CROSS

Signature scheme with restricted errors

Violetta Weger

3. PQC Update
Fraunhofer AISEC

May 13, 2024

2016 NIST standardization call for post-quantum PKE/KEM and signatures

CROSS - Timeline

2016	NIST standardization call	for post-quantum PKE/KEM and signatures
|		
2022	Standardized signatures:	Dilithium, FALCON, SPHINCS+

CROSS - Timeline

2016	NIST standardization call	for post-quantum PKE/KEM and signatures
2022	Standardized signatures:	Dilithium, FALCON, SPHINCS+
2023	NIST additional call	for signature schemes
	1st round candidates:	40 submissions 11 code-based

2016	NIST standardization call	for post-quantum PKE/KEM and signatures
2022	Standardized signatures:	Dilithium, FALCON, SPHINCS+
2023	NIST additional call	for signature schemes
	1st round candidates:	29 survivors 9 code-based

2016	NIST standardization call	for post-quantum PKE/KEM and signatures	
2022	Standardized signatures:	Dilithium, FALCON, SPHINCS+	
2023	NIST additional call	for signature schemes	
	1st round candidates:	29 survivors	9 code-based
2024	2nd round announced	approx 15 schemes	

CROSS - Timeline

2016	NIST standardization call	for post-quantum PKE/KEM and signatures
2022	Standardized signatures:	Dilithium, FALCON, SPHINCS+
2023	NIST additional call	for signature schemes
	1st round candidates:	29 survivors CROSS
2024	2nd round announced	approx 15 schemes

Implementation

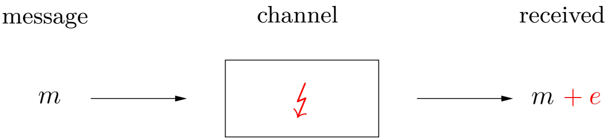
- optimized AVX2 — fast < 1 MCycle (NIST cat. I)
- memory-optimized — fits on Cortex-M4 microcontroller
- constant worst-case runtime — no signature rejection

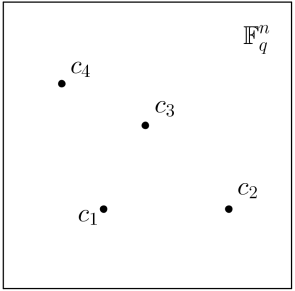
Ingredients

- Restricted Syndrome Decoding
  - → compact objects & efficient arithmetic
  - → NP-hard problem
- Zero-Knowledge protocol
  - → simple and well-studied
  - → EUF-CMA security
  - → standard optimizations

message channel received

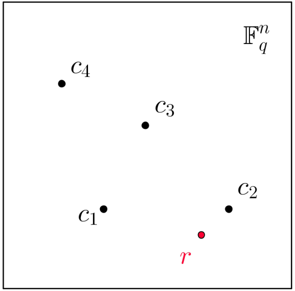
$$m \longrightarrow \boxed{\quad} \longrightarrow m + e$$





- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- G generator matrix $\rightarrow$ $c = mG$
- H parity-check matrix $\rightarrow$ $cH^\top = 0$

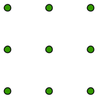
message	codeword	channel	received	message
m $\longrightarrow$	$c = mG$ $\longrightarrow$	$\lightning$ $\longrightarrow$	$r = c + e$ $\longrightarrow$	m

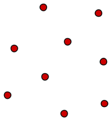


- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- G generator matrix $\quad \rightarrow \quad c = mG$
- H parity-check matrix $\quad \rightarrow \quad rH^\top = eH^\top = s$
- Hamming weight: $\mathrm{wt}(e) = |\{i \mid e_i \neq 0\}|$

Algebraic structure
(Reed-Solomon, Goppa,..)
→ efficient decoders

$\mathcal{C}$





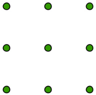
$\mathcal{C}'$

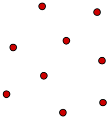
random code

→ how hard to decode?

Algebraic structure
(Reed-Solomon, Goppa,..)
$\rightarrow$ efficient decoders

$\mathcal{C}$





$\mathcal{C}'$

random code

$\rightarrow$ how hard to decode?

Syndrome Decoding Problem (SDP)

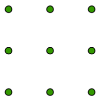
Given p.c. matrix H, syndrome s, target weight t, find e s.t.

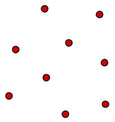
1. $s = eH^\top$ 2. $\mathrm{wt}(e) \leq t$

CROSS - Hard Problems

Algebraic structure
(Reed-Solomon, Goppa,..)
$\rightarrow$ efficient decoders

$\mathcal{C}$





$\mathcal{C}'$

random code

$\rightarrow$ how hard to decode?

Syndrome Decoding Problem (SDP)

Given p.c. matrix H, syndrome s, target weight t, find e s.t.

lin. constraint 1. $s = eH^\top$ 2. $\mathrm{wt}(e) \leq t$ non-lin. constraint

- SDP is NP-hard
- ISD: exponential cost

E. Berlekamp, R. McEliece, H. Van Tilborg. "On the inherent intractability of certain coding problems", IEEE TIT, 1978.

E. Prange. "The use of information sets in decoding cyclic codes", IRE TIT, 1962.

Prover	Verifier
secret	public
	✓

Prover		Verifier
	$\longleftarrow$	
secret	Interaction	public
	$\longrightarrow$	✓

signature scheme

Prover		Verifier
secret	Fiat-Shamir	public
	$\longrightarrow$	✓

signature scheme

Prover

secret

Fiat-Shamir

$\longrightarrow$

Verifier

public

✓

SDP Given H, s, t, find e s.t. 1. $s = eH^\top$, 2. $\mathrm{wt}(e) = t$

CROSS - Zero-Knowledge Protocol

signature scheme

Prover		Verifier
secret	Fiat-Shamir $\longrightarrow$	public ✓

SDP Given H, s, t, find e s.t. 1. $s = eH^\top$, 2. $\mathrm{wt}(e) = t$

e of $\mathrm{wt}(e) = t$

H, s, t

1. ✓ / 2. ✓

CROSS - Zero-Knowledge Protocol

signature scheme

Prover		Verifier
secret	Fiat-Shamir	public
	$\longrightarrow$	✓

SDP Given H, s, t, find e s.t. 1. $s = eH^\top$, 2. $\mathrm{wt}(e) = t$

e of $\mathrm{wt}(e) = t$

$e \xrightarrow{\varphi} \varphi(e)$

H, s, t

φ: 1. ✓ / $\varphi(e)$: 2. ✓

signature scheme

Prover		Verifier
secret	Fiat-Shamir	public
	$\longrightarrow$	✓

SDP Given H, s, t, find e s.t. 1. $s = eH^\top$, 2. $\mathrm{wt}(e) = t$

e of $\mathrm{wt}(e) = t$

$e \xrightarrow{\varphi} \varphi(e)$

H, s, t

φ: 1. ✓ / $\varphi(e)$: 2. ✓

J. Stern. "A new identification scheme based on syndrome decoding", Annual Int. Cryptology Conf., 1993.

P.-L. Cayrel, P. Véron, S. El Yousfi Alaoui. "A zero-knowledge identification scheme based on the q-ary syndrome decoding problem", Int. Workshop on Selected Areas in Cryptography, 2011.

CROSS - Zero-Knowledge Protocol

signature scheme

Prover		Verifier
secret	Fiat-Shamir $\longrightarrow$	public ✓

SDP Given H, s, t, find e s.t. 1. $s = eH^\top$, 2. $\mathrm{wt}(e) = t$

e of $\mathrm{wt}(e) = t$

$e \xrightarrow{\varphi} \varphi(e)$

H, s, t

φ: 1. ✓ / $\varphi(e)$: 2. ✓

e

	0	0			0

$\rightarrow \varphi \in (\mathbb{F}_q^\star)^n \rtimes S_n$

permutations are costly

Syndrome Decoding Problem Given p.c. matrix H, syndrome s, weight t, find e s.t.

lin. constraint 1. $s = eH^\top$ 2. $\mathrm{wt}(e) \leq t$ non-lin. constraint

Restricted SDP (R-SDP) Given p.c. matrix H, syndrome s, restriction $\mathbb{E}$, find e s.t.

lin. constraint 1. $s = eH^\top$ 2. $e \in \mathbb{E}^n$ non-lin. constraint

$$\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} < \mathbb{F}_q^\star$$

$g \in \mathbb{F}_q^\star$ of prime order z

Restricted SDP (R-SDP) Given p.c. matrix H, syndrome s, restriction $\mathbb{E}$, find e s.t.

lin. constraint 1. $s = eH^\top$ 2. $e \in \mathbb{E}^n$ non-lin. constraint

$\mathbb{E} = \{g^i \mid i \in \{1, \ldots, z\}\} < \mathbb{F}_q^\star$ $g \in \mathbb{F}_q^\star$ of prime order z

$$e \; \begin{array}{|c|c|c|c|c|c|} \hline & 0 & 0 & & & 0 \\ \hline \end{array} \quad \rightarrow \quad e \; \begin{array}{|c|c|c|c|c|c|} \hline & & & & & \\ \hline \end{array}$$

$\mathbb{F}_q^\star$ $\mathbb{F}_q^\star$ $\mathbb{F}_q^\star$ g^{i_1} g^{i_2} $\ldots$ g^{i_n}

- NP-hard
- adaption of ISD: exponential cost

Benefits of R-SDP

restriction $\mathbb{E} = \{g^i \mid i \in \{1, \ldots, z\}\}$

rest. vectors $e = (g^{i_1}, \ldots, g^{i_n}) \in \mathbb{F}_q^n$

Benefits of R-SDP

$$\text{restriction } \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \xrightarrow{\ \ell\ } \text{exponents } \mathbb{F}_z^n$$

$$\text{rest. vectors } e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n \qquad \ell(e) = (i_1, \dots, i_n) \in \mathbb{F}_z^n$$

Benefits of R-SDP

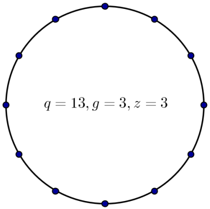
restriction $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$ $\xrightarrow{\ell}$ exponents $\mathbb{F}_z^n$

rest. vectors $e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n$ $\qquad$ $\ell(e) = (i_1, \dots, i_n) \in \mathbb{F}_z^n$

Example

- $g = 3 \in \mathbb{F}_{13}$ of order $z = 3$
- $\mathbb{E} = \{1, 3, 9\}$
- $e = (1, 9, 3, 3) \in \mathbb{E}^4$

$\rightarrow$ exponent $\ell(e) = (0, 2, 1, 1) \in \mathbb{F}_3^4$



CROSS - R-SDP

Benefits of R-SDP

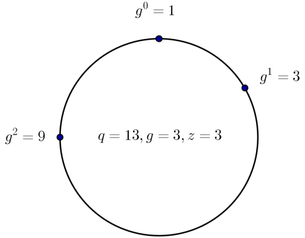
$$\text{restriction } \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \xrightarrow{\ell} \text{exponents } \mathbb{F}_z^n$$

$$\text{rest. vectors } e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n \qquad \ell(e) = (i_1, \dots, i_n) \in \mathbb{F}_z^n$$

Example

- $g = 3 \in \mathbb{F}_{13}$ of order $z = 3$
- $\mathbb{E} = \{1, 3, 9\}$
- $e = (1, 9, 3, 3) \in \mathbb{E}^4$

$\rightarrow$ exponent $\ell(e) = (0, 2, 1, 1) \in \mathbb{F}_3^4$



CROSS - R-SDP

Benefits of R-SDP

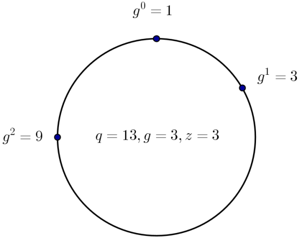
$$\text{restriction } \mathbb{E} = \{g^i \mid i \in \{1, \ldots, z\}\} \xrightarrow{\ell} \text{exponents } \mathbb{F}_z^n$$

$$\text{rest. vectors } e = (g^{i_1}, \ldots, g^{i_n}) \in \mathbb{F}_q^n \qquad \ell(e) = (i_1, \ldots, i_n) \in \mathbb{F}_z^n$$

Example

- $g = 3 \in \mathbb{F}_{13}$ of order $z = 3$
- $\mathbb{E} = \{1, 3, 9\}$
- $e = (1, 9, 3, 3) \in \mathbb{E}^4$

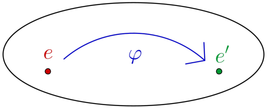
$\rightarrow$ exponent $\ell(e) = (0, 2, 1, 1) \in \mathbb{F}_3^4$



size $|e|$ SDP: $t\log_2(n) + t\log_2(q-1)$ R-SDP: $n\log_2(z)$

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$

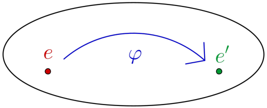


- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

CROSS - R-SDP

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$



- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

$$e = (g^{i_1}, \dots, g^{i_n})$$

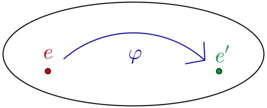
φ

$$e' = (g^{j_1}, \dots, g^{j_n})$$

CROSS - R-SDP

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$



- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

$$e = (g^{i_1}, \dots, g^{i_n})$$

$$\cdot \qquad \cdot$$

$$\tilde{e} = (g^{j_1 - i_1}, \dots, g^{j_n - i_n})$$

$$=$$

$$e' = (g^{j_1}, \dots, g^{j_n})$$

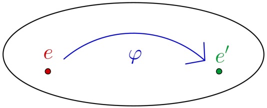
φ

$\rightarrow$ $\varphi(e) = e \star \tilde{e}$

$\rightarrow$ $\tilde{e} \in \mathbb{E}^n$

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$



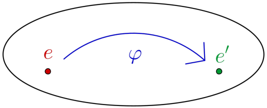
- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

$$
\begin{array}{llll}
 & e = (g^{i_1}, \dots, g^{i_n}) & (i_1, \dots, i_n) & \to \varphi(e) = e \star \tilde{e} \\
 & \quad\;\cdot \qquad\qquad\;\; \cdot & & \\
\varphi & \tilde{e} = (g^{j_1 - i_1}, \dots, g^{j_n - i_n}) & (j_1 - i_1, \dots, j_n - i_n) & \to \tilde{e} \in \mathbb{E}^n \\
 & \qquad\qquad = & & \\
 & e' = (g^{j_1}, \dots, g^{j_n}) & (j_1, \dots, j_n) &
\end{array}
$$

CROSS - R-SDP

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$

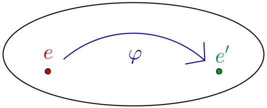


- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

$$
\begin{array}{lll}
e = (g^{i_1}, \dots, g^{i_n}) & (i_1, \dots, i_n) & \rightarrow \varphi(e) = e \star \tilde{e} \\
\quad\quad \cdot \quad\quad\quad\quad \cdot & \quad + \quad\quad\quad + & \\
\tilde{e} = (g^{j_1 - i_1}, \dots, g^{j_n - i_n}) & (j_1 - i_1, \dots, j_n - i_n) & \rightarrow \tilde{e} \in \mathbb{E}^n \\
\quad\quad\quad = & \quad\quad\quad = & \\
e' = (g^{j_1}, \dots, g^{j_n}) & (j_1, \dots, j_n) & \rightarrow \varphi(e) \text{ is } (\mathbb{F}_z^n, +)
\end{array}
$$

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$



- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

Example

$\mathbb{E}^4 = \{1, 3, 9\}^4 \subset \mathbb{F}_{13}^4$

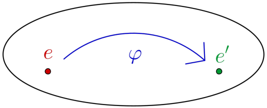
- $e = (1, 9, 3, 3)$
  $\star(3, 3, 9, 1)$
- $e' = (3, 1, 1, 3)$

exponents $\mathbb{F}_3^4$

- $\ell(e) = (0, 2, 1, 1)$
  $+(1, 1, 2, 0)$
- $\ell(e') = (1, 0, 0, 1)$

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$



- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

Example

$\mathbb{E}^4 = \{1,3,9\}^4 \subset \mathbb{F}_{13}^4$

- $e = (1,9,3,3)$
  $\star(3,3,9,1)$
- $e' = (3,1,1,3)$

exponents $\mathbb{F}_3^4$

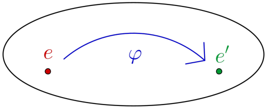
- $\ell(e) = (0,2,1,1)$
  $+(1,1,2,0)$
- $\ell(e') = (1,0,0,1)$

size $|\varphi|$ SDP: $n\log_2(n) + t\log_2(q-1)$ R-SDP: $n\log_2(z)$

CROSS - R-SDP

Benefits of R-SDP

ZK protocols need linear transitive maps $\varphi : S \to S$



- SDP: $S = \{e \mid \mathrm{wt}(e) = t\}$
- R-SDP: $S = \mathbb{E}^n$

Example

$\mathbb{E}^4 = \{1, 3, 9\}^4 \subset \mathbb{F}_{13}^4$

- $e = (1, 9, 3, 3)$
  $\star(3, 3, 9, 1)$
- $e' = (3, 1, 1, 3)$

exponents $\mathbb{F}_3^4$

- $\ell(e) = (0, 2, 1, 1)$
  $+(1, 1, 2, 0)$
- $\ell(e') = (1, 0, 0, 1)$

size $|\varphi|$ SDP: $n \log_2(n) + t \log_2(q-1)$ R-SDP: $n \log_2(z)$

$\varphi(e)$ SDP: $S_n \rtimes (\mathbb{F}_q^n, \cdot)$ R-SDP: $(\mathbb{F}_z^n, +)$

CROSS - R-SDP(G)

R-SDP Given H, s, $\mathbb{E}$, find e s.t. 1. $s = eH^\top$ 2. $e \in \mathbb{E}^n$

R-SDP(G) Given H, s, G, find e s.t. 1. $s = eH^\top$ 2. $e \in G$

subgroup $G = \langle x_1, \ldots, x_m \rangle < \mathbb{E}^n$

$G = \{e = {x_1}^{u_1} \star \cdots \star {x_m}^{u_m} \mid u_i \in \mathbb{F}_z\}$

R-SDP(G) Given H, s, G, find e s.t. 1. $s = eH^\top$ 2. $e \in G$

subgroup $G = \langle x_1, \dots, x_m \rangle < \mathbb{E}^n$

$G = \{e = {x_1}^{u_1} \star \cdots \star {x_m}^{u_m} \mid u_i \in \mathbb{F}_z\}$

Example

$\mathbb{E} = \{1, 3, 9\} \subset \mathbb{F}_{13}$

- $x_1 = (3, 1, 1, 3)$
  $x_2 = (1, 3, 9, 1)$
- $e = x_1^2 \star x_2^1 = (9, 3, 9, 9)$

R-SDP(G) Given H, s, G, find e s.t. 1. $s = eH^\top$ 2. $e \in G$

subgroup $G = \langle x_1, \dots, x_m \rangle < \mathbb{E}^n$

$G = \{e = {x_1}^{u_1} \star \cdots \star {x_m}^{u_m} \mid u_i \in \mathbb{F}_z\}$

Example

$\mathbb{E} = \{1, 3, 9\} \subset \mathbb{F}_{13}$

- $x_1 = (3, 1, 1, 3)$
  $x_2 = (1, 3, 9, 1)$
- $e = x_1^2 \star x_2^1 = (9, 3, 9, 9)$

exponents $\mathbb{F}_3^4$

- $M_G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix} \in \mathbb{F}_z^{m \times n}$
- $(2, 1)M_G = (2, 1, 2, 2)$
- send $(u_1, \dots, u_m) \in \mathbb{F}_z^m$

R-SDP(G) Given H, s, G, find e s.t. 1. $s = eH^\top$ 2. $e \in G$

subgroup $G = \langle x_1, \dots, x_m \rangle < \mathbb{E}^n$

$G = \{e = {x_1}^{u_1} \star \dots \star {x_m}^{u_m} \mid u_i \in \mathbb{F}_z\}$

Example

$\mathbb{E} = \{1, 3, 9\} \subset \mathbb{F}_{13}$

- $x_1 = (3, 1, 1, 3)$
  $x_2 = (1, 3, 9, 1)$
- $e = x_1^2 \star x_2^1 = (9, 3, 9, 9)$

exponents $\mathbb{F}_3^4$

- $M_G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix} \in \mathbb{F}_z^{m \times n}$
- $(2, 1)M_G = (2, 1, 2, 2)$
- send $(u_1, \dots, u_m) \in \mathbb{F}_z^m$

$|e| = |\varphi|$

R-SDP: $n \log_2(z)$

R-SDP(G): $m \log_2(z) < 1.5\lambda$

- $\mathbb{E}, G$ have multiplicative structure
  $e = (g^{i_1}, \ldots, g^{i_n})$
- $s = eH^\top$ has additive structure
  $s_j = \sum_{\ell=1}^{n} h_{j,\ell} g^{i_\ell}$ for $j \in \{1, \ldots, n-k\}$

- $\mathbb{E}, G$ have multiplicative structure
  $e = (g^{i_1}, \dots, g^{i_n})$
- Take $\mathbb{E}$ with no additive structure
- $s = eH^\top$ has additive structure
  $s_j = \sum_{\ell=1}^{n} h_{j,\ell} g^{i_\ell}$ for $j \in \{1, \dots, n-k\}$

- $\mathbb{E}, G$ have multiplicative structure
  $e = (g^{i_1}, \dots, g^{i_n})$
- $s = eH^\top$ has additive structure
  $s_j = \sum_{\ell=1}^{n} h_{j,\ell} g^{i_\ell}$ for $j \in \{1, \dots, n-k\}$
- Take $\mathbb{E}$ with no additive structure
- good: $q = 13, g = 3, \mathbb{E} = \{1, 3, 9\}$
- bad: $q = 13, g = 5, \mathbb{E} = \{1, 5, -1, -5\}$

- $\mathbb{E}, G$ have multiplicative structure
  $e = (g^{i_1}, \ldots, g^{i_n})$
- $s = eH^\top$ has additive structure
  $s_j = \sum_{\ell=1}^{n} h_{j,\ell} g^{i_\ell}$ for $j \in \{1, \ldots, n-k\}$
- Take $\mathbb{E}$ with no additive structure
- good: $q = 13, g = 3, \mathbb{E} = \{1, 3, 9\}$
- bad: $q = 13, g = 5, \mathbb{E} = \{1, 5, -1, -5\}$
- combinatorial:
  ISD algorithms

S. Bitzer, A. Pavoni, V. Weger, P. Santini, M. Baldi, and A. Wachter-Zeh. "Generic Decoding of Restricted Errors", ISIT, 2023.

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, and V. Weger. "Zero knowledge protocols and signatures from the restricted syndrome decoding problem", PKC, 2024.

- $\mathbb{E}, G$ have multiplicative structure
  $e = (g^{i_1}, \dots, g^{i_n})$
- $s = eH^\top$ has additive structure
  $s_j = \sum_{\ell=1}^{n} h_{j,\ell} g^{i_\ell}$ for $j \in \{1, \dots, n-k\}$
- Take $\mathbb{E}$ with no additive structure
- good: $q = 13, g = 3, \mathbb{E} = \{1, 3, 9\}$
- bad: $q = 13, g = 5, \mathbb{E} = \{1, 5, -1, -5\}$
- combinatorial:
  ISD algorithms
- algebraic attacks:
  $e_i^z = 1$ Gröbner basis

S. Bitzer, A. Pavoni, V. Weger, P. Santini, M. Baldi, and A. Wachter-Zeh. "Generic Decoding of Restricted Errors", ISIT, 2023.

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, and V. Weger. "Zero knowledge protocols and signatures from the restricted syndrome decoding problem", PKC, 2024.

M. Baldi, et al. "CROSS", NIST PQC round 1, 2023.

W. Beullens, P. Briaud, M. Øygarden. "A Security Analysis of Restricted Syndrome Decoding Problems", 2024.

CROSS - Performance

Standard optimizations

- Hash trees
- weighted challenges

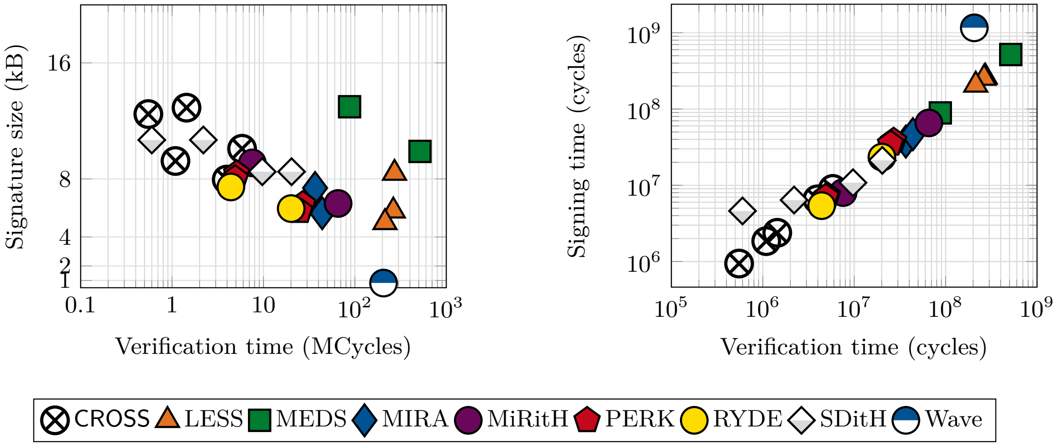
NIST cat. I

Problem	q, z	**Type**	(n, k, m)	**rounds**	**|Sign.|** (kB)	**Sign** (MCycles)	**Verify** (MCycles)
R-SDP	$(127, 7)$	fast	$(127, 76, -)$	163	19.1	1.28	0.78
		balanced		252	12.9	2.38	1.44
		short		960	10.1	8.96	5.84
R-SDP(G)	$(509, 127)$	fast	$(55, 36, 25)$	153	12.5	0.94	0.55
		balanced		243	9.2	1.85	1.09
		short		871	7.9	6.54	3.96

private and public keys < 0.1 kB

key gen. < 0.1 MCycle

Measurements collected on an AMD Ryzen 5 Pro 3500U, clocked at 2.1GHz. The computer was running Debian GNU/Linux 12



Timings taken from `https://pqshield.github.io/nist-sigs-zoo/`

What's next?

- Hardware implementation
- Side-channel protection
- Worst-case to average-case reduction
- Smaller signatures?

CROSS

Codes & Restricted Objects Signature Scheme
`http://cross-crypto.com/`

Slides

Website

What's next?

- Hardware implementation
- Side-channel protection
- Worst-case to average-case reduction
- Smaller signatures?

Slides

Website

CROSS

Codes & Restricted Objects Signature Scheme

`http://cross-crypto.com/`

Thank you!

CVE

PROVER		VERIFIER
KEY GENERATION		
Choose e with $\mathrm{wt}(e) \leq t$		
H parity-check matrix		
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$	
		VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\sigma \in \mathcal{S}_n$		
Set $c_1 = \mathrm{Hash}(\sigma, uH^\top)$		
Set $c_2 = \mathrm{Hash}(\sigma(u), \sigma(e))$	$\xrightarrow{c_1, c_2}$	
	$\xleftarrow{z}$	Choose $z \in \mathbb{F}_q^\times$
Set $y = \sigma(u + ze)$	$\xrightarrow{y}$	
$r_1 = \sigma$	$\xleftarrow{b}$	Choose $b \in \{1, 2\}$
$r_2 = \sigma(e)$	$\xrightarrow{r_b}$	$b = 1$: $c_1 = \mathrm{Hash}(\sigma, \sigma^{-1}(y)H^\top - zs)$
		$b = 2$: $\mathrm{wt}(\sigma(e)) = t$
		and $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

CVE

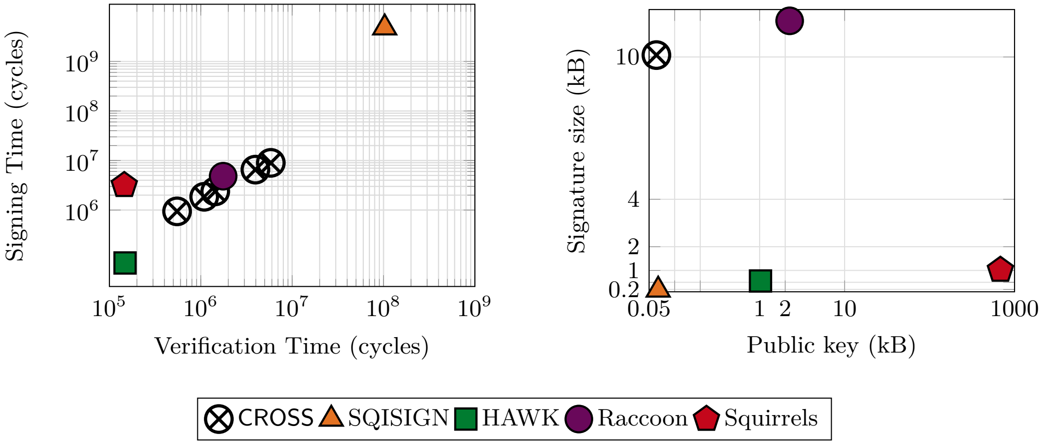
PROVER		VERIFIER
KEY GENERATION		
Choose e with $\mathrm{wt}(e) \leq t$		
H parity-check matrix		
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$	
		VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\sigma \in \mathcal{S}_n$		
Set $c_1 = \mathrm{Hash}(\sigma, uH^\top)$		
Set $c_2 = \mathrm{Hash}(\sigma(u), \sigma(e))$	$\xrightarrow{c_1, c_2}$	
	$\xleftarrow{z}$	Choose $z \in \mathbb{F}_q^\times$
Set $y = \sigma(u + ze)$	$\xrightarrow{y}$	
$r_1 = \sigma$	$\xleftarrow{b}$	Choose $b \in \{1, 2\}$
$r_2 = \sigma(e)$	$\xrightarrow{r_b}$	$b = 1$: $c_1 = \mathrm{Hash}(\sigma, \sigma^{-1}(y)H^\top - zs)$
		$b = 2$: $\mathrm{wt}(\sigma(e)) = t$
		and $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

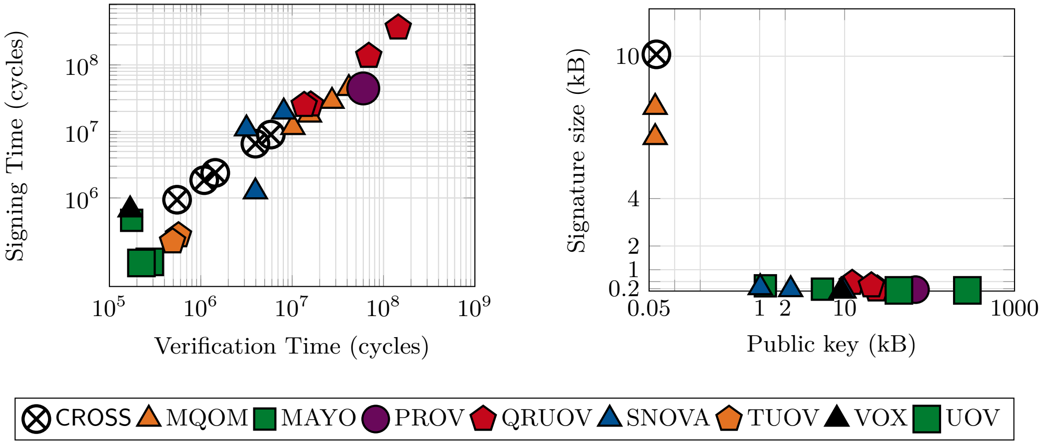
Recall SDP: (1) $s = eH^\top$ (2) $\mathrm{wt}(e) \leq t$

CVE

PROVER		VERIFIER
KEY GENERATION		
Choose e with $\mathrm{wt}(e) \leq t$		
H parity-check matrix		
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$	
		VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\sigma \in \mathcal{S}_n$		
Set $c_1 = \mathrm{Hash}(\sigma, uH^\top)$		
Set $c_2 = \mathrm{Hash}(\sigma(u), \sigma(e))$	$\xrightarrow{c_1, c_2}$	
	$\xleftarrow{z}$	Choose $z \in \mathbb{F}_q^\times$
Set $y = \sigma(u + ze)$	$\xrightarrow{y}$	
$r_1 = \sigma$	$\xleftarrow{b}$	Choose $b \in \{1, 2\}$
$r_2 = \sigma(e)$	$\xrightarrow{r_b}$	$b = 1$: $c_1 = \mathrm{Hash}(\sigma, \sigma^{-1}(y)H^\top - zs)$
		$b = 2$: $\mathrm{wt}(\sigma(e)) = t$
		and $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

$\boxed{\text{Problem: big signature sizes}}$


Signing Time (cycles)
10^9
10^8
10^7
10^6
10^5
10^6
10^7
10^8
10^9
Verification Time (cycles)
Signature size (kB)
10
4
2
1
0.2
0.05
1
2
10
1000
Public key (kB)
CROSS
SQISIGN
HAWK
Raccoon
Squirrels


Signing Time (cycles)
10^6
10^7
10^8
10^5
10^6
10^7
10^8
10^9
Verification Time (cycles)
Signature size (kB)
10
4
2
1
0.2
0.05
1
2
10
1000
Public key (kB)
CROSS
MQOM
MAYO
PROV
QRUOV
SNOVA
TUOV
VOX
UOV