

CROSS: Round 2 Update

Codes & Restricted Objects Signature Scheme

Patrick Karl

TUM School of Computation, Information and Technology
Technical University of Munich

Sixth PQC Standardization Conference
NIST, Gaithersburg, September 26, 2025



TUM Uhrenturm

Outline

- 1** Overview
- 2 Round 2: parameters and specification
- 3 Implementation efforts and attacks
- 4 What else?

Overview

■ Based on variants of Syndrome Decoding Problem

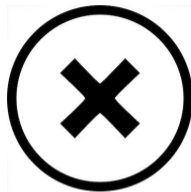
- ✓ Compact representations
- ✓ Efficient arithmetic

■ Fiat-Shamir transform on ZK protocol

- ✓ Trade-off: signature size & performance

■ Simple and efficient operations

- ✓ Low implementation complexity
- ✓ Quite efficient in HW
- ✓ Can run on microcontrollers



<https://www.cross-crypto.com/>
<https://github.com/CROSS-signature>



(Restricted-) Syndrome Decoding Problem

Syndrome Decoding Problem (SDP) [Bar94; BMVT78]

Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $t \in \mathbb{N}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exists an $\mathbf{e} \in \mathbb{F}_p^n$ such that $wt(\mathbf{e}) < t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

(Restricted-) Syndrome Decoding Problem

Syndrome Decoding Problem (SDP) [Bar94; BMVT78]

Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $t \in \mathbb{N}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exists an $e \in \mathbb{F}_p^n$ such that $wt(e) < t$ and $e\mathbf{H}^\top = \mathbf{s}$.

Restricted Syndrome Decoding Problem (R-SDP) [Bal+21; Bal+23]

Given $g \in \mathbb{F}_p^*$ of order z , $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$, and $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$, decide if there exists an $e \in \mathbb{E}^n$ such that $e\mathbf{H}^\top = \mathbf{s}$.

(Restricted-) Syndrome Decoding Problem

Syndrome Decoding Problem (SDP) [Bar94; BMVT78]

Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $t \in \mathbb{N}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exists an $\mathbf{e} \in \mathbb{F}_p^n$ such that $wt(\mathbf{e}) < t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

Restricted Syndrome Decoding Problem (R-SDP) [Bal+21; Bal+23]

Given $g \in \mathbb{F}_p^*$ of order z , $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$, and $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$, decide if there exists an $\mathbf{e} \in \mathbb{E}^n$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

Restricted Syndrome Decoding Problem with Subgroup G (R-SDP(G)) [Bal+23]

Let $G = \langle \mathbf{a}_1, \dots, \mathbf{a}_m \rangle = \left\{ \star_{i=1}^m \mathbf{a}_i^{\bar{u}_i} \mid \bar{u}_i \in \mathbb{F}_z \right\}$ for $\mathbf{a}_i \in \mathbb{E}^n$, $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exist an $\mathbf{e} \in G$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

(Restricted-) Syndrome Decoding Problem

Syndrome Decoding Problem (SDP) [Bar94; BMVT78]

Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $t \in \mathbb{N}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exists an $\mathbf{e} \in \mathbb{F}_p^n$ such that $wt(\mathbf{e}) < t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

Restricted Syndrome Decoding Problem (R-SDP) [Bal+21; Bal+23]

Given $g \in \mathbb{F}_p^*$ of order z , $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$, and $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$, decide if there exists an $\mathbf{e} \in \mathbb{E}^n$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

Restricted Syndrome Decoding Problem with Subgroup G (R-SDP(G)) [Bal+23]

Let $G = \langle \mathbf{a}_1, \dots, \mathbf{a}_m \rangle = \left\{ \star_{i=1}^m \mathbf{a}_i^{\bar{u}_i} \mid \bar{u}_i \in \mathbb{F}_z \right\}$ for $\mathbf{a}_i \in \mathbb{E}^n$, $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, decide if there exist an $\mathbf{e} \in G$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

- ✓ No weight restriction, smaller n compared to SDP, compact representation

Zero-Knowledge protocol

Private Key $\mathbf{e} \in G$

Public Key $G \subseteq \mathbb{E}^n$, $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} = \mathbf{e}\mathbf{H}^\top \in \mathbb{F}_p^{n-k}$

PROVER

Seed $\xleftarrow{\$} \{0, 1\}^\lambda$, $(\mathbf{e}', \mathbf{u}') \leftarrow \text{CSPRNG}(\text{Seed})$

$\mathbf{v} \leftarrow \mathbf{e} * (\mathbf{e}')^{-1}$ // compute transform \mathbf{v}

$\mathbf{u} \leftarrow \mathbf{v} * \mathbf{u}'$, $\mathbf{s}' \leftarrow \mathbf{u}\mathbf{H}^\top$

$\text{cmt}_0 \leftarrow \text{Hash}(\mathbf{s}' \mid \mathbf{v})$, $\text{cmt}_1 \leftarrow \text{Hash}(\mathbf{u}' \mid \mathbf{e}')$

$\mathbf{y} \leftarrow \mathbf{u}' + \text{chall}_1 \mathbf{e}'$

$\text{digest}_y \leftarrow \text{Hash}(\mathbf{y})$ // 1st response

If $\text{chall}_2 = 0$, $\text{resp} \leftarrow (\mathbf{y}, \mathbf{v})$ // 2nd response, long

If $\text{chall}_2 = 1$, $\text{resp} \leftarrow \text{Seed}$ // 2nd response, short

VERIFIER

$\xrightarrow{\text{cmt}_0, \text{cmt}_1}$

$\xleftarrow{\text{chall}_1}$

$\text{chall}_1 \xleftarrow{\$} \mathbb{F}_p^*$

$\xrightarrow{\text{digest}_y}$

$\xleftarrow{\text{chall}_2}$

$\text{chall}_2 \xleftarrow{\$} \{0, 1\}$

$\xrightarrow{\text{resp}}$

Verify $\text{cmt}_{\text{chall}_2}$ using resp

Zero-Knowledge protocol

Private Key $\mathbf{e} \in G$

Public Key $G \subseteq \mathbb{E}^n, \mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}, \mathbf{s} = \mathbf{e}\mathbf{H}^\top \in \mathbb{F}_p^{n-k}$

PROVER

VERIFIER

Seed $\xleftarrow{\$} \{0, 1\}^\lambda, (\mathbf{e}', \mathbf{u}') \leftarrow \text{CSPRNG}(\text{Seed})$

$\mathbf{v} \leftarrow \mathbf{e} * (\mathbf{e}')^{-1}$ // compute transform \mathbf{v}

$\mathbf{u} \leftarrow \mathbf{v} * \mathbf{u}', \mathbf{s}' \leftarrow \mathbf{u}\mathbf{H}^\top$

Apply **FS-transform** and additional **standard optimizations**:

→ GGM/Merkle trees, fixed-weight second challenge

$\xrightarrow{\text{digest}_y}$

$\text{chall}_2 \xleftarrow{\$} \{0, 1\}$

$\xleftarrow{\text{chall}_2}$

If $\text{chall}_2 = 0, \text{resp} \leftarrow (y, \mathbf{v})$ // 2nd response, long

If $\text{chall}_2 = 1, \text{resp} \leftarrow \text{Seed}$ // 2nd response, short

$\xrightarrow{\text{resp}}$

Verify $\text{cmt}_{\text{chall}_2}$ using resp

Outline

- 1 Overview
- 2 Round 2: parameters and specification**
- 3 Implementation efforts and attacks
- 4 What else?

Security analysis: R-SDP and R-SDP(G)

- Improved solver for R-SDP(G) making use of G
 - slightly increased code parameters (v1.0 → v1.1) ☹️

Security analysis: R-SDP and R-SDP(G)

- Improved solver for R-SDP(G) making use of G
 - slightly increased code parameters (v1.0 → v1.1) ☹️

A Security Analysis of Restricted Syndrome Decoding Problems [BBO24]

- New collision attack on R-SDP(G) using G
- Concrete bounds for algebraic attacks on R-SDP
- (new) code parameters not threatened 😊

A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures [Bat+25]

- Extensive security analysis of the CROSS-ID protocol
 - proof that CROSS is EUF-CMA secure! 😊

Security analysis: ZK protocol I

A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures [Bat+25]

- Extensive security analysis of the CROSS-ID protocol
 - proof that CROSS is EUF-CMA secure! 😊
- Novel forgery attack adapted from [KZ20]
 - relies on non-interactivity of transformed ZK protocol (not R-SDP or R-SDP(G))
 - exploits unbalanced fixed-weighted challenge
 - required to adapt parameters (t and w) mainly for balanced and small versions 😞

A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures [Bat+25]

■ Extensive

→ proof

■ Novel for

relies

exploits unbalanced fixed-weighted challenge

→ required to adapt parameters (t and w) mainly for balanced and small versions 😞

Session X – Security/Cryptanalysis II

Session Chair: Carl Miller, NIST

11:10 – 11:30

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

Presented by: Michele Battagliola, Università Politecnica delle Marche (virtual)

→ Details in Michele's talk!

$DP(G)$

Security analysis: ZK protocol II

Changes on rounds t and signature size from v1.2 to v2.2

Version and Security Level	Optim. Corner	p	z	n	k	m	t	w	Pri. Key Size (B)	Pub. Key Size (B)	Signature Size (B)
R-SDP 1	fast	127	7	127	76	-	157 (-3.68%)	82	32	77	18432 (-3.76%)
	balanced	127	7	127	76	-	256 (+1.59%)	215	32	77	13152 (+1.86%)
	small	127	7	127	76	-	520 (-45.8%)	488	32	77	12432 (+23.3%)
R-SDP 3	fast	127	7	187	111	-	239 (-2.45%)	125	48	115	41406 (-2.99%)
	balanced	127	7	187	111	-	384 (-3.52%)	321	48	115	29853 (+5.78%)
	small	127	7	187	111	-	580 (-38.6%)	527	48	115	28391 (+20.1%)
R-SDP 5	fast	127	7	251	150	-	321 (-1.83%)	167	64	153	74590 (-2.24%)
	balanced	127	7	251	150	-	512 (+0.99%)	427	64	153	53527 (+4.84%)
	small	127	7	251	150	-	832 (-14.0%)	762	64	153	50818 (+16.6%)
R-SDP ^(G) 1	fast	509	127	55	36	25	147 (-3.92%)	76	32	54	11980 (-3.94%)
	balanced	509	127	55	36	25	256 (+5.35%)	220	32	54	9120 (-1.26%)
	small	509	127	55	36	25	512 (-41.2%)	484	32	54	8960 (+12.6%)
R-SDP ^(G) 3	fast	509	127	79	48	40	224 (-2.61%)	119	48	83	26772 (-2.31%)
	balanced	509	127	79	48	40	268 (+5.10%)	196	48	83	22464 (-3.92%)
	small	509	127	79	48	40	512 (-46.0%)	463	48	83	20452 (+12.4%)
R-SDP ^(G) 5	fast	509	127	106	69	48	300 (-1.96%)	153	64	106	48102 (-1.71%)
	balanced	509	127	106	69	48	356 (0)	258	64	106	40100 (\approx 0%)
	small	509	127	106	69	48	642 (-35.5%)	575	64	106	36454 (+11.3%)

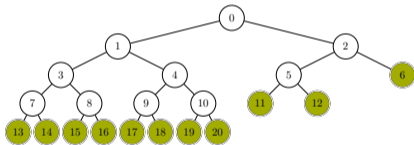
Implementation related, KAT changing etc.

■ SHAKE as CSPRNG and Hash

- consistent little-endian domain separation
- fixed randomness estimation for rejection sampling

■ Unified GGM/Merkle trees

- same structure
- bound for worst-case path/proof size is proven [Bor+23]



■ Further changes

- Ordering of elements in signature (better alignment)
- Sampling order of public matrices
- Big endian \rightarrow little endian bitpacking
- Seed dependent KATs 😊

Signature \leftarrow (Salt, d_{01} , d_b , MerkleProofs, SeedPaths, rsp_0 , rsp_1)



Sgn \leftarrow (Salt, $digest_{cmt}$, $digest_{chall_2}$, Path, Proof, resp)

Outline

- 1 Overview
- 2 Round 2: parameters and specification
- 3 Implementation efforts and attacks**
- 4 What else?

SW
(AVX2)

AVX2 optimizations

- SIMD version of Keccak from XKCP
 - 4-parallel states used to accelerate tree structures
- R-SDP(G) exponentiation $g^{\bar{e}} \pmod{509}$ (since v2.2):
 - $g^{\bar{e}} = g^{\bar{e}_6 \bar{e}_5 \bar{e}_4 \bar{e}_3 \bar{e}_2 \bar{e}_1 \bar{e}_0} = (g^{2^4 \bar{e}_6 \bar{e}_5 \bar{e}_4} g^{\bar{e}_3 \bar{e}_2 \bar{e}_1 \bar{e}_0})$
 - 1 mult + 1 reduction using two precomputed look-up tables
- Extensive vectorization; improved vectorized Barret reduction for $p = 509$

Implementation II



SW
(AVX2)

SW
(embedded)

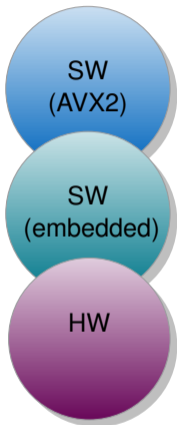
LightCROSS: A Secure and Memory Optimized Post-Quantum Digital Signature CROSS [Har+24]

- ARM Cortex-M4, CROSS v2.0
- Memory consumption Table 3:
 - ≈ 48 – 520kB (sign)
 - ≈ 14 – 158kB (verify)

Embedded SW – upcoming

- ARM Cortex-M4, CROSS v2.2
- 5 – 24kB stack, < 128kB total mem incl. signature + code
- < 47% cc overhead for sign, up to 18% less cc for verify

Implementation III



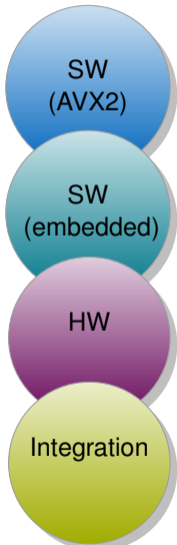
High-Performance FPGA Accelerator for the Post-quantum Signature Scheme CROSS [Kar+25]

- AMD Artix-7, CROSS v2.2
- Code release planned

Security level	Param.	Resources						Freq. MHz	KEYGEN		SIGN		VERIFY	
		LUT	FF	BRAM	DSP	KeSlice	ms		AT	ms	AT	ms	AT	
	RSDP-1-f	25805	11525	44.5	0	15.8	125	0.033	0.529	0.502	7.97	0.438	6.95	
	RSDP-1-b	26524	11654	57.0	0	18.7	117	0.036	0.666	0.902	16.8	0.731	13.6	
	RSDP-1-s	26947	11744	111.0	0	30.2	105	0.040	1.20	2.01	61.0	1.57	47.7	
	RSDPG-1-f	27456	11706	28.5	0	12.9	117	0.009	0.114	0.352	4.54	0.316	4.08	
	RSDPG-1-b	28026	11879	37.0	0	14.8	126	0.008	0.122	0.643	9.55	0.495	7.34	
	RSDPG-1-s	28620	12210	63.0	0	20.5	105	0.010	0.202	1.54	31.6	1.14	23.4	

→ See yesterday's talk

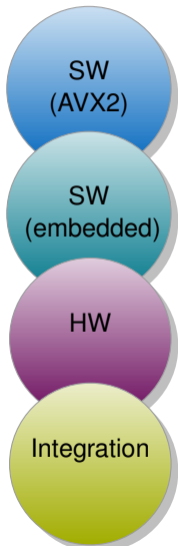
Implementation IV



Framework integration (CROSS v2.0)

- liboqs (Open Quantum Safe)
- SUPERCOP v2025.03.07
- pqm4 soon!

Implementation IV



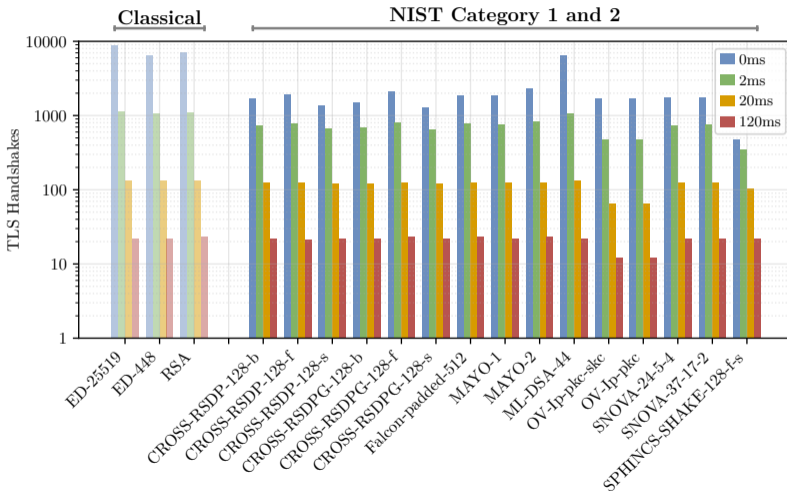
Framework integration (CROSS v2.0)

- liboqs (Open Quantum Safe)
- SUPERCOP v2025.03.07
- pqm4 soon!

TLS 1.3 experiments using oqs-provider – upcoming

- Root → Intermediate → Server certificate chain
- Network delay via Linux Traffic Control, BW capped at 0.5Gbps
- Server generates one signature, client verifies three signatures
- Set up certificate chain, then perform handshakes for 10s
- Code: <https://github.com/rtjk/CROSS-experiments>

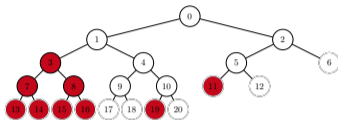
TLS 1.3 experiments



Physical attacks

■ *ZKFault: Fault Attack Analysis on Zero-Knowledge Based Post-quantum Digital Signature Schemes [Mon+24]*

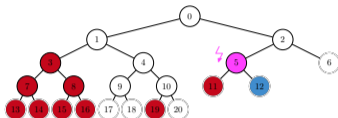
- Secret key recovery with 1 successful fault
- Attacks helper tree → reveal different seeds



Physical attacks

■ *ZKFault: Fault Attack Analysis on Zero-Knowledge Based Post-quantum Digital Signature Schemes* [Mon+24]

- Secret key recovery with 1 successful fault
- Attacks helper tree \rightarrow reveal different seeds



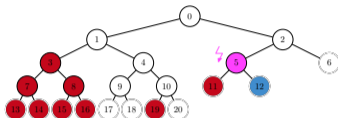
■ *A Horizontal Attack on the Codes and Restricted Objects Signature Scheme (CROSS)* [SS25]

- Targets $\mathbf{u}[i]$ during syndrome computation $\mathbf{s}'[i] = \mathbf{u}[i]\mathbf{H}^\top$ via SCA
- Allows to recover map $\mathbf{v}[i]$ and afterwards secret e from single power trace
- Should be preventable via masking or shuffling

Physical attacks

■ *ZKFault: Fault Attack Analysis on Zero-Knowledge Based Post-quantum Digital Signature Schemes* [Mon+24]

- Secret key recovery with 1 successful fault
- Attacks helper tree \rightarrow reveal different seeds



■ *A Horizontal Attack on the Codes and Restricted Objects Signature Scheme (CROSS)* [SS25]

- Targets $\mathbf{u}[i]$ during syndrome computation $s'[i] = \mathbf{u}[i]\mathbf{H}^\top$ via SCA
- Allows to recover map $\mathbf{v}[i]$ and afterwards secret e from single power trace
- Should be preventable via masking or shuffling

■ *Correlation Power Analysis of LESS and CROSS* [CMR25]

- same attack target as [SS25], but improved analysis

Outline

- 1 Overview
- 2 Round 2: parameters and specification
- 3 Implementation efforts and attacks
- 4 What else?**

What else?

- *Hash Your Keys Before Signing - BUFF Security of the Additional NIST PQC Signatures* [Aul+24]
 - CROSS achieves investigated BUFF security (S-CEO, S-DEO, MBS, wNR)

¹ Slides and abstract: <https://www.cb-crypto.org/previous-editions/cbcrypto2025/program>

What else?

- *Hash Your Keys Before Signing - BUFF Security of the Additional NIST PQC Signatures* [Aul+24]
 - CROSS achieves investigated BUFF security (S-CEO, S-DEO, MBS, wNR)

- *VOLeith-based Signatures from Restricted Decoding Problems* [BW25]¹
 - CROSS RSDP-1 code params: $|sig| \approx 4.9 \text{ kB}$ 😊
 - Loss of core benefits (e.g. simplicity, performance) 😞
 - No change planned

¹ Slides and abstract: <https://www.cb-crypto.org/previous-editions/cbcrypto2025/program>

Thank you for your attention!



CROSS: Codes & Restricted Objects Signature Scheme

info@cross-crypto.com

- ⊗ Marco Baldi
- ⊗ Alessandro Barenghi
- ⊗ Michele Battagliola
- ⊗ Sebastian Bitzer
- ⊗ Marco Gianvecchio
- ⊗ Patrick Karl
- ⊗ Felice Manganiello
- ⊗ Alessio Pavoni
- ⊗ Gerardo Pelosi
- ⊗ Federico Pintore
- ⊗ Paolo Santini
- ⊗ Jonas Schupp
- ⊗ Edoardo Signorini
- ⊗ Freeman Slaughter
- ⊗ Antonia Wachter-Zeh
- ⊗ Violetta Weger

References I

- [Aul+24] T. Aulbach et al. “Hash Your Keys Before Signing - BUFF Security of the Additional NIST PQC Signatures”. In: *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part II*. Ed. by M. O. Saarinen and D. Smith-Tone. Vol. 14772. Lecture Notes in Computer Science. Springer, 2024, pp. 301–335.
- [Bal+21] M. Baldi et al. *A New Path to Code-based Signatures via Identification Schemes with Restricted Errors*. 2021. arXiv: 2008.06403 [cs.CR].
- [Bal+23] M. Baldi et al. *Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem*. Cryptology ePrint Archive, Paper 2023/385. <https://eprint.iacr.org/2023/385>. 2023.
- [Bar94] S. Barg. “Some new NP-complete coding problems”. In: *Problemy Peredachi Informatsii* 30.3 (1994), pp. 23–28.
- [Bat+25] M. Battagliola et al. *A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures*. Cryptology ePrint Archive, Paper 2025/127. <https://eprint.iacr.org/2025/127>. 2025.
- [BBO24] W. Beullens, P. Briaud, and M. Øyngarden. *A Security Analysis of Restricted Syndrome Decoding Problems*. Cryptology ePrint Archive, Paper 2024/611. 2024.
- [BMVT78] E. Berlekamp, R. McEliece, and H. Van Tilborg. “On the inherent intractability of certain coding problems (corresp.)”. In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386.

References II

- [Bor+23] G. Borin et al. *A Guide to the Design of Digital Signatures based on Cryptographic Group Actions*. Cryptology ePrint Archive, Paper 2023/718. <https://eprint.iacr.org/2023/718>. 2023.
- [BW25] S. Bitzer and V. Weger. *VOLeith-based Signatures from Restricted Decoding Problems*. <https://drive.google.com/file/d/1uZ7rgzazRT0RqNZyWUw6Ch2wTX4h12Zf/view>. 2025.
- [CMR25] M. Czuprynko, A. Mukherjee, and S. S. Roy. “Correlation Power Analysis of LESS and CROSS”. In: *Progress in Cryptology - AFRICACRYPT 2025 - 16th International Conference on Cryptology in Africa, Rabat, Morocco, July 21-23, 2025, Proceedings*. Ed. by A. Nitaj, S. Petkova-Nikova, and V. Rijmen. Vol. 15651. Lecture Notes in Computer Science. Springer, 2025, pp. 270–295.
- [Har+24] H. Hart et al. *LightCROSS: A Secure and Memory Optimized Post-Quantum Digital Signature CROSS*. Cryptology ePrint Archive, Paper 2024/1929. <https://eprint.iacr.org/2024/1929>. 2024.
- [Kar+25] P. Karl et al. *High-Performance FPGA Accelerator for the Post-quantum Signature Scheme CROSS*. Cryptology ePrint Archive, Paper 2025/1161. <https://eprint.iacr.org/2025/1161>. 2025.
- [KZ20] D. Kales and G. Zaverucha. “An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes”. In: *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*. Ed. by S. Krenn, H. Schulmann, and S. Vaudenay. Vol. 12579. Lecture Notes in Computer Science. Springer, 2020, pp. 3–22.

References III

- [Mon+24] P. Mondal et al. “ZKFault: Fault Attack Analysis on Zero-Knowledge Based Post-quantum Digital Signature Schemes”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part VIII*. Ed. by K. Chung and Y. Sasaki. Vol. 15491. Lecture Notes in Computer Science. Springer, 2024, pp. 132–167.
- [SS25] J. Schupp and G. Sigl. “A Horizontal Attack on the Codes and Restricted Objects Signature Scheme (CROSS)”. In: *IACR Cryptol. ePrint Arch.* (2025), p. 116.

Performance numbers

NIST Cat.	Parameter Set	KeyGen (Mcycles)	Sign (Mcycles)	Verify (Mcycles)
1	CROSS-R-SDP-f	0.052	1.366	0.781
	CROSS-R-SDP-b	0.052	2.361	1.539
	CROSS-R-SDP-s	0.051	4.783	3.290
	CROSS-R-SDP-(G)-f	0.027	0.744	0.482
	CROSS-R-SDP-(G)-b	0.031	1.452	0.989
	CROSS-R-SDP-(G)-s	0.027	2.849	1.995
3	CROSS-R-SDP-f	0.118	3.110	1.909
	CROSS-R-SDP-b	0.119	5.099	3.500
	CROSS-R-SDP-s	0.119	7.612	5.381
	CROSS-R-SDP-(G)-f	0.055	1.745	1.166
	CROSS-R-SDP-(G)-b	0.056	2.225	1.508
	CROSS-R-SDP-(G)-s	0.055	4.159	3.052
5	CROSS-R-SDP-f	0.184	5.501	3.453
	CROSS-R-SDP-b	0.184	8.802	6.054
	CROSS-R-SDP-s	0.183	14.062	10.009
	CROSS-R-SDP-(G)-f	0.094	2.912	1.961
	CROSS-R-SDP-(G)-b	0.094	3.577	2.463
	CROSS-R-SDP-(G)-s	0.092	6.289	4.509

Measurements collected on an Intel Core i7-12700K, clocked at 3.6GHz, averaged over 10k runs.

Compactness of R-SDP and R-SDP(G)

R-SDP

- Recall: $e \in \mathbb{E}^n$ such that $e\mathbf{H}^\top = \mathbf{s}$, $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$, g constant.
- e representable with exponents $\bar{e} \rightarrow n \log_2(z)$ bits.
- e.g. CROSS-1 ($n = 127$, $z = 7$, $p = 127$):
 - $127 * 3 = 381\text{b}$ instead of 889b if represented over \mathbb{F}_p .

R-SDP(G)

- Recall: $e \in G$ such that $e\mathbf{H}^\top = \mathbf{s}$, $G = \{\star_{i=1}^m \mathbf{a}_i^{\bar{u}_i} \mid \bar{u}_i \in \mathbb{F}_z\}$, g constant.
- e representable with exponents $\bar{u} \rightarrow m \log_2(z)$ bits, as $\bar{e} = \bar{u}\bar{M}_G$.
- e.g. CROSS-1 ($n = 55$, $m = 25$, $z = 127$, $p = 509$):
 - $25 * 7 = 175\text{b}$ instead of 495b if represented over \mathbb{F}_p .