# Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Interactive Proofs

Edoardo Signorini
Joint work with Michele Battagliola, Riccardo Longo, Federico Pintore and Giovanni Tognolini

November 13, 2024

# Interactive Proofs

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

## Goal

Prove the knowledge of a witness $w$ for a public statement $x$.

## Public-coin

We consider interactive proofs where the challenges $c_i$ are sampled uniformly at random.

**Prover**$(x, w)$ **Verifier**$(w)$

$$\xrightarrow{\quad a_0 \quad}$$

$$\xleftarrow{\quad c_1 \quad}$$

$$\xrightarrow{\quad a_1 \quad}$$

$$\vdots$$

$$\xleftarrow{\quad c_\mu \quad}$$

$$\xrightarrow{\quad a_\mu \quad} \quad 1/0$$

# Properties

**Completeness**

Honest provers (almost) always succeed in convincing a verifier.

**Soundness**

A dishonest prover (almost) never convince a verifier that a false statement $x \notin L_R = \{x \mid \exists w : (x, w) \in R\}$ is true.

**Zero-knowledge**

No information about $w$ is revealed.

# Properties

**Completeness**

Honest provers (almost) always succeed in convincing a verifier.

**Soundness**

A dishonest prover (almost) never convince a verifier that a false statement $x \notin L_R = \{x \mid \exists w : (x, w) \in R\}$ is true.

**Zero-knowledge**

No information about $w$ is revealed.

Soundness does not mean the prover knows a witness!

# Knowledge Soundness (Informal)

Informally, a dishonest prover $\mathcal{P}^*$ (almost) never succeed without the knowledge of a witness $w$.

Knowledge soundness $\iff$ exists a knowledge extractor $\mathcal{E}$.

## Knowledge Extractor

**Input:** Statement $x$, rewindable oracle access to a prover $\mathcal{P}^*$.

**Output:** A witness $w$ such that $(x, w) \in R$.

# Knowledge Soundness

Consider any (dishonest) prover $\mathcal{P}^*$ against the protocol on statement $x$ and a knowledge extractor $\mathcal{E}$.

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

# Knowledge Soundness

Consider any (dishonest) prover $\mathcal{P}^*$ against the protocol on statement $x$ and a knowledge extractor $\mathcal{E}$.

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

**Knowledge Soundness**

If $\varepsilon(x, \mathcal{P}^*) > \kappa(|x|)$, then $\mathcal{E}$ extracts a witness $w$ such that $(x, w) \in R$ in expected running time at most

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

# Knowledge Soundness

Consider any (dishonest) prover $\mathcal{P}^*$ against the protocol on statement $x$ and a knowledge extractor $\mathcal{E}$.

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

**Knowledge Soundness**

If $\varepsilon(x, \mathcal{P}^*) > \kappa(|x|)$, then $\mathcal{E}$ extracts a witness $w$ such that $(x, w) \in R$ in expected running time at most

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

Knowledge Soundness is hard to prove in general!

# Special-Soundness

From now on we restrict to $\Sigma$-protocols (i.e, 3-move protocols) with challenge space $\mathsf{Ch} = \{0, 1, \dots, N-1\}$.

**2-out-of-N special-soundness**

There exists an efficient algorithm to extract a witness $w$ from 2 *colliding* accepting protocol transcripts $(a, c, z)$ and $(a, c', z')$ with $c \neq c' \in \mathsf{Ch}$.

# Special-Soundness

From now on we restrict to $\Sigma$-protocols (i.e, 3-move protocols) with challenge space $\mathsf{Ch} = \{0, 1, \dots, N-1\}$.

**2-out-of-N special-soundness**

There exists an efficient algorithm to extract a witness $w$ from 2 *colliding* accepting protocol transcripts $(a, c, z)$ and $(a, c', z')$ with $c \neq c' \in \mathsf{Ch}$.

(2-out-of-N) special-soundness implies knowledge soundness with $\kappa = 1/N$.

# Special-Soundness

From now on we restrict to Σ-protocols (i.e, 3-move protocols) with challenge space $\mathrm{Ch} = \{0, 1, \dots, N-1\}$.

**2-out-of-N special-soundness**

There exists an efficient algorithm to extract a witness $w$ from 2 *colliding* accepting protocol transcripts $(a, c, z)$ and $(a, c', z')$ with $c \neq c' \in \mathrm{Ch}$.

(2-out-of-N) special-soundness implies knowledge soundness with $\kappa = 1/N$.

**k-out-of-N special-soundness**

There exists an efficient algorithm to extract a witness $w$ from $k$ *colliding* accepting protocol transcripts $(a, c_1, z_1), \dots, (a, c_k, z_k)$ with pairwise distinct challenges $c_1, \dots, c_k \in \mathrm{Ch}$.

k-out-of-N special-soundness implies knowledge soundness with $\kappa = (k-1)/N$.

# Reducing the Knowledge Error

- In many applications we need the knowledge error to be negligible.
- The $t$-fold *parallel repetition* $\Pi^t$ of a $2$-out-of-$N$ special-sound $\Sigma$-protocol $\Pi$ is still a proof of knowledge with knowledge error $1/N^t$.

[1] *Attema and Fehr. "Parallel Repetition of $(k_1, \dots, k_\mu)$-Special-Sound Multi-round Interactive Proofs". CRYPTO 2022, Part I.*

# Reducing the Knowledge Error

- In many applications we need the knowledge error to be negligible.
- The $t$-fold *parallel repetition* $\Pi^t$ of a $2$-out-of-$N$ special-sound $\Sigma$-protocol $\Pi$ is still a proof of knowledge with knowledge error $1/N^t$.

What about $k$-out-of-$N$ special-sound $\Sigma$-protocols?

[1] *Attema and Fehr. "Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-round Interactive Proofs". CRYPTO 2022, Part I.*

# Reducing the Knowledge Error

- In many applications we need the knowledge error to be negligible.
- The $t$-fold *parallel repetition* $\Pi^t$ of a $2$-out-of-$N$ special-sound $\Sigma$-protocol $\Pi$ is still a proof of knowledge with knowledge error $1/N^t$.

What about $k$-out-of-$N$ special-sound $\Sigma$-protocols?

Basic reasoning for $k = 2$ is to observe that $\Pi^t$ is still $l$-special sound with $l = (k-1)^t + 1$.

[1] *Attema and Fehr. "Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-round Interactive Proofs". CRYPTO 2022, Part I.*

# Reducing the Knowledge Error

- In many applications we need the knowledge error to be negligible.
- The $t$-fold *parallel repetition* $\Pi^t$ of a $2$-out-of-$N$ special-sound $\Sigma$-protocol $\Pi$ is still a proof of knowledge with knowledge error $1/N^t$.

What about $k$-out-of-$N$ special-sound $\Sigma$-protocols?

Basic reasoning for $k = 2$ is to observe that $\Pi^t$ is still $l$-special sound with $l = (k-1)^t + 1$.
This reasoning does not apply in general, since $l$ grows exponentially in $t$ for $k > 2$.

[1] *Attema and Fehr. "Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-round Interactive Proofs". CRYPTO 2022, Part I.*

# Reducing the Knowledge Error

- In many applications we need the knowledge error to be negligible.
- The $t$-fold *parallel repetition* $\Pi^t$ of a $2$-out-of-$N$ special-sound $\Sigma$-protocol $\Pi$ is still a proof of knowledge with knowledge error $1/N^t$.

What about $k$-out-of-$N$ special-sound $\Sigma$-protocols?

Basic reasoning for $k = 2$ is to observe that $\Pi^t$ is still $l$-special sound with $l = (k-1)^t + 1$.
This reasoning does not apply in general, since $l$ grows exponentially in $t$ for $k > 2$.

**Theorem 2 [AF22]**[1]

If $\Pi$ has knowledge error $\kappa$, then $\Pi^t$ has knowledge error $\kappa^t$.

[1] *Attema and Fehr. "Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-round Interactive Proofs". CRYPTO 2022, Part I.*

# Fixed-Weight Repetition

- When we build signature schemes from interactive protocols, the size of the signature is typically dominated by the length of the responses.
- Some challenges may be matched by much smaller responses.

# Fixed-Weight Repetition

- When we build signature schemes from interactive protocols, the size of the signature is typically dominated by the length of the responses.
- Some challenges may be matched by much smaller responses.

There is a standard optimization for this scenario:

**Unbalanced Challenges**

Use a challenge string with a fixed small weight on unfavorable challenges.

- 👍 Fewer large responses to be sent $\implies$ smaller signature.
- 👎 More repetitions $\implies$ less efficient signing and verification.

# Fixed-Weight Repetition

- When we build signature schemes from interactive protocols, the size of the signature is typically dominated by the length of the responses.
- Some challenges may be matched by much smaller responses.

There is a standard optimization for this scenario:

**Unbalanced Challenges**

Use a challenge string with a fixed small weight on unfavorable challenges.

- Fewer large responses to be sent $\implies$ smaller signature.
- More repetitions $\implies$ less efficient signing and verification.

**Research Question**

*Does a fixed-weight repetition of a $k$-special-sound public-coin interactive proof enjoy knowledge soundness?*

# Knowledge Extractor on $k$-out-of-$N$ Special-Sound Protocols I

Let $\Pi$ be a $k$-out-of-$N$ special sound $\Sigma$-protocol, and let $\mathcal{P}^*$ be a *deterministic* prover attacking $\Pi$ on input a statement $x$

- $\mathcal{P}^*$'s first message $a$ is fixed.
- $\mathcal{P}^* : \mathsf{Ch} \to \{0,1\}^*, c \mapsto z$.
- $\mathcal{P}^*$ is successful if $(a, c, z)$ is an accepting transcript.

# Knowledge Extractor on $k$-out-of-$N$ Special-Sound Protocols I

Let $\Pi$ be a $k$-out-of-$N$ special sound $\Sigma$-protocol, and let $\mathcal{P}^*$ be a *deterministic* prover attacking $\Pi$ on input a statement $x$

- $\mathcal{P}^*$'s first message $a$ is fixed.
- $\mathcal{P}^* : \mathrm{Ch} \to \{0,1\}^*, c \mapsto z$.
- $\mathcal{P}^*$ is successful if $(a, c, z)$ is an accepting transcript.

$\mathcal{P}^*$'s behavior can be described by a binary vector $H(\mathcal{P}^*)$ indexed by the challenges $c_i$.

$$H(\mathcal{P}^*) = \begin{array}{c} \begin{matrix} c_0 & c_1 & c_2 & \dots & c_{N-2} & c_{N-1} \end{matrix} \\ \begin{pmatrix} 0 & 1 & 1 & \dots & 1 & 0 \end{pmatrix} \end{array}$$

- $H(\mathcal{P}^*)[c_i] = 1$ corresponds to $\mathcal{P}^*$ succeeding on input $c_i$
- $H(\mathcal{P}^*)[c_i] = 0$ corresponds to $\mathcal{P}^*$ failing on input $c_i$
- The success probability $\varepsilon(x, \mathcal{P}^*)$ of $\mathcal{P}^*$ on input $x$ is fraction of 1-entries.

# Knowledge Extractor on $k$-out-of-$N$ Special-Sound Protocols II

Basic extraction algorithm:

1. Samples random challenges $c_1$ until $H(\mathcal{P}^*)[c_1] = 1 \implies$ Expected time:

$$1/\varepsilon(x, \mathcal{P}^*).$$

# Knowledge Extractor on $k$-out-of-$N$ Special-Sound Protocols II

Basic extraction algorithm:

1. Samples random challenges $c_1$ until $H(\mathcal{P}^*)[c_1] = 1 \implies$ Expected time:
$$1/\varepsilon(x, \mathcal{P}^*).$$
2. Samples random challenges $c_2 \neq c_1$ until $H(\mathcal{P}^*)[c_2] = 1 \implies$ Expected time:
$$\leq \frac{1}{\varepsilon(x, \mathcal{P}^*) - 1/N}.$$

# Knowledge Extractor on $k$-out-of-$N$ Special-Sound Protocols II

Basic extraction algorithm:

1. Samples random challenges $c_1$ until $H(\mathcal{P}^*)[c_1] = 1 \implies$ Expected time:

$$1/\varepsilon(x, \mathcal{P}^*).$$

2. Samples random challenges $c_2 \neq c_1$ until $H(\mathcal{P}^*)[c_2] = 1 \implies$ Expected time:

$$\leq \frac{1}{\varepsilon(x, \mathcal{P}^*) - 1/N}.$$

$\vdots$

$k$. Samples random challenges $c_k \neq c_1, \dots, c_{k-1}$ until $H(\mathcal{P}^*)[c_k] = 1 \implies$ Expected time:

$$\leq \frac{1}{\varepsilon(x, \mathcal{P}^*) - (k-1)/N}.$$

# Knowledge Extractor on $k$-out-of-$N$ Special-Sound Protocols II

Basic extraction algorithm:

1. Samples random challenges $c_1$ until $H(\mathcal{P}^*)[c_1] = 1 \implies$ Expected time:
$$1/\varepsilon(x, \mathcal{P}^*).$$
2. Samples random challenges $c_2 \neq c_1$ until $H(\mathcal{P}^*)[c_2] = 1 \implies$ Expected time:
$$\leq \frac{1}{\varepsilon(x, \mathcal{P}^*) - 1/N}.$$

$\vdots$

$k$. Samples random challenges $c_k \neq c_1, \dots, c_{k-1}$ until $H(\mathcal{P}^*)[c_k] = 1 \implies$ Expected time:
$$\leq \frac{1}{\varepsilon(x, \mathcal{P}^*) - (k-1)/N}.$$

Expected runtime $\leq \frac{k}{\varepsilon(x,\mathcal{P}^*)-(k-1)/N} \implies$ knowledge error $(k-1)/N$.

# 2-Fold Parallel Repetition

Consider $\mathcal{P}^*$ attacking the $t = 2$-fold parallel repetition $\Pi^t$.
We can treat $\mathcal{P}^*$ as a (deterministic) function where the first message $(a_1, a_2)$ is fixed

$$\mathcal{P}^* : \mathsf{Ch} \times \mathsf{Ch} \to \{0,1\}^*, \qquad (c_1, c_2) \mapsto (z_1, z_2).$$

# 2-Fold Parallel Repetition

Consider $\mathcal{P}^*$ attacking the $t = 2$-fold parallel repetition $\Pi^t$.
We can treat $\mathcal{P}^*$ as a (deterministic) function where the first message $(a_1, a_2)$ is fixed

$$\mathcal{P}^* : \mathsf{Ch} \times \mathsf{Ch} \to \{0,1\}^*, \qquad (c_1, c_2) \mapsto (z_1, z_2).$$

$\mathcal{P}^*$ defines two (probabilistic) provers $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$ attacking a single invocation of $\Pi$

$$\mathcal{P}_1^* : c_1 \mapsto \begin{bmatrix} c_2 \xleftarrow{\$} \mathsf{Ch} \\ (z_1, z_2) \leftarrow \mathcal{P}^*(c_1, c_2) \end{bmatrix} \mapsto z_1$$

$$\mathcal{P}_2^* : c_2 \mapsto \begin{bmatrix} c_1 \xleftarrow{\$} \mathsf{Ch} \\ (z_1, z_2) \leftarrow \mathcal{P}^*(c_1, c_2) \end{bmatrix} \mapsto z_2$$

# 2-Fold Parallel Repetition

Consider $\mathcal{P}^*$ attacking the $t = 2$-fold parallel repetition $\Pi^t$.
We can treat $\mathcal{P}^*$ as a (deterministic) function where the first message $(a_1, a_2)$ is fixed

$$\mathcal{P}^* : \mathsf{Ch} \times \mathsf{Ch} \to \{0,1\}^*, \qquad (c_1, c_2) \mapsto (z_1, z_2).$$

$\mathcal{P}^*$ defines two (probabilistic) provers $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$ attacking a single invocation of $\Pi$

$$\mathcal{P}_1^* : c_1 \mapsto \begin{bmatrix} c_2 \leftarrow_\$ \mathsf{Ch} \\ (z_1, z_2) \leftarrow \mathcal{P}^*(c_1, c_2) \end{bmatrix} \mapsto z_1$$

$$\mathcal{P}_2^* : c_2 \mapsto \begin{bmatrix} c_1 \leftarrow_\$ \mathsf{Ch} \\ (z_1, z_2) \leftarrow \mathcal{P}^*(c_1, c_2) \end{bmatrix} \mapsto z_2$$

Notice that

$$\varepsilon(x, \mathcal{P}_i^*) = \Pr\big[V(c_i, \mathcal{P}_i^*(c_i)) = 1\big] = \Pr\big[V(c, \mathcal{P}^*(c)) = 1\big] = \varepsilon(x, \mathcal{P}^*),$$

where $c_i \leftarrow_\$ \mathsf{Ch}$ and $c \leftarrow_\$ \mathsf{Ch}^t$.

# Naive Extraction for 2-Fold Parallel Repetition

**Knowledge Extractor**

- Run the extractor $\mathcal{E}$ for $\Pi$ for both $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$.
- Hope that at least one of them succeed.
- The same analysis as before holds, even though $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$ are not deterministic.

# Naive Extraction for 2-Fold Parallel Repetition

**Knowledge Extractor**

- Run the extractor $\mathcal{E}$ for $\Pi$ for both $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$.
- Hope that at least one of them succeed.
- The same analysis as before holds, even though $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$ are not deterministic.

This does not work!

- The obtained knowledge error is still $(k-1)/N$.
- We hope to reduce knowledge error down to $(k-1)^2/N^2$.

# Solution of [AF22]

- Introduce a more fine-grained quality measure of success.
- Currently the quality of the extractor is expressed in terms of $\varepsilon(x, \mathcal{P}^*)$

# Solution of [AF22]

- Introduce a more fine-grained quality measure of success.
- Currently the quality of the extractor is expressed in terms of $\varepsilon(x, \mathcal{P}^*)$

**Punctured success probability**

Define the following measure

$$\delta_k(x, \mathcal{P}^*) = \min_{S \subset \mathsf{Ch}: |S| = k-1} \Pr\big[\mathcal{P}^*(C) \text{ succeeds} \mid C \notin S\big],$$

where $C$ is a random variable uniformly random in $\mathsf{Ch}$.

$\delta_k(x, \mathcal{P}^*)$ lower bounds the success probability of $\mathcal{P}^*$ when removing $k-1$ challenges.

# Solution of [AF22]

- Introduce a more fine-grained quality measure of success.
- Currently the quality of the extractor is expressed in terms of $\varepsilon(x, \mathcal{P}^*)$

**Punctured success probability**

Define the following measure

$$\delta_k(x, \mathcal{P}^*) = \min_{S \subset \mathrm{Ch} : |S| = k-1} \Pr\left[\mathcal{P}^*(C) \text{ succeeds} \mid C \notin S\right],$$

where $C$ is a random variable uniformly random in $\mathrm{Ch}$.

$\delta_k(x, \mathcal{P}^*)$ lower bounds the success probability of $\mathcal{P}^*$ when removing $k-1$ challenges.

**New Extractor**

On a single invocation $\mathcal{E}^{\mathcal{P}^*}$ has expected runtime

$$\leq \frac{k}{\delta_k(x, \mathcal{P}^*)} \leq \frac{k(1-\kappa)}{\varepsilon(x, \mathcal{P}^*) - \kappa},$$

where $\kappa = \frac{k-1}{N}$.

# Refined Parallel Repetition I

Consider again $\mathcal{P}^*$ attacking the $t = 2$-fold parallel repetition $\Pi^t$.
$\mathcal{P}^*$'s behaviour can be described by a binary matrix $H(\mathcal{P}^*)$:

$$H(\mathcal{P}^*) = \begin{array}{c} \\ \end{array} \begin{array}{cc} \begin{array}{cccccc} c_0 & c_1 & c_2 & \dots & c_{N-2} & c_{N-1} \end{array} & \\ \begin{pmatrix} 0 & 0 & 1 & \dots & 0 & 0 \\ 1 & 1 & 0 & \dots & 1 & 1 \\ 1 & 1 & 0 & \dots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 1 & \dots & 1 & 0 \\ 0 & 0 & 1 & \dots & 1 & 0 \end{pmatrix} & \begin{array}{c} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{N-2} \\ c_{N-1} \end{array} \end{array}$$

# Refined Parallel Repetition I

Consider again $\mathcal{P}^*$ attacking the $t = 2$-fold parallel repetition $\Pi^t$.
$\mathcal{P}^*$'s behaviour can be described by a binary matrix $H(\mathcal{P}^*)$:

$$H(\mathcal{P}^*) = \begin{array}{c} \begin{array}{cccccc} c_0 & c_1 & c_2 & \cdots & c_{N-2} & c_{N-1} \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 0 & 1 & \cdots & 1 & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{N-2} \\ c_{N-1} \end{array}$$

The behavior of $\mathcal{P}_1^*$ (resp. $\mathcal{P}_2^*$) can be described by looking at the columns (resp. rows) of $H(\mathcal{P}^*)$.

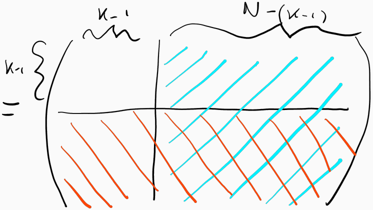
# Refined Parallel Repetition II

W.l.o.g assume $H(\mathcal{P}^*)$'s rows and columns are sorted based on fraction of 1-entries.

W.l.o.g assume $H(\mathcal{P}^*)$'s rows and columns are sorted based on fraction of 1-entries.

- $\delta_k(x, \mathcal{P}_1^*)$ is the fraction of 1-entries in blue region.
- $\delta_k(x, \mathcal{P}_2^*)$ is the fraction of 1-entries in red region.

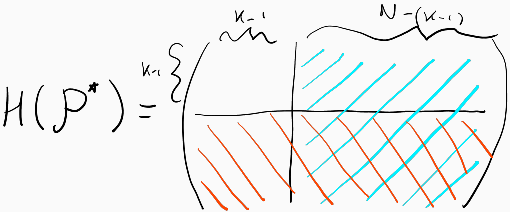
$H(\mathcal{P}^*) =$



# Refined Parallel Repetition II

W.l.o.g assume $H(\mathcal{P}^*)$'s rows and columns are sorted based on fraction of 1-entries.

- $\delta_k(x, \mathcal{P}_1^*)$ is the fraction of 1-entries in blue region.
- $\delta_k(x, \mathcal{P}_2^*)$ is the fraction of 1-entries in red region.




By running the single instance extractor in parallel on $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$, the extraction probability is given by

$$\delta_k(x, \mathcal{P}_1^*) + \delta_k(x, \mathcal{P}_2^*) \geq \varepsilon(x, \mathcal{P}^*) - \frac{(k-1)^2}{N^2}$$

$$\implies \max(\delta_k(x, \mathcal{P}_1^*), \delta_k(x, \mathcal{P}_2^*)) \geq \left(\varepsilon(x, \mathcal{P}^*) - \frac{(k-1)^2}{N^2}\right)/2$$

# Fixed-Weight Repetition

Consider $\mathcal{P}^*$ attacking the $(t,\omega)$-fixed-weight repetition $\Pi^{t,\omega}$. The challenge space is given by $\mathrm{Ch}^{t,\omega} = \{c \in \mathrm{Ch}^t \,:\, \mathrm{wt}_0(c) = \omega\}$.

# Fixed-Weight Repetition

Consider $\mathcal{P}^*$ attacking the $(t, \omega)$-fixed-weight repetition $\Pi^{t,\omega}$. The challenge space is given by $\mathsf{Ch}^{t,\omega} = \{c \in \mathsf{Ch}^t : \mathsf{wt}_0(c) = \omega\}$.
Again, we can treat $\mathcal{P}^*$ as a (deterministic) function

$$\mathcal{P}^* : \mathsf{Ch}^{t,\omega} \to \{0,1\}^*, \qquad c \mapsto (z_1, \dots, z_t).$$

# Fixed-Weight Repetition

Consider $\mathcal{P}^*$ attacking the $(t,\omega)$-fixed-weight repetition $\Pi^{t,\omega}$. The challenge space is given by $\mathsf{Ch}^{t,\omega} = \{c \in \mathsf{Ch}^t : \mathrm{wt}_0(c) = \omega\}$.

Again, we can treat $\mathcal{P}^*$ as a (deterministic) function

$$\mathcal{P}^* : \mathsf{Ch}^{t,\omega} \to \{0,1\}^*, \qquad c \mapsto (z_1, \dots, z_t).$$

We can define $t$ probabilistic provers $\mathcal{P}_1^*, \dots, \mathcal{P}_t^*$ attacking a single invocation of $\Pi$

$$\mathcal{P}_i^* : c_i \mapsto \begin{bmatrix} \bar{c} \xleftarrow{\$} \begin{cases} \mathsf{Ch}^{t-1,\omega-1} & \text{if } c_i = 0 \\ \mathsf{Ch}^{t-1,\omega} & \text{if } c_i \neq 0 \end{cases} \\ (z_1, \dots, z_t) \leftarrow \mathcal{P}^*(c = (c_i, \bar{c})) \end{bmatrix} \mapsto z_i$$

# Fixed-Weight Repetition

Consider $\mathcal{P}^*$ attacking the $(t, \omega)$-fixed-weight repetition $\Pi^{t,\omega}$. The challenge space is given by $\mathsf{Ch}^{t,\omega} = \{c \in \mathsf{Ch}^t \,:\, \mathrm{wt}_0(c) = \omega\}$.
Again, we can treat $\mathcal{P}^*$ as a (deterministic) function

$$\mathcal{P}^* : \mathsf{Ch}^{t,\omega} \to \{0,1\}^*, \qquad c \mapsto (z_1, \dots, z_t).$$

We can define $t$ probabilistic provers $\mathcal{P}_1^*, \dots, \mathcal{P}_t^*$ attacking a single invocation of $\Pi$

$$\mathcal{P}_i^* : c_i \mapsto \begin{bmatrix} \bar{c} \leftarrow_{\$} \begin{cases} \mathsf{Ch}^{t-1,\omega-1} & \text{if } c_i = 0 \\ \mathsf{Ch}^{t-1,\omega} & \text{if } c_i \neq 0 \end{cases} \\ (z_1, \dots, z_t) \leftarrow \mathcal{P}^*(c = (c_i, \bar{c})) \end{bmatrix} \mapsto z_i$$

Notice that, if we take $c_i \leftarrow_{\$} \mathsf{Ch}$ it does not hold that $\varepsilon(x, \mathcal{P}_i^*) = \varepsilon(x, \mathcal{P}^*)$, since $c = (c_i, \bar{c})$ is not uniformly distributed in $\mathsf{Ch}^{t,\omega}$.

# Fixed-Weight Repetition

Consider $\mathcal{P}^*$ attacking the $(t,\omega)$-fixed-weight repetition $\Pi^{t,\omega}$. The challenge space is given by $\mathsf{Ch}^{t,\omega} = \{c \in \mathsf{Ch}^t : \mathrm{wt}_0(c) = \omega\}$.
Again, we can treat $\mathcal{P}^*$ as a (deterministic) function

$$\mathcal{P}^* : \mathsf{Ch}^{t,\omega} \to \{0,1\}^*, \qquad c \mapsto (z_1, \dots, z_t).$$

We can define $t$ probabilistic provers $\mathcal{P}_1^*, \dots, \mathcal{P}_t^*$ attacking a single invocation of $\Pi$

$$\mathcal{P}_i^* : c_i \mapsto \begin{bmatrix} \bar{c} \leftarrow_\$ \begin{cases} \mathsf{Ch}^{t-1,\omega-1} & \text{if } c_i = 0 \\ \mathsf{Ch}^{t-1,\omega} & \text{if } c_i \neq 0 \end{cases} \\ (z_1, \dots, z_t) \leftarrow \mathcal{P}^*(c = (c_i, \bar{c})) \end{bmatrix} \mapsto z_i$$

Notice that, if we take $c_i \leftarrow_\$ \mathsf{Ch}$ it does not hold that $\varepsilon(x, \mathcal{P}_i^*) = \varepsilon(x, \mathcal{P}^*)$, since $c = (c_i, \bar{c})$ is not uniformly distributed in $\mathsf{Ch}^{t,\omega}$.

We need to sample $c_i$ according to a particular distribution over $\mathsf{Ch}$.

# "Generalized" Punctured Success Probability

Let $\mathcal{D}$ a probability distribution over $D \subset \mathsf{Ch}$ with $|D| \geq k$. We define the success probability of $\mathcal{P}^*$ restricted on $\mathcal{D}$ as

$$\varepsilon(\mathcal{P}^*, \mathcal{D}) = \Pr\left[\mathcal{P}^*(C) \text{ succeeds}\right],$$

where $C$ is a random variable being distributed as $\mathcal{D}$. When $\mathcal{D}$ is the uniform distribution over $\mathsf{Ch}$, then $\varepsilon(\mathcal{P}^*, \mathcal{D}) = \varepsilon(\mathcal{P}^*)$.

# “Generalized” Punctured Success Probability

Let $\mathcal{D}$ a probability distribution over $D \subset \mathsf{Ch}$ with $|D| \geq k$. We define the success probability of $\mathcal{P}^*$ restricted on $\mathcal{D}$ as

$$\varepsilon(\mathcal{P}^*, \mathcal{D}) = \Pr\left[\mathcal{P}^*(C) \text{ succeeds}\right],$$

where $C$ is a random variable being distributed as $\mathcal{D}$. When $\mathcal{D}$ is the uniform distribution over $\mathsf{Ch}$, then $\varepsilon(\mathcal{P}^*, \mathcal{D}) = \varepsilon(\mathcal{P}^*)$.

**Restricted punctured success probability**

$$\delta_k(\mathcal{P}^*, \mathcal{D}) = \min_{S \subset D : |S| < k} \Pr\left[\mathcal{P}^*(C) \text{ succeeds} \mid C \notin S\right],$$

where $C$ is a random variable being distributed as $\mathcal{D}$.

# "Generalized" Punctured Success Probability

Let $\mathcal{D}$ a probability distribution over $D \subset \mathsf{Ch}$ with $|D| \geq k$. We define the success probability of $\mathcal{P}^*$ restricted on $\mathcal{D}$ as

$$\varepsilon(\mathcal{P}^*, \mathcal{D}) = \Pr\left[\mathcal{P}^*(C) \text{ succeeds}\right],$$

where $C$ is a random variable being distributed as $\mathcal{D}$. When $\mathcal{D}$ is the uniform distribution over $\mathsf{Ch}$, then $\varepsilon(\mathcal{P}^*, \mathcal{D}) = \varepsilon(\mathcal{P}^*)$.

**Restricted punctured success probability**

$$\delta_k(\mathcal{P}^*, \mathcal{D}) = \min_{S \subset D : |S| < k} \Pr\left[\mathcal{P}^*(C) \text{ succeeds} \mid C \notin S\right],$$

where $C$ is a random variable being distributed as $\mathcal{D}$.

**Extension of [AttFeh22, Lemma 2]**

There exists an extraction algorithm $\mathcal{E}^{\mathcal{P}^*}(\mathcal{D})$ that succeed with probability at least

$$\delta_k(\mathcal{P}^*, \mathcal{D})/k$$

# Main Result

**Theorem**

The $(t, \omega)$-fixed-weight repetition of a $k$-out-of-$N$ special-sound interactive proof is knowledge sound, with knowledge error

$$\kappa_{t,\omega} = \binom{t}{\omega}^{-1} \frac{\eta_{t,\omega}}{(N-1)^{t-\omega}},$$

where

$$\eta_{t,\omega} = \begin{cases} \binom{\omega(k-1)}{\omega}(k-2)^{\omega(k-2)}(k-1)^{t-\omega(k-1)} & \text{if } t \geq \omega(k-1) \\ \binom{t}{\omega}(k-2)^{t-\omega} & \text{otherwise} \end{cases}.$$

# Main Result

**Theorem**

The $(t, \omega)$-fixed-weight repetition of a $k$-out-of-$N$ special-sound interactive proof is knowledge sound, with knowledge error

$$\kappa_{t,\omega} = \binom{t}{\omega}^{-1} \frac{\eta_{t,\omega}}{(N-1)^{t-\omega}},$$

where

$$\eta_{t,\omega} = \begin{cases} \binom{\omega(k-1)}{\omega}(k-2)^{\omega(k-2)}(k-1)^{t-\omega(k-1)} & \text{if } t \geq \omega(k-1) \\ \binom{t}{\omega}(k-2)^{t-\omega} & \text{otherwise} \end{cases}.$$

- $\kappa_{t,\omega}$ cannot be expressed in terms of the knowledge error of the single istance.
- However, $\kappa_{t,\omega}$ coincides with the maximal cheating probability of a dishonest prover $\implies$ the result is optimal!

# Extending to Multi-Round Protocols

- Our result can be extended to multi-round $(k_1, \dots, k_\mu)$-special-sound protocols.
- The expression for the knowledge error became quite complex (Theorem 2 in the paper)
- The result is still optimal!

**Theorem**

The $(t, \omega)$-fixed-weight repetition of a $(k_1, \dots, k_\mu)$-out-of-$(N_1, \dots, N_\mu)$ special-sound interactive proof is knowledge sound.

# Knowledge Soundness of CROSS Protocol

- CROSS[2] is a $(2,2)$-out-of-$(p-1,2)$ special-sound 5-pass protocol.
- Fixed-weight optimization is employed in all parameter sets of the scheme.

**CROSS Specs**

Cheating probability:

$$\sum_{l=0}^{\min(\omega,t-\omega)} \frac{\binom{\omega}{l}\binom{t-\omega}{l}}{\binom{t}{\omega}}(p-1)^{-2l}$$

**Our work**

Knowledge error:

$$\max_{\alpha\in\{0,\dots,t\}} \sum_{l=\max(0,\omega-t+\alpha)}^{\min(\omega,\alpha)} \frac{\binom{\alpha}{l}\binom{t-\alpha}{\omega-l}}{\binom{t}{\omega}}(p-1)^{-(\alpha-l)-(\omega-l)}$$

[2] *Baldi, Barenghi, Bitzer, Karl, Manganiello, Pavoni, Pelosi, Santini, Schupp, Slaughter, Wachter-Zeh, and Weger. CROSS — Codes and Restricted Objects Signature Scheme.*

Telsy A TIM ENTERPRISE BRAND

# Knowledge Soundness of CROSS Protocol

- CROSS[2] is a $(2,2)$-out-of-$(p-1,2)$ special-sound 5-pass protocol.
- Fixed-weight optimization is employed in all parameter sets of the scheme.

**CROSS Specs**

Cheating probability:

$$\sum_{l=0}^{\min(\omega,t-\omega)} \frac{\binom{\omega}{l}\binom{t-\omega}{l}}{\binom{t}{\omega}}(p-1)^{-2l}$$

**Our work**

Knowledge error:

$$\max_{\alpha\in\{0,\dots,t\}} \sum_{l=\max(0,\omega-t+\alpha)}^{\min(\omega,\alpha)} \frac{\binom{\alpha}{l}\binom{t-\alpha}{\omega-l}}{\binom{t}{\omega}}(p-1)^{-(\alpha-l)-(\omega-l)}$$

The expressions coincide for $\alpha = \omega$, which is not always the case for CROSS parameter sets.

This does not immediately translate to CROSS parameters after the application of Fiat-Shamir!

[2] *Baldi, Barenghi, Bitzer, Karl, Manganiello, Pavoni, Pelosi, Santini, Schupp, Slaughter, Wachter-Zeh, and Weger. CROSS — Codes and Restricted Objects Signature Scheme.*

# Conclusions and Future Works

**Summary**:

- The fixed-weight repetition of (multi-round) interactive proofs is knowledge-sound.
- Explicit expression of adversary's cheating probability against $(k_1, \dots, k_\mu)$-special-sound protocols.
- The knowledge error matches the optimal cheating probability.

**Future works**:

- Investigate the non-interactive case.
- Extend to "generalized" fixed-weight optimization for intermediate rounds.

ia.cr/2024/884

# Thank you!