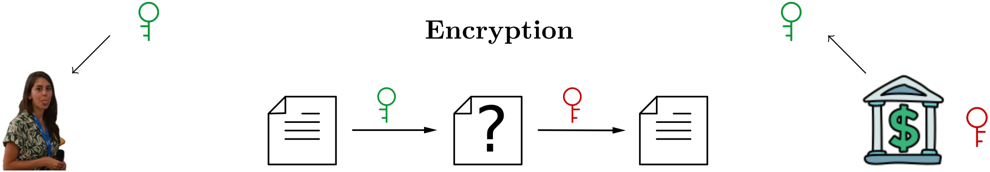
Open problems in code-based cryptography

Violetta Weger

Coding Theory Colloquium

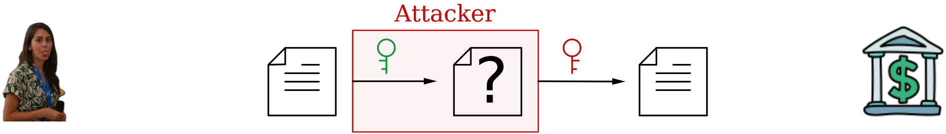
November 8, 2023

Gentle Introduction to Crypto

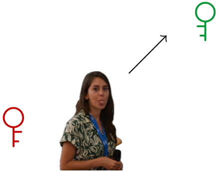


Gentle Introduction to Crypto

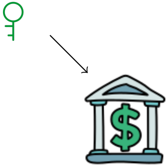
Encryption



Gentle Introduction to Crypto

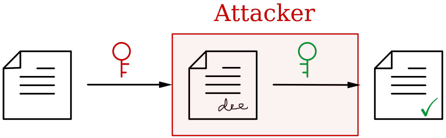


Signature



Gentle Introduction to Crypto

Signature



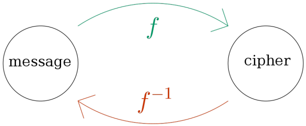
Gentle Introduction to Crypto

Encryption

Trapdoor

- f easy to compute with
- f^{-1} hard to compute with

→ f^{-1} easy with secret



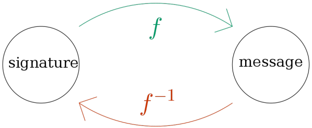
Gentle Introduction to Crypto

Signature

Trapdoor

- f easy to compute with
- f^{-1} hard to compute with

→ f^{-1} easy with secret



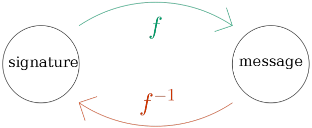
Gentle Introduction to Crypto

Signature

Trapdoor

- f easy to compute with
- f^{-1} hard to compute with

→ f^{-1} easy with secret



Attacks

- message recovery/forgery: f^{-1} without secret
- key recovery: find secret

→ security level λ: best algo. needs 2^{λ} ops.

Constraints

- public, signature **small**
- decrypt/sign:

  f^{-1} with secret **fast**

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- Integer factorization: $f(p, q) = p \cdot q = n$
- DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- Integer factorization: $f(p,q) = p \cdot q = n$
- DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- Shor's algorithm

→ find period of function in poly. time

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p,q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

Classic Crypto vs. Post-quantum Crypto

Classic crypto

× Integer factorization: $f(p,q) = p \cdot q = n$

× DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

∘ Shor's algorithm

→ find period of function in poly. time

all public-key crypto is broken!

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p, q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

all public-key crypto is broken! still far away..

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p,q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

all public-key crypto is broken! still far away.. ..but should transition now

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p,q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

all public-key crypto is broken! still far away.. ..but should transition now

Post-quantum crypto

- ∘ (preferably) NP-hard problem
- ∘ quantum algos. need exp. time

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p,q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

all public-key crypto is broken! still far away.. ..but should transition now

Post-quantum crypto

- ∘ (preferably) NP-hard problem
- ∘ quantum algos. need exp. time

NIST standardization calls

- ∘ 2016: 3 code-based encryption

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p,q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

all public-key crypto is broken! still far away.. ..but should transition now

Post-quantum crypto

- ∘ (preferably) NP-hard problem
- ∘ quantum algos. need exp. time

NIST standardization calls

- ∘ 2016: 3 code-based encryption
- ∘ 2023: 9 code-based signatures

Classic Crypto vs. Post-quantum Crypto

Classic crypto

- × Integer factorization: $f(p,q) = p \cdot q = n$
- × DLP: $f(c) = a^c = b$ in $\mathbb{F}_q$ or ell. curve

Quantum algorithms

- ∘ Shor's algorithm
- → find period of function in poly. time

all public-key crypto is broken! still far away.. ..but should transition now

Post-quantum crypto

- ∘ (preferably) NP-hard problem
- ∘ quantum algos. need exp. time

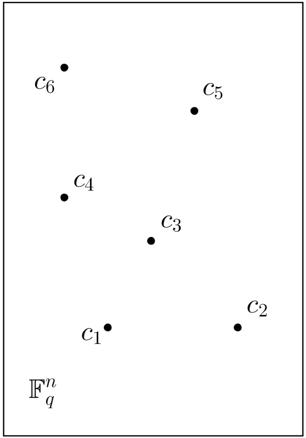
NIST standardization calls

- ∘ 2016: 3 code-based encryption
- ∘ 2023: 9 code-based signatures

Today's talk: open questions for these schemes

- ∘ Classic McEliece
- ∘ McEliece signature
- ∘ decoding rank-metric codes
- ∘ code equivalence problems

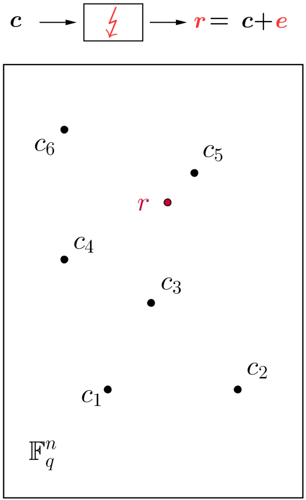
Coding Theory



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*

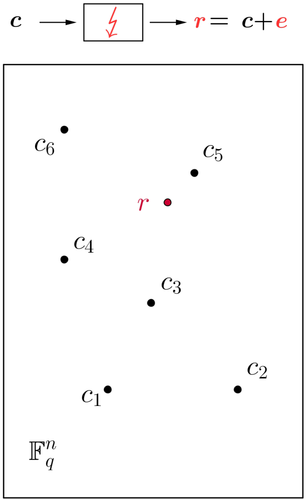
Coding Theory



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

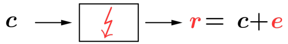
Coding Theory

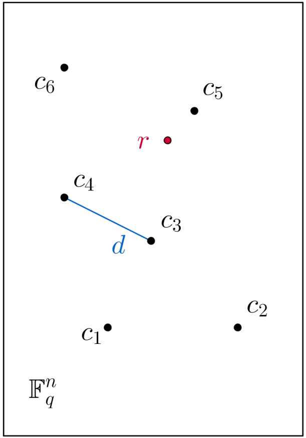


Set Up

- *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



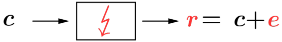


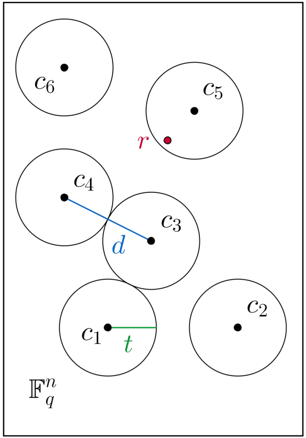
Set Up

- *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*:

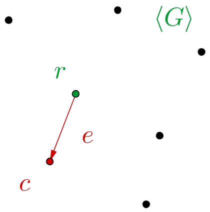
$$d(\mathcal{C}) = \min\{d_H(x,y) \mid x \neq y \in \mathcal{C}\}$$

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

Syndrome Decoding Problem

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. $\mathrm{wt}_H(e) \leq t$

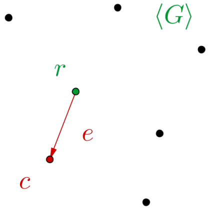


Syndrome Decoding Problem

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. $\mathrm{wt}_H(e) \leq t$

NP-hard

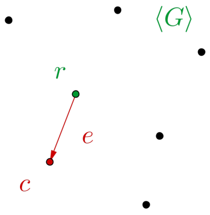


Syndrome Decoding Problem

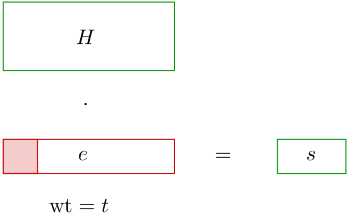
Syndrome Decoding Problem (SDP):
Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

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

NP-hard



Information set decoding (ISD)



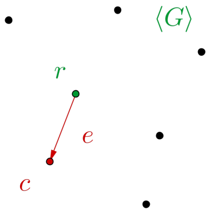
Syndrome Decoding Problem

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. $\mathrm{wt}_H(e) \leq t$

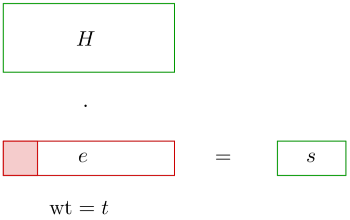
NP-hard



Information set decoding (ISD)

- $I \subset \{1, \ldots, n\}$: $|\mathcal{C}_I| = |\mathcal{C}|$

→ G_I invertible, H_{I^C} invertible

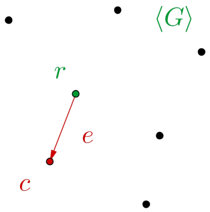


Syndrome Decoding Problem

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. $\mathrm{wt}_H(e) \le t$

NP-hard



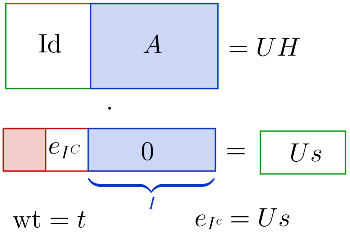
Information set decoding (ISD)

- $I \subset \{1,\ldots,n\}$: $|\mathcal{C}_I| = |\mathcal{C}|$

→ G_I invertible, H_{I^C} invertible

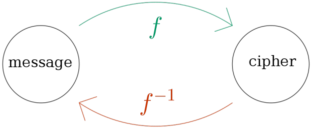
- find error-free information set I
- cost $= \binom{n}{t}\binom{n-k}{t}^{-1}$
- assume $t = (d-1)/2$, d from GV

→ cost $q^{nf(n,R)} \sim 2^{0.05n}$



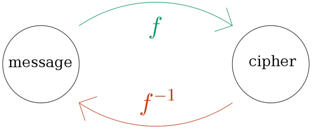
Syndrome Decoding Problem

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



Syndrome Decoding Problem

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



Encryption scheme

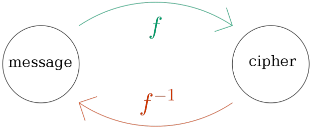
- secret H (with efficient decoder)
- public scrambled H', s, t
- → cipher = f(message)

trapdoor

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}_H(e) \leq t\} \to \mathbb{F}_q^{n-k},$$
$$e \mapsto eH'^\top = s$$

Syndrome Decoding Problem

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



Encryption scheme

- secret H (with efficient decoder)
- public scrambled H', s, t
- → cipher = f(message)

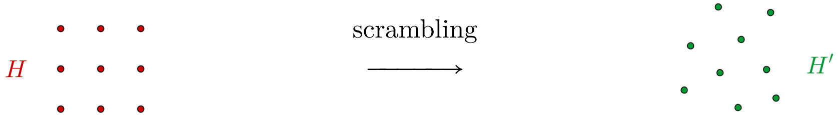
trapdoor

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}_H(e) \le t\} \to \mathbb{F}_q^{n-k},$$
$$e \mapsto eH'^\top = s$$

Which secret code to choose?

Classic McEliece

- secret H Goppa code
- public $H' = SHP$, S invertible, P permutation

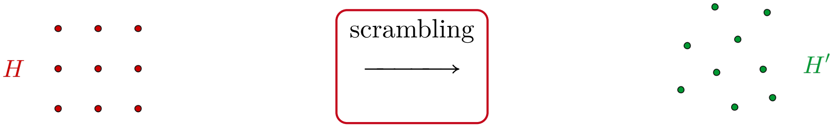


Classic McEliece

secret H Goppa code

public $H' = SHP$, S invertible, P permutation

Distinguishing Problem



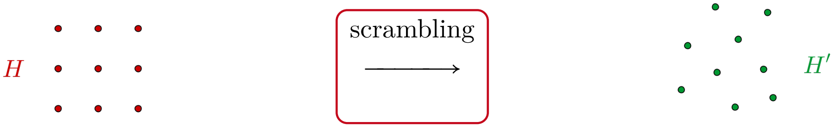
1. Open problem: Distinguish Goppa code from random code

Classic McEliece

secret H Goppa code

public $H' = SHP$, S invertible, P permutation

Distinguishing Problem



1. Open problem: Distinguish Goppa code from random code

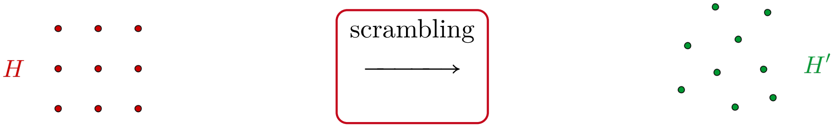
- 4th round candidate NIST
- standardized in Germany

Classic McEliece

secret H Goppa code

public $H' = SHP$, S invertible, P permutation

Distinguishing Problem



1. Open problem: Distinguish Goppa code from random code

- 4th round candidate NIST
- standardized in Germany

TII McEliece Challenges:

Theoretical key recovery: 10'000 $

Distinguish Goppa Codes

Famous distinguisher: Square code

- $a, b \in \mathbb{F}_q^n : a \star b = (a_1 b_1, \ldots, a_n b_n)$
- $\mathcal{C}^{(2)} = \langle \{a \star b : a, b \in \mathcal{C}\} \rangle$

Distinguish Goppa Codes

Famous distinguisher: Square code

- $a, b \in \mathbb{F}_q^n : a \star b = (a_1 b_1, \ldots, a_n b_n)$
- $\mathcal{C}^{(2)} = \langle \{ a \star b : a, b \in \mathcal{C} \} \rangle$

$$\mathcal{C} \text{ random code} \to \dim(\mathcal{C}^{(2)}) = \min\{\binom{k+1}{2}, n\}$$

Distinguish Goppa Codes

Famous distinguisher: Square code

- $a, b \in \mathbb{F}_q^n : a \star b = (a_1 b_1, \dots, a_n b_n)$
- $\mathcal{C}^{(2)} = \langle \{ a \star b : a, b \in \mathcal{C} \} \rangle$

$$\mathcal{C} \text{ random code} \to \dim(\mathcal{C}^{(2)}) = \min\{\binom{k+1}{2}, n\}$$

$\mathsf{GRS}(\alpha, \beta) = \{(f(\alpha_1)\beta_1, \dots, f(\alpha_n)\beta_n) : f \in \mathbb{F}_{p^m}[x], \deg < k\}$

$$H = \begin{pmatrix} \beta_1' & \beta_2' & \cdots & \beta_n' \\ \alpha_1\beta_1' & \alpha_2\beta_2' & \cdots & \alpha_n\beta_n' \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1}\beta_1' & \alpha_2^{t-1}\beta_2' & \cdots & \alpha_n^{t-1}\beta_n' \end{pmatrix} \in \mathbb{F}_{p^m}^{t \times n}$$

$\mathsf{GRS}(\alpha, \beta) \in \mathbb{F}_{p^m}^n$ of dim $k = n - t$

Distinguish Goppa Codes

Famous distinguisher: Square code

- $a, b \in \mathbb{F}_q^n : a \star b = (a_1 b_1, \dots, a_n b_n)$
- $\mathcal{C}^{(2)} = \langle \{ a \star b : a, b \in \mathcal{C} \} \rangle$

$$\mathcal{C} \text{ random code} \to \dim(\mathcal{C}^{(2)}) = \min\{\binom{k+1}{2}, n\}$$

$\mathsf{GRS}(\alpha, \beta) = \{(f(\alpha_1)\beta_1, \dots, f(\alpha_n)\beta_n) : f \in \mathbb{F}_{p^m}[x], \deg < k\}$

$$H = \begin{pmatrix} \beta_1' & \beta_2' & \cdots & \beta_n' \\ \alpha_1\beta_1' & \alpha_2\beta_2' & \cdots & \alpha_n\beta_n' \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1}\beta_1' & \alpha_2^{t-1}\beta_2' & \cdots & \alpha_n^{t-1}\beta_n' \end{pmatrix} \in \mathbb{F}_{p^m}^{t \times n}$$

$\mathsf{GRS}(\alpha, \beta) \in \mathbb{F}_{p^m}^n$ of dim $k = n - t$ $\to$ $\dim(\mathsf{GRS}(\alpha, \beta)^{(2)}) = \min\{2k - 1, n\}$

Distinguish Goppa Codes

$\mathsf{Goppa}(\alpha, g) \in \mathbb{F}_p^n$ of dim $k' = n - tm$

- $g \in \mathbb{F}_{p^m}[x]$ irreducible
- $\beta_i = g(\alpha_i)^{-1}$

$\longrightarrow$ $\mathsf{Goppa}(\alpha, g) = \mathsf{GRS}(\alpha, \beta) \cap \mathbb{F}_p^n$

- Γ basis of $\mathbb{F}_{p^m} \, / \, \mathbb{F}_p$ $\longrightarrow$ $\mathsf{Goppa}(\alpha, g) = \Gamma(\mathsf{GRS}(\alpha, \beta))$

$H_{\mathsf{GRS}} \in \mathbb{F}_{p^m}^{t \times n} \xrightarrow{\Gamma} H_{\mathsf{Goppa}} \in \mathbb{F}_p^{mt \times n}$

Distinguish Goppa Codes

$\mathsf{Goppa}(\alpha, g) \in \mathbb{F}_p^n$ of dim $k' = n - tm$

- $g \in \mathbb{F}_{p^m}[x]$ irreducible
- $\beta_i = g(\alpha_i)^{-1}$

$\longrightarrow$ $\mathsf{Goppa}(\alpha, g) = \mathsf{GRS}(\alpha, \beta) \cap \mathbb{F}_p^n$

- Γ basis of $\mathbb{F}_{p^m} / \mathbb{F}_p$ $\longrightarrow$ $\mathsf{Goppa}(\alpha, g) = \Gamma(\mathsf{GRS}(\alpha, \beta))$

$H_{\mathsf{GRS}} \in \mathbb{F}_{p^m}^{t \times n} \xrightarrow{\Gamma} H_{\mathsf{Goppa}} \in \mathbb{F}_p^{mt \times n}$

$\rightarrow$ $\dim(\mathsf{Goppa}(\alpha, g)^{(2)}) = \min\{n, \binom{k'+1}{2} - \ell\}, \quad \ell = \frac{mt}{2}(2t\log_2(t) - t - 1)$

Distinguish Goppa Codes

$\text{Goppa}(\alpha, g) \in \mathbb{F}_p^n$ of dim $k' = n - tm$

- $g \in \mathbb{F}_{p^m}[x]$ irreducible
- $\beta_i = g(\alpha_i)^{-1}$

$\longrightarrow$ $\text{Goppa}(\alpha, g) = \text{GRS}(\alpha, \beta) \cap \mathbb{F}_p^n$

- Γ basis of $\mathbb{F}_{p^m} / \mathbb{F}_p$ $\longrightarrow$ $\text{Goppa}(\alpha, g) = \Gamma(\text{GRS}(\alpha, \beta))$

$H_{\text{GRS}} \in \mathbb{F}_{p^m}^{t \times n} \xrightarrow{\Gamma} H_{\text{Goppa}} \in \mathbb{F}_p^{mt \times n}$

$\rightarrow$ $\dim(\text{Goppa}(\alpha, g)^{(2)}) = \min\{n, \binom{k'+1}{2} - \ell\}, \quad \ell = \frac{mt}{2}(2t\log_2(t) - t - 1)$

Parameters Classic McEliece: $p = 2, m = 13, R = 0.75 \;\rightarrow\; \dim(\text{Goppa}(\alpha, g)^{(2)}) = n$ ↯

Distinguish Goppa Codes

Goppa$(\alpha, g) \in \mathbb{F}_p^n$ of dim $k' = n - tm$

- $g \in \mathbb{F}_{p^m}[x]$ irreducible
- $\beta_i = g(\alpha_i)^{-1}$

$\longrightarrow$ Goppa$(\alpha, g) =$ GRS$(\alpha, \beta) \cap \mathbb{F}_p^n$

- Γ basis of $\mathbb{F}_{p^m} \;/\; \mathbb{F}_p$ $\longrightarrow$ Goppa$(\alpha, g) = \Gamma($GRS$(\alpha, \beta))$

$H_{\mathsf{GRS}} \in \mathbb{F}_{p^m}^{t \times n} \xrightarrow{\Gamma} H_{\mathsf{Goppa}} \in \mathbb{F}_p^{mt \times n}$

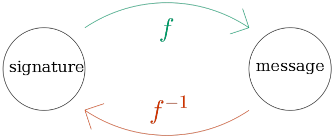
$\rightarrow$ $\dim(\text{Goppa}(\alpha, g)^{(2)}) = \min\{n, \binom{k'+1}{2} - \ell\}, \quad \ell = \frac{mt}{2}(2t\log_2(t) - t - 1)$

Parameters Classic McEliece: $p = 2, m = 13, R = 0.75 \;\rightarrow\; \dim(\text{Goppa}(\alpha, g)^{(2)}) = n$ ↯

Goal: Given $SH_{\mathsf{Goppa}(\alpha,g)}P$ recover α, g

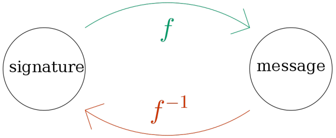
Hash & Sign

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



Hash & Sign

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



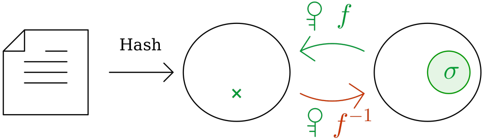
Signature scheme

- secret H (with efficient decoder)
- public scrambled $H' = HP, s, t$
- → signature $\sigma = f^{-1}$(message)

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}(e) \leq t\} \to \mathbb{F}_q^{n-k},$$
$$e \mapsto eH'^\top = s$$

Hash & Sign

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



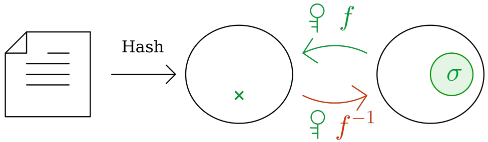
Signature scheme

- secret H (with efficient decoder)
- public scrambled $H' = HP, s, t$
- → signature $\sigma = f^{-1}(\mathsf{Hash}(\text{message}))$

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}(e) \le t\} \to \mathbb{F}_q^{n-k},$$
$$e \mapsto eH'^\top = s$$

Hash & Sign

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



Signature scheme

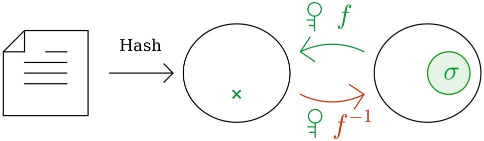
- secret H (with efficient decoder)
- public scrambled $H' = HP, s, t$

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

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}(e) \le t\} \to \mathbb{F}_q^{n-k},$$
$$e \mapsto eH'^\top = s$$

Hash & Sign

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



Signature scheme

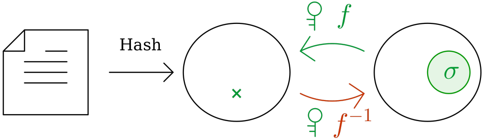
- secret H (with efficient decoder)
- public scrambled $H' = HP, s, t$
- → signature $\sigma = f^{-1}(\mathsf{Hash}(\text{message}))$

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}(e) \le t\} \to \mathbb{F}_q^{n-k}, \quad e \mapsto eH'^\top = s$$

f not bijective

Hash & Sign

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



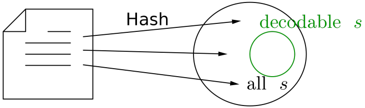
Signature scheme

- secret H (with efficient decoder)
- public scrambled $H' = HP, s, t$
- → signature $\sigma = f^{-1}(\mathsf{Hash}(\text{message}))$

$$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}(e) \le t\} \to \mathbb{F}_q^{n-k},$$
$$e \mapsto eH'^\top = s$$

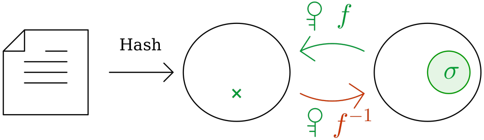
f not bijective

- $\mathsf{Hash}(m) = \sigma H'^\top = (eP)(HP)^\top$
- $\mathsf{Hash}(m) = eH^\top = s, \mathrm{wt}_H(e) \le t$



Hash & Sign

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



Signature scheme

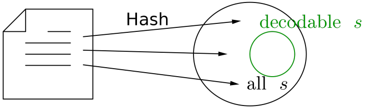
- secret H (with efficient decoder)
- public scrambled $H' = HP, s, t$
- → signature $\sigma = f^{-1}(\mathsf{Hash}(\text{message}))$

$f : \{e \in \mathbb{F}_q^n : \mathrm{wt}(e) \le t\} \to \mathbb{F}_q^{n-k},$

$e \mapsto eH'^\top = s$

f not bijective

- $\mathsf{Hash}(m) = \sigma H'^\top = (eP)(HP)^\top$
- $\mathsf{Hash}(m) = eH^\top = s, \mathrm{wt}_H(e) \le t$
- → salting the Hash → slow



Hash & Sign

Problem

$\mathsf{Hash}(m)$ not decodable syndrome → Hash & Sign scheme: slow

Decodable syndromes $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ $<$ q^{n-k} All syndromes

Hash & Sign

Problem

$\mathsf{Hash}(m)$ not decodable syndrome → Hash & Sign scheme: slow

Decodable syndromes $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \text{poly}(n)$ = q^{n-k} All syndromes

Need an almost perfect code!

Hash & Sign

Problem

$\mathsf{Hash}(m)$ not decodable syndrome → Hash & Sign scheme: slow

Decodable syndromes $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \text{poly}(n) \quad = \quad q^{n-k}$ All syndromes

Need an almost perfect code!

Idea CFS

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

- secret H high rate Goppa

Hash & Sign

Problem

Hash(m) not decodable syndrome → Hash & Sign scheme: slow

Decodable syndromes $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \text{poly}(n) \quad = \quad q^{n-k}$ All syndromes

Need an almost perfect code!

Idea CFS

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

secret H high rate Goppa → square code attack works!

Hash & Sign

Problem

$\mathsf{Hash}(m)$ not decodable syndrome → Hash & Sign scheme: slow

Decodable syndromes $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \text{poly}(n) = q^{n-k}$ All syndromes

Need an almost perfect code!

Idea CFS

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

secret H high rate Goppa → square code attack works!

2. Open problem: Find code

- efficiently decodable
- almost perfect
- not distinguishable

Rank Metric

$\mathbb{F}_{q^m}$-linear 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 $x \in \mathbb{F}_{q^m}^k$

$\mathbb{F}_q$-linear codes/Matrix codes

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

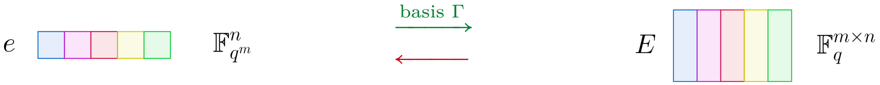
Rank Metric

$\mathbb{F}_{q^m}$-linear 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 $x \in \mathbb{F}_{q^m}^k$

$\mathbb{F}_q$-linear codes/Matrix codes

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



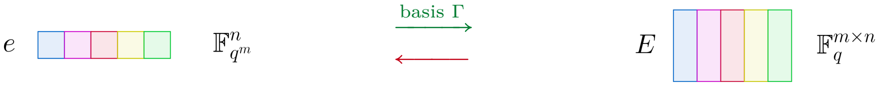
Rank Metric

$\mathbb{F}_{q^m}$-linear 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 $x \in \mathbb{F}_{q^m}^k$

$\mathbb{F}_q$-linear codes/Matrix codes

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



- Support: $\mathcal{E} = \langle e_1, \dots, e_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(e) = \dim_{\mathbb{F}_q}(\mathcal{E})$

- Support: $\mathcal{E} = \mathrm{rowsp}(E) \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(E) = \mathrm{rk}(E)$

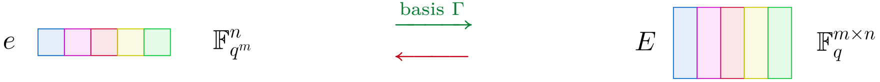
Rank Metric

$\mathbb{F}_{q^m}$-linear 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 $x \in \mathbb{F}_{q^m}^k$

$\mathbb{F}_q$-linear codes/Matrix codes

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



- Support: $\mathcal{E} = \langle e_1, \ldots, e_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(e) = \dim_{\mathbb{F}_q}(\mathcal{E})$

- Support: $\mathcal{E} = \mathrm{rowsp}(E) \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(E) = \mathrm{rk}(E)$

→ SDP: NP-hard (MinRank)

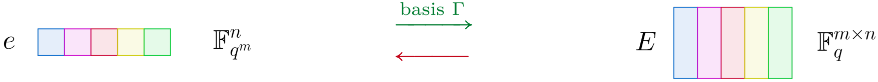
Rank Metric

$\mathbb{F}_{q^m}$-linear 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 $x \in \mathbb{F}_{q^m}^k$

$\mathbb{F}_q$-linear codes/Matrix codes

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



$\mathbb{F}_{q^m}$-linear codes:

- Support: $\mathcal{E} = \langle e_1, \ldots, e_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(e) = \dim_{\mathbb{F}_q}(\mathcal{E})$

→ SDP: not known if NP-hard

Matrix codes:

- Support: $\mathcal{E} = \mathrm{rowsp}(E) \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(E) = \mathrm{rk}(E)$

→ SDP: NP-hard (MinRank)

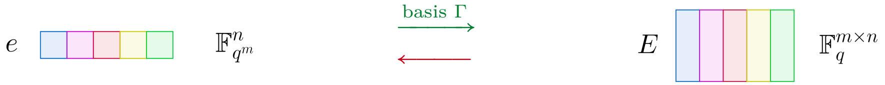
Rank Metric

$\mathbb{F}_{q^m}$-linear 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 $x \in \mathbb{F}_{q^m}^k$

$\mathbb{F}_q$-linear codes/Matrix codes

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



$\mathbb{F}_{q^m}$-linear codes:

- Support: $\mathcal{E} = \langle e_1, \dots, e_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(e) = \dim_{\mathbb{F}_q}(\mathcal{E})$

→ SDP: not known if NP-hard

- Used in: ROLLO, RQC, RYDE

$\mathbb{F}_q$-linear codes/Matrix codes:

- Support: $\mathcal{E} = \mathrm{rowsp}(E) \subset \mathbb{F}_q^m$
- $\mathrm{wt}_R(E) = \mathrm{rk}(E)$

→ SDP: NP-hard (MinRank)

- Used in: MIRA, MiRitH

Hardness of Rank SDP

Rank SDP:
Given p.c. matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_R(e) \leq t$

Hardness of Rank SDP

Rank SDP:
Given p.c. matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_R(e) \leq t$

3. Open problem: Hardness of Rank SDP

- Is Rank SDP NP-hard?
- How to solve Rank SDP?

Hardness of Rank SDP

Rank SDP:
Given p.c. matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_R(e) \leq t$

3. Open problem: Hardness of Rank SDP

- Is Rank SDP NP-hard?
- How to solve Rank SDP?

How to show a problem $\mathcal{P}$ is NP-hard?

Hardness of Rank SDP

Rank SDP:
Given p.c. matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_R(e) \leq t$

3. Open problem: Hardness of Rank SDP

- Is Rank SDP NP-hard?
- How to solve Rank SDP?

Reduction from $\mathcal{Q}$ to $\mathcal{P}$:

1. Pick $\mathcal{Q}$ NP-hard problem
2. I random instance of $\mathcal{Q}$ $\to$ (poly. time) J instance of $\mathcal{P}$
3. Oracle solves $\mathcal{P} \to$ solution t
4. Solution $t \to$ (poly. time) solution s of I from $\mathcal{Q}$

Hardness of Rank SDP

Rank SDP:
Given p.c. matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_R(e) \leq t$

3. **Open problem:** Hardness of Rank SDP
   - Is Rank SDP NP-hard?
   - How to solve Rank SDP?

Reduction from $\mathcal{Q}$ to $\mathcal{P}$:

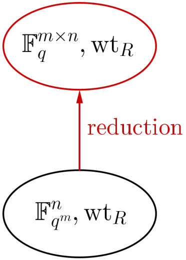
→ If we can solve $\mathcal{P}$
  → we can solve $\mathcal{Q}$

→ hardness $\mathcal{P} \geq$ hardness $\mathcal{Q}$

→ $\mathcal{P}$ is NP-hard

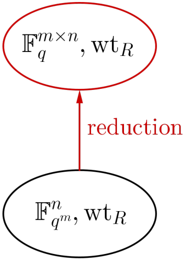
1. Pick $\mathcal{Q}$ NP-hard problem
2. I random instance of $\mathcal{Q}$
   → (poly. time) J instance of $\mathcal{P}$
3. Oracle solves $\mathcal{P}$ → solution t
4. Solution t → (poly. time)
   solution s of I from $\mathcal{Q}$

Connections to Other Problems



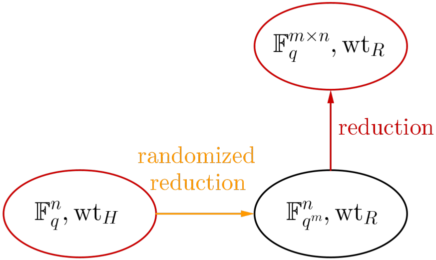
1. expand code $\mathcal{C}$ to $\mathbb{F}_q^{m\times n}$ via basis Γ → $d_R(\Gamma(\mathcal{C})) = d_R(\mathcal{C})$

Connections to Other Problems



1. expand code $\mathcal{C}$ to $\mathbb{F}_q^{m\times n}$ via basis Γ $\rightarrow$ $d_R(\Gamma(\mathcal{C})) = d_R(\mathcal{C})$ $\rightarrow$ hardness $(\mathbb{F}_q^{m\times n}, \mathrm{wt}_R) \geq (\mathbb{F}_{q^m}^n, \mathrm{wt}_R)$

Connections to Other Problems

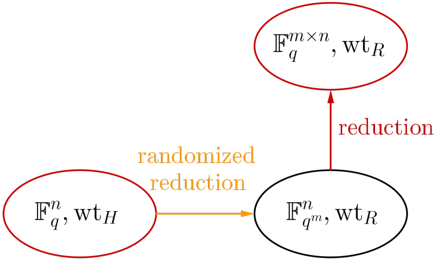


$\alpha \in \mathbb{F}_{q^m}^n$ lin. indep.

$\psi_\alpha : x \mapsto \alpha \star x$

2. $\mathrm{wt}_R(\psi_\alpha(x)) = \mathrm{wt}_H(x)$ $\rightarrow$ $d_R(\psi_\alpha(\mathcal{C})) \leq d_H(\mathcal{C})$

Connections to Other Problems

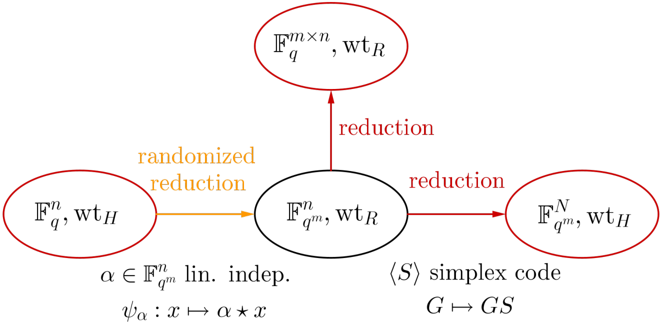


$\alpha \in \mathbb{F}_{q^m}^n$ lin. indep.

$\psi_\alpha : x \mapsto \alpha \star x$

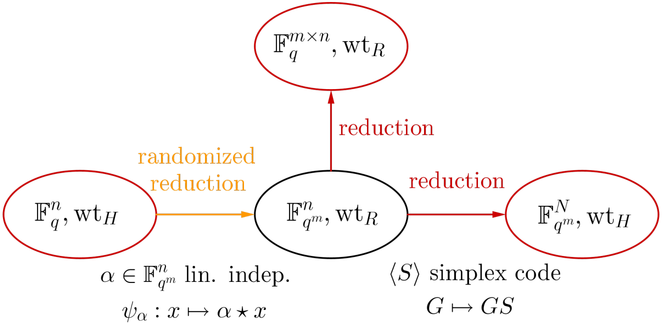
2. $\mathrm{wt}_R(\psi_\alpha(x)) = \mathrm{wt}_H(x)$ → $d_R(\psi_\alpha(\mathcal{C})) \leq d_H(\mathcal{C})$ → only w.h.p. equal

Connections to Other Problems



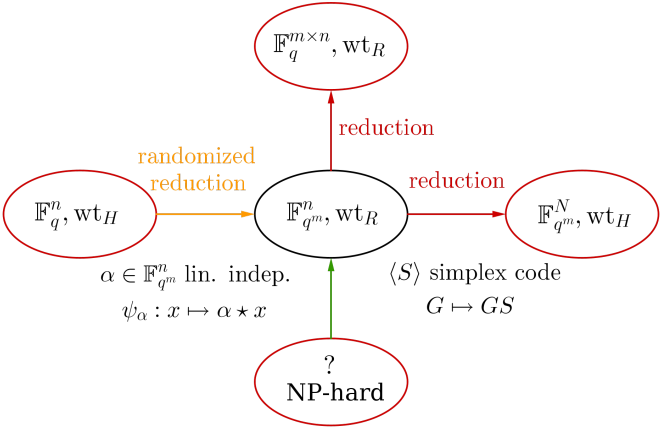
3. $S \in \mathbb{F}_q^{n\times N}$, $N = \frac{q^n-1}{q-1}$ $\quad\rightarrow\quad d_R(\langle G\rangle) = d_H(\langle GS\rangle)$

Connections to Other Problems



3. $S \in \mathbb{F}_q^{n\times N}$, $N = \frac{q^n-1}{q-1}$ → $d_R(\langle G\rangle) = d_H(\langle GS\rangle)$ → hardness $(\mathbb{F}_{q^m}^N, \mathrm{wt}_H) \geq (\mathbb{F}_{q^m}^n, \mathrm{wt}_R)$

Connections to Other Problems



→ new NP-hard problem to reduce from?

How to solve Rank SDP

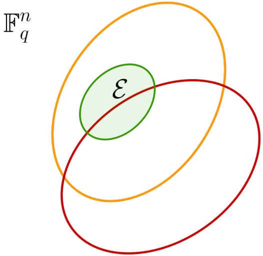
More costly than Hamming ISD? $\begin{bmatrix} n \\ t \end{bmatrix}_q > \binom{n}{t}$

How to solve Rank SDP

More costly than Hamming ISD? $\begin{bmatrix} n \\ t \end{bmatrix}_q > \binom{n}{t}$

Combinatorial solver:

- search for supersupport $\mathcal{F} \supset \mathcal{E}$ of dim. $n - k > t$ in $\mathbb{F}_q^n$
- $T = t/n$, $t = d/2$ from rank GV
- cost: $\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1} \sim q^{tk} = q^{n^2 RT}$

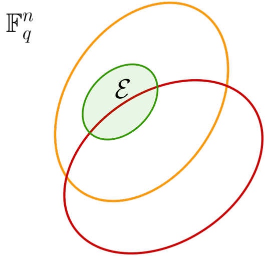


How to solve Rank SDP

More costly than Hamming ISD? $\begin{bmatrix} n \\ t \end{bmatrix}_q > \binom{n}{t}$ $q^{n^2 RT}$ vs. $2^{n0.05}$

Combinatorial solver:

- search for supersupport $\mathcal{F} \supset \mathcal{E}$ of dim. $n-k > t$ in $\mathbb{F}_q^n$
- $T = t/n$, $t = d/2$ from rank GV
- cost: $\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1} \sim q^{tk} = q^{n^2 RT}$



How to solve Rank SDP

More costly than Hamming ISD? $\begin{bmatrix} n \\ t \end{bmatrix}_q > \binom{n}{t}$ $q^{3T\log(n)^2}$ vs. $2^{n0.05}$

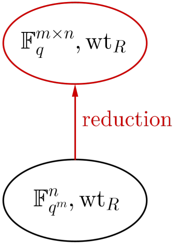
Combinatorial solver:

- search for supersupport $\mathcal{F} \supset \mathcal{E}$ of dim. $n-k > t$ in $\mathbb{F}_q^n$
- $T = t/n$, $t = d/2$ from rank GV
- cost: $\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1} \sim q^{tk} = q^{n^2RT}$

MinRank solver:

- if $t \sim \log(n)$, $T = t/\log(n)$
- cost: $\sim q^{3T\log(n)^2}$

→ not the case for random codes



How to solve Rank SDP

More costly than Hamming ISD? $\begin{bmatrix} n \\ t \end{bmatrix}_q > \binom{n}{t}$ $q^{3T\log(n)^2}$ vs. $2^{n0.05}$

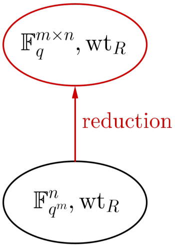
Combinatorial solver:

- search for supersupport $\mathcal{F} \supset \mathcal{E}$ of dim. $n-k > t$ in $\mathbb{F}_q^n$
- $T = t/n$, $t = d/2$ from rank GV
- cost: $\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1} \sim q^{tk} = q^{n^2 RT}$

MinRank solver:

- if $t \sim \log(n)$, $T = t/\log(n)$
- cost: $\sim q^{3T\log(n)^2}$

→ not the case for random codes



How to solve Rank SDP

More costly than Hamming ISD? $\begin{bmatrix} n \\ t \end{bmatrix}_q > \binom{n}{t}$

Combinatorial solver:

- search for supersupport $\mathcal{F} \supset \mathcal{E}$ of dim. $n-k > t$ in $\mathbb{F}_q^n$
- $T = t/n$, $t = d/2$ from rank GV
- cost: $\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1} \sim q^{tk} = q^{n^2 RT}$

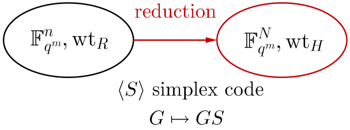
MinRank solver:

- if $t \sim \log(n)$, $T = t/\log(n)$
- cost: $\sim q^{3T \log(n)^2}$

→ not the case for random codes

Hamming ISD:

→ $q^{n^2 RT}$ optimal



Other solvers?

Code Equivalence

linear isometry: $\mathrm{wt}(x) = \mathrm{wt}(\varphi(x)) \ \forall x \to$ Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n \times \mathrm{Aut}(\mathbb{F}_q)$

code equivalence: $\mathcal{C} \sim \mathcal{C}'$ if exists lin. isometry φ: $\varphi(\mathcal{C}) = \mathcal{C}'$

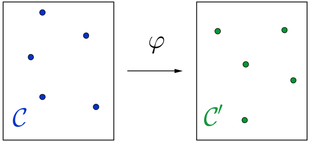
Code Equivalence

linear isometry: $\mathrm{wt}(x) = \mathrm{wt}(\varphi(x)) \ \forall x$ → Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n \times \mathrm{Aut}(\mathbb{F}_q)$

code equivalence: $\mathcal{C} \sim \mathcal{C}'$ if exists lin. isometry φ: $\varphi(\mathcal{C}) = \mathcal{C}'$

Linear Equivalence Problem (LEP)

Given $G, G' \in \mathbb{F}_q^{k \times n}$, find $\varphi \in (\mathbb{F}_q^\star)^n \rtimes S_n$
s.t. $\varphi(\langle G \rangle) = \langle G' \rangle$.



LEP

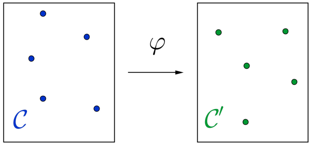
- LEP used in: LESS

Code Equivalence

linear isometry: $\mathrm{wt}(x) = \mathrm{wt}(\varphi(x))\ \forall x \to$ Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n \times \mathrm{Aut}(\mathbb{F}_q)$

code equivalence: $\mathcal{C} \sim \mathcal{C}'$ if exists lin. isometry φ: $\varphi(\mathcal{C}) = \mathcal{C}'$

Permutation Equivalence Problem (PEP)
Given $G, G' \in \mathbb{F}_q^{k \times n}$, find $\varphi \in S_n$
s.t. $\varphi(\langle G \rangle) = \langle G' \rangle$.



- LEP used in: LESS

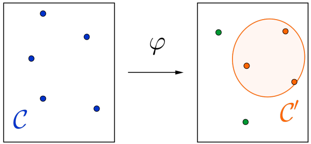
Code Equivalence

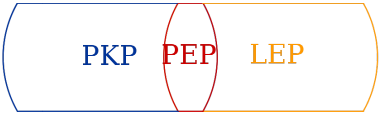
linear isometry: $\mathrm{wt}(x) = \mathrm{wt}(\varphi(x))\ \forall x \to$ Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n \times \mathrm{Aut}(\mathbb{F}_q)$

code equivalence: $\mathcal{C} \sim \mathcal{C}'$ if exists lin. isometry φ: $\varphi(\mathcal{C}) = \mathcal{C}'$

Permuted Kernel Problem (PKP)

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





- LEP used in: LESS

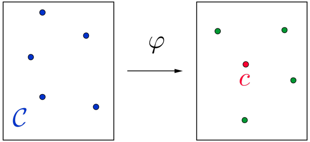
Code Equivalence

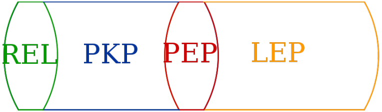
linear isometry: $\mathrm{wt}(x) = \mathrm{wt}(\varphi(x))\ \forall x$ → Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n \times \mathrm{Aut}(\mathbb{F}_q)$

code equivalence: $\mathcal{C} \sim \mathcal{C}'$ if exists lin. isometry φ: $\varphi(\mathcal{C}) = \mathcal{C}'$

Relaxed PKP

Given $G \in \mathbb{F}_q^{k \times n}$, $G' \in \mathbb{F}_q^{k' \times n}$, find $x \in \mathbb{F}_q^k$, perm. P s.t. $xGP \in \langle G' \rangle$.





- LEP used in: LESS
- rel. PKP used in: PERK

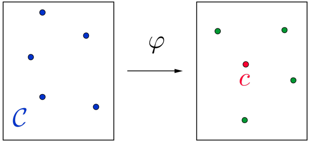
Code Equivalence

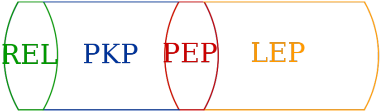
linear isometry: $\mathrm{wt}(x) = \mathrm{wt}(\varphi(x))\ \forall x \to$ Hamming metric: $(\mathbb{F}_q^\star)^n \rtimes S_n \times \mathrm{Aut}(\mathbb{F}_q)$

code equivalence: $\mathcal{C} \sim \mathcal{C}'$ if exists lin. isometry φ: $\varphi(\mathcal{C}) = \mathcal{C}'$

Relaxed PKP

Given $G \in \mathbb{F}_q^{k\times n}$, $G' \in \mathbb{F}_q^{k'\times n}$, find $x \in \mathbb{F}_q^k$, perm. P s.t. $xGP \in \langle G' \rangle$.





- LEP used in: LESS
- rel. PKP used in: PERK

4. Open problem: Hardness of Code Equivalence

- How hard is LEP/ relaxed PKP?
- How to solve LEP/ relaxed PKP?

Connections to Other Problems

Graph Isomorphism (GI)

Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \to V$, s.t. $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.

Connections to Other Problems

Graph Isomorphism (GI)

Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \to V$, s.t. $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.

- Hardness?

→ Assume quasi-polynomial (Babai)

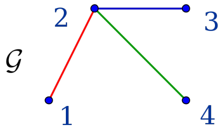
Connections to Other Problems

Graph Isomorphism (GI)

Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \to V$, s.t. $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.

- Hardness?

→ Assume quasi-polynomial (Babai)



$|E| = k$

$$D = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$G = [\mathrm{Id}_k \ \mathrm{Id}_k \ \mathrm{Id}_k \ D]$$

- sub-GI NP-hard

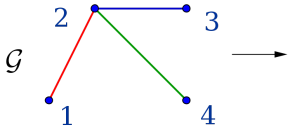
→ PKP NP-hard

→ hardness LEP ≥ PEP ≥ GI

Connections to Other Problems

Graph Isomorphism (GI)

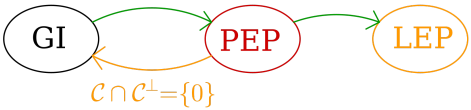
Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \to V$, s.t. $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.



$$D = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$|E| = k$

$G = [\mathrm{Id}_k \ \mathrm{Id}_k \ \mathrm{Id}_k \ D]$



→ hardness LEP ≥ PEP ≥ GI

→ random codes: PEP = GI

- Hardness?

→ Assume quasi-polynomial (Babai)

- sub-GI NP-hard

→ PKP NP-hard

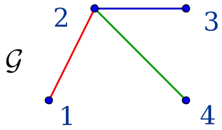
Connections to Other Problems

Graph Isomorphism (GI)

Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \to V$, s.t. $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.

- Hardness?

→ Assume quasi-polynomial (Babai)

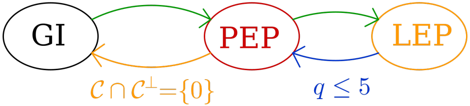


$$D = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$|E| = k$ $\qquad G = [\mathrm{Id}_k \ \mathrm{Id}_k \ \mathrm{Id}_k \ D]$

- sub-GI NP-hard

→ PKP NP-hard



→ hardness LEP ≥ PEP ≥ GI

→ random codes: PEP = GI

→ if $q \leq 5$ LEP = PEP

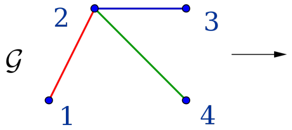
Connections to Other Problems

Graph Isomorphism (GI)

Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \to V$, s.t. $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.

- Hardness?

→ Assume quasi-polynomial (Babai)

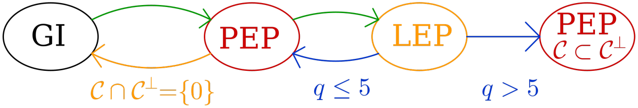


$$D = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$|E| = k$ $\qquad$ $G = [\mathrm{Id}_k \ \mathrm{Id}_k \ \mathrm{Id}_k \ D]$

- sub-GI NP-hard

→ PKP NP-hard



→ hardness LEP ≥ PEP ≥ GI $\qquad$ → random codes: PEP = GI $\qquad$ → if $q \leq 5$ LEP = PEP

How to solve Code Equivalence

- LEP $q \leq 5$ = PEP random codes $\rightarrow$ Babai's quasi-poly. algo. for GI

How to solve Code Equivalence

- LEP $q \leq 5$ = PEP random codes → Babai's quasi-poly. algo. for GI

- LEP $q > 5$ = PEP self orthogonal codes → invariant: weight distribution

How to solve Code Equivalence

- LEP $q \leq 5$ = PEP random codes → Babai's quasi-poly. algo. for GI

- LEP $q > 5$ = PEP self orthogonal codes → invariant: weight distribution

$\mathcal{C} \xrightarrow{\text{ISD}} c_1, \dots, c_N$ of wt $w > d \longrightarrow c_i = \{a, a, a, b, b, \dots, d\}$

$\mathcal{C}' \xrightarrow{\text{ISD}} c'_1, \dots, c'_N$ of wt $w > d \longrightarrow c'_i = \{a, a, a, b, b, \dots, d\}$

How to solve Code Equivalence

- LEP $q \leq 5$ = PEP random codes → Babai's quasi-poly. algo. for GI

- LEP $q > 5$ = PEP self orthogonal codes → invariant: weight distribution

$\mathcal{C}$ $\xrightarrow{\text{ISD}}$ $c_1, \ldots, c_N$ of wt $w > d$ $\longrightarrow$ $c_i = \{a, a, a, b, b, \ldots, d\}$

find permutation π $\updownarrow$

$\mathcal{C}'$ $\xrightarrow{\text{ISD}}$ $c'_1, \ldots, c'_N$ of wt $w > d$ $\longrightarrow$ $c'_i = \{a, a, a, b, b, \ldots, d\}$

How to solve Code Equivalence

- LEP $q \leq 5$ = PEP random codes → Babai's quasi-poly. algo. for GI

- LEP $q > 5$ = PEP self orthogonal codes → invariant: weight distribution

$\mathcal{C} \xrightarrow{\text{ISD}}$ $c_1, \dots, c_N$ of wt $w > d$ $\longrightarrow$ $c_i = \{a, a, a, b, b, \dots, d\}$

find permutation π $\updownarrow$

$\mathcal{C}' \xrightarrow{\text{ISD}}$ $c'_1, \dots, c'_N$ of wt $w > d$ $\longrightarrow$ $c'_i = \{a, a, a, b, b, \dots, d\}$

other solvers?

Questions?

Open Problems

1. Distinguish Goppa codes
2. Find code for Hash & Sign
3. Hardness of Rank SDP
4. Hardness of Code Equivalence

Questions?

Open Problems

1. Distinguish Goppa codes
2. Find code for Hash & Sign
3. Hardness of Rank SDP
4. Hardness of Code Equivalence

Announcement:

CBCrypto 2024

May 25-26 in Zurich

Questions?

Open Problems

1. Distinguish Goppa codes
2. Find code for Hash & Sign
3. Hardness of Rank SDP
4. Hardness of Code Equivalence

Announcement:

CBCrypto 2024

May 25-26 in Zurich

Slides

Thank you!