Recent Advances in Code-based Signatures

Violetta Weger

Rudolf Mößbauer Tenure Track Professorship:
Symposium "Selected Topics in Science and Technology"

March 22, 2023

Outline

1. **Code-based Cryptography**
   - **Introduction to Coding Theory**
   - **Hard Problems from Coding Theory**
   - **Previous Work**

2. **Code-based Signature Schemes**
   - **Idea and Previous Work**
   - **FuLeeca**
   - **Restricted Errors**

3. **Future Research**
   - **Rank-metric Decoding**
   - **Quantum Codes**
   - **Further Research Directions**

Outline

Motivation

- Quantum computers: break all currently used asymmetric cryptosystems

$\rightarrow$ Need quantum-secure alternatives

- Candidates for post-quantum cryptography: Systems based NP-hard problems

Motivation

- Quantum computers: break all currently used asymmetric cryptosystems

→ Need quantum-secure alternatives

- Candidates for post-quantum cryptography: Systems based NP-hard problems

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

Motivation

- Quantum computers: break all currently used asymmetric cryptosystems

→ Need quantum-secure alternatives

- Candidates for post-quantum cryptography: Systems based NP-hard problems

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

- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

Motivation

- Quantum computers: break all currently used asymmetric cryptosystems

$\rightarrow$ Need quantum-secure alternatives

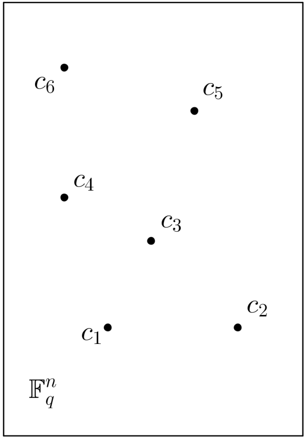
- Candidates for post-quantum cryptography: Systems based NP-hard problems

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

- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

2022 NIST reopened standardization call for signature schemes

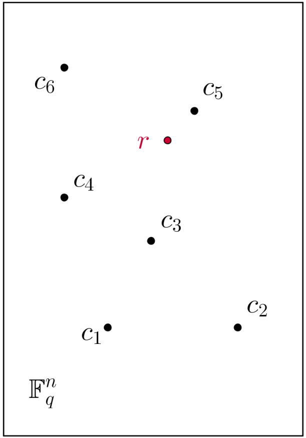
Coding Theory



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*
  $\mathcal{C} = \{c \in \mathbb{F}_q^n \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*

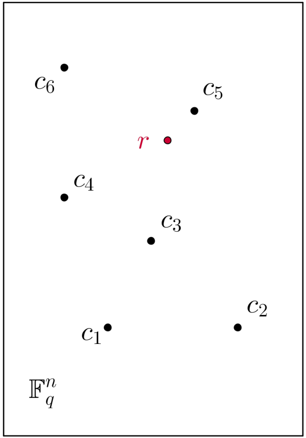
Coding Theory



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*
  $\mathcal{C} = \{c \in \mathbb{F}_q^n \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword

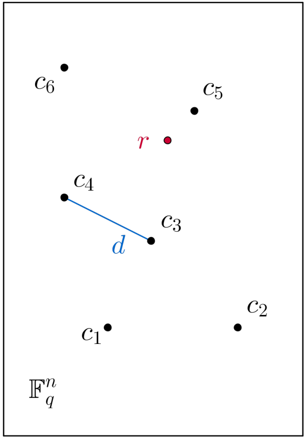
Coding Theory



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*
  $\mathcal{C} = \{c \in \mathbb{F}_q^n \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: For $x, y \in \mathbb{F}_q^n$
  $d_H(x,y) = \mid \{i \mid x_i \neq y_i\} \mid$

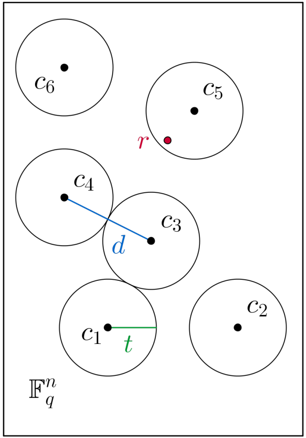
Coding Theory



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*
  $\mathcal{C} = \{c \in \mathbb{F}_q^n \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: For $x, y \in \mathbb{F}_q^n$
  $d_H(x,y) = \mid \{i \mid x_i \neq y_i\} \mid$
- *minimum distance of a code*:
  $d(\mathcal{C}) = \min\{d_H(x,y) \mid x \neq y \in \mathcal{C}\}$

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*
  $\mathcal{C} = \{c \in \mathbb{F}_q^n \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: For $x, y \in \mathbb{F}_q^n$
  $d_H(x, y) = \mid \{i \mid x_i \neq y_i\} \mid$
- *minimum distance of a code*:
  $d(\mathcal{C}) = \min\{d_H(x, y) \mid x \neq y \in \mathcal{C}\}$
- *error-correction capacity*: $t = (d(\mathcal{C}) - 1)/2$

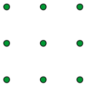
Hard Problems from Coding Theory

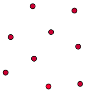
Algebraic structure

(Reed-Solomon, Goppa,..)

$\rightarrow$ efficient decoders

$\langle G \rangle$





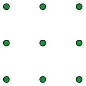
$\langle \widetilde{G} \rangle$

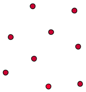
random code

$\rightarrow$ how hard to decode?

Hard Problems from Coding Theory

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

$\langle G \rangle$ 

 $\langle \widetilde{G} \rangle$

random code

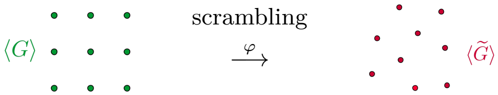
$\rightarrow$ how hard to decode?

- 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



Seemingly random code

$\rightarrow$ how hard to decode?

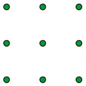
- Decoding random linear code is NP-hard
- First code-based cryptosystem based on this problem

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

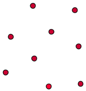
R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory", DSNP Report, 1978

Hard Problems from Coding Theory

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

$\langle G \rangle$ 

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
- 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.

Previous Work

Lee Metric

For $x, y \in \mathbb{Z}/p^s\mathbb{Z}^n$

- *Lee weight*: $\mathrm{wt}_L(x) = \sum_{i=1}^n \mathrm{wt}_L(x_i) = \sum_{i=1}^n \min\{x_i, \mid p^s - x_i \mid\}$
- *Lee distance*: $d_L(x, y) = \mathrm{wt}_L(x - y).$

$\rightarrow$ $d_L(\mathcal{C})$ much larger than $d_H(\mathcal{C})$

Previous Work

Lee Metric

For $x, y \in \mathbb{Z}/p^s\mathbb{Z}^n$

- *Lee weight*: $\mathrm{wt}_L(x) = \sum_{i=1}^{n} \mathrm{wt}_L(x_i) = \sum_{i=1}^{n} \min\{x_i, \mid p^s - x_i \mid\}$
- *Lee distance*: $d_L(x, y) = \mathrm{wt}_L(x - y)$.

$\rightarrow$ $d_L(\mathcal{C})$ much larger than $d_H(\mathcal{C})$

- Decoding random linear code in Lee-metric is NP-hard
- Fastest solvers: Lee-metric ISD, exponential time
- Behaviour of random ring-linear codes

V.W., K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, E. Persichetti. "On the hardness of the Lee syndrome decoding problem", Advances in Mathematics of Communications, 2021.

J. Bariffi, K. Khathuria, **V.W.** "Information Set Decoding for Lee-Metric Codes using Restricted Balls", CBCrypto, 2022.

E. Byrne, A.-L. Horlemann, K. Khathuria, **V.W.** "Density of free modules over finite chain rings", Linear Algebra and its Applications, 2022.

Outline

1. Code-based Cryptography
   - Introduction to Coding Theory
   - Hard Problems from Coding Theory
   - Previous Work

2. **Code-based Signature Schemes**
   - **Idea and Previous Work**
   - **FuLeeca**
   - **Restricted Errors**

3. Future Research
   - Rank-metric Decoding
   - Quantum Codes
   - Further Research Directions

Idea of Signature Schemes

Signer **Verifier**

Key Generation

Secret key $\mathcal{S}$, public key $\mathcal{P}$

$\xrightarrow{\mathcal{P}}$

Signing

Message m, signature σ

$\xrightarrow{m,\sigma}$

Verification

Verify σ

Idea of Signature Schemes

Signer **Verifier**

Key Generation

Secret key $\mathcal{S}$, public key $\mathcal{P}$

$\xrightarrow{\mathcal{P}}$

Signing

Message m, signature σ

$\xrightarrow{m,\sigma}$

Verification

Verify σ

Two approaches to get a code-based signature scheme:

- Hash-and-sign
- Through ZK protocol

Idea of Signature Schemes

Signer | **Verifier**

Key Generation

Secret key $\mathcal{S}$, public key $\mathcal{P}$

$\xrightarrow{\mathcal{P}}$

Signing

Message m, signature σ

$\xrightarrow{m,\sigma}$

Verification

Verify σ

Two approaches to get a code-based signature scheme:

- Hash-and-sign

$\rightarrow$ large public key sizes

$\rightarrow$ our solution: FuLeeca

- Through ZK protocol

$\rightarrow$ large signature sizes

$\rightarrow$ our solution: restricted errors

Idea of Signature Schemes

Signer | **Verifier**

Key Generation

Secret key $\mathcal{S}$, public key $\mathcal{P}$

$\xrightarrow{\mathcal{P}}$

Signing

Message m, signature σ

$\xrightarrow{m,\sigma}$

Verification

Verify σ

Two approaches to get a code-based signature scheme:

- Hash-and-sign

$\rightarrow$ large public key sizes

$\rightarrow$ our solution: FuLeeca

- Through ZK protocol

$\rightarrow$ large signature sizes

$\rightarrow$ our solution: restricted errors

Hash-and-Sign

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

- Following idea of McEliece:

$\rightarrow$ start with structured code $\rightarrow$ large public key sizes

$\rightarrow$ publish scrambled code

- $\mathrm{Hash}(m) = eH^\top$, $\mathrm{wt}_H(e) \leq t$ $\rightarrow$ slow signing
- Signature is scrambled e

Hash-and-Sign

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

- Following idea of McEliece:

$\rightarrow$ start with structured code $\rightarrow$ large public key sizes

$\rightarrow$ publish scrambled code

- $\text{Hash}(m) = eH^\top$, $\text{wt}_H(e) \leq t$ $\rightarrow$ slow signing
- Signature is scrambled e

- Reduce key sizes:

$\rightarrow$ use quasi-cyclic codes $\rightarrow$ statistical attacks

$\rightarrow$ use low density generators

Hash-and-Sign

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

- Following idea of McEliece:

$\rightarrow$ start with structured code $\rightarrow$ large public key sizes

$\rightarrow$ publish scrambled code

- Hash$(m) = eH^\top$, $\mathrm{wt}_H(e) \leq t$
- Signature is scrambled e

$\rightarrow$ slow signing

- Reduce key sizes:

$\rightarrow$ use quasi-cyclic codes $\rightarrow$ statistical attacks

$\rightarrow$ use low density generators

How to reduce public key sizes/ thwart statistical attacks?
How to speed-up signing?

FuLeeca

S. Ritterhoff, G. Maringer, S. Bitzer, **V.W.**, P. Karl, T. Schamberger, J. Schupp, A. Wachter-Zeh, G. Sigl. "FuLeeca: A Lee-based Signature Scheme", Preprint, 2023.

Secret key	Quasi-cyclic, low Lee weight generators
Public key	Systematic form, scrambled generator matrix
Signature	Codeword σ with low Lee weight and full Hamming weight, σ and Hash(m) have many signs matching

FuLeeca

S. Ritterhoff, G. Maringer, S. Bitzer, **V.W.**, P. Karl, T. Schamberger, J. Schupp, A. Wachter-Zeh, G. Sigl. "FuLeeca: A Lee-based Signature Scheme", Preprint, 2023.

Secret key	Quasi-cyclic, low Lee weight generators
Public key	Systematic form, scrambled generator matrix
Signature	Codeword σ with low Lee weight and full Hamming weight, σ and $\mathrm{Hash}(m)$ have many signs matching

	public key size	signature size	total size
Falcon	897 B	666 B	1563 B
Dilithium	1312 B	2420 B	3732 B
Sphincs+	32 B	7856 B	7888 B
FuLeeca	389 B	276 B	665 B

$\rightarrow$ Can beat all standardized signature schemes in total size

Code-based ZK Protocols

ZK protocol $\xrightarrow{\text{Fiat-Shamir}}$ Signature scheme

Syndrome Decoding Problem

Given parity-check matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_H(e) \leq t$

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.

- Random H, e of weight t, compute $s = eH^\top$ $\rightarrow$ small public key sizes
- Verifier challenges either 1. or 2. by asking for transformation φ or transformed secret $\varphi(e)$

Code-based ZK Protocols

ZK protocol $\xrightarrow{\text{Fiat-Shamir}}$ Signature scheme

Syndrome Decoding Problem

Given parity-check matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_H(e) \leq t$

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.

- Random H, e of weight t, compute $s = eH^\top$ $\rightarrow$ small public key sizes
- Verifier challenges either 1. or 2. by asking for transformation φ or transformed secret $\varphi(e)$
- Large cheating probability $\rightarrow$ many rounds, large signature size, CVE: 40 KB
- Recent improvements through in the head computations $\rightarrow$ smaller signature sizes, 10 KB

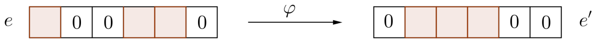
T. Feneuil, A. Joux, M. Rivain "Shared permutation for syndrome decoding: New zero-knowledge protocol and code-based signature", Designs, Codes and Cryptography, 2022.

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

Restricted Errors

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

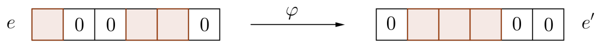


Can we avoid permutations - but keep the hardness of the problem?

Restricted Errors

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



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

Restricted Errors

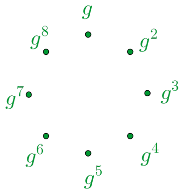
M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem ", Preprint, 2023

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

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

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



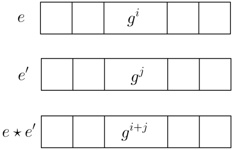
Idea

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

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

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



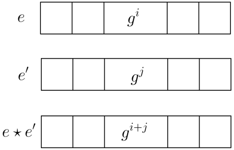
Idea

- $g \in \mathbb{F}_q^{\star}$ of order z, $E = \{g^i \mid i \in \{1, \dots, z\}\}$
- transf. $\varphi : E^n \to E^n, e \mapsto e \star e'$ for $e' \in E^n$
- size of φ is $n \log_2(z)$ (instead of $n \log_2((q-1)n)$)

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

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



Idea

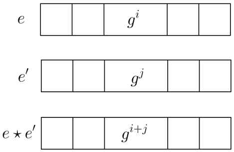
- $g \in \mathbb{F}_q^\star$ of order z, $E = \{g^i \mid i \in \{1, \dots, z\}\}$
- transf. $\varphi : E^n \to E^n, e \mapsto e \star e'$ for $e' \in E^n$
- size of φ is $n \log_2(z)$ (instead of $n \log_2((q-1)n)$)

Can replace SDP with Restricted SDP in any code-based ZK protocol: 10 KB $\to$ 7.2 KB

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

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



Idea

- $g \in \mathbb{F}_q^{\star}$ of order z, $E = \{g^i \mid i \in \{1, \dots, z\}\}$
- transf. $\varphi : E^n \to E^n, e \mapsto e \star e'$ for $e' \in E^n$
- size of φ is $n \log_2(z)$ (instead of $n \log_2((q-1)n)$)

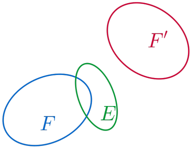
Can replace SDP with Restricted SDP in any code-based ZK protocol: 10 KB $\to$ 7.2 KB

Open Question

Can we exploit the commutativity of the restricted transformations?

Outline

Future Research: Rank-metric Decoding



- For $x \in \mathbb{F}_{q^m}^n$: *Rank metric*: $wt_R(x) = \dim(\langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q})$
- Rank Syndrome Decoding Problem: no NP-hard reduction
- Hamming-metric decoders have cost in $\mathcal{O}\left(q^{nc}\right)$ for some constant c
- Rank-metric decoders have cost in $\mathcal{O}\left(q^{n^2c'}\right)$ for some constant c'

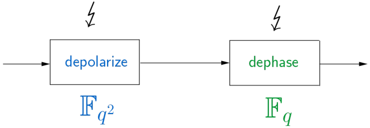
  $\rightarrow$ Small key sizes

$\rightarrow$ **Goal: Improve decoders**

- *Error support* $E = \langle e_1, \ldots, e_n \rangle_{\mathbb{F}_q}$
- candidate supersupports F, F'

TUM	Antonia Wachter-Zeh
International	Alberto Ravagnani (TU/e)

Future Research: Quantum Codes



- Quantum error-corrections:
  (1) depolarizing channel,
  (2) dephasing channel
- Introduced errors:
  (1) Z and X-errors,
  (2) only Z-errors
- X-errors are in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$
  Z-errors are in $\mathbb{F}_q \setminus \{0\}$

$\rightarrow$ Errors in base field more likely

$\rightarrow$ New metric:
$wt_\lambda(x) = \lambda$ if $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$
$wt_\lambda(x) = 1$ if $x \in \mathbb{F}_q \setminus \{0\}$

$\rightarrow$ **Goal: New bounds and constructions**

TUM	Robert König
International	Markus Grassl (ICTQT)

Further Research Directions

- **Quantum-Private Information Retrieval**
  - Retrieve file from database managed by untrusted server
  - without revealing to the server which file was requested
  - single server: only number-theoretic solutions: not quantum-secure

  → **Goal:** code-based quantum-private information retrieval

TUM	Antonia Wachter-Zeh
International	Camilla Hollanti (Aalto University)

- **Locally Recoverable Codes**

  → **Goal:** New constructions

  TUM Gregor Kemper

- **Isogeny-based Cryptography**

  → **Goal:** New systems

  TUM Christian Liedtke

Questions?

Thank you!

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 $s = \mathrm{Hash}(m)$ Find e: $s = eH^\top = eP(HP)^\top$, and $\mathrm{wt}(e) \leq t$	$\xrightarrow{m, eP}$	
		VERIFICATION
		Check if $\mathrm{wt}(eP) \leq t$ and $eP(HP)^\top = \mathrm{Hash}(m)$

Not any s is syndrome of low weight e

ZKID

PROVER		VERIFIER
		VERIFICATION
commitments c_0, c_1	$\xrightarrow{c_0, c_1}$	
	$\xleftarrow{b}$	$b \in \{0, 1\}$
response r_b	$\xrightarrow{r_b}$	
		Verify c_b using $r_b, \mathcal{P}$

SIGNING		
Choose message m		
Construct signature s from $\mathcal{S}$, m		
	$\xrightarrow{m, s}$	
		VERIFICATION
		Verify signature s using $\mathcal{P}$, m

Signature Scheme

ZKID

PROVER		VERIFIER
		VERIFICATION
commitments c_0, c_1	$\xrightarrow{c_0, c_1}$	
	$\xleftarrow{b}$	$b \in \{0, 1\}$
response r_b	$\xrightarrow{r_b}$	
		Verify c_b using $r_b, \mathcal{P}$

Fiat-Shamir $\downarrow$

SIGNING		
Choose message m		
Construct signature s from $\mathcal{S}$, m		
	$\xrightarrow{m, s}$	
		VERIFICATION
		Verify signature s using $\mathcal{P}$, m

Signature Scheme

Fiat-Shamir

PROVER		VERIFIER
KEY GENERATION		
Given $\mathcal{P}, \mathcal{S}$ of some ZKID and message m		
SIGNING		
Choose commitment c $b = \text{Hash}(m, c)$ Compute response r_b Signature $s = (b, r_b)$		
	$\xrightarrow{m,s}$	
		VERIFICATION
		Using $r_b, \mathcal{P}$ construct c check if $b = \text{Hash}(m, c)$

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 $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

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

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^{λ} want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^{N}

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^{λ} want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N
- might need many rounds: large communication cost

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^λ want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N
- might need many rounds: large communication cost
- solution: compression technique
- do not send c_0^i, c_1^i in each round i
- before 1. round send $c = \text{Hash}(c_0^1, c_1^1, \ldots, c_0^N, c_1^N)$
- ith round: receiving challenge b prover sends r_b^i, c_{1-b}^i
- end: verifier checks $c = \text{Hash}(c_0^1, c_1^1, \ldots, c_0^N, c_1^N)$

C. Aguilar, P. Gaborit, J. Schrek. "A new zero-knowledge code based identification scheme with reduced communication", IEEE Information Theory Workshop, 2011.

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^λ want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N
- might need many rounds: large communication cost
- other solution: MPC in the head
- third party: trusted helper sends commitments $\rightarrow \delta = 0$
- instead prover sends seeds of commitment: not ZK $\rightarrow$ cut and choose
- $x < N$ times send response, $N - x$ times send the seed of commitment
- to compress: use Merkle root or seed tree

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

Comparison

	ZKID	Hash-and-Sign
reduction to NP-hard		
low public key size		
low signature size		
fast verification		

Comparison

	ZKID	Hash-and-Sign
reduction to NP-hard	✓	×
low public key size		
low signature size		
fast verification		

Comparison

	ZKID	Hash-and-Sign
reduction to NP-hard	✓	×
low public key size	✓	×
low signature size		
fast verification		

Comparison

	ZKID	Hash-and-Sign	
reduction to NP-hard	✓	×	
low public key size	CVE: 70 B	WAVE: 3 MB	NIST: 3 KB
low signature size			
fast verification			

Comparison

	ZKID	Hash-and-Sign	
reduction to NP-hard	✓	×	
low public key size	CVE: 70 B	WAVE: 3 MB	NIST: 3 KB
low signature size	∼	✓	
fast verification			

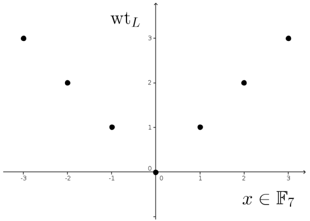
Comparison

	ZKID	Hash-and-Sign	
reduction to NP-hard	$\checkmark$	$\times$	
low public key size	CVE: 70 B	WAVE: 3 MB	NIST: 3 KB
low signature size	CVE: 43 KB	WAVE: 1 KB	NIST: 2 KB
fast verification			

Comparison

	ZKID	Hash-and-Sign	
reduction to NP-hard	✓	×	
low public key size	CVE: 70 B	WAVE: 3 MB	NIST: 3 KB
low signature size	CVE: 43 KB	WAVE: 1 KB	NIST: 2 KB
fast verification	∼	✓	

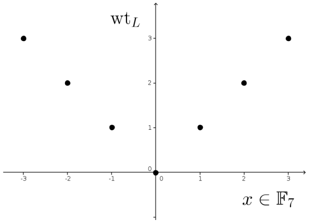
FuLeeca



Set up

- For $x \in \mathbb{F}_p$: $\mathrm{wt}_L(x) = \min\{x, \mid p - x \mid\}$.
  For $x \in \mathbb{F}_p^n$: $\mathrm{wt}_L(x) = \sum_{i=1}^n \mathrm{wt}_L(x_i)$.
- Representing $\mathbb{F}_p = \{-\frac{p-1}{2}, \ldots, 0, \ldots, \frac{p-1}{2}\}$,
  $\mathrm{wt}_L(x) = \mid x \mid$.

FuLeeca



x	-1	-3	1	2

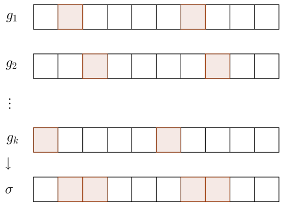
y	-3	1	2	0

$\mathrm{mt}(x, y) = 2$

Set up

- For $x \in \mathbb{F}_p$: $\mathrm{wt}_L(x) = \min\{x, \mid p - x \mid\}$.
  For $x \in \mathbb{F}_p^n$: $\mathrm{wt}_L(x) = \sum_{i=1}^n \mathrm{wt}_L(x_i)$.
- Representing $\mathbb{F}_p = \{-\frac{p-1}{2}, \dots, 0, \dots, \frac{p-1}{2}\}$,
  $\mathrm{wt}_L(x) = \mid x \mid$.
- Number of matches between $x, y \in \mathbb{F}_p^n$
  $\mathrm{mt}(x, y) = \mid \{i \mid \mathrm{sgn}(x_i) = \mathrm{sgn}(y_i)\} \mid$.

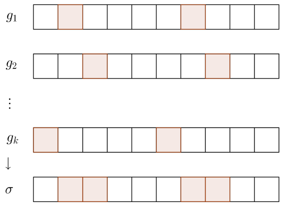
Statistical Attacks



Set up

- Low Hamming weight generators will produce low Hamming weight signatures
- Observing many signatures reveals the support of the secret low Hamming weight generators

Statistical Attacks



g_1	1	1	2	1	3	0
g_2	0	1	1	2	1	3
$\vdots$						
g_k	1	2	1	3	0	1
$\downarrow$						
σ	2	4	4	6	4	4

Set up

- Low Hamming weight generators will produce low Hamming weight signatures
- Observing many signatures reveals the support of the secret low Hamming weight generators

- Low Lee weight generators: $\text{supp}_L(x) = (\text{wt}_L(x_1), \dots, \text{wt}_L(x_n))$
- Signatures have low Lee weight
- Recovering Lee support of secret generators: much harder

FuLeeca

PROVER		VERIFIER
KEY GENERATION		
Secret key: $G = [A \;\; B]$, quasi-cyclic matrix, with low Lee weight		
Public key: $G' = [\mathrm{Id} \;\; A^{-1}B]$	$\xrightarrow{(G',t,\mu)}$	
SIGNING		
Choose message m		
$c = \mathrm{Hash}(m) \in \{\pm 1\}^n$		
Iteratively use G to construct codeword σ with		
$\mathrm{wt}_L(\sigma) \leq t$,		
$\mathrm{mt}(\sigma, c) \geq \mu$	$\xrightarrow{m,\sigma}$	
		VERIFICATION
		Verify that: $(1)\sigma H^\top = 0$,
		$(2)\mathrm{wt}_L(\sigma) \leq t$,
		$(3)\mathrm{mt}(c, \sigma) \geq \mu$