A Compressed $\Sigma$-Protocol Theory for Lattices

Joint work with Thomas Attema and Ronald Cramer

Lisa Kohl, Cryptology Group

CWI Scientific Meetings, 17 June
About me

Jun – Dec 2015
• Master’s thesis in the CWI Cryptology Group
• PhD at Karlsruhe Institute of Technology, Germany
• Postdoc at Technion, Israel

Since Oct 2020
• TT in the Cryptology Group

Research interest: Practical post-quantum secure multi-party computation

Input Privacy
Proof of Knowledge (PoK)

Goal: Alice wants to convince Bob that she knows $x$ ($y$, $x$)

Example: $y$: description of a sudoku instance  
$x$: solution to sudoku  
$s.t. x$ valid solution to sudoku
Proof of Knowledge (PoK)

Goal: Alice wants to convince Bob that she knows $x$

Desired properties:

- **Zero-knowledge:** Bob learns *nothing* beyond (in particular: doesn’t learn $x$)
- **Succinctness:** $|\text{Communication}| \ll |x|$

Yes (for all NP)!

“PCP theorem” AroraSafra’92, AroraLundMotwaniSudanSzedegy’92

Yes (for all NP)!

GoldwasserMicaliRackoff’85

This work: Constraint-Satisfiability

$f$: description of a function

$x$: input such that $f(x) = 0$

Possible?

Practical?
Proof of Knowledge (PoK)

**Goal:** Alice wants to convince Bob that she *knows* $x$

**Desired properties:**
- **Zero-knowledge:** Bob learns *nothing* beyond (in particular: doesn’t learn $x$)
- **Succinctness:** $|\text{Communication}| \ll |x|$

PCP-based approaches have inherently high concrete overhead

*Alternative:* Use “Bulletproof” folding [BCC+’16, BBB+’18, AC’20]

*Problem:* Not quantum-safe!

This work: Constraint-Satisfiability

$f$: description of a function

$x$: input such that $f(x) = 0$
Part I: Compressed Σ-Protocols [AttemaCramer’20]
Compressed $\Sigma$-protocols [AC’20]

- **Fact:** Can write every function $f$ as **arithmetic circuit** of *addition* (linear) and *multiplication* (non-linear) gates

- **High-level paradigm:**

  Solve linear instances first, and then linearize non-linear instances

1. **PoK for linear constraints** $f(x) = \langle L, x \rangle$ from *homomorphic commitments*
2. **Communication** $\sim \log |x|$ via *adaptation of Bulletproof PoK* [BCC+’16, BBB+’18]
3. **PoK for arbitrary constraints** via *arithmetic secret sharing*
(Succinct) Homomorphic Commitments

**Commitment scheme:** Commit to $x$ via $\square$ such that:

- **Hiding:** $\square$ hides $x$
- **Binding:** $\square$ can only be opened to $x$

**Additional required properties:**

- **Homomorphic:** $\square + c \cdot \square = \square$

- **Succinct:** $|\square| \ll |x|$

**Simplified:** Given $x$ can verify if commitment is commitment to $x$

**In this talk:** $x$ from large space, infeasible to guess
3-move protocol:
- **Completeness**: If the prover is honest and knows $x$, the verifier always accepts.
- **(Honest verifier) zero knowledge**: An accepting transcript can be efficiently simulated.
- **(Special) soundness**: Given accepting transcripts $(a, c, z), (a, c', z')$ one can efficiently extract a witness $x$.

Knowledge error: $\frac{1}{|C|}$

Verifier could have made up the transcript itself → did not *learn* anything from the interaction.

Output: 0: reject, or 1: accept.

If the prover can successfully answer on two different challenges it must *know* the witness.
**Σ-Protocols for Commitment Opening**

Sample random $r \leftarrow \mathbb{F}$

Set $z = r + c \cdot x$

**Goal:** Prove knowledge of opening $x \in \mathcal{X}$

- **First attempt:** Send $x$
- **Second attempt:** Send random $r$

Cannot be efficiently simulated $\rightarrow$ not zero knowledge

Does not allow to extract witness $\rightarrow$ not special sound
Towards Compressed Σ-Protocols [AC'20]

**Goal:** Prove knowledge of opening $x \in \mathbb{F}^n$

Sample random $r \leftarrow \mathbb{F}^n$

Set $z = r + c \cdot x$

**Problem:** $|z| = |x| = n \cdot \log |\mathbb{F}|$

**Idea:** “Fold” $z = (z_1, z_2)$ as $z' := z_1 + d \cdot z_2$ and send $z'$

**Problem:** Bob can compute $z$ but not $z'$

New challenge!

How to verify??
Folding Commitments [BCC+’16, BBB+’18]

• **Recall:** $z' := z_1 + d \cdot z_2$

• **Observation:**

\[
\begin{pmatrix}
  (d \cdot z') \\
  z'
\end{pmatrix} = \begin{pmatrix}
  (d \cdot (z_1 + d \cdot z_2)) \\
  z_1 + d \cdot z_2
\end{pmatrix} = \begin{pmatrix}
  0 \\
  z_1
\end{pmatrix} + d \cdot \begin{pmatrix}
  z_1 \\
  z_2
\end{pmatrix} + d^2 \cdot \begin{pmatrix}
  z_2 \\
  0
\end{pmatrix}
\]

- Can be computed from transcript
- Have to be provided by prover
Towards Compressed $\Sigma$-Protocols [AC’20]

**Goal:** Prove knowledge of opening $x \in \mathbb{F}^n$

- Sample random $r \leftarrow \mathbb{F}^n$
- Set $z = r + c \cdot x$

- $z' := z_1 + d \cdot z_2$

- $(d \cdot z') = \begin{pmatrix} 0 \\ z_1 \\ z_2 \end{pmatrix}$
  $+$ $d \cdot \begin{pmatrix} r \\ +c \cdot x \end{pmatrix}$ $+$ $d^2 \cdot \begin{pmatrix} z_2 \\ 0 \end{pmatrix}$

- **After $\log n$ repetitions:** Communication $\approx \log n \cdot \log |\mathbb{F}|$ (in $\log n$ rounds)
Instantiating Compressed Σ-Protocols [AC’20]

• **Discrete logarithm, strong-RSA**: (poly)logarithmic communication
• **Knowledge of exponent assumption**: constant communication
• **Assumptions in pairing groups**: direct ZK for bilinear circuits [ACR’20]
⇒ All broken by quantum computer

Towards quantum-safe Σ-protocol theory:
• Have to build on quantum-safe assumption
Part II: Compressed Σ-Protocols from Lattices
(Module-)Short Integer Solution ((M-)SIS)

• **(Module-)SIS Assumption:** It is difficult to find short integer solution $s$ with $\|s\| < \beta$ and $A \cdot s = 0$ (over ring $R := \mathbb{Z}_q [X]/(f(X))$).

Public = Easy to solve without $\|s\| < \beta$ and Believed to be hard to break even with a quantum computer
Homomorphic Commitments from MSIS

- **Hiding**: ✓ (when using randomness)
- **Binding**: ✓ (based on MSIS)
- **Homomorphic**: ✓
- **Succinct**: ✓

$x = \text{Simplified}$

$x$ has to be small, e.g., in binary representation.
This Work

Lattice-based instantiation of compressed $\Sigma$-protocol theory

• **Idea:** Instantiate with MSIS-based commitment scheme
  $\Rightarrow$ general constraint zero-knowledge with (poly-)logarithmic communication?

• **What goes wrong?**
Towards Compressed $\Sigma$-Protocols for Lattices

Problem: Protocol allows to extract $x'$ s.t. $x' = x$

(Standard-)Solution: change distribution of $r, c, d$

In particular: Require $(c - c')^{-1}$ small for all $c, c' \in C$

Goal: Prove knowledge of opening $x \in R^n$, $\|x\| < \beta$

Sample random $r \leftarrow R^n$

Set $z = r + c \cdot x$

Without additional guarantee $\|x'\| < \beta'$ meaningless!!
Towards Compressed $\Sigma$-Protocols for Lattices

**Main challenge:**
- $\log n$-round $\Sigma$-protocols more challenging than 3-round $\Sigma$-protocols

**Previously:**
- No *tight* extractor analysis for $\log n$-round $\Sigma$-protocols
- No suitable *parallel repetition theorem* for multi-round PoKs

**Require:** Require $(c - c')^{-1}$ small for all $c, c' \in C$

$|C| \text{ small (e.g., } C = \{0, 1\} \text{)}$  

Knowledge error $1/|C|$ large!!

Need sequential or parallel repetition
Compressed $\Sigma$-protocols for lattices:

**Motivation:** Practical quantum-safe succinct zero-knowledge PoK

**This work:**
- Abstract framework to uniformize & simplify analysis
- Tight extractor analysis (also improving non-lattice instantiations)
- New parallel repetition theorem for PoKs (recently improved by [AttemaFehr'21])
- Adaptation of linearization techniques to work over rings

Open questions:
- Improve concrete parameters
- Give quantum proof of security

Thank you!!