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

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

CrypTO Conference 2025 - May 23, 2025

CROSS

The scheme:

- Code-based signature scheme.
- Second round candidate in NIST *on-ramp* standardization call.
- Zero-Knowledge protocol + Fiat-Shamir transform.
- Well-known protocol based on decoding random oracle (with restricted errors).
- Standard optimization techniques.
- Competitive public-keys size and fast execution.

cross-crypto.com

CROSS

The scheme:

- Code-based signature scheme.
- Second round candidate in NIST *on-ramp* standardization call.
- Zero-Knowledge protocol + Fiat-Shamir transform.
- Well-known protocol based on decoding random oracle (with restricted errors).
- Standard optimization techniques.
- Competitive public-keys size and fast execution.

cross-crypto.com

Our contribution:

- Formal security proof for CROSS.
    - EUF-CMA security of Fiat-Shamir transform for special-sound multi-round proofs.
- Novel forgery attack.
    - Improves upon previous attack by Kales and Zaverucha.[1]
    - Security loss up to 24% in worst case.

[1] *Kales and Zaverucha. "An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes". CANS 20.*

(Multi-Round) Interactive Proofs

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

Prover(x, w)		**Verifier**(x)
$\mathsf{com} \leftarrow \mathsf{P}_0(w)$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_{\$} \mathsf{Ch}[1]$
$\mathsf{rsp}_1 \leftarrow \mathsf{P}_1(w, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{rsp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_{\$} \mathsf{Ch}[2]$
$\mathsf{rsp}_2 \leftarrow \mathsf{P}_2(w, \mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{rsp}_2}$	
		$1/0 \leftarrow \mathsf{V}(x, \mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1, \mathsf{ch}_2, \mathsf{rsp}_2)$

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.

Prover(x, w)		**Verifier**(x)
$\mathsf{com} \leftarrow \mathsf{P}_0(w)$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow \mathsf{H}(\mathsf{com})$
$\mathsf{rsp}_1 \leftarrow \mathsf{P}_1(w, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{rsp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1)$
$\mathsf{rsp}_2 \leftarrow \mathsf{P}_2(w, \mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{rsp}_2}$	
		$1/0 \leftarrow \mathsf{V}(x, \mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1, \mathsf{ch}_2, \mathsf{rsp}_2)$

Fiat-Shamir Transform

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

Prover(x, w)		**Verifier**(x)
$\mathsf{com} \leftarrow \mathsf{P}_0(w)$	$\xrightarrow{\mathsf{com}}$	
$\mathsf{ch}_1 \leftarrow \mathsf{H}(\mathsf{com})$		
$\mathsf{rsp}_1 \leftarrow \mathsf{P}_1(w, \mathsf{com}, \mathsf{ch}_1)$		
$\mathsf{ch}_2 \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1)$		
$\mathsf{rsp}_2 \leftarrow \mathsf{P}_2(w, \mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{com}, \mathsf{rsp}_1, \mathsf{rsp}_2}$	
		$\mathsf{ch}_1 \leftarrow \mathsf{H}(\mathsf{com})$
		$\mathsf{ch}_2 \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1)$
		$1/0 \leftarrow \mathsf{V}(x, \mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1, \mathsf{ch}_2, \mathsf{rsp}_2)$

Idea: replace the challenge from the verifier with the output of a random oracle on the current transcript (add a message to obtain a signature-scheme).

Properties

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 κ, it is always possible to efficiently extract a witness from P^*.

Properties

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 κ, 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

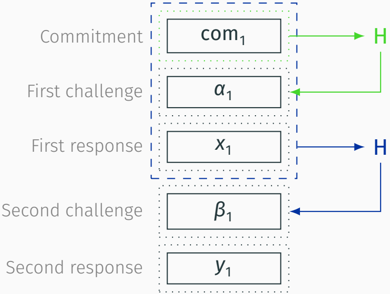
There is an extracting algorithm which can compute a witness given enough accepting transcript relative to a true statement.

Fixed-Weight Repetition of Multi-Round Interactive Proofs

Parallel Repetition

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

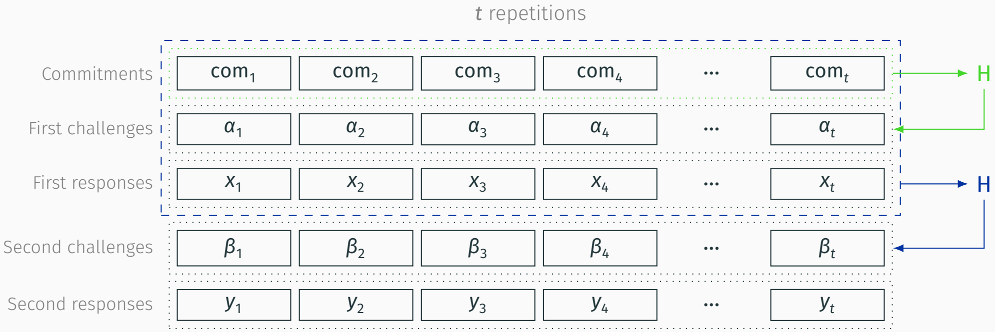
- To build digital signatures, we need the knowledge error to be negligible.



Parallel Repetition

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

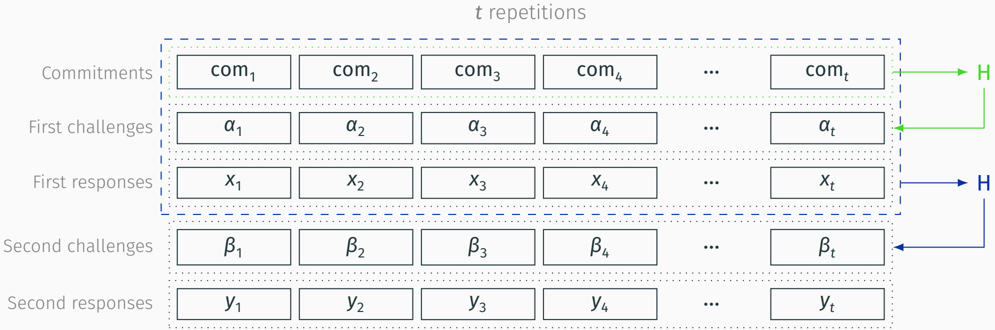
- To build digital signatures, we need the knowledge error to be negligible.
- We can reduce the knowledge error of Π by considering the t-fold parallel repetition Π^t of the protocol.



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 Π by considering the t-fold parallel repetition Π^t of the protocol.



Theorem[2]

If Π is special-sound and has knowledge error κ, then Π^t has knowledge error κ^t.

[2] *Attema and Fehr. "Parallel Repetition of $(k_1, \dots, k_\mu)$-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:

(t, ω)-Fixed-Weight Repetition

Repeat the protocol t times, with the last challenge sampled from a space with a fixed large weight ω of favorable 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:

(t, ω)-Fixed-Weight Repetition

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

👍 Fewer large responses to be sent $\implies$ smaller signature.

👎 More repetitions $\implies$ less efficient signing and verification.

Theorem[3]

The (t, ω)-fixed-weight repetition of a special-sound multi-round interactive proof Π is knowledge sound.

[3] *Battagliola, Longo, Pintore, S., and Tognolini. Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Proofs.*

EUF-CMA Security Proof for CROSS

Theorem
The Fiat-Shamir transform of a knowledge-sound interactive proof is EUF-CMA secure.

Key steps in the proof:

1. Prove security against impersonation under passive attack
2. Show that this implies EUF-CMA security with a security loss of at most $\binom{Q}{\mu}$.
    - Q is the number of signature queries.
    - $2\mu + 1$ is the number of rounds.

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

Attacking the Parallel Repetition

Piecewise Simulatability

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.

Piecewise Simulatability

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.

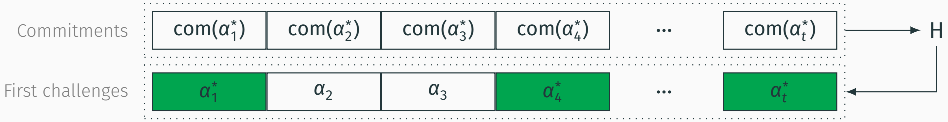
The Kales-Zaverucha Attack

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 α_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:

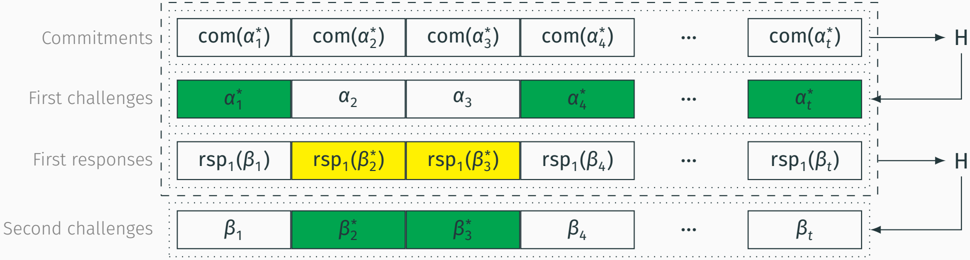
1. Generates new commitment until t^* first challenges α_i are correctly guessed.
2. Generates responses rsp_1 until the second challenges β_i are correctly guessed for the remaining $t - t^*$ repetitions.

Commitments	$\mathsf{com}(\alpha_1^*)$	$\mathsf{com}(\alpha_2^*)$	$\mathsf{com}(\alpha_3^*)$	$\mathsf{com}(\alpha_4^*)$	...	$\mathsf{com}(\alpha_t^*)$	H
First challenges	α_1^*	α_2	α_3	α_4^*	...	α_t^*	
First responses	$\mathsf{rsp}_1(\beta_1)$	$\mathsf{rsp}_1(\beta_2^*)$	$\mathsf{rsp}_1(\beta_3^*)$	$\mathsf{rsp}_1(\beta_4)$	...	$\mathsf{rsp}_1(\beta_t)$	

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 α_i are correctly guessed.
2. Generates responses rsp_1 until the second challenges β_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 α_i are correctly guessed.
2. Generates responses rsp_1 until the second challenges β_i are correctly guessed for the remaining $t - t^*$ repetitions.

Compute final responses rsp_2.

Commitments	$\mathsf{com}(\alpha_1^*)$	$\mathsf{com}(\alpha_2^*)$	$\mathsf{com}(\alpha_3^*)$	$\mathsf{com}(\alpha_4^*)$	...	$\mathsf{com}(\alpha_t^*)$	$\to$ H
First challenges	α_1^*	α_2	α_3	α_4^*	...	α_t^*	
First responses	$\mathsf{rsp}_1(\beta_1)$	$\mathsf{rsp}_1(\beta_2^*)$	$\mathsf{rsp}_1(\beta_3^*)$	$\mathsf{rsp}_1(\beta_4)$	...	$\mathsf{rsp}_1(\beta_t)$	$\to$ H
Second challenges	β_1	β_2^*	β_3^*	β_4	...	β_t	
Second responses	rsp_2^*	rsp_2^*	rsp_2^*	rsp_2^*	...	rsp_2^*	

Attacking the Fixed-Weight Repetition

Intuition

In the following we will restrict to $q2$-interactive proofs. In particular $|\mathrm{Ch}[1]| = q$ and $|\mathrm{Ch}[2]| = 2$.

Intuition

In the following we will restrict to $q2$-interactive proofs. In particular $|\mathrm{Ch}[1]| = q$ and $|\mathrm{Ch}[2]| = 2$.

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 $t = 10, \omega = 9$:

	First t^* rounds				Last $t - t^*$ rounds					
Guessed β	1	1	0	1	1	1	1	1	1	1

Intuition

In the following we will restrict to $q2$-interactive proofs. In particular $|\mathrm{Ch}[1]| = q$ and $|\mathrm{Ch}[2]| = 2$.

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 $t = 10, \omega = 9$:

	First t^* rounds				Last $t - t^*$ rounds					
Guessed β	1	1	0	1	1	1	1	1	1	1

Intuition

In the following we will restrict to $q2$-interactive proofs. In particular $|\mathrm{Ch}[1]| = q$ and $|\mathrm{Ch}[2]| = 2$.

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 $t = 10, \omega = 9$:

	First t^* rounds				Last $t - t^*$ rounds					
Guessed β	1	1	0	1	1	1	1	1	1	1
Actual β	1	0	1	1	1	1	1	1	1	1

Intuition

In the following we will restrict to $q2$-interactive proofs. In particular $|\mathrm{Ch}[1]| = q$ and $|\mathrm{Ch}[2]| = 2$.

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 ω 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					
Guessed β	1	1	0	1	1	1	1	1	1	1
Actual β	1	0	1	1	1	1	1	1	1	1
Improved β	1	1	1	1	1	1	1	1	1	1

Novel Forgery

Two phases in our improved attack:

1. Try to guess the first challenges α_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).

Two phases in our improved attack:

1. Try to guess the first challenges α_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 ω^* depends on the choice of ω 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	ω	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`.

Conclusions

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.
    - *Fast* variant: $\omega \approx t/2$, maintains security.
    - *Balanced* and *small* variants: ω close to t, vulnerable.
    - For *small* variant, security loss up to 24%.

Full paper:

ia.cr/2025/127

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.
- Investigating alternative schemes with different security properties (e.g., early abort).

Thank You!