RLWE-based Zero-Knowledge Proofs for linear and multiplicative relations

Ramiro Martínez Paz Morillo

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

17th IMA International Conference on Cryptography and Coding

Learning With Errors (LWE)

Definition

- $n, q \in \mathbb{Z}_{>0}$
- χ a discrete probability distribution in $\mathbb{Z}$
- $\mathbf{s}$ a secret vector in $\mathbb{Z}_q^n$

$\mathcal{L}_{\mathbf{s},\chi}$ is the probability distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}$ following χ and computing $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Learning With Errors (LWE)

Definition

- $n, q \in \mathbb{Z}_{>0}$
- χ a discrete probability distribution in $\mathbb{Z}$
- $\mathbf{s}$ a secret vector in $\mathbb{Z}_q^n$

$\mathcal{L}_{\mathbf{s},\chi}$ is the probability distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}$ following χ and computing $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Learning With Errors (LWE)

Definition

- $n, q \in \mathbb{Z}_{>0}$
- χ a discrete probability distribution in $\mathbb{Z}$
- $\mathbf{s}$ a secret vector in $\mathbb{Z}_q^n$

$\mathcal{L}_{\mathbf{s},\chi}$ is the probability distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}$ following χ and computing $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Learning With Errors (LWE)

Definition

- $n, q \in \mathbb{Z}_{>0}$
- χ a discrete probability distribution in $\mathbb{Z}$
- $\mathbf{s}$ a secret vector in $\mathbb{Z}_q^n$

$\mathcal{L}_{\mathbf{s},\chi}$ is the probability distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}$ following χ and computing $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Learning With Errors (LWE)

Definition

- $n, q \in \mathbb{Z}_{>0}$
- χ a discrete probability distribution in $\mathbb{Z}$
- $\mathbf{s}$ a secret vector in $\mathbb{Z}_q^n$

$\mathcal{L}_{\mathbf{s},\chi}$ is the probability distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}$ following χ and computing $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Decisional-LWE

is the problem of deciding if pairs $(\mathbf{a}, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ are samples from $\mathcal{L}_{\mathbf{s},\chi}$ or samples from the uniform distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Learning With Errors (LWE)

Definition

- $n, q \in \mathbb{Z}_{>0}$
- χ a discrete probability distribution in $\mathbb{Z}$
- $\mathbf{s}$ a secret vector in $\mathbb{Z}_q^n$

$\mathcal{L}_{\mathbf{s},\chi}$ is the probability distribution in $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}$ following χ and computing $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Search-LWE

is the problem of recovering $\mathbf{s}$ from samples $(\mathbf{a}, c = \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ chosen following $\mathcal{L}_{\mathbf{s},\chi}$.

Learning With Errors (LWE)

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ a_{31} & a_{32} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{pmatrix}$$

$$\mathbf{As} + \mathbf{e}$$

Learning With Errors (LWE)

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ a_{31} & a_{32} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{pmatrix}$$

$$\mathbf{As} + \mathbf{e}$$

Learning With Errors (LWE)

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{pmatrix}$$

$$\mathbf{As} + \mathbf{e}$$

Learning With Errors (LWE)

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{pmatrix}$$

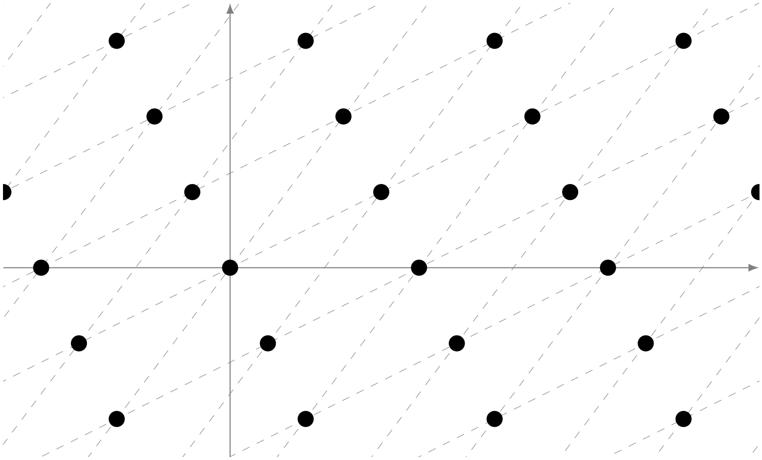
$\mathbf{A}\mathbf{s} + \mathbf{e}$

Learning With Errors (LWE)

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ a_{31} & a_{32} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{pmatrix}$$

$$\mathbf{As} + \mathbf{e}$$

$$\Lambda_q(\mathbf{A}) = \{\mathbf{b} \quad | \quad \mathbf{b} = \mathbf{A}\mathbf{z} \mod q,\ \mathbf{z} \in \mathbb{Z}^n\}$$



Ring Learning With Errors (RLWE)

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \\ b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & \dots & b_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \dots & b_0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \\ e_{n+1} \\ e_{n+2} \\ e_{n+3} \\ \vdots \\ e_{2n} \\ \vdots \end{pmatrix}$$

Ring Learning With Errors (RLWE)

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \\ b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & \dots & b_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \dots & b_0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \\ e_{n+1} \\ e_{n+2} \\ e_{n+3} \\ \vdots \\ e_{2n} \\ \vdots \end{pmatrix}$$

Ring Learning With Errors (RLWE)

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \\ b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & \dots & b_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \dots & b_0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \\ e_{n+1} \\ e_{n+2} \\ e_{n+3} \\ \vdots \\ e_{2n} \\ \vdots \end{pmatrix}$$

Ring Learning With Errors (RLWE)

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \\ b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & \dots & b_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \dots & b_0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \\ e_{n+1} \\ e_{n+2} \\ e_{n+3} \\ \vdots \\ e_{2n} \\ \vdots \end{pmatrix}$$

Ring Learning With Errors (RLWE)

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \\ b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & \dots & b_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \dots & b_0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \\ e_{n+1} \\ e_{n+2} \\ e_{n+3} \\ \vdots \\ e_{2n} \\ \vdots \end{pmatrix}$$

Ring Learning With Errors (RLWE)

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \\ b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & \dots & b_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & \dots & b_0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \\ e_{n+1} \\ e_{n+2} \\ e_{n+3} \\ \vdots \\ e_{2n} \\ \vdots \end{pmatrix}$$

Ring Learning With Errors (RLWE)

$$R_q = \mathbb{Z}_q[x]/\left\langle x^n + 1 \right\rangle$$

$$\begin{pmatrix} a(x) \\ b(x) \\ \vdots \end{pmatrix} s(x) + \begin{pmatrix} e_1(x) \\ e_2(x) \\ \vdots \end{pmatrix}$$

Goal

Given a pair of vectors of polynomials $(\mathbf{a}, \mathbf{b}) \in R_q^m \times R_q^m$ we want to prove that we know a polynomial $s \in R_q$ and a vector of small polynomials $\mathbf{e} \in R_q^m$ such that:

$$\mathbf{b} = \mathbf{a}s + \mathbf{e}, \ \|\mathbf{e}\| \leq 2^{\kappa}$$

Interactive Zero-Knowledge Proofs

Definition

An *Interactive Zero-Knowledge Proof* is a protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$ in which, given x, $\mathcal{P}$ tries to convince $\mathcal{V}$ that he knows a witness w related to x, $(x, w) \in \mathcal{R}$. To do so they exchange some messages and the verifier decides if he is convinced depending on the conversation.

Definition

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

- **Completeness**: if an honest $\mathcal{P}$ knows $(x, w) \in R$ 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. ?

Naïve approach

$\mathcal{P}(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e}; s, \mathbf{e})$		$\mathcal{V}(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$
$r \xleftarrow{\$} R_q, \mathbf{f} \xleftarrow{\$} \chi$		
$\mathbf{c} = \mathbf{a}r + \mathbf{f}$		
	$\xrightarrow{\quad \mathbf{c} \quad}$	
		$\alpha \xleftarrow{\$} R_q$
	$\xleftarrow{\quad \alpha \quad}$	
$t = r + \alpha s$		
$\mathbf{g} = \mathbf{f} + \alpha \mathbf{e}$		
	$\xrightarrow{\quad t, \mathbf{g} \quad}$	
		$\mathbf{a}t + \mathbf{g} \stackrel{?}{=} \mathbf{c} + \alpha \mathbf{b}$

Naïve approach

$\mathcal{P}(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e}; s, \mathbf{e})$		$\mathcal{V}(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$
$r \xleftarrow{\$} R_q, \mathbf{f} \xleftarrow{\$} \chi$		
$\mathbf{c} = \mathbf{a}r + \mathbf{f}$		
	$\xrightarrow{\quad \mathbf{c} \quad}$	
		$\alpha \xleftarrow{\$} R_q$
	$\xleftarrow{\quad \alpha \quad}$	
$t = r + \alpha s$		
$\mathbf{g} = \mathbf{f} + \alpha \mathbf{e}$		
	$\xrightarrow{\quad t, \mathbf{g} \quad}$	
		$\mathbf{a}t + \mathbf{g} \stackrel{?}{=} \mathbf{c} + \alpha \mathbf{b}$

There are two alternatives:

Rejection sampling

- abort probability
- gap Σ-protocol

Stern's protocols

- t-soundness
- more moves

Stern protocol

Given $(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$, we sample $r \xleftarrow{\$} R_q$, $\mathbf{f} \xleftarrow{\$} R_q^k$ and prove:

a) $\|\mathbf{e}\| \leq 2^{\kappa}$
b) $\mathbf{c} = \mathbf{a}r + \mathbf{f}$
c) $\mathbf{c} + \mathbf{b} = \mathbf{a}(r + s) + (\mathbf{f} + \mathbf{e})$

[Ste96]

From codes to Lattices

[LNSW13]

- $(8, 3, -12, 15) = \varphi^{-1}(8 + 3x - 12x^2 + 15x^3)$
- $(24, 19, 4, 31) = (8, 3, -12, 15) + (2^4, 2^4, 2^4, 2^4)$
- $(24, 19, 4, 31) =$

$$\begin{pmatrix} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

- $\mathbf{b} = \mathbf{a}s + \phi(\mathbf{I}' \sum_j 2^j \mathbf{e}_j - 2^\kappa \mathbb{1}_{nk})$

From codes to Lattices

[LNSW13]

- $(8, 3, -12, 15) = \varphi^{-1}(8 + 3x - 12x^2 + 15x^3)$
- $(24, 19, 4, 31) = (8, 3, -12, 15) + (2^4, 2^4, 2^4, 2^4)$
- $(24, 19, 4, 31) =$

$$\begin{pmatrix} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

- $\mathbf{b} = \mathbf{a}\mathbf{s} + \phi(\mathbf{I}' \sum_j 2^j \mathbf{e}_j - 2^\kappa \mathbb{1}_{nk})$

From codes to Lattices

[LNSW13]

- $(8, 3, -12, 15) = \varphi^{-1}(8 + 3x - 12x^2 + 15x^3)$
- $(24, 19, 4, 31) = (8, 3, -12, 15) + (2^4, 2^4, 2^4, 2^4)$
- $(24, 19, 4, 31) =$

$$\left(2^0\ 2^1\ 2^2\ 2^3\ 2^4\right)\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

- $\mathbf{b} = \mathbf{a}s + \phi(\mathbf{I}' \sum_j 2^j \mathbf{e}_j - 2^\kappa \mathbb{1}_{nk})$

From codes to Lattices

[LNSW13]

- $(8, 3, -12, 15) = \varphi^{-1}(8 + 3x - 12x^2 + 15x^3)$
- $(24, 19, 4, 31) = (8, 3, -12, 15) + (2^4, 2^4, 2^4, 2^4)$
- $(24, 19, 4, 31) =$

$$\begin{pmatrix} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

- $\mathbf{b} = \mathbf{a}\mathbf{s} + \phi(\mathbf{I}' \sum_j 2^j \mathbf{e}_j - 2^\kappa \mathbb{1}_{nk})$

From codes to Lattices

[LNSW13]

- $(8, 3, -12, 15) = \varphi^{-1}(8 + 3x - 12x^2 + 15x^3)$
- $(24, 19, 4, 31) = (8, 3, -12, 15) + (2^4, 2^4, 2^4, 2^4)$
- $(24, 19, 4, 31) =$

$$\begin{pmatrix} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

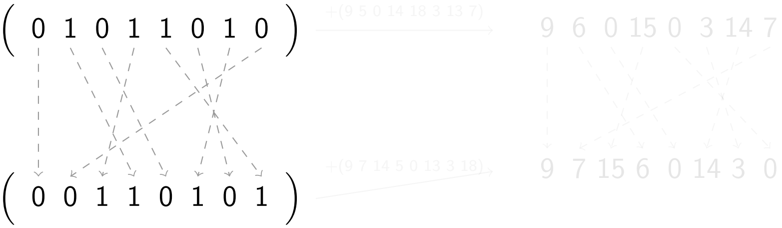
- $\mathbf{b} = \mathbf{a}s + \phi(\mathbf{I}' \sum_j 2^j \mathbf{e}_j - 2^\kappa \mathbb{1}_{nk})$

Hiding errors

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{+(9\ 5\ 0\ 14\ 18\ 3\ 13\ 7)} 9\ \ 6\ \ 0\ \ 15\ \ 0\ \ 3\ \ 14\ \ 7$$

$$0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1 \xrightarrow{+(9\ 7\ 14\ 5\ 0\ 13\ 3\ 18)} 9\ \ 7\ \ 15\ \ 6\ \ 0\ \ 14\ \ 3\ \ 0$$

Hiding errors



Hiding errors

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{+(9\ 5\ 0\ 14\ 18\ 3\ 13\ 7)} \begin{pmatrix} 9 & 6 & 0 & 15 & 0 & 3 & 14 & 7 \end{pmatrix}$$

$$\begin{matrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{matrix} \xrightarrow{+(9\ 7\ 14\ 5\ 0\ 13\ 3\ 18)} \begin{matrix} 9 & 7 & 15 & 6 & 0 & 14 & 3 & 0 \end{matrix}$$

Hiding errors

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{+(9\ 5\ 0\ 14\ 18\ 3\ 13\ 7)} \begin{pmatrix} 9 & 6 & 0 & 15 & 0 & 3 & 14 & 7 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{+(9\ 7\ 14\ 5\ 0\ 13\ 3\ 18)} \begin{pmatrix} 9 & 7 & 15 & 6 & 0 & 14 & 3 & 0 \end{pmatrix}$$

Stern protocol

Given $(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$, we sample $r \xleftarrow{\$} R_q$, $\mathbf{f}_j \xleftarrow{\$} R_q^k$ and prove:

Properties

a) $\mathbf{e}_j \in \mathcal{B}_{nk} \subseteq \{0,1\}^{2nk}$

b) $\mathbf{c} = \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

c) $\mathbf{c} + \mathbf{b} = \mathbf{a}(r+s) + \phi(\mathbf{I}' \sum_j 2^j (\mathbf{f}_j + \mathbf{e}_j) - 2^\kappa \mathbb{1}_{nk})$

Commitments

i) $\pi_j, \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

ii) $\pi_j(\mathbf{f}_j)$

iii) $\pi_j(\mathbf{f}_j + \mathbf{e}_j)$

Stern protocol

Given $(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$, we sample $r \xleftarrow{\$} R_q$, $\mathbf{f}_j \xleftarrow{\$} R_q^k$ and prove:

Properties

a) $\mathbf{e}_j \in \mathcal{B}_{nk} \subseteq \{0,1\}^{2nk}$

b) $\mathbf{c} = \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

c) $\mathbf{c} + \mathbf{b} = \mathbf{a}(r+s) + \phi(\mathbf{I}' \sum_j 2^j (\mathbf{f}_j + \mathbf{e}_j) - 2^\kappa \mathbb{1}_{nk})$

Commitments

i) $\pi_j, \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

ii) $\pi_j(\mathbf{f}_j)$

iii) $\pi_j(\mathbf{f}_j + \mathbf{e}_j)$

Stern protocol

Given $(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$, we sample $r \xleftarrow{\$} R_q$, $\mathbf{f}_j \xleftarrow{\$} R_q^k$ and prove:

Properties

a) $\mathbf{e}_j \in \mathcal{B}_{nk} \subseteq \{0,1\}^{2nk}$

b) $\mathbf{c} = \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

c) $\mathbf{c} + \mathbf{b} = \mathbf{a}(r+s) + \phi(\mathbf{I}' \sum_j 2^j (\mathbf{f}_j + \mathbf{e}_j) - 2^\kappa \mathbb{1}_{nk})$

Commitments

i) $\pi_j, \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

ii) $\pi_j(\mathbf{f}_j)$

iii) $\pi_j(\mathbf{f}_j + \mathbf{e}_j)$

Stern protocol

Given $(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$, we sample $r \xleftarrow{\$} R_q$, $\mathbf{f}_j \xleftarrow{\$} R_q^k$ and prove:

Properties

a) $\mathbf{e}_j \in \mathcal{B}_{nk} \subseteq \{0,1\}^{2nk}$

b) $\mathbf{c} = \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

c) $\mathbf{c} + \mathbf{b} = \mathbf{a}(r+s) + \phi(\mathbf{I}' \sum_j 2^j (\mathbf{f}_j + \mathbf{e}_j) - 2^\kappa \mathbb{1}_{nk})$

Commitments

i) $\pi_j, \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

ii) $\pi_j(\mathbf{f}_j)$

iii) $\pi_j(\mathbf{f}_j + \mathbf{e}_j)$

Stern protocol

Given $(\mathbf{a}, \mathbf{b} = \mathbf{a}s + \mathbf{e})$, we sample $r \xleftarrow{\$} R_q$, $\mathbf{f}_j \xleftarrow{\$} R_q^k$ and prove:

Properties

a) $\mathbf{e}_j \in \mathcal{B}_{nk} \subseteq \{0,1\}^{2nk}$

b') $\mathbf{c} + \alpha\mathbf{b} = \mathbf{a}(r + \alpha s) + \phi(\mathbf{I}' \sum_j 2^j(\mathbf{f}_j + \alpha\mathbf{e}_j))$

Commitments

i) $\pi_j, \mathbf{a}r + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j)$

ii') $\pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j)$

[CVEYA11]

Reducing Soundness Error

- Combine (*ii*) and (*iii*): $\pi(\mathbf{f}_j + \alpha \mathbf{e}_j)$
- 3-move protocol $\rightarrow$ 5-move protocol
- allows to prove multiplicative relations

Reducing Soundness Error

- Combine (*ii*) and (*iii*): $\pi(\mathbf{f}_j + \alpha \mathbf{e}_j)$
- 3-move protocol $\rightarrow$ 5-move protocol
- allows to prove multiplicative relations

Reducing Soundness Error

- Combine (*ii*) and (*iii*): $\pi(\mathbf{f}_j + \alpha \mathbf{e}_j)$
- 3-move protocol $\rightarrow$ 5-move protocol
- allows to prove multiplicative relations

Lattice-based commitments

Based on the commitment scheme of [BKLP15]

$$(\mathbf{c}, d) = \mathrm{Com}_{\mathbf{a},\mathbf{b}}(m, (r, \mathbf{e})) = (\mathbf{a}m + \mathbf{b}r + \mathbf{e}, (r, \mathbf{e}))$$

$$\mathbf{a}, \mathbf{b} \in R_q^k,\ r \in R_q,\ \mathbf{e} \in \chi_{\sigma_{\mathbf{e}}}$$

$\mathrm{Ver}_{\mathbf{a},\mathbf{b}}(m, \mathbf{c}, (r, \mathbf{e}))$ accepts if:

- $\mathbf{c} = \mathbf{a}m + \mathbf{b}r + \mathbf{e}$
- $\|\mathbf{e}\|_\infty \leq n$

Lattice-based commitments

Based on the commitment scheme of [BKLP15]

$$(\mathbf{c}, d) = \mathsf{Com}_{\mathbf{a},\mathbf{b}}(m, (r, \mathbf{e})) = (\mathbf{a}m + \mathbf{b}r + \mathbf{e}, (r, \mathbf{e}))$$

$$\mathbf{a}, \mathbf{b} \in R_q^k,\ r \in R_q,\ \mathbf{e} \in \chi_{\sigma_{\mathbf{e}}}$$

$\mathsf{Ver}_{\mathbf{a},\mathbf{b}}(m, \mathbf{c}, (r, \mathbf{e}))$ accepts if:

- $\mathbf{c} = \mathbf{a}m + \mathbf{b}r + \mathbf{e}$
- $\|\mathbf{e}\|_\infty \le n$

Lattice-based commitments

Based on the commitment scheme of [BKLP15]

$$(\mathbf{c}, d) = \mathrm{Com}_{\mathbf{a},\mathbf{b}}(m, (r, \mathbf{e})) = (\mathbf{a}m + \mathbf{b}r + \mathbf{e}, (r, \mathbf{e}))$$

$$\mathbf{a}, \mathbf{b} \in R_q^k,\ r \in R_q,\ \mathbf{e} \in \chi_{\sigma_{\mathbf{e}}}$$

$\mathrm{Ver}_{\mathbf{a},\mathbf{b}}(m, \mathbf{c}, (r, \mathbf{e}))$ accepts if:

- $\mathbf{c} = \mathbf{a}m + \mathbf{b}r + \mathbf{e}$
- $\|\mathbf{e}\|_\infty \leq n$

$\mathcal{P}\left((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e}\right)$ $\mathcal{V}\left((\mathbf{a},\mathbf{b}),\mathbf{c}\right)$

$$\pi_0,\ldots,\pi_{\kappa-1} \xleftarrow{\$} \mathfrak{S}_{2nk}$$

$$\mathbf{f}_0,\ldots,\mathbf{f}_{\kappa-1} \xleftarrow{\$} \mathbb{Z}_q^{2nk}$$

$$\mu,\rho \xleftarrow{\$} R_q$$

$$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}'\textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{c_1,\,c_2}$$

$$\xleftarrow{\alpha} \qquad \alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j) \qquad \xrightarrow{\{\mathbf{g}_j\}_j}$$

$$\xleftarrow{b} \qquad b \xleftarrow{\$} \{0,1\}$$

Open c

$\mathcal{P}((\mathbf{a}, \mathbf{b}), \mathbf{c}; m, r, \mathbf{e})$ $\qquad$ $\mathcal{V}((\mathbf{a}, \mathbf{b}), \mathbf{c})$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu, \rho \xleftarrow{\$} R_q$$

$$(c_1, d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2, d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{c_1, c_2}$$

$$\xleftarrow{\alpha} \qquad \alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha \mathbf{e}_j) \qquad \xrightarrow{\{\mathbf{g}_j\}_j}$$

$$\xleftarrow{b} \qquad b \xleftarrow{\$} \{0, 1\}$$

Open c

$\mathcal{P}((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e})$ $\qquad$ $\mathcal{V}((\mathbf{a},\mathbf{b}),\mathbf{c})$

$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu,\rho \xleftarrow{\$} R_q$

$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j))$

$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$

$\xrightarrow{c_1,\, c_2}$

$\xleftarrow{\alpha}$ $\qquad$ $\alpha \xleftarrow{\$} \mathbb{Z}_q$

$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j)$

$\xrightarrow{\{\mathbf{g}_j\}_j}$

$\xleftarrow{b}$ $\qquad$ $b \xleftarrow{\$} \{0,1\}$

Open c

$\mathcal{P}\left((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e}\right)$ $\qquad$ $\mathcal{V}\left((\mathbf{a},\mathbf{b}),\mathbf{c}\right)$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu,\rho \xleftarrow{\$} R_q$$

$$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{c_1,\,c_2}$$

$$\alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\xleftarrow{\alpha}$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j)$$

$$\xrightarrow{\{\mathbf{g}_j\}_j}$$

$$b \xleftarrow{\$} \{0,1\}$$

$$\xleftarrow{b}$$

Open c

$\mathcal{P}\left((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e}\right)$ $\mathcal{V}\left((\mathbf{a},\mathbf{b}),\mathbf{c}\right)$

$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu,\rho \xleftarrow{\$} R_q$

$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j))$

$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$

$\xrightarrow{c_1,\,c_2}$

$\xleftarrow{\alpha}$ $\alpha \xleftarrow{\$} \mathbb{Z}_q$

$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j)$ $\xrightarrow{\{\mathbf{g}_j\}_j}$

$b \xleftarrow{\$} \{0,1\}$

$\xleftarrow{b}$

Open c

$\mathcal{P}((\mathbf{a},\mathbf{b}),\mathbf{c}; m, r, \mathbf{e})$ $\qquad$ $\mathcal{V}((\mathbf{a},\mathbf{b}),\mathbf{c})$

$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu, \rho \xleftarrow{\$} R_q$

$(c_1, d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \sum_j 2^j \mathbf{f}_j))$

$(c_2, d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$

$\xrightarrow{c_1, c_2}$

$\alpha \xleftarrow{\$} \mathbb{Z}_q$

$\xleftarrow{\alpha}$

$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j)$

$\xrightarrow{\{\mathbf{g}_j\}_j}$

$b \xleftarrow{\$} \{0,1\}$

$\xleftarrow{b}$

Open c

$\mathcal{P}((\mathbf{a},\mathbf{b}),\mathbf{c}; m, r, \mathbf{e})$ $\qquad\qquad$ $\mathcal{V}((\mathbf{a},\mathbf{b}),\mathbf{c})$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu, \rho \xleftarrow{\$} R_q$$

$$(c_1, d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2, d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{\quad c_1, c_2 \quad}$$

$$\alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\xleftarrow{\quad \alpha \quad}$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha \mathbf{e}_j) \qquad \xrightarrow{\quad \{\mathbf{g}_j\}_j \quad}$$

$$b \xleftarrow{\$} \{0, 1\}$$

$$\xleftarrow{\quad b \quad}$$

Open c

$$\mathcal{P}\left((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e}\right) \qquad \mathcal{V}\left((\mathbf{a},\mathbf{b}),\mathbf{c}\right)$$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu,\rho \xleftarrow{\$} R_q$$

$$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}'\textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{c_1,\,c_2}$$

$$\xleftarrow{\alpha} \qquad \alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j) \qquad \xrightarrow{\{\mathbf{g}_j\}_j}$$

$$b \xleftarrow{\$} \{0,1\}$$

$$\xleftarrow{b}$$

Open c

$$\mathcal{P}\left((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e}\right) \qquad\qquad \mathcal{V}\left((\mathbf{a},\mathbf{b}),\mathbf{c}\right)$$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu,\rho \xleftarrow{\$} R_q$$

$$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{l}' \textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{\quad c_1,\, c_2 \quad}$$

$$\xleftarrow{\quad \alpha \quad} \qquad \alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j) \qquad \xrightarrow{\quad \{\mathbf{g}_j\}_j \quad}$$

$$\xleftarrow{\quad b \quad} \qquad b \xleftarrow{\$} \{0,1\}$$

Open c

$$\mathcal{P}\left((\mathbf{a},\mathbf{b}),\mathbf{c};m,r,\mathbf{e}\right) \qquad\qquad \mathcal{V}\left((\mathbf{a},\mathbf{b}),\mathbf{c}\right)$$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu,\rho \xleftarrow{\$} R_q$$

$$(c_1,d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}'\textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2,d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{\quad c_1,\,c_2 \quad}$$

$$\xleftarrow{\quad \alpha \quad} \qquad \alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha\mathbf{e}_j) \qquad \xrightarrow{\quad \{\mathbf{g}_j\}_j \quad}$$

$$\xleftarrow{\quad b=0 \quad} \qquad b \xleftarrow{\$} \{0,1\}$$

Open c_1

$$\mathcal{P}((\mathbf{a},\mathbf{b}),\mathbf{c}; m, r, \mathbf{e}) \qquad\qquad \mathcal{V}((\mathbf{a},\mathbf{b}),\mathbf{c})$$

$$\pi_j \xleftarrow{\$} \mathfrak{S}_{2nk}, \quad \mathbf{f}_j \xleftarrow{\$} \mathbb{Z}_q^{2nk}, \quad \mu, \rho \xleftarrow{\$} R_q$$

$$(c_1, d_1) = \mathrm{Com}(\{\pi_j\}_j, \mathbf{a}\mu + \mathbf{b}\rho + \phi(\mathbf{I}' \textstyle\sum_j 2^j \mathbf{f}_j))$$

$$(c_2, d_2) = \mathrm{Com}(\{\pi_j(\mathbf{f}_j)\}_j, \{\pi_j(\mathbf{e}_j)\}_j)$$

$$\xrightarrow{\quad c_1,\, c_2 \quad}$$

$$\xleftarrow{\quad \alpha \quad} \qquad \alpha \xleftarrow{\$} \mathbb{Z}_q$$

$$\mathbf{g}_j = \pi_j(\mathbf{f}_j + \alpha \mathbf{e}_j) \qquad \xrightarrow{\quad \{\mathbf{g}_j\}_j \quad}$$

$$\xleftarrow{\quad b = 1 \quad} \qquad b \xleftarrow{\$} \{0,1\}$$

Open c_2

Linear Relation

$$\text{ZK-proof}\left[m_i, r_i, \mathbf{e}_i \;\middle|\; \begin{array}{c} \mathbf{c}_i = \mathbf{a}m_i + \mathbf{b}r_i + \mathbf{e}_i \\ \|\mathbf{e}_i\| \leq 2^{\kappa}, \quad m_3 = \lambda_1 m_1 + \lambda_2 m_2 \end{array} \right]$$

$$\mu_3 = \lambda_1 \mu_1 + \lambda_2 \mu_2$$

Linear Relation

$$\text{ZK-proof}\left[\, m_i, r_i, \mathbf{e}_i \;\middle|\; \begin{array}{c} \mathbf{c}_i = \mathbf{a} m_i + \mathbf{b} r_i + \mathbf{e}_i \\ \|\mathbf{e}_i\| \leq 2^{\kappa}, \quad m_3 = \lambda_1 m_1 + \lambda_2 m_2 \end{array} \right]$$

$$\mu_3 = \lambda_1 \mu_1 + \lambda_2 \mu_2$$

Multiplicative Relation

$$\text{ZK-proof}\left[m_i, r_i, \mathbf{e}_i \;\middle|\; \begin{array}{c} \mathbf{c}_i = \mathbf{a}m_i + \mathbf{b}r_i + \mathbf{e}_i \\ \|\mathbf{e}_i\| \leq 2^{\kappa}, \quad m_3 = m_1 m_2 \end{array} \right]$$

$$(m_1 + \mu_1)(m_2 + \mu_2) = m_3 + (\mu_1 m_2 + \mu_2 m_1) + \mu_1\mu_2$$

$$m_\times = \mu_1\mu_2, \quad m_+ = \mu_1 m_2 + \mu_2 m_1$$

Multiplicative Relation

$$\text{ZK-proof}\left[m_i, r_i, \mathbf{e}_i \;\middle|\; \begin{array}{c} \mathbf{c}_i = \mathbf{a}m_i + \mathbf{b}r_i + \mathbf{e}_i \\ \|\mathbf{e}_i\| \leq 2^\kappa, \quad m_3 = m_1 m_2 \end{array} \right]$$

$$(m_1 + \mu_1)(m_2 + \mu_2) = m_3 + (\mu_1 m_2 + \mu_2 m_1) + \mu_1 \mu_2$$

$$m_\times = \mu_1 \mu_2, \quad m_+ = \mu_1 m_2 + \mu_2 m_1$$

Multiplicative Relation

$$\text{ZK-proof}\left[\, m_i, r_i, \mathbf{e}_i \;\middle|\; \begin{array}{c} \mathbf{c}_i = \mathbf{a}m_i + \mathbf{b}r_i + \mathbf{e}_i \\ \|\mathbf{e}_i\| \leq 2^{\kappa}, \quad m_3 = m_1 m_2 \end{array} \right]$$

$$(m_1 + \mu_1)(m_2 + \mu_2) = m_3 + (\mu_1 m_2 + \mu_2 m_1) + \mu_1 \mu_2$$

$$m_\times = \mu_1 \mu_2, \quad m_+ = \mu_1 m_2 + \mu_2 m_1$$

Multiplicative Relation

$$\text{ZK-proof}\left[\, m_i, r_i, \mathbf{e}_i \;\middle|\; \begin{array}{c} \mathbf{c}_i = \mathbf{a}m_i + \mathbf{b}r_i + \mathbf{e}_i \\ \|\mathbf{e}_i\| \leq 2^{\kappa}, \quad m_3 = m_1 m_2 \end{array} \right]$$

$$(m_1 + \mu_1)(m_2 + \mu_2) = m_3 + (\mu_1 m_2 + \mu_2 m_1) + \mu_1\mu_2$$

$$m_\times = \mu_1\mu_2, \quad m_+ = \mu_1 m_2 + \mu_2 m_1$$

$$\pi_{i0}, \ldots, \pi_{i(\kappa-1)} \xleftarrow{\$} \mathfrak{S}_{2nk}$$

$$\mathbf{f}_{i0}, \ldots, \mathbf{f}_{i(\kappa-1)} \xleftarrow{\$} \mathbb{Z}_q^{2nk}$$

$$\mu_i, \mu_\times, \mu_+, \rho_i \xleftarrow{\$} R_q$$

$$(c_1, d_1) = \mathsf{Com}\big(\{\pi_{ij}\}_{i,j}, \{\mathbf{a}\mu_i + \mathbf{b}\rho_i + \phi(\mathbf{l}' \textstyle\sum_j 2^j \mathbf{f}_{ij})\}_i\big)$$
$$(c_2, d_2) = \mathsf{Com}\big(\mu_3, \mu_\times, \mu_+\big)$$
$$(c_3, d_3) = \mathsf{Com}\big(\{\pi_{ij}(\mathbf{f}_{ij})\}_{i,j}, \{\pi_{ij}(\mathbf{e}_{ij})\}_{i,j}\big)$$
$$(c_4, d_4) = \mathsf{Com}\big(\mu_\times + m_\times, \mu_+ + m_+\big)$$

$$\begin{pmatrix} \alpha^2(\widetilde{\mu}_3 - \overline{\mu}_3 + \beta(\overline{m}_1\overline{m}_2 - \overline{m}_3)) \\ + \alpha(\beta(\overline{\mu}_1\overline{m}_2 + \overline{\mu}_2\overline{m}_1 - \widetilde{m}_+)) \\ + (\beta(\overline{\mu}_1\overline{\mu}_2 - \widetilde{m}_\times)) \end{pmatrix} = 0$$

Multiplicative Relation

$$\begin{pmatrix} \alpha^2(\widetilde{\mu}_3 - \overline{\mu}_3 + \beta(\overline{m}_1\overline{m}_2 - \overline{m}_3)) \\ + \alpha(\beta(\overline{\mu}_1\overline{m}_2 + \overline{\mu}_2\overline{m}_1 - \widetilde{m}_+)) \\ + (\beta(\overline{\mu}_1\overline{\mu}_2 - \widetilde{m}_\times)) \end{pmatrix} = 0$$

$$\begin{pmatrix} \alpha^2(\widetilde{\mu}_3 - \overline{\mu}_3 + \beta(\overline{m}_1\overline{m}_2 - \overline{m}_3)) \\ + \alpha(\beta(\overline{\mu}_1\overline{m}_2 + \overline{\mu}_2\overline{m}_1 - \widetilde{m}_+)) \\ + (\beta(\overline{\mu}_1\overline{\mu}_2 - \widetilde{m}_\times)) \end{pmatrix} = 0$$

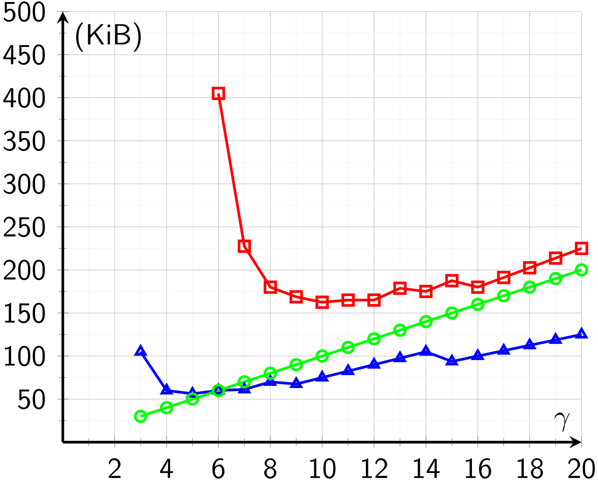
$$\begin{pmatrix} \alpha^2(\widetilde{\mu}_3 - \overline{\mu}_3 + \beta(\overline{m}_1\overline{m}_2 - \overline{m}_3)) \\ + \alpha(\beta(\overline{\mu}_1\overline{m}_2 + \overline{\mu}_2\overline{m}_1 - \widetilde{m}_+)) \\ + (\beta(\overline{\mu}_1\overline{\mu}_2 - \widetilde{m}_\times)) \end{pmatrix} = 0$$

$$\begin{pmatrix} \alpha^2(\widetilde{\mu}_3 - \overline{\mu}_3 + \beta(\overline{m}_1\overline{m}_2 - \overline{m}_3)) \\ + \alpha(\beta(\overline{\mu}_1\overline{m}_2 + \overline{\mu}_2\overline{m}_1 - \widetilde{m}_+)) \\ + (\beta(\overline{\mu}_1\overline{\mu}_2 - \widetilde{m}_\times)) \end{pmatrix} = 0$$

Comparison with other methods

- *Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise*
  [JKPT12]
  Only 0 and 1, code-based, $2/3$ soundness error.
- *Zero-Knowledge Proofs from Ring-LWE*
  [XXW13]
  $2/3$ soundness error and size proportional to $(\log q)^2$.

Figure: Commitment's size of Xie *et al.* (—○—), Benhamouda *et al.* (—□—) and our proposal (—△—)



RLWE-based Zero-Knowledge Proofs for linear and multiplicative relations

Ramiro Martínez Paz Morillo

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

17th IMA International Conference on Cryptography and Coding