A Compressed Σ-Protocol Theory for Lattices

Thomas Attema and Ronald Cramer and Lisa Kohl

August 17, 2021

Setting - Proving General Constraints in Zero-Knowledge

ZK for General Constraint-Satisfiability:

- *Prove knowledge of commitment opening x such that $f(x) = 0$; i.e., x is f-constrained.*
- *Zero-Knowledge (ZK): no info released except veracity of claim.*

Goal:

- Low communication *for general f: minimize number of bits transmitted.*
- *Lattice-based.*
- *Commit-and-Prove.*

Prior Work - Compressed Σ-Protocol Theory (CRYPTO 2020 [AC20])

High-Level Paradigm:

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

1. Natural Σ-protocol for *linear* constraints.
   - Σ-protocol theory is a well-established, widely-used basis for zero-knowledge proofs.
   - E.g., general-constraint ZK: $O(|C|) \cdot \kappa$ communication [CD97].

$$[\mathbf{x}] \text{ s.t. } L(\mathbf{x}) = y$$

$$\begin{array}{ccc} \mathcal{P} & & \mathcal{V} \\ & \xrightarrow{[\mathbf{r}], L(\mathbf{r})} & \\ & \xleftarrow{c} & \\ \mathbf{z} = \mathbf{r} + c\mathbf{x} & \xrightarrow{\mathbf{z}} & \text{Accept?} \end{array}$$

2. Adaptation of Bulletproof PoK [BCC+16, BBB+18].
   - Bulletproofs core: recursive PoK for *quadratic* relations $\implies$ logarithmic communication.
   - Repurposed as a *blackbox* compression for Σ-protocol 1.

Prior Work - Compressed Σ-Protocol Theory (CRYPTO 2020 [AC20])

3. Linearization strategy to handle non-linear constraints in a black-box manner.
   - Using arithmetic secret-sharing.

4. Instantiations.
   - *Logarithmic-communication*: DL, strong-RSA (class groups, RSA + set-up).
   - **Constant-communication**: Knowledge of Exponent Assumption.
   - Pairing based languages (bilinear circuit model) [ACR20].

Lattice instantiation?

This Work

Lattice-based Instantiation of Compressed Σ-Protocol Theory

Homomorphic Ring-SIS based commitment scheme
$\implies$ circuit ZK with polylogarithmic communication.

Challenges and our contributions:

1. Soundness slack, approximation factor, rejection sampling (non-abort SHVZK), ...

- Also encountered in lattice instantiations of standard Σ-protocols.
- Careful analysis/instantiation required: propagation through the logarithmically many rounds of compressed Σ-protocols.
- **Our contribution**: *Abstract framework capturing various design choices and uniformizing/simplifying analysis.*
  - In contrast, many other works are tailored to specific lattice instantiations.

2. Extractor Analysis.

- Lattice instantiations have much smaller challenges sets
  $\implies$ larger knowledge error.
- **Our contribution**: *tight extractor analysis.*
- Also better parameters for non-lattice instantiations.

3. Parallel Repetition.

- Parallel repetition is required to reduce knowledge error.
- **Our contribution**: *novel parallel repetition for PoKs.*

4. Linearizing non-linear lattice instances.

- Requires an arithmetic secret sharing over a ring instead of a field.
- **Our contribution**: *adaptation of existing linearization technique.*

Related Work - Sublinear Lattice-Based Circuit ZK

- Sublinear circuit ZK from lattice assumptions [BBC$^+$18].
  - Communication is not polylogarithmic.
- Lattice-based Bulletproofs [BLNS20]:
  - Restricted to proving knowledge of an SIS preimage.
  - Not zero-knowledge.
  - Tailored to specific lattice instantiation (power-of-two cyclotomic number fields).

Concurrent and independent work at CRYPTO 2021:

- Theory of sumcheck arguments with application to lattice-based succinct arguments [BCS21].
  - Alternative abstract framework.
  - Given our extractor analysis $\implies$ comparable parameters for circuit ZK.
- Upper and lower bounds for lattice-based succinct zero-knowledge [AL21].
  - Better parameters for certain protocols, impossibility results
  - Our work: Tight extractor analysis ($\kappa \leq 2 \log n/|C|$ vs. $\kappa \approx 8.16 \log n/|C|$)

Technical Overview

1. Soundness slack, approximation factor, rejection sampling (non-abort SHVZK), ...
2. Extractor Analysis
3. Parallel Repetition Theorem
4. Linearization Techniques

Extractor Analysis for $(2\mu + 1)$-Round Protocols

Knowledge extractor

- Input: Statement x and rewindable access to $\mathcal{P}$.
- Goal: Compute a witness w for statement x.

A protocol is *knowledge sound* if there exists an extractor with certain properties.

- Informally: The prover can only convince the verifier if it knows a witness.

$$
\begin{array}{ccc}
 & (x;w) \in R & \\
\mathcal{P}(x;w) & & \mathcal{V}(x) \\
 & \xrightarrow{\quad a_0 \quad} & \\
 & \xleftarrow{\quad c_1 \quad} & \\
 & \xrightarrow{\quad a_1 \quad} & \\
 & \vdots & \\
 & \xleftarrow{\quad c_\mu \quad} & \\
 & \xrightarrow{\quad a_\mu \quad} & \text{Accept/Reject}
\end{array}
$$

Two Equivalent Definitions for Knowledge Soundness

- $\epsilon(x)$: success probability of the prover on public input x.
- $\kappa(x)$: knowledge error of the protocol.

Definition (Standard Definition - Knowledge Soundness)

Knowledge extractor has expected runtime

$$\frac{\text{poly}(|x|)}{\epsilon(x) - \kappa(x)} .$$

Definition (Alternative Definition - Knowledge Soundness)

Knowledge extractor has expected polynomial runtime and success probability

$$\frac{\epsilon(x) - \kappa(x)}{\text{poly}(|x|)} .$$

Special Soundness

Alternative notion of soundness that is easier to handle.

- Typically much easier to prove special soundness than knowledge soundness.

Definition (Special-Soundness)

A 3-move protocol is *special-sound* if there exists an efficient algorithm that on input a two accepting transcripts (a, c, z) and (a, c', z') with $c \neq c'$ outputs a witness w for statement x.

Special-soundness implies knowledge soundness with knowledge error $1/N$, where N is the size of the challenge set.

Natural generalization of 2-special-soundness:

- k-special-soundness implies knowledge soundness with knowledge error

$$\frac{k-1}{N}.$$

Generalization from 3-round to $(2\mu + 1)$-round protocols

Informally: $(k_1, \ldots, k_\mu)$-special soundness if the protocol is k_i special sound with respect to the i-th challenge.

Our Result: $(k_1, \ldots, k_\mu)$-special soundness *tightly* implies knowledge soundness.

Prior works:

- Asymptotic analysis: exponential challenge set implies negl. knowledge error [BCC$^+$16].
  - No concrete knowledge error. Not applicable to lattice setting.
- Concrete analysis of the asymptotic approach [dPLS19, AL21].
  - Not tight ($\kappa \approx 8.16 \log n / |C|$, whereas we obtain $\kappa \leq 2 \log n / |C|$).

Our techniques:

- Alternative definition for knowledge soundness.
- Simplified extractor for 3-round protocols; sampling *with* replacement.
- In contrast to prior extractors, this extractor can be applied recursively to multi-round protocols.

Knowledge extractor for special sound protocols

Extractor $\mathcal{E}$ with rewindable black-box access to a prover:

Step 1. Query the prover on a random challenge c.
Step 2a. If prover fails, the extractor aborts.
Step 2b. Else the extractor keeps rewinding (fixing the prover's first message a) and sampling challenges *with* replacement until it has found a second accepting transcript or until it has exhausted all challenges.

Lemma (Runtime)

The expected number of queries to $\mathcal{P}$ from $\mathcal{E}$ is at most 2.

Lemma (Success Probability)

Extractor $\mathcal{E}$ succeeds with probability at least $\epsilon - 1/N$.

Expected Runtime

Random variable A indicates the prover's randomness.

- If A is fixed, so is the prover's first message.

Lemma (Runtime)

The expected number of queries to $\mathcal{P}$ from $\mathcal{E}$ is at most 2.

Intuition:

If the success probability ϵ of $\mathcal{P}$ is:

- "large", $\mathcal{E}$ will quickly find two transcripts,
- "small", w.h.p. $\mathcal{E}$ will abort after 1 query.

Expected Runtime

Random variable A indicates the prover's randomness.

- If A is fixed, so is the prover's first message.

Lemma (Runtime)

The expected number of queries to $\mathcal{P}$ from $\mathcal{E}$ is at most 2.

Proof.

Conditioned on $A = a$, Step 1 succeeds with probability

$$\epsilon_a := \Pr(\mathcal{P} \text{ succeeds } | A = a).$$

Step 2b is a negative hypergeometric experiment with expected value at most $1/\epsilon_a$.
Expected number of queries is at most

$$\sum_a \Pr(A = a) \left(1 + \epsilon_a \frac{1}{\epsilon_a}\right) = 2\,.$$

Success Probability

Lemma (Success Probability)

Extractor $\mathcal{E}$ succeeds with probability at least $\epsilon - 1/N$.

Intuition:

- **Step 1.** succeeds with probability ϵ.
- **Step 2.** succeeds if and only if there exists a second accepting challenge (for the same prover's randomness).

Success Probability

Lemma (Success Probability)

Extractor $\mathcal{E}$ succeeds with probability at least $\epsilon - 1/N$.

Proof.

Conditioned on $A = a$, success if step 1 is successful *and* if $\epsilon_a > 1/N$.

Hence, the success probability of the extractor equals

$$\sum_{a \mid \epsilon_a > 1/N} \Pr(A = a)\epsilon_a = \sum_{a} \Pr(A = a)\epsilon_a - \sum_{a \mid \epsilon_a \leq 1/N} \Pr(A = a)\epsilon_a \,,$$

$$\geq \epsilon - \frac{1}{N} \,,$$

$\square$

Multi-Round Extractor

Recursive application of the 3-round extractor.

- Careful analysis is required.

Theorem

A $(k_1, \dots, k_\mu)$-special sound protocol is knowledge sound with knowledge error

$$\kappa = 1 - \prod_{i=1}^{\mu} \left(1 - \frac{k_i - 1}{N_i}\right) \leq \sum_{i=1}^{\mu} \frac{k_i - 1}{N_i},$$

where N_i is the size of the i-th challenge set.

Tightness:

- Typically there exists a cheating strategy that succeeds with probability κ.

Conclusion

- First (non-PCP) lattice-based circuit ZK protocol with polylogarithmic communication.
  - Inherits the modularity of Compressed Σ-Protocol Theory.
  - Supports commit-and-prove.
  - Transparent (no trusted set-up).
- General and tight extractor analysis for $(k_1, \ldots, k_\mu)$-special-sound protocols.
- Novel parallel repetition theorem for proofs of knowledge.

Thanks!

Bibliography I

Thomas Attema and Ronald Cramer.
Compressed sigma-protocol theory and practical application to plug & play secure algorithmics.
In *CRYPTO (3)*, volume 12172 of *Lecture Notes in Computer Science*, pages 513–543. Springer, 2020.

Thomas Attema, Ronald Cramer, and Matthieu Rambaud.
Compressed sigma-protocols for bilinear circuits and applications to logarithmic-sized transparent threshold signature schemes.
IACR Cryptol. ePrint Arch., 2020:1447, 2020.

Martin Albrecht and Russell W. F. Lai.
Subtractive sets over cyclotomic rings: Limits of schnorr-like arguments over lattices.
In *CRYPTO 2021 (to appear)*, 2021.

Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Gregory Maxwell.
Bulletproofs: Short proofs for confidential transactions and more.
In *IEEE Symposium on Security and Privacy*, pages 315–334. IEEE Computer Society, 2018.

Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky.
Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits.
In *CRYPTO (2)*, volume 10992 of *Lecture Notes in Computer Science*, pages 669–699. Springer, 2018.

Bibliography III

Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit.
Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting.
In *EUROCRYPT (2)*, volume 9666 of *Lecture Notes in Computer Science*, pages 327–357. Springer, 2016.

Jonathan Bootle, Alessandro Chiesa, and Katerina Sotiraki.
Sumcheck arguments and their applications.
In *CRYPTO 2021 (to appear)*, 2021.

Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler.
A non-pcp approach to succinct quantum-safe zero-knowledge.
In *CRYPTO (2)*, volume 12171 of *Lecture Notes in Computer Science*, pages 441–469. Springer, 2020.

Ronald Cramer and Ivan Damgård.
Linear zero-knowledge - A note on efficient zero-knowledge proofs and arguments.
In *STOC*, pages 436–445. ACM, 1997.

Rafaël del Pino, Vadim Lyubashevsky, and Gregor Seiler.
Short discrete log proofs for FHE and ring-lwe ciphertexts.
In *Public Key Cryptography (1)*, volume 11442 of *Lecture Notes in Computer Science*, pages 344–373. Springer, 2019.