Lattice-Based Zero-Knowledge Arguments for Integer Relations

Benoît Libert[1] San Ling[2] **Khoa Nguyen**[2] Huaxiong Wang[2]

[1]CNRS and ENS Lyon, France

[2]Nanyang Technological University, Singapore

CRYPTO 2018, 20 August 2018

Zero-Knowledge Proofs/Arguments for Integer Relations

We study the problem of **proving in ZK and under standard lattice assumptions that large committed integers satisfy certain relations**.

⋆ **"Large"**: Committed integers X, Y, Z are of bit-size $L = \text{poly}(n)$.

Zero-Knowledge Proofs/Arguments for Integer Relations

We study the problem of **proving in ZK and under standard lattice assumptions that large committed integers satisfy certain relations**.

⋆ **"Large"**: Committed integers X, Y, Z are of bit-size $L = \mathsf{poly}(n)$.

⋆ **"Relations"**:

- Addition: $X + Y = Z$ over $\mathbb{Z}$
- Multiplication: $X \cdot Y = Z$ over $\mathbb{Z}$
- Range: $X \in [\alpha, \beta]$
- Set non-membership: $X \notin SET$, where SET is a public set.

Zero-Knowledge Proofs/Arguments for Integer Relations

We study the problem of **proving in ZK and under standard lattice assumptions that large committed integers satisfy certain relations**.

⋆ **"Large"**: Committed integers X, Y, Z are of bit-size $L = \text{poly}(n)$.

⋆ **"Relations"**:

- Addition: $X + Y = Z$ over $\mathbb{Z}$
- Multiplication: $X \cdot Y = Z$ over $\mathbb{Z}$
- Range: $X \in [\alpha, \beta]$
- Set non-membership: $X \notin SET$, where SET is a public set.

⋆ **"Assumptions"**: Solutions from DL/strong-RSA, e.g.

- $+$ and $\times$: Fujisaki-Okamoto (C'97), Damgård-Fujisaki (AC'02), Lipmaa (AC'03), Couteau et al. (EC'17)
- Range: Camenisch et al. (AC'08), Gonzalez-Ràfols (ACNS'17)
- Set non-membership: Camenisch-Lysyanskaya (C'02), Nakanishi et al. (PKC'09), Bayer-Groth (EC'13)

In the Lattice Setting...

The considered problem is still open!

- If we were to use known ZK proofs in ideal lattices to prove that X, Y, Z of bit-size $L = \text{poly}(n)$ satisfy $X + Y = Z$ over $\mathbb{Z}$:
  - Require to prove $X + Y = Z \bmod q$ for a large modulus $q = 2^{\text{poly}(n)}$.
  - Each ring element (used in the commitment) would cost thousand times L bits.
  - Proving that X, Y are small w.r.t. q (i.e., no reduction mod q occurs) and proving the additive relation would cost $k \cdot L$ bits, where $k \approx 10^5$.
  - Strong assumptions: at least sub-exponential approximation factors.
  - Ensuring soundness is non-trivial.

In the Lattice Setting...

The considered problem is still open!

- If we were to use known ZK proofs in ideal lattices to prove that X, Y, Z of bit-size $L = \text{poly}(n)$ satisfy $X + Y = Z$ over $\mathbb{Z}$:
  - Require to prove $X + Y = Z \bmod q$ for a large modulus $q = 2^{\text{poly}(n)}$.
  - Each ring element (used in the commitment) would cost thousand times L bits.
  - Proving that X, Y are small w.r.t. q (i.e., no reduction mod q occurs) and proving the additive relation would cost $k \cdot L$ bits, where $k \approx 10^5$.
  - Strong assumptions: at least sub-exponential approximation factors.
  - Ensuring soundness is non-trivial.
- Some limited forms of range proofs/arguments, e.g., $X \in [0, 2^m - 1]$.
- No efficient non-membership argument is known.

Our Results

Statistical ZK arguments for relations among committed integers, under mild assumptions in general (i.e., non-ideal) lattices.

- Integers of bit-size $L = \mathrm{poly}(n)$ are committed via the SIS-based commitment scheme by Kawachi-Tanaka-Xagawa (AC'08).
  - Small modulus: $q = \widetilde{\mathcal{O}}(\sqrt{L} \cdot n)$.
  - Weak assumption: SIVP_γ is hard for $\gamma = \widetilde{\mathcal{O}}(\sqrt{L} \cdot n)$.

Our Results

Statistical ZK arguments for relations among committed integers, under mild assumptions in general (i.e., non-ideal) lattices.

- Integers of bit-size $L = \mathrm{poly}(n)$ are committed via the SIS-based commitment scheme by Kawachi-Tanaka-Xagawa (AC'08).
  - Small modulus: $q = \widetilde{\mathcal{O}}(\sqrt{L} \cdot n)$.
  - Weak assumption: SIVP_γ is hard for $\gamma = \widetilde{\mathcal{O}}(\sqrt{L} \cdot n)$.
- Addition argument with comm. cost $\zeta + 20L \cdot \kappa$, where ζ is the cost of proving openings and $\kappa = \omega(\log n)$ - the number of repetitions.
- Range arguments with comm. cost $\zeta + \mathcal{O}(L) \cdot \kappa$, for ranges of size 2^L.
- Non-membership argument with comm. cost $\mathcal{O}(n \cdot \log |SET|)$.
- Multiplication arguments that can achieve sub-quadratic complexity $\mathcal{O}(L^{1.585})$ in both computation and comm. aspects.

Outline

Binary Additions with Carries

Main idea: View integer additions as binary additions **with carries**, then prove in ZK that they are done correctly.

Binary Additions with Carries

Main idea: View integer additions as binary additions **with carries**, then prove in ZK that they are done correctly.

Suppose that we add two bits x and y with carry-in c_{in} to obtain a bit z and carry-out c_{out}.

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
c_{in}	0	1	0	1	0	1	0	1
z	0	1	1	0	1	0	0	1
c_{out}	0	0	0	1	0	1	1	1

Then, the relations among these bits are captured by equations

$$z = x + y + c_{in} \mod 2, \qquad c_{out} = x \cdot y + z \cdot c_{in} + c_{in} \mod 2.$$

Additions of Committed Integers

Let $X = (x_{L-1}, \ldots, x_0)_2$, $Y = (y_{L-1}, \ldots, y_0)_2$, $Z = (z_L, z_{L-1}, \ldots, z_0)_2$.
For $i \in [0, L-1]$, let c_{i+1} be the carry-out of the i-th addition. We have:

$$\begin{aligned}
z_0 + x_0 + y_0 &= 0 \bmod 2 \\
c_1 + x_0 \cdot y_0 &= 0 \bmod 2 \\
z_1 + x_1 + y_1 + c_1 &= 0 \bmod 2 \\
c_2 + x_1 \cdot y_1 + z_1 \cdot c_1 + c_1 &= 0 \bmod 2 \\
&\vdots \\
z_{L-1} + x_{L-1} + y_{L-1} + c_{L-1} &= 0 \bmod 2 \\
z_L + x_{L-1} \cdot y_{L-1} + z_{L-1} \cdot c_{L-1} + c_{L-1} &= 0 \bmod 2.
\end{aligned}$$

Additions of Committed Integers

Let $X = (x_{L-1}, \ldots, x_0)_2$, $Y = (y_{L-1}, \ldots, y_0)_2$, $Z = (z_L, z_{L-1}, \ldots, z_0)_2$.
For $i \in [0, L-1]$, let c_{i+1} be the carry-out of the i-th addition. We have:

$$\begin{aligned}
z_0 + x_0 + y_0 &= 0 \bmod 2 \\
c_1 + x_0 \cdot y_0 &= 0 \bmod 2 \\
z_1 + x_1 + y_1 + c_1 &= 0 \bmod 2 \\
c_2 + x_1 \cdot y_1 + z_1 \cdot c_1 + c_1 &= 0 \bmod 2 \\
&\vdots \\
z_{L-1} + x_{L-1} + y_{L-1} + c_{L-1} &= 0 \bmod 2 \\
z_L + x_{L-1} \cdot y_{L-1} + z_{L-1} \cdot c_{L-1} + c_{L-1} &= 0 \bmod 2.
\end{aligned}$$

X, Y, Z are committed via [KTX-AC'08] $\rightarrow$ equations modulo q.

$$\begin{aligned}
\mathbf{a}_0 \cdot x_0 + \ldots + \mathbf{a}_{L-1} \cdot x_{L-1} + \sum \mathbf{b}_j \cdot r_{1,j} &= \mathbf{c}_x \bmod q; \\
\mathbf{a}_0 \cdot y_0 + \ldots + \mathbf{a}_{L-1} \cdot y_{L-1} + \sum \mathbf{b}_j \cdot r_{2,j} &= \mathbf{c}_y \bmod q; \\
\mathbf{a}_0 \cdot z_0 + \ldots + \mathbf{a}_L \cdot x_L + \sum \mathbf{b}_j \cdot r_{3,j} &= \mathbf{c}_z \bmod q.
\end{aligned}$$

Goal: Prove in ZK that we know the secret bits $x_i, y_i, z_i, c_i, r_{k,j}$ such that all equations mod 2 and mod q hold $\Leftarrow$ **Stern-like techniques**.

Stern-like Zero-Knowledge Techniques

Stern (Crypto'93): ZK protocol for the Syndrome Decoding problem.

- Use random permutations to prove constraints of secret witnesses satisfying matrix-vector equations.
- Recently adapted into the lattice setting.

Stern-like Zero-Knowledge Techniques

Stern (Crypto'93): ZK protocol for the Syndrome Decoding problem.

- Use random permutations to prove constraints of secret witnesses satisfying matrix-vector equations.
- Recently adapted into the lattice setting.

$\star$ Handling secret bits [Libert, Ling, N, Wang - EC'16]:

- For any $b \in \{0,1\}$, let $\overline{b} = 1 - b$ and $ext_2(b) = (\overline{b}, b) \in \{0,1\}^2$.
- For any $c \in \{0,1\}$, define P_c as the permutation transforming $\mathbf{v} = (v_0, v_1) \in \mathbb{Z}^2$ into $P_c(\mathbf{v}) = (v_c, v_{\overline{c}})$.

Observation:

$$\mathbf{v} = ext_2(b) \iff P_c(\mathbf{v}) = ext_2(b + c \bmod 2). \tag{1}$$

$\Rightarrow$ Proving knowledge of secret bit b that may appear in several correlated equations.

Stern-like Zero-knowledge Techniques (cont.)

⋆ Products of 2 secret bits [Libert, Ling, Mouhartem, N, Wang - AC'16]:

- For any bits b_1, b_2, define

$$ext_4(b_1, b_2) = (\overline{b}_1 \cdot \overline{b}_2, \overline{b}_1 \cdot b_2, b_1 \cdot \overline{b}_2, b_1 \cdot b_2) \in \{0,1\}^4.$$

- For any bits c_1, c_2, define T_{c_1,c_2} as the permutation transforming

$$\mathbf{v} = (v_{0,0}, v_{0,1}, v_{1,0}, v_{1,1}) \in \mathbb{Z}^4 \to T_{c_1,c_2}(\mathbf{v}) = (v_{c_1,c_2}, v_{c_1,\overline{c}_2}, v_{\overline{c}_1,c_2}, v_{\overline{c}_1,\overline{c}_2}).$$

Observation:

$$\mathbf{v} = ext_4(b_1, b_2) \iff T_{c_1,c_2}(\mathbf{v}) = ext_4(b_1 + c_1 \bmod 2, b_2 + c_2 \bmod 2). \quad (2)$$

$\Rightarrow$ Proving knowledge of product of secret bits $b_1 \cdot b_2$, where b_1, b_2 may appear in other equations.

Stern-like ZK Arguments for Integer Additions

⋆ Using permuting techniques, we can prove that all the secrets in the equations mod 2 and mod q are well-formed:

- Bits $x_i,\ y_i,\ z_i,\ c_i,\ r_{k,j}$
- Bit products $x_0 \cdot y_0,\ x_1 \cdot y_1, \ldots,\ x_{L-1} \cdot y_{L-1},\ z_1 \cdot c_1, \ldots,\ z_{L-1} \cdot c_{L-1}$.

⋆ To prove that the equations hold:

1. Transform all equations into $\mathbf{M}_2 \cdot \mathbf{s} = 0 \bmod 2$ and $\mathbf{M}_q \cdot \mathbf{t} = \mathbf{c} \bmod q$.
2. Random masking with vectors over $\mathbb{Z}_2$ and $\mathbb{Z}_q$:

$$\begin{aligned} \mathbf{M}_2 \cdot (\mathbf{s} + \mathbf{r}_s) &= \mathbf{M}_2 \cdot \mathbf{r}_s \bmod 2 \\ \mathbf{M}_q \cdot (\mathbf{t} + \mathbf{r}_t) - \mathbf{c} &= \mathbf{M}_q \cdot \mathbf{r}_t \bmod q. \end{aligned}$$

Inequalities and Range Arguments

Additions of non-negative integers $\Rightarrow$ Inequalities, ranges

- Inequalities
  - $X \leq Y$: There exists non-negative Z s.t. $X + Z = Y$.
  - $X < Y$: There exists non-negative Z s.t. $X + Z + 1 = Y$.

Inequalities and Range Arguments

Additions of non-negative integers $\Rightarrow$ Inequalities, ranges

- Inequalities
  - $X \leq Y$: There exists non-negative Z s.t. $X + Z = Y$.
  - $X < Y$: There exists non-negative Z s.t. $X + Z + 1 = Y$.
- Ranges $X \in [\alpha, \beta], [\alpha, \beta), (\alpha, \beta], [\alpha, \beta]$, where α, β may be hidden.
  - Two inequalities, e.g., $X \geq \alpha$ and $X < \beta$.

Inequalities and Range Arguments

Additions of non-negative integers $\Rightarrow$ Inequalities, ranges

- Inequalities
  - $X \leq Y$: There exists non-negative Z s.t. $X + Z = Y$.
  - $X < Y$: There exists non-negative Z s.t. $X + Z + 1 = Y$.
- Ranges $X \in [\alpha, \beta], [\alpha, \beta), (\alpha, \beta], [\alpha, \beta]$, where α, β may be hidden.
  - Two inequalities, e.g., $X \geq \alpha$ and $X < \beta$.

Next: Range arguments + additional techniques $\Rightarrow$ Set non-membership arguments.

Non-Membership Arguments

Problem

- Given a public set $SET = \{S_1, \ldots, S_M\}$ containing $M = \text{poly}(n)$ integers of bit-size n, where $S_1 < S_2 < \ldots < S_M$.
- Prove in ZK that committed integer X does not belong to SET.
- Target: Communication complexity $\mathcal{O}(\log M)$.

Non-Membership Arguments

Problem

- Given a public set $SET = \{S_1, \ldots, S_M\}$ containing $M = \text{poly}(n)$ integers of bit-size n, where $S_1 < S_2 < \ldots < S_M$.
- Prove in ZK that committed integer X does not belong to SET.
- Target: Communication complexity $\mathcal{O}(\log M)$.

Let $S_0 = 0^n$ and $S_{M+1} = 1^n$. Prove that $X \in (S_j, S_{j+1})$, for some j.

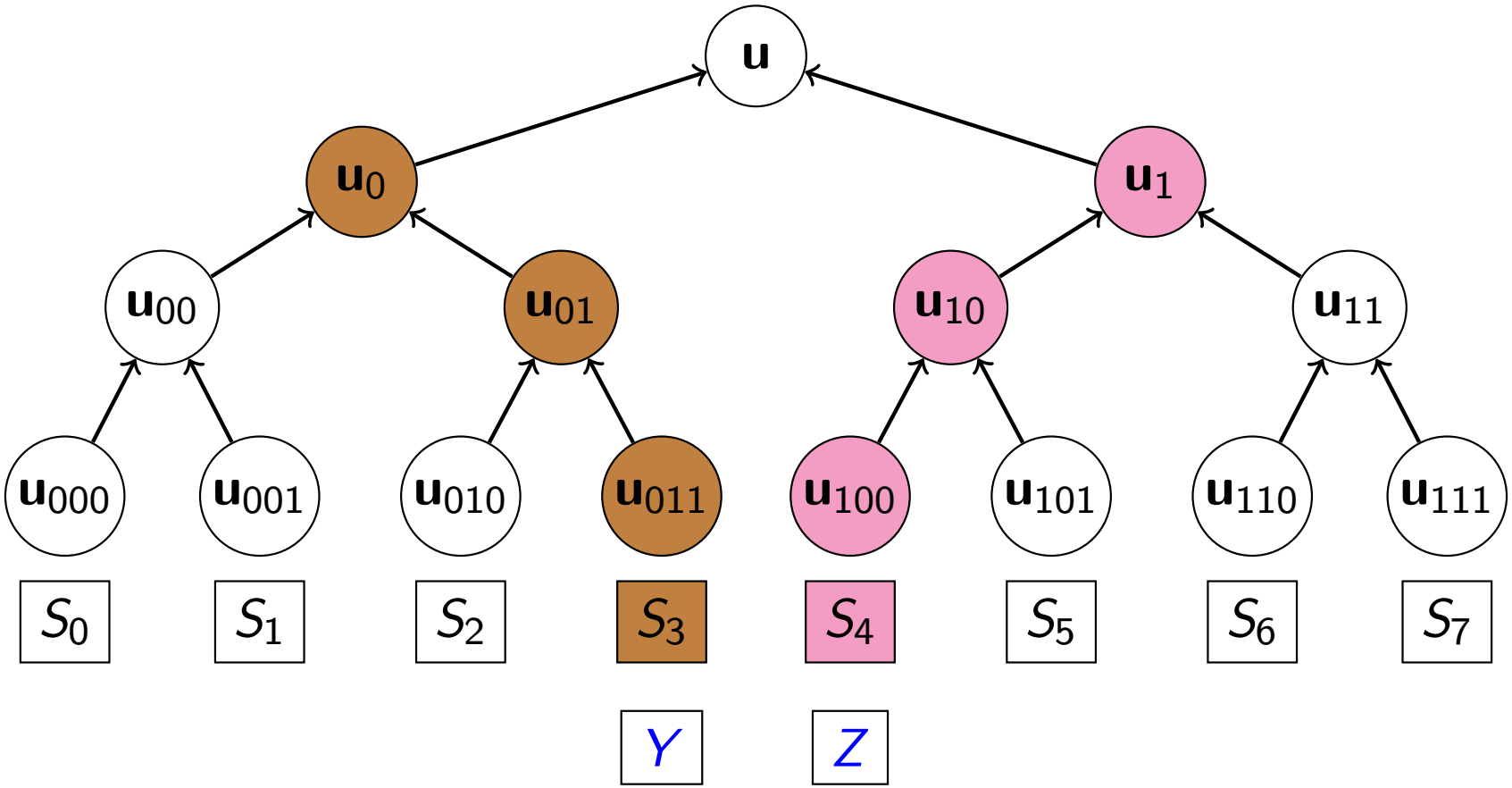
1. $Y < X < Z$, for some secret Y, Z.

   $\Leftarrow$ Range argument.

2. $Y, Z \in \{S_0, S_1, \ldots, S_M, S_{M+1}\}$ and Y, Z are "consecutive".

   $\Leftarrow$ Structures/techniques allowing $\mathcal{O}(\log M)$ membership argument.

Lattice-Based Merkle Hash Trees



- Build a Merkle tree over $\{S_0, S_1, \ldots, S_M, S_{M+1}\}$ and prove knowledge of 2 tree paths from leaves Y and Z to root $\mathbf{u}$ [LLNW-EC'16].
- Prove that the two tree paths are consecutive: $V = (011)_2$ and $W = (100)_2$ satisfy $V + 1 = W$ (integer addition).

Arguments for Integer Multiplications

Prove committed L-bit integers X, Y and $2L$-bit integer Z satisfy $XY = Z$.

- $\mathcal{O}(L)$ addition arguments $\rightarrow$ $\mathcal{O}(L^2)$ multiplication argument.
  - Straightforward; suitable for practical values of L, e.g., $L \leq 8000$
- Can we break the quadratic barrier? E.g., with Karatsuba algorithm?

Arguments for Integer Multiplications

Prove committed L-bit integers X, Y and $2L$-bit integer Z satisfy $XY = Z$.

- $\mathcal{O}(L)$ addition arguments $\rightarrow$ $\mathcal{O}(L^2)$ multiplication argument.
  - Straightforward; suitable for practical values of L, e.g., $L \leq 8000$
- Can we break the quadratic barrier? E.g., with Karatsuba algorithm?

$$\begin{cases} X = X_1 | X_0 \\ Y = Y_1 | Y_0 \end{cases} \Rightarrow \begin{cases} X = 2^{L/2} \cdot X_1 + X_0 \\ Y = 2^{L/2} \cdot Y_1 + Y_0. \end{cases}$$

Arguments for Integer Multiplications

Prove committed L-bit integers X, Y and $2L$-bit integer Z satisfy $XY = Z$.

- $\mathcal{O}(L)$ addition arguments $\rightarrow$ $\mathcal{O}(L^2)$ multiplication argument.
  - Straightforward; suitable for practical values of L, e.g., $L \leq 8000$
- Can we break the quadratic barrier? E.g., with Karatsuba algorithm?

$$\begin{cases} X = X_1 | X_0 \\ Y = Y_1 | Y_0 \end{cases} \Rightarrow \begin{cases} X = 2^{L/2} \cdot X_1 + X_0 \\ Y = 2^{L/2} \cdot Y_1 + Y_0. \end{cases}$$

Karasuba's observation: The number of partial products can be reduced from 4 to 3 $\rightarrow$ complexity $\mathcal{O}(L^{\log_2 3})$

$$X \cdot Y = (2^L - 2^{L/2})(X_1 Y_1) + (1 - 2^{L/2})(X_0 Y_0) + 2^{L/2}(X_1 + X_0)(Y_1 + Y_0).$$

Arguments for Integer Multiplications

Prove committed L-bit integers X, Y and $2L$-bit integer Z satisfy $XY = Z$.

- $\mathcal{O}(L)$ addition arguments $\rightarrow$ $\mathcal{O}(L^2)$ multiplication argument.
  - Straightforward; suitable for practical values of L, e.g., $L \leq 8000$
- Can we break the quadratic barrier? E.g., with Karatsuba algorithm?

$$\begin{cases} X = X_1 | X_0 \\ Y = Y_1 | Y_0 \end{cases} \Rightarrow \begin{cases} X = 2^{L/2} \cdot X_1 + X_0 \\ Y = 2^{L/2} \cdot Y_1 + Y_0. \end{cases}$$

Karasuba's observation: The number of partial products can be reduced from 4 to 3 $\rightarrow$ complexity $\mathcal{O}(L^{\log_2 3})$

$$X \cdot Y = (2^L - 2^{L/2})(X_1 Y_1) + (1 - 2^{L/2})(X_0 Y_0) + 2^{L/2}(X_1 + X_0)(Y_1 + Y_0).$$

Our method: Emulate the Karatsuba multiplication $X \cdot Y$ and prove that it gives Z in ZK $\rightarrow$ ZK argument for multiplicative relations with sub-quadratic communication/computation complexity $\mathcal{O}(L^{\log_2 3})$.

- Reduce relations of large integers to binary additions with carries.
- Proving binary operations in ZK using Stern-like techniques.
- Small modulus, weak lattice assumptions, scalability.

- Reduce relations of large integers to binary additions with carries.
- Proving binary operations in ZK using Stern-like techniques.
- Small modulus, weak lattice assumptions, scalability.

Some concrete estimations of comm cost for range argument $X \in [\alpha, \beta]$:

Range size $\beta - \alpha$	2^{1000}	2^{2000}	2^{4000}	2^{8000}
Commitment opening	3.16	3.65	4.63	6.59
Membership $X \in [\alpha, \beta]$	0.38	0.75	1.5	3
Total comm. cost	3.54 MB	4.4 MB	6.13 MB	9.59 MB

- Reduce relations of large integers to binary additions with carries.
- Proving binary operations in ZK using Stern-like techniques.
- Small modulus, weak lattice assumptions, scalability.

Some concrete estimations of comm cost for range argument $X \in [\alpha, \beta]$:

Range size $\beta - \alpha$	2^{1000}	2^{2000}	2^{4000}	2^{8000}
Commitment opening	3.16	3.65	4.63	6.59
Membership $X \in [\alpha, \beta]$	0.38	0.75	1.5	3
Total comm. cost	3.54 MB	4.4 MB	6.13 MB	9.59 MB

Thank you for your attention!