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].

2. Adaptation of Bulletproof PoK [BCC\(^+16\), BBB\(^+18\)].
   - Bulletproofs core: recursive PoK for quadratic relations \( \Longrightarrow \) logarithmic communication.
   - Repurposed as a blackbox compression for Σ-protocol 1.
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?*
Lattice-based Instantiation of Compressed $\Sigma$-Protocol Theory

Homomorphic Ring-SIS based commitment scheme

$\Rightarrow$ 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 $\Sigma$-protocols.
   - Careful analysis/instantiation required: propagation through the logarithmically many rounds of compressed $\Sigma$-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 ⇒ 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\textsuperscript{+}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 $\Rightarrow$ 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
Knowledge extractor

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

A protocol is \textit{knowledge sound} if there exists an extractor with certain properties.

- Informally: The prover can only convince the verifier if it knows a witness.
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.
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 $\epsilon - 1/N$.***
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 $\epsilon$ of $\mathcal{P}$ is:
- “large”, $\mathcal{E}$ will quickly find two transcripts,
- “small”, w.h.p. $\mathcal{E}$ will abort after 1 query.
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 $P$ from $E$ 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

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

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

Intuition:

- **Step 1.** succeeds with probability $\epsilon$.
- **Step 2.** succeeds if and only if there exists a second accepting challenge (for the same prover’s randomness).
**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 \textit{and} if $\epsilon_a > 1/N$.

Hence, the success probability of the extractor equals

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

$$\geq \epsilon - \frac{1}{N},$$
Multi-Round Extractor

Recursive application of the 3-round extractor.

- Careful analysis is required.

**Theorem**

A \((k_1, \ldots, k_\mu)\)-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 \(\kappa\).
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!
Thomas Attema and Ronald Cramer.
Compressed sigma-protocol theory and practical application to plug & play secure algorithmics.

Thomas Attema, Ronald Cramer, and Matthieu Rambaud.
Compressed sigma-protocols for bilinear circuits and applications to logarithmic-sized transparent threshold signature schemes.

Martin Albrecht and Russell W. F. Lai.
Subtractive sets over cyclotomic rings: Limits of schnorr-like arguments over lattices.
Bulletproofs: Short proofs for confidential transactions and more.

Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky.
Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits.

