ZAMA

AUGUST 26, 2026

SNAKE-EYE RESISTANT AND ROBUST PKE FROM (RING-)LWE WITH SMALL SECRETS

SAC 2026

AMIT DEO BENOÎT LIBERT
Zama

Snake-Eye Resistance & Robustness

δ-Snake-eye resistance (Liu et al., Eurocrypt'25; Mohassel, Asiacrypt'10)

Given pk_1 and pk_2, finding ct decrypting to the **same** valid plaintext under both keys is hard:

$$\Pr[Dec(sk_1, ct) = Dec(sk_2, ct) \neq \perp] \leq \delta$$

Snake-Eye Resistance & Robustness

δ-Snake-eye resistance (Liu et al., Eurocrypt'25; Mohassel, Asiacrypt'10)

Given pk_1 and pk_2, finding ct decrypting to the **same** valid plaintext under both keys is hard:

$$\Pr[Dec(sk_1, ct) = Dec(sk_2, ct) \neq \perp] \leq \delta$$

δ-Strong robustness (stronger) (Abdalla-Bellare-Neven, TCC'10)

Hard to find ct decrypting to **any** valid (possibly distinct) plaintexts under both keys:

$$\Pr[Dec(sk_1, ct) \neq \perp \ \wedge \ Dec(sk_2, ct) \neq \perp] \leq \delta$$

- Strongly robust $\Rightarrow$ snake-eye resistant
- Black-box transform: snake-eye resistance $\Rightarrow$ strong robustness (Liu et al., Eurocrypt'25)
- **Non-trivial** for key-private PKE (Bellare-Boldyreva-Pointcheval-Desai, Asiacrypt'01)

Outline

Background
- Snake-eye Resistance & Robustness
- Oblivious Message Retrieval
- Hardness Assumptions

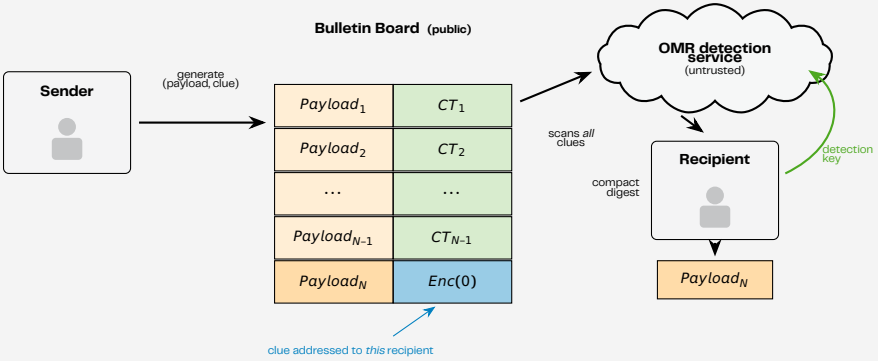
Prior work & difficulty of snake-eye resistance with short keys

Constructions
- Snake-Eye Resistant PKE from Short-key LWE
- Strongly Robust PKE from Ring-LWE
- Optimized Signaling from RLWE + Binary-Secret LWE

Efficiency Considerations

Motivation: Oblivious Message Retrieval

- Senders post **(payload, clue)** on a public board;
- Recipient delegates detection to an *untrusted* server `(Liu-Tromer, Crypto'22)`



- **Server learns nothing** about *which* entries belong to the recipient

Motivation: DoS-Resistance in Oblivious Message Retrieval

Bulletin board entries = (payload, **clue**), where a clue is a lightweight PKE ciphertext encrypting 0

- Recipient gives the server an **FHE encryption** of the clue secret key
- Server **homomorphically** decrypts clues

Motivation: DoS-Resistance in Oblivious Message Retrieval

Bulletin board entries = (payload, **clue**), where a clue is a lightweight PKE ciphertext encrypting 0

- Recipient gives the server an **FHE encryption** of the clue secret key
- Server **homomorphically** decrypts clues

DoS attack (`Liu-Tromer, Crypto'22`)

- Malicious sender crafts a clue that is a **false positive for many recipients** at once
- Snake-eye resistance is exactly what rules this out

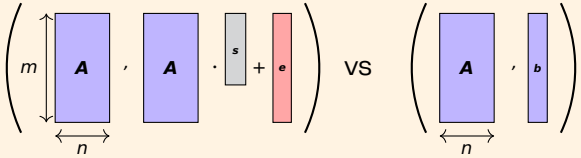
Two PKE requirements: **snake-eye resistant / robust** and **FHE-friendly decryption**

Hardness Assumptions

The Learning-With-Errors (LWE) problem

Parameters: dimension n, samples $m \geq n$, modulus q.

For secret $\boldsymbol{s} \hookleftarrow \chi_s^n$ (*small*) and error $\boldsymbol{e} \hookleftarrow \chi_e^m$ (typically Gaussian), distinguish



for uniform $\boldsymbol{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ and $\boldsymbol{b} \hookleftarrow U(\mathbb{Z}_q^m)$.

- As hard as *worst-case* lattice problems when $\chi_s = \chi_e = D_{\mathbb{Z},\alpha q}$ with $\alpha q = \Omega(\sqrt{n})$
- Small (binary) secrets keep decryption FHE-friendly — but raise difficulties for snake-eye resistance

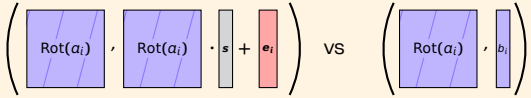
Hardness Assumptions

The Ring-Learning-With-Errors (RLWE) problem

Let $R = \mathbb{Z}[X]/(X^N + 1)$, $R_q = R/qR$ and a distribution χ over R

For $s \hookleftarrow \chi$, distinguish

$$\left\{ (a_i,\ a_i \cdot s + e_i)_i \mid a_i \hookleftarrow U(R_q),\ e_i \hookleftarrow \chi \right\}_{i=1}^{k} \quad \text{vs} \quad \left\{ (a_i, b_i) \hookleftarrow U(R_q^2) \right\}_{i=1}^{k}$$



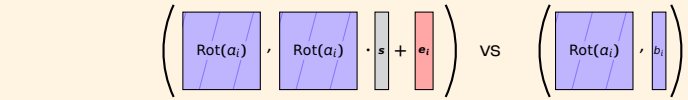
Hardness Assumptions

The Ring-Learning-With-Errors (RLWE) problem

Let $R = \mathbb{Z}[X]/(X^N + 1)$, $R_q = R/qR$ and a distribution χ over R

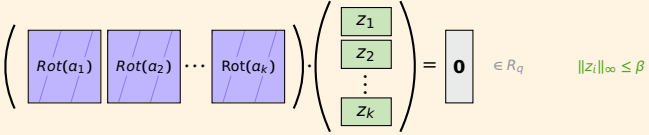
For $s \hookleftarrow \chi$, distinguish

$$\left\{ \left(a_i,\ a_i \cdot s + e_i\right)_i \mid a_i \hookleftarrow U(R_q),\ e_i \hookleftarrow \chi \right\}_{i=1}^{k} \quad \text{vs} \quad \left\{ (a_i, b_i) \hookleftarrow U(R_q^2) \right\}_{i=1}^{k}$$



The Ring-Short-Integer-Solution (RSIS) problem

Given $\boldsymbol{a} = (a_1, \ldots, a_k) \sim U(R_q^k)$, find a short, non-zero $\boldsymbol{z} = (z_1, \ldots, z_k) \in R^k$ s.t. $\langle \boldsymbol{a}, \boldsymbol{z} \rangle = 0 \bmod q$



Difficulty: Snake-eye Resistance & Short Keys

Prior work (Liu et al., Eurocrypt'25):

- Proved PVW (Crypto'08) and a new LWEmongrass scheme snake-eye resistant **under LWE**
- But gave an **attack** on (R)LWE schemes with **small-norm secret keys**

Difficulty: Snake-eye Resistance & Short Keys

Prior work (Liu et al., Eurocrypt'25):

- Proved PVW (Crypto'08) and a new LWEmongrass scheme snake-eye resistant **under LWE**
- But gave an **attack** on (R)LWE schemes with **small-norm secret keys**

The attack in one line

Ciphertexts $(\boldsymbol{a}, b) \in \mathbb{Z}_q^{n+1}$ decrypt via $b - \langle \boldsymbol{a}, \boldsymbol{s} \rangle \bmod q$

Output a **small-norm** $(\boldsymbol{a}, b)$: it decrypts to 0 under **any** sufficiently small key $\boldsymbol{s}$.

Open: efficient, FHE-friendly, snake-eye resistant PKE **from (R)LWE with small secrets**?

Difficulty: Snake-eye Resistance & Short Keys

Prior work (Liu et al., Eurocrypt'25):

- Proved PVW (Crypto'08) and a new LWEmongrass scheme snake-eye resistant **under LWE**
- But gave an **attack** on (R)LWE schemes with **small-norm secret keys**

The attack in one line

Ciphertexts $(\boldsymbol{a}, b) \in \mathbb{Z}_q^{n+1}$ decrypt via $b - \langle \boldsymbol{a}, \boldsymbol{s} \rangle \bmod q$

Output a **small-norm** $(\boldsymbol{a}, b)$: it decrypts to 0 under **any** sufficiently small key $\boldsymbol{s}$.

Open: efficient, FHE-friendly, snake-eye resistant PKE **from (R)LWE with small secrets**?

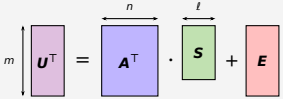
Idea

Reject $(\boldsymbol{a}, b)$ if $\|(\boldsymbol{a}, b)\|_\infty$ is too small

Construction 1: shortLWE with Binary Keys

Variant of (Lindner-Peikert, CT-RSA'11) with a binary key; uses error bound B

- **Keygen:** $\boldsymbol{A} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$, $\boldsymbol{S} \hookleftarrow U(\{0,1\}^{n \times \ell})$, $\boldsymbol{E} \hookleftarrow \chi_e^{m \times \ell}$



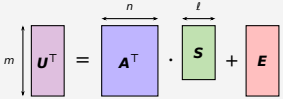
$pk = (\boldsymbol{A}, \boldsymbol{U})$

$sk = \boldsymbol{S}$

Construction 1: shortLWE with Binary Keys

Variant of (Lindner-Peikert, CT-RSA'11) with a binary key; uses error bound B

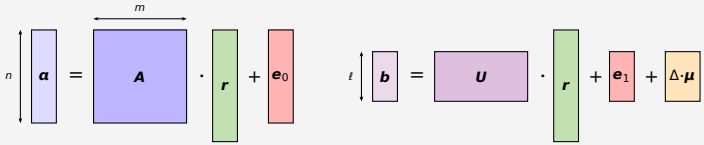
- **Keygen:** $\boldsymbol{A} \hookleftarrow U(\mathbb{Z}_q^{n\times m})$, $\boldsymbol{S} \hookleftarrow U(\{0,1\}^{n\times \ell})$, $\boldsymbol{E} \hookleftarrow \chi_e^{m\times \ell}$



$pk = (\boldsymbol{A}, \boldsymbol{U})$

$sk = \boldsymbol{S}$

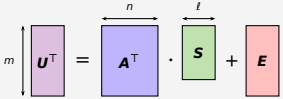
- **Encrypt($\boldsymbol{\mu}$):** $\boldsymbol{r} \hookleftarrow U(\{0,1\}^m)$, $\boldsymbol{e}_0 \hookleftarrow \chi_e^n$, $\boldsymbol{e}_1 \hookleftarrow \chi_e^\ell$, $\Delta = \lfloor q/p \rfloor$



Construction 1: shortLWE with Binary Keys

Variant of (Lindner-Peikert, CT-RSA'11) with a binary key; uses error bound B

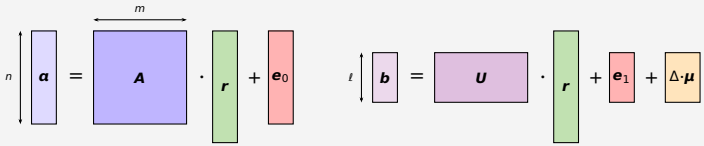
- **Keygen:** $\boldsymbol{A} \hookleftarrow U(\mathbb{Z}_q^{n\times m})$, $\boldsymbol{S} \hookleftarrow U(\{0,1\}^{n\times \ell})$, $\boldsymbol{E} \hookleftarrow \chi_e^{m\times \ell}$



$pk = (\boldsymbol{A}, \boldsymbol{U})$

$sk = \boldsymbol{S}$

- **Encrypt($\boldsymbol{\mu}$):** $\boldsymbol{r} \hookleftarrow U(\{0,1\}^m)$, $\boldsymbol{e}_0 \hookleftarrow \chi_e^n$, $\boldsymbol{e}_1 \hookleftarrow \chi_e^\ell$, $\Delta = \lfloor q/p \rfloor$



Snake-eye resistance fix: extra public check in Decrypt

- **Step 1.** Return $\perp$ if $\|\boldsymbol{a}\|_\infty < 4B$
- **Step 2.** $\boldsymbol{\mu} = \lfloor (\boldsymbol{b} - \boldsymbol{S}^\top \boldsymbol{a})/\Delta \rceil$; return $\perp$ if $\|\boldsymbol{b} - \boldsymbol{S}^\top \boldsymbol{a} - \Delta \cdot \boldsymbol{\mu}\|_\infty > B$; else output $\boldsymbol{\mu}$

Snake-eye Resistance

The correlation LWE (CorLWE) problem (Liu et al., Eurocrypt'25)

For $\boldsymbol{A}_1, \boldsymbol{A}_2 \sim U(\mathbb{Z}_q^{n\times m})$, $\boldsymbol{S}_1, \boldsymbol{S}_2 \sim \chi_s^{n\times \ell}$, $\boldsymbol{E}_1, \boldsymbol{E}_2, \sim \chi_e^{m\times \ell}$, distinguish

$$\left(\boldsymbol{S}_1 - \boldsymbol{S}_2,\ \{\boldsymbol{A}_i,\ \boldsymbol{A}_i^\top \boldsymbol{S}_i + \boldsymbol{E}_i\}_{i=1,2}\right) \quad \text{from} \quad \left(\boldsymbol{S}_1 - \boldsymbol{S}_2,\ \{\boldsymbol{A}_i,\ \boldsymbol{U}_i \sim U(\mathbb{Z}_q^{m\times \ell})\}_{i=1,2}\right),$$

If $\chi_s \sim U(\{0,1\})$, then **CorLWE** is as hard as **LWE** with $\chi_s \sim U(\{0,1\})$ in dimension $\approx n/2$.

Snake-eye Resistance

The correlation LWE (CorLWE) problem (Liu et al., Eurocrypt'25)

For $\boldsymbol{A}_1, \boldsymbol{A}_2 \sim U(\mathbb{Z}_q^{n\times m})$, $\boldsymbol{S}_1, \boldsymbol{S}_2 \sim \chi_s^{n\times \ell}$, $\boldsymbol{E}_1, \boldsymbol{E}_2, \sim \chi_e^{m\times \ell}$, distinguish

$$\left(\boldsymbol{S}_1 - \boldsymbol{S}_2,\ \{\boldsymbol{A}_i,\ \boldsymbol{A}_i^\top \boldsymbol{S}_i + \boldsymbol{E}_i\}_{i=1,2}\right) \quad \text{from} \quad \left(\boldsymbol{S}_1 - \boldsymbol{S}_2,\ \{\boldsymbol{A}_i,\ \boldsymbol{U}_i \sim U(\mathbb{Z}_q^{m\times \ell})\}_{i=1,2}\right),$$

If $\chi_s \sim U(\{0,1\})$, then **CorLWE** is as hard as **LWE** with $\chi_s \sim U(\{0,1\})$ in dimension $\approx n/2$.

If $(\boldsymbol{a}, \boldsymbol{b})$ decrypts to $\boldsymbol{\mu}^*$ under both $\boldsymbol{S}_1$ and $\boldsymbol{S}_2$, then $\|\boldsymbol{a}\|_\infty \geq 4B$ and

$$\|(\boldsymbol{S}_1 - \boldsymbol{S}_2)^\top \boldsymbol{a} \bmod q\|_\infty \leq 2B$$

Snake-eye Resistance

The correlation LWE (CorLWE) problem (Liu et al., Eurocrypt'25)

For $\boldsymbol{A}_1, \boldsymbol{A}_2 \sim U(\mathbb{Z}_q^{n\times m})$, $\boldsymbol{S}_1, \boldsymbol{S}_2 \sim \chi_s^{n\times \ell}$, $\boldsymbol{E}_1, \boldsymbol{E}_2, \sim \chi_e^{m\times \ell}$, distinguish

$$\left(\boldsymbol{S}_1 - \boldsymbol{S}_2,\ \{\boldsymbol{A}_i,\ \boldsymbol{A}_i^\top \boldsymbol{S}_i + \boldsymbol{E}_i\}_{i=1,2}\right) \quad \text{from} \quad \left(\boldsymbol{S}_1 - \boldsymbol{S}_2,\ \{\boldsymbol{A}_i,\ \boldsymbol{U}_i \sim U(\mathbb{Z}_q^{m\times \ell})\}_{i=1,2}\right),$$

If $\chi_s \sim U(\{0,1\})$, then **CorLWE** is as hard as **LWE** with $\chi_s \sim U(\{0,1\})$ in dimension $\approx n/2$.

If $(\boldsymbol{a}, \boldsymbol{b})$ decrypts to $\boldsymbol{\mu}^*$ under both $\boldsymbol{S}_1$ and $\boldsymbol{S}_2$, then $\|\boldsymbol{a}\|_\infty \geq 4B$ and

$$\|(\boldsymbol{S}_1 - \boldsymbol{S}_2)^\top \boldsymbol{a} \bmod q\|_\infty \leq 2B$$

Reduction from CorLWE:

- Build $\{pk_i\}_{i=1}^2$ using $\{(\boldsymbol{A}_i, \boldsymbol{U}_i \stackrel{?}{=} \boldsymbol{A}_i^\top \boldsymbol{S}_i + \boldsymbol{E}_i)\}_{i=1}^2$; keep $\bar{\boldsymbol{S}} \triangleq \boldsymbol{S}_1 - \boldsymbol{S}_2 \in \{-1, 0, 1\}^{m\times \ell}$ internally
- When $\mathcal{A}$ outputs $(\boldsymbol{a}, \boldsymbol{b})$, return 1 iff $\bar{\boldsymbol{S}}$ satisfies $\|\bar{\boldsymbol{S}}^\top \boldsymbol{a} \bmod q\|_\infty \leq 2B$
- If $\boldsymbol{U}_1, \boldsymbol{U}_2 \sim U(\mathbb{Z}_q^{m\times \ell})$, $\bar{\boldsymbol{S}}$ is independent of $\mathcal{A}$'s view and $\bar{\boldsymbol{S}} \sim \mathcal{D}$ with $\mathcal{D}[0] = 1/2$ and $\mathcal{D}[\pm 1] = 1/4$;

$$\Pr\left[\|\bar{\boldsymbol{S}}^\top \boldsymbol{a} \bmod q\|_\infty \leq \tfrac{1}{2}\|\boldsymbol{a}\|_\infty\right] \leq 2^{-\ell}$$

(Lyubashevsky-Nguyen-Seiler, PKC'21)

Construction 2: Randomness-Recovering RLWE PKE

- Cyclotomic ring $R = \mathbb{Z}[X]/(X^n + 1)$, *fully splitting* $R_q = R/(qR)$ with $q \equiv 1 \pmod{2n}$
- Three moduli: q (ciphertext), p (randomness recovery), t (plaintext)

- **Keygen:** Choose $s, e \hookleftarrow \chi$; set $b = p \cdot (a \cdot s + e)$, re-sample until $b \in R_q^\times$
  Output $sk = s$ and $pk = (a, b)$

Construction 2: Randomness-Recovering RLWE PKE

- Cyclotomic ring $R = \mathbb{Z}[X]/(X^n + 1)$, *fully splitting* $R_q = R/(qR)$ with $q \equiv 1 \pmod{2n}$
- Three moduli: q (ciphertext), p (randomness recovery), t (plaintext)

- **Keygen:** Choose $s, e \hookleftarrow \chi$; set $b = p \cdot (a \cdot s + e)$, re-sample until $b \in R_q^\times$
  Output $sk = s$ and $pk = (a, b)$
- **Encrypt(μ):** Sample $r, e_1, e_2 \hookleftarrow \chi$ and compute

$$c_1 = a \cdot r + e_1, \qquad c_2 = b \cdot r + e_2 + \mu \cdot \lfloor q/t \rceil$$

Construction 2: Randomness-Recovering RLWE PKE

- Cyclotomic ring $R = \mathbb{Z}[X]/(X^n + 1)$, *fully splitting* $R_q = R/(qR)$ with $q \equiv 1 \pmod{2n}$
- Three moduli: q (ciphertext), p (randomness recovery), t (plaintext)

- **Keygen:** Choose $s, e \hookleftarrow \chi$; set $b = p \cdot (a \cdot s + e)$, re-sample until $b \in R_q^\times$
  Output $sk = s$ and $pk = (a, b)$
- **Encrypt(μ):** Sample $r, e_1, e_2 \hookleftarrow \chi$ and compute

$$c_1 = a \cdot r + e_1, \qquad c_2 = b \cdot r + e_2 + \mu \cdot \lfloor q/t \rceil$$

Robustness mechanism: recover encryption randomness (variant of Hoffmann *et al.*; PKC '23)

- Decrypt rejects if $\|c_1\|_\infty < B$
- Otherwise,

$$c_2 - c_1 \cdot (p \cdot s) \bmod q \;=\; (p \cdot noise + e_2) + \mu \cdot \lfloor q/t \rceil$$

  reveals $\mu \in R_t$, and then $(e_2, r, e_1) \in R^3$ (rejecting if $\|(e_2, r, e_1)\|_\infty > B$)
- A non-rejected c_1 certifies small $(r, e_1) \in R^2$ with $c_1 = a \cdot r + e_1$

Strong Robustness under Ring-SIS

A collision $(r, e_1) \in R^2$, $(r', e_1') \in R^2$ means one c_1 opens under both keys:

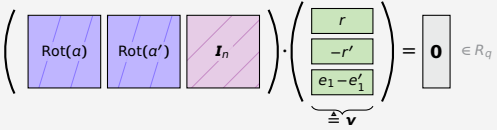
$$c_1 = a \cdot r + e_1 = a' \cdot r' + e_1' \mod q$$

Strong Robustness under Ring-SIS

A collision $(r, e_1) \in R^2$, $(r', e_1') \in R^2$ means one c_1 opens under both keys:

$$c_1 = a \cdot r + e_1 = a' \cdot r' + e_1' \mod q$$

Reduction obtains a **short** $\boldsymbol{v} = (r, -r', e_1 - e_1') \in R^3$ with



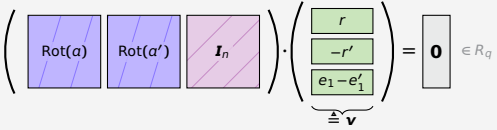
- $\boldsymbol{v} \neq \boldsymbol{0}$: if $\|c_1\|_\infty < B$, ciphertext is rejected ($\boldsymbol{v} = \boldsymbol{0} \Rightarrow r = r' = 0$ and $c_1 = e_1 = e_1'$)
- Solves an $RSIS_{n,k,q,\beta}$ instance $(a_1, \ldots, a_k) \in R_q^k$: set $a = a_1 a_i^{-1}$, $a' = a_2 a_i^{-1}$ with $a_i \in R_q^\times$

Strong Robustness under Ring-SIS

A collision $(r, e_1) \in R^2$, $(r', e_1') \in R^2$ means one c_1 opens under both keys:

$$c_1 = a \cdot r + e_1 = a' \cdot r' + e_1' \mod q$$

Reduction obtains a **short** $\boldsymbol{v} = (r, -r', e_1 - e_1') \in R^3$ with



- $\boldsymbol{v} \neq \boldsymbol{0}$: if $\|c_1\|_\infty < B$, ciphertext is rejected ($\boldsymbol{v} = \boldsymbol{0} \Rightarrow r = r' = 0$ and $c_1 = e_1 = e_1'$)
- Solves an $RSIS_{n,k,q,\beta}$ instance $(a_1, \ldots, a_k) \in R_q^k$: set $a = a_1 a_i^{-1}$, $a' = a_2 a_i^{-1}$ with $a_i \in R_q^\times$

Result

Strong robustness under $RSIS_{n,k,q,\beta}$, with $k = O(\lambda / \log(q/n))$ and $q > n$

First strongly robust PKE from RLWE **in the standard model**

Problem: Expensive Homomorphic Detection

Homomorphically detecting encryptions of 0 is expensive

- Computing $e_2 = \zeta \bmod p$ is non-linear — needs a homomorphic reduction mod p
- Via interpolation (`Iliashenko-Nègre-Zucca, WHAC'21`):

$$\approx \sqrt{q} \text{ homomorphic mults, } \lceil \log(q-1) \rceil + 1 \text{ levels}$$

- At depth > 30: $N \geq 2^{16}$, so that $q \geq 786433$ and $\sqrt{q} - 3 > 886$ mults *per* mod-p reduction

Bottleneck

For $n = 1024$: ≈ one million homomorphic multiplications just for the mod-p step (prohibitive)

Construction 3: A KEM–DEM Twist

Idea: replace randomness recovery with encapsulation of a **binary** secret

- **Encapsulate** a binary $\boldsymbol{r} \in \{0,1\}^d$ with a truncated LPR ciphertext
  `(Lyubashevsky-Peikert-Regev, Eurocrypt'10)`
- Commit to $\boldsymbol{r}$ via $\boldsymbol{c}_3 = \boldsymbol{A}^\top \boldsymbol{r} + \boldsymbol{e}_3$
- Binary $\boldsymbol{r}$ $\Rightarrow$ homomorphic decoding uses two batched range checks
  (no homomorphic rounding / mod-p)

Construction 3: A KEM–DEM Twist

Idea: replace randomness recovery with encapsulation of a **binary** secret

- **Encapsulate** a binary $\boldsymbol{r} \in \{0,1\}^d$ with a truncated LPR ciphertext
  `(Lyubashevsky-Peikert-Regev, Eurocrypt'10)`
- Commit to $\boldsymbol{r}$ via $\boldsymbol{c}_3 = \boldsymbol{A}^\top \boldsymbol{r} + \boldsymbol{e}_3$
- Binary $\boldsymbol{r}$ ⇒ homomorphic decoding uses two batched range checks
  (no homomorphic rounding / mod-p)

Why LWE *and* RLWE?

- $\boldsymbol{c}_3$ is a **statistically binding commitment** to $\boldsymbol{r}$ (statistical snake-eye resistance)
- LWE dimension d is flexible: can be $< n$ and need not be a power of 2 (shorter ciphertext)
- Deriving $\boldsymbol{A}$ from a random oracle ⇒ public key is one ring element $b \in R_q$

Concrete Performance of Construction 3

Removing the mod-p reduction cuts the dominant cost of Construction 2

Example parameters (128-bit, $\epsilon_n \approx 2^{-30}$)	
RLWE dim $n = 1024$	LWE dim $d = 680$, $m = 124$
Hamming weight $h = 80$	$B_e = B' = 45$
BFV ring $N = 2^{17}$	plaintext mod $q = 786433$
mult. depth $= 61$	clue key $\approx 2.44\,\text{kB}$

Concrete Performance of Construction 3

Removing the mod-p reduction cuts the dominant cost of Construction 2

Example parameters (128-bit, $\epsilon_n \approx 2^{-30}$)	
RLWE dim $n = 1024$	LWE dim $d = 680$, $m = 124$
Hamming weight $h = 80$	$B_e = B' = 45$
BFV ring $N = 2^{17}$	plaintext mod $q = 786433$
mult. depth $= 61$	clue key ≈ 2.44 kB

- **Good:** public/clue keys $\approx 2\times$ smaller than LWE solutions
- **Still:** homomorphic detection slower than `LWEmongrass` (`Liu et al., Eurocrypt'25`) due to $d = 680$ affine transforms and two sequential batch range checks

Takeaways & Open Problems

What we showed

- A **simple public norm check** makes short-key LWE PKE snake-eye resistant (binary *and* binomial secrets)
- First **RLWE** robust PKE *without* KEM–DEM or random oracles: randomness recovery + Ring-SIS assumption (or statistically, in partially splitting rings)
- Optimized RLWE+LWE with 2× smaller keys and statistical snake-eye resistance

Takeaways & Open Problems

What we showed

- A **simple public norm check** makes short-key LWE PKE snake-eye resistant (binary *and* binomial secrets)
- First **RLWE** robust PKE *without* KEM–DEM or random oracles: randomness recovery + Ring-SIS assumption (or statistically, in partially splitting rings)
- Optimized RLWE+LWE with 2× smaller keys and statistical snake-eye resistance

Open

- Close the gap to LWE-based OMR performance (fewer affine transforms / range checks)
- Ring analogue of the Construction-1 argument (correlated *ring*-LWE)

First step towards DoS-resistant OMR under structured lattice assumptions

Contact and Links

benoit.libert@zama.ai

zama.org

github.com/zama-ai

zama.org/community