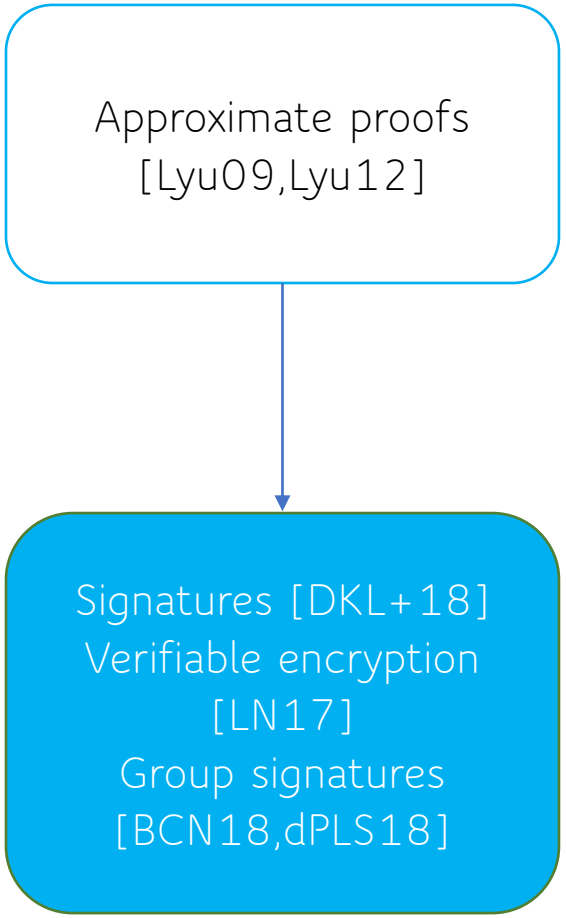
BLOOM: Bimodal Lattice One-Out-of-Many Proofs and Applications

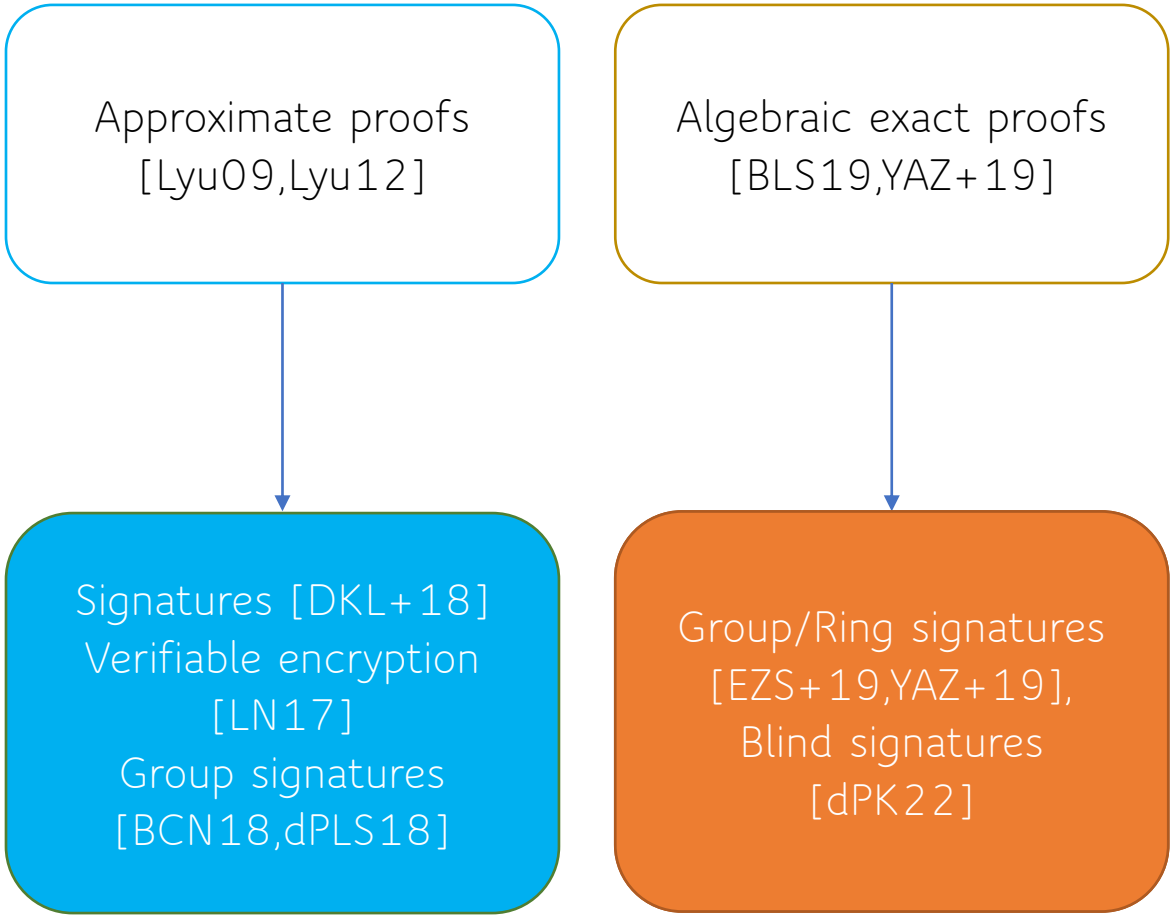
Vadim Lyubashevsky
IBM Research Europe-Zurich

Ngoc Khanh Nguyen
EPFL

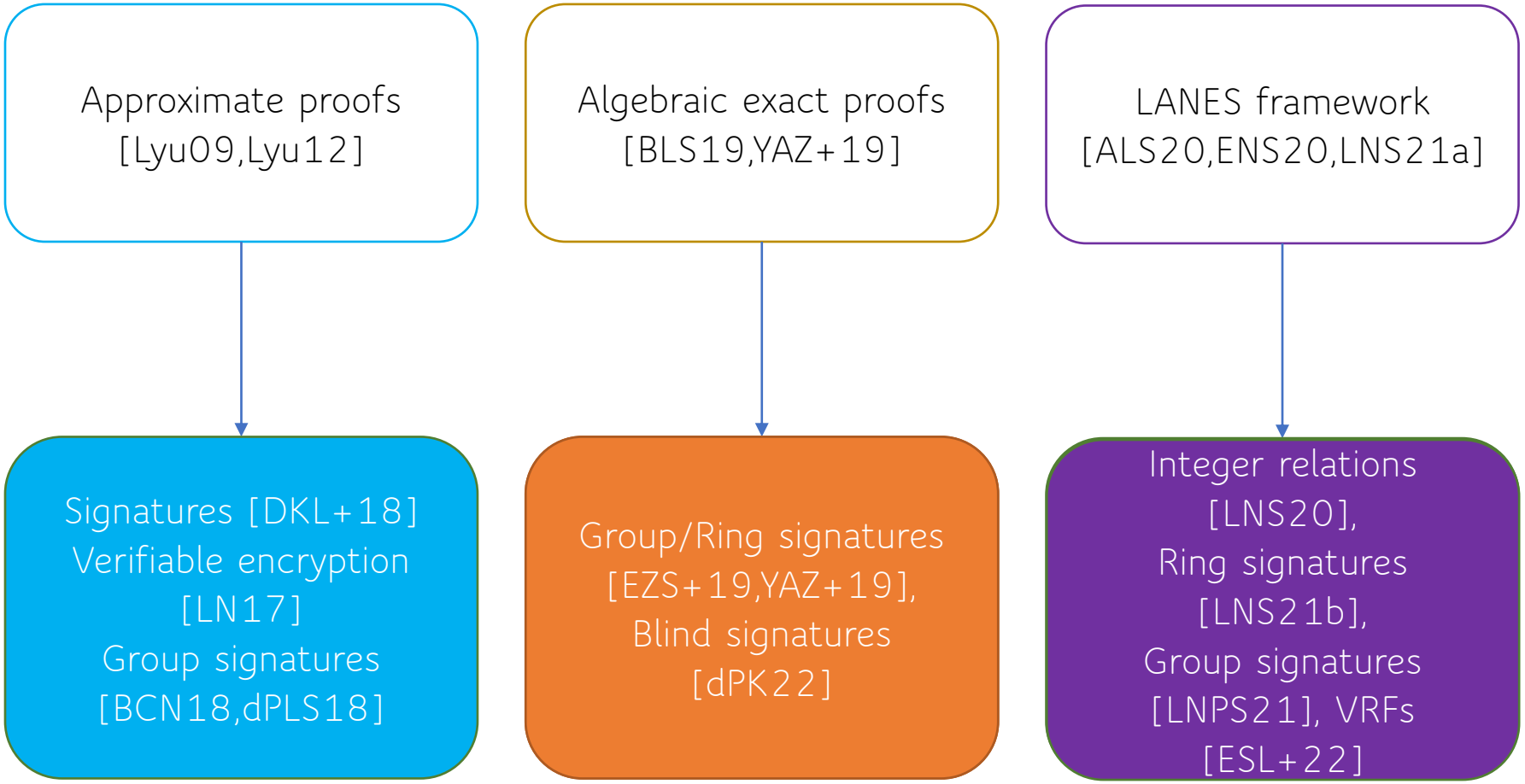
Lattice-based Zero-Knowledge Proofs and Applications



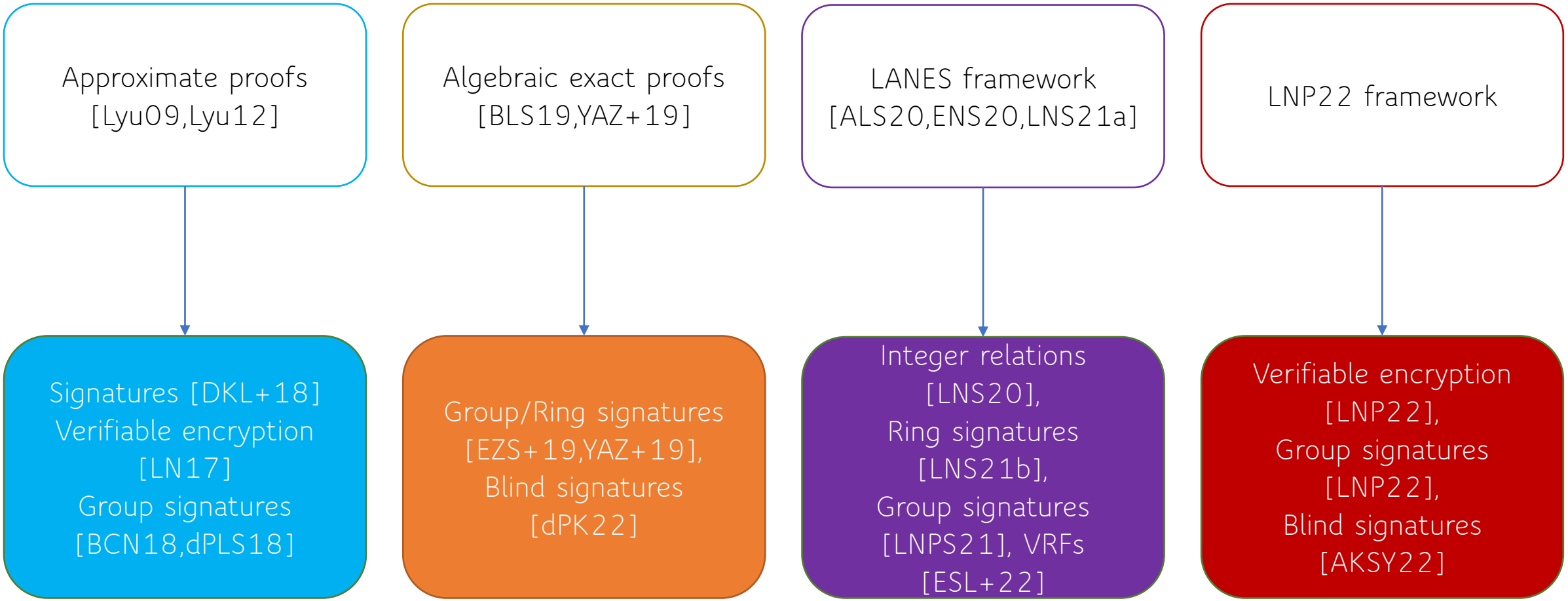
Lattice-based Zero-Knowledge Proofs and Applications



Lattice-based Zero-Knowledge Proofs and Applications



Lattice-based Zero-Knowledge Proofs and Applications



Our contributions

- Efficient one-out-of-many proofs from LNP22
- Optimized proofs of integer relations (addition, multiplication)
- Improving the LNP22 framework using bimodal Gaussians (around 15% gain)

Our contributions

- Efficient one-out-of-many proofs from LNP22
- Optimized proofs of integer relations (addition, multiplication)
- Improving the LNP22 framework using bimodal Gaussians (around 15% gain)
- (Actually useful in real life?) We made a music video

Our contributions

- **Efficient one-out-of-many proofs from LNP22**

- Optimized proofs of integer relations (addition, multiplication)
- Improving the LNP22 framework using bimodal Gaussians (around 15% gain)
- (Actually useful in real life?) We made a music video

Preliminaries

- $R_q = \mathbb{Z}_q[X]/(X^d + 1)$
- Let σ be the automorphism of R_q which maps $X \mapsto X^{-1}$
- For fixed number of variables k, we define the **quadratic-automorphic** (QA) polynomial $P: R_q^k \to R_q$ to be a function for which there exists a $2k$-variate quadratic polynomial T such that

$$P(m_1, \ldots, m_k) = T\big(m_1, \sigma(m_1), \ldots, m_k, \sigma(m_k)\big).$$

Examples: $m_1 m_2 - \sigma(m_3)$ or $m_1 \sigma(m_1) - X^{\frac{d}{2}} + 2$

LNP22 Framework (simplified)

$R_q = \mathbb{Z}_q[X]/(X^d + 1)$

Prove knowledge of short polynomials $m_1, \ldots, m_k$ in R_q which satisfy relations:

- For public QA polynomials $P_1, \ldots, P_l$: $P_i(m_1, \ldots, m_k) = 0$ over R_q

- For public QA polynomials $P'_1, \ldots, P'_n$: the constant coefficient of $P_i'(m_1, \ldots, m_k)$ is equal to 0

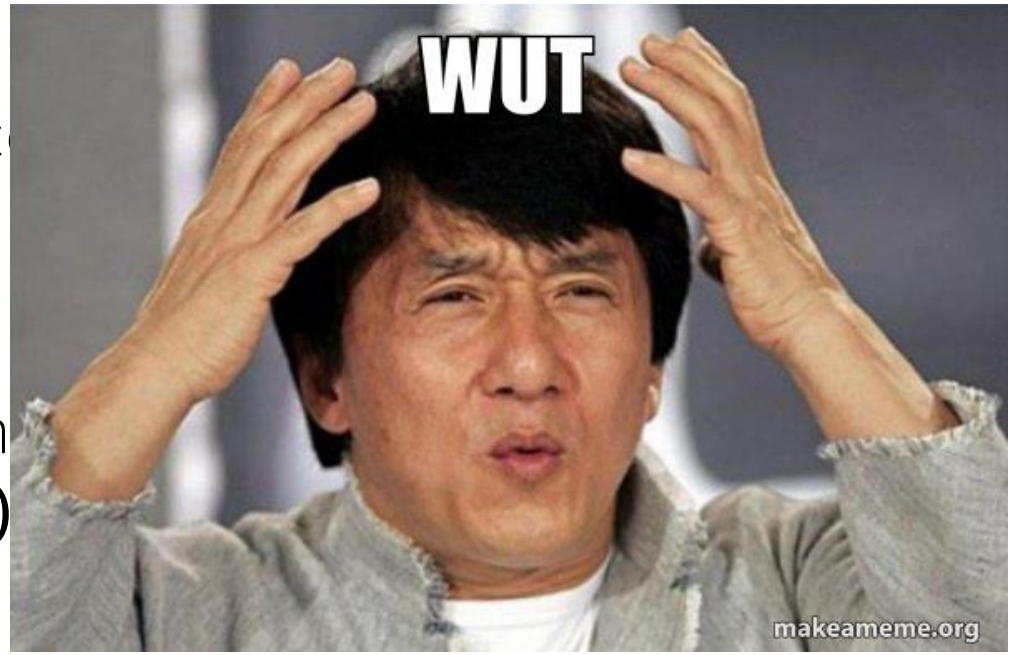
- Various norm bounds: for public linear functions $Q_1, \ldots, Q_t$: $||Q_i(m_1, \ldots, m_k)|| \leq B_i$ or $Q_i(m_1, \ldots, m_k) \in \{0,1\}^d$

LNP22 Framework (simplified)

$R_q = \mathbb{Z}_q[X]/(X^d + 1)$

Prove knowledge of short polynomials $m_1, \ldots, m_k$ in R_q which satisfy relations:

- For public QA polynomials $P_1, \ldots, P_l$: $P_i(m_1, \ldots, m_k) = 0$ over R_q
- For public QA polynomials $P'_1, \ldots, P'_n$: the c
  $P_i'(m_1, \ldots, m_k)$ is equal to 0
- Various norm bounds: for public linear fun
  $||Q_i(m_1, \ldots, m_k)|| \leq B_i$ or $Q_i(m_1, \ldots, m_k)$



Why do we need QA?

It is needed when one wants to prove basic relations over integers or over $\mathbb{Z}_q$.

Proving binary:

Suppose you want to prove that a polynomial $m \in R_q$ has binary coefficients.

Note that this is the case if and only if $\langle \vec{m}, \vec{m} - \vec{1} \rangle = 0$ over integers!

Then, to prove this inner product we use the following observation:

Lemma: For any $x, y \in R_q^n$, the constant coefficient of $x^T \sigma(y)$ is equal to $\langle \vec{x}, \vec{y} \rangle$

So we need to prove that the QA polynomial $P'(m)$ has constant coefficient equal to 0, where $P'(m) = m \cdot \sigma(m - \sum_{i=0}^{d-1} X^i)$.

Why do we need QA?

It is needed when one wants to prove basic relations over integers or over $\mathbb{Z}_q$.

<u>Proving binary:</u>

Suppose you want to prove that a poly

Note that this is the case if and only

Then, to prove this inner product w

Lemma: For any $x, y \in R_q^n$, the

LNP22 Framework (simplified)

$R_q = \mathbb{Z}_q[X]/(X^d + 1)$

Prove knowledge of short polynomials $m_1, \ldots, m_k$ *in* R_q *which satisfy relations:*

- *For public QA polynomials* $P_1, \ldots, P_l$: $P_i(m_1, \ldots, m_k) = 0$ *over* R_q
- *For public QA polynomials* $P'_1, \ldots, P'_n$: *the constant coefficient of* $P'(m_1, \ldots, m_k)$ *is equal to* 0
- *Various norm bounds: for public linear functions* $Q_1, \ldots, Q_t$: $||Q_i(m_1, \ldots, m_k)|| \leq \beta_i$ *or* $Q_i(m_1, \ldots, m_k) \in \{0,1\}^d$

So we need to prove that the QA polynomial $P'(m)$ has constant coefficient equal to 0, where $P'(m) = m \cdot \sigma(m - \sum_{i=0}^{d-1} X^i)$.

Why do we need QA?

It is needed when one wants to prove basic relations over integers or over $\mathbb{Z}_q$.

Proving linear:

Suppose you want to prove that $\langle \vec{a}, \vec{m} \rangle = u \ (mod\ q)$ for public $\vec{a}$ and u. Then, just prove that the constant coefficient of $\sigma(a)m - u$ is equal to zero.

Lemma: For any $x, y \in R_q^n$, the constant coefficient of $x^T \sigma(y)$ is equal to $\langle \vec{x}, \vec{y} \rangle$

One-out-of-many proofs [GK15]

- Suppose we have N public values $\vec{t}_1, \ldots, \vec{t}_N$ where $N = \beta^l$
- We want to prove that we know the opening $(\vec{m}, \vec{r})$ such that there exists some index i such that $Com(\vec{m}; \vec{r}) = t_i$
- We want the proof to be zero-knowledge

Technical Overview ([GK15,EZS+19,LNS21])

- *Put the members in the matrix, call it* $U = [\vec{t}_1 \ \vec{t}_2 \ \vec{t}_3 \ \dots \ \vec{t}_N]$
- *Multiply by the selector, name it* $\vec{v} = (0,0,\dots,0,1,0,\dots 0)$

- *That's a linear equation, it's easy to see*

In the i-th position

$$Com(\vec{m},\vec{r}) = [\vec{t}_1 \ \vec{t}_2 \ \vec{t}_3 \ \dots \ \vec{t}_N] \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = U\vec{v}$$

Technical Overview ([GK15,EZS+19,LNS21])

- *Put the members in the matrix, call it* $U = [\vec{t}_1 \ \vec{t}_2 \ \vec{t}_3 \ \dots \ \vec{t}_N]$
- *Multiply by the selector, name it* $\vec{v} = (0,0,\dots,0,1,0,\dots 0)$

- *That's a linear equation, it's easy to see*

In the i-th position

$$A\vec{m} + B\vec{r} = Com(\vec{m},\vec{r}) = [\vec{t}_1 \ \vec{t}_2 \ \vec{t}_3 \ \dots \ \vec{t}_N] \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = U\vec{v}$$

Technical Overview ([GK15,EZS+19,LNS21])

- *We don't want to commit to it, that's linear size:* $\vec{v} \in \{0,1\}^N$ *(*$N = \beta^l$*)*
  so we tensor decompose into small v_i*'s:*

$$\vec{v} = \vec{v}_1 \otimes \cdots \otimes \vec{v}_l \text{ where each } \vec{v}_i \in \{0,1\}^\beta \text{ with one } 1\text{-entry.}$$

Example : $\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Technical Overview

We want to prove that (simplified)

$$A\vec{s} = U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l)$$

Technical Overview

We want to prove that (simplified)

$$A\vec{s} = U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l)$$

To this end, we do the folklore random linear combination trick:

$$\begin{aligned} 0 &= \left\langle U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), \vec{\phi} \right\rangle - \left\langle A\vec{s}, \vec{\phi} \right\rangle \\ &= \left\langle (\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), U^T\vec{\phi} \right\rangle - \left\langle \vec{s}, A^T\vec{\phi} \right\rangle \\ &= \langle \vec{v}_1, \overline{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \rangle - \left\langle \vec{s}, A^T\vec{\phi} \right\rangle \end{aligned}$$

where $\overline{U} \in \mathbb{Z}_q^{\beta \times \beta^{l-1}}$.

Technical Overv

We want to prove that

Lemma: Let $\vec{a} \in \mathbb{Z}^n, \vec{b} \in \mathbb{Z}^m$ and $\vec{w} = (\overrightarrow{w_1}, \ldots, \vec{w}_n) \in \mathbb{Z}^{nm}$. Then

$$\langle \vec{a} \otimes \vec{b}, \vec{w} \rangle = \langle \vec{a}, \begin{bmatrix} \vec{w}_1^T \\ \vdots \\ \vec{w}_n^T \end{bmatrix} \vec{b} \rangle$$

To this end, we do the folklore random linear combination trick:

$$\begin{aligned} 0 &= \langle U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), \vec{\phi} \rangle - \langle A\vec{s}, \vec{\phi} \rangle \\ &= \langle (\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), U^T \vec{\phi} \rangle - \langle \vec{s}, A^T \vec{\phi} \rangle \\ &= \langle \vec{v}_1, \overline{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \rangle - \langle \vec{s}, A^T \vec{\phi} \rangle \end{aligned}$$

where $\overline{U} \in \mathbb{Z}_q^{\beta \times \beta^{l-1}}$.

Technical Overview

We want to prove that (simplified)

$$A\vec{s} = U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l)$$

To this end, we do the folklore random linear combination trick:

$$\begin{aligned} 0 &= \left\langle U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), \vec{\phi} \right\rangle - \left\langle A\vec{s}, \vec{\phi} \right\rangle \\ &= \left\langle (\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), U^T\vec{\phi} \right\rangle - \left\langle \vec{s}, A^T\vec{\phi} \right\rangle \\ &= \langle \vec{v}_1, \overline{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \rangle - \left\langle \vec{s}, A^T\vec{\phi} \right\rangle \end{aligned}$$

where $\overline{U} \in \mathbb{Z}_q^{\beta \times \beta^{l-1}}$. Then commit to $\vec{x}_1 = \overline{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$ and prove:

$\rightarrow \vec{x}_1 = \overline{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$ and $\rightarrow 0 = \langle \vec{v}_1, \vec{x}_1 \rangle - \left\langle \vec{s}, A^T\vec{\phi} \right\rangle$

Technical Overview (case $\beta = d$)

$\vec{x}_1 = \overline{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$ and $\rightarrow 0 = \langle \vec{v}_1, \vec{x}_1 \rangle - \langle \vec{s}, A^T \vec{\phi} \rangle$

Technical Overview (case $\beta = d$)

$\vec{x}_1 = \bar{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$ and $\rightarrow 0 = \langle \vec{v}_1, \vec{x}_1 \rangle - \langle \vec{s}, A^T \vec{\phi} \rangle$

Equivalent to proving that the constant coefficient of $\sigma(v_1)x_1 - \sigma(A^T \vec{\phi})^T s$ is equal to zero.

Technical Overview (case $\beta = d$)

$\vec{x}_1 = \bar{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$ and $\rightarrow 0 = \langle \vec{v}_1, \vec{x}_1 \rangle - \langle \vec{s}, A^T \vec{\phi} \rangle$

Prove this statement by recursion.
One ends up committing to β vectors $\vec{x}_1, \ldots, \vec{x}_\beta \in \mathbb{Z}_q$.

Equivalent to proving that the constant coefficient of $\sigma(v_1)x_1 - \sigma\left(A^T \vec{\phi}\right)^T s$ is equal to zero.

Technical Overview (case $\beta = d$)

$\vec{x}_1 = \bar{U}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$ and $\rightarrow 0 = \langle \vec{v}_1, \vec{x}_1 \rangle -$

We still need to prove that some vectors are short/binary, but that's covered by the framework

Prove this statement by recursion.
One ends up committing to β vectors $\vec{x}_1, \ldots, \vec{x}_\beta \in \mathbb{Z}_q$.

Equivalent to proving that the constant coefficient of $\sigma(v_1)x_1 - \sigma\left(A^T\vec{\phi}\right)^T s$ is equal to zero.

Soundness error?

If the statement is not true then

$$0 = \left\langle U(\vec{v}_1 \otimes \cdots \otimes \vec{v}_l), \vec{\phi} \right\rangle - \left\langle A\vec{s}, \vec{\phi} \right\rangle$$

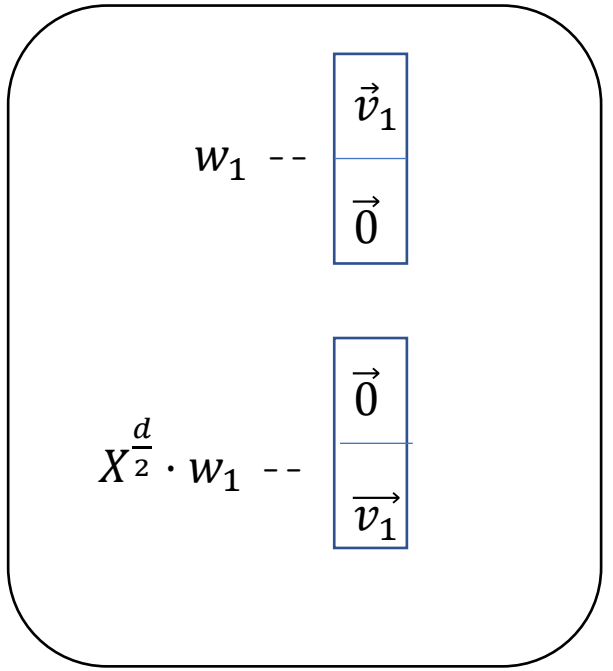
With probability at most $\frac{1}{q}$. What if this is not negligible?

For instance, $q \approx 2^{64}$ then naively we would repeat the protocol twice.

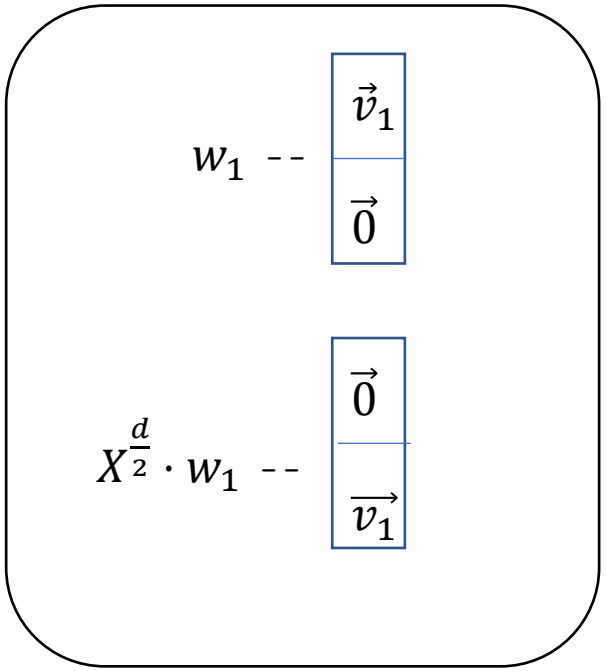
Achieving one-shot property

- Consider $\beta = \frac{d}{2}$ and commit to polynomials $w_i \in R_q$ such that

$$\vec{w_i} = (\vec{v_i}, \vec{0}), \text{ i.e. } w_i = \sum_{j=1}^{\beta} v_{i,j} X^{j-1} \in R_q.$$



Achieving one-shot property



- Consider $\beta = \frac{d}{2}$ and commit to polynomials $w_i \in R_q$ such that

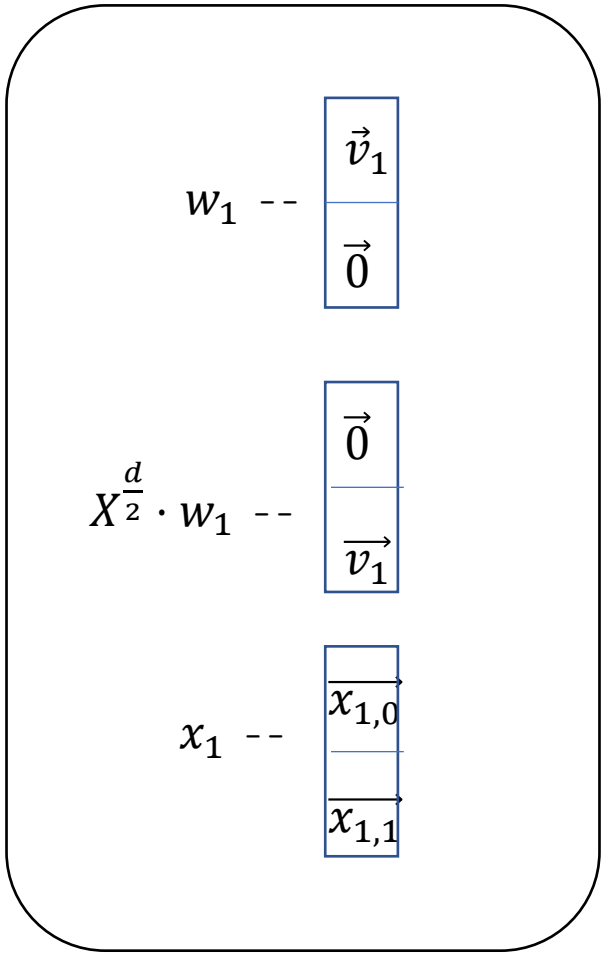
$$\vec{w}_i = (\vec{v}_i, \vec{0}), \text{ i.e. } w_i = \sum_{j=1}^{\beta} v_{i,j} X^{j-1} \in R_q.$$

- Run the proof with random $\vec{\phi}_0$ and $\vec{\phi}_1$:

$$\begin{cases} \vec{x}_{1,0} = \overline{U_0}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ 0 = \langle \vec{v}_1, \vec{x}_{1,0} \rangle - \langle \vec{s}, A^T \overrightarrow{\phi_0} \rangle \end{cases} \qquad \begin{cases} \vec{x}_{1,1} = \overline{U_1}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ 0 = \langle \vec{v}_1, \vec{x}_{1,1} \rangle - \langle \vec{s}, A^T \overrightarrow{\phi_1} \rangle \end{cases}$$

and commit to $\vec{x}_1 := (\vec{x}_{1,0}, \vec{x}_{1,1}) \in \mathbb{Z}^d$.

Achieving one-shot property



- Consider $\beta = \frac{d}{2}$ and commit to polynomials $w_i \in R_q$ such that

$$\vec{w}_i = (\vec{v}_i, \vec{0}), \text{ i.e. } w_i = \sum_{j=1}^{\beta} v_{i,j} X^{j-1} \in R_q.$$

- Run the proof with random $\vec{\phi}_0$ and $\vec{\phi}_1$:

$$\begin{cases} \vec{x}_{1,0} = \overline{U_0}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ 0 = \langle \vec{v}_1, \vec{x}_{1,0} \rangle - \langle \vec{s}, A^T \overrightarrow{\phi_0} \rangle \end{cases} \qquad \begin{cases} \vec{x}_{1,1} = \overline{U_1}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ 0 = \langle \vec{v}_1, \vec{x}_{1,1} \rangle - \langle \vec{s}, A^T \overrightarrow{\phi_1} \rangle \end{cases}$$

and commit to $\vec{x}_1 := (\vec{x}_{1,0}, \vec{x}_{1,1}) \in \mathbb{Z}^d$.

- This is equivalent to:

→Constant coefficient of $\sigma(w_1)x_1 - \sigma(A^T\vec{\phi}_0)^T s$ and $\sigma\left(X^{\frac{d}{2}} w_1\right) x_1 - \sigma(A^T\vec{\phi}_1)^T s$ are zeroes

$$\rightarrow \overrightarrow{x_1} = \begin{bmatrix} \vec{x}_{1,0} \\ \vec{x}_{1,1} \end{bmatrix} = \begin{bmatrix} \overline{U_0}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ \overline{U_1}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \end{bmatrix} = \begin{bmatrix} \overline{U}_0 \\ \overline{U}_1 \end{bmatrix} (\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$$

Achieving one-shot property

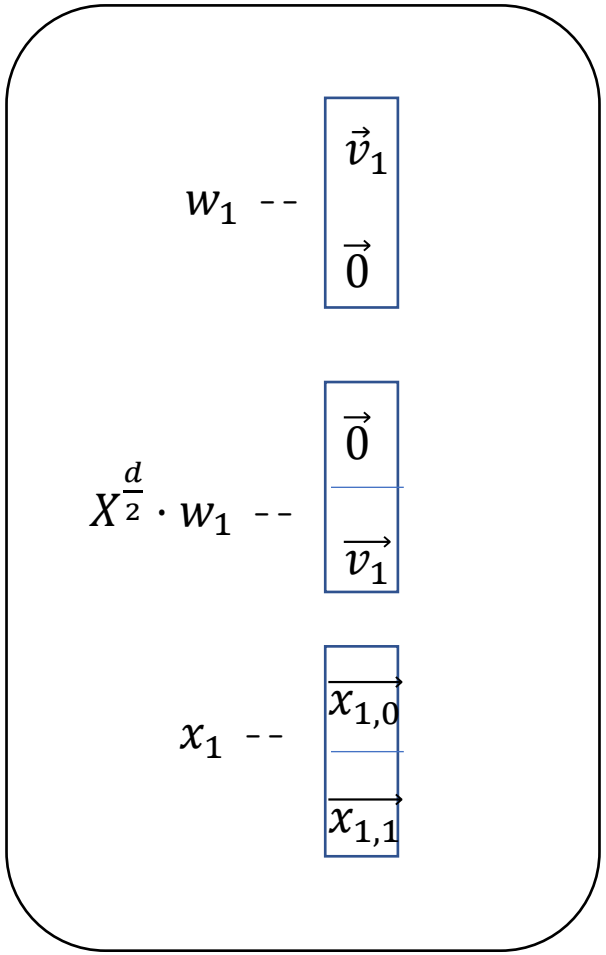
- Consider $\beta = \frac{d}{2}$ and commit to polynomials $w_i \in R_q$ such that

$$\vec{w}_i = (\vec{v}_i, \vec{0}), \text{ i.e. } w_i = \sum_{j=1}^{\beta} v_{i,j} X^{j-1} \in R_q.$$

- Run the proof with random $\vec{\phi}_0$ and $\vec{\phi}_1$:

$$\begin{cases} \vec{x}_{1,0} = \overline{U_0}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ 0 = \langle \vec{v}_1, \vec{x}_{1,0} \rangle - \langle \vec{s}, A^T \overrightarrow{\phi_0} \rangle \end{cases} \qquad \begin{cases} \vec{x}_{1,1} = \overline{U_1}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ 0 = \langle \vec{v}_1, \vec{x}_{1,1} \rangle - \langle \vec{s}, A^T \overrightarrow{\phi_1} \rangle \end{cases}$$

and commit to $\vec{x}_1 := (\vec{x}_{1,0}, \vec{x}_{1,1}) \in \mathbb{Z}^d$.



- This is equivalent to:

→Constant coefficient of $\sigma(w_1)x_1 - \sigma\left(A^T\vec{\phi}_0\right)^T s$ and $\sigma\left(X^{\frac{d}{2}}w_1\right)x_1 - \sigma\left(A^T\vec{\phi}_1\right)^T s$ are zeroes

$$\rightarrow \overrightarrow{x_1} = \begin{bmatrix} \vec{x}_{1,0} \\ \vec{x}_{1,1} \end{bmatrix} = \begin{bmatrix} \overline{U_0}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \\ \overline{U_1}(\vec{v}_2 \otimes \cdots \otimes \vec{v}_l) \end{bmatrix} = \begin{bmatrix} \overline{U}_0 \\ \overline{U}_1 \end{bmatrix} (\vec{v}_2 \otimes \cdots \otimes \vec{v}_l)$$

→ Continue with recursion

Ring Signatures

	sig. sizes for N: 2^6	2^{12}	2^{21}	asymptotic sig. size	hardness assumption	(user) public key size
Raptor [LAZ19]	81	5161	–	$O(N)$	NTRU	0.9
DualRing-LB [YEL+21]	6	106	–	$O(N)$	MSIS, MLWE	$[2.8, 3.4]$
Falafl [BKP20]	32	35	39	$O(\log N)$	MSIS, MLWE	1.9
MatRiCT [EZS+19]	31	59	148	$O(\log^{1.7} N)$	MSIS, MLWE	$[3.4, 22.7]$
MatRiCT+ [ESZ21]	11	18	40(?)	$O(\log^{1.7} N)$	MSIS, MLWE	3
SMILE [LNS21b]	18	19	22	$O(\log N)$	MSIS, E-MLWE	2
Calamari [BKP20]	8	14	23	$O(\log N)$	CSIDH-512	0.06
This Work	**13**	**14**	**16**	$O(\log N)$	**MSIS, E-MLWE**	**0.13**

Proving integer relations

Addition

N	128	512
[LNS20]	25KB	45KB
This Work	12KB	14KB

Multiplication

N	128	512
[LNS20]	40KB	100KB
This Work	15KB	19KB

Thank you!