrete Gaussian), and $\gamma_i \leftarrow \mathcal{C}$

- Generalized notion of Hint-LWE [CKK+18] and Multi-Hint Extended RLWE [BKMS22]

[CKK+18] Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, Joohee Lee, Junbum Shin, and Yongsoo Song. "Lattice-based secure biometric authentication for hamming distance." *ACISP 2021.*

[BKMS22] Jose Maria Bermudo Mera, Angshuman Karmakar, Tilen Marc, and Azam Soleimanian. "Efficient lattice-based inner-product functional encryption." *PKC 2022.*

Hint-MLWE

Computational Hardness

Theorem: Let $\sigma, \sigma_1, \sigma_2 > 0$ be reals such that $\frac{1}{\sigma^2} = 2\left(\frac{1}{\sigma_1^2} + \frac{B}{\sigma_2^2}\right)$ where $B \coloneqq \ell \cdot \max_{\gamma \leftarrow \mathcal{C}} \|\gamma\|_1^2$. If $\sigma \geq \eta_\epsilon(\mathbb{Z}^n)$, there exists poly-time reduction from $\mathbf{MLWE}_{\boldsymbol{R,d,m,q,\sigma}}$ to $\textbf{Hint-MLWE}^{\boldsymbol{\ell,\sigma_2,\mathcal{C}}}_{\boldsymbol{R,d,m,q,\sigma_1}}$ with advantage loss $\leq (d+m) \cdot 2\epsilon$.

Implication

- Hint-MLWE w/ **width** $\boldsymbol{\sigma_1 = 2\sigma, \sigma_2 = 2\sqrt{B}\sigma}$ is harder than MLWE w/ **width** $\boldsymbol{\sigma}$
  - 1-bit larger size of secret $\mathbf{r}$ $(\sigma_1$ v.s. $\sigma)$
  - $\|\mathbf{y}_i\|_2 = O\left(\sqrt{\ell} \cdot \|\gamma_i \cdot \mathbf{r}\|_2\right)$ $(\sigma_2$ v.s. $\sigma_1)$

Hint-MLWE

Computational Hardness

Theorem: Let $\sigma, \sigma_1, \sigma_2 > 0$ be reals such that $\frac{1}{\sigma^2} = 2\left(\frac{1}{\sigma_1^2} + \frac{B}{\sigma_2^2}\right)$ where $B \coloneqq \ell \cdot \max_{\gamma \leftarrow \mathcal{C}} \|\gamma\|_1^2$.
If $\sigma \geq \eta_\epsilon(\mathbb{Z}^n)$, there exists poly-time reduction from $\mathbf{MLWE}_{\boldsymbol{R,d,m,q,\sigma}}$ to $\textbf{Hint-MLWE}^{\boldsymbol{\ell,\sigma_2,\mathcal{C}}}_{\boldsymbol{R,d,m,q,\sigma_1}}$
with advantage loss $\leq (d+m) \cdot 2\epsilon$.

How to Prove?

- Reverse the point of view ☺
- Analyze the **"conditional distribution"** of $\mathbf{r}$ for given hints $(\gamma_i \cdot \mathbf{r} + \mathbf{y}_i)_i$
- Then, $[\mathbf{I} \mid \mathbf{A}]\mathbf{r}$ can be simulated "from" $\mathbf{A}$, $(\gamma_i \cdot \mathbf{r} + \mathbf{y}_i)_i$, and given MLWE instance

Results

Comparison v.s. Previous Methods

Method	**Type**	**Zero-Knowledge**	**Soundness slack**
Noise Flooding	Statistical Analysis	Message & Randomness	$\|\mathbf{z}_i\|_2 = O\left(2^{\lambda_{zk}/2} \cdot \|\gamma_i \cdot \mathbf{r}\|_2\right)$
Rejection Sampling			$\|\mathbf{z}_i\|_2 = O\left(\sqrt{dn} \cdot \|\gamma_i \cdot \mathbf{r}\|_2\right)$
Hint-MLWE	**Cryptographic Assumption**	**Message**	$\|\mathbf{z}_i\|_2 = O\left(\sqrt{\ell} \cdot \|\gamma_i \cdot \mathbf{r}\|_2\right)$

The slack is "independent" to dimension

Results

Practicality: Application to various Lattice-based ZKPs

- Hint-MLWE framework is naturally applicable to various BDLOP-based proof systems:
  - Proof of **multiplicative relation** [ALS20]
  - Proof of knowledge for a **(ternary) solution of linear system** over $\mathbb{Z}_q$ [ENS20]
- **Smaller Parameters** than previous results based on rejection sampling
- Please refer to the full version for more details: https://ia.cr/2023/623

[ALS20] Thomas Attema, Vadim Lyubashevsky, and Gregor Seiler. "Practical product proofs for lattice commitments“, *CRYPTO 2020*.

[ENS20] Muhammed F. Esgin, Ngoc K. Nguyen, and Gregor Seiler. "Practical exact proofs from lattices: New techniques to exploit fully-splitting rings.” *ASIACRYPT 2020*.

thank you!