Knowledge Soundness Analysis for Interactive (Oracle) Proofs

Thomas Attema
TNO & CWI

Lattices Meet Hashes Workshop — Lausanne
May 2, 2023

Based on unpublished work with Serge Fehr and Nicolas Resch.

Technical Overview

1. Preliminaries
2. Knowledge Extraction: IPs vs IOPs
3. Special-Soundness
4. Non-Special-Sound Protocols
5. Generalized Notion of Special-Soundness
6. Generic Extractor
7. Application to the FRI Protocol

Preliminaries - Interactive Proofs (IPs)

A (binary) relation is a set $R = \{(x; w)\}$ of statement-witness pairs.

Goal of an Interactive Proof (of Knowledge):

- *Prove that a statement x admits a witness, or*
- *Prove knowledge of a witness w for a public statement x.*

We only consider public-coin protocols, i.e., the verifier publishes all its randomness during the protocol execution.

$$(x; w) \in R$$

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

Preliminaries - Interactive *Oracle* Proofs (IOPs)

$$(x; w) \in R$$

$$\begin{array}{ccccc}
\mathcal{P}(x; w) & & \mathcal{V}(x) & & \text{Oracles} \\
 & \xrightarrow{\mathcal{O}^{a_0}} & & & \mathcal{O}^{a_0} \\
 & \xleftarrow{c_1} & & & \\
 & \xrightarrow{\mathcal{O}^{a_1}} & & & \mathcal{O}^{a_1} \\
 & \vdots & & & \\
 & \xleftarrow{c_\mu} & & & \\
 & \xrightarrow{\mathcal{O}^{a_\mu}} & & & \mathcal{O}^{a_\mu} \\
 & & & \xrightarrow{t_{i,j}} & \\
 & & & \xleftarrow{y_{i,j}} & y_{i,j} \leftarrow \mathcal{O}^{a_i}(t_{i,j}) \\
 & & \text{Accept/Reject} & &
\end{array}$$

Preliminaries - Compiling an IOP into an IP

Let $[\cdot]$ be a *binding* commitment scheme with local openings.

$$(x; w) \in R$$

$\mathcal{P}(x; w)$ $\mathcal{V}(x)$

$$\xrightarrow{[a_0]}$$

$$\xleftarrow{c_1}$$

$$\xrightarrow{[a_1]}$$

$$\vdots$$

$$\xleftarrow{c_\mu}$$

$$\xrightarrow{[a_\mu]}$$

$$\xleftarrow{t_{i,j}}$$

$$\xrightarrow[\text{Opening info}]{y_{i,j}}$$

Accept/Reject

Desirable Security Properties:

- Completeness: *Honest provers always succeed in convincing a verifier.*
- **(Knowledge) Soundness:** ***Dishonest provers (almost) never succeed.***
- Zero-Knowledge: *No information about the witness is revealed.*

- **Soundness**: When proving that a statement *admits* a witness.
- **Knowledge Soundness**: When proving *knowledge* of a witness.

Preliminaries - Knowledge Soundness

Knowledge soundness $\iff$ existence of a *knowledge extractor*.

Knowledge extractor

- Input: Statement x and oracle access to a prover $\mathcal{P}^*$ attacking the protocol.
- Goal: Compute a witness w for statement x.

Knowledge Extraction – Subtle Difference Between IPs and IOPs

IP: Answers to different queries to a dishonest prover $\mathcal{P}^*$ do **not** have to be consistent.

- Rewinding $\mathcal{P}^*$ and sending a different challenge c_i may result in a completely different message a_i (or oracle $\mathcal{O}^{a_i}$).

IOP: Answers to different queries to the oracles $\mathcal{O}^{a_i}$ produced by $\mathcal{P}^*$ have to be consistent.

- Queries to $\mathcal{O}^{a_i}$ on different subsets S and S' of the coordinates of a_i are guaranteed to be consistent, i.e., output is equal on the intersection $S \cap S'$.

$$(x; w) \in R$$

$$\begin{array}{ccccc}
\mathcal{P}(x; w) & & \mathcal{V}(x) & & \text{Oracles} \\
 & \xrightarrow{\mathcal{O}^{a_0}} & & & \mathcal{O}^{a_0} \\
 & \xleftarrow{c_1} & & & \\
 & \xrightarrow{\mathcal{O}^{a_1}} & & & \mathcal{O}^{a_1} \\
 & \vdots & & & \\
 & \xleftarrow{c_\mu} & & & \\
 & \xrightarrow{\mathcal{O}^{a_\mu}} & & & \mathcal{O}^{a_\mu} \\
 & & & \xrightarrow{t_{i,j}} & \\
 & & & \xleftarrow{y_{i,j}} & y_{i,j} \leftarrow \mathcal{O}^{a_i}(t_{i,j}) \\
 & & \text{Accept/Reject} & &
\end{array}$$

Knowledge Extractor

Hence, knowledge extraction can be (somewhat) easier for IOPs than for IPs.

- (Knowledge) soundness of the IOP + binding property of the commitment scheme
  $\Longrightarrow$ (knowledge) soundness of the compiled IP

- Binding property is typically computational
  $\Longrightarrow$ compilation degrades (knowledge) soundness to computational
  $\Longrightarrow$ the resulting IP is actually an *Interactive Argument*

We will focus on knowledge extraction for IPs:

1. This avoids the subtle difference between the different oracles the extractor can query;
2. In practice, IOPs are compiled into IPs anyway.

Two Equivalent Definitions for Knowledge Soundness

- $\epsilon(x, \mathcal{P}^*)$: success probability of $\mathcal{P}^*$ on public input x.
- $\kappa(|x|)$: knowledge error of the protocol.

Definition (Standard Definition - Knowledge Soundness)

If $\epsilon(x, \mathcal{P}^*) > \kappa(|x|)$, knowledge extractor extracts in expected runtime

$$\frac{\mathsf{poly}(|x|)}{\epsilon(x, \mathcal{P}^*) - \kappa(|x|)}.$$

Definition (Alternative Definition - Knowledge Soundness)

Knowledge extractor has expected polynomial runtime and success probability

$$\frac{\epsilon(x, \mathcal{P}^*) - \kappa(|x|)}{\mathsf{poly}(|x|)}.$$

Knowledge Soundness - Deterministic Provers

Lemma (Informal)

It is sufficient to consider deterministic provers $\mathcal{P}^*$.

Hence, $\mathcal{P}^*$ always starts with the same message.

Proof.

Let $\mathcal{P}^*$ be a probabilistic prover and $\mathcal{E}_{\text{det}}$ and extractor for deterministic provers.
The extractor $\mathcal{E}^{\mathcal{P}^*}$ samples the random coins r of $\mathcal{P}^*$ and runs $\mathcal{E}_{\text{det}}^{\mathcal{P}^*[r]}$.
It succeeds with probability

$$\mathbb{E}_r\left[\frac{\epsilon(x, \mathcal{P}^*[r]) - \kappa(|x|)}{\text{poly}(|x|)}\right] = \frac{\epsilon(x, \mathcal{P}^*) - \kappa(|x|)}{\text{poly}(|x|)} .$$

$\square$

Another Notion for IPs - Special-Soundness

- Introduced in the context of Σ-protocols.
- Easier to prove special-soundness than knowledge soundness.

$$(x; w) \in R$$

$$\begin{array}{ccc} \mathcal{P}(x; w) & & \mathcal{V}(x) \\ & \xrightarrow{\quad a \quad} & \\ & \xleftarrow{\quad c \quad} & \\ & \xrightarrow{\quad z \quad} & \text{Accept/} \\ & & \text{Reject} \end{array}$$

Definition

2-out-of-N special-soundness: Efficient algorithm to extract a witness w from 2 'colliding' protocol transcripts (a, c, z) and (a, c', z').

2-out-of-N special-soundness implies knowledge soundness with knowledge error $1/N$.

- $1/N$ matches the trivial cheating probability.

Natural Generalizations of Special-Soundness (1/2)

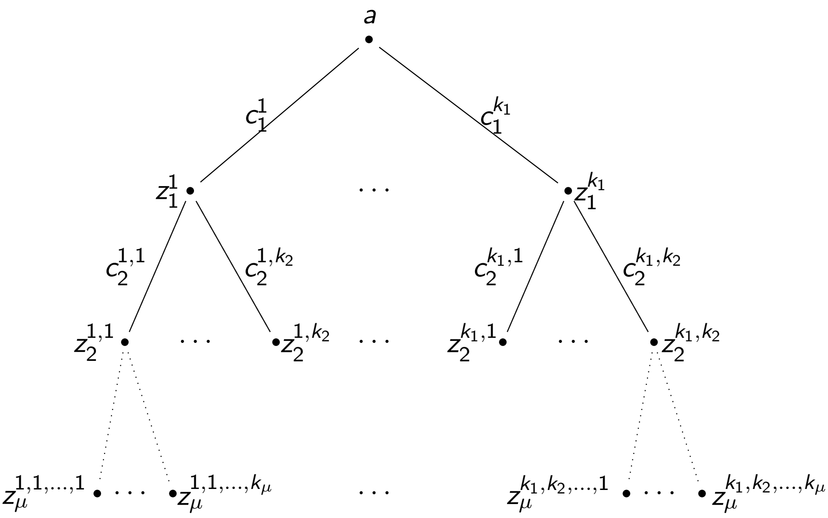
1. k-out-of-N special-soundness $\implies$ knowledge error $(k-1)/N$.
   - Requires k accepting transcripts;
   - Cheating prover (typically) succeeds if challenge hits $(k-1)$-subset guessed by the prover.

2. $(k_1, \ldots, k_\mu)$-out-of-$(N_1, \ldots, N_\mu)$ special-sound multi-round interactive proofs:
   - Require a tree of transcripts to *recursively* extract;
   - Typical cheating probability

$$\kappa = \mathrm{Er}(k_1, \ldots, k_\mu; N_1, \ldots, N_\mu) = 1 - \prod_{i=1}^{\mu} \left(1 - \frac{k_i - 1}{N_i}\right),$$

(the probability that the adversary guesses a $(k_i - 1)$-subset correctly for some $1 \leq i \leq \mu$).

$(k_1, \ldots, k_\mu)$-Tree of Transcripts of a $(2\mu + 1)$-Round Interactive Proof.



Extractor Analysis for Special-Sound Interactive Proofs

Extractor Analysis:

- Show that special-soundness implies *knowledge soundness*.

Results: Tight extractor analysis for

- (interactive) special-sound protocols [ACK21];
- the parallel repetition of special-sound protocols [AF22];

> t-fold parallel repetition reduces the knowledge error κ of special-sound interactive proofs to κ^t.

- the Fiat-Shamir transform of special-sound protocols [AFK22].

> The security loss of the Fiat-Shamir transformation of special-sound protocols is independent of the number of rounds.

Knowledge extractor for 2-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 *without* 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 $1 + \epsilon\frac{1}{\epsilon} = 2$.

Lemma (Success Probability)

Extractor $\mathcal{E}$ succeeds with probability ϵ if $\epsilon > 1/N$, i.e., it succeeds with probability at least $\epsilon - 1/N$.

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 κ.

Non-Special-Sound Interactive Proofs - Amortization (1/2)

- Sometimes additional structure is required to extract from sets of accepting transcripts.

Proving Knowledge of n Pre-Images $\mathbb{Z}_q$-Module Homomorphism Ψ

$$\Psi(x_1) = P_1 \,, \ldots \,, \Psi(x_n) = P_n$$

$\mathcal{P}(x_1, P_1, \ldots, x_n, P_n)$		$\mathcal{V}(P_1, \ldots, P_n)$
	$\xleftarrow{c_1,\ldots,c_n}$	$c_1, \ldots, c_n \leftarrow_R \mathbb{Z}_q$
$z = \sum_i c_i x_i$		
	$\xrightarrow{z}$	$\Psi(z) \stackrel{?}{=} \sum_i c_i P_i$

Non-Special-Sound Interactive Proofs - Amortization (2/2)

$$
\begin{array}{ccc}
\mathcal{P}(x_1, P_1, \ldots, x_n, P_n) & & \mathcal{V}(P_1, \ldots, P_n) \\
 & \xleftarrow{\quad c_1,\ldots,c_n \quad} & c_1, \ldots, c_n \leftarrow_R \mathbb{Z}_q \\
z = \sum_i c_i x_i & & \\
 & \xrightarrow{\quad z \quad} & \Psi(z) \stackrel{?}{=} \sum_i c_i P_i
\end{array}
$$

- To extract accepting transcripts $(\mathbf{c}_1, z_1), \ldots, (\mathbf{c}_n, z_n)$, s.t. $\mathbf{c}_1, \ldots, \mathbf{c}_n$ is a basis of $\mathbb{Z}_q^n$, are required.
- This IP is $(q^{n-1} + 1)$-special-sound;
  - Useless property because q is typically exponentially large, i.e., generic extractor is inefficient.

Non-Special-Sound Interactive Proofs - Merkle Tree Commitment

Proving Knowledge of Opening $x_1, \ldots, x_n$ of Merkle Tree Commitment P

$\mathcal{P}(x_1, \ldots, x_n, P)$		$\mathcal{V}(P)$
	$\xleftarrow{i_1,\ldots,i_k}$	$i_1, \ldots, i_k \leftarrow_R \{1, \ldots, n\}$
	$\xrightarrow[+\text{Validation Paths}]{x_{i_1},\ldots,x_{i_k}}$	Check local openings.

- Extraction requires accepting $(\mathbf{i}_1, \mathbf{x}_1), \ldots, (\mathbf{i}_t, \mathbf{x}_t)$, s.t. $\mathbf{i}_1, \ldots, \mathbf{i}_t$ cover $\{1, \ldots, t\}$.
- This IP is $\big((n-1)^k + 1\big)$-special-sound;

  $\Longrightarrow$ generic knowledge extractor is inefficient.
- If indices are chosen pairwise distinct, then the IP is $\big(\binom{n-1}{k} + 1\big)$-special-sound;

  $\Longrightarrow$ generic knowledge extractor is still inefficient for many k and n.

Non-Special-Sound Interactive Proofs - Parallel Repetition

t-fold parallel repetition of k-special-sound Σ-protocol.

$$
\begin{array}{ccc}
\mathcal{P}(w,x) & & \mathcal{V}(x) \\
& \xrightarrow{A_1,\ldots,A_t} & \\
& \xleftarrow{c_1,\ldots,c_t} & c_1,\ldots,c_t \leftarrow \mathcal{C} \\
& \xrightarrow{z_1,\ldots,z_t} & \text{Check all } t \text{ transcripts.}
\end{array}
$$

- Extraction requires accepting $(\mathbf{A},\mathbf{c}_1,\mathbf{z}_1),\ldots,(\mathbf{A},\mathbf{c}_T,\mathbf{z}_T)$, s.t. at least on of the t-coordinates contains k different challenges.
- This IP is $\left((k-1)^t+1\right)$-special-sound;

  $\implies$ generic knowledge extractor is inefficient.
- Different extractor analysis presented at CRYPTO'22 [ACF21], also applicable to multi-round special-sound interactive proofs.

A Generalized Special-Soundness Notion (1/2)

- The special soundness notion should capture the additional structure required to extract.

$\Gamma \subseteq 2^{\mathcal{C}}$ is a **monotone structure** if

- $A \subseteq B \subseteq \mathcal{C}$ and $A \in \Gamma$ implies $B \in \Gamma$;
- $\mathcal{C} \in \Gamma$;
- $\emptyset \notin \Gamma$.

A Generalized Special-Soundness Notion (2/2)

$\Gamma \subseteq 2^{\mathcal{C}}$ is a **monotone structure** if

- $A \subseteq B \subseteq \mathcal{C}$ and $A \in \Gamma$ implies $B \in \Gamma$'.

A 3-round interactive proof with challenge set $\mathcal{C}$ is **Γ-out-of-$\mathcal{C}$ special-sound**, if there exists an efficient algorithm to extract a witness from accepting transcripts $(a, c_1, z_1), \ldots, (a, c_k, z_k)$ with $\{c_1, \ldots, c_k\} \in \Gamma$.

Examples of Γ-special-sound IPs

Examples:

- k-special-sound IPs:
  - $\Gamma = \{S \subseteq \mathcal{C} : |S| \geq k\}$.
- Amortization:
  - $\mathcal{C} = \mathbb{Z}_q^n$;
  - $\Gamma = \{S \subseteq \mathbb{Z}_q^n : \mathsf{span}(S) = \mathbb{Z}_q^n\}$.
- Merkle tree IP:
  - $\mathcal{C} = \{A \subseteq \{1, \ldots, n\} : |A| \leq k\}$;
  - $\Gamma = \{S \subseteq \mathcal{C} : \cup_{A \in S} A = \{1, \ldots, n\}\}$.

Next Step: Extractor for Γ-Special-Sound IPs (1/2)

Key Observation:

- At any stage the extractor can partition $\mathcal{C}$ into a set of "useful" and "useless" challenges.

Suppose the extractor has found accepting transcripts for challenges $A \subseteq \mathcal{C}$ with $A \notin \Gamma$.

The function $U_\Gamma(A)$ defines the useful challenges.

Examples:

- k-special-sound IPs:
  - $U_\Gamma(A) = \mathcal{C} \setminus A$.
- Amortization:
  - $\mathcal{C} = \mathbb{Z}_q^n$;
  - $U_\Gamma(A) = \mathcal{C} \setminus \text{span}(A)$.
- Merkle tree IP:
  - $\mathcal{C} = \{S \subseteq \{1, \ldots, n\} : |S| \leq k\}$;
  - $U_\Gamma(A) = \{B \in \mathcal{C} : B \not\subseteq \cup_{S \in A} S\}$.

Next Step: Useful Challenges

We have to be careful when formally defining the useful challenge function U_Γ.

<u>Formal Definition</u>

$$U_\Gamma : 2^{\mathcal{C}} \to 2^{\mathcal{C}}, \quad S \mapsto \{c \in \mathcal{C} \setminus S : \exists A \in \Gamma \text{ s.t. } S \subset A \wedge A \setminus \{c\} \notin \Gamma\}$$

Next Step: Extractor for Γ-Special-Sound IPs (2/2)

We adapt the extractor for k-special-sound IPs.

- This adaptation does not work for the knowledge extractor from [ACK21];
- It requires the extractor introduced to handle parallel repetition [AF22].

k-special-sound IPs:

- Rewind and sample new challenge from $\mathcal{C} \setminus A$;
- (A is the set of challenges for which the extractor has already found accpeting transcripts).

Γ-special-sound IPs:

- Rewind and sample new challenge from $U_\Gamma(A)$.

Properties of the Knowledge Extractor

Expected Run-Time:
The extractor $\mathcal{E}^{\mathcal{P}^*}$ makes (in expectation) at most $2K_\Gamma - 1$ queries to $\mathcal{P}^*$, where

$$K_\Gamma := \max\left\{ k \in \mathbb{N}0 : \begin{array}{c} \exists c_1, \ldots, c_k \in \mathcal{C} \text{ s.t.} \\ c_i \in U_\Gamma\big(\{c_1, \ldots, c_{i-1}\}\big) \ \forall i \end{array} \right\},$$

Success Probability:
The extractor succeeds with probability

$$\frac{\delta_\Gamma(\mathcal{P}^*)}{K_\Gamma} \geq \frac{\epsilon(\mathcal{P}^*) - \kappa_\Gamma}{K_\Gamma(1 - \kappa_\Gamma)},$$

where $\kappa_\Gamma = \max_{S \notin \Gamma} \frac{|S|}{|\mathcal{C}|}$.

- This proves knowledge soundness if K_Γ is $poly(|x|)$.

Examples

- k-special-sound IPs:
  - Original special-soundness parameter k.
  - $K_\Gamma = k$.

- Amortization:
  - $\mathcal{C} = \mathbb{Z}_q^n$;
  - Original special-soundness parameter $q^{n-1} + 1$;
  - $K_\Gamma = n$.

- Merkle tree IP:
  - Original special-soundness parameter $(n-1)^k + 1$.
  - $K_\Gamma = n - k + 1$.

- t-fold parallel repetition of k-special-sound IP:
  - Original special-soundness parameter $(k-1)^t + 1$.
  - $K_\Gamma = (k-1)^t + 1$.
  - This example still requires another approach [AF22].

Multiround Interactive Proofs

The approach naturally generalizes to multi-round interactive proofs:

$(\Gamma_1, \ldots, \Gamma_\mu)$-out-of-$(\mathcal{C}_1, \ldots, \mathcal{C}_\mu)$ special-soundness.

The FRI-Protocol: An IOP of Proximity (1/2)

Notation:

- $0 \leq \rho \leq 1$
- $S \subseteq \mathbb{F}$
- $n = |S| = 2^{\mu}$
- $f(X) \in \mathbb{F}[X]$ of degree $< \rho n = 2^k$

Then $f(S) \in \mathbb{F}^n$ is a Reed-Solomon codeword, i.e., $f(S) \in \mathrm{RS}[\mathbb{F}, S, \rho]$.

The FRI protocol aims to prove that a polynomial $g \colon S \to \mathbb{F}$ is of degree $< \rho n$.

- s.t. the verifier does not need to query g too often.

Hence, the FRI-protocol aims to prove that $g(S) \in \mathrm{RS}[\mathbb{F}, S, \rho]$.

It is actually an IOP of **proximity**, i.e., it proves that $g(S)$ has relative Hamming distance at most $0 \leq \delta < 1$ to $\mathrm{RS}[\mathbb{F}, S, \rho]$.

The FRI-Protocol: An IOP of Proximity (2/2)

FRI-folding Mechanism (applied recursively).

$\mathcal{P}$	$f\colon S \to \mathbb{F}$ $\mathcal{O}^{f(S)}$	$\mathcal{V}$
$g(x^2) = \dfrac{f(x)+f(-x)}{2} + c\dfrac{f(x)-f(-x)}{2x}$	$\xleftarrow{\quad c \quad}$	$c \leftarrow_R \mathbb{F}$
	$\mathcal{O}^{g(S^2)}$	

FRI-Protocol: (Knowledge) Soundness Analysis

Trivial cheating probability:

$$1 - \delta\left(1 - \frac{1}{|\mathbb{F}|}\right)^{\log_2(\rho n)} \leq 1 - \delta + \frac{\log_2(\rho n)}{|\mathbb{F}|}$$

The FRI-protocol satisfies the generalized (multi-round) notion of special-soundness, implying knowledge error:

$$1 - \frac{\delta}{\rho n}\left(1 - \frac{1}{|\mathbb{F}|}\right)^{\log_2(\rho n)} \leq 1 - \frac{\delta}{\rho n} + \frac{\log_2(\rho n)}{|\mathbb{F}|}$$

FRI-Protocol: Prior Works + Better Special-Soundness Property[1]

The original analysis of FRI [BBHR18] gave soundness error:

$$\approx 1 - \delta + \frac{2n}{|\mathbb{F}|}$$

Crucial lemma shows that folding can only decrease relative Hamming distance to RS-code for small number of challenges.

Using this lemma a different special-soundness property can be derived, implying knowledge error

$$1 - \delta \prod_{i=1}^{\log(\rho n)} \left(1 - \frac{n}{2^{i-1}|\mathbb{F}|}\right) \leq 1 - \delta + \frac{2n}{|\mathbb{F}|}$$

[1]Some details have been omitted

Summary

- Generalized special-soundness notion also useful for IOP(P)s.
- Special-soundness implies knowledge soundness, instead of ordinary soundness.
- Special-soundness easier to prove than (knowledge) soundness.
- Random Oracle Model (ROM) not required in the analysis.
  - Only requires the commitment scheme to be binding.

Thanks!

Bibliography I

Thomas Attema, Ronald Cramer, and Serge Fehr.
Compressing proofs of k-out-of-n partial knowledge.
In *CRYPTO (4)*, volume 12828 of *Lecture Notes in Computer Science*, pages 65–91. Springer, 2021.

Thomas Attema, Ronald Cramer, and Lisa Kohl.
A compressed Σ-protocol theory for lattices.
In *CRYPTO (2)*, volume 12826 of *Lecture Notes in Computer Science*, pages 549–579. Springer, 2021.

Thomas Attema and Serge Fehr.
Parallel repetition of $(k_1, \ldots, k_\mu)$-special-sound multi-round interactive proofs.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO*, volume 13507 of *Lecture Notes in Computer Science*, pages 415–443. Springer, 2022.

Bibliography II

- Thomas Attema, Serge Fehr, and Michael Klooß.
  Fiat-shamir transformation of multi-round interactive proofs.
  In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography Conference (TCC)*, volume 13747 of *Lecture Notes in Computer Science*, pages 113–142. Springer, 2022.

- Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev.
  Fast reed-solomon interactive oracle proofs of proximity.
  In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*, volume 107 of *LIPIcs*, pages 14:1–14:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.