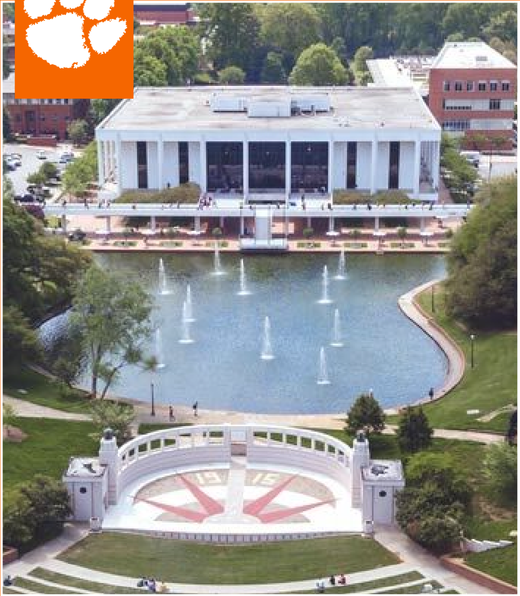


Code-based Cryptography: The Future of Security Against Quantum Threats

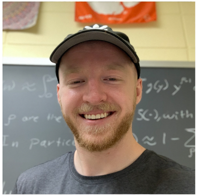
Felice Manganiello

Spring 2023 Section Meeting

April 29, 2023

Partially funded by
NSF DMS grant nr. 1547399

People Involved



Freeman Slaughter (Clemson University)

- Marco Baldi, Paolo Santini (Università Politecnica delle Marche)
- Alessandro Barenghi, Gerardo Pelosi (Politecnico di Milano)
- Sebastian Bitzer, Patrick Karl, Alessio Pavoni, Jonas Schupp, Antonia Wachter-Zeh, Violetta Weger (TUM)

Cryptography and Post-Quantum Cryptography

Coding Theory

Generic-Error Coding Theory

Zero-Knowledge Protocols

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.

- Authenticated pages (https)
- Digital signatures
- Zero-Knowledge protocols
- blockchain and cryptocurrencies
- etc.

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.

- Authenticated pages (https)
- Digital signatures
- Zero-Knowledge protocols
- blockchain and cryptocurrencies
- etc.

Number theory, commutative algebra, combinatorics, etc.

Cryptography Today

Problem **(Integer factorization - IF)**

Given a composite number N, find two integers a and b such that $ab = N$.

Easy: $N = 6$

Difficult: $N \approx 2^{2048} \approx 3.23 \cdot 10^{616}$

$\longrightarrow$ RSA cryptosystem (70's)

Cryptography Today

Problem (Integer factorization - IF)

Given a composite number N, find two integers a and b such that $ab = N$.

Easy: $N = 6$

Difficult: $N \approx 2^{2048} \approx 3.23 \cdot 10^{616}$

$\longrightarrow$ RSA cryptosystem (70's)

Problem (Discrete logarithm problem - DLP)

Given a cyclic group $G = \langle g \rangle$ and an element $a \in G$, find $e \in \mathbb{N}$ such that $a = g^e$.

Easy: $\mathbb{R}_{>0}$

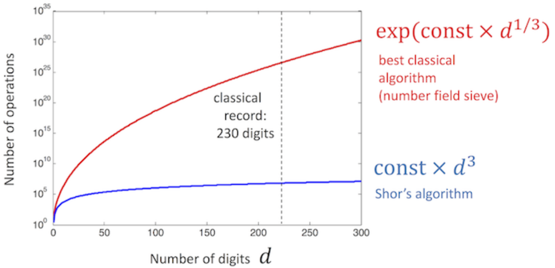
Difficult: $|G| \approx 2^{2048} \approx 3.23 \cdot 10^{616}$

$\longrightarrow$ Diffie-Hellman key exchange (70's)

Quantum computers and their threat

Theorem (Shor's Algorithm - '94)

There exists a polynomial-time quantum algorithm that breaks IF and DLP.



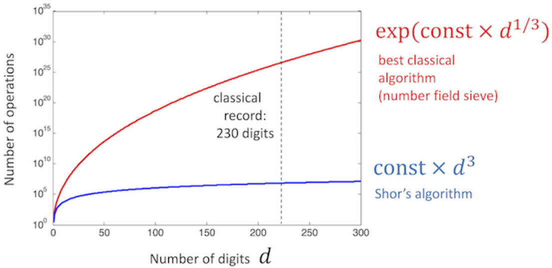
[1]

[1] image credit: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

Quantum computers and their threat

Theorem (Shor's Algorithm - '94)

There exists a polynomial-time quantum algorithm that breaks IF and DLP.



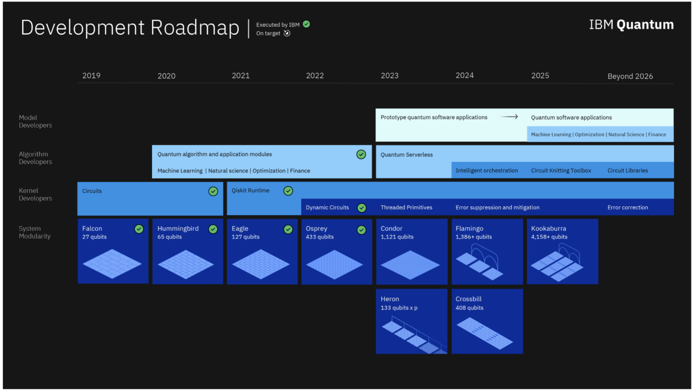
[1]

Remark

A full-scale quantum computer can break today's public key crypto!!

[1] image credit: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

Progress in quantum computing



[2]

Remark

Some experts predict 10-15 years, no one knows for sure.

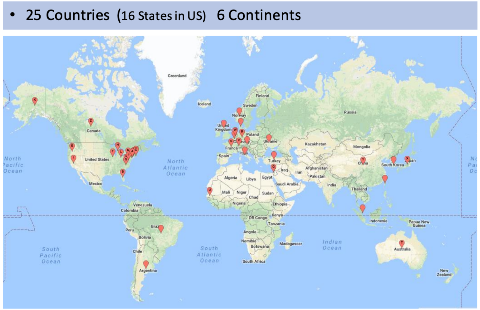
[2] image credit: https://www.ibm.com/quantum/roadmap

Post-quantum Cryptography and the NIST competition

Definition (Post-Quantum Cryptography (PQC))

Classical cryptographic algorithms which are secure against attacks by both classical and quantum computers.

- Dec 2, 2016: Call for proposal.
- Nov 30, 2017: Deadline
- 2018 - Round 1: 69 candidates
- 2019 - Round 2: 26 candidates
- 2020 - Round 3: 7 finalists and 8 alternates
- 2022 - NIST selects 4 finalists and 4 candidates



[a]

[a]image credit: NIST

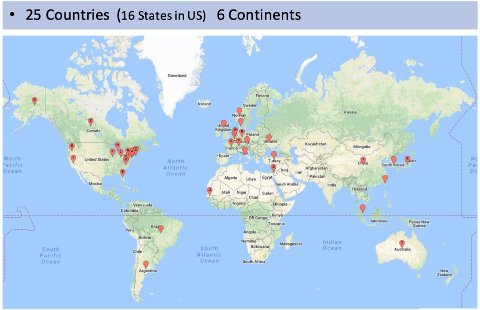
Post-quantum Cryptography and the NIST competition

Definition (Post-Quantum Cryptography (PQC))

Classical cryptographic algorithms which are secure against attacks by both classical and quantum computers.

- Dec 2, 2016: Call for proposal.
- Nov 30, 2017: Deadline
- 2018 - Round 1: 69 candidates
- 2019 - Round 2: 26 candidates
- 2020 - Round 3: 7 finalists and 8 alternates
- 2022 - NIST selects 4 finalists and 4 candidates

- NIST Call for Additional Digital Signatures



[a]

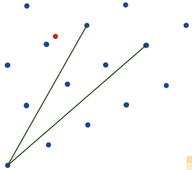
[a] image credit: NIST

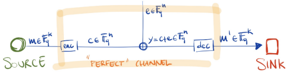
Goal: standards ready in about 1 year, complete compliance expected by 2035.

Post-Quantum Cryptography

Active research on:

- Lattice-based
- Code-based
- Multivariate
- Hash/Symmetric key-based signatures
- Isogeny-based



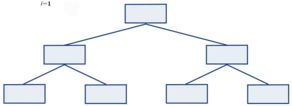


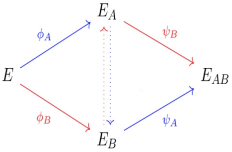
$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

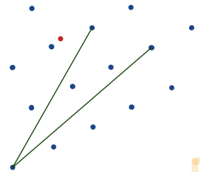


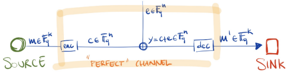


Post-Quantum Cryptography

Active research on:

- Lattice-based
- Code-based
- Multivariate
- Hash/Symmetric key-based signatures
- Isogeny-based



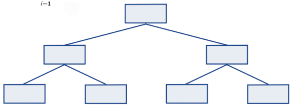


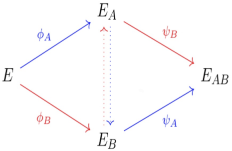
$$p^{(1)}(x_1,\dots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(1)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n}p_i^{(1)}\cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\dots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n}p_i^{(2)}\cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\dots,x_n)=\sum_{i=1}^{n}\sum_{j=i}^{n}p_{ij}^{(m)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n}p_i^{(m)}\cdot x_i + p_0^{(m)}$$





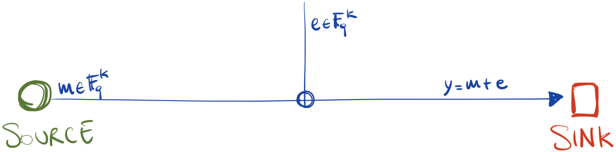
Cryptography and Post-Quantum Cryptography

Coding Theory

Generic-Error Coding Theory

Zero-Knowledge Protocols

Noisy-Channel Coding Theorem - Shannon 1948)



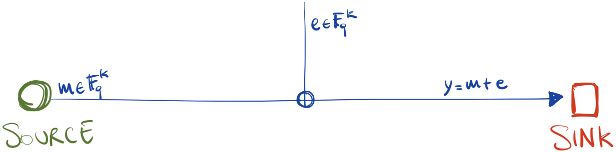
Over $\mathbb{F}_2$:

$m = 1$

$e = 1$

$y = 0$

Noisy-Channel Coding Theorem - Shannon 1948)



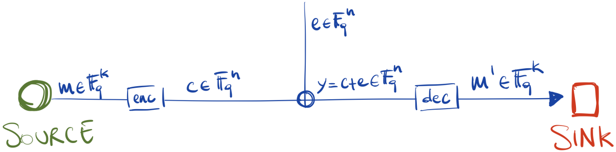
Over $\mathbb{F}_2$:
$m = 1$
$e = 1$
$y = 0$

Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

"In communication theory any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can, in principle, always be attained with an arbitrarily small probability of error."

Solved: Turbo codes (LTE networks), Polar & spatially-coupled LDPC codes (5G networks)

Noisy-Channel Coding Theorem - Shannon 1948)



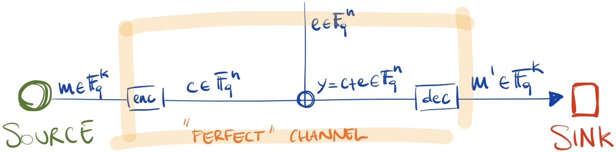
Over $\mathbb{F}_2$:
$m = 1$
$c = (111)$
$e = (010)$
$y = (101)$

Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

“In communication theory any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can, in principle, always be attained with an arbitrarily small probability of error."

Solved: Turbo codes (LTE networks), Polar & spatially-coupled LDPC codes (5G networks)

Noisy-Channel Coding Theorem - Shannon 1948)



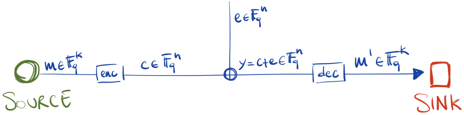
Over $\mathbb{F}_2$:
$m = 1$
$c = (111)$
$e = (010)$
$y = (101)$
$m' = 1$

Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

“In communication theory any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can, in principle, always be attained with an arbitrarily small probability of error."

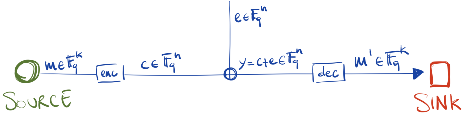
Solved: Turbo codes (LTE networks), Polar & spatially-coupled LDPC codes (5G networks)

Error-Correcting codes



- $\mathbb{F}_q^k$ message space.

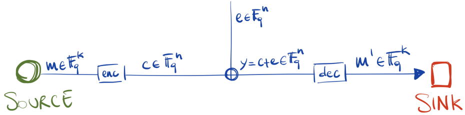
Error-Correcting codes



- $\mathbb{F}_q^k$ message space.
- $(\mathbb{F}_q^n, d_H)$ is a metric space with the Hamming distance

$$d_H(v, w) := wt(w - v) = |supp(w - v)| = \{i \in [n] \mid w_i \neq v_i\}.$$

Error-Correcting codes

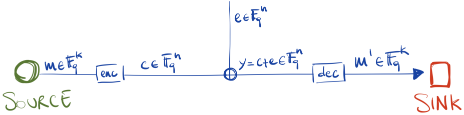


- $\mathbb{F}_q^k$ message space.
- $(\mathbb{F}_q^n, d_H)$ is a metric space with the Hamming distance

$$d_H(v, w) := wt(w - v) = |supp(w - v)| = \{i \in [n] \mid w_i \neq v_i\}.$$

- enc : $\mathbb{F}_q^k \to \mathbb{F}_q^n$ injective linear map.

Error-Correcting codes



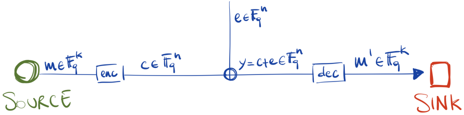
- $\mathbb{F}_q^k$ message space.
- $(\mathbb{F}_q^n, d_H)$ is a metric space with the Hamming distance

$$d_H(v,w) := wt(w-v) = |supp(w-v)| = \{i \in [n] \mid w_i \neq v_i\}.$$

- enc : $\mathbb{F}_q^k \to \mathbb{F}_q^n$ injective linear map.
- $\mathcal{C} :=$ enc$(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$ is a $[n,k,d]_q$ linear code if it is a k-dimensional vector space and

$$d(\mathcal{C}) = \min_{c_1,c_2 \in \mathcal{C},\ c_1 \neq c_2} d_H(c_1,c_2).$$

Error-Correcting codes



- $\mathbb{F}_q^k$ message space.
- $(\mathbb{F}_q^n, d_H)$ is a metric space with the Hamming distance

$$d_H(v,w) := wt(w-v) = |supp(w-v)| = \{i \in [n] \mid w_i \neq v_i\}.$$

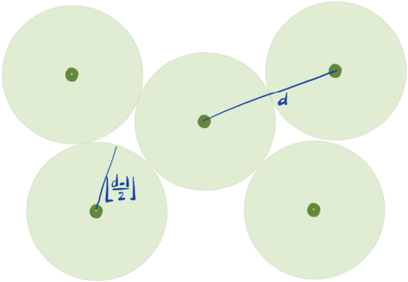
- $\mathrm{enc} : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$ injective linear map.
- $\mathcal{C} := \mathrm{enc}(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$ is a $[n,k,d]_q$ linear code if it is a k-dimensional vector space and

$$d(\mathcal{C}) = \min_{c_1,c_2 \in \mathcal{C},\ c_1 \neq c_2} d_H(c_1,c_2).$$

- $c = (c_1,\ldots,c_n) \in \mathcal{C}$ is a codeword.

Error-Correcting codes (cont'd)

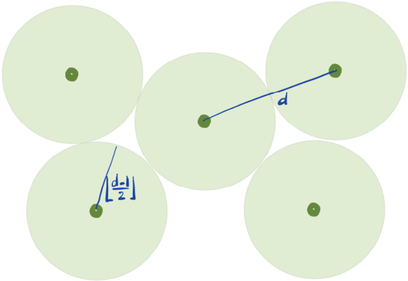
Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code with minimum distance d.



$$\begin{aligned} \pi : \mathbb{F}_q^n &\longrightarrow \mathcal{C} \\ y &\longmapsto \operatorname{argmin}\{d(y,c) \mid c \in \mathcal{C}\} \end{aligned}$$

Error-Correcting codes (cont'd)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code with minimum distance d.

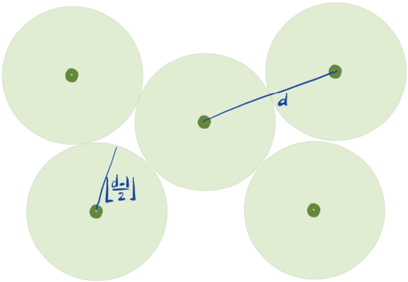


$$\pi : \mathbb{F}_q^n \longrightarrow \mathcal{C}$$
$$y \longmapsto \operatorname{argmin}\{d(y, c) \mid c \in \mathcal{C}\}$$

$$\mathrm{dec} := \mathrm{enc}^{-1} \circ \pi$$

Error-Correcting codes (cont'd)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code with minimum distance d.



$$\pi : \mathbb{F}_q^n \to \mathcal{C}$$
$$y \mapsto \operatorname{argmin}\{d(y,c) \mid c \in \mathcal{C}\}$$

$$\mathrm{dec} := \mathrm{enc}^{-1} \circ \pi$$

dec is able to uniquely correct at least $\lfloor \frac{d-1}{2} \rfloor$ errors

Error-Correcting codes (cont'd)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code.

- A generator matrix $G \in \mathbb{F}_q^{k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that

$$\mathcal{C} = \mathrm{im}(G) = \{mG \mid m \in \mathbb{F}_q^k\}.$$

Error-Correcting codes (cont'd)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code.

- A generator matrix $G \in \mathbb{F}_q^{k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that

$$\mathcal{C} = \text{im}(G) = \{mG \mid m \in \mathbb{F}_q^k\}.$$

- A parity check matrix $H \in \mathbb{F}_q^{n-k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that $\mathcal{C} = \ker(H^t)$.

Error-Correcting codes (cont'd)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code.

- A generator matrix $G \in \mathbb{F}_q^{k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that

$$\mathcal{C} = \mathrm{im}(G) = \{mG \mid m \in \mathbb{F}_q^k\}.$$

- A parity check matrix $H \in \mathbb{F}_q^{n-k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that $\mathcal{C} = \ker(H^t)$.

- It holds that

$$GH^t = 0.$$

Error-Correcting codes (cont'd)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code.

- A generator matrix $G \in \mathbb{F}_q^{k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that

$$\mathcal{C} = \mathrm{im}(G) = \{mG \mid m \in \mathbb{F}_q^k\}.$$

- A parity check matrix $H \in \mathbb{F}_q^{n-k \times n}$ for $\mathcal{C}$ is a fullrank matrix such that $\mathcal{C} = \ker(H^t)$.

- It holds that

$$GH^t = 0.$$

- Syndrome of $y \in \mathbb{F}_q^n$ is $s_y := yH^t \in \mathbb{F}_q^{n-k}$.

Example: repetition code

- $\mathbb{F}_2$ message space
- $\mathsf{enc} : \mathbb{F}_2 \to \mathbb{F}_2^3$ such that

$$\mathsf{enc}(0) = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathsf{enc}(1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

Example: repetition code

- $\mathbb{F}_2$ message space

- $\mathsf{enc} : \mathbb{F}_2 \to \mathbb{F}_2^3$ such that

$$\mathsf{enc}(0) = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathsf{enc}(1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

- $\mathcal{C}$ is a $[3, 1, 3]$ linear code that corrects 1 error.

Example: repetition code

- $\mathbb{F}_2$ message space
- $\mathsf{enc} : \mathbb{F}_2 \to \mathbb{F}_2^3$ such that

$$\mathsf{enc}(0) = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathsf{enc}(1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

- $\mathcal{C}$ is a $[3, 1, 3]$ linear code that corrects 1 error.
- $G := \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$ and $H := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

The Syndrome Decoding Problem

Problem

For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, a syndrome $s \in \mathbb{F}_q^{n-k}$, and some $t \in \mathbb{N}$, find a vector $e \in \mathbb{F}_q^n$ such that $eH^t = s$ and $wt(e) = t$.

Theorem (Berlekamp et al. 1978, and Barg 1997)

This problem is NP-complete.

Cryptography and Post-Quantum Cryptography

Coding Theory

Generic-Error Coding Theory

Zero-Knowledge Protocols

Difference Sets

Let $\mathbb{F}_q$ be the field with q elements, with $q = p^N$ a prime power.

Difference Sets

Let $\mathbb{F}_q$ be the field with q elements, with $q = p^N$ a prime power.

For a k-element set $E \subseteq \mathbb{F}_q^n$, let $\langle E \rangle_{\mathbb{F}_p}$ be the span of E over $\mathbb{F}_p$:

$$\langle E \rangle_{\mathbb{F}_p} = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_k e_k \text{ for } \lambda_i \in \mathbb{F}_p, e_i \in E.$$

Difference Sets

Let $\mathbb{F}_q$ be the field with q elements, with $q = p^N$ a prime power.

For a k-element set $E \subseteq \mathbb{F}_q^n$, let $\langle E \rangle_{\mathbb{F}_p}$ be the span of E over $\mathbb{F}_p$:

$$\langle E \rangle_{\mathbb{F}_p} = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_k e_k \text{ for } \lambda_i \in \mathbb{F}_p, e_i \in E.$$

For any set E, the set difference of E is

$$\Delta E = \{e_1 - e_2 \mid e_1, e_2 \in E\}.$$

Difference Sets

Let $\mathbb{F}_q$ be the field with q elements, with $q = p^N$ a prime power.

For a k-element set $E \subseteq \mathbb{F}_q^n$, let $\langle E \rangle_{\mathbb{F}_p}$ be the span of E over $\mathbb{F}_p$:

$$\langle E \rangle_{\mathbb{F}_p} = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_k e_k \text{ for } \lambda_i \in \mathbb{F}_p, e_i \in E.$$

For any set E, the set difference of E is

$$\Delta E = \{e_1 - e_2 \mid e_1, e_2 \in E\}.$$

Theorem (M.,Slaugther 2023)

For a set $E \subseteq \mathbb{F}_q^n$, the chain $E \subseteq \Delta E \subseteq \Delta^2 E \subseteq \ldots$ stabilizes. That is, there exists some $k \in \mathbb{N}$ such that $\Delta^k E = \Delta^{k+1} E$. In this case, $\Delta^k E = \langle E \rangle_{\mathbb{F}_p}$.

Difference Sets

Let $\mathbb{F}_q$ be the field with q elements, with $q = p^N$ a prime power.

For a k-element set $E \subseteq \mathbb{F}_q^n$, let $\langle E \rangle_{\mathbb{F}_p}$ be the span of E over $\mathbb{F}_p$:

$$\langle E \rangle_{\mathbb{F}_p} = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_k e_k \text{ for } \lambda_i \in \mathbb{F}_p, e_i \in E.$$

For any set E, the set difference of E is

$$\Delta E = \{e_1 - e_2 \mid e_1, e_2 \in E\}.$$

Theorem (M.,Slaugther 2023)

For a set $E \subseteq \mathbb{F}_q^n$, the chain $E \subseteq \Delta E \subseteq \Delta^2 E \subseteq \ldots$ stabilizes. That is, there exists some $k \in \mathbb{N}$ such that $\Delta^k E = \Delta^{k+1} E$. In this case, $\Delta^k E = \langle E \rangle_{\mathbb{F}_p}$.

Definition

For a set E, the Δ-closure of E is $\overline{E}^{\Delta} = \lim_{k \to \infty} \Delta^k E$. We say that E is Δ-closed if $E = \overline{E}^{\Delta}$.

Generic Error Sets

Definition

An error set $E \subseteq \mathbb{F}_q^n$ is detectable by some code $\mathcal{C} \subseteq \mathbb{F}_q^n$ if $E \cap \mathcal{C} = \{0\}$. Similarly, this set of errors E is correctable by $\mathcal{C}$ if $\Delta E \cap \mathcal{C} = \{0\}$.

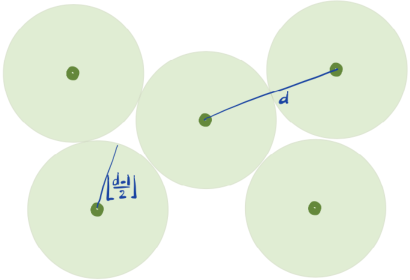
Generic Error Sets

Definition

An error set $E \subseteq \mathbb{F}_q^n$ is detectable by some code $\mathcal{C} \subseteq \mathbb{F}_q^n$ if $E \cap \mathcal{C} = \{0\}$. Similarly, this set of errors E is correctable by $\mathcal{C}$ if $\Delta E \cap \mathcal{C} = \{0\}$.

Example

In the case of Hamming balls, $\Delta B_t(0) \subseteq B_{d-1}(0)$, where $t = \lfloor \frac{d-1}{2} \rfloor$. This means that any error detectable under the set difference definition is also detectable under the minimum distance of a code.



Detection and Correction

It follows that Δ-closed sets are maximal sets for which detectability corresponds to correctability.

It follows that Δ-closed sets are maximal sets for which detectability corresponds to correctability.

Corollary

Given a code , a set E is detectable and correctable if and only if E is Δ-closed, meaning that $\overline{E}^{\Delta} = E$.

Detection and Correction

It follows that Δ-closed sets are maximal sets for which detectability corresponds to correctability.

Corollary

Given a code , a set E is detectable and correctable if and only if E is Δ-closed, meaning that $\overline{E}^{\Delta} = E$.

Proposition

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code with parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$. The set $E \subseteq \mathbb{F}_q^n$ is correctable by $\mathcal{C}$ if and only if its syndromes are unique, meaning that for $e, e' \in E$,

$$eH^t = e'H^t \iff e = e'.$$

Gilbert-Varshamov Bound

Theorem (M., Slaughter 2023)

There exists a code $\mathcal{C}$ correcting E once

$$|\Delta E| < q^{n-k}.$$

Gilbert-Varshamov Bound

Theorem (M., Slaughter 2023)

There exists a code $\mathcal{C}$ correcting E once

$$|\Delta E| < q^{n-k}.$$

This recovers the standard Gilbert-Varshamov bound by taking $E \subseteq B_t(0)$:

Theorem (Gilbert-Varshamov Bound)

Let n, k, and d be such that

$$\sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i < q^{n-k}.$$

Then there exists $\mathcal{C}$ an $[n, k]$ code $\mathcal{C}$ of minimum distance d.

GE-SDP

Problem (SDP)

For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, a syndrome $s \in \mathbb{F}_q^{n-k}$, and some $t \in \mathbb{N}$, find a vector $e \in \mathbb{F}_q^n$ such that $eH^t = s$ and $wt(e) = t$.

GE-SDP

Problem (SDP)

For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, a syndrome $s \in \mathbb{F}_q^{n-k}$, and some $t \in \mathbb{N}$, find a vector $e \in \mathbb{F}_q^n$ such that $eH^t = s$ and $wt(e) = t$.

Problem (GE-SDP)

For an $[n, k]$ code $\mathcal{C}$ with parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, a syndrome $s \in \mathbb{F}_q^{n-k}$, and some set $E \subseteq \mathbb{F}_q^n$, find a vector $e \in E$ such that $eH^t = s$.

Proposition (M., Slaughter 2023)

The GE-SDP is NP-complete.

Complexity of already known SPDs

SDP

$E = B_t(0)$

NP-complete[a]

[a] Berlekamp *et al.* 1978, and Barg 1997

Restricted SDP

$E = \{0, \pm 1\}^n$

NP-complete[a]

[a] Baldi *et al.* 2020

Rank SDP

$E = B_t^R(0)$

?

R-SDP(G)

$E = G^n$

NP-complete[a]

[a] Baldi *et al.* 2023

Complexity of already known SPDs

SDP
$E = B_t(0)$
NP-complete[a]

[a] Berlekamp *et al.* 1978, and Barg 1997

Restricted SDP
$E = \{0, \pm 1\}^n$
NP-complete[a]

[a] Baldi *et al.* 2020

Rank SDP
$E = B_t^R(0)$
?

R-SDP(G)
$E = G^n$
NP-complete[a]

[a] Baldi *et al.* 2023

Theorem (M., Slaughter 2023)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code and $E \subseteq \mathbb{F}_q^n$ an error set such that $\overline{E}^\Delta \cap \mathcal{C} = \{0\}$. Then the GE-SDP can be solved in $\mathcal{O}(n^3)$.

If $E = \{0, \pm 1\}^n$, then $\overline{E}^\Delta = \mathbb{F}_p^n$. In this case,

$$\frac{k}{n} \leq \frac{N-1}{N},$$

meaning that the SDP might be easy for code with low rates.

Cryptography and Post-Quantum Cryptography

Coding Theory

Generic-Error Coding Theory

Zero-Knowledge Protocols

Zero-Knowledge Protocols (ZKP)

A ZKP is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.

A zero-knowledge proof must satisfy three properties:

- *Completeness*: an honest prover can convince a verifier.
- Soundness: a cheating prover can convince a verifier with a probability less than 1.
- Zero-Knowledge: the verifier learns nothing other than the statement's veracity.

Zero-knowledge protocol (ZKP) based on DLP

Private: $x \in \mathbb{N}$

Public: g such that $\mathbb{F}_p^* = \langle g \rangle$, and $y = g^x$

Prover

Verifier

Zero-knowledge protocol (ZKP) based on DLP

Private: $x \in \mathbb{N}$ — Public: g such that $\mathbb{F}_p^* = \langle g \rangle$, and $y = g^x$

Prover		**Verifier**
Create $x = x_1 + \cdots + x_n \pmod{p-1}$		
Compute $y_i = g^{x_i}$ for all i		
$(y_1, \ldots, y_n)$	$\longrightarrow$	

Zero-knowledge protocol (ZKP) based on DLP

Private: $x \in \mathbb{N}$ Public: g such that $\mathbb{F}_p^* = \langle g \rangle$, and $y = g^x$

Prover		**Verifier**
Create $x = x_1 + \cdots + x_n \pmod{p-1}$		
Compute $y_i = g^{x_i}$ for all i		
$(y_1, \ldots, y_n)$	$\longrightarrow$	
	$\longleftarrow$	$j \in \{1, \ldots, n\}$

Zero-knowledge protocol (ZKP) based on DLP

Private: $x \in \mathbb{N}$ | Public: g such that $\mathbb{F}_p^* = \langle g \rangle$, and $y = g^x$

Prover		**Verifier**
Create $x = x_1 + \cdots + x_n \pmod{p-1}$		
Compute $y_i = g^{x_i}$ for all i		
$(y_1, \ldots, y_n)$	$\longrightarrow$	
	$\longleftarrow$	$j \in \{1, \ldots, n\}$
$(x_1, \ldots, x_n)$ except for j	$\longrightarrow$	

Zero-knowledge protocol (ZKP) based on DLP

Private: $x \in \mathbb{N}$

Public: g such that $\mathbb{F}_p^* = \langle g \rangle$, and $y = g^x$

Prover		Verifier
Create $x = x_1 + \cdots + x_n \pmod{p-1}$		
Compute $y_i = g^{x_i}$ for all i		
$(y_1, \ldots, y_n)$	$\longrightarrow$	
	$\longleftarrow$	$j \in \{1, \ldots, n\}$
$(x_1, \ldots, x_n)$ except for j	$\longrightarrow$	
		Checks $y_i = g^{x_i}$ for $i \neq j$ and $\prod_{i=1}^{n} y_i = y$

Zero-knowledge protocol (ZKP) based on DLP

Private: $x \in \mathbb{N}$

Public: g such that $\mathbb{F}_p^* = \langle g \rangle$, and $y = g^x$

Prover

Create $x = x_1 + \cdots + x_n \pmod{p-1}$

Compute $y_i = g^{x_i}$ for all i

$(y_1, \ldots, y_n)$ $\longrightarrow$

Verifier

$\longleftarrow$ $j \in \{1, \ldots, n\}$

$(x_1, \ldots, x_n)$ except for j $\longrightarrow$

Checks $y_i = g^{x_i}$ for $i \neq j$ and $\prod_{i=1}^{n} y_i = y$

Figure: Prover - Jess

Figure: Verifier - Felice

GE-CVE - a ZKP based on GE-SDP (M., Slaughter 2023)

[3]

Public data: $q, n, k \in \mathbb{N}, E \subset \mathbb{F}_q^n, H \in \mathbb{F}_q^{(n-k)\times n}$

Private Key: $e \in E$

Public Key: $s = eH^t \in \mathbb{F}_q^{n-k}$

PROVER		VERIFIER
$u \xleftarrow{\$} \mathbb{F}_q^n,\ M \xleftarrow{\$} \mathfrak{S}_E$		
Set $c_0 = \text{Hash}(M, uH^t)$		
Set $c_1 = \text{Hash}(uM, eM)$	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{z}$	$z \xleftarrow{\$} \mathbb{F}_q^*$
Set $y = (u + ze)M$	$\xrightarrow{y}$	
	$\xleftarrow{b}$	Choose $b \in \{0, 1\}$
If $b = 0,$ set $f := M$		
If $b = 1,$ set $f := eM$	$\xrightarrow{f}$	
		If $b = 0,$ accept if $c_0 = \text{Hash}(f, (yf^{-1})H^t - zs)$. If $b = 1,$ accept if $f \in E$ and $c_1 = \text{Hash}(y - zf, f)$.

[3] Adaptation of CVE by Cayrel, Veron, El Yousfi Alaoui 2010

GE-CVE - a ZKP based on GE-SDP (M., Slaughter 2023)

This is genuinely a zero-knowledge identification scheme:

- Completeness: an honest prover can convince a verifier.
- Soundness: a cheating prover can convince a verifier with only a small probability $\left(\frac{q}{2(q-1)}\right)$.
- Zero-Knowledge: the verifier learns nothing other than the statement's veracity.

Future for GE-SDP

We plan on submitting on June 1, 2023 a digital signature scheme based on R-SDP(G)

Universities involved:

- Clemson University
- Università Politecnica delle Marche
- Politecnico di Milano
- Technical University of Munich

Future for GE-SDP

We plan on submitting on June 1, 2023 a digital signature scheme based on R-SDP(G)

Universities involved:

- Clemson University
- Università Politecnica delle Marche
- Politecnico di Milano
- Technical University of Munich

Thank you.