



CROSS

A signature scheme with restricted errors

Violetta Weger

Joint Mathematics Meetings
Cryptography and Related Fields

January 11, 2025



CROSS

-

Timeline

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



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 9 code-based



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 9 code-based
2024	2nd round announced	14 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	9 code-based
2024	2nd round announced	14 schemes	CROSS



Implementation

- optimized AVX2
- memory-optimized
- constant worst-case runtime
- available on lib open quantum safe

fast < 1 MCycle (NIST cat. I)
fits on Cortex-M4 microcontroller
no signature rejection



Ingredients

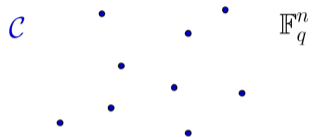
- Restricted Syndrome Decoding → compact objects & efficient arithmetic
- Zero-Knowledge protocol → NP-hard problem
- → simple and well-studied
- → EUF-CMA security
- → BUFF security
- → standard optimizations



CROSS

-

Basics



- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace

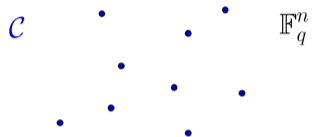
- G generator matrix $\rightarrow c = mG$



CROSS

-

Basics



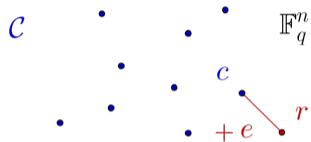
- Code $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace
- H parity-check matrix $\rightarrow cH^T = 0$



CROSS

-

Basics



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

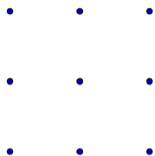


CROSS

-

Basics

\mathcal{C}



\mathbb{F}_q^n

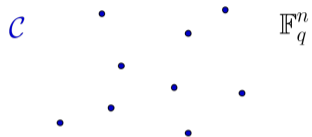
- algebraic structure
- e.g. RS, Goppa codes
- efficient decoders



CROSS

-

Basics



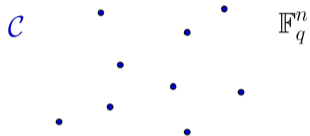
- random code
- decoding is NP-hard
- Information set decoding



CROSS

-

Basics



- random code
- decoding is NP-hard
- Information set decoding

Syndrome Decoding Problem (SDP)

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

1. $s = eH^T$

2. $\text{wt}(e) = t$



CROSS

-


Zero-Knowledge Protocol

Signature Scheme

Signer

 secret

Verifier

 public





CROSS

-

Zero-Knowledge Protocol


Signature Scheme

Signer

 secret



Verifier

 public





CROSS

-

Zero-Knowledge Protocol


Signature Scheme

Signer

 secret



Verifier

 public





CROSS

-

Zero-Knowledge Protocol

ZK Protocol

Prover

♀ secret



Interaction



Verifier

♀ public





CROSS

-

Zero-Knowledge Protocol

Signature Scheme

Signer

🔑 secret

Fiat-Shamir



Verifier

🔑 public





CROSS

-

Zero-Knowledge Protocol

Signature Scheme

Impersonator

cheating prob.

Fiat-Shamir



Verifier

♀ public

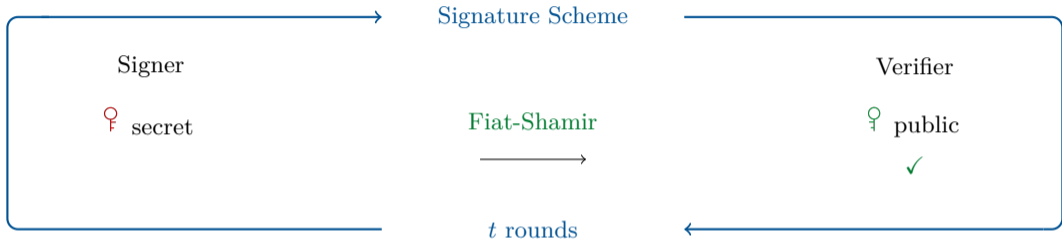




CROSS

-

Zero-Knowledge Protocol





CROSS

-

Zero-Knowledge Protocol

ZK Protocol

Prover

♀ secret



Interaction



Verifier

♀ public



SDP

Given H , s , t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$



CROSS

-

Zero-Knowledge Protocol

ZK Protocol

Prover

♀ secret



Interaction



Verifier

♀ public



SDP

Given H, s, t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$

♀ H, s, t

1. ✓ / 2. ✓



CROSS

-

Zero-Knowledge Protocol

ZK Protocol

Prover

♀ secret



Interaction



Verifier

♀ public



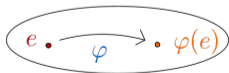
SDP

Given H, s, t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$



♀ H, s, t

φ : 1. ✓ / $\varphi(e)$: 2. ✓



SDP

Given H, s, t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$ ♀ 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.



SDP

Given H, s, t , find e s.t.

1. $s = eH^T,$

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$



♀ 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.

1. Problem

cheating prob. $\sim \frac{1}{2}$ \rightarrow many rounds



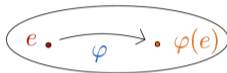
SDP

Given H, s, t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$



♀ 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.

1. Problem

cheating prob. $\sim \frac{1}{2}$

→ many rounds

→ Solution

MPCitH: change protocol

→ slow



SDP

Given H, s, t , find e s.t.

1. $s = eH^T,$

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$ ♀ 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.

1. Problem

cheating prob. $\sim \frac{1}{2}$

→ many rounds

→ Solution

MPCitH: change protocol

→ slow

 $S = \{e \mid \text{wt}(e) = t\}$ $\varphi : S \rightarrow S$ linear, transitive→ $|\varphi|$ large



SDP

Given H, s, t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$ ♀ 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.

1. Problem

cheating prob. $\sim \frac{1}{2}$

→ many rounds

→ Solution

MPCitH: change protocol

→ slow

$S = \{e \mid \text{wt}(e) = t\}$

 $\varphi: S \rightarrow S$ linear, transitive→ $|\varphi|$ large

2. Problem

1 round: large commun. cost

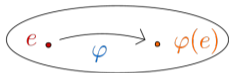


SDP

Given H, s, t , find e s.t.

1. $s = eH^T$,

2. $\text{wt}(e) = t$

♀ e of $\text{wt}(e) = t$ ♀ 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.

1. Problem

cheating prob. $\sim \frac{1}{2}$

→ many rounds

→ Solution

MPCitH: change protocol

→ slow

$S = \{e \mid \text{wt}(e) = t\}$

 $\varphi: S \rightarrow S$ linear, transitive→ $|\varphi|$ large

2. Problem

1 round: large commun. cost

→ Solution

change underlying problem

→ CROSS



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

lin. constraint

1. $s = eH^T$

2. $\text{wt}(e) = t$

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

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

$g \in \mathbb{F}_q^*$ 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. $s = eH^T$

2. $e \in \mathbb{E}^n$

non-lin. constraint

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

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

e

	0	0			0
--	---	---	--	--	---

\mathbb{F}_q^* \mathbb{F}_q^* \mathbb{F}_q^*

→

e

--	--	--	--	--	--

g^{i_1} g^{i_2} ... g^{i_n}

○ NP-hard

○ adaption of ISD: exponential cost



CROSS

-

R-SDP

Benefits

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

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



CROSS

-

R-SDP

Benefits

$$\begin{array}{l} \text{restriction } \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \\ \text{rest. vectors } e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n \end{array} \xrightarrow{\ell} \begin{array}{l} \text{exponents } \mathbb{F}_z^n \\ \ell(e) = (i_1, \dots, i_n) \end{array}$$



CROSS

-

R-SDP

Benefits

restriction $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$	$\xrightarrow{\ell}$	exponents \mathbb{F}_z^n
rest. vectors $e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n$		$\ell(e) = (i_1, \dots, i_n)$
secret space $S = \mathbb{E}^n, \varphi : S \rightarrow S$	$\xrightarrow{\ell}$	$ e = \varphi = n \log_2(z)$
$\varphi(e) = e' \star e, e' = (g^{j_1}, \dots, g^{j_n})$		



CROSS

-

R-SDP

Benefits

restriction $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$	$\xrightarrow{\ell}$	exponents \mathbb{F}_z^n
rest. vectors $e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n$		$\ell(e) = (i_1, \dots, i_n)$
secret space $S = \mathbb{E}^n, \varphi : S \rightarrow S$	$\xrightarrow{\ell}$	$ e = \varphi = n \log_2(z)$
$\varphi(e) = e' \star e, e' = (g^{j_1}, \dots, g^{j_n})$		$\ell(\varphi(e)) = \ell(e) + \ell(e')$



CROSS

-

R-SDP

Benefits

$$\begin{array}{lcl}
 \text{restriction } \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} & \xrightarrow{\ell} & \text{exponents } \mathbb{F}_z^n \\
 \text{rest. vectors } e = (g^{i_1}, \dots, g^{i_n}) \in \mathbb{F}_q^n & & \ell(e) = (i_1, \dots, i_n) \\
 \text{secret space } S = \mathbb{E}^n, \varphi : S \rightarrow S & \xrightarrow{\ell} & |e| = |\varphi| = n \log_2(z) \\
 \varphi(e) = e' \star e, e' = (g^{j_1}, \dots, g^{j_n}) & & \ell(\varphi(e)) = \ell(e) + \ell(e')
 \end{array}$$

Example

$$\begin{array}{lcl}
 \mathbb{E} = \{1, 3, 9\} \subset \mathbb{F}_{13} & \xrightarrow{\ell} & \text{exponents in } \mathbb{F}_3^4 \\
 e = (1, 9, 3, 3) & & \ell(e) = (0, 2, 1, 1) \\
 \downarrow \star(3, 3, 9, 1) & & \downarrow + (1, 1, 2, 0) \\
 \tilde{e} = (3, 1, 1, 3) & & \ell(\tilde{e}) = (1, 0, 0, 1)
 \end{array}$$



CROSS

-

R-SDP(G)

R-SDP

Given H, s, \mathbb{E} , find e s.t. 1. $s = eH^T$ 2. $e \in \mathbb{E}^n$ $(\mathbb{E}^n, \star) \simeq (\mathbb{F}_z^n, +)$



CROSS

-

R-SDP(G)

R-SDP(G) Given H, s, G , find e s.t. 1. $s = eH^T$ 2. $e \in G$ (G, \star) $<$ (\mathbb{E}^n, \star)

Benefits

$$x_1 = (g^{i_1}, \dots, g^{i_n})$$

$$\vdots$$

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



CROSS

-

R-SDP(G)

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

Benefits

$$x_1 = (g^{i_1}, \dots, g^{i_n})$$

$$\vdots$$

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

$$\xrightarrow{\ell}$$

$$M = \begin{pmatrix} i_1 & \cdots & i_n \\ \vdots & & \vdots \\ j_1 & \cdots & j_n \end{pmatrix} \in \mathbb{F}_z^{m \times n}$$



CROSS

-

R-SDP(G)

R-SDP(G) Given H, s, G , find e s.t. 1. $s = eH^\top$ 2. $e \in G$ $G \simeq \mathcal{C} \subset \mathbb{F}_z^n$

Benefits

$$\begin{array}{l}
 \mathbf{x}_1 = (g^{i_1}, \dots, g^{i_n}) \\
 \vdots \\
 \mathbf{x}_m = (g^{j_1}, \dots, g^{j_n}) \\
 e = \mathbf{x}_1^{u_1} \star \dots \star \mathbf{x}_m^{u_m} \\
 \varphi : G \rightarrow G, \varphi(e) = e' \star e
 \end{array}
 \xrightarrow{\ell}
 \begin{array}{l}
 M = \begin{pmatrix} i_1 & \cdots & i_n \\ \vdots & & \vdots \\ j_1 & \cdots & j_n \end{pmatrix} \in \mathbb{F}_z^{m \times n} \\
 \ell(e) = (u_1, \dots, u_m)M \\
 |e| = |\varphi| = m \log_2(z) < 1.5\lambda
 \end{array}$$



R-SDP(G) Given H, s, G , find e s.t. 1. $s = eH^\top$ 2. $e \in G$ $G \simeq \mathcal{C} \subset \mathbb{F}_z^n$

Benefits

$$\begin{array}{l} x_1 = (g^{i_1}, \dots, g^{i_n}) \\ \vdots \\ x_m = (g^{j_1}, \dots, g^{j_n}) \end{array} \xrightarrow{\ell} M = \begin{pmatrix} i_1 & \cdots & i_n \\ \vdots & & \vdots \\ j_1 & \cdots & j_n \end{pmatrix} \in \mathbb{F}_z^{m \times n}$$

$$e = x_1^{u_1} \star \cdots \star x_m^{u_m} \quad \ell(e) = (u_1, \dots, u_m)M$$

$$\varphi : G \rightarrow G, \varphi(e) = e' \star e \xrightarrow{\ell} |e| = |\varphi| = m \log_2(z) < 1.5\lambda$$

Example

$$\mathbb{E} = \{1, 3, 9\} \subset \mathbb{F}_{13} \xrightarrow{\ell} \text{exponents in } \mathbb{F}_3^4$$

$$x_1 = (3, 1, 1, 3) \quad M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix}$$

$$x_2 = (1, 3, 9, 1)$$

$$e = x_1^{\textcircled{2}} \star x_2^{\textcircled{1}} = (9, 3, 9, 9) \quad \ell(e) = (2, 1, 2, 2) = (2, 1)M$$



CROSS

-

Attacks

- \mathbb{E}, G have **multiplicative** structure

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

- $s = eH^\top$ has **additive** structure

$$s_j = \sum_{\ell=1}^n h_{j,\ell} g^{i_\ell} \text{ for } j \in \{1, \dots, n-k\}$$



CROSS

-

Attacks

- \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

$$s_j = \sum_{\ell=1}^n h_{j,\ell} g^{i_\ell} \text{ for } j \in \{1, \dots, n-k\}$$



CROSS

-

- \mathbb{E}, G have **multiplicative** structure
 $e = (g^{i_1}, \dots, g^{i_n})$
- Take \mathbb{E} with **no** additive structure
- **good**: $q = 13, g = 3, \mathbb{E} = \{1, 3, 9\}$

Attacks

- $s = eH^\top$ has **additive** structure
 $s_j = \sum_{\ell=1}^n h_{j,\ell} g^{i_\ell}$ for $j \in \{1, \dots, n-k\}$
- **bad**: $q = 13, g = 5, \mathbb{E} = \{1, 5, -1, -5\}$



CROSS

-

Attacks

- o \mathbb{E}, G have **multiplicative** structure

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

- o Take \mathbb{E} with **no** additive structure

- o **good**: $q = 13, g = 3, \mathbb{E} = \{1, 3, 9\}$

- o combinatorial:

ISD algorithms

- o $s = eH^\top$ has **additive** structure

$$s_j = \sum_{\ell=1}^n h_{j,\ell} g^{i_\ell} \text{ for } j \in \{1, \dots, n-k\}$$

- o **bad**: $q = 13, g = 5, \mathbb{E} = \{1, 5, -1, -5\}$



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.



CROSS

-

Attacks

- o \mathbb{E}, G have **multiplicative** structure

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

- o Take \mathbb{E} with **no** additive structure

- o **good**: $q = 13, g = 3, \mathbb{E} = \{1, 3, 9\}$

- o combinatorial:

ISD algorithms

- o algebraic attacks:

$e_i^z = 1$ Gröbner basis

- o $s = eH^\top$ has **additive** structure

$$s_j = \sum_{\ell=1}^n h_{j,\ell} g^{i_\ell} \text{ for } j \in \{1, \dots, n - k\}$$

- o **bad**: $q = 13, g = 5, \mathbb{E} = \{1, 5, -1, -5\}$



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.



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

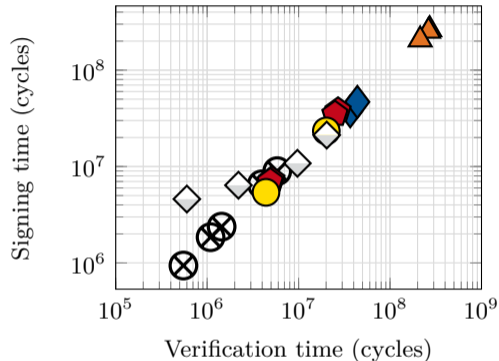
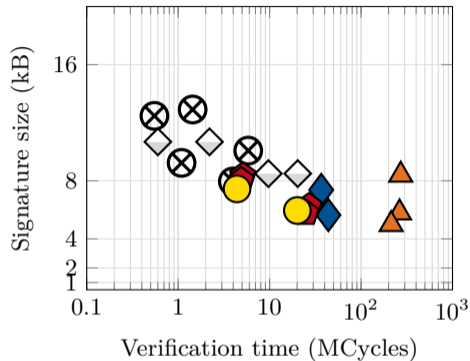
Measurements collected on an AMD Ryzen 5 Pro 3500U, clocked at 2.1GHz. The computer was running Debian GNU/Linux 12



CROSS

-

Comparison



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?



Slides



CROSS

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



Website



What's next?

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



Slides



CROSS

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



Website

Thank you!

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

CVE

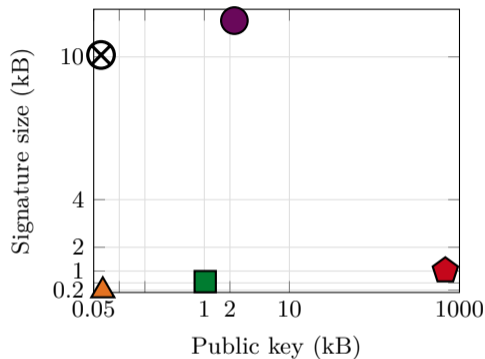
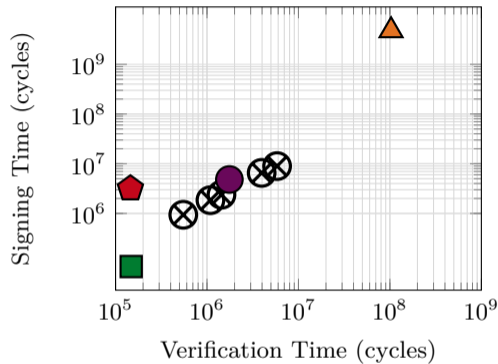
PROVER	VERIFIER
KEY GENERATION	Recall SDP: (1) $s = eH^\top$ (2) $\text{wt}(e) = t$
Choose e with $\text{wt}(e) = t$ H parity-check matrix Compute $s = eH^\top$	
	VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\varphi \in \mathcal{M}_n$ Set $c_1 = \text{Hash}(\varphi, uH^\top)$ Set $c_2 = \text{Hash}(\varphi(u),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

PROVER	VERIFIER
KEY GENERATION	
Choose e with $\text{wt}(e) = t$	
H parity-check matrix	
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$
VERIFICATION	
Choose $u \in \mathbb{F}_q^n, \varphi \in \mathcal{M}_n$	
Set $c_1 = \text{Hash}(\varphi, uH^\top)$	
Set $c_2 = \text{Hash}(\varphi(u), \varphi(e))$	$\xrightarrow{c_1, c_2}$
	\xleftarrow{z}
Set $y = \varphi(u + ze)$	\xrightarrow{y}
$r_1 = \varphi$	\xleftarrow{b}
$r_2 = \varphi(e)$	$\xrightarrow{r_b}$
	<div style="border: 1px solid red; padding: 5px; display: inline-block; color: red;"> Problem: big signature sizes </div>
	Choose $z \in \mathbb{F}_q^\times$
	Choose $b \in \{1, 2\}$
	$b = 1: c_1 = \text{Hash}(\varphi, \varphi^{-1}(y)H^\top - zs)$
	$b = 2: \text{wt}(\varphi(e)) = t$
	and $c_2 = \text{Hash}(y - z\varphi(e), \varphi(e))$



CROSS

- vs: Isogenies and lattices





CROSS

-

vs: Multivariate

