Algebraic Techniques for Short(er) Lattice-Based Zero-Knowledge Proofs

Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications

Jonathan Bootle, Vadim Lyubashevsky and **Gregor Seiler**

Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu and William Whyte

Aug 19, 2019

Lattice-Based Zero-Knowledge Proofs

In zero-knowledge proofs for lattice cryptography we want to prove knowledge of a short vector $\vec{\boldsymbol{w}}$ over $\mathbb{Z}_q$ such that

$$\boldsymbol{A}\vec{\boldsymbol{w}} = \vec{\boldsymbol{v}},$$

where the matrix $\boldsymbol{A}$ and the vector $\vec{\boldsymbol{v}}$ are publicly known.

Example:

Proving knowledge of a Ring-LWE secret $\boldsymbol{s} \in \mathcal{R}$ such that $\boldsymbol{v} = \boldsymbol{as} + \boldsymbol{e}$. In this case

$$\boldsymbol{A} = (\boldsymbol{a}, 1) \qquad \vec{\boldsymbol{w}} = \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix}$$

In our works:

New more efficient proof systems! Size for Ring-LWE sample: 384KB

Other Proof Systems

Approximate Proofs

Prove knowledge of *longer* vector $\vec{\boldsymbol{v}}$ such that $\boldsymbol{A}\vec{\boldsymbol{w}} = \bar{\alpha}\vec{\boldsymbol{v}}$ where $\bar{\alpha}$ is a short polynomial.

Ammortized Proofs

Prove knowledge of many *longer* vectors $\vec{\boldsymbol{w}}_i$ such that $\boldsymbol{A}\vec{\boldsymbol{w}}_i = \vec{\boldsymbol{v}}_i$ for all i.

Timed Post-Quantum Proofs

Prove equation $\boldsymbol{A}\vec{\boldsymbol{w}} = \vec{\boldsymbol{v}}$ exactly but using discrete-log assumption

Overview

Prover provides masked secret polynomial $\boldsymbol{z} = \boldsymbol{r} + \alpha \boldsymbol{w}$ with masking polynomial $\boldsymbol{r}$ and challenge polynomial α

In approximate proofs: Intermediately sized $\boldsymbol{r}$ masks short $\alpha \boldsymbol{w}$ via rejection sampling; length of $\boldsymbol{z}$ determines length of extracted secret (after rewinding)

Committing to masking vector $\vec{\boldsymbol{r}}$ via $\vec{\boldsymbol{t}} = \boldsymbol{A}\vec{\boldsymbol{r}}$ shows extracted secret is solution to the equation

Overview of our Techniques

Prover also proves that each coefficient of secret vector is in a small interval, e.g. binary.

The polynomial $\boldsymbol{w}$ has binary coefficients if and only if

$$\boldsymbol{w} \circ (\hat{\mathbf{1}} - \boldsymbol{w}) = \mathbf{0}$$

Replacing $\boldsymbol{w}$ by a masking $\boldsymbol{z} = \boldsymbol{r} + \alpha \boldsymbol{w}$ of $\boldsymbol{w}$ means the term we are interested in appears as the leading coefficient of the resulting polynomial in $\alpha \in \mathbb{Z}_q$ and is separated from *garbage terms*:

$$\boldsymbol{z} \circ (\alpha \hat{\mathbf{1}} - \boldsymbol{z}) = -\boldsymbol{r} \circ \boldsymbol{r} + \boldsymbol{r} \circ (\hat{\mathbf{1}} - 2\boldsymbol{w})\alpha + \boldsymbol{w} \circ (\hat{\mathbf{1}} - \boldsymbol{w})\alpha^2$$

If the verifier is convinced that $\boldsymbol{z}$ is of the correct form, independently of α, then he is convinced that $\boldsymbol{w}$ is binary if the leading term vanishes

Overview of our Techniques

Observations:

1. Proving something about individual coeffcients is inherently componentwise. This seems to preclude polynomial challenges.
2. Uniform challenges $\alpha \in \mathbb{Z}_q$ mean we need uniform masking polynomials $\vec{\boldsymbol{r}}$
3. $\vec{\boldsymbol{t}} = \boldsymbol{A}\vec{\boldsymbol{r}}$ does not bind $\vec{\boldsymbol{r}}$ anymore

Homomorphic Commitment scheme

Will need a commitment scheme over $\mathcal{R}$ that permits to compute $\mathcal{R}$-linear expressions in committed form.

$$\boldsymbol{a}\,\mathrm{Commit}(\boldsymbol{m}) + \boldsymbol{b}\,\mathrm{Commit}(\boldsymbol{m}') = \mathrm{Commit}(\boldsymbol{am} + \boldsymbol{b}\vec{\boldsymbol{m}}')$$

Then a proof that a commitment is a commitment to zero can be used to prove linear relations in zero-knowledge

Proving that Masking is of Correct Form

The prover provides commitments

$$C_{\boldsymbol{r}} = \mathrm{Commit}(\boldsymbol{r}),$$
$$C_{\boldsymbol{w}} = \mathrm{Commit}(\boldsymbol{w}),$$

and a proof that $C_{\boldsymbol{r}} + \alpha C_{\boldsymbol{w}}$ is a commitment to $\boldsymbol{z} = \boldsymbol{r} + \alpha \boldsymbol{w}$.

That is, a proof that $C_{\boldsymbol{r}} + \alpha C_{\boldsymbol{w}} - \mathrm{Commit}(\boldsymbol{z})$ is a commitment to zero

Proving Binary Coefficients — First Method

The prover provides commitments to the garbage terms,

$$\begin{aligned} C_0 &= \mathrm{Commit}(-\boldsymbol{r} \circ \boldsymbol{r}), \\ C_1 &= \mathrm{Commit}(\boldsymbol{r} \circ (\hat{\mathbf{1}} - \mathbf{2}\boldsymbol{w})), \end{aligned}$$

and gives a proof that $C_0 + \alpha C_1$ is a commitment to $\boldsymbol{z} \circ (\alpha \hat{\mathbf{1}} - \boldsymbol{z})$

Proving Binary Coefficients — Second Method

A different approach in Bootle-Lyubashevsky-Seiler

Polynomial product translates to pointwise product in NTT representation

$$
\begin{aligned}
&\mathrm{NTT}(\boldsymbol{z}(\alpha - \boldsymbol{z})) \\
&= \mathrm{NTT}(-\boldsymbol{r}^2 + \alpha \boldsymbol{r}(\mathbf{1} - \mathbf{2}\boldsymbol{w}) + \alpha^2 \boldsymbol{w}(\mathbf{1} - \boldsymbol{w})) \\
&= -\mathrm{NTT}(\boldsymbol{r}^2) + \alpha\,\mathrm{NTT}(\boldsymbol{r}(\mathbf{1} - \mathbf{2}\boldsymbol{w})) + \alpha^2\,\mathrm{NTT}(\boldsymbol{w}) \circ (\hat{\mathbf{1}} - \mathrm{NTT}(\boldsymbol{w}))
\end{aligned}
$$

A proof that $\boldsymbol{z}(\alpha - \boldsymbol{z})$ is of degree one in α shows that the NTT of the secret has binary coefficients

Outline

- The Main Protocol☜
- Applications of the Main Protocol
- Our Results

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

$$\begin{cases} \boldsymbol{A} \cdot \boldsymbol{w} = \boldsymbol{v} \\ \mathtt{f}(\boldsymbol{w}) = \boldsymbol{0} \\ deg(\mathtt{f}) = 2 \end{cases}$$

A Simplified Example

$$\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases} \qquad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal:
$$\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases} \qquad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$$

Starting Point:

$$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$$
$$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$$

$$\xrightarrow{\quad \boldsymbol{t} \quad}$$

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

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

$$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$$

$$\xrightarrow{\quad \boldsymbol{z} \quad}$$

$$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal:

$$\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases} \qquad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$$

Observation:

$$\begin{cases} z_2 z_3 = w_2 w_3 \alpha^2 + (r_2 w_3 + r_3 w_2)\alpha + r_2 r_3 \\ z_1 \alpha = w_1 \alpha^2 + r_1 \alpha \end{cases}$$

$$\underbrace{z_2 z_3 - z_1 \alpha}_{d} = (w_2 w_3 - w_1)\alpha^2 + \underbrace{(r_2 w_3 + r_3 w_2 - r_1)}_{a}\alpha + \underbrace{r_2 r_3}_{b}$$

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$\xrightarrow{\boldsymbol{t}}$

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

$\xleftarrow{\alpha}$

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$\xrightarrow{\boldsymbol{z}}$

$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $\begin{cases} A \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = v \\ w_1 = w_2 \cdot w_3 \end{cases}$ $\quad A \in \mathbb{Z}_q^{1\times 3}$

Attempt I:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \text{Com}(a; s_a)$

$C_b = \text{Com}(b; s_b)$ $\xrightarrow{\boldsymbol{t}, C_a, C_b}$

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

$\xleftarrow{\alpha}$

$z = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$\xrightarrow{z}$

$d = z_2 z_3 - z_1 \alpha$

$\boldsymbol{A}z \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\text{Com}(d) \stackrel{?}{=} \alpha \cdot C_a + C_b$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $$\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases} \qquad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$$

Attempt I:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \mathsf{Com}(a; s_a)$

$C_b = \mathsf{Com}(b; s_b)$ $\xrightarrow{\boldsymbol{t}, C_a, C_b}$

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

$\xleftarrow{\alpha}$

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$\xrightarrow{z}$

$d = z_2 z_3 - z_1 \alpha$

$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\mathsf{Com}(d) \stackrel{?}{=} \alpha \cdot C_a + C_b$

How to check this?

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases}$ $\quad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$

Attempt II:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \mathsf{Com}(a; s_a)$

$C_b = \mathsf{Com}(b; s_b)$ $\xrightarrow{\boldsymbol{t}, C_a, C_b}$

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

$\xleftarrow{\alpha}$

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$s = \alpha \cdot s_a + s_b$ $\xrightarrow{\boldsymbol{z}, s}$

$d = z_2 z_3 - z_1 \alpha$

$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\mathsf{Com}(d; s) \stackrel{?}{=} \alpha \cdot C_a + C_b$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases}$ $\quad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$

Attempt II:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \mathsf{Com}(a; s_a)$

$C_b = \mathsf{Com}(b; s_b)$ $\xrightarrow{\boldsymbol{t}, C_a, C_b}$

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

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$s = \alpha \cdot s_a + s_b$ $\xrightarrow{\boldsymbol{z}, s}$

Zero-Knowledge?

$d = z_2 z_3 - z_1 \alpha$

$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\mathsf{Com}(d; s) \stackrel{?}{=} \alpha \cdot C_a + C_b$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases}$ $\quad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$

A Variant of [BDL+ 18] Commitment:

Public Key: Random matrices $\boldsymbol{B}_1, \boldsymbol{B}_2$

Commit a message a: $s \leftarrow D_\sigma$; $c = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{B}_1 \\ \boldsymbol{0} & \boldsymbol{I}\ \boldsymbol{B}_2 \end{pmatrix} \cdot s + \begin{pmatrix} 0 \\ a \end{pmatrix}$

Attempt III:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \text{Com}(a; s_a)$

$C_b = \text{Com}(b; s_b)$ $\xrightarrow{\boldsymbol{t}, C_a, C_b}$

$\alpha \leftarrow \mathbb{Z}_p$

$\xleftarrow{\alpha}$

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$s = \alpha \cdot s_a + s_b$ $\xrightarrow{z, s}$

Abort with Probability

$1 - \dfrac{D_\sigma(s)}{M \cdot D_{\alpha \cdot s_a, \sigma}(s)}$

$d = z_2 z_3 - z_1 \alpha$

$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\text{Com}(d; s) \stackrel{?}{=} \alpha \cdot C_a + C_b$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases}$ $\quad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$

Protocol:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \text{Com}(a; s_a)$

$C_b = \text{Com}(b; s_b)$ $\xrightarrow{\boldsymbol{t}, C_a, C_b}$

$\alpha \leftarrow \mathbb{Z}_p$

$\xleftarrow{\alpha}$

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$s = \alpha \cdot s_a + s_b$ $\xrightarrow{\boldsymbol{z}, s}$

Abort with Probability

$1 - \dfrac{D_\sigma(s)}{M \cdot D_{\alpha \cdot s_a, \sigma}(s)}$

$d = z_2 z_3 - z_1 \alpha$

$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\text{Com}(d; s) \stackrel{?}{=} \alpha \cdot C_a + C_b$

Some tedious part:
1. Commit the witness.
2. Arguing correctness of commitments (Using Fiat-Shamir with Abort Protocol for commitments).

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Quadratic Constraints

Goal: $\begin{cases} \boldsymbol{A} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \boldsymbol{v} \\ w_1 = w_2 \cdot w_3 \end{cases}$ $\quad \boldsymbol{A} \in \mathbb{Z}_q^{1\times 3}$

Standard Soundness: ✔

High Efficiency: ✔ (if p is not too small)

Protocol:

$\boldsymbol{r} \leftarrow \mathbb{Z}_q^3$

$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{r}$

$a = (r_2 w_3 + r_3 w_2 - r_1), b = r_2 r_3$

$C_a = \text{Com}(a; s_a)$

$C_b = \text{Com}(b; s_b)$

$\xrightarrow{\boldsymbol{t}, C_a, C_b}$

$\alpha \leftarrow \mathbb{Z}_p$

$\xleftarrow{\alpha}$

$\boldsymbol{z} = \alpha \cdot \boldsymbol{w} + \boldsymbol{r}$

$s = \alpha \cdot s_a + s_b$

$\xrightarrow{\boldsymbol{z}, s}$

Abort with Probability

$1 - \frac{D_\sigma(s)}{M \cdot D_{\alpha \cdot s_a, \sigma}(s)}$

$d = z_2 z_3 - z_1 \alpha$

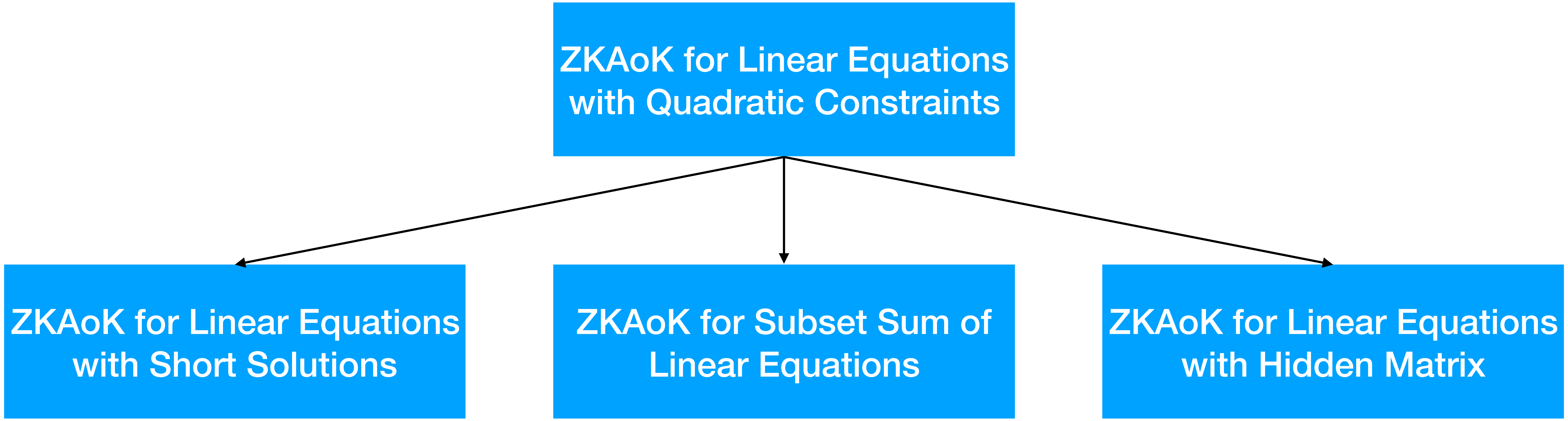
$\boldsymbol{A}\boldsymbol{z} \stackrel{?}{=} \alpha \cdot \boldsymbol{v} + \boldsymbol{t}$

$\text{Com}(d; s) \stackrel{?}{=} \alpha \cdot C_a + C_b$

Outline

- The Main Protocol
- Applications of the Main Protocol☜
- Our Results

Applications of the Main Protocol



Zero-Knowledge Arguments (of Knowledge)
for
Linear Equations with Short Solutions

Goal: $\begin{cases} A \cdot \boldsymbol{w} = \boldsymbol{v} \\ \forall i \in [n],\ 0 \leq \boldsymbol{w}_i \leq \beta \end{cases}$ **(Assume** $\beta = 2^k - 1$**)**

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Short Solutions

Goal: $\begin{cases} A \cdot \mathbf{w} = \mathbf{v} \\ \forall i \in [n],\ 0 \leq \mathbf{w}_i \leq \beta \end{cases}$ **(Assume $\beta = 2^k - 1$)**

Observation I: $0 \leq a \leq \beta \iff \exists a_1, \ldots a_k \in \{0,1\}^k, a = \sum_{i=1}^{k} a_i \cdot 2^{k-1}$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Short Solutions

Goal: $\begin{cases} A \cdot w = v \\ \forall i \in [n],\ 0 \le w_i \le \beta \end{cases}$ **(Assume $\beta = 2^k - 1$)**

Step I:

$$w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \xrightarrow{\text{Bit Decomposition}} \begin{pmatrix} w_{1,1} \\ \vdots \\ w_{1,k} \\ \vdots \\ w_{n,1} \\ \vdots \\ w_{n,k} \end{pmatrix} = w'$$

$$w_i = \begin{pmatrix} 1 & 2 & 4 & \dots & 2^{k-1} \end{pmatrix} \cdot \begin{pmatrix} w_{i,1} \\ w_{i,2} \\ w_{i,3} \\ \vdots \\ w_{i,k} \end{pmatrix}$$

$$A' = A \cdot G, \quad G = \begin{pmatrix} g & & & \\ & g & & \\ & & \ddots & \\ & & & g \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 4 & \dots & 2^{k-1} \end{pmatrix}$$

New Goal: $\begin{cases} A' \cdot w' = v \\ w' \in \{0,1\}^{nk} \end{cases}$

Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Short Solutions

Goal: $\begin{cases} \boldsymbol{A}' \cdot \boldsymbol{w}' = \boldsymbol{v} \\ \boldsymbol{w}' \in \{0,1\}^{nk} \end{cases}$

Observation II: $a \in \{0,1\} \iff a^2 = a \mod q$ (**Assume** q **is a prime**)

Zero-Knowledge Arguments (of Knowledge)
for
Linear Equations with Short Solutions

Goal: $\begin{cases} \mathbf{A}' \cdot \mathbf{w}' = \mathbf{v} \\ \mathbf{w}' \in \{0,1\}^{nk} \end{cases}$

Step II:

$w'_i \in \{0,1\} \Rightarrow w'^2_i = w'_i$

Linear Equation

New Goal: $\begin{cases} \boxed{\mathbf{A}' \cdot \mathbf{w}' = \mathbf{v}} \\ \boxed{\forall i \in [nk],\ \mathbf{w}'_i = \mathbf{w}'_i \cdot \mathbf{w}'_i} \end{cases}$

Quadratic Constraints

Zero-Knowledge Arguments (of Knowledge)
for
Subset Sum of Linear Equations

$$\begin{cases} \sum_{i=1}^{m} b_i \cdot \boldsymbol{A}_i \cdot \boldsymbol{w}_i = \boldsymbol{v} \\ b_i \in \{0,1\} \end{cases}$$

A Simplified Example

$$\begin{cases} b_1 \cdot \boldsymbol{A}_1 \cdot \boldsymbol{w}_1 + b_2 \cdot \boldsymbol{A}_2 \cdot \boldsymbol{w}_2 = \boldsymbol{v} \\ b_1 \in \{0,1\} \\ b_2 \in \{0,1\} \end{cases}$$

$$\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{Z}_q^1$$

Zero-Knowledge Arguments (of Knowledge)
for
Subset Sum of Linear Equations

Goal: $\begin{cases} b_1 \cdot \boldsymbol{A}_1 \cdot \boldsymbol{w}_1 + b_2 \cdot \boldsymbol{A}_2 \cdot \boldsymbol{w}_2 = \boldsymbol{v} \\ b_1 \in \{0,1\} \\ b_2 \in \{0,1\} \end{cases}$ $\quad \boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{Z}_q^1$

$$\boldsymbol{w}_1' = b_1 \cdot \boldsymbol{w}_1$$
$$\boldsymbol{w}_2' = b_2 \cdot \boldsymbol{w}_2$$

New Goal: $\begin{cases} \boldsymbol{A}_1 \cdot \boldsymbol{w}_1' + \boldsymbol{A}_2 \cdot \boldsymbol{w}_2' = \boldsymbol{v} \\ \boldsymbol{w}_1' = b_1 \cdot \boldsymbol{w}_1 \\ \boldsymbol{w}_2' = b_2 \cdot \boldsymbol{w}_2 \\ b_1 = b_1 \cdot b_1 \\ b_2 = b_2 \cdot b_2 \end{cases}$

Linear Equation

Quadratic Constraints

Zero-Knowledge Arguments (of Knowledge)
for
Linear Equations with Hidden Matrix

$\boldsymbol{A} \cdot \boldsymbol{w} = \boldsymbol{v}$

A Simplified Example

$$\begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \boldsymbol{v}$$

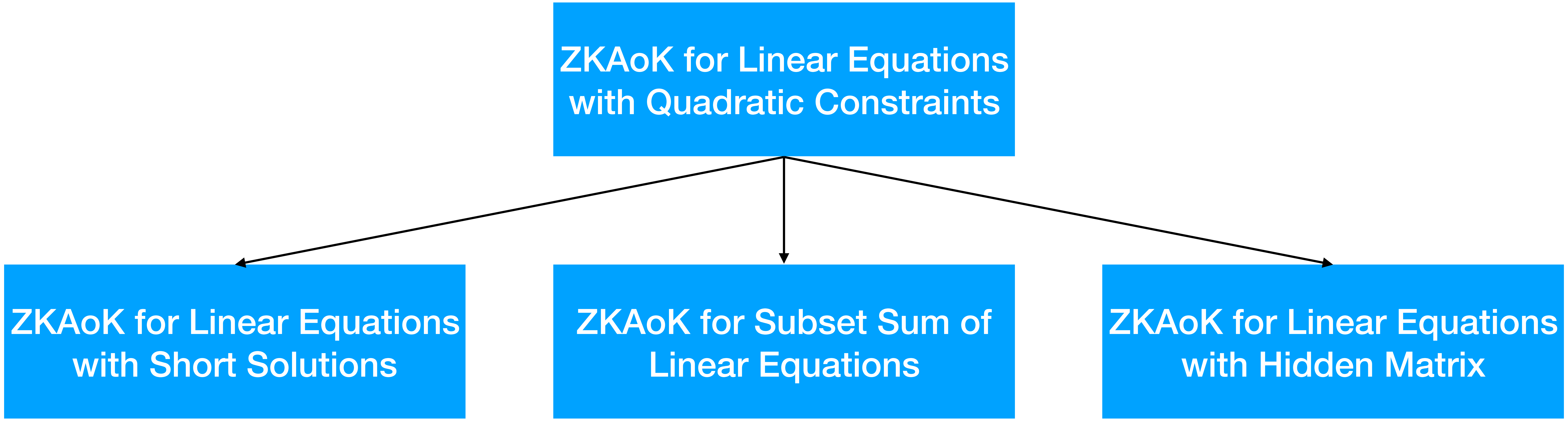
Zero-Knowledge Arguments (of Knowledge) for Linear Equations with Hidden Matrix

Goal: $\begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \boldsymbol{v}$

$$u_{1,1} = A_{1,1} \cdot w_1, \quad u_{1,2} = A_{1,2} \cdot w_2$$
$$u_{2,1} = A_{2,1} \cdot w_1, \quad u_{2,2} = A_{2,2} \cdot w_2$$

New Goal: $\begin{cases} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} u_{1,1} \\ u_{1,2} \\ u_{2,1} \\ u_{2,2} \end{pmatrix} = \boldsymbol{v} & \text{Linear Equation} \\ u_{i,j} = A_{i,j} \cdot w_j & \text{Quadratic Constraints} \end{cases}$

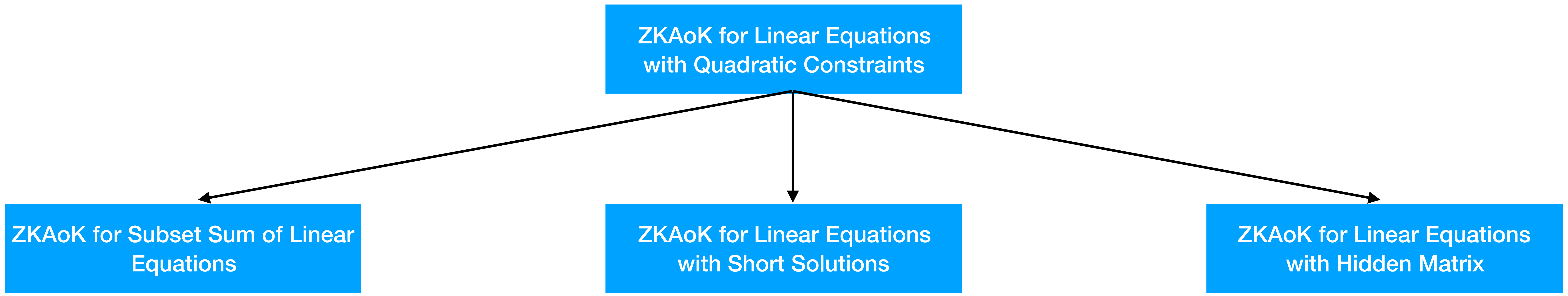
Summary


ZKAoK for Linear Equations with Quadratic Constraints
ZKAoK for Linear Equations with Short Solutions
ZKAoK for Subset Sum of Linear Equations
ZKAoK for Linear Equations with Hidden Matrix

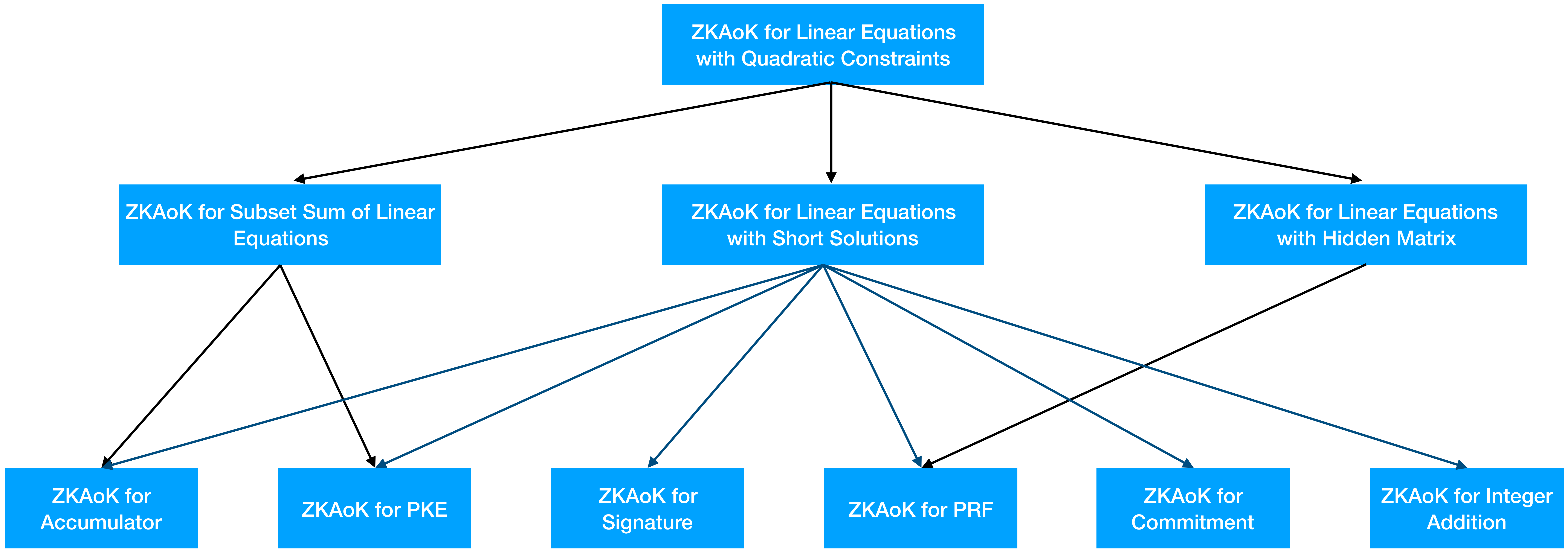
Outline

- The Main Protocol
- Applications of the Main Protocol
- Our Results☜

The Roadmap


ZKAoK for Linear Equations with Quadratic Constraints
ZKAoK for Subset Sum of Linear Equations
ZKAoK for Linear Equations with Short Solutions
ZKAoK for Linear Equations with Hidden Matrix

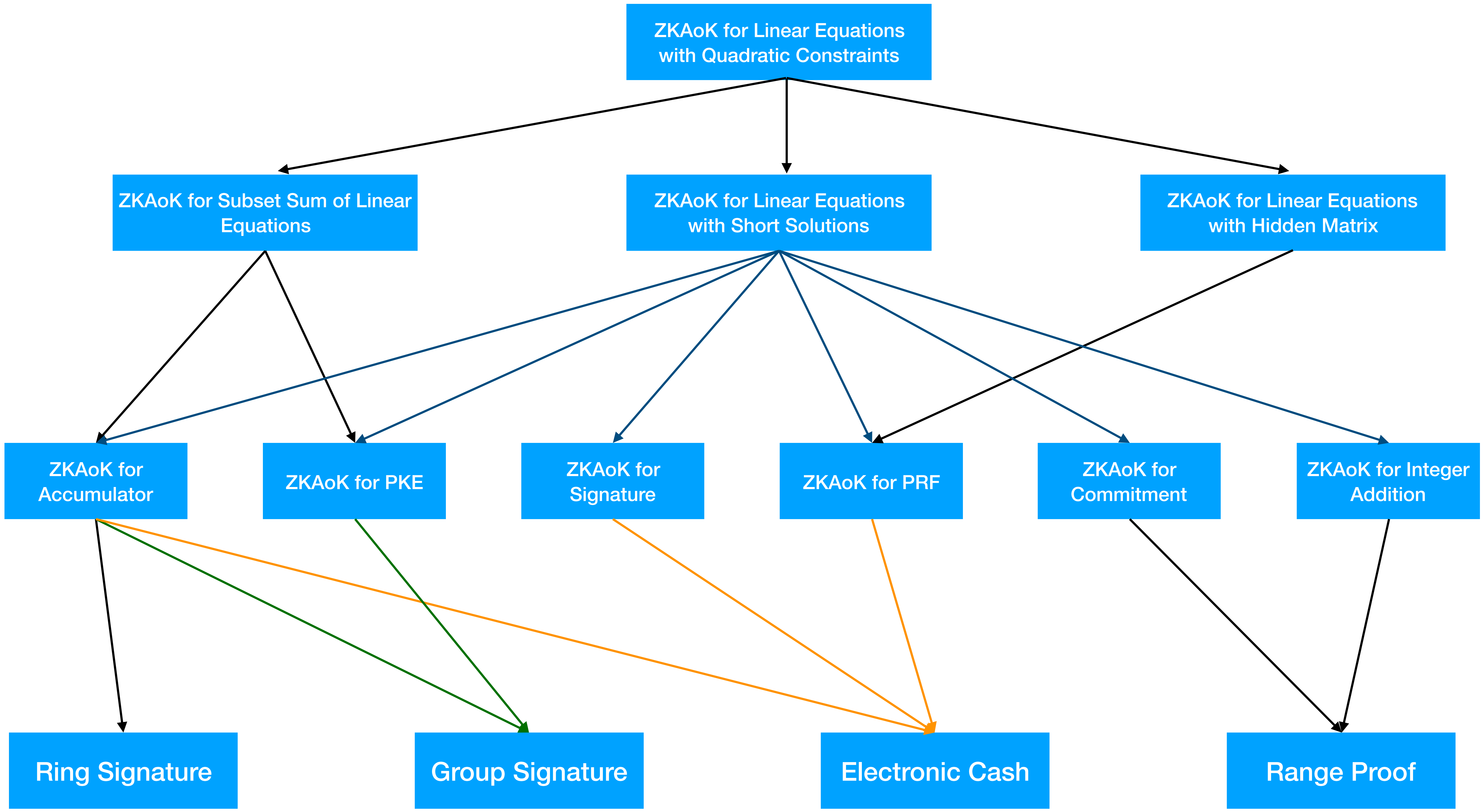
The Roadmap


ZKAoK for Linear Equations with Quadratic Constraints
ZKAoK for Subset Sum of Linear Equations
ZKAoK for Linear Equations with Short Solutions
ZKAoK for Linear Equations with Hidden Matrix
ZKAoK for Accumulator
ZKAoK for PKE
ZKAoK for Signature
ZKAoK for PRF
ZKAoK for Commitment
ZKAoK for Integer Addition

The Comparison

	Stern-Type	Our Solution	Fiat-Shamir with Abort
ZKAoK for PKE	[LNSW 13]	✔	[BCK+ 14]
ZKAoK for Commitment	[XXW 13]	✔	[BKLP 15]
ZKAoK for Signature	[LLM+ 16]	✔	[BCN 18]
ZKAoK for Accumulator	[LLNW 16]	✔	-
ZKAoK for (w)PRF	[LLNW 17]	✔	-

The Roadmap



ZKAoK for Linear Equations with Quadratic Constraints
ZKAoK for Subset Sum of Linear Equations
ZKAoK for Linear Equations with Short Solutions
ZKAoK for Linear Equations with Hidden Matrix
ZKAoK for Accumulator
ZKAoK for PKE
ZKAoK for Signature
ZKAoK for PRF
ZKAoK for Commitment
ZKAoK for Integer Addition
Ring Signature
Group Signature
Electronic Cash
Range Proof

The Comparison

	Stern-Type	Our Solution	FSwA (Ideal Lattice)
Ring Signature	47.3MB	4.24MB	1.41MB
Group Signature	61.5MB	6.94MB	0.58MB
E-Cash	$\approx$ 720TB	262MB	N/A
Range Proof	3.54MB	1.21MB	N/A

Communication Cost for typical applications $(2^{10}$ **users,** 80**-bit security**$)$.

More Efficient

THANK YOU!

HIRE ME!

orbbyrp@gmail.com