Recent Advances in Code-based Signatures

Violetta Weger

CAST Workshop:
Quantentechnologie und Quantencomputer-resistente Sicherheit

September 7, 2023

Motivation

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

Motivation

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

Standardized:	Signatures:	Dilithium, FALCON, SPHINCS+
	PKE/KEM:	KYBER
4th round:	PKE/KEM:	Classic McEliece, BIKE, HQC

Motivation

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

		based on structured lattices	Hash-based
Standardized:	Signatures:	Dilithium, FALCON,	SPHINCS+
	PKE/KEM:	KYBER	
4th round:	PKE/KEM:	Classic McEliece, BIKE, HQC	Code-based

Motivation

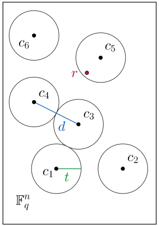
2016 NIST standardization call for post-quantum PKE/KEM and signatures

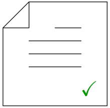
		based on structured lattices	Hash-based
Standardized:	Signatures:	Dilithium, FALCON,	SPHINCS+
	PKE/KEM:	KYBER	
4th round:	PKE/KEM:	Classic McEliece, BIKE, HQC	Code-based

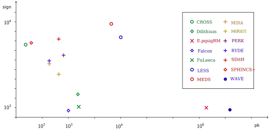
2023 NIST additional call for signature schemes → This talk

Outline

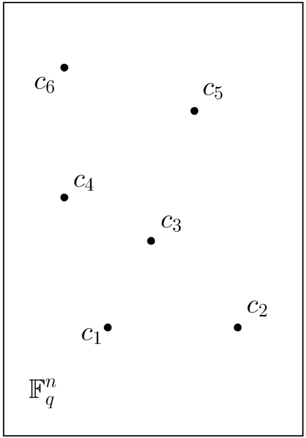
1. **Code-based Cryptography**
   - Introduction to Coding Theory
   - Hard Problems from Coding Theory
2. **Code-based Signature Schemes**
   - What is a Signature Scheme
   - Techniques to Construct Signatures
   - Our Scheme: CROSS
3. **Round 1 Submissions**
   - Survivors after 2 months of cryptanalysis
   - Efficiency and Performance







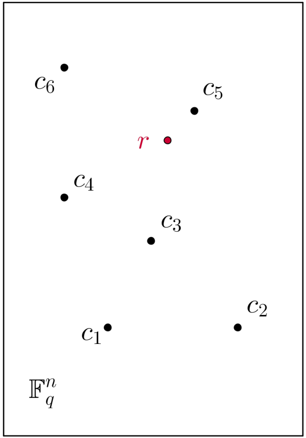
Coding Theory



Set Up

- *Code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- $c \in \mathcal{C}$ *codeword*
- $G \in \mathbb{F}_q^{k \times n}$ *generator matrix* $\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\}$
- $H \in \mathbb{F}_q^{(n-k) \times n}$ *parity-check matrix* $\mathcal{C} = \{c \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*

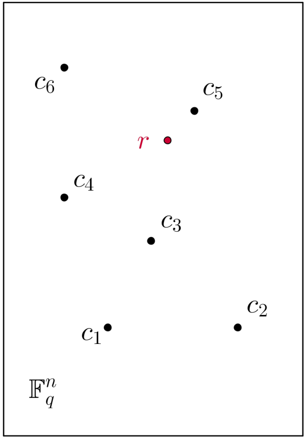
Coding Theory



Set Up

- *Code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- $c \in \mathcal{C}$ *codeword*
- $G \in \mathbb{F}_q^{k\times n}$ *generator matrix* $\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\}$
- $H \in \mathbb{F}_q^{(n-k)\times n}$ *parity-check matrix* $\mathcal{C} = \{c \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword

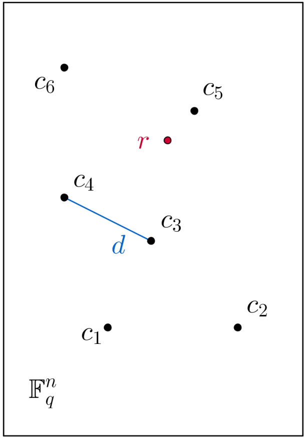
Coding Theory



Set Up

- *Code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- $c \in \mathcal{C}$ *codeword*
- $G \in \mathbb{F}_q^{k\times n}$ *generator matrix* $\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\}$
- $H \in \mathbb{F}_q^{(n-k)\times n}$ *parity-check matrix* $\mathcal{C} = \{c \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: $d_H(x,y) = \mid \{i \mid x_i \neq y_i\} \mid$

Coding Theory

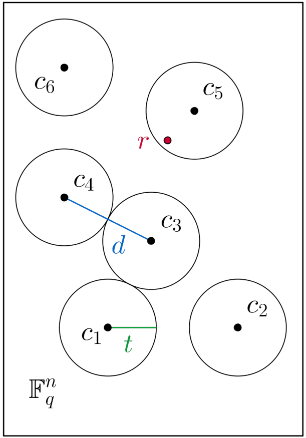


Set Up

- *Code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- $c \in \mathcal{C}$ *codeword*
- $G \in \mathbb{F}_q^{k \times n}$ *generator matrix* $\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\}$
- $H \in \mathbb{F}_q^{(n-k) \times n}$ *parity-check matrix* $\mathcal{C} = \{c \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: $d_H(x, y) = | \{i \mid x_i \neq y_i\} |$
- *minimum distance of a code:*

$$d(\mathcal{C}) = \min\{d_H(x, y) \mid x \neq y \in \mathcal{C}\}$$

Coding Theory



Set Up

- *Code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- $c \in \mathcal{C}$ *codeword*
- $G \in \mathbb{F}_q^{k \times n}$ *generator matrix* $\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\}$
- $H \in \mathbb{F}_q^{(n-k)\times n}$ *parity-check matrix* $\mathcal{C} = \{c \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: $d_H(x,y) = \mid \{i \mid x_i \neq y_i\} \mid$
- *minimum distance of a code*:

$$d(\mathcal{C}) = \min\{d_H(x,y) \mid x \neq y \in \mathcal{C}\}$$

- *error-correction capacity*: $t = \lfloor (d(\mathcal{C})-1)/2 \rfloor$

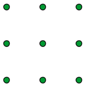
Hard Problems from Coding Theory

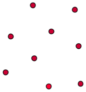
Algebraic structure

(Reed-Solomon, Goppa,..)

→ efficient decoders

$\langle G \rangle$





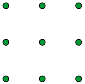
$\langle \widetilde{G} \rangle$

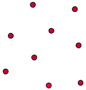
random code

→ how hard to decode?

Hard Problems from Coding Theory

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

$\langle G \rangle$ 

 $\langle \widetilde{G} \rangle$

random code

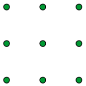
→ how hard to decode?

- Decoding random linear code is NP-hard

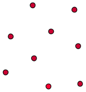
E. Berlekamp, R. McEliece, H. Van Tilborg. "On the inherent intractability of certain coding problems ", IEEE Trans. Inf. Theory, 1978.

Hard Problems from Coding Theory

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

$\langle G \rangle$ 

scrambling
$\xrightarrow{\varphi}$

 $\langle \widetilde{G} \rangle$

Seemingly random code

$\rightarrow$ how hard to decode?

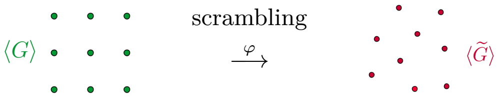
- Decoding random linear code is NP-hard
- First code-based cryptosystem based on this problem

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

R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory", DSNP Report, 1978

Hard Problems from Coding Theory

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



Seemingly random code
$\rightarrow$ how hard to decode?

- Decoding random linear code is NP-hard
- First code-based cryptosystem based on this problem
- Fastest solvers: ISD, exponential time

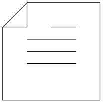
E. Berlekamp, R. McEliece, H. Van Tilborg. “On the inherent intractability of certain coding problems ”, IEEE Trans. Inf. Theory, 1978.

R. J. McEliece. “A public-key cryptosystem based on algebraic coding theory”, DSNP Report, 1978

A. Becker, A. Joux, A. May, A. Meurer “Decoding random binary linear codes in $2^{n/20}$: How 1+ 1= 0 improves information set decoding”, Eurocrypt, 2012.

Idea of Signature Schemes

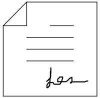
Signer



Verifier

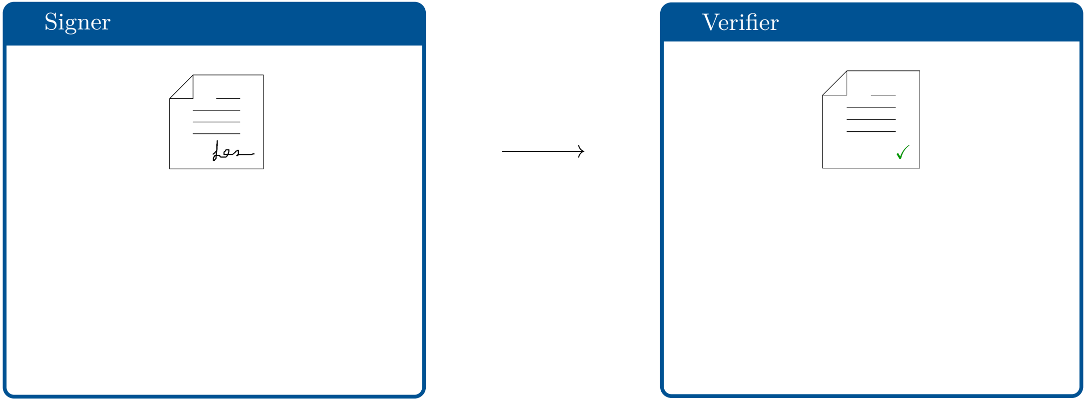
Idea of Signature Schemes

Signer



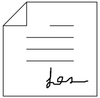
Verifier

Idea of Signature Schemes



Idea of Signature Schemes

Signer

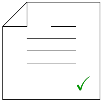


- Key Generation: $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\xrightarrow{\mathcal{P}}$

$\xrightarrow{m,\ \sigma}$

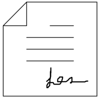
Verifier



- Verification: use $\mathcal{P}$ and message m to verify signature σ

Idea of Signature Schemes

Signer

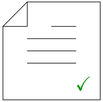


- Key Generation:
  $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

small $\mathcal{P}$

small σ

Verifier



fast verification

- Verification: use $\mathcal{P}$ and message m to verify signature σ

Idea of Signature Schemes

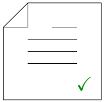
Signer

- Key Generation:
  $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

small $\mathcal{P}$

small σ

Verifier



fast verification

- Verification: use $\mathcal{P}$ and message m to verify signature σ

Approaches for signatures:

- Hash-and-Sign
- ZK Protocol
- ZK + MPC

Hash-and-Sign

First introduced in

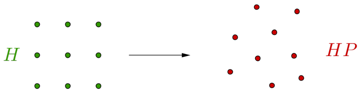
M. Bellare, P. Rogaway. "The exact security of digital signatures-How to sign with RSA and Rabin.", Int. conf. on the theory and app. of crypto. tech., 1996.

Following idea of McEliece

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

→ start with structured code H

→ publish scrambled code HP



Hash-and-Sign

First introduced in

Following idea of McEliece

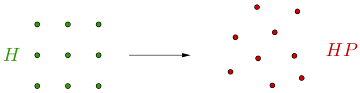
M. Bellare, P. Rogaway. "The exact security of digital signatures-How to sign with RSA and Rabin.", Int. conf. on the theory and app. of crypto. tech., 1996.

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

→ start with structured code H

→ publish scrambled code HP

→ large public key sizes



Hash-and-Sign

First introduced in

M. Bellare, P. Rogaway. "The exact security of digital signatures-How to sign with RSA and Rabin.", Int. conf. on the theory and app. of crypto. tech., 1996.

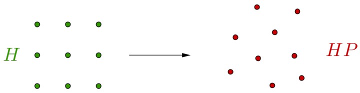
Following idea of McEliece

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

→ start with structured code H

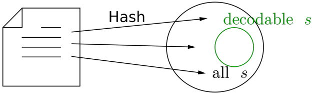
→ publish scrambled code HP

→ large public key sizes



→ $\text{Hash}(m) = eH^\top$, $\text{wt}_H(e) \leq t$

→ signature $\sigma = eP$



Hash-and-Sign

First introduced in

M. Bellare, P. Rogaway. “The exact security of digital signatures-How to sign with RSA and Rabin.”, Int. conf. on the theory and app. of crypto. tech., 1996.

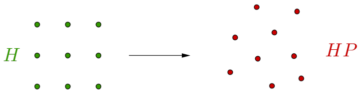
Following idea of McEliece

N. Courtois, M. Finiasz, N. Sendrier. “How to achieve a McEliece-based digital signature scheme”, Asiacrypt, 2001.

→ start with structured code H

→ publish scrambled code HP

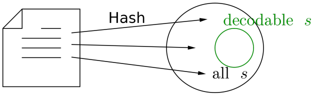
→ large public key sizes



→ $\text{Hash}(m) = eH^\top$, $\text{wt}_H(e) \leq t$

→ signature $\sigma = eP$

→ slow signing



Hash-and-Sign

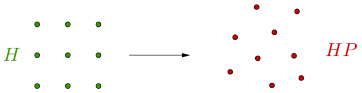
First introduced in

Following idea of McEliece

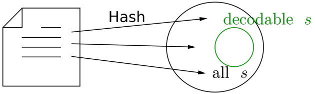
M. Bellare, P. Rogaway. “The exact security of digital signatures-How to sign with RSA and Rabin.”, Int. conf. on the theory and app. of crypto. tech., 1996.

N. Courtois, M. Finiasz, N. Sendrier. “How to achieve a McEliece-based digital signature scheme”, Asiacrypt, 2001.

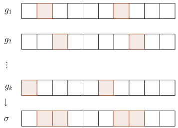
- → start with structured code H
- → publish scrambled code HP
- → large public key sizes



- → $\text{Hash}(m) = eH^\top$, $\text{wt}_H(e) \leq t$
- → signature $\sigma = eP$
- → slow signing



- → reduce key sizes:
- → use quasi-cyclic codes
- → use low density generators



Hash-and-Sign

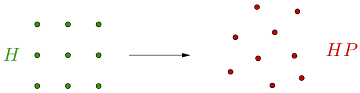
First introduced in

Following idea of McEliece

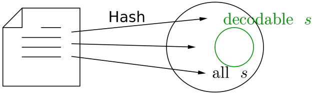
M. Bellare, P. Rogaway. "The exact security of digital signatures-How to sign with RSA and Rabin.", Int. conf. on the theory and app. of crypto. tech., 1996.

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

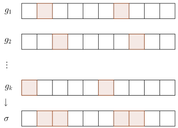
- → start with structured code H
- → publish scrambled code HP
- → large public key sizes



- → $\text{Hash}(m) = eH^{\top}$, $\text{wt}_H(e) \leq t$
- → signature $\sigma = eP$
- → slow signing



- → reduce key sizes:
- → use quasi-cyclic codes
- → use low density generators
- → statistical attacks



Idea of ZK Protocol

Prover

$\mathcal{S}$: secret
$\mathcal{P}$: related public key
c: commitments to secret
r_b: response to challenge b

$\xrightarrow{\mathcal{P},\ c}$

$\xleftarrow{b}$

$\xrightarrow{r_b}$

Verifier

b: challenge
Recover c from r_b and $\mathcal{P}$

Idea of ZK Protocol

Prover	Interaction	**Verifier**
$\mathcal{S}$: secret $\mathcal{P}$: related public key c: commitments to secret r_b: response to challenge b	$\xrightarrow{\mathcal{P},\ c}$ $\xleftarrow{b}$ $\xrightarrow{r_b}$	b: challenge Recover c from r_b and $\mathcal{P}$

Idea of ZK Protocol

Prover	Fiat-Shamir	**Verifier**
$\mathcal{S}$: secret $\mathcal{P}$: related public key c: commitments to secret b: Hash of message, c r_b: response to challenge b	$\xrightarrow{\mathcal{P},(b,r_b)}$	Recover c from r_b and $\mathcal{P}$ Verify $b = \text{Hash}(m, c)$

A. Fiat, A. Shamir. "How to prove yourself: Practical solutions to identification and signature problems.", Proceedings on Advances in cryptology-CRYPTO, 1986.

Idea of ZK Protocol

Prover | **Verifier**

N (repeat)

$\mathcal{S}$: secret
$\mathcal{P}$: related public key
c: commitments to secret
b: Hash of message, c
r_b: response to challenge b

$\xrightarrow{\mathcal{P},(b,r_b)}$

Recover c from r_b and $\mathcal{P}$
Verify $b = \text{Hash}(m, c)$

- α cheating probability, λ bit security level
- *Rounds*: have to repeat ZK protocol N times: $2^\lambda < (1/\alpha)^N$
- Signature size: communication within all N rounds

A. Fiat, A. Shamir. "How to prove yourself: Practical solutions to identification and signature problems.", Proceedings on Advances in cryptology-CRYPTO, 1986.

Code-based ZK Protocols

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

Syndrome Decoding Problem

Given parity-check matrix H, syndrome s, weight t, find e s.t.

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

Prover		**Verifier**
$\mathcal{S}$: e of weight t,		
$\mathcal{P}$: random H, $s = eH^\top$, t	$\xrightarrow{\mathcal{P}, c_1, c_2}$	
c_1: commitment to syndrome equation 1.		
c_2: commitment to weight 2.	$\xleftarrow{b}$	$b \in \{1, 2\}$
response: transformation, e.g. permutation $r_1 = \varphi$, or transformed secret $r_2 = \varphi(e)$	$\xrightarrow{r_b}$	recover c_b from r_b and $\mathcal{P}$

Code-based ZK Protocols

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

Syndrome Decoding Problem

Given parity-check matrix H, syndrome s, weight t, find e s.t.

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

Prover **Verifier**

$\mathcal{S}$: e of weight t,

$\mathcal{P}$: random H, s =

c_1: commitment t

c_2: commitment t

1. Problem: large cheating probability → big signature sizes

CVE $\lambda = 128$ bit security → signature size: 43 kB

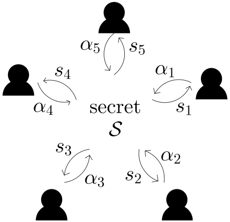
response: transformation, e.g. permutation
$r_1 = \varphi$, or transformed secret $r_2 = \varphi(e)$ $\xrightarrow{r_b}$ recover c_b from r_b and $\mathcal{P}$

MPC in-the-head

1.Solution: Multiparty Computation (MPC) in-the-head

Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. "Zero-knowledge from secure multiparty computation."ACM symposium on Theory of computing, 2007.

T. Feneuil, A. Joux, M. Rivain "Syndrome decoding in the head: shorter signatures from zero-knowledge proofs", Crypto, 2022.



Prover		**Verifier**
Split secret $\mathcal{S}$ into N shares s_i Commitments c_i to s_i Compute $\varphi(s_i) = \alpha_i$	$\xrightarrow{c_i, \alpha_i}$	Challenge $\ell \in \{1, \ldots, N\}$
	$\xleftarrow{\ell}$	
Response: all shares but ℓ	$\xrightarrow{s_i}$	Check α_i, c_i from s_i

→ New cheating probability: $1/N$

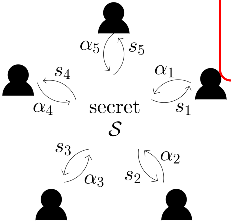
MPC in-the-head

1.Solution: Multiparty Computation (MPC) in-the-head

Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. "Zero-knowledge from secure multiparty computation."ACM symposium on Theory of computing, 2007.

T. Feneuil, A. Joux, M. Rivain "Syndrome decoding in the head: shorter signatures from zero-knowledge proofs", Crypto, 2022.

ifier



Problem: complex implementation

Verification and signing is slow

Compute $\varphi(s_i) = \alpha_i$ $\xrightarrow{c_i, \alpha_i}$ Challenge $\ell \in \{1, \dots, N\}$

$\xleftarrow{\ell}$

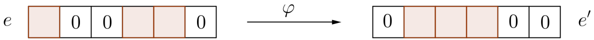
Response: all shares but ℓ $\xrightarrow{s_i}$ Check α_i, c_i from s_i

$\rightarrow$ New cheating probability: $1/N$

Code-Based ZK Protocols

Syndrome Decoding Problem

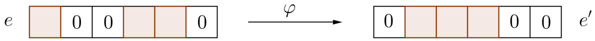
Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}_H(e) \leq t$ and $s = eH^\top$.



Code-Based ZK Protocols

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}_H(e) \leq t$ and $s = eH^\top$.

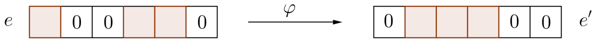


Which φ are allowed?

Code-Based ZK Protocols

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}_H(e) \le t$ and $s = eH^\top$.



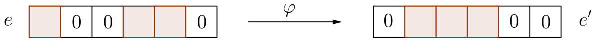
Which φ are allowed?

$\to \varphi$: linear isometries of Hamming metric:
permutation + scalar multiplication

Code-Based ZK Protocols

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}_H(e) \leq t$ and $s = eH^\top$.



Which φ are allowed?

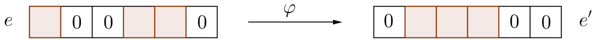
$\rightarrow \varphi$: linear isometries of Hamming metric:
permutation + scalar multiplication

2. Problem: permutations are costly $\quad \rightarrow \varphi : n\log_2(q-1) + n\log_2(n)$

Code-Based ZK Protocols

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}_H(e) \leq t$ and $s = eH^\top$.

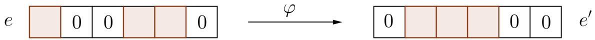


Can we avoid permutations - but keep the hardness of the problem?

Code-Based ZK Protocols

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $\mathrm{wt}_H(e) \leq t$ and $s = eH^\top$.



Can we avoid permutations - but keep the hardness of the problem?

$\downarrow$

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ such that $s = eH^\top$.

Restricted Errors

2. Solution: Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$(\mathbb{E}, \cdot) < (\mathbb{F}_q^\star, \cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1, \ldots, z\}\}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1, 3, 9\}$$

Restricted Errors

2. Solution: Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$(\mathbb{E}, \cdot) < (\mathbb{F}_q^\star, \cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1, 3, 9\}$$

$$(\mathbb{E}^n, \star) \quad \xrightarrow{\ell} \quad (\mathbb{F}_z^n, +)$$

- $e = (1, 9, 3, 3) \in \{1, 3, 9\}^4$

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

Restricted Errors

2. Solution: Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$(\mathbb{E}, \cdot) < (\mathbb{F}_q^\star, \cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1, 3, 9\}$$

$$(\mathbb{E}^n, \star) \quad \xrightarrow{\ell} \quad (\mathbb{F}_z^n, +)$$

- $e = (1, 9, 3, 3) \in \{1, 3, 9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3, 9, 1, 3) \in \mathbb{E}^n$

- $\ell(e) = (0, 2, 1, 1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1, 2, 0, 1) \in \mathbb{F}_3^4$

Restricted Errors

2. Solution: Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$(\mathbb{E}, \cdot) < (\mathbb{F}_q^\star, \cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$$

$$q = 13 \quad\rightarrow\quad g = 3 \text{ order } z = 3 \quad\rightarrow\quad \mathbb{E} = \{1, 3, 9\}$$

$$(\mathbb{E}^n, \star) \xrightarrow{\ell} (\mathbb{F}_z^n, +)$$

- $e = (1, 9, 3, 3) \in \{1, 3, 9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3, 9, 1, 3) \in \mathbb{E}^n$
- $\varphi(e) = e \star e' \in (\mathbb{E}^n, \star)$
- $\varphi(e) = (1, 9, 3, 3) \star (3, 9, 1, 3)$

- $\ell(e) = (0, 2, 1, 1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1, 2, 0, 1) \in \mathbb{F}_3^4$
- $\ell(e) + \ell(e') \in (\mathbb{F}_z^n, +)$
- $(0, 2, 1, 1) + (1, 2, 0, 1)$

Restricted Errors

2. Solution: Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** “Zero knowledge protocols and signatures from the restricted syndrome decoding problem ”, Preprint, 2023

$$(\mathbb{E}, \cdot) < (\mathbb{F}_q^\star, \cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1, 3, 9\}$$

$$(\mathbb{E}^n, \star) \quad \xrightarrow{\ell} \quad (\mathbb{F}_z^n, +)$$

→ Smaller sizes: $n \log_2(z)$ instead of $n \log_2((q-1)n)$

→ Faster arithmetic: ops. in $(\mathbb{F}_z^n, +)$ instead of $(\mathbb{F}_q^n, \cdot)$

CROSS

Basis

- Restricted SDP
- ZK + Fiat-Shamir

→ compact

Optimizations

- Merkle trees
- unbalanced challenges

→ efficient

Security

- no trapdoor needed
- EUF-CMA security

→ secure

CROSS

Basis

- Restricted SDP
- ZK + Fiat-Shamir

→ compact

Optimizations

- Merkle trees
- unbalanced challenges

→ efficient

Security

- no trapdoor needed
- EUF-CMA security

→ secure

Sizes in bytes, times in MCycles

⚠ No optimized implementation

Level		$\lvert pk \rvert$	$\lvert sign \rvert$	t_{sign}	t_{verify}
I	fast	38	8’665	3.08	2.11
	short	38	7’625	11.04	7.81
III	fast	56	21’697	4.91	3.23
	short	56	17’429	18.06	12.24
V	fast	77	37’924	11.05	7.49
	short	77	31’696	29.08	19.44

CROSS

- Marco Baldi
- Alessandro Barenghi
- Sebastian Bitzer
- Patrick Karl
- Felice Manganiello
- Alessio Pavoni
- Gerardo Pelosi
- Paolo Santini
- Jonas Schupp
- Freeman Slaughter
- Antonia Wachter-Zeh
- Violetta Weger

CROSS

- Marco Baldi
- Alessandro Barenghi
- Sebastian Bitzer
- Patrick Karl
- Felice Manganiello
- Alessio Pavoni
- Gerardo Pelosi
- Paolo Santini
- Jonas Schupp
- Freeman Slaughter
- Antonia Wachter-Zeh
- Violetta Weger

Scan me

CROSS

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

Round 1 Submissions

Submitted: 50	→	Complete & Proper: 40

- Multivariate: 12
- Code-based: 11
- Lattice-based: 7
- Symmetric: 4
- Other: 5
- Isogeny-based: 1

Round 1 Submissions

Submitted: 50 → Complete & Proper: 40

Cryptanalysis → Survivors: 29

- Multivariate: 12 → 9
- Code-based: 11 → 9
- Lattice-based: 7 → 5
- Symmetric: 4 → 4
- Other: 5 → 1
- Isogeny-based: 1 → 1

Round 1 Submissions

Submitted: 50 → Complete & Proper: 40

Cryptanalysis → Survivors: 29

- Multivariate: 12 → 9
- Code-based: 11 → 9
- Lattice-based: 7 → 5
- Symmetric: 4 → 4
- Other: 5 → 1
- Isogeny-based: 1 → 1

→ all of the schemes and their performances:

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

Round 1 Submissions

Submitted: 50 → Complete & Proper: 40

Cryptanalysis → Survivors: 29

- Multivariate: 12 → 9
- Code-based: 11 → 9
- Lattice-based: 7 → 5
- Symmetric: 4 → 4
- Other: 5 → 1
- Isogeny-based: 1 → 1

→ all of the schemes and their performances:

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

Code-Based Round 1 Submissions

MPC in-the-head

- SDitH: SDP
- RYDE: Rank SDP
- MIRA/MiRitH: matrix rank SDP
- PERK: permuted kernel

ZK Protocol

- LESS: code equivalence
- CROSS: restricted SDP
- MEDS: matrix rank CE

Hash & Sign

- FuLeeca: Lee SDP
- WAVE: $(U, U+V)$, large weight SDP
- Enh. pqsigRM: Reed-Muller

Code-Based Round 1 Submissions

MPC in-the-head

- SDitH: SDP
- RYDE: Rank SDP
- MIRA/MiRitH: matrix rank SDP
- PERK: permuted kernel

→ slow signing and verification

ZK Protocol

- LESS: code equivalence
- CROSS: restricted SDP
- MEDS: matrix rank CE

→ large signatures

Hash & Sign

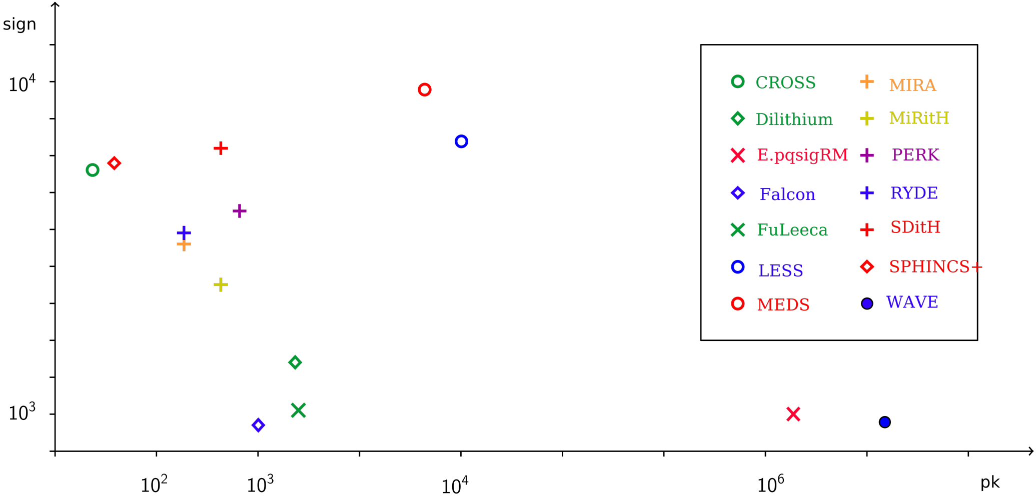
- × FuLeeca: Lee SDP
- WAVE: $(U, U+V)$, large weight SDP
- × Enh. pqsigRM: Reed-Muller

→ attacked

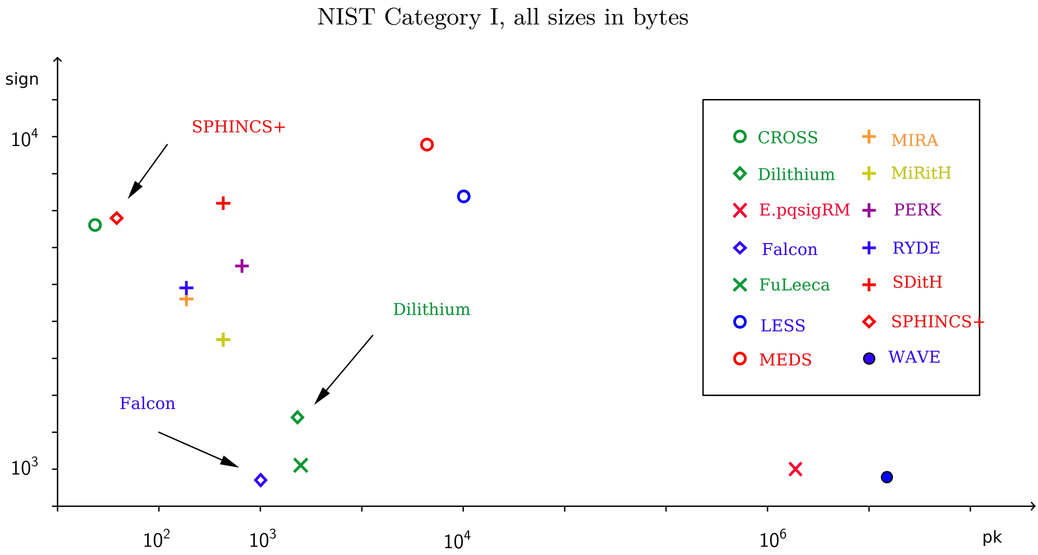
→ large public keys

Performance

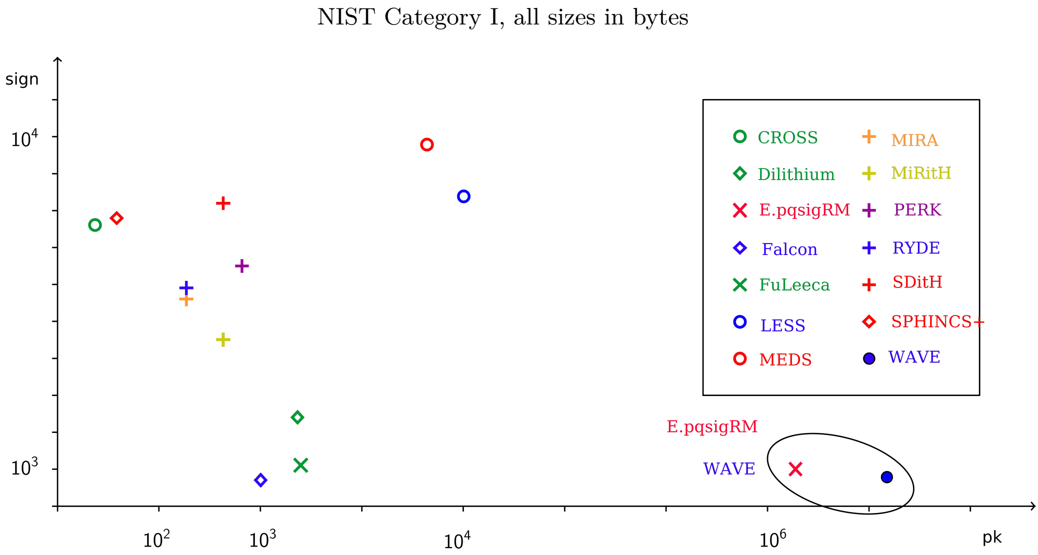
NIST Category I, all sizes in bytes



Performance

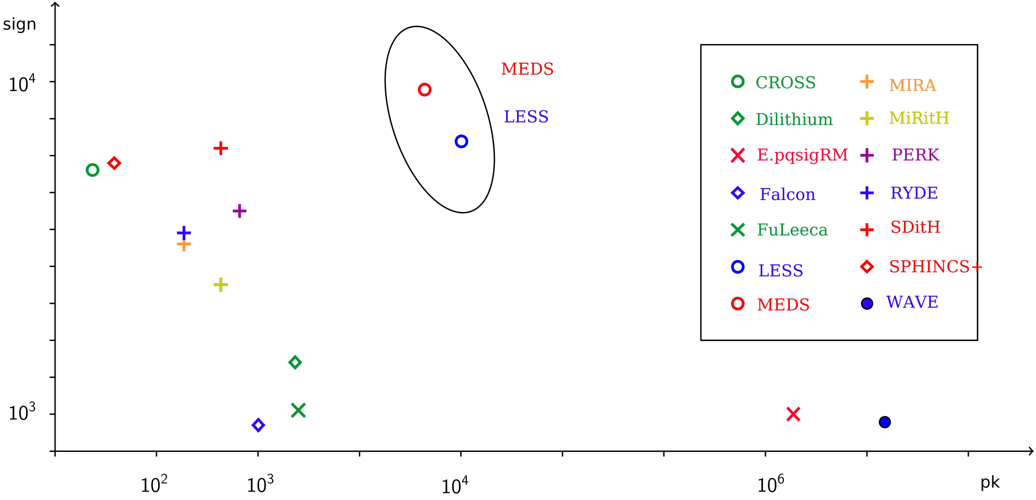


Performance

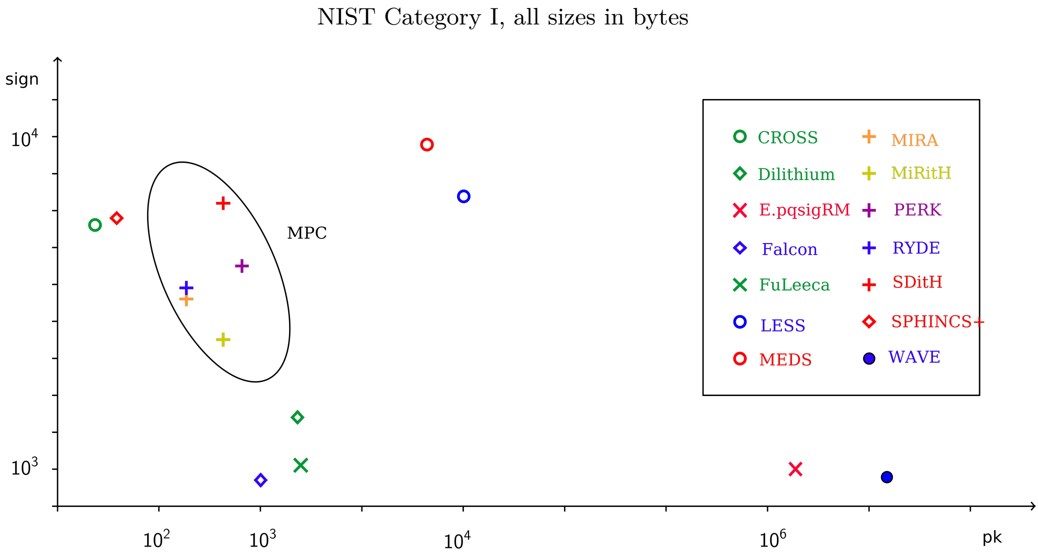


Performance

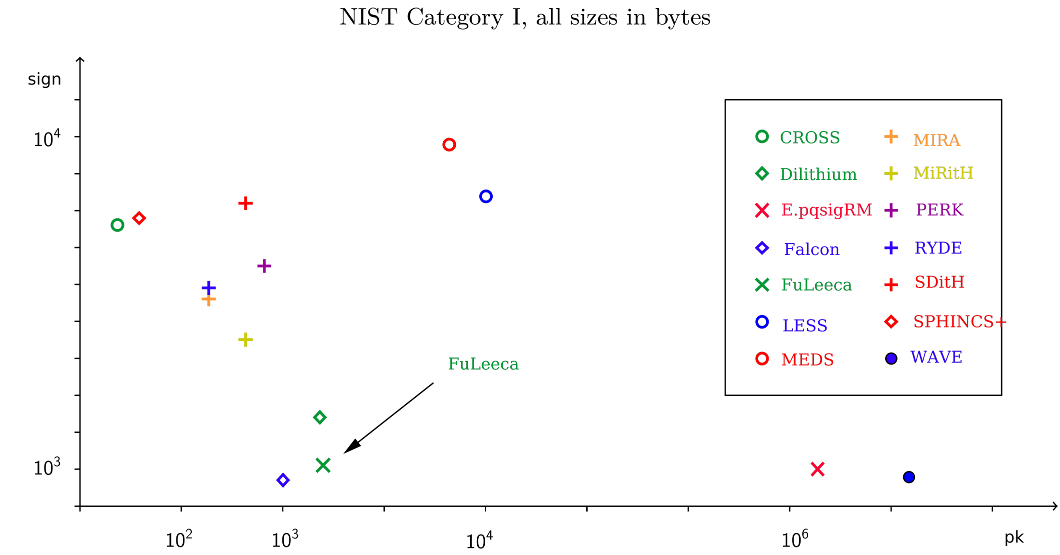
NIST Category I, all sizes in bytes



Performance

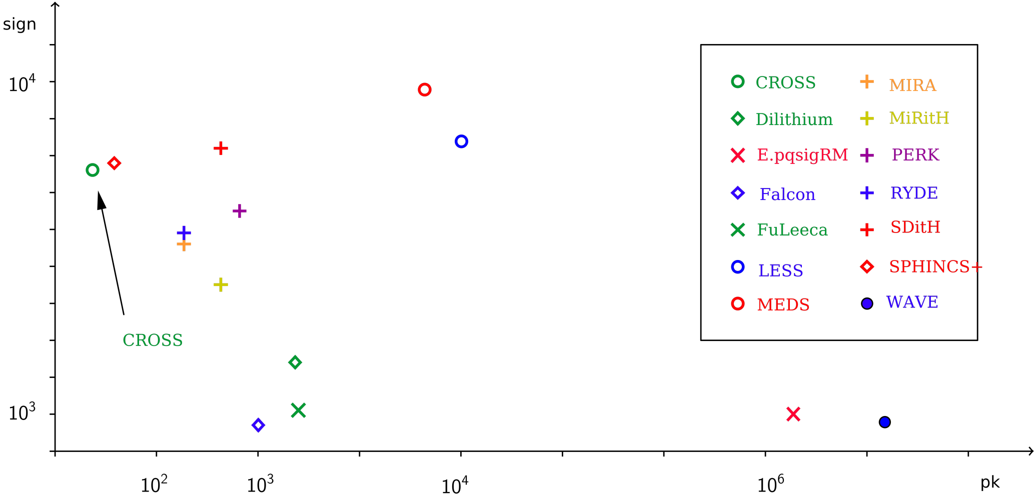


Performance

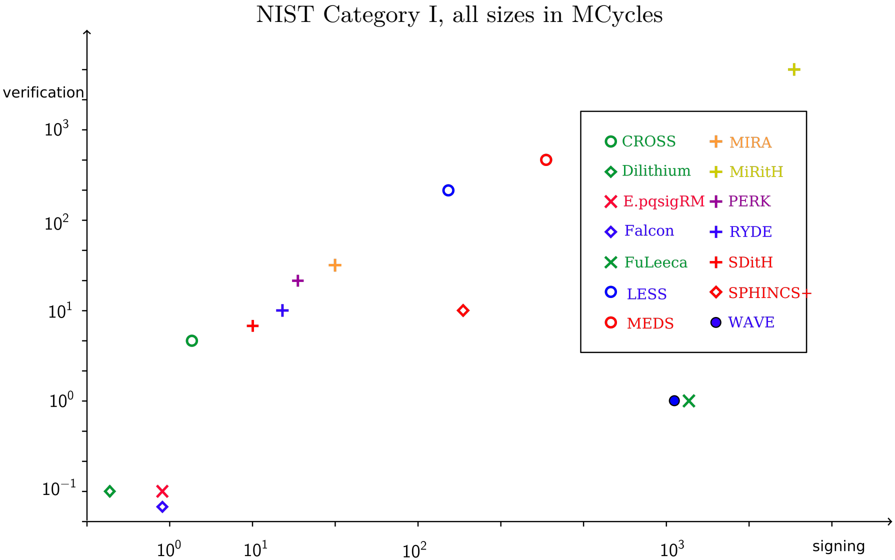


Performance

NIST Category I, all sizes in bytes

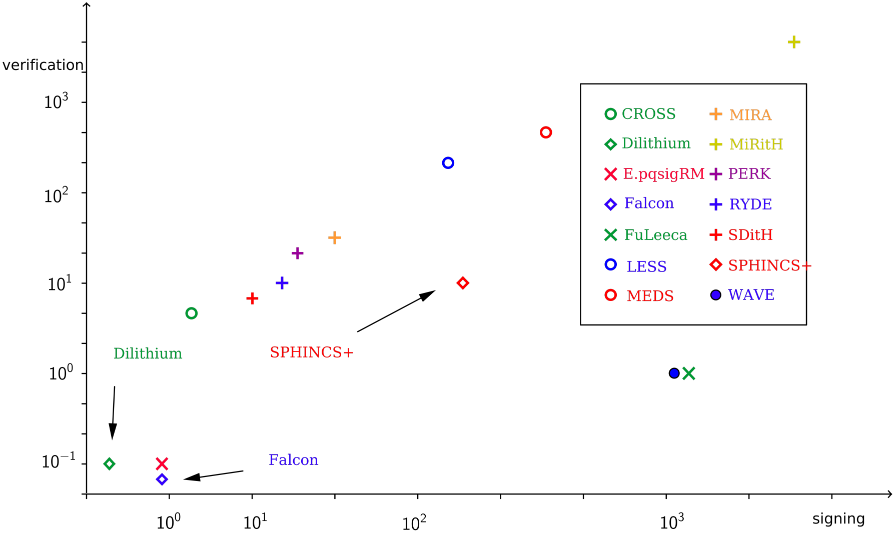


Performance

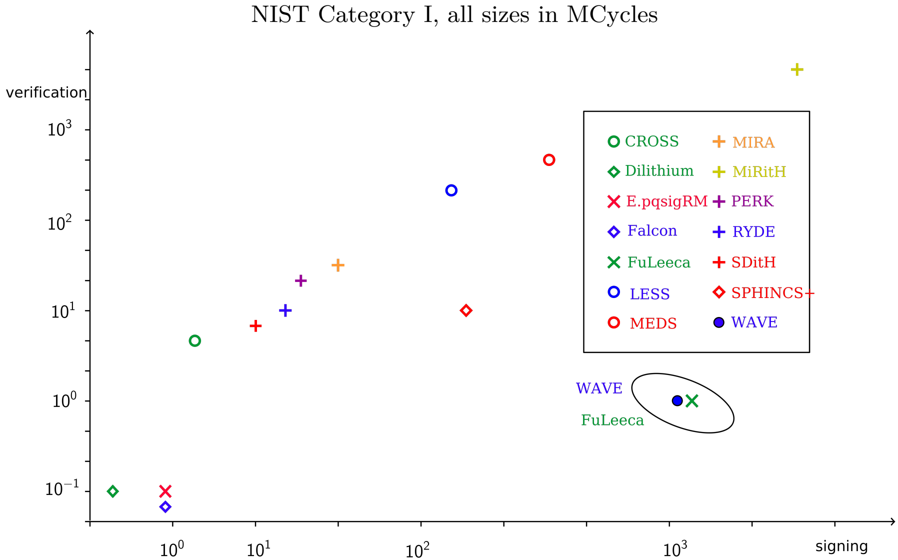


Performance

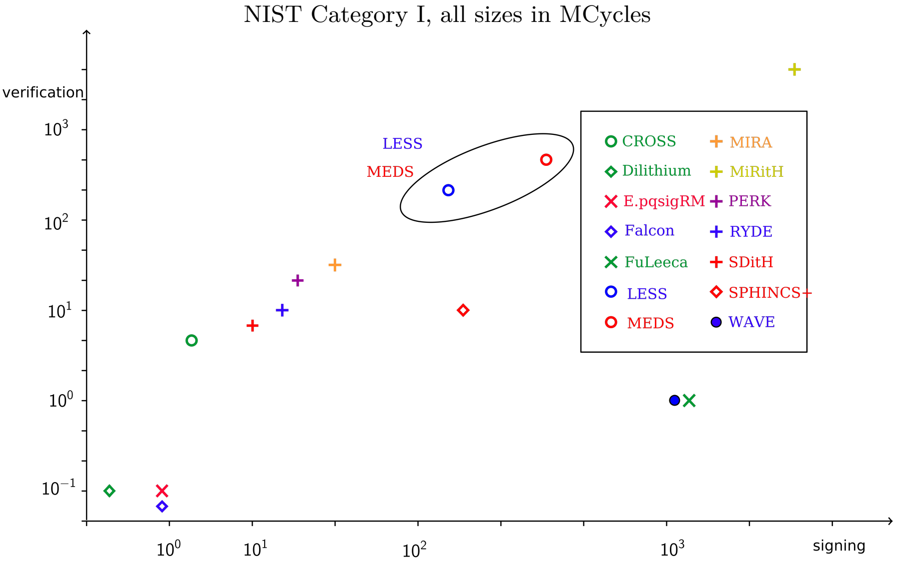
NIST Category I, all sizes in MCycles



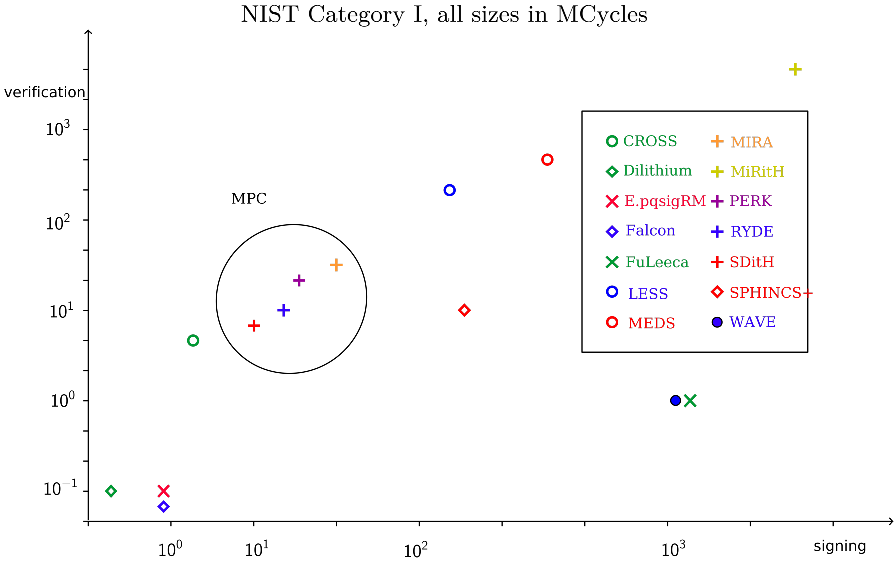
Performance



Performance

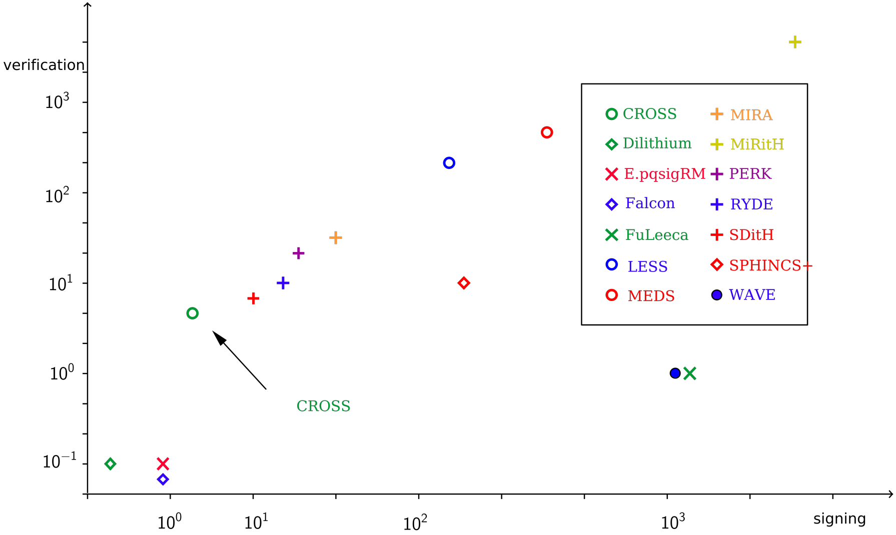


Performance



Performance

NIST Category I, all sizes in MCycles



Questions?

What's next?

- Cryptanalysis continues
- Improvements?
- How many rounds?

Slides

Thank you!

Code-Based Submissions

All sizes in bytes, times in MCycles.

Scheme	Based on	Technique	| Pk |	| Sig |	Sign	Verify
CROSS	Restricted SDP	ZK	32	7’625	11	7.4
Enh. pqsigRM	Reed-Muller	Hash & Sign	2’000’000	1’032	1.3	0.2
FuLeeca	Lee SDP	Hash & Sign	1’318	1’100	1’846	1.3
LESS	Code equiv.	ZK	13’700	8’400	206	213
MEDS	Matrix rank equiv.	ZK	9’923	9’896	518	515
MIRA	Matrix rank SDP	MPC	84	5’640	46’8	43’9
MiRitH	Matrix rank SDP	MPC	129	4’536	6’108	6’195
PERK	Permuted Kernel	MPC	150	6’560	39	27
RYDE	Rank SDP	MPC	86	5’956	23.4	20.1
SDitH	SDP	MPC	120	8’241	13.4	12.5
WAVE	Large wt $(U, U+V)$	Hash & Sign	3’677’390	822	1’160	1.23

Not all schemes have optimized implementations → Numbers may change