Introduction to Code-based Signatures

Violetta Weger

Finite Geometry and Friends

September 20, 2023

Finite Friends & Geometry

18-22 September 2023
Brussels
VUB Main campus Etterbeek

http://summerschool.fining.org/

MAIN LECTURERS
Anna-Lena Horlemann-Trautmann (St. Gallen)
Krystal Guo (Amsterdam)
Valentina Pepe (Roma)
John Sheekey (Dublin)

ORGANIZERS
Sam Adriaensen
Jan De Beule
Leen Demuys
Jonathan Mannaert
Sam Mattheus

VRIJE UNIVERSITEIT BRUSSEL

Finite Friends & Geometry

18-22 September 2023
Brussels

VUB Main campus Etterbeek

http://summerschool.fining.org/

MAIN LECTURERS
Anna-Lena Horlemann-Trautmann (St. Gallen)
Krystal Guo (Amsterdam)
Valentina Pepe (Roma)
John Sheekey (Dublin)

ORGANIZERS
Sam Adriaensen
Jan De Beule
Leen Demuys
Jonathan Mannaert
Sam Mattheus

VRIJE UNIVERSITEIT BRUSSEL

2023: NIST standardization process for post-quantum digital signature schemes

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

→ Who is NIST?

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

→ Who is NIST?

→ What is a standardization process?

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

→ Who is NIST?

→ What is a standardization process?

→ What is post-quantum crypto?

→ What is a signature scheme?

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

→ Who is NIST?

→ What is a standardization process?

→ What is post-quantum crypto?

→ What is a signature scheme?

2016: NIST standardization call

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

→ Who is NIST?

→ What is a standardization process?

→ What is post-quantum crypto?

→ What is a signature scheme?

2016: NIST standardization call

(Not over yet)

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

↑

New call

→ Who is NIST?

→ What is a standardization process?

→ What is post-quantum crypto?

→ What is a signature scheme?

2016: NIST standardization call

(Not over yet)

Big Hype

2023: NIST standardization process for post-quantum digital signature schemes

(Huge thing)

↑

New call

→ Who is NIST?

→ What is a standardization process?

→ What is post-quantum crypto?

→ What is a signature scheme?

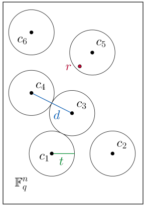
2016: NIST standardization call

(Not over yet)

→ Aim: understand & able to contribute

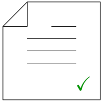
Outline

1. **What is post-quantum crypto?**
   - Basics of crypto
   - Post-quantum candidates

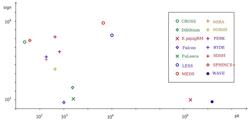


2. **What is code-based crypto?**
   - Introduction to coding theory
   - Hard problems in the submissions

3. **What is a signature scheme?**
   - Idea of signatures
   - Techniques to construct signatures



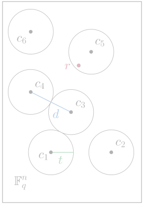
4. **Round 1 submissions**
   - Survivors
   - Performance



Outline

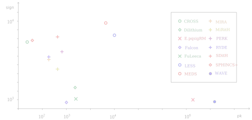
1. **What is post-quantum crypto?**
   - Basics of crypto
   - Post-quantum candidates

2. **What is code-based crypto?**
   - Introduction to coding theory
   - Hard problems in the submissions



3. **What is a signature scheme?**
   - Idea of signatures
   - Techniques to construct signatures

4. **Round 1 submissions**
   - Survivors
   - Performance



Crypto is for Cryptography

Symmetric

Crypto is for Cryptography

Symmetric

Asymmetric PKE

aka public-key

cryptography

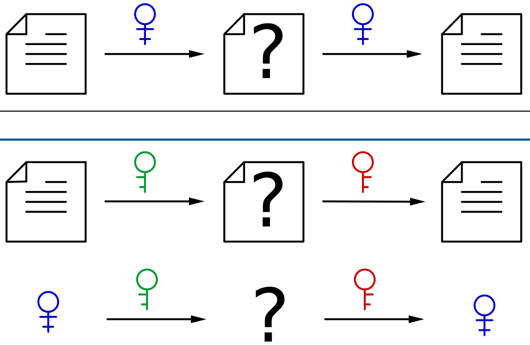
Crypto is for Cryptography

Symmetric

Asymmetric

PKE

KEM



aka public-key

cryptography

Crypto is for Cryptography

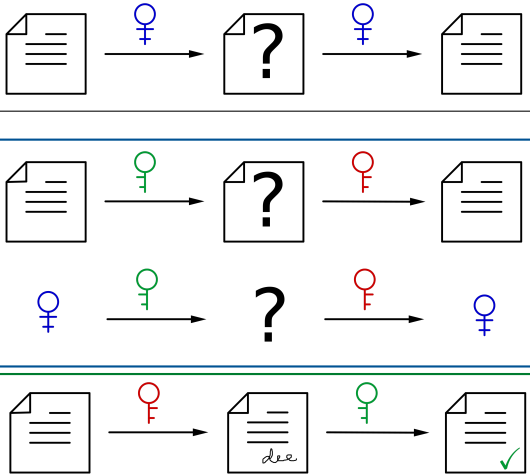
Symmetric

Asymmetric
aka public-key
cryptography

PKE

KEM

signature



Classic Heroes

Classical attackers 

Classic Heroes

Classical attackers  → Classical heroes 

- ✓ RSA
- ✓ DLP
- ✓ EC DLP

Classic Heroes

Classical attackers  → Classical heroes 

- ✓ RSA
- ✓ DLP
- ✓ EC DLP

Quantum attackers → Quantum heroes

Classic Heroes vs. Quantum Avengers

Classical attackers  → Classical heroes 

X ~~RSA~~

X ~~DLP~~

X ~~EC-DLP~~

Quantum attackers  → Quantum heroes

post-quantum

Classic Heroes vs. Quantum Avengers

Classical attackers  → Classical heroes 

X ~~RSA~~

X ~~DLP~~

X ~~EC DLP~~

Quantum attackers  → Quantum heroes post-quantum

 Lattice-based

Classic Heroes vs. Quantum Avengers

Classical attackers  → Classical heroes 

- X ~~RSA~~
- X ~~DLP~~
- X ~~EC-DLP~~

Quantum attackers  → Quantum heroes

post-quantum

 Lattice-based

 Multivariate

Classic Heroes vs. Quantum Avengers

Classical attackers  → Classical heroes 

- X ~~RSA~~
- X ~~DLP~~
- X ~~EC DLP~~

Quantum attackers  → Quantum heroes post-quantum

 Lattice-based

 Multivariate

 Hash-based

Classic Heroes vs. Quantum Avengers

Classical attackers  → Classical heroes 

X ~~RSA~~

X ~~DLP~~

X ~~EC DLP~~

Quantum attackers  → Quantum heroes post-quantum

 Lattice-based

 Multivariate

 Hash-based

 Isogeny-based

Classic Heroes vs. Quantum Avengers

Classical attackers → Classical heroes

X ~~RSA~~
X ~~DLP~~
X ~~EC DLP~~

Quantum attackers → Quantum heroes post-quantum

Lattice-based

Multivariate

Hash-based

Isogeny-based

Code-based

Why do we need a new call?

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

Why do we need a new call?

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

Why do we need a new call?

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

based on structured lattices — Hash-based

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

Why do we need a new call?

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

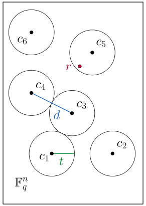
based on structured lattices | Hash-based

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

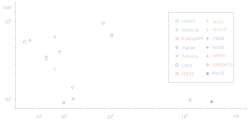
1. **What is post-quantum crypto?**
   - Basics of crypto
   - Post-quantum candidates



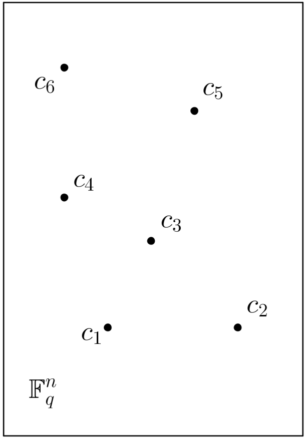
2. **What is code-based crypto?**
   - Introduction to coding theory
   - Hard problems in the submissions

3. **What is a signature scheme?**
   - Idea of signatures
   - Techniques to construct signatures

4. **Round 1 submissions**
   - Survivors
   - Performance



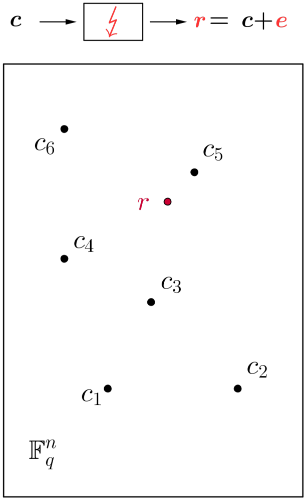
Coding Theory



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*

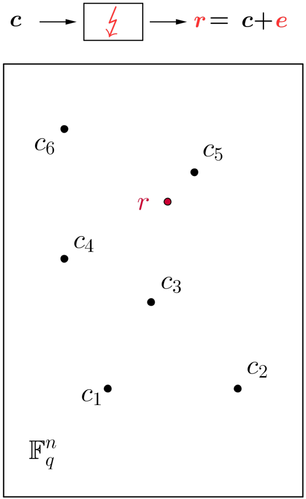
Coding Theory



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

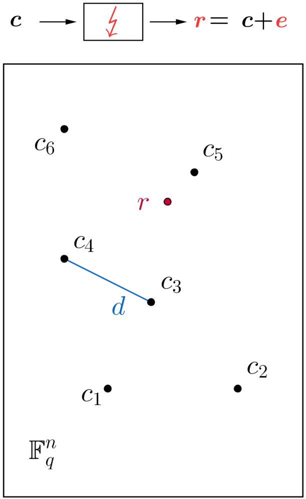
Coding Theory



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*: $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$

Coding Theory

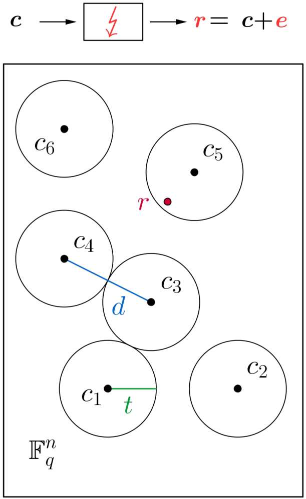


Set Up

- *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*: $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$
- *minimum distance of a code*:

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

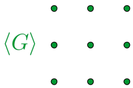
- *error-correction capacity*: $t = \lfloor (d(\mathcal{C}) - 1)/2 \rfloor$

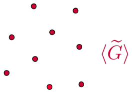
Classic Approach: McEliece

Algebraic structure

(Reed-Solomon, Goppa,..)

→ efficient decoders



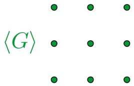


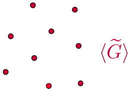
random code

→ how hard to decode?

Classic Approach: McEliece

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





random code

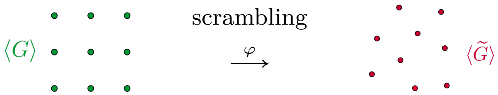
→ NP-hard

- 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.

Classic Approach: McEliece

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



Seemingly random code
→ NP-hard?

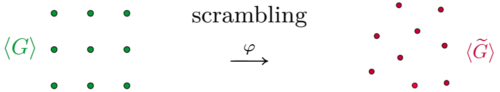
- Decoding random linear code is NP-hard
- First code-based cryptosystem based on this problem

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

Classic Approach: McEliece

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



Seemingly random code
→ NP-hard?

- 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.

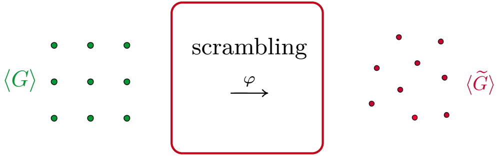
R. J. McEliece. “A public-key cryptosystem based on algebraic coding theory”, DSNP Report, 1978

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.

Classic Approach: McEliece

Distinguishing Problem

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



Seemingly random code

→ NP-hard?

- 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.

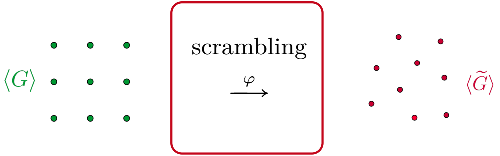
Classic Approach: McEliece

Distinguishing Problem

Algebraic structure

(Reed-Solomon, Goppa,..)

→ efficient decoders



Seemingly random code

→ NP-hard?

- 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

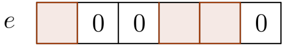
A. Becker, A. Joux, A. May, A. Meurer "Decoding random binary linear codes in $2^{n/20}$: How 1+ 1= 0 improves information set decoding", Eurocrypt, 2012.

New Approaches

Different Metrics

Hamming metric

$e \in \mathbb{F}_q^n \;\to \mathrm{wt}_H(e) = |\{i \mid e_i \neq 0\}|$



Decoding Problem (DP)

Given gen. matrix $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

1. $r - e \in \langle G \rangle$
2. $\mathrm{wt}_H(e) \leq t$

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

NP-hard

Different Metrics

Hamming metric

$e \in \mathbb{F}_q^n \rightarrow \mathrm{wt}_H(e) = |\{i \mid e_i \neq 0\}|$

e		0	0			0

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

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

DP $\leftrightarrow$ SDP

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

NP-hard

Different Metrics

Hamming metric

$e \in \mathbb{F}_q^n \rightarrow \mathrm{wt}_H(e) = |\{i \mid e_i \neq 0\}|$

e		0	0			0

Low Weight Codeword Problem (LWCP)

Given gen. matrix $G \in \mathbb{F}_q^{k\times n}$, target weight t, find $c \in \mathbb{F}_q^n$ s.t.

1. $c \in \langle G \rangle$
2. $\mathrm{wt}_H(c) \leq t$

DP $\leftrightarrow$ SDP $\leftrightarrow$ LWCP

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

NP-hard

Different Metrics

Hamming metric

$e \in \mathbb{F}_q^n \ \rightarrow \mathrm{wt}_H(e) = |\{i \mid e_i \neq 0\}|$

e

	0	0			0

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

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

DP $\leftrightarrow$ SDP $\leftrightarrow$ LWCP

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

NP-hard

Different Metrics

Hamming metric

$e \in \mathbb{F}_q^n \rightarrow \mathrm{wt}_H(e) = |\{i \mid e_i \neq 0\}|$

e						
		0	0			0

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

lin. constraint 1. $s = eH^\top$

2. $\mathrm{wt}_H(e) \leq t$ non-lin. constraint

DP $\leftrightarrow$ SDP $\leftrightarrow$ LWCP

Any metric

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

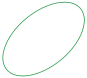
NP-hard

Different Metrics

Rank metric

$$e \in \mathbb{F}_{q^m}^n \rightarrow \mathrm{wt}_R(e) = \dim_{\mathbb{F}_q}(\langle e_1, \dots, e_n \rangle_{\mathbb{F}_q}) = \dim_{\mathbb{F}_q}(E)$$

E



Rank SDP

Given p.c. matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_{q^m}^{n-k}$, target weight t find $e \in \mathbb{F}_{q^m}^n$ s.t.

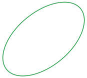
1. $s = eH^\top$
2. $\mathrm{wt}_R(e) \leq t$.

P. Gaborit, G. Zémor "On the hardness of the decoding and the minimum distance problems for rank codes.", IEEE TIT, 2016.

Different Metrics

Rank metric

$$e \in \mathbb{F}_{q^m}^n \rightarrow \mathrm{wt}_R(e) = \dim_{\mathbb{F}_q}(\langle e_1, \ldots, e_n \rangle_{\mathbb{F}_q}) = \dim_{\mathbb{F}_q}(E)$$

E 

Rank SDP

Given p.c. matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_{q^m}^{n-k}$, target weight t find $e \in \mathbb{F}_{q^m}^n$ s.t.

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

P. Gaborit, G. Zémor "On the hardness of the decoding and the minimum distance problems for rank codes.", IEEE TIT, 2016.

NP-hard?

Different Metrics

Matrix codes

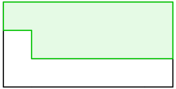
- $\mathcal{C} \subset \mathbb{F}_{q^m}^n$
- $\mathcal{C} = \langle G \rangle$, $G \in \mathbb{F}_{q^m}^{k \times n}$
- codewords $c = xG$ for $x \in \mathbb{F}_{q^m}^k$

- $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$
- $\mathcal{C} = \langle G_1, \dots, G_k \rangle$, $G_i \in \mathbb{F}_q^{m \times n}$
- $C = \lambda_1 G_1 + \cdots + \lambda_k G_k$ for $\lambda_i \in \mathbb{F}_q$

e  $\mathbb{F}_{q^m}^n$ $\rightarrow$ E  $\mathbb{F}_q^{m \times n}$

Matrix rank metric

$E \in \mathbb{F}_q^{m \times n} \rightarrow \mathrm{wt}_R(E) = \mathrm{rk}(E)$

E 

Different Metrics

Low Rank Weight Codeword Problem

Given gen. matrices $G_1, \ldots, G_k \in \mathbb{F}_q^{m\times n}$, target weight t, find $C \in \mathbb{F}_q^{m\times n}$ s.t.

1. $C \in \langle G_1, \ldots, G_k \rangle$ 2. $\mathrm{wt}_R(C) \leq t$.

J. Buss, S. Gudmund, J. Shallit. "The computational complexity of some problems of linear algebra.", Journal of Computer and System Sciences, 1999.

Different Metrics

Low Rank Weight Codeword Problem (MinRank)

Given gen. matrices $G_1, \dots, G_k \in \mathbb{F}_q^{m \times n}$, target weight t, find $C \in \mathbb{F}_q^{m \times n}$ s.t.

1. $C \in \langle G_1, \dots, G_k \rangle$ 2. $\mathrm{wt}_R(C) \leq t$.

J. Buss, S. Gudmund, J. Shallit. "The computational complexity of some problems of linear algebra.", Journal of Computer and System Sciences, 1999.

NP-hard

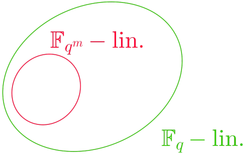
Different Metrics

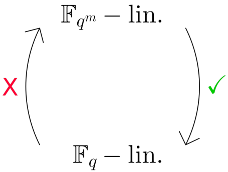
Low Rank Weight Codeword Problem (MinRank)

Given gen. matrices $G_1, \dots, G_k \in \mathbb{F}_q^{m \times n}$, target weight t, find $C \in \mathbb{F}_q^{m \times n}$ s.t.

1. $C \in \langle G_1, \dots, G_k \rangle$ 2. $\mathrm{wt}_R(C) \leq t$.

J. Buss, S. Gudmund, J. Shallit. "The computational complexity of some problems of linear algebra.", Journal of Computer and System Sciences, 1999.



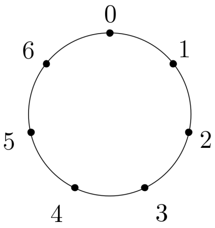


NP-hard

Different Metrics

Lee Metric

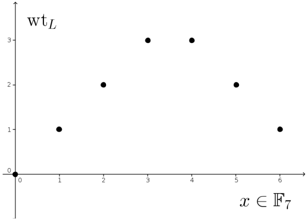
- $x \in \mathbb{Z}/m\mathbb{Z} = \{0, \ldots, m-1\}$ → $\mathrm{wt}_L(x) = \min\{x, |m-x|\}$



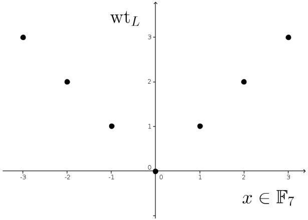
Different Metrics

Lee Metric

- $x \in \{-\lfloor \frac{m}{2} \rfloor, \ldots, \lfloor \frac{m}{2} \rfloor\}$ $\rightarrow$ $\mathrm{wt}_L(x) = |x|$



$\rightarrow$

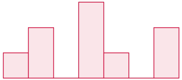


Different Metrics

Lee metric

$$e \in \mathbb{F}_p^n \rightarrow \mathrm{wt}_L(e) = \sum_{i=1}^n \min\{e_i, |p - e_i|\}$$

e



Lee SDP

Given p.c. matrix $H \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_p^{n-k}$ target weight t, find $e \in \mathbb{F}_p^n$ s.t.

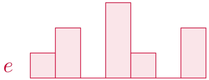
1. $s = eH^\top$
2. $\mathrm{wt}_L(e) \leq t.$

V. W., K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, E. Persichetti. "On the hardness of the Lee syndrome decoding problem.", AMC, 2022.

Different Metrics

Lee metric

$$e \in \mathbb{F}_p^n \rightarrow \text{wt}_L(e) = \sum_{i=1}^n \min\{e_i, |p - e_i|\}$$



Lee SDP

Given p.c. matrix $H \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_p^{n-k}$ target weight t, find $e \in \mathbb{F}_p^n$ s.t.

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

V. W., K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, E. Persichetti. "On the hardness of the Lee syndrome decoding problem.", AMC, 2022.

NP-hard

Different Problems

Code equivalence

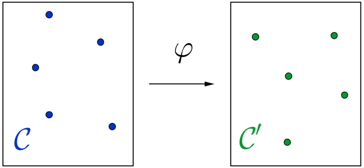
φ = linear isometry:
$\mathrm{wt}(x) = \mathrm{wt}(\varphi(x))\ \forall x$

Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n$
Matrix rank metric: $\mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$

(Matrix) Code Equivalence Problem (CEP)

Given gen. matrices $G, G' \in \mathbb{F}_q^{k\times n}$, find isometry φ s.t. $\varphi(\langle G\rangle) = \langle G'\rangle$.

E. Petrank, R. Roth "Is code equivalence easy to decide?", 1997.



Different Problems

Code equivalence

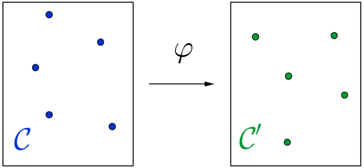
φ = linear isometry:
$\mathrm{wt}(x) = \mathrm{wt}(\varphi(x)) \ \forall x$

Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n$
Matrix rank metric: $\mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$

(Matrix) Code Equivalence Problem (CEP)

Given gen. matrices $G, G' \in \mathbb{F}_q^{k \times n}$, find isometry φ s.t. $\varphi(\langle G \rangle) = \langle G' \rangle$.

E. Petrank, R. Roth "Is code equivalence easy to decide?", 1997.



not NP-hard

Different Problems

Permuted Kernel Problem (PKP)

Given $G \in \mathbb{F}_q^{k \times n}$, $H' \in \mathbb{F}_q^{(n-k') \times n}$, find perm. matrix P s.t. $H'(GP)^\top = 0$.

A. Shamir "An efficient identification scheme based on permuted kernels", 1990.

Different Problems

Permuted Kernel Problem (PKP)

Given $G \in \mathbb{F}_q^{k \times n}$, $H' \in \mathbb{F}_q^{(n-k') \times n}$, find perm. matrix P s.t. $H'(GP)^\top = 0$.

$\updownarrow$

Subcode Equivalence Problem (SEP)

Given gen. matrices $G \in \mathbb{F}_q^{k \times n}, G' \in \mathbb{F}_q^{k' \times n}$, find perm. matrix P s.t. $\langle G' \rangle \subset \langle GP \rangle$.

P. Santini, M. Baldi, F. Chiaraluce. "Computational Hardness of the Permuted Kernel and Subcode Equivalence Problems.", 2022.

Different Problems

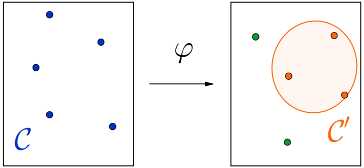
Permuted Kernel Problem (PKP)

Given $G \in \mathbb{F}_q^{k\times n}$, $H' \in \mathbb{F}_q^{(n-k')\times n}$, find perm. matrix P s.t. $H'(GP)^\top = 0$.

$\updownarrow$

Subcode Equivalence Problem (SEP)

Given gen. matrices $G \in \mathbb{F}_q^{k\times n}, G' \in \mathbb{F}_q^{k'\times n}$, find perm. matrix P s.t. $\langle G' \rangle \subset \langle GP \rangle$.



Different Problems

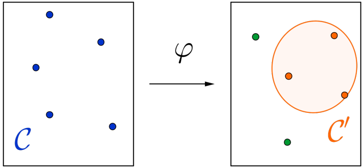
Permuted Kernel Problem (PKP)

Given $G \in \mathbb{F}_q^{k \times n}$, $H' \in \mathbb{F}_q^{(n-k') \times n}$, find perm. matrix P s.t. $H'(GP)^\top = 0$.

$\updownarrow$

Subcode Equivalence Problem (SEP)

Given gen. matrices $G \in \mathbb{F}_q^{k \times n}$, $G' \in \mathbb{F}_q^{k' \times n}$, find perm. matrix P s.t. $\langle G' \rangle \subset \langle GP \rangle$.



NP-hard

Different Problems

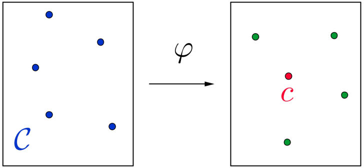
Permuted Kernel Problem (PKP)

Given $G \in \mathbb{F}_q^{k\times n}$, $H' \in \mathbb{F}_q^{(n-k')\times n}$, find perm. matrix P s.t. $H'(GP)^\top = 0$.

$\downarrow$

Relaxed PKP

Given gen. matrix $G \in \mathbb{F}_q^{k\times n}$, p.c. matrix $H' \in \mathbb{F}_q^{(n-k')\times n}$, find $x \in \mathbb{F}_q^{k}$, perm. matrix P s.t. $H'(xGP)^\top = 0$.



Different Problems

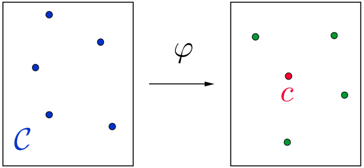
Permuted Kernel Problem (PKP)

Given $G \in \mathbb{F}_q^{k \times n}$, $H' \in \mathbb{F}_q^{(n-k') \times n}$, find perm. matrix P s.t. $H'(GP)^\top = 0$.

$\downarrow$

Relaxed PKP

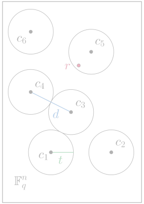
Given gen. matrix $G \in \mathbb{F}_q^{k \times n}$, p.c. matrix $H' \in \mathbb{F}_q^{(n-k') \times n}$, find $x \in \mathbb{F}_q^k$, perm. matrix P s.t. $H'(xGP)^\top = 0$.



NP-hard?

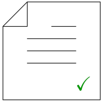
Outline

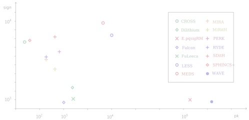
1. **What is post-quantum crypto?**
    - Basics of crypto
    - Post-quantum candidates



2. **What is code-based crypto?**
    - Introduction to coding theory
    - Hard problems in the submissions

3. **What is a signature scheme?**
    - Idea of signatures
    - Techniques to construct signatures

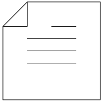




4. **Round 1 submissions**
    - Survivors
    - Performance

Idea of Signature Schemes

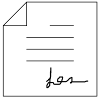
Signer



Verifier

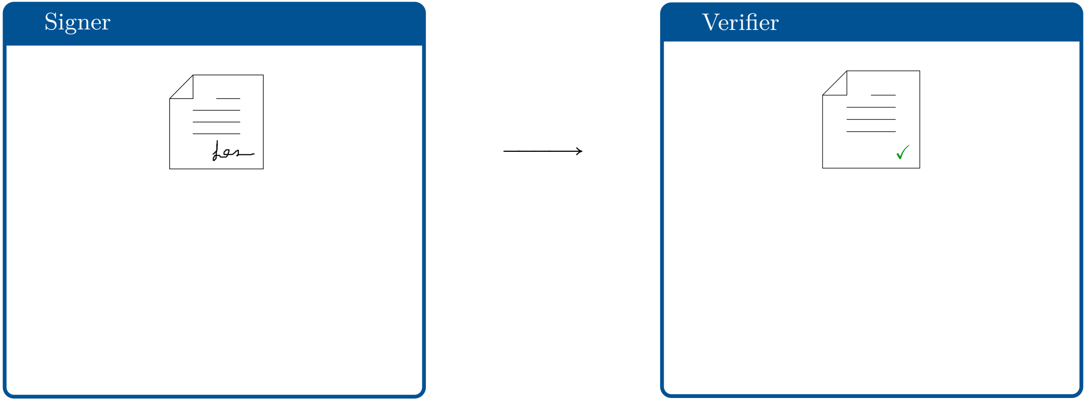
Idea of Signature Schemes

Signer



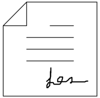
Verifier

Idea of Signature Schemes



Idea of Signature Schemes

Signer

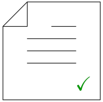


- Key Generation: $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\xrightarrow{\mathcal{P}}$

$\xrightarrow{m,\ \sigma}$

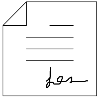
Verifier



- 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

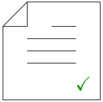
EUF secure

→

small $\mathcal{P}$

small σ

Verifier

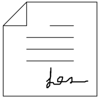


fast verification

- 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

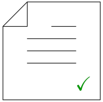
EUF secure

$\longrightarrow$

small $\mathcal{P}$

small σ

Verifier



fast verification

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

Approaches for signatures:

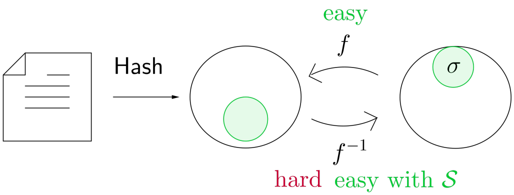
- Hash-and-Sign
- ZK Protocol
- ZK + MPC

Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

→ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$

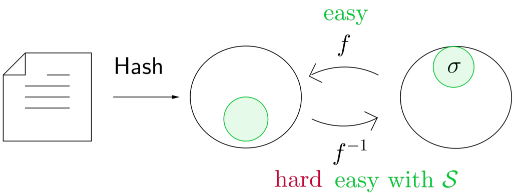


Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

→ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$



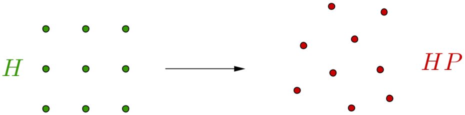
CFS: first code-based

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

- $\mathcal{S} = H$ structured code → $\mathcal{P} = HP$

→ large public key sizes

→ distinguishers

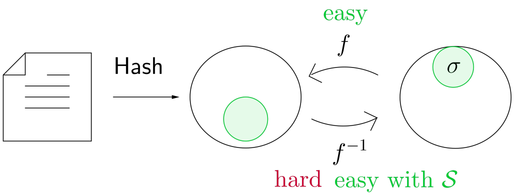


Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

→ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$



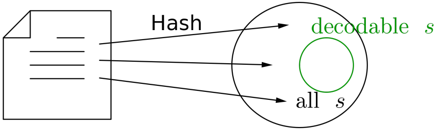
CFS: first code-based

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

- $\mathcal{S} = H$ structured code → $\mathcal{P} = HP$
- $f(x) = x(HP)^\top$
- $\mathsf{Hash}(m) = eH^\top$, $\mathrm{wt}_H(e) \leq t \to \sigma = eP$

→ slow signing

→ σ not random: attacks

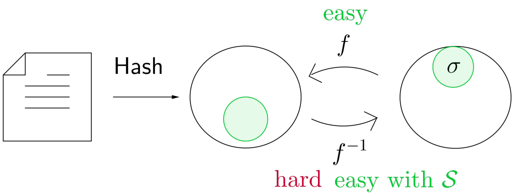


Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

→ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$



CFS: first code-based

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

- $\mathcal{S} = H$ structured code $\rightarrow \mathcal{P} = HP$
- $f(x) = x(HP)^\top$
- $\mathsf{Hash}(m) = eH^\top$, $\mathrm{wt}_H(e) \leq t \rightarrow \sigma = eP$

Problems:

→ large public keys

→ slow signing

→ security?

Idea of ZK Protocol

Prover

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

N

Prover

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

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

Verifier

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.

Idea of ZK Protocol

Prover | **Verifier**

N (repeat)

$\mathcal{S}$: secret key
$\mathcal{P}$: 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

Good Security:
→ EUF secure
→ no trapdoor
→ no distinguisher

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: 1. Problem

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.

Prover		**Verifier**
$\mathcal{S}$: e of weight t,		
$\mathcal{P}$: random H, $s = eH^\top$, t		
c_1 : commitment to syndrome equation 1.	$\xrightarrow{\mathcal{P}, c_1, c_2}$	
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 $\mathcal{P}$

Recall SDP: given H, s, t find e s.t.

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

Code-based ZK Protocols: 1. Problem

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.

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 $\mathcal{P}$

1. Problem: large cheating probability → big signature sizes

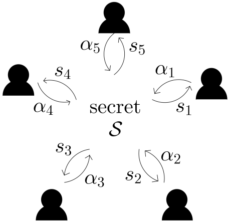
CVE $\lambda = 128$ bit security → signature size: 43 kB

1. Solution: MPC in-the-head

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

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

Ingredients: ZK protocol + $(N-1)$-private MPC



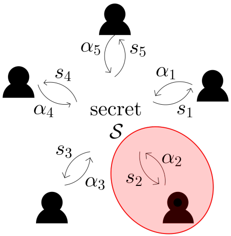
Prover		**Verifier**
Split $\mathcal{S}$ into N shares s_i Commitments c_i to s_i Compute $f(s_i) = \alpha_i$	$\xrightarrow{c_i,\alpha_i}$ $\xleftarrow{\ell}$	Challenge $\ell \in \{1, \dots, N\}$
Response: all shares but ℓ	$\xrightarrow{s_i}$	Check α_i, c_i from s_i

1. Solution: MPC in-the-head

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

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

Ingredients: ZK protocol + $(N-1)$-private MPC



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

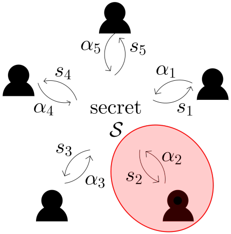
→ New cheating probability: $1/N$

1. Solution: MPC in-the-head

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

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

Ingredients: ZK protocol + $(N-1)$-private MPC



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

Problem: Verification and signing is slow

Code-based ZK Protocols: 2. Problem

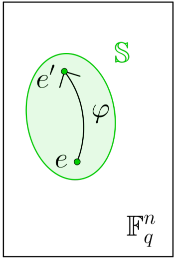
Transformations:

- allow to check lin. constraint

→ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

→ acts trans. on secret space $\mathbb{S}$



Code-based ZK Protocols: 2. Problem

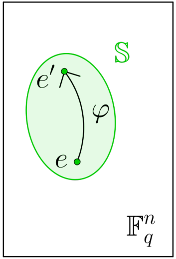
Transformations:

- allow to check lin. constraint

→ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

→ acts trans. on secret space $\mathbb{S}$



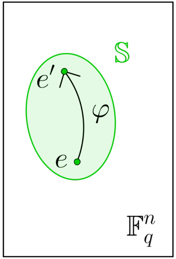
$\mathbb{S} = B_H(t)$ → lin. isometry in Hamming metric → $\varphi \in (\mathbb{F}_q^\star)^n \rtimes S_n$

→ Problem: Permutations are costly! $t \log_2(n(q-1))$ bits per round!

Code-based ZK Protocols: 2. Problem

Transformations:

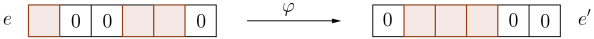
- allow to check lin. constraint
- → linear map
- allow to check non-lin. constraint
- should not reveal info. on secret e
- → acts trans. on secret space $\mathbb{S}$



$\mathbb{S} = B_H(t)$ → lin. isometry in Hamming metric → $\varphi \in (\mathbb{F}_q^\star)^n \rtimes S_n$

→ Problem: Permutations are costly! $t\log_2(n(q-1))$ bits per round!

How to avoid permutations?



Code-based ZK Protocols: 2. Problem

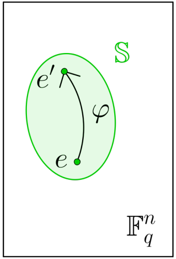
Transformations:

- allow to check lin. constraint

→ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

→ acts trans. on secret space $\mathbb{S}$



2. Solution: exchange $\mathbb{S} = B_H(t)$ with $\mathbb{S} = \mathbb{E}^n$

Non-lin. constraint: 2. $\mathrm{wt}_H(e) \leq t$ → 2. $e \in \mathbb{E}^n$

Restricted Errors

Restricted errors

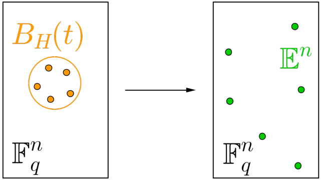
$e \in \mathbb{F}_q^n \;\to e \in \mathbb{E}^n,\ \mathbb{E} < \mathbb{F}_q^\star$

Restricted SDP (R-SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} < \mathbb{F}_q^\star$, find $e \in \mathbb{F}_q^n$ s.t.

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

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, V. W. "Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem.", 2023.



NP-hard

Restricted Errors

⚠ Self advertisement ⚠

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

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

Restricted Errors

⚠ Self advertisement ⚠

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

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

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

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

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

Restricted Errors

⚠ Self advertisement ⚠

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

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

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

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

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

Restricted Errors

⚠ Self advertisement ⚠

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

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

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

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

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

Restricted Errors

⚠ Self advertisement ⚠

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

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

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

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

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

Summary of Techniques

Hash-and-Sign

Needs:

- trapdoor
- secret code

☹ large pk
☹ slow sign.
☹ security?
☺ small sign.

ZK Protocol

Needs:

- hard problem

☹ large sign.
☺ small pk

ZK+MPC

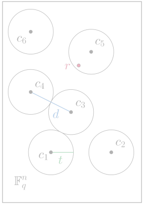
Needs:

- hard problem
- $(N-1)$-private MPC

☹ slow sign.
☹ slow verify
☺ small pk
☺ smaller sign.

Outline

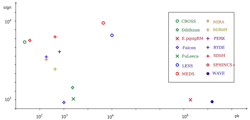
1. **What is post-quantum crypto?**
    - Basics of crypto
    - Post-quantum candidates



2. **What is code-based crypto?**
    - Introduction to coding theory
    - Hard problems in the submissions

3. **What is a signature scheme?**
    - Idea of signatures
    - Techniques to construct signatures

4. **Round 1 submissions**
    - Survivors
    - Performance



Round 1 Submissions

Submitted: 50 → Complete & Proper: 40

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

Round 1 Submissions

Submitted: 50 → Complete & Proper: 40

Cryptanalysis → Survivors: 29

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

Round 1 Submissions

Submitted: 50 → Complete & Proper: 40

Cryptanalysis → Survivors: 29

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

→ all of the schemes and their performances:

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

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme
Lee SDP	QC Lee code	

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme
Lee SDP	QC Lee code	FuLeeca

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme
Lee SDP	QC Lee code	FuLeeca
SDP	Reed-Muller	

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme
Lee SDP	QC Lee code	FuLeeca
SDP	Reed-Muller	Enh. pqsigRM

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme
Lee SDP	QC Lee code	FuLeeca
SDP	Reed-Muller	Enh. pqsigRM
SDP (large wt)	$(U, U+V)$	

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme
Lee SDP	QC Lee code	FuLeeca
SDP	Reed-Muller	Enh. pqsigRM
SDP (large wt)	$(U, U+V)$	WAVE

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme	
Lee SDP	QC Lee code	FuLeeca	broken
SDP	Reed-Muller	Enh. pqsigRM	
SDP (large wt)	$(U, U+V)$	Wave	

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme	
Lee SDP	QC Lee code	FuLeeca	broken
SDP	Reed-Muller	Enh. pqsigRM	broken
SDP (large wt)	$(U, U+V)$	WAVE	

Code-Based Round 1 Submissions

Hash-and-Sign

Trapdoor	Secret code	→ Scheme	
Lee SDP	QC Lee code	FuLeeca	broken
SDP	Reed-Muller	Enh. pqsigRM	broken
SDP (large wt)	$(U, U+V)$	WAVE	large pk

Code-Based Round 1 Submissions

ZK Protocols

Hard problem → Scheme

Code-Based Round 1 Submissions

ZK Protocols

Hard problem → Scheme

CEP

Code-Based Round 1 Submissions

ZK Protocols

Hard problem	→ Scheme
CEP	< LESS

Code-Based Round 1 Submissions

ZK Protocols

Hard problem → Scheme

CEP $<$ LESS

Matrix CEP

Code-Based Round 1 Submissions

ZK Protocols

Hard problem	→ Scheme
CEP	< LESS
Matrix CEP	MEDS

Code-Based Round 1 Submissions

ZK Protocols

Hard problem	→ Scheme
CEP	< LESS
Matrix CEP	MEDS
R-SDP	

Code-Based Round 1 Submissions

ZK Protocols

Hard problem	→ Scheme
CEP	< LESS
Matrix CEP	MEDS
R-SDP	CROSS

Code-Based Round 1 Submissions

ZK Protocols

Hard problem → Scheme

CEP	< LESS	large sizes
Matrix CEP	MEDS	
R-SDP	CROSS	

Code-Based Round 1 Submissions

ZK Protocols

Hard problem	→ Scheme	
CEP	< LESS	large sizes
Matrix CEP	MEDS	large sizes
R-SDP	CROSS	

Code-Based Round 1 Submissions

ZK Protocols

Hard problem → Scheme

CEP	< LESS	large sizes
Matrix CEP	MEDS	large sizes
R-SDP	CROSS	☺

Code-Based Round 1 Submissions

ZK + MPC

Hard problem → Scheme

Code-Based Round 1 Submissions

ZK + MPC

Hard problem → Scheme

SDP

Code-Based Round 1 Submissions

ZK + MPC

Hard problem → Scheme

SDP	SDitH

Code-Based Round 1 Submissions

ZK + MPC

Hard problem	→ Scheme
SDP	SDitH
rank SDP	

Code-Based Round 1 Submissions

ZK + MPC

Hard problem	→ Scheme
SDP	SDitH
rank SDP	RYDE

Code-Based Round 1 Submissions

ZK + MPC

Hard problem → Scheme

SDP	SDitH
rank SDP	RYDE
PKP	

Code-Based Round 1 Submissions

ZK + MPC

Hard problem	→ Scheme
SDP	SDitH
rank SDP	RYDE
PKP	PERK

Code-Based Round 1 Submissions

ZK + MPC

Hard problem	→ Scheme
SDP	SDitH
rank SDP	RYDE
PKP	PERK
MinRank	

Code-Based Round 1 Submissions

ZK + MPC

Hard problem	→ Scheme
SDP	 SDitH
rank SDP	 RYDE
PKP	PERK
MinRank	 MIRA/MiRitH

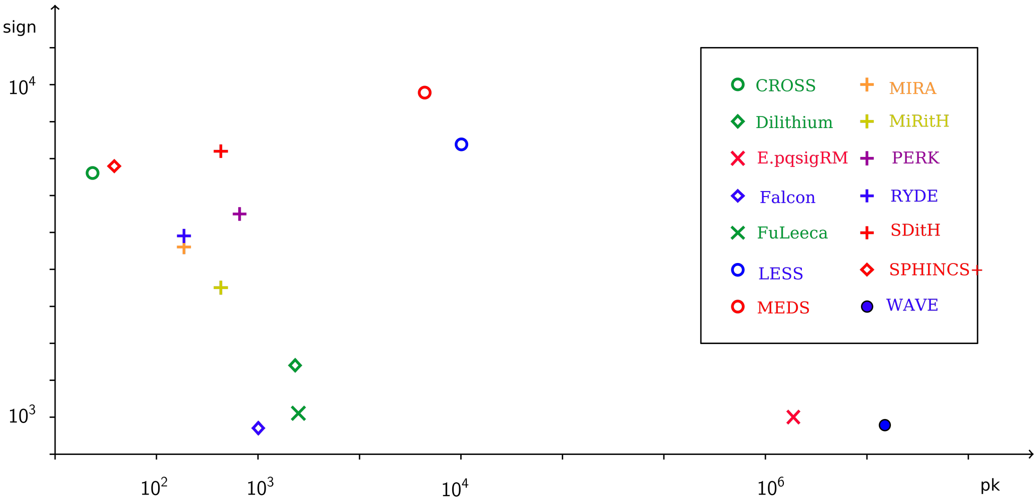
Code-Based Round 1 Submissions

ZK + MPC

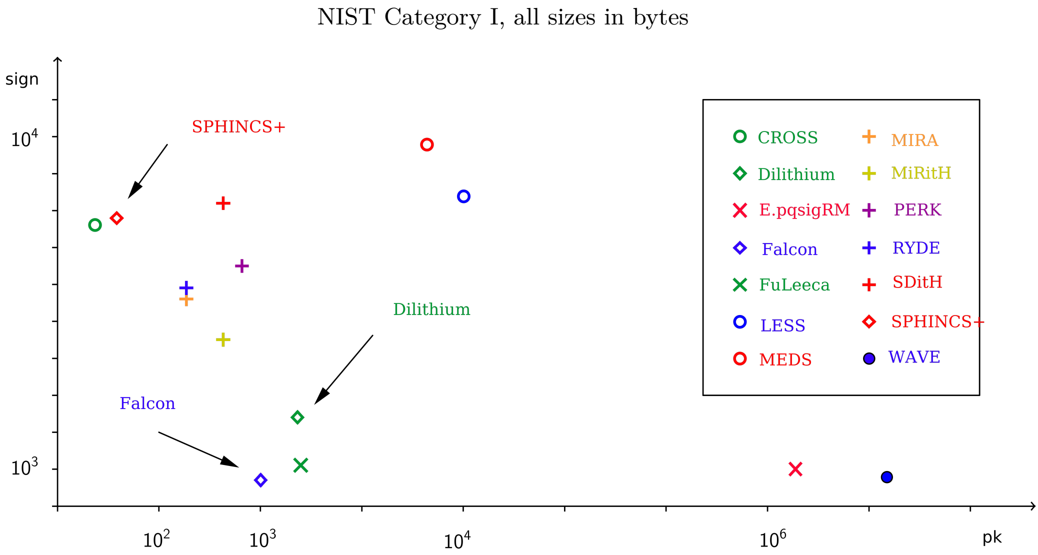
Hard problem	→ Scheme	
SDP	SDitH	slow
rank SDP	RYDE	slow
PKP	PERK	slow
MinRank	MIRA/MiRitH	slow

Performance

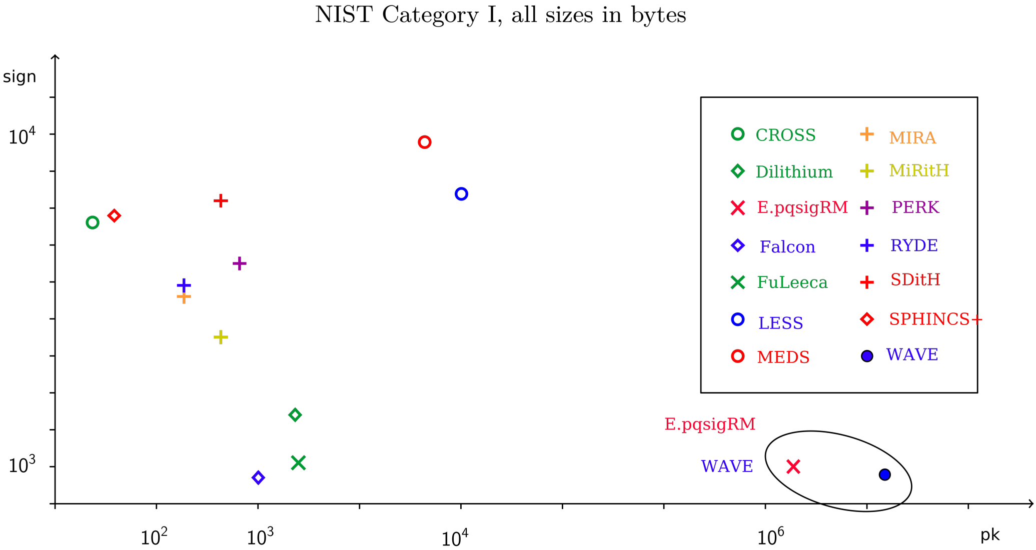
NIST Category I, all sizes in bytes



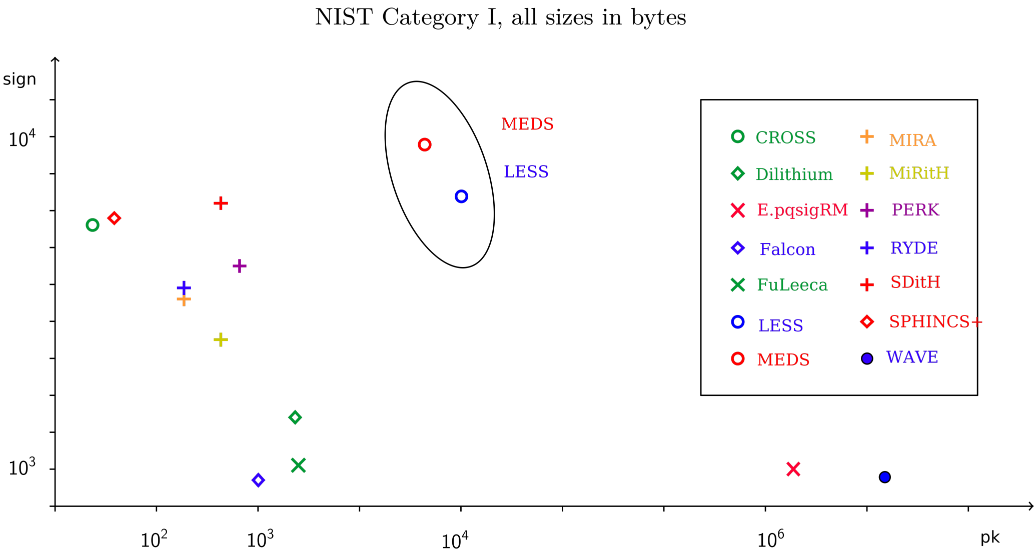
Performance



Performance

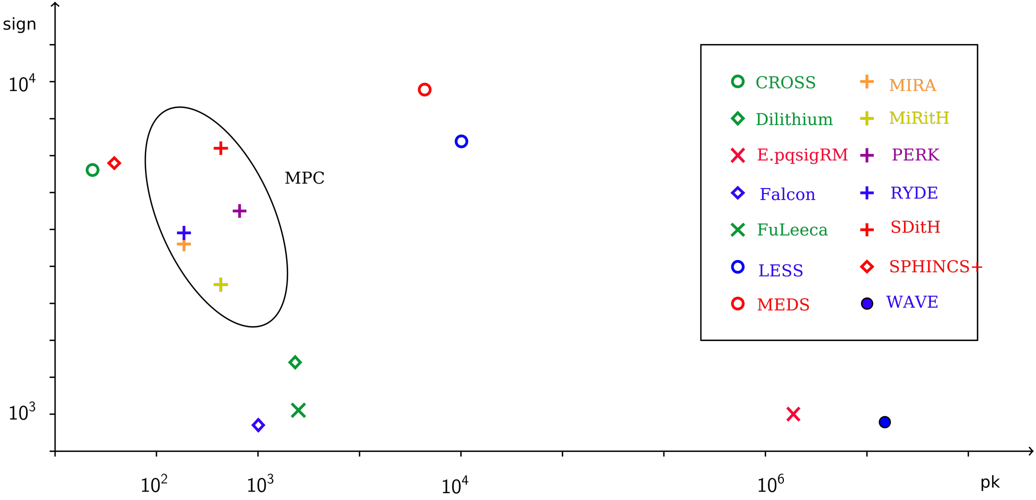


Performance



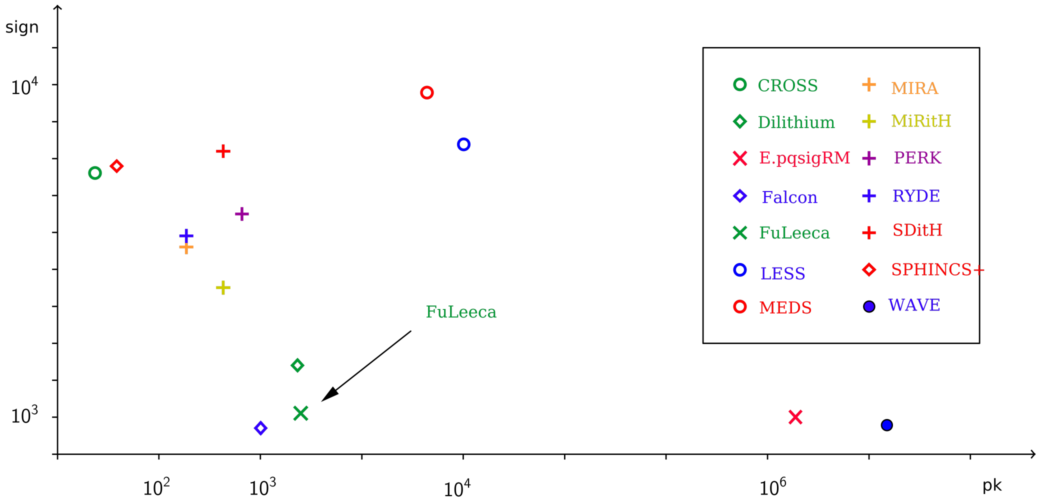
Performance

NIST Category I, all sizes in bytes



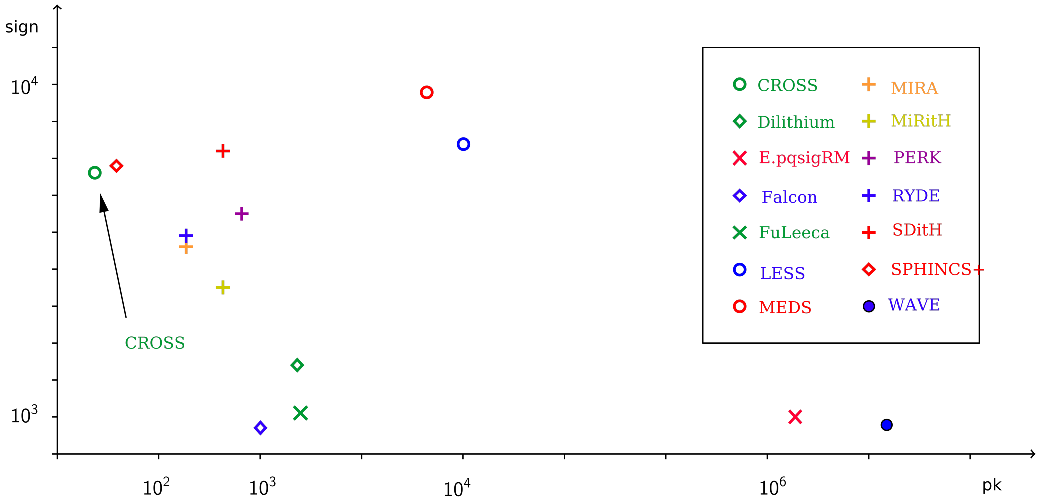
Performance

NIST Category I, all sizes in bytes

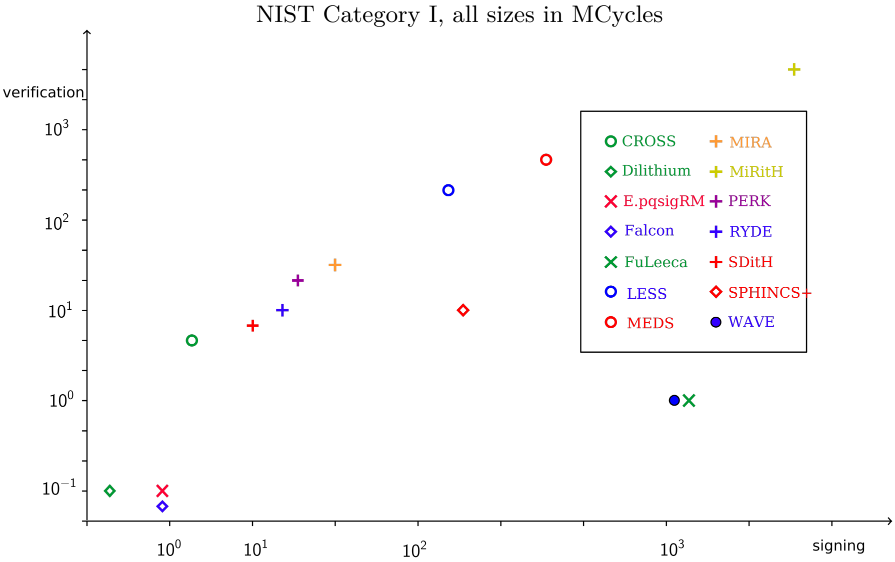


Performance

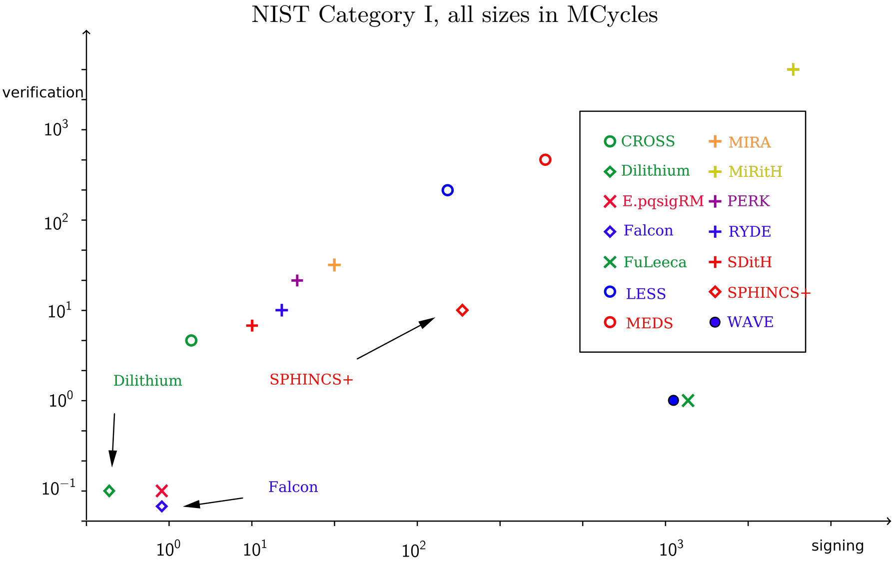
NIST Category I, all sizes in bytes



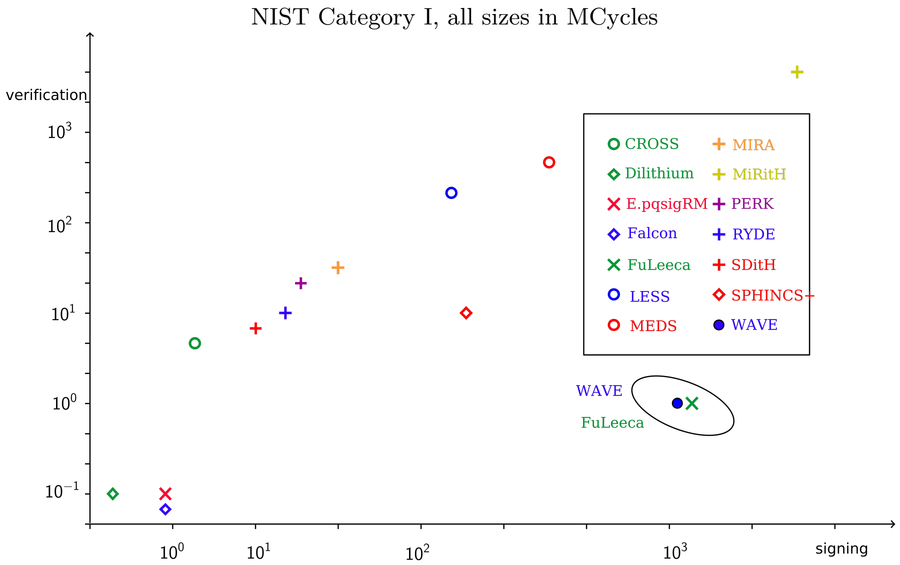
Performance



Performance

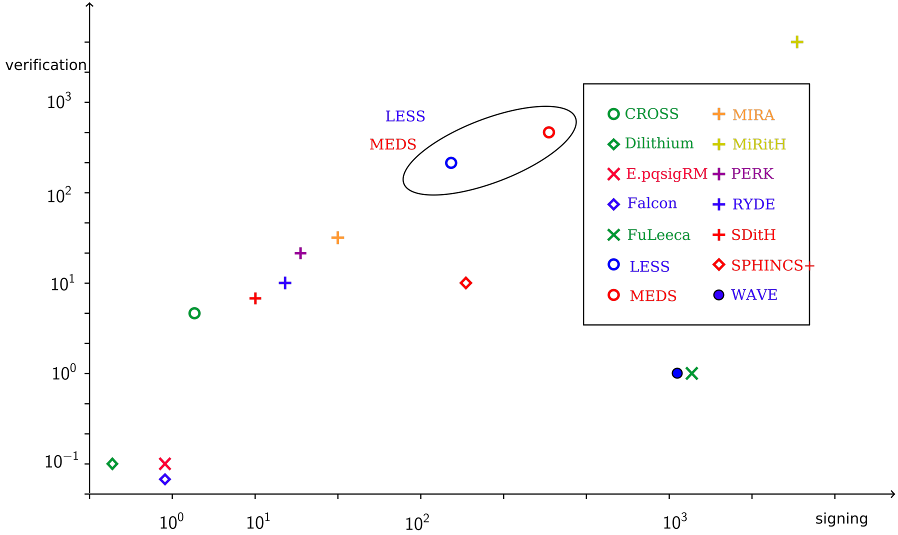


Performance

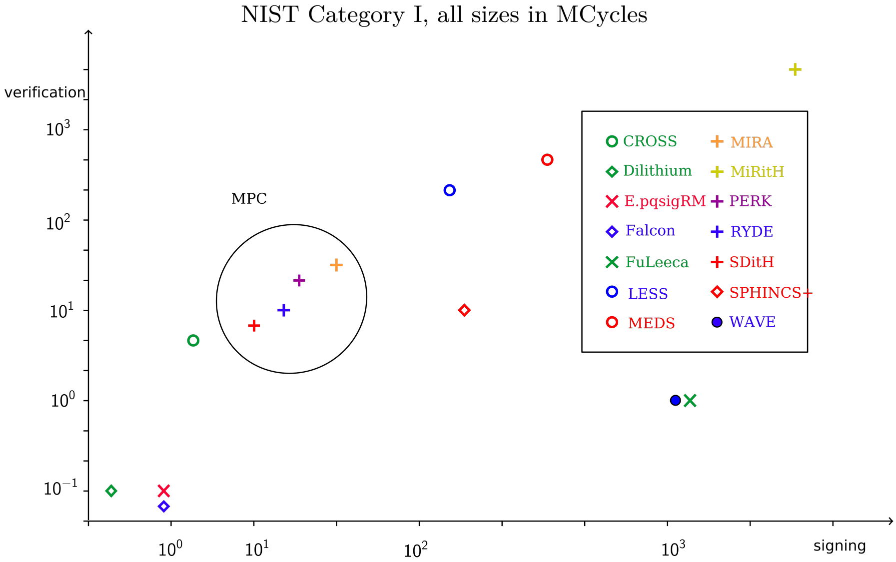


Performance

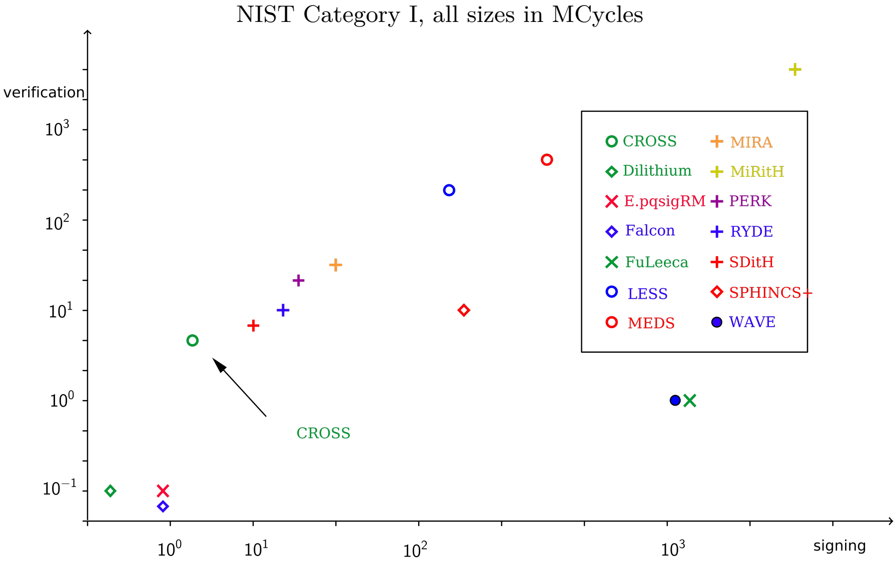
NIST Category I, all sizes in MCycles



Performance



Performance



Questions?

What's next?

- Cryptanalysis continues
- Improvements?
- How many rounds?

Questions?

What's next?

- Cryptanalysis continues
- Improvements?
- How many rounds?

Announcement:

CBCrypto 2024

May 25-26 in Zurich

Questions?

What's next?

- Cryptanalysis continues
- Improvements?
- How many rounds?

Announcement:

CBCrypto 2024

May 25-26 in Zurich

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

Hash-and-Sign: CFS

PROVER		VERIFIER
KEY GENERATION		
$\mathcal{S} = H$ parity-check matrix $\mathcal{P} = (t, HP)$ permuted H		
SIGNING		
Choose message m $s = \text{Hash}(m)$ Find e: $s = eH^\top = eP(HP)^\top$, and $\text{wt}(e) \leq t$	$\xrightarrow{m, eP}$	
		VERIFICATION
		Check if $\text{wt}(eP) \leq t$ and $eP(HP)^\top = \text{Hash}(m)$

Hash-and-Sign: CFS

PROVER		VERIFIER
KEY GENERATION		
$\mathcal{S} = H$ parity-check matrix $\mathcal{P} = (t, HP)$ permuted H		
SIGNING		
Choose message m $s = \text{Hash}(m)$ Find e: $s = eH^\top = eP(HP)^\top$, and $\text{wt}(e) \leq t$	$\xrightarrow{m, eP}$	
		VERIFICATION
		Check if $\text{wt}(eP) \leq t$ and $eP(HP)^\top = \text{Hash}(m)$

Problem: Distinguishability

Hash-and-Sign: CFS

PROVER		VERIFIER
KEY GENERATION		
$\mathcal{S} = H$ parity-check matrix $\mathcal{P} = (t, HP)$ permuted H		
SIGNING		
Choose message m $s = \text{Hash}(m)$ Find e: $s = eH^\top = eP(HP)^\top$, and $\text{wt}(e) \leq t$	$\xrightarrow{m, eP}$	
		VERIFICATION
		Check if $\text{wt}(eP) \leq t$ and $eP(HP)^\top = \text{Hash}(m)$

Not any s is syndrome of low weight 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 $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

CVE

PROVER		VERIFIER
KEY GENERATION		Recall SDP: (1) $s = eH^\top$ (2) $\mathrm{wt}(e) \leq t$
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 $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

Problem: big signature sizes