Generalized Special-Sound Interactive Proofs and their Knowledge Soundness

Thomas Attema and Serge Fehr and Nicolas Resch

TCC 2023
December 1, 2023
Taipei, Taiwan

Preliminaries - Interactive Proofs (IPs)

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.*

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

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

Preliminaries - Security Properties

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.*

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.

Another Notion for IPs - Special-Soundness

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

Another Notion for IPs - Special-Soundness

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

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').

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

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

Another Notion for IPs - Special-Soundness

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

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

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

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. k-out-of-N special-soundness $\implies$ knowledge error $(k-1)/N$.
   - Requires k accepting transcripts with common first message a.

Natural Generalizations of Special-Soundness

1. k-out-of-N special-soundness $\implies$ knowledge error $(k-1)/N$.
   - Requires k accepting transcripts with common first message a.

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 extract.

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

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

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)

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

- Extraction requires:
  - 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 $\mathbb{Z}_q^n$.

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

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

- Extraction requires:
  - 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 $\mathbb{Z}_q^n$.
- This IP is $(q^{n-1} + 1)$-special-sound;

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

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

- Extraction requires:
  - 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 $\mathbb{Z}_q^n$.
- This IP is $(q^{n-1} + 1)$-special-sound;
  - q is typically exponentially large $\implies$ 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

$\mathcal{P}(x_1, \ldots, x_n, P)$ | $\mathcal{V}(P)$

$$\xleftarrow{\quad i_1,\ldots,i_k \quad} \qquad i_1, \ldots, i_k \leftarrow_R \{1, \ldots, n\}$$

$$\xrightarrow[+\text{Validation Paths}]{\quad x_{i_1},\ldots,x_{i_k} \quad} \qquad \text{Check local openings.}$$

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:
  - Transcripts $(\mathbf{i}_1, \mathbf{x}_1), \ldots, (\mathbf{i}_t, \mathbf{x}_t)$ s.t. $\mathbf{i}_1, \ldots, \mathbf{i}_t$ cover $\{1, \ldots, t\}$.

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

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:
  - Transcripts $(\mathbf{i}_1, \mathbf{x}_1), \ldots, (\mathbf{i}_t, \mathbf{x}_t)$ 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.

This Work

- A more general notion of special-soundness,
  - capturing the above examples;
- A novel knowledge extractor;
- A generalization to multi-round interactive proofs;
- Parallel repetition theorem;
- An application to the FRI-protocol (IOP).

A Generalized Special-Soundness Notion

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

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

A Generalized Special-Soundness Notion

$\Gamma \subseteq 2^{\mathcal{C}}$ 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:
  - Challenge set $\mathcal{C}$;
  - $\Gamma = \{S \subseteq \mathcal{C} : |S| \geq k\}$.

Examples of Γ-special-sound IPs

Examples:

- k-special-sound IPs:
  - Challenge set $\mathcal{C}$;
  - $\Gamma = \{S \subseteq \mathcal{C} : |S| \geq k\}$.
- Amortization:
  - Challenge set $\mathbb{Z}_q^n$;
  - $\Gamma = \{S \subseteq \mathbb{Z}_q^n : \mathrm{span}(S) = \mathbb{Z}_q^n\}$.

Examples of Γ-special-sound IPs

Examples:

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

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.

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.

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:
  - $U_\Gamma(A) = \mathcal{C} \setminus A$.

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:
  - $\mathcal{C} = \mathbb{Z}_q^n$;
  - $U_\Gamma(A) = \mathcal{C} \setminus \mathrm{span}(A)$.

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

Useful Challenges

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

Formal Definition

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

Useful Challenges

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

Formal Definition

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

It holds that:

- $U_\Gamma(A) \cap A = \emptyset$ for all A;

Useful Challenges

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

Formal Definition

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

It holds that:

- $U_\Gamma(A) \cap A = \emptyset$ for all A;
- $U_\Gamma(B) \subseteq U_\Gamma(A)$ for all $A \subseteq B$;

Useful Challenges

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

Formal Definition

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

It holds that:

- $U_\Gamma(A) \cap A = \emptyset$ for all A;
- $U_\Gamma(B) \subseteq U_\Gamma(A)$ for all $A \subseteq B$;
- $U_\Gamma(A) = \emptyset$ for all $A \in \Gamma$.

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

Main idea.

- To find the ℓ-th transcript:
  rewind and sample new challenge from $U_\Gamma(\{c_1, \ldots, c_{\ell-1}\})$.

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

Main idea.

- To find the ℓ-th transcript:
  rewind and sample new challenge from $U_\Gamma(\{c_1, \ldots, c_{\ell-1}\})$.

More precisely, we adapt the extractor for k-special-sound IPs.

- Fails for the extractor from [ACK21];
- Works for the extractor introduced to handle parallel repetition [AF22].

Extractor Analysis

Crucial parameter in the analysis:

$$\boxed{t_\Gamma := \max\left\{ k \in \mathbb{N}_0 : \begin{array}{c} \exists c_1, \ldots, c_k \in \mathcal{C} \text{ s.t.} \\ c_i \in U_\Gamma\big(\{c_1, \ldots, c_{i-1}\}\big) \ \forall i \end{array} \right\}}$$

Extractor Analysis

Crucial parameter in the analysis:

$$\boxed{t_\Gamma := \max\left\{ k \in \mathbb{N}_0 : \begin{array}{c} \exists c_1, \ldots, c_k \in \mathcal{C} \text{ s.t.} \\ c_i \in U_\Gamma\big(\{c_1, \ldots, c_{i-1}\}\big) \ \forall i \end{array} \right\}}$$

Expected running time grows linearly in t_Γ:

- $\implies$ knowledge soundness if t_Γ is polynomial.

Examples

k_Γ : Threshold special-soundness parameters.

t_Γ : Refined special-soundness parameters.

	Challenge Set	k_Γ	t_Γ
k-special-sound Π	$\mathcal{C}$	k	k
Amortization	$\mathbb{Z}_q^n$	$q^{n-1}+1$	n
Merkle Tree Opening	$\{1,\dots,n\}^k$	$(n-1)^k+1$	$n-k+1$
t-fold Parallel of Π[1]	$\mathcal{C}^t$	$(k-1)^t+1$	$t\cdot(k-1)+1$

Another example: Local Special-Soundness

[1]Correction of the paper. Parallel repetition ***is*** appropriately captured by this generalization.

Summary

This presentation:

- Introduced a more general notion of special-soundness,
  - together with the tools to analyze this property;
- Claimed that it implies knowledge soundness.

In the paper:

- The knowledge extractor;
- A generalization to multi-round interactive proofs;
- Parallel repetition theorem;
- An application to the FRI-protocol (IOP).
  - With a discussion on the limitations of this approach.

Next:

- Analyzing the Fiat-Shamir transformation of $(\Gamma_1, \ldots, \Gamma_\mu)$-special-sound IPs.
  - Follow-up work to appear soon.
- Improve our FRI-extractor.
  - Open question.

Thanks!

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

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.