



UNIVERSITÀ  
POLITECNICA  
DELLE MARCHE

# **A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures**

---

Michele Battagliola

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

Cifris25 - September 11th, 2025

## The scheme:

- Code-based signature scheme.
- Second round candidate in NIST *on-ramp* standardization call.
- Zero-Knowledge protocol + Fiat-Shamir transform.
- Competitive public-keys size and fast execution.
- Fiat-Shamir Transform of a five-pass protocol with Fixed-Weight Optimization



cross-crypto.com

## The scheme:

- Code-based signature scheme.
- Second round candidate in NIST *on-ramp* standardization call.
- Zero-Knowledge protocol + Fiat-Shamir transform.
- Competitive public-keys size and fast execution.
- Fiat-Shamir Transform of a five-pass protocol with Fixed-Weight Optimization



cross-crypto.com

## Main questions:

- Is the Fiat-Shamir Transform of a five-pass protocol secure?
  - Attema et al. proved that the interactive version is secure.<sup>1</sup>
  - The non-interactive version has some lower bounds on the security loss but not upper bounds<sup>2</sup>
- How the fixed-weight impacts the security?

---

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

<sup>2</sup>Kales and Zaverucha. "An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes". CANS 20; Attema, Fehr, and Klooß. "Fiat-Shamir Transformation of Multi-round Interactive Proofs". TCC 2022, Part I.



Formal security proof for CROSS.

- EUF-CMA security of Fiat-Shamir transform for special-sound multi-round proofs.
- Reasonable security loss.
- Cover also the fixed-weight optimization.



Novel forgery attack.

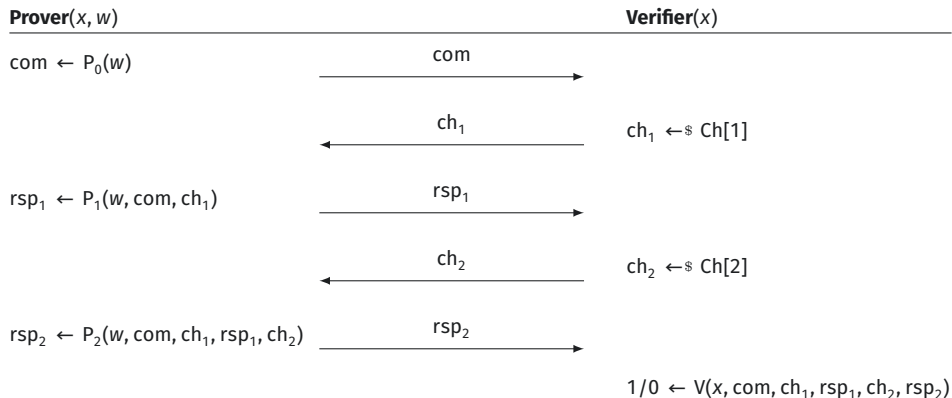
- Improves upon previous attack by Kales and Zaverucha.<sup>3</sup>
- Security loss up to 24% in worst case.
- Parameters worsened accordingly

---

<sup>3</sup>Kales and Zaverucha. "An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes". CANS 20.

# Five Pass Interactive Proofs

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



## Goal

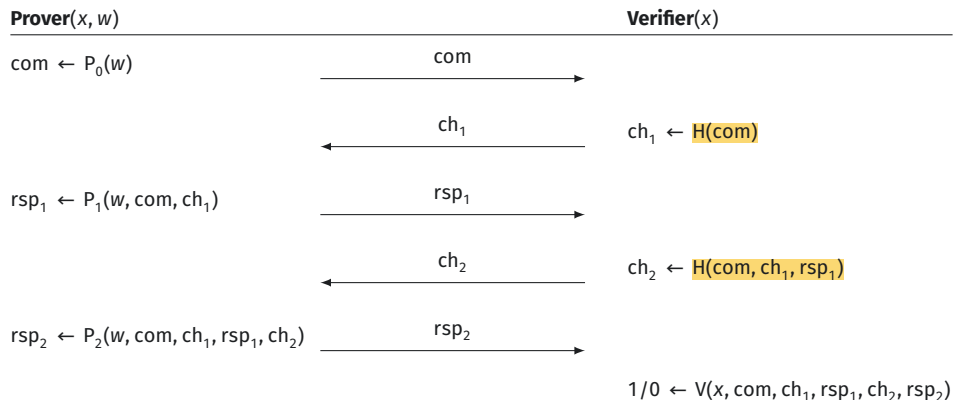
Prove the knowledge of a witness  $w$  for a public statement  $x$ .

## Digital Signature

We can obtain a digital signature by applying the Fiat-Shamir transform.

# Fiat-Shamir Transform

Transform any public-coin interactive proof into a *non-interactive* proof in the random oracle model.



# Fiat-Shamir Transform

Transform any public-coin interactive proof into a *non-interactive* proof in the random oracle model.

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

$\text{com} \leftarrow P_0(w)$

$\text{ch}_1 \leftarrow H(\text{com})$

$\text{rsp}_1 \leftarrow P_1(w, \text{com}, \text{ch}_1)$

$\text{ch}_2 \leftarrow H(\text{com}, \text{ch}_1, \text{rsp}_1)$

$\text{rsp}_2 \leftarrow P_2(w, \text{com}, \text{ch}_1, \text{rsp}_1, \text{ch}_2)$

**Verifier**( $x$ )

$\text{com}$

$\text{ch}_1 \leftarrow H(\text{com})$

$\text{ch}_2 \leftarrow H(\text{com}, \text{ch}_1, \text{rsp}_1)$

$1/0 \leftarrow V(x, \text{com}, \text{ch}_1, \text{rsp}_1, \text{ch}_2, \text{rsp}_2)$

## Completeness

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

## Zero-knowledge

No information about  $w$  is revealed. Usually enough to prove **Honest-Verifier Zero-Knowledge**.

## Knowledge Soundness

Given a dishonest prover  $P^*$  with a success probability greater than the **knowledge error**  $\kappa$ , it is always possible to efficiently extract a witness from  $P^*$ .

## Completeness

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

## Zero-knowledge

No information about  $w$  is revealed. Usually enough to prove **Honest-Verifier Zero-Knowledge**.

## Knowledge Soundness

Given a dishonest prover  $P^*$  with a success probability greater than the **knowledge error**  $\kappa$ , it is always possible to efficiently extract a witness from  $P^*$ .

Knowledge soundness is hard to prove in general and is often implied by the simpler notion of **special soundness**.

## Special Soundness

There is an extracting algorithm which can compute a witness given enough accepting transcript relative to a true statement.

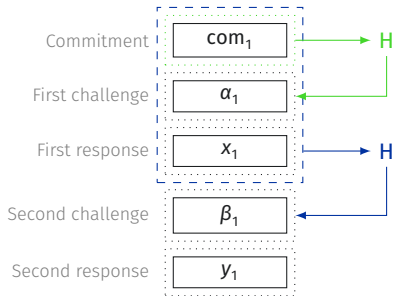
# **Fixed-Weight Repetition of Multi-Round Interactive Proofs**

---

# Parallel Repetition

Many protocols have large knowledge error  $\kappa \approx 1/2$ .

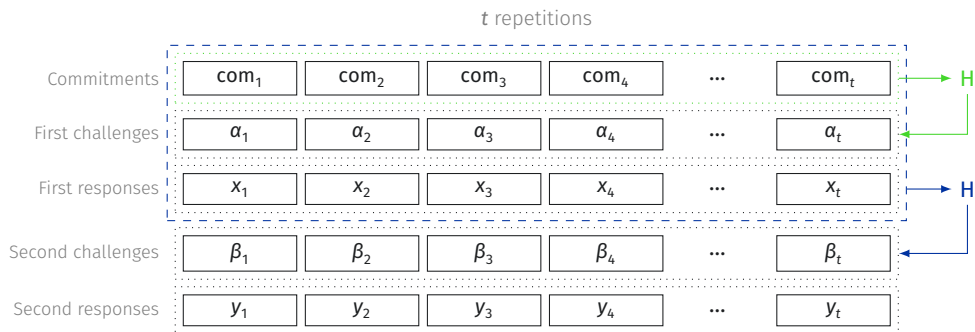
- To build digital signatures, we need the knowledge error to be negligible.



# Parallel Repetition

Many protocols have large knowledge error  $\kappa \approx 1/2$ .

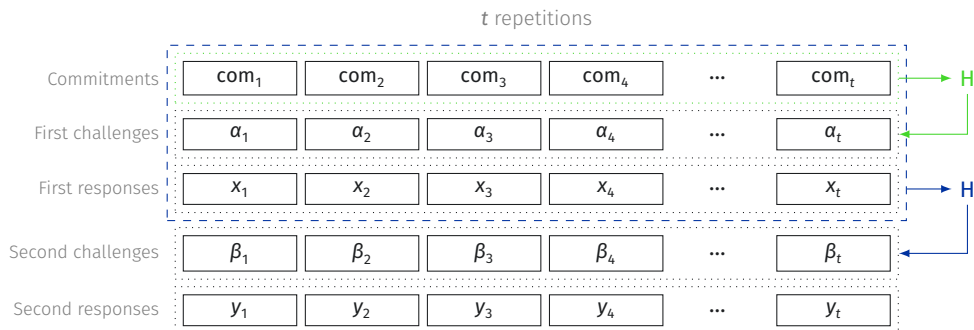
- To build digital signatures, we need the knowledge error to be negligible.
- We can **reduce** the knowledge error of  $\Pi$  by considering the  $t$ -fold parallel repetition  $\Pi^t$  of the protocol.



# Parallel Repetition

Many protocols have large knowledge error  $\kappa \approx 1/2$ .

- To build digital signatures, we need the knowledge error to be negligible.
- We can **reduce** the knowledge error of  $\Pi$  by considering the  $t$ -fold parallel repetition  $\Pi^t$  of the protocol.



## Theorem<sup>4</sup>

If  $\Pi$  is special-sound and has knowledge error  $\kappa$ , then  $\Pi^t$  has knowledge error  $\kappa^t$ .

<sup>4</sup>Attema and Fehr. "Parallel Repetition of  $(R_1, \dots, R_\mu)$ -Special-Sound Multi-round Interactive Proofs". CRYPTO 2022, Part I.

# Unbalanced Response



- 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. For example, this happens when:
  - for one challenge, the prover simply need to reveal all the random choice  $\implies$  can reveal simply a seed.
  - for the other challenge the prover needs to reveal some *structured data*, e.g. matrices or vector of fields elements.

# Fixed-Weight Repetition

The idea is to minimize the number of repetitions having the long response:

## $(t, \omega)$ -Fixed-Weight Repetition

Repeat the protocol  $t$  times, with the last challenge sampled from a space with a fixed large weight  $\omega$  of favorable challenges.

-  Fewer large responses to be sent  $\implies$  smaller signature.
-  Challenge space is now  $\binom{n}{\omega}$  instead of  $2^n$   $\implies$  more repetitions  $\implies$  slower algorithm.

## Theorem<sup>5</sup>

The  $(t, \omega)$ -fixed-weight repetition of a special-sound multi-round interactive proof  $\Pi$  is knowledge sound.

---

<sup>5</sup>Battagliola, Longo, Pintore, Signorini, and Tognolini. Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Proofs.

## **Attacking the Parallel Repetition**

---

## Warm Up: Three-pass case

- In the interactive case, the adversary has only one shot at guessing the challenge.
- In the non-interactive case, the adversary can try  $Q$  hash queries, and hope that one of them is the guessed one.
- The overall probability that at least one of them is guessed correctly is:

$$1 - \left(1 - \frac{1}{2^\lambda}\right)^Q \sim \frac{Q}{2^\lambda} = Q \cdot \frac{1}{2^\lambda}$$

Thus the overall security loss is a factor  $Q$ .

Critical property required for the attack:

- An adversary can win by guessing **only one** of the two challenges.
- Somewhat surprising but true for most protocols.

Critical property required for the attack:

- An adversary can win by guessing **only one** of the two challenges.
- Somewhat surprising but true for most protocols.

Can be formalized with the notion of **Piecewise Simulatability**:

- Stronger property than HVZK.
- Split the simulator in two algorithms.
- Allows one of the two challenges to be randomly chosen, while the simulator can choose the other challenge and produce a valid transcript.

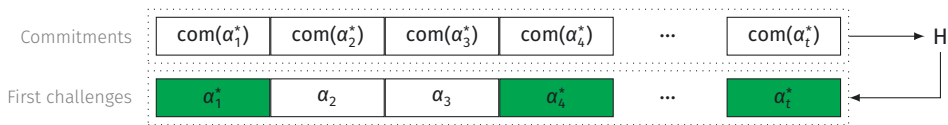
## The Kales-Zaverucha Attack

In the signature, the lack of interaction and piecewise simulatability can be exploited to split the attack in two **independent** phases:

# The Kales-Zaverucha Attack

In the signature, the lack of interaction and piecewise simulatability can be exploited to split the attack in two **independent** phases:

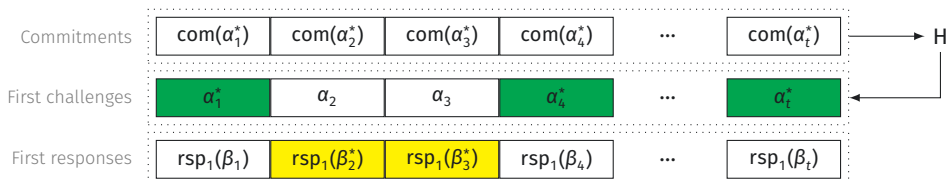
1. Generates new commitment until  $t^*$  first challenges  $\alpha_i$  are correctly guessed.



# The Kales-Zaverucha Attack

In the signature, the lack of interaction and piecewise simulatability can be exploited to split the attack in two **independent** phases:

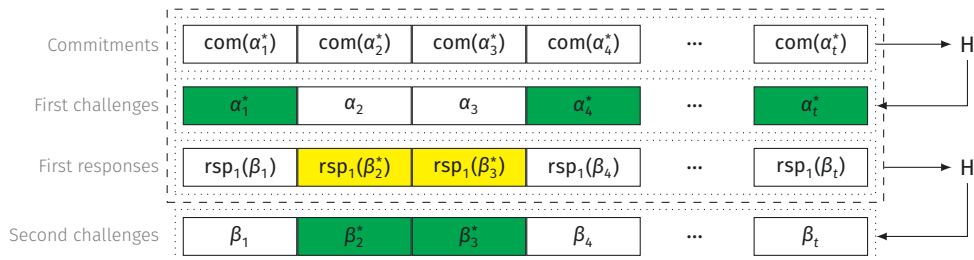
1. Generates new commitment until  $t^*$  first challenges  $\alpha_i$  are correctly guessed.
2. Generates responses  $\text{rsp}_1$  until the second challenges  $\beta_i$  are correctly guessed for the remaining  $t - t^*$  repetitions.



# The Kales-Zaverucha Attack

In the signature, the lack of interaction and piecewise simulatability can be exploited to split the attack in two **independent** phases:

1. Generates new commitment until  $t^*$  first challenges  $\alpha_i$  are correctly guessed.
2. Generates responses  $\text{rsp}_1$  until the second challenges  $\beta_i$  are correctly guessed for the remaining  $t - t^*$  repetitions.

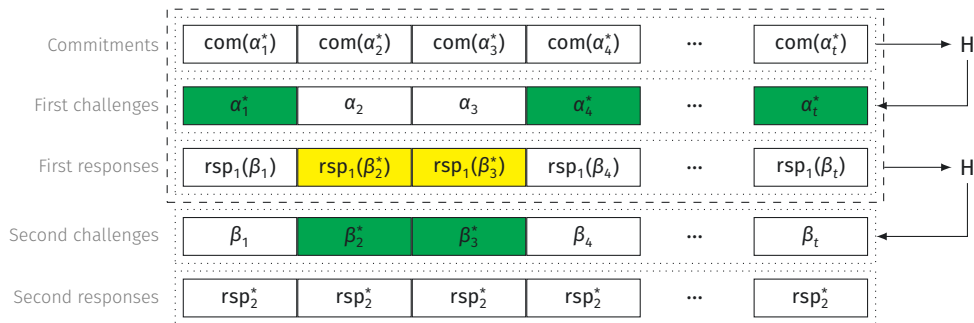


# The Kales-Zaverucha Attack

In the signature, the lack of interaction and piecewise simulatability can be exploited to split the attack in two **independent** phases:

1. Generates new commitment until  $t^*$  first challenges  $\alpha_i$  are correctly guessed.
2. Generates responses  $\text{rsp}_1$  until the second challenges  $\beta_i$  are correctly guessed for the remaining  $t - t^*$  repetitions.

Compute final responses  $\text{rsp}_2$ .



## Overall security loss

- In the interactive case, the adversary has only one shot at guessing at least one of two the challenges.
- In the non-interactive case, the adversary can try  $\frac{Q}{2}$  to guess at least half of the first challenge.
- Then uses the remaining  $\frac{Q}{2}$  queries to guess the second half
- The overall probability that at least one of them is guessed correctly is:

$$\frac{Q}{2} \frac{1}{2^{\lambda/2}} \cdot \frac{Q}{2} \frac{1}{2^{\lambda/2}} = \frac{Q^2}{4} \frac{1}{2^\lambda}$$

Thus the overall security loss is a factor  $\frac{Q^2}{4}$ .

In general for a  $(2\mu + 1)$ -pass protocol it is, at least,  $\frac{Q^\mu}{\mu^\mu}$ .

## **Attacking the Fixed-Weight Repetition**

---

In the following we will restrict to  $q^2$ -interactive proofs. In particular  $|\text{Ch}[1]| = q$  and  $|\text{Ch}[2]| = 2$ .

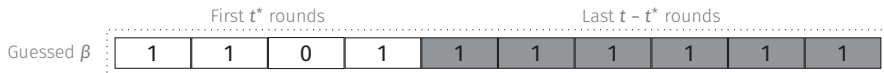
# Intuition

In the following we will restrict to  $q=2$ -interactive proofs. In particular  $|\text{Ch}[1]| = q$  and  $|\text{Ch}[2]| = 2$ .

## Previous strategy:

- CROSS adapted KZ's attack by taking extra advantage of the fixed-weight challenge of the second round.
  - The second challenge is guessed with the same weight as the actual challenge.

Example with  $t = 10, \omega = 9$ :



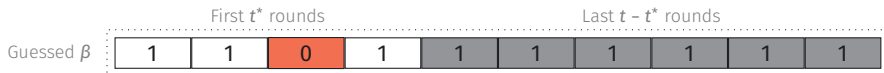
# Intuition

In the following we will restrict to  $q$ -interactive proofs. In particular  $|\text{Ch}[1]| = q$  and  $|\text{Ch}[2]| = 2$ .

## Previous strategy:

- CROSS adapted KZ's attack by taking extra advantage of the fixed-weight challenge of the second round.
  - The second challenge is guessed with the same weight as the actual challenge.

Example with  $t = 10, \omega = 9$ :



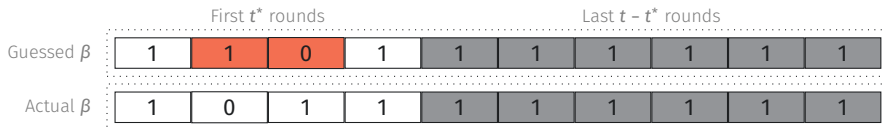
# Intuition

In the following we will restrict to  $q_2$ -interactive proofs. In particular  $|\text{Ch}[1]| = q$  and  $|\text{Ch}[2]| = 2$ .

## Previous strategy:

- CROSS adapted KZ's attack by taking extra advantage of the fixed-weight challenge of the second round.
  - The second challenge is guessed with the same weight as the actual challenge.
- This strategy is optimal **only** when  $\omega \approx t/2$ .

Example with  $t = 10, \omega = 9$ :



In the following we will restrict to  $q=2$ -interactive proofs. In particular  $|\text{Ch}[1]| = q$  and  $|\text{Ch}[2]| = 2$ .

## Previous strategy:

- CROSS adapted KZ's attack by taking extra advantage of the fixed-weight challenge of the second round.
  - The second challenge is guessed with the same weight as the actual challenge.
- This strategy is optimal **only** when  $\omega \approx t/2$ .

## Improved strategy:

- Select **at least**  $\omega^* \geq \omega$  positions where attacker expects the special challenge.
- When  $\omega \approx t$ , choosing more than  $\omega$  positions gives better results.
  - Making mistakes in a few positions is more efficient than trying to guess perfectly.

Example with  $t = 10, \omega = 9, \omega^* = 10$ :

	First $t^*$ rounds				Last $t - t^*$ rounds					
Gussed $\beta$	1	1	0	1	1	1	1	1	1	1
Actual $\beta$	1	0	1	1	1	1	1	1	1	1
Improved $\beta$	1	1	1	1	1	1	1	1	1	1

Two phases in our improved attack:

1. Try to guess the first challenges  $\alpha_j$  for at least  $t^*$  parallel executions.
2. Try to guess the second challenge for remaining **fixed-weight** executions.
  - **Key improvement:** Select  $\omega^* \geq \omega$  positions for the fixed-weight element.

Still requires *piecewise simulatability* (similar to Kales-Zaverucha attack).

Two phases in our improved attack:

1. Try to guess the first challenges  $\alpha_i$  for at least  $t^*$  parallel executions.
2. Try to guess the second challenge for remaining **fixed-weight** executions.
  - **Key improvement:** Select  $\omega^* \geq \omega$  positions for the fixed-weight element.

Still requires *piecewise simulatability* (similar to Kales-Zaverucha attack).

## Choosing attack parameters:

- The choice of  $t^*$  depends on the size of the challenge sets.
  - Ideally, phase 1 should have a similar cost to phase 2.
- The choice of  $\omega^*$  depends on the choice of  $\omega$  relative to  $t$ .
  - The attack is most effective for very unbalanced parameters.

## Impact on CROSS Parameters

Significant security reduction for *balanced* and *small* parameter sets!

Parameter Set		$t$	$\omega$	Forgery Cost	Loss
CROSS-R-SDP 1	balanced	252	212	120	6%
	small	960	938	97	24%
CROSS-R-SDP 3	balanced	398	340	180	6%
	small	945	907	156	19%
CROSS-R-SDP 5	balanced	507	427	241	6%
	small	968	912	217	15%
CROSS-R-SDP(G) 1	balanced	243	206	123	4%
	small	871	850	108	15%
CROSS-R-SDP(G) 3	balanced	255	176	190	1%
	small	949	914	168	13%
CROSS-R-SDP(G) 5	balanced	356	257	253	1%
	small	996	945	229	11%

Detailed cost analysis: <https://github.com/edoars/revise-cross-parameters>.

## **EUFCMA Proof**

---

The attacks provide a better lower bound for the security loss. To prove the EUF-CMA security we need an upper bound. **No general results were known also for the standard parallel repetitions**

## **Roadmap of the Proof:**

The attacks provide a better lower bound for the security loss. To prove the EUF-CMA security we need an upper bound. **No general results were known also for the standard parallel repetitions**

## **Roadmap of the Proof:**

1. show that any honest-verifier zero-knowledge and knowledge sound multi-round protocol is secure against impersonation attack.

The attacks provide a better lower bound for the security loss. To prove the EUF-CMA security we need an upper bound. **No general results were known also for the standard parallel repetitions**

## **Roadmap of the Proof:**

1. show that any honest-verifier zero-knowledge and knowledge sound multi-round protocol is secure against impersonation attack.
2. show that the Fiat-Shamir transform of any multi round protocol secure against impersonation attack is EUF-CMA

The attacks provide a better lower bound for the security loss. To prove the EUF-CMA security we need an upper bound. **No general results were known also for the standard parallel repetitions**

## **Roadmap of the Proof:**

1. show that any honest-verifier zero-knowledge and knowledge sound multi-round protocol is secure against impersonation attack.
2. show that the Fiat-Shamir transform of any multi round protocol secure against impersonation attack is EUF-CMA
3. show that the fixed weight optimization of a special sound protocol is knowledge sound

In a nutshell, a dishonest prover is not able to successfully interact with a verifier, even having access to a polynomial number of previous accepting conversation.

**Experiment 3:**  $\text{Exp}_{(\mathcal{P}, \mathcal{V}), \mathcal{I}}^{\text{IMP}}(\lambda)$

```
1:  $(x, y) \leftarrow_{\$} R$   
2:  $\text{com} \leftarrow_{\$} \mathcal{I}^{\text{OTrGen}}(x)$   
3: for  $i \leftarrow 1, \dots, \mu$  do  
4:    $\text{ch}^{[i]} \leftarrow_{\$} \text{Ch}^{[i]}$   
5:    $\text{rsp}^{[i]} \leftarrow_{\$} \mathcal{I}(\text{com}, \{\text{ch}^{[j]}\}_{j \leq i}, \{\text{rsp}^{[j]}\}_{j < i})$   
6: return  $\mathcal{V}(x, \text{com}, \{\text{ch}^{[i]}, \text{rsp}^{[i]}\}_{i=1}^{\mu})$ 
```

```
OTrGen( $x$ ):  
  return  $(\mathcal{P}(y), \mathcal{V})(x)$ 
```

1. **HVZK + KS  $\implies$  IMP:**

- HVZK  $\implies$  the transcript oracle OTrGen can be simulated.
- KS  $\implies$  it is possible to extract the witness

2. **IMP  $\implies$  EUF-CMA<sup>6</sup>**

- the transcript from OTrGen can be used to answer the sign queries
- the simulator inject the challenge in the hash queries and hope to guess correctly which hash queries the adversary will use in the forgery  $\implies \binom{Q}{\mu}^{-1}$  probability of guessing correctly.

3. **FW + original is SS  $\implies$  FW is KS<sup>7</sup>**

---

<sup>6</sup>Abdalla, An, Bellare, and Namprepme. "From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security". EUROCRYPT 2002.

<sup>7</sup>Battagliola, Longo, Pintore, Signorini, and Tognolini. Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Proofs.

## Theorem

The Fiat-Shamir transform of a knowledge-sound interactive proof is EUFCMA secure.

### Key steps in the proof:

1. Prove security against impersonation under passive attack

2. Show that this implies EUFCMA security with a security loss of at most  $\binom{Q}{\mu} > \frac{Q^\mu}{\mu^\mu}$ .

Since the fixed-weight repetition of a special-sound protocol is knowledge sound, we can apply this result to CROSS.

## Main results:

- Proved EUF-CMA security of CROSS.
- Presented a novel forgery attack for the fixed-weight repetition of q2-identification schemes.
- Showed significant security reductions for CROSS parameter sets.

## Implications:

- Fixed-weight parameters for CROSS re-chosen for round 2.
- The underlying hard problem is **not affected**.

## Future work:

- Proving optimality of our attack.
- Fill the gap between  $\binom{Q}{\mu}$  and  $\frac{Q^\mu}{\mu^\mu}$ .
- Investigating alternative schemes with different security properties (e.g., **early abort**).

Full paper:



[ia.cr/2025/127](https://ia.cr/2025/127)

## Acknowledgment of support

- the Italian Ministry of University and Research (MUR) under the PRIN PNRR 2022 program with project “Mathematical Primitives for Post Quantum Digital Signatures” (P2022J4HRR) funded by the European Union - Next Generation EU, Missione 4 “Istruzione e Ricerca” del Piano Nazionale di Ripresa e Resilienza
- the Italian Ministry of University and Research (MUR) under the PRIN PNRR 2022 program with project “POst quantum Identification and eNcryption primiTives: dEsign and Realization (POINTER)” (2022M2JLF2)



**Finanziato  
dall'Unione europea**  
NextGenerationEU



**Ministero  
dell'Università  
e della Ricerca**