Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications

Muhammed F. Esgin, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu

Monash University and Data61, CSIRO

Faculty of IT

Monash University

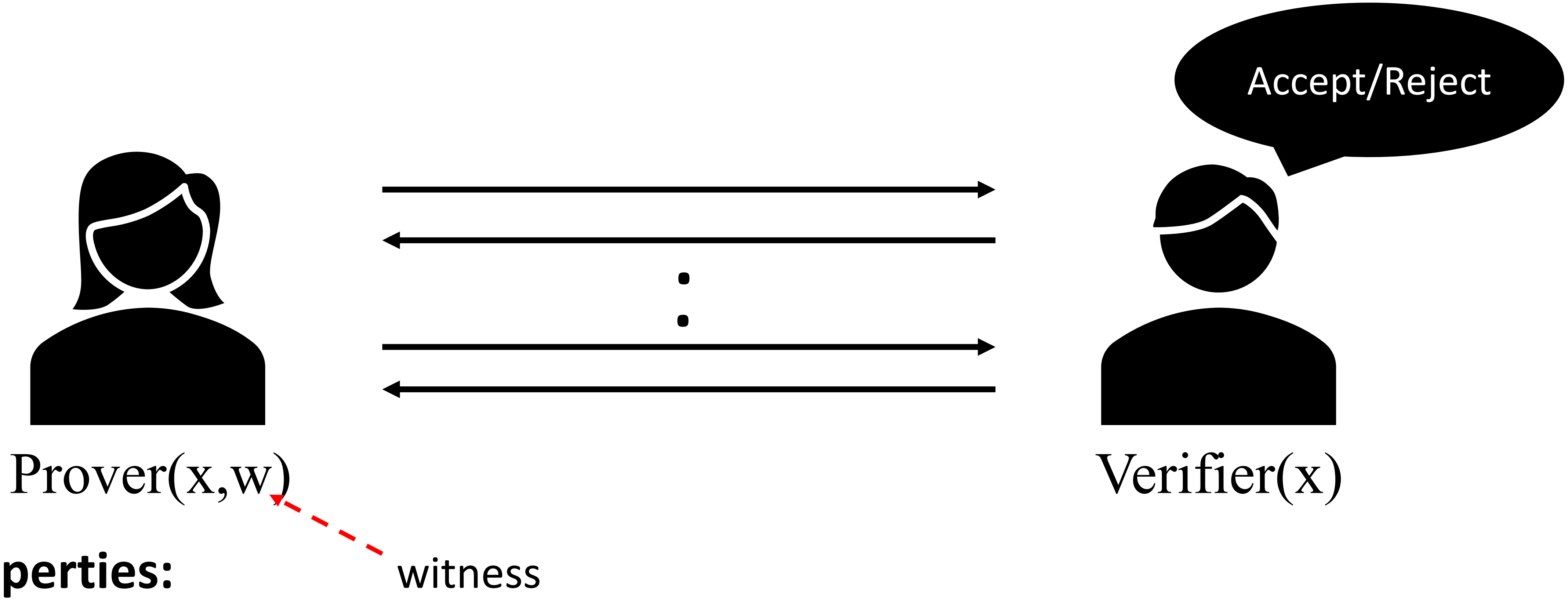
Acknowledgement: Some Slides courtesy of Muhammed. F. Esgin.

Outline

- **Background:** Efficient Zero-Knowledge Proofs (ZKPs) for linear relations
  - Schnorr proof ZKP of knowledge of discrete-log
  - Lattice analogue of DL: Module-RingSIS / Module-RingLWE
  - Difficulties and solutions in porting DL-based to lattice-based proof
  - Lyubahsevky proof of knowledge of Module-Ring-LWE witness [Lyu12]

- **Our new techniques:** Efficient Lattice-based ZKPs for `non-linear' relations of degree k > 1
  - Framework for ZKPs for non-linear relation of degree k > 1
    - Issues in porting DL-based to lattice-based proofs in non-linear setting
      - Our `one-shot' (short proof) soundness analysis technique: adjugate matrices
    - Application: Commitments of Bits Proofs
      - Speed-up technique 1: Extraction with large challenges and NTT-friendly rings
    - Application: One-of-Many Proofs
    - Application: anonymous authentication -- Ring Signatures
    - Application: Integer Range Proofs
      - Speed-up technique 2: CRT-packing technique supporting inter-slot operations
      - Improves run-time by packing factor s

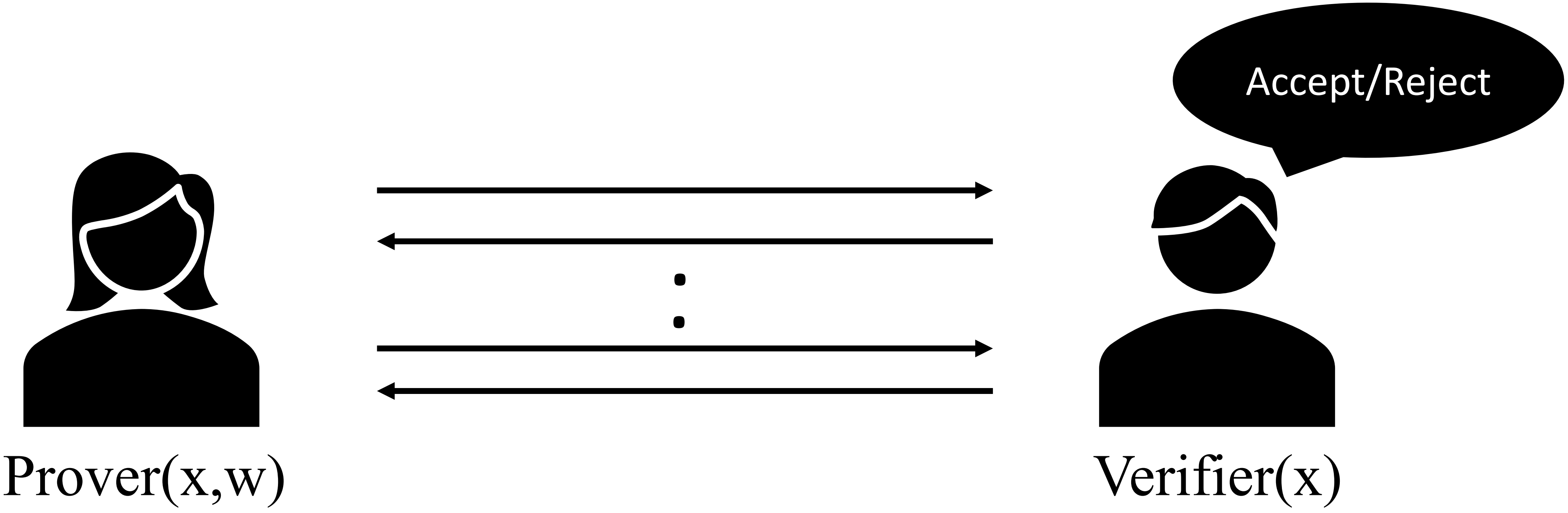
Zero-Knowledge Proofs [GMR85]



Properties:

1) Completeness
2) Soundness
3) Zero-Knowledge

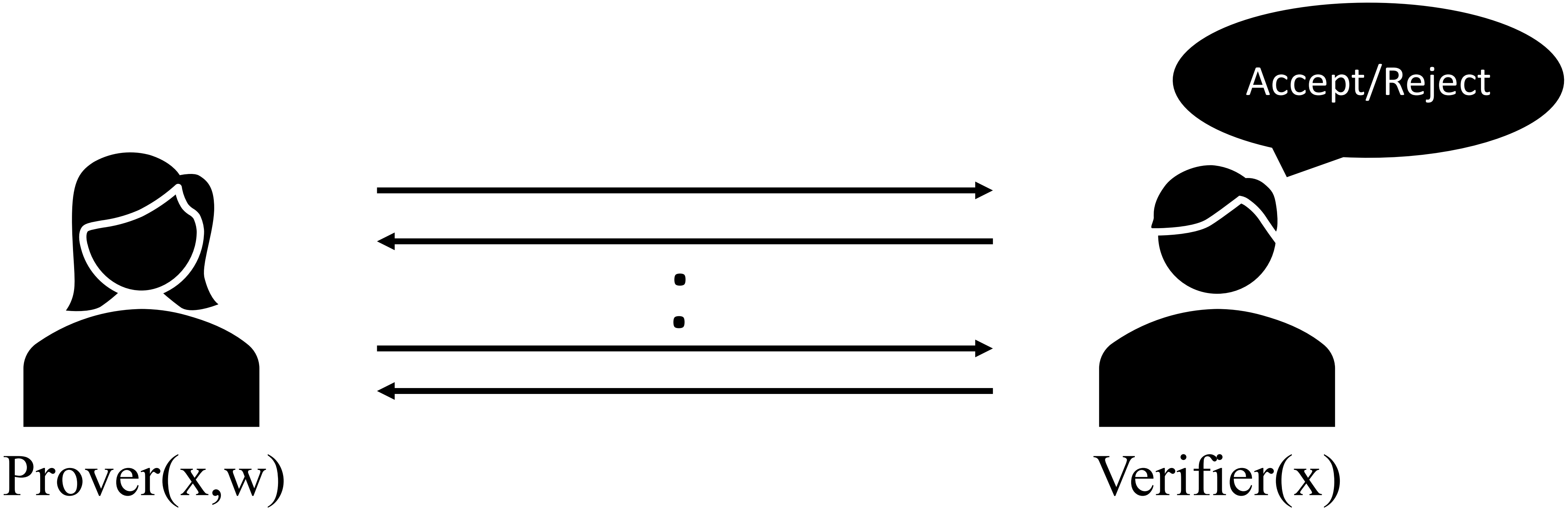
Zero-Knowledge Proofs [GMR85]



Properties:

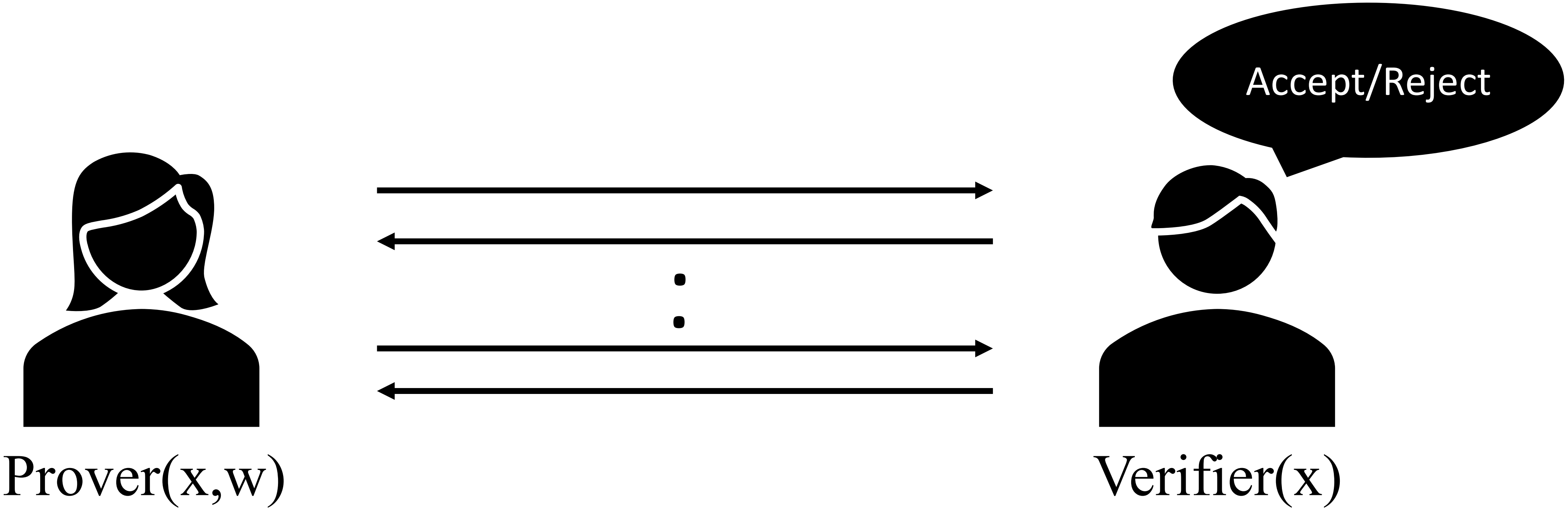
1) Completeness
2) Soundness
3) Zero-Knowledge

Zero-Knowledge Proofs [GMR85]



Properties:
1) Completeness
2) Soundness
3) Zero-Knowledge

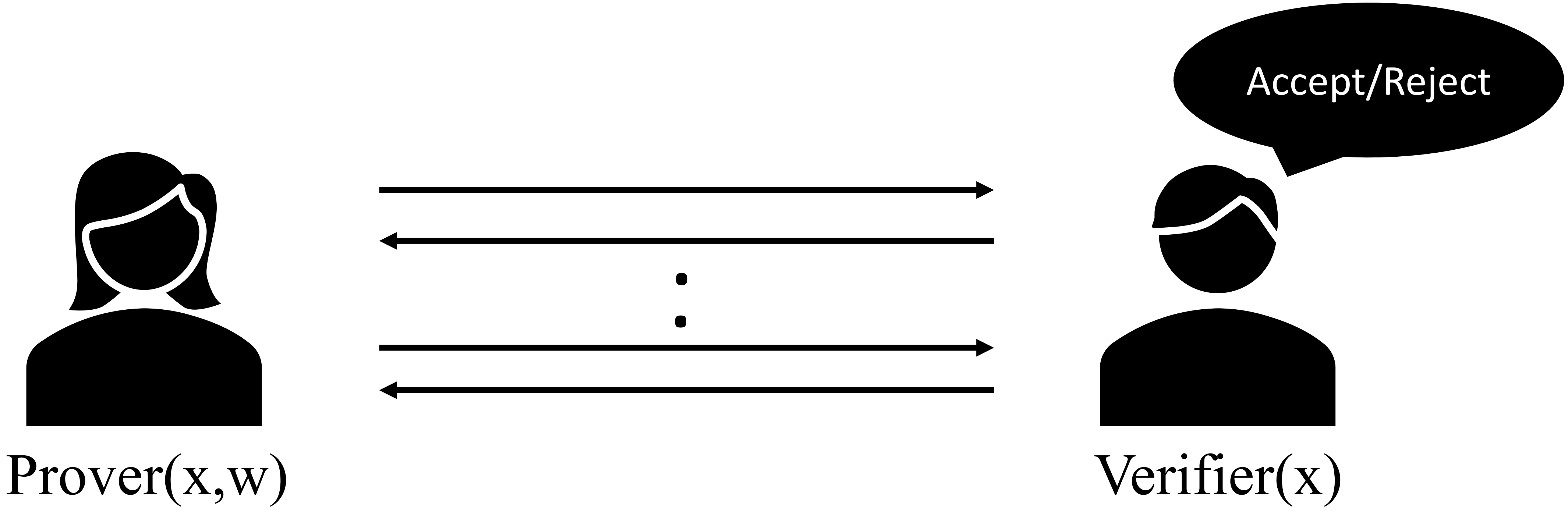
Zero-Knowledge Proofs [GMR85]



Properties:

1) Completeness
2) Soundness
3) Zero-Knowledge

Zero-Knowledge Proofs [GMR85]



Properties:

1) Completeness
2) Soundness
3) Zero-Knowledge

We work in particular with Sigma protocols.
Easily made non-interactive using Fiat-Shamir heuristic.

Background: Types of ZKPs in Lattice-Based Crypto

- Two main types of ZK Proofs investigated in lattice-based crypto:
  - "Combinatorial" type (aka `Stern-type' [St96] ZK proofs) :
    - Verifier challenge chosen from a very small set (of size typically **3**)
    - Different prover response algorithm explicitly specified for each possible challenge
    - Pro: Very powerful – can be adapted to prove complex relations (e.g. [BLNW18])
    - Con: long/slow proofs: Many protocol repeats needed for high soundness level
  - "Algebraic" type (aka `Schnorr-type' [Sch89] ZK proofs) :
    - Verifier challenge can be chosen from a huge set (of size $> 2^{\lambda}$ for security parameter λ)
    - Prover response algorithm is an algebraic function of the verifier's challenge
    - Pro: can achieve short/fast proofs: `one-shot' challenge may be possible
    - Cons:
      - More limited in types of proofs so far achievable efficiently
      - May prove "approximate" (relaxed) relations rather than exact relations

Our focus in this talk

Classical ZKP 1: Schnorr proof ZKP of knowledge of discrete-log

Setup of Schnorr's ZKP of Knowledge of Discrete Log [Sch89]:

- Works in a cyclic multiplicative group $G = \langle g \rangle = \{1, g^1, g^2, \ldots, g^{q-1}\}$
  - where Discrete-Logarithm (DL) problem is hard
- Fixed public generator $g \in G$ for G
- Denote order (size) of G by q (assumed prime).
- Prover's Discrete-Log private-key (witness): $s \leftarrow U(Z_q)$.
- Prover's public-key (common input): $h = g^s \in G$.
- Write $h = Com(s)$.
  - Com is homomorphic from Z_q to G: $Com(s + t) = Com(s) \cdot Com(t)$

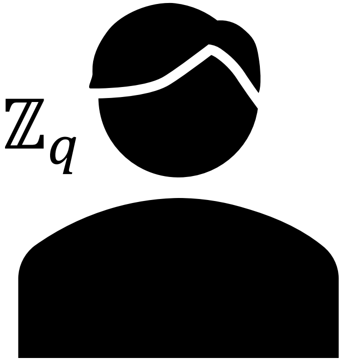
Classical ZKP 1: Schnorr proof ZKP of knowledge of discrete-log

$s \leftarrow \text{RandSet} = \mathbb{Z}_q$ $\quad u \leftarrow \mathbb{Z}_q$ $\qquad$ $A_1 = \text{Com}(s)$

$A_0 = \text{Com}(u)$ $\longrightarrow$

$x \leftarrow \text{ChallengeSet} = \mathbb{Z}_q$ $\longleftarrow$

$\boldsymbol{f} = u + x \cdot s$ $\quad \boldsymbol{f}$ $\longrightarrow$



Prover $\qquad\qquad$ Verifier

Correctness: homomorphic property of Com

Com(f) = Com(u+ x · s) = Com(u) · Com(s)^x

Soundness (2-special soundness): prover succeeds with prob > 1/|ChSet| → prover knows a **valid** opening (DL) of A_1

- Given commitment A_0, from **two** distinct successful challenge response pair pairs (x,f), (x',f'), extract witness s'

$$\boxed{A_0 \cdot A_1^x \stackrel{?}{=} \text{Com}(\boldsymbol{f})}$$

$$A_0 \cdot A_1^x = \text{Com}(\boldsymbol{f})$$
$$A_0 \cdot A_1^{x'} = \text{Com}(\boldsymbol{f}')$$
$$\Rightarrow A_1 = \text{Com}\left(\frac{f - f'}{x - x'}\right)$$

s'

Classical ZKP 1: Schnorr proof ZKP of knowledge of discrete-log

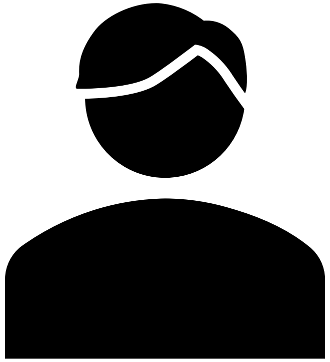
$s \leftarrow$ RSet = $\mathbb{Z}_q$

$h = \mathrm{Com}(s)$

$u \leftarrow \mathbb{Z}_n$ $\quad A_0 = \mathrm{Com}(u) \longrightarrow$

$\longleftarrow x \leftarrow$ CSet = $\mathbb{Z}_q$

$\boldsymbol{f} = u + x \cdot s \quad \boldsymbol{f} \longrightarrow$



Prover

Verifier

Honest-Verifier Zero-Knowledge (HVZK): An honest verified can efficiently simulate a proof transcript without the prover's witness!

$$\boxed{A_0 \cdot A_1^x \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f})}$$

Transcript Simulator, given A_1:

- $x \leftarrow$ CSet = $\mathbb{Z}_q$
- $f \leftarrow \mathbb{Z}_q$
- $A_0 \cdot \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f}) \cdot A_1^{-x}$

Application 1: Digital Signatures [Sch91]

- Fiat-Shamir Transformation: Generic conversion of an interactive ZK Sigma (3-move) proof to a non-interactive digital signature
  - Idea:
    - Prover uses a cryptographic one-way hash function H to generate challenge by hashing his protocol commitment A_0 and the signed message m
      - $x = H(A_0, m)$
- → Schnorr digital signature (similar to Digital Signature Standard, DSS):
    - **KG:** sk = s, $A_1 = \mathrm{Com}(s)$
    - **Sign**(s, m) = (x,f)
      - $A_0 = \mathrm{Com}(u)$
      - $x = H(A_0,m)$
      - $f = r + x \cdot s$
    - **Ver**(m,(x,f),pk):
      - $A_0 = \mathrm{Com}(\boldsymbol{f}) \cdot A_1^{-x}$
      - $x \stackrel{?}{=} H(A_0,m)$

Lattice analogue of DL Problem: Module-RingSIS / Module-RingLWE Problems

Structured lattice Setup:

- Work over a polynomial ring $R_q = \mathbb{Z}_q[x]/(x^d + 1)$ for integer q
- Fixed public uniformly random matrix $A \in {R_q}^{n \times m}$
- Conjectured-Hard Lattice problems
- Module−Ring−SIS$_{n,m,q,\beta}$ Problem:
  - Given $A \in {R_q}^{n \times m}$, find \`short' $v \in R_q^m$ ($\|v\| \leq \beta$) s.t. $A \cdot v = 0$
- Module−Ring−LWE$_{n,m,q,\alpha}$ Problem:
  - Given $A \in {R_q}^{n \times m}$, and $t = A \cdot s \in R_q^n$ for a \`short' $s \in R_q^m$ ($\|s\| \leq \alpha\, q \sqrt{m}$), find s (search-LWE) or distinguish t from uniform in R_q^n (decision-LWE)

→Typical Prover's private-key (witness): \`short' $s \leftarrow \mathrm{U}([-B, B]^{n \times m})$ = RandSet

→Typical Prover's public-key (common input): $t = A \cdot s \in R_q^n$

- Write $t = Com(s)$
  - Com is homomorphic from Dom$_s$ to R_q^n : Com(s + t) = Com(s) + Com(t)

Best known attacks take time 2^{λ} if

- $dn \geq \Omega(\lambda \cdot \frac{\log^2 \beta}{\log q})$, $\beta < q$ (SIS)
- $d(m-n) \geq \Omega(\lambda \cdot \frac{\log^2 \alpha^{-1}}{\log q})$, $\alpha^{-1} > 1$ (LWE)

→ Balanced with $m = 2n$, $\beta = \alpha^{-1}$

Hardness decreases with β → aim to minimize extracted witness norm in ZKPs!

Many SIS solutions /
Unique LWE solution with
$\mathrm{m} = 2\mathrm{n}, \beta = \alpha^{-1} \geq \sqrt{dm} \cdot q^{1/2}$

Lattice ZKP 1 Lattice-analogue of Schnorr ZKP
`Attempt 1'

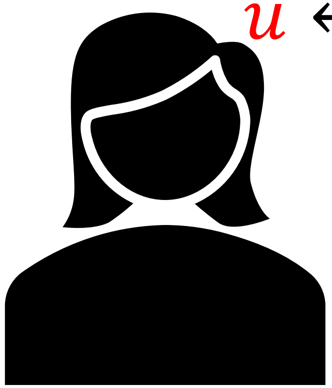
$s \leftarrow \text{SSet} = [-B, B]^{dm}$

$u \leftarrow RSet = [-B', B']^{dm}$ $A_0 = \text{Com}(u)$

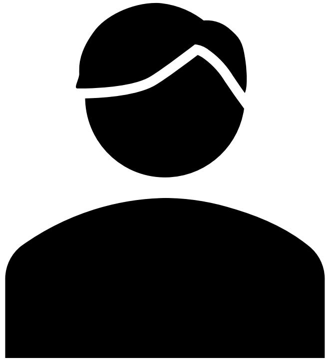
$A_1 = \text{Com}(s)$

$x \leftarrow \text{CSet} \subseteq R_q$

$\boldsymbol{f} = u + x \cdot s$ $\boldsymbol{f}$



Prover



Verifier

Correctness: homomorphic property of Com

Com(f) = Com(u+ x · s) = Com(u) · Com(s)^x

Soundness (2-special soundness): prover succeeds with prob > 1/|ChSet| → prover knows a **valid** opening of A_1

- Given commitment A_0, from **two** distinct successful challenge response pair pairs (x,f), (x',f'), extract witness s'

$A_0 + x \cdot A_1 \stackrel{?}{=} \text{Com}(\boldsymbol{f})$

$\|f\| \; ?< B' + \max_{x,s} \|x \cdot s\|_\infty$

$A_0 + x \cdot A_1 = \text{Com}(\boldsymbol{f})$

$A_0 + x' \cdot A_1 = \text{Com}(\boldsymbol{f}')$

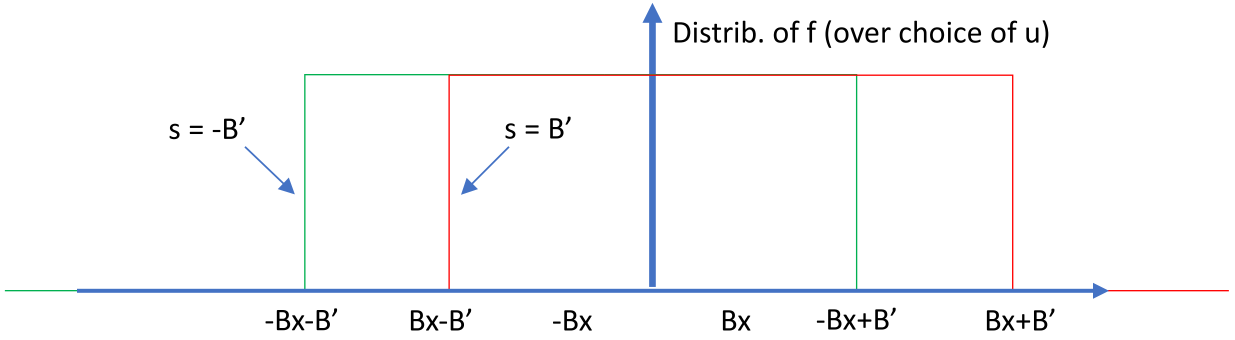
$\Rightarrow A_1 = \text{Com}\left(\frac{f - f'}{x - x'}\right)$ s'?

Difficulties & Solutions in porting DL-based to lattice-based ZK Proof

But, `Attempt 1' does not quite work…

Issues with `Attempt 1':

1. Zero-Knowledge Property is not satisfied:
   - Domain SSet and RSet for secrets s and u is `**short**' interval [-B,B] (< q)
     - Needed for hardness of the LWE/SIS lattice problems
     - Challenges x in ChallSet have to be `**short**' for same reason
   - Prover's response value $\boldsymbol{f} = u + x \cdot s$ leaks info. on secret s : $\mathbb{E}[\boldsymbol{f}] = x \cdot s$

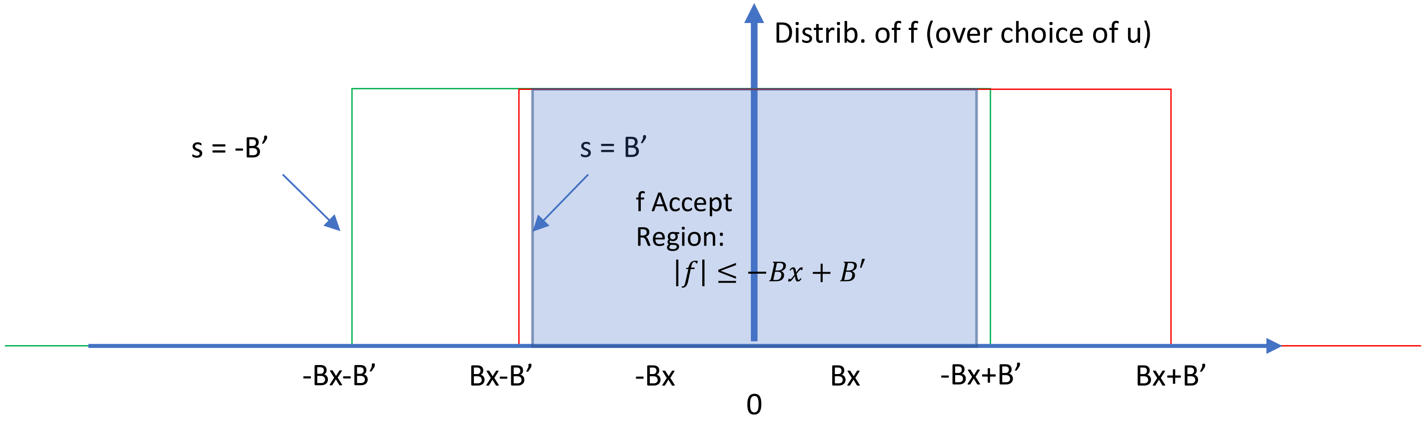


Difficulties & Solutions in porting DL-based to lattice-based ZK Proof

Main Issues with `Attempt 1':

1. Zero-Knowledge Property is not satisfied:

- Solution ([Lyu09,Lyu12]): Rejection sampling
  - Restart protocol with fresh u (and x) until f is independent of s, $\mathbb{E}[\boldsymbol{f}] = 0$



Acceptance probability
$p = (1 - \frac{|Bx|}{B'})^{md} = \Omega(1)$ if
$\frac{B'}{|Bx|} = O(md)$
Masking size linear in dimension.

Using discrete Gaussian (instead of uniform) distribution for u can reduce masking size [Lyu12].

Porting DL-based to lattice-based ZK Proof

Main Issues with `Attempt 1':

$$A_0 + x \cdot A_1 = \mathrm{Com}(\boldsymbol{f})$$
$$A_0 + x' \cdot A_1 = \mathrm{Com}(\boldsymbol{f}')$$
$$\Rightarrow A_1 = \mathrm{Com}\left(\frac{f-f'}{x-x'}\right)$$

2. Soundness Property is not satisfied

- Problem: extracted witness $s' = \frac{f-f'}{x-x'} \in R_q$
- s' may not be **`short' (<<q) → not in valid (secure) `short' Com domain**
  - **Issue:** $(x-x')^{-1}$ in R_q is usually not short in when $x-x'$ is short

- Solutions
  - Solution 1 (special challenges - efficiency compromise) [L+14,L+19]:
    - Use a special challenge space CSet $\subseteq R_q$ such that $(x-x')^{-1}$ is `short' for all x ≠ x' in CSet
    - But, largest such challenge space known is small (size 2*d* = *O*(λ))
      - *Low efficiency:* Many protocol repeats needed for high soundness level
  - Solution 2 (approximate relations – functionality compromise) [Lyu09,Lyu12]:
    - Prove knowledge of witness (c',s') to **approximate** relation $c' \cdot A_1 = \mathrm{Com}(s')$
    - c' is the `approximation' factor (must be `short' but not 1 as in exact relation)
    - ZK proof application must work securely with approximate proof

$$\Rightarrow (x - x') \cdot A_1 = \mathrm{Com}(f - f')$$

Lattice ZKP 1 Lattice-analogue of Schnorr ZKP
`Fixed Proof' idea (a-la [Lyu12])

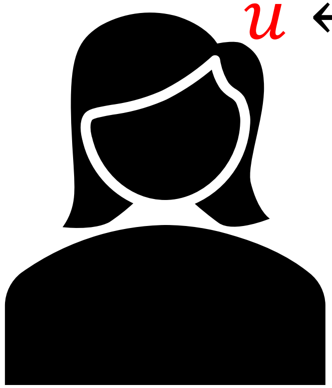
$s \leftarrow$ SSet $=[-B,B]^{dm}$ $\qquad A_1 = \mathrm{Com}(s)$

$u \leftarrow RSet = [-B',B']^{dm}$ $\quad A_0 = \mathrm{Com}(u)$ $\longrightarrow$

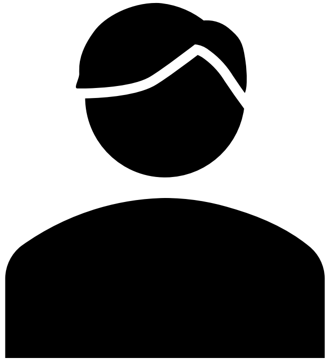
$x \leftarrow$ Cset=$\{0,1\}^d \subseteq R_q$ $\longleftarrow$

$\boldsymbol{f} = u + x \cdot s$ $\qquad \boldsymbol{f}$ $\longrightarrow$

Restart if $\|\boldsymbol{f}\|_\infty > \boldsymbol{B' - max_{x,s}\|x \cdot s\|_\infty}$



Prover



Verifier

$\boxed{A_0 + x \cdot A_1 \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f})}$

$\boxed{\|f\| \;?< B' - max_{x,s}\|x \cdot} \; s\|_\infty$

Correctness: homomorphic property of Com

Com(f) = Com(u+ x · s) = Com(u) · Com(s)^x

Soundness (2-special soundness): prover succeeds with prob > 1/|ChSet| → prover knows a **valid** opening of A_1

- Given commitment A_0, from **two** distinct successful challenge response pair pairs (x,f), (x',f'), extract witness s'

$$A_0 + x \cdot A_1 = \mathrm{Com}(\boldsymbol{f})$$
$$A_0 + x' \cdot A_1 = \mathrm{Com}(\boldsymbol{f}')$$

s'

$$(\boldsymbol{x} - \boldsymbol{x}') \cdot \boldsymbol{A_1} = \mathbf{Com}(\boldsymbol{f} - \boldsymbol{f}')$$

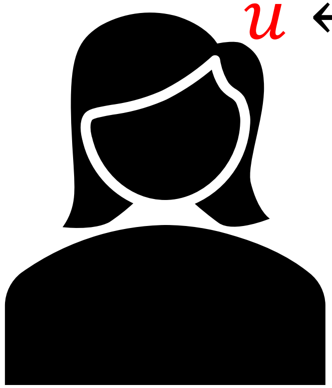
Relaxation factor

Lattice ZKP 1 Lattice-analogue of Schnorr ZKP
`Fixed Proof' idea (a-la [Lyu12])

$s \leftarrow$ SSet $=[-B, B]^{dm}$

$A_1 = \mathrm{Com}(s)$

$u \leftarrow RSet = [-B', B']^{dm}$ $A_0 = \mathrm{Com}(u)$

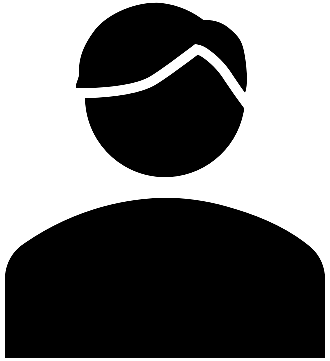


$x \leftarrow$ CSet $\subseteq R_q$

$\boldsymbol{f} = u + x \cdot s$ $\boldsymbol{f}$

Restart if $\|\boldsymbol{f}\|_\infty > B' - \boldsymbol{max_{x,s}}\|\boldsymbol{x} \cdot \boldsymbol{s}\|_\infty$

Prover



Verifier

$$\boxed{A_0 + x \cdot A_1 \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f})}$$

Honest-Verifier Zero-Knowledge (HVZK): An honest verified can efficiently simulate a proof transcript without the prover's witness!

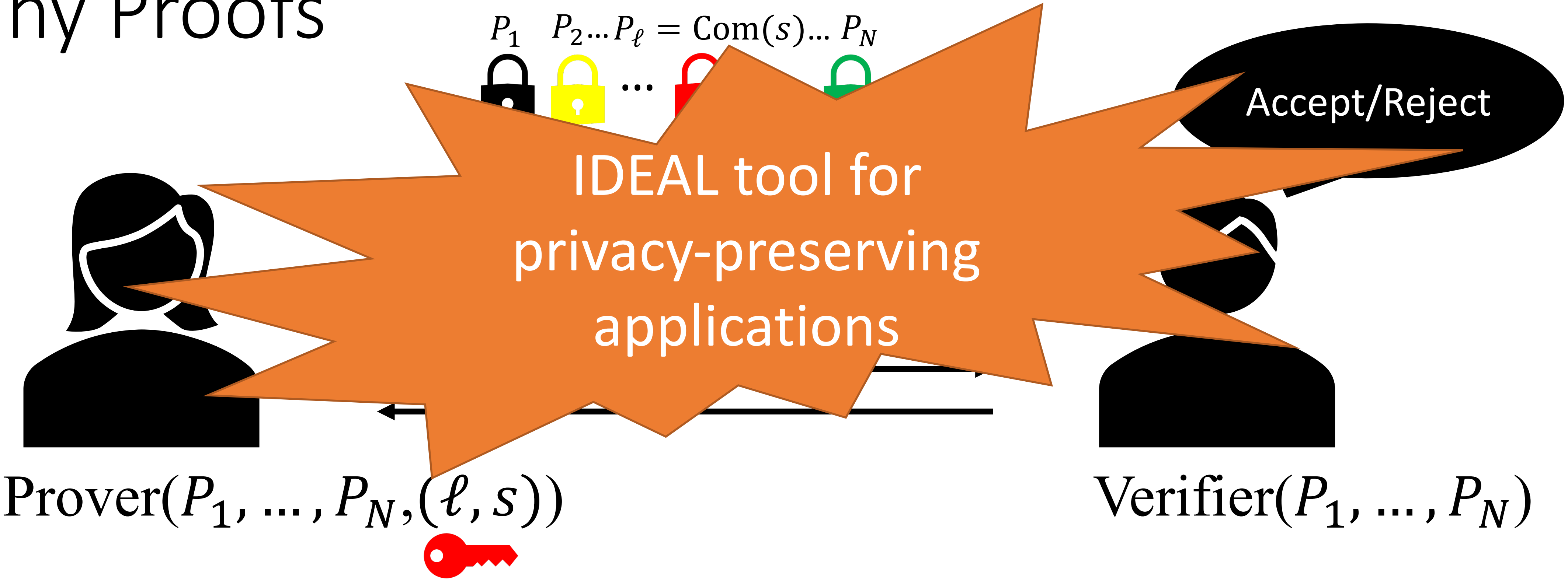
Accepted Transcript Simulator, given A_1:

- $x \leftarrow$ CSet $\subseteq R_q$
- $f \leftarrow$ AccSet = $[-(B' - \boldsymbol{max_{x,s}}\|\boldsymbol{x} \cdot \boldsymbol{s}\|_\infty), (B' - \boldsymbol{max_{x,s}}\|\boldsymbol{x} \cdot \boldsymbol{s}\|_\infty)]^{dm}$
- $A_0 = \mathrm{Com}(\boldsymbol{f}) - x \cdot A_1$

Application 1: Digital Signatures [Lyu12,L17+]

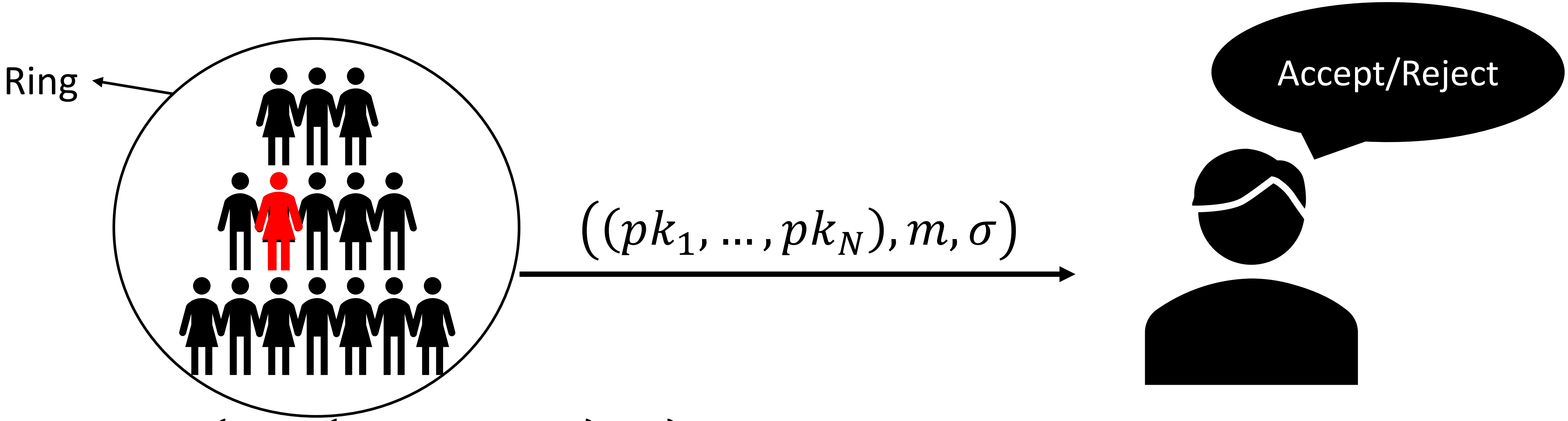
- Lyubashevsky digital signature idea [variant of Lyu12]
  - **KG:** sk = s, A_1 = Com(s)
  - **Sign**(s, m) = (x,f)
    - A_0 = Com(u)
    - x = H(A_0,m) ∈ $\{0,1\}^d$
    - f = u + x·s **Restart if $\|f\|_\infty > B' - max_{x,s}\|x \cdot s\|_\infty$.**
  - **Ver**(m,(x,f),pk):
    - $A_0 = \mathrm{Com}(f) - x \cdot A_1$
    - $x \stackrel{?}{=}$ H(A_0,m)
    - $\|f\| \, ?< B' - max_{x,s}\|x \cdot s\|_\infty$
- Unforgeability proof ideas:
  - ZK simulator → simulate obs signatures by programming H, without secret key s
  - Approx. relation soundness → forging alg. can be used to extract s' = $f - f'$ s.t
  - $(x - x') \cdot A_1 = \mathrm{Com}(f - f')$ → solve Module-RingSIS : Com($(x - x') \cdot s - (f - f')$) = 0
  - Hardness of decision Module-RingLWE → non-trivial solution for Module-RingSIS
- Optimised signature variants of above in NIST PQC second round:
  - Dilithium, Tesla

ZKPs for non-linear relations: One-out-of-Many Proofs



Goal: Prove knowledge of a secret associated to one of the public values without revealing the secret and the index of the public value

Ring Signatures [RST01, BKM09]



$$\sigma \leftarrow \mathrm{Sign}(sk_\ell, (pk_1, \dots, pk_N), m)$$

Properties:

1) Correctness
2) Unforgeability
3) Anonymity

1-out-of-N proof $\rightarrow$ Ring Signature

- Users commit to their secret keys to form their public keys:

$$pk_i = \mathrm{Com}(sk_i)$$

- Signer generates a non-interactive 1-out-of-N proof to prove knowledge of an opening of one of pk_i's
  - i.e., proving knowledge of sk_ℓ without revealing ℓ

1-out-of-N ZKP		**Ring Signature**
Completeness	$\Longrightarrow$	Correctness
Soundness	$\Longrightarrow$	Unforgeability
Zero-Knowledge	$\Longrightarrow$	Anonymity

The transition may not go so smoothly in the lattice setting!

Applications and Our Focus

- Set membership proofs, group signatures, …
- Privacy-aware cryptocurrencies, e.g., RingCT protocol in Monero
- e-voting systems
- …

- **We want:** short (sublinear-sized) and
  "post-quantum" one-out-of-many proofs
  with no trusted setup

Advanced Zero-Knowledge Proofs

Discrete Log.

- ZK proofs run smoothly
  - No protocol repetitions (negligible soundness error in single execution)
  - Exact soundness
  - **Any** commitment opening is valid
- Very short and scalable 1-out-of-N proofs due to Groth and Kohlweiss [GK15] and Bootle et al. [BCC+15]
  - Proof length: $O(\log N)$
  - Short **in practice** as well
  - Only a few KB even for $N = 10^9$

Lattice

- If you care about **efficiency**, then you have to make compromises
  - Relaxed soundness:
    prove knowledge of $(\gamma, \vec{s})$ s.t
    $\gamma \cdot C = \mathrm{Com}(\vec{s})$
- Only **short** openings are valid
  - $||\vec{s}|| \leq T$ for some $T < q$
- You may have to work
  - with a **small** set of challenges
  - over a **ring**, not a field
- Log-sized ring signature due to Libert et al. [LLNW15]
  - **NOT short** in practice
  - 75 MB for $N = 1000$

Our Results: Summary

- New technical tools for algebraic lattice-based protocols
  - Handling approximate ZK protocols for non-linear (degree $k > 1$) relations in lattice setting
    - **Many special sound protocols: Generalization of Lyubashevsky 2-sound protocol to $k > 1$ - non-linear relations**
      - Bounds on length of extracted witnesses and approximation factors
    - Speed-up Techniques: CRT message packing in commitment and adapting NTT-friendly rings
- Short one-out-of-many proofs from lattices
  - One shot challenges
  - Short both asymptotically and in practice
- Short ring signature from standard lattice assumptions
  - Based on Module-LWE and Module-SIS
  - No trusted setup
  - New ideas for soundness $\Longrightarrow$ unforgeability in a constraint (lattice) setting
- Variant proofs for range and set membership proofs
- Exploiting module variants of standard lattice assumptions for efficiency purposes [see the papers for details]

Lattice-Based Commitment schemes

- To hide low-entropy messages, need a randomised (hiding) commitment scheme Com(m; r)
- For remainder of this talk, Com will denote one of the two lattice-based (Module-LWE, Module-SIS) randomised commitment schemes [B+18]:
  - Hashed Message Commitment (HMC):

$$\mathrm{Com}(m, r) = \begin{pmatrix} G_r & G_m \end{pmatrix} \begin{pmatrix} r \\ m \end{pmatrix}$$

  - Unbounded-Message Commitment (UMC):

$$\mathrm{Com}(m, r) = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix} r + \begin{pmatrix} 0 \\ m \end{pmatrix}$$

Framework: ZKPs for non-linear relations

Prover

$$\xrightarrow{A_0, \ldots, A_k}$$

$$\xleftarrow{x \leftarrow \text{ChallengeSet}}$$

$$\xrightarrow{\boldsymbol{f}, \boldsymbol{r}}$$

<u>Witness Extraction</u>

How to extract **useful** secret information given a set of **accepting** protocol transcripts with the same initial message for a lattice-based commitment scheme Com?

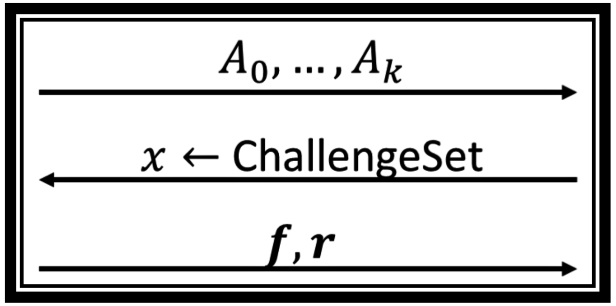
$$\boxed{A_0 + xA_1 + \cdots + x^k A_k \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f}; \boldsymbol{r})}$$

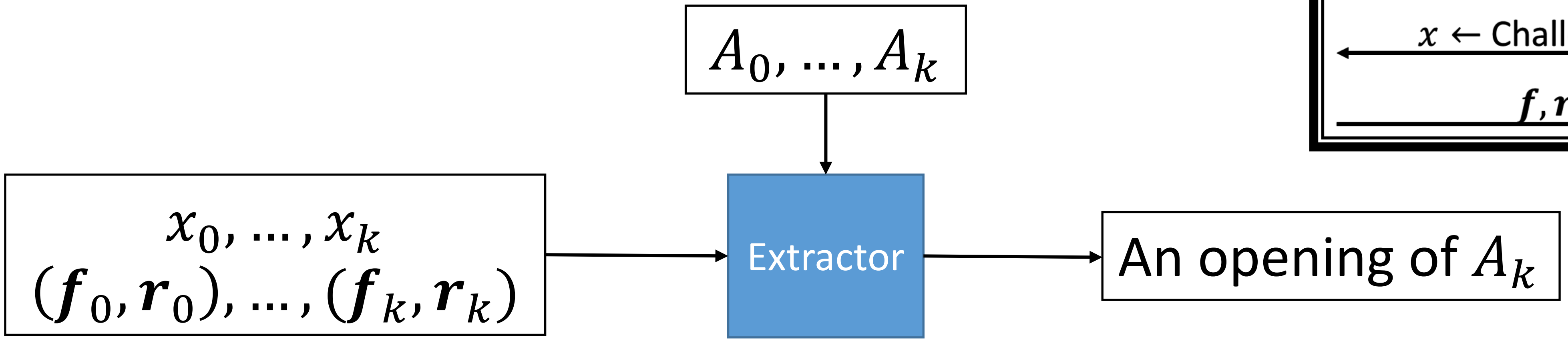
Efficient proof systems from [GK15] and [BCC+15] have this structure!

We need to 1) prove a degree-k relation for $k \geq 1$

2) extract a **valid** opening of A_k

Witness Extraction ($(k+1)$-special soundness)





s.t. $A_0 + x_i A_1 + \cdots + x_i^k A_k \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f}_i; \boldsymbol{r}_i)$ for $i = 0, \ldots, k$

Proves a soundness error $\leq \frac{k}{|\mathrm{ChSet}|}$
(a cheating prover's max. success probability)

Witness Extraction

- We know that $A_0 + x_i A_1 + \cdots + x_i^k A_k \stackrel{?}{=} \mathrm{Com}(\boldsymbol{f}_i; \boldsymbol{r}_i)$ for $i = 0, \ldots, k$

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^k \\ 1 & x_1 & x_1^2 & \cdots & x_1^k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^k \end{pmatrix} \cdot \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_k \end{pmatrix} = \begin{pmatrix} \mathrm{Com}(\boldsymbol{f}_0; \boldsymbol{r}_0) \\ \mathrm{Com}(\boldsymbol{f}_1; \boldsymbol{r}_1) \\ \vdots \\ \mathrm{Com}(\boldsymbol{f}_k; \boldsymbol{r}_k) \end{pmatrix}$$

over a ring $\mathfrak{R}$

$\boldsymbol{V}$, Vandermonde Matrix

- **Goal:** Recover an opening of A_k

For our lattice-based commitment, $(\vec{m}, \vec{r})$ is a valid opening of C if $C = \mathrm{Com}(\vec{m}; \vec{r})$ AND $(\vec{m}, \vec{r})$ is short!

Witness Extraction

We have $\boldsymbol{V} \cdot \boldsymbol{a} = \boldsymbol{c}$, and we want to eliminate $\boldsymbol{V}$

[Turner66]

$$\boldsymbol{V}^{-1} = \begin{pmatrix} \frac{*}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} & \frac{*}{(x_0-x_1)(x_1-x_2)\cdots(x_1-x_k)} & \cdots & \frac{*}{(x_0-x_k)(x_1-x_k)\cdots(x_{k-1}-x_k)} \\ \frac{*}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} & \frac{*}{(x_0-x_1)(x_1-x_2)\cdots(x_1-x_k)} & \cdots & \frac{*}{(x_0-x_k)(x_1-x_k)\cdots(x_{k-1}-x_k)} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{1}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} & \frac{-1}{(x_0-x_1)(x_1-x_2)\cdots(x_1-x_k)} & \cdots & \frac{(-1)^k}{(x_0-x_k)(x_1-x_k)\cdots(x_{k-1}-x_k)} \end{pmatrix}$$

Two approaches:

- Approach 1 [E+19a]: Use special challenge space so that challenge differences
  1) are invertible, and
  2) have a \`short' inverse!
  - Drawback: Small challenge space → multiple repetitions needed for high soundness security → Long proofs, length = $\tilde{O}(\lambda^2)$
- Approach 2 [This work]: Clear the denominators by multiplying by det(V) and find good bounds on det(V) for a set of \`short' challenges
  - Advantage: can support large challenge space (\`\`one-shot') → short proofs, length = $\tilde{O}(\lambda)$

Our approach: adjugate matrices

- Instead of multiplying by V^{-1} , we multiply by adj(V):
  - We have $\boldsymbol{V} \cdot \boldsymbol{a} = \boldsymbol{c} \rightarrow \boldsymbol{det}(\boldsymbol{V}) \cdot \boldsymbol{a} = \boldsymbol{adj}(\boldsymbol{V}) \cdot \boldsymbol{c}$
  - Relaxation factor: $\det(V) = \prod_{0 \leq i < j \leq k} (x_i - x_j)$

$$adj(V) = \begin{pmatrix} \frac{*}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} & \frac{*}{(x_0-x_1)(x_1-x_2)\cdots(x_1-x_k)} & \cdots & \frac{*}{(x_0-x_k)(x_1-x_k)\cdots(x_{k-1}-x_k)} \\ \frac{*}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} & \frac{*}{(x_0-x_1)(x_1-x_2)\cdots(x_1-x_k)} & \cdots & \frac{*}{(x_0-x_k)(x_1-x_k)\cdots(x_{k-1}-x_k)} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\det(V)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} & \frac{-\det(V)}{(x_0-x_1)(x_1-x_2)\cdots(x_1-x_k)} & \cdots & \frac{(-1)^k \det(V)}{(x_0-x_k)(x_1-x_k)\cdots(x_{k-1}-x_k)} \end{pmatrix}$$

  - Extracted witness for last commitment:

$$\det(V) \cdot A_k = \sum_{i=0}^{k} \Gamma_i \cdot Com(f_i; r_i) = Com(\underbrace{\sum_{i=0}^{k} \Gamma_i \cdot f_i}_{\hat{m}_k}; \underbrace{\sum_{i=0}^{k} \Gamma_i \cdot r_i}_{\hat{r}_k})$$

where $\Gamma_i = (-1)^{i+k} \prod_{0 \leq l < j \leq k \; l,j \neq i} (x_j - x_l)$

Our approach: adjugate matrices

- In particular, our adjugate matrix analysis approach allows large challenge spaces of the form

$$\mathcal{C}^d_{w,p} = \{ x \in \mathbb{Z}[X] \, : \, \deg(x) = d - 1 \wedge \mathsf{HW}(x) = w \wedge \|x\|_\infty = p \}.$$

  - \`One shot' possible with \`short' challenges
    - e.g. size of $\mathcal{C}^d_{w,p}$ > 2^{256} if $(d, w, p) = (256, 60, 1)$
  - No invertibility condition on challenge space needed (V can even be singular)
    → no special condition on ring modulus q needed
    → can use \`NTT-friendly' *q*
  - Moderately short bounds on relaxation factor / witness size for small *k:*
    - *Relaxation factor:* $\det(V) \ \leq (2p)^{k(k+1)/2} \cdot w^{k(k+1)/2-1}$
    - *Extracted witness norm:*

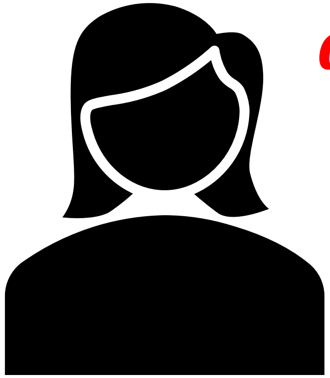
$$\|\widehat{m}_k\| \leq (k+1) \cdot d \cdot (2p)^{k(k-1)/2} \cdot w^{k(k-1)/2-1} \cdot max_i \|f_i\|$$
$$\|\hat{r}_k\| \leq (k+1) \cdot d \cdot (2p)^{k(k-1)/2} \cdot w^{k(k-1)/2-1} \cdot max_i \|r_i\|$$

Application: Commitments of Bits **Relaxed** ZKP

- One-shot variant of multi-shot lattice ZKP [E+19a], DL ZKP in [GK15]
  - Prover witness $\boldsymbol{b} \in \{\mathbf{0}, \mathbf{1}\}^{s}, \boldsymbol{r}$ ← Sset (`short')
  - Verifier input: $B = \mathrm{Com}(\boldsymbol{b}\ ; \boldsymbol{r})$
  - Original Goal: prove that b is a vector of **bits**
  - **Relaxed Goal: prove that b = y b' for vector of bits b' and `short' relaxation factor y**
  - ZKP Idea – encode binary requirement as a quadratic relation:
    - $b_i \in \{0,1\} \leftarrow (over\ a\ field) \quad b_i \cdot (1 - b_i) = 0$
    - Usual basic setting:
      - Prover sends commitment of masking randomness $A = Com(\boldsymbol{a}\ ; \boldsymbol{r_a})$
      - Verifier sends challenge x
      - Prover sends response encodings $f_i = a_i + \mathrm{x} \cdot b_i$
    - To verify binary requirement, verifier computes quadratic function of x over encodings:
      - $g_i(x) = f_i \cdot (x - f_i) = \left[-a_i^2\right] + [a_i(1 - 2b_i)] \cdot x + [b_i(1 - b_i)] \cdot x^2$
      - And checks that x^2 coefficient is zero, by checking
      - $Com(g_i(x))$ =? Com($\left[-a_i^2\right]$) + Com($[a_i(1 - 2b_i)]$)*x
      - To allow verifier to do this, prover also sends in first step commitments to the non-zero coefficients

Application: Commitment to bits ZKP (basic idea)

$\boldsymbol{b} \in \{\mathbf{0}, \mathbf{1}\}^{s}, \boldsymbol{r} \leftarrow \text{SSet}$



Prover

$A = Com(\boldsymbol{a}\,; \boldsymbol{r_a})$

$C = Com([a_i(1-2b_i)]; \boldsymbol{r_c})$

$D = Com([-a_i^2]; \boldsymbol{r_d})$

$\boldsymbol{a}, \boldsymbol{r_a} \longrightarrow$

$x \leftarrow \text{CSet} \subseteq R_q$

$\longleftarrow$

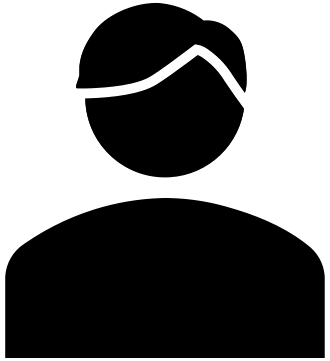
$\boldsymbol{f_i} = a_i + x \cdot b_i \qquad (\boldsymbol{f}, \boldsymbol{z_b}, \boldsymbol{z_c}) \longrightarrow$

$\boldsymbol{z_b} = \boldsymbol{r_a} + x \cdot \boldsymbol{r}$

$\boldsymbol{z_c} = \boldsymbol{r_d} + x \cdot \boldsymbol{r_c}$

Restart if $\|(\boldsymbol{f}, \boldsymbol{z_b}, \boldsymbol{z_c})\|_\infty > \boldsymbol{B'}$

$B = \text{Com}(\boldsymbol{b}\,; \boldsymbol{r})$



Verifier

$\boxed{A + x \cdot B \stackrel{?}{=} \text{Com}(\boldsymbol{f}; z_b)}$

$\boxed{D + x \cdot C \stackrel{?}{=} \text{Com}(\boldsymbol{g}; \boldsymbol{z_c})}$

$\|(\boldsymbol{f}, \boldsymbol{z_b}, \boldsymbol{z_c})\| \,?< B'$

$\boldsymbol{g} = [\boldsymbol{g_i}(\boldsymbol{x})] = [\boldsymbol{f_i} \cdot (\boldsymbol{x} - \boldsymbol{f_i})]$

Application: Commitment to bits ZKP (basic idea)

- Commit to bits ZKP Soundness argument sketch:
  - Using **three** rewindings of a prover on distinct challenges: x_1, x_2, x_3 (same commitments, but different responses $f_{i,j}$ ($j = 1,2,3$)
  - -> Get 3 relaxed openings $(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{b}}, \widehat{\boldsymbol{c}}, \widehat{\boldsymbol{d}})$ of A,B,C,D
    - with relaxation factor $y = x_1 - x_2$
    - Must be same openings by binding of Com, hence:
    - $y \cdot f_{i,j} = x_j \cdot \hat{b}_i + \hat{a}_i$ (j=1,2,3)
    - $y \cdot f_{i,j} \cdot (x_j - f_{i,j}) = x_j \cdot \hat{c}_i + \hat{d}_i$ (j=1,2,3)
    - → Combine above pairs of relations to get a Vandermonde linear system over R_q:

$$\begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \cdot \begin{pmatrix} -\hat{a}_i^2 - y\hat{d}_i \\ \hat{a}_i(y - 2\hat{b}_i) - y\hat{c}_i \\ \hat{b}_i(y - \hat{b}_i) \end{pmatrix} = 0$$

- Our adjugate technique implies $\det(V)\, \hat{b}_i(y - \hat{b}_i) = 0$ in R_q

Application: Commitment to bits ZKP (basic idea)

- Commit to bits ZKP Soundness argument sketch (cont.):
- Our adjugate technique implies $\det(V)\,\hat{b}_i\left(y-\hat{b}_i\right)$ = 0 in R_q, where
- $det(V) = (x_1 - x_2)\,(x_1 - x_3)(x_2 - x_3)$
- Want to use `NTT-friendly' rings and `large' challenges
  - Cannot assume det(V) is invertible in R_q
- But, still want to "cancel" det(V) factor
- → Speed-up Lemma 1:

Lemma 7. *Let* $f_1, \dots, f_n \in R$ *for some* $n \geq 1$. *If* $\prod_{i=1}^{n} f_i = 0$ *in* R_q *and* $q/2 > \|f_1\|_\infty \cdot \prod_{i=2}^{n} \|f_i\|_1$, *then there exists* $1 \leq j \leq n$ *such that* $f_j = 0$.

- -> We choose q large enough s.t. Lemma 7 applies: $q/2 > \det(V)\,\hat{b}_i\left(y-\hat{b}_i\right)$ → can cancel det(V) to conclude
  - $\hat{b}_i\left(y-\hat{b}_i\right)$ = 0 → "relaxed" soundness holds: $\hat{b}_i = y \cdot b_i'$ with $b_i' \in \{0,1\}$

Application: One-of-N ZKP

- One-shot variant of multi-shot lattice ZKP [E+19a], DL ZKP in [GK15]
  - Prover witness $\boldsymbol{\ell} \in [\boldsymbol{N}], \boldsymbol{r} \leftarrow$ Sset (\`short')
  - Verifier input: $(P_1, \dots, P_N)$
  - Original Goal [GK15]: prove that $P_\ell = \mathrm{Com}(\mathbf{0}\,;\boldsymbol{r})$
  - **Relaxed Goal (Our protocol): prove that $\boldsymbol{y}' \cdot P_\ell = \boldsymbol{Com}(\mathbf{0}\,;\hat{\boldsymbol{r}})$ for \`short' y' and $\hat{\boldsymbol{r}}$**
  - ZKP Idea – encode requirement as a polynomial relation:
    - Decompose $\ell = \sum_{j=0}^{k-1} \ell_j \boldsymbol{\beta}^j$ and $\boldsymbol{i} = \sum_{j=0}^{k-1} \boldsymbol{i}_j \boldsymbol{\beta}^j \in [\boldsymbol{N}]$ into $k = O(\log N)$ base-β digits
    - Write each digit ℓ_j in unary: $\boldsymbol{\delta}_j = (\delta_{\ell_j,0}, \dots, \delta_{\ell_j,\beta-1})$ is a bit vector with 1 in ℓ_j'th pos. and 0 else.
    - Then $P_\ell = \mathrm{Com}(\mathbf{0}\,;\boldsymbol{r})$ is equiv. to $\sum_{i\in[N]} \left(\prod_{j\in[k]} \delta_{\ell_j,i_j}\right) \cdot P_i = Com(0\,;r)$ (*)
    - Prover commits to $\boldsymbol{\delta}_j$'s and uses \`Commit to Bits' Protocol variant to prove $\boldsymbol{\delta}_j$'s are well formed
      - Prover sends commitments of masking randomness $A = Com(\boldsymbol{a}\,;\boldsymbol{r_a})$ (and C, D)
      - Verifier sends challenge x
      - Prover sends response encodings $f_{j,i_j} = a_{j,i_j} + \mathrm{x} \cdot \delta_{\ell_j,i_j}$
    - To verify 1-of-N relation (*), verifier computes degree k function of x over encodings:
      - $P(x) = \sum_{i\in[N]} p_i(x) \cdot P_i = \sum_{i\in[N]} \left(\prod_{j\in[k]} f_{j,i_j}\right) \cdot P_i = \sum_{i\in[N]} \left([e_{i,0}] + [e_{i,1}] \cdot x + \cdots + \left[\prod_{j\in[k]} \delta_{\ell_j,i_j}\right] \cdot x^k\right) \cdot P_i$
      - And checks that x^k coefficient is a commitment zero, by checking
      - $P(x) - ([\sum e_{i,0} P_i] + [\sum e_{i,1} P_i] \cdot x + \cdots + [\sum e_{i,k-1} P_i] \cdot x^{k-1})$ = Com(0,z) for a z sent by the prover
      - To allow verifier to do this, prover also sends in first step commitments in the coefficients of x^j (j < k)

Application: One-of-N ZKP

- Commit to bits ZKP Soundness argument sketch:
  - Using the extractor of our Relaxed `Commit to Bits' protocol with relaxation factor y = $x_1 - x_2$, we extract an opening $\hat{\ell}$ and $\widehat{p_i}$
  - Using **k+1** rewindings of a prover on distinct challenges: $x_1, \ldots, x_{k+1}$
  - → get a (k+1)'th order Vandermonde linear system with matrix V over R_q
  - → By our adjugate technique, extract a relaxed decommitment of the form
  - $\det(V)\, y^k P_{\hat{\ell}} = Com(0, \sum_{i \in [N]} \Gamma_i\, y^k \boldsymbol{z}_i)$
  - To reduce the relaxation factor to $\det(V)\, y$, we apply another observation:

Lemma 6. *Let $f, g \in R = \mathbb{Z}[X]/(X^d+1)$. If $f \cdot g^k = 0$ in $R_q = \mathbb{Z}_q[X]/(X^d+1)$ for some $k \in \mathbb{Z}^+$, then $f \cdot g = 0$ in R_q.*

  - We apply our bounds on det(V) and y to bound the extracted witness norm.
  - Moderately practical since k+1 = O(log N) is small –
    - in practice for N up to millions, usually optimal to use k a small constant k < 3

Application: Ring Signature Length Comparison

Ring Size	2^6	2^{10}	2^{16}	2^{20}	2^{30}
[LLNW15]	47000	75000	118000	146000	217000
[ESSLL19]	774	1021	1487	1862	3006
[**E**SLL19]	57	89	154	241	541

eprint.iacr.org/2018/773 – ”multi-shot” proofs (ACNS’19)

eprint.iacr.org/2019/445 – Advanced “one-shot” proofs

(to appear in CRYPTO’19)

Signature lengths are in KB.
Security level ≈ 128 bits

Application: Integer Range ZKP

- Integer range Proofs:
- Prover witness: $\ell \in [0, 2^k - 1]$, r `$short'$
- Verifier input: $(P \quad)$
- Original Goal: prove that $P = Com(\ell \,; r\,)$ with $\ell \in [0, 2^k - 1]$
- **Relaxed Goal (Ours): prove that $\boldsymbol{y' \cdot P \quad = Com(y' \cdot \ell \,; \hat{r})}$ for `short' y' and $\boldsymbol{\hat{r}}$**
- Basic ZKP idea:
  - Decompose $\ell = \boldsymbol{\sum_{i=0}^{k-1} \ell_i 2^i}$ in binary, $\ell_i \in \{0,1\}$
  - Prover commits to bits $B = Com(\ell_0, \ldots, \ell_{k-1};\ )$
  - Use `Commit to Bits' protocol to prove $\ell_i \in \{0,1\}$
    - Prover sends commitment of masking randomness $A = Com(\boldsymbol{a} \,; \boldsymbol{r_a})$
    - Verifier sends challenge x
    - Prover sends response encodings $f_i = Enc_x(\ell_i) = a_i + \mathrm{x} \cdot \ell_i$
  - Verifier checks `Commit to Bits' Proof and also checks that bits decompose ℓ
    - Inter-bit homomorphic encoding operation on encodings:
      - Verifier computes encoding v = $Enc_x\left(\sum_{i=0}^{k-1} 2^i \ell_i\right)$ from encodings of ℓ_i
      - $\sum_{i=0}^{k-1} 2^i \cdot Enc_x(\ell_i) = \sum_{i=0}^{k-1} 2^i \cdot a_i + x \ \cdot \sum_{i=0}^{k-1} 2^i \ell_i$
      - Checks that Com(v) and x*P are commitments to same ℓ

Speed-up technique 2: CRT-packing technique supporting inter-slot operations

- Efficiency problem:
  - Each bit ℓ_i consumes a whole ring element in the B commitment (UMC)

$$\mathrm{Com}(\ell, r) = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} r + \begin{bmatrix} 0 \\ \ell \end{bmatrix}$$

  - →k additional ring elements in commitment output
  - →Can maintain commitment length (set ring dimension d → d/k)
  - →But Com eval run-time still goes up by factor k (G_2 has $\geq k^2$ Ring elements)

- Our Speedup Technique 2: Use CRT-packing (a-la FHE) to pack k bits into 1 ring element

Speed-up technique 2: CRT-packing technique supporting inter-slot operations

- CRT message packing of k bits into 1 ring element:
  - Use R_q such that $z^d + 1$ splits into k irreducible factors $P_i(z)$ mod q (each of degree d/k:
    - $R_q \simeq R_q^{(1)} \times \cdots \times R_q^{(k)}$
    - $m \to CRT(m) = (m_1, \ldots, m_k) = (m \, mod \, P_1, \ldots, m \, mod \, P_k)$
- Packed Encoding is now:
  - $f = Enc_x(\ell_1, \ldots, \ell_k) = CRT^{-1}(a_1, \ldots, a_k) + \mathrm{x} \cdot CRT^{-1}(\ell_1, \ldots, \ell_k)$
  - Can extract from f encodings of individual slots:
    - $f_i = Enc_{x \, mod \, P_i}(\ell_i) = a_i + x \, mod \, P_i \cdot \ell_i$
  - But to support interslot homomrphic property of Enc, need all extracted encodings with respect to same x → need $x \, mod \, P_i = x$ for all i
    - $\sum_{i=0}^{k-1} 2^i \cdot Enc_x(\ell_i) = \sum_{i=0}^{k-1} 2^i \cdot a_i + x \cdot \sum_{i=0}^{k-1} 2^i \, \ell_i$
  - Our solution: choose challenge x of degree < d/k → $x \, mod \, P_i = x$ for all i

Speed-up technique 2: CRT-packing technique supporting inter-slot operations

Table 2: The (minimal) asymptotic time and space complexities of lattice-based protocols involving commitment to $k = O(\log q)$ messages. β_{SIS}: M-SIS solution norm, q: modulus, κ: the number of protocol repetitions, n: module rank for M-SIS, v: message vector dimension in a commitment, d: polynomial ring dimension, m: randomness vector dimension in a commitment. Assume: $\log q < \log^2 \beta_{\mathrm{SIS}}/2$ and degree-d polynomial multiplication costs $\widetilde{O}(d)$. To optimize both costs, one would set $n = v$ in all cases.

	Formula	**Multi-shot**[26, 19] $\kappa = \widetilde{O}(\lambda), v = k$	**One-shot** $\kappa = 1, v = k$	**One-shot + CRT** $\kappa = 1, v = O(1)$
Space UMC	$\kappa(n+v)d\log q$	$\widetilde{O}(\lambda^2 \log^2 \beta_{\mathrm{SIS}})$	$\widetilde{O}(\lambda \log^2 \beta_{\mathrm{SIS}})$	$\widetilde{O}(\lambda \log^2 \beta_{\mathrm{SIS}})$
Time UMC	$\kappa(n+v)md$	$\widetilde{O}(\lambda^2 \log^2 \beta_{\mathrm{SIS}})$	$\widetilde{O}(\lambda \log^2 \beta_{\mathrm{SIS}})$	$\widetilde{O}(\lambda \log^2 \beta_{\mathrm{SIS}}/\log q)$
Space HMC	$\kappa n d \log q$	$\widetilde{O}(\lambda^2 \log^2 \beta_{\mathrm{SIS}})$	$\widetilde{O}(\lambda \log^2 \beta_{\mathrm{SIS}})$	N/A
Time HMC	$\kappa n(m+v)d$	$\widetilde{O}(\lambda^2 \log^2 \beta_{\mathrm{SIS}})$	$\widetilde{O}(\lambda \log^2 \beta_{\mathrm{SIS}})$	N/A

Selected references

- [GMR85] Goldwasser et al., “The knowledge complexity of interactive proof-systems”, STOC ‘85.
- [Sch89] Schnorr, “Efficient identification and signatures for smart cards”, CRYPTO ‘89.
- [Lyu09] Lyubashevsky, “Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures”, ASIACRYPT ’09.
- [Lyu12] Lyubashevsky, “Lattice Signatures without Trapdoors.”, EUROCRYPT ‘12.
- [GK15] Groth and Kohlweiss, “One-out-of-many proofs: Or how to leak a secret and spend a coin”, EUROCRYPT ‘15.
- [D+17] Ducas et al., “CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme”, CHES ‘18.
- [E+19a] Esgin et al., “Short lattice-based one-out-of-many proofs and applications to ring signatures, ACNS ‘19
- [E+19b] Esgin et al., “Lattice-based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications”, CRYPTO ‘19 (to appear)

THANK YOU