Reproducible Codes and Cryptographic Applications

Edoardo Persichetti

(Joint work with Paolo Santini and Marco Baldi, Università Politecnica delle Marche)

14 August 2019

FAU
Charles E. Schmidt College of Science
Florida Atlantic University

In This Talk

- Motivation
- Preliminaries
- Sparse-matrix Codes
- Reproducibility
- Codes in Reproducible Form
- Defeating Attacks and Explicit Constructions

Part I

Motivation

Post-Quantum Cryptography

In a few years time large-scale quantum computers might be reality.
But then (Shor, '95):

- RSA
- DSA
- ECC
- Diffie-Hellman key exchange
- and many others ... **not secure** !

$\rightarrow$ NIST's Post-Quantum Cryptography Standardization Call

Main areas of research:

- Lattice-based cryptography.
- Hash-based cryptography.
- Code-based cryptography (McEliece, Niederreiter).
- Multivariate cryptography.
- Isogeny-based cryptography.

Structured Codes

Structured codes are a very promising research direction for code-based cryptography.

The major reduction in public-key size is very appealing, however...

...introducing additional algebraic structure may compromise security.

Structured Codes

Structured codes are a very promising research direction for code-based cryptography.

The major reduction in public-key size is very appealing, however...

...introducing additional algebraic structure may compromise security.

Sparse-matrix codes (LDPC/MDPC) do not possess algebraic properties and are not affected by structure (e.g. QC).

Structured Codes

Structured codes are a very promising research direction for code-based cryptography.

The major reduction in public-key size is very appealing, however...

...introducing additional algebraic structure may compromise security.

Sparse-matrix codes (LDPC/MDPC) do not possess algebraic properties and are not affected by structure (e.g. QC).

Is there any other structure we can use? Can we generalize this, do it better/differently?

(We have a pretty strong hint about this).

A. Shamir, personal communication.

Part II

PRELIMINARIES

Error-Correcting Codes

$[n, k]$ linear code over $\mathbb{F}_q$

A subspace of dimension k of $\mathbb{F}_q^n$.
ω-error correcting: exists decoding algorithm that corrects up to ω errors occurred on a codeword.

Error-Correcting Codes

$[n, k]$ linear code over $\mathbb{F}_q$

A subspace of dimension k of $\mathbb{F}_q^n$.
ω-error correcting: exists decoding algorithm that corrects up to ω errors occurred on a codeword.

Hamming weight

Number of non-zero entries: $wt(x) = |\{i : x_i \neq 0, 1 \leq i \leq n\}|$.

Generator matrix

$G \in \mathbb{F}_q^{k \times n}$ defines the code as follows: $x \in \mathcal{C} \iff x = \mu G$.
Systematic form: $(I_k | M)$.

Error-Correcting Codes

$[n, k]$ linear code over $\mathbb{F}_q$

A subspace of dimension k of $\mathbb{F}_q^n$.
ω-error correcting: exists decoding algorithm that corrects up to ω errors occurred on a codeword.

Hamming weight

Number of non-zero entries: $wt(x) = |\{i : x_i \neq 0, 1 \leq i \leq n\}|$.

Generator matrix

$G \in \mathbb{F}_q^{k \times n}$ defines the code as follows: $x \in \mathcal{C} \iff x = \mu G$.
Systematic form: $(I_k | M)$.

Parity-check matrix

$H \in \mathbb{F}_q^{(n-k) \times n}$ defines the code as follows: $x \in \mathcal{C} \iff Hx^T = 0$.
Systematic form: $(-M^T | I_{n-k})$.

Code-based PKE Schemes

McEliece: first cryptosystem using error correcting codes (1978).

Based on the hardness of decoding random linear codes.

KeyGen chooses random error-correcting code from chosen family[1].

Generator matrix G is scrambled to form public key (e.g. *SGP*).

Plaintext is encrypted as noisy codeword.

Decryption uses private key i.e. input to decoding algorithm.

Simple description and very fast encryption algorithm.

No known vulnerabilities against quantum computers[2].

Drawback: relatively large keys.

[1] Binary Goppa codes in original proposal.

[2] Speedup results in half security exponent.

McEliece PKE (Modern)

Key Generation

- Choose ω-error correcting code $\mathcal{C}$.
- SK: code description Δ for $\mathcal{C}$.
- PK: generator matrix G in systematic form for $\mathcal{C}$.

Encryption

- Message is a word $\mu \in \mathbb{F}_2^k$.
- Select random error vector $e \in \mathbb{F}_2^n$ of weight ω.
- $c = \mu G + e$.

Decryption

- Set $\mu = Decode_\Delta(c)$ and return μ.
- Return $\perp$ if decoding fails.

NIEDERREITER

"Dual" version proposed by Niederreiter (1985).

Based on well-known Syndrome Decoding Problem (SDP).

Niederreiter

"Dual" version proposed by Niederreiter (1985).

Based on well-known Syndrome Decoding Problem (SDP).

Proved to be NP-complete (Berlekamp, McEliece and van Tilborg, 1978).

Problem 1 (Computational Syndrome Decoding)

Given: $H \in \mathbb{F}_q^{(n-k)\times n}$, $y \in \mathbb{F}_q^{(n-k)}$ and $\omega \in \mathbb{N}$.
Goal: find a word $e \in \mathbb{F}_q^n$ with $wt(e) \leq \omega$ such that $He^T = y$.

Unique solution only if w is below a certain threshold (GV bound).

Niederreiter

"Dual" version proposed by Niederreiter (1985).

Based on well-known Syndrome Decoding Problem (SDP).

Proved to be NP-complete (Berlekamp, McEliece and van Tilborg, 1978).

Problem 1 (Computational Syndrome Decoding)

Given: $H \in \mathbb{F}_q^{(n-k)\times n}$, $y \in \mathbb{F}_q^{(n-k)}$ *and* $\omega \in \mathbb{N}$.
Goal: find a word $e \in \mathbb{F}_q^n$ *with* $wt(e) \leq \omega$ *such that* $He^T = y$.

Unique solution only if w is below a certain threshold (GV bound).

Easy to show that this problem is equivalent to decoding random linear codes.

Unlike McEliece, Niederreiter's scheme is deterministic.

Niederreiter PKE (Modern)

Key Generation

- Choose ω-error correcting code $\mathcal{C}$.
- SK: code description Δ for $\mathcal{C}$.
- PK: parity-check matrix H in systematic form for $\mathcal{C}$.

Encryption

- Message is a word $e \in \mathbb{F}_2^n$ of weight ω.
- $c = He^T$.

Decryption

- Set $e = Decode_\Delta(c)$ and return e.
- Return $\perp$ if decoding fails.

Structured Codes

Idea: public matrix with compact description (Gaborit '05).

Quasi-Cyclic Codes (Berger, Cayrel, Gaborit, Otmani '09).

Structured Codes

Idea: public matrix with compact description (Gaborit '05).

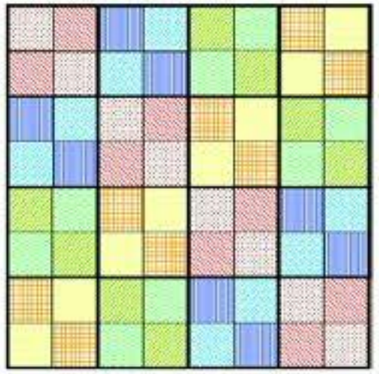
Quasi-Cyclic Codes (Berger, Cayrel, Gaborit, Otmani '09).

Matrices formed by circulant blocks

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-1} \\ a_{p-1} & a_0 & \dots & a_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}$$

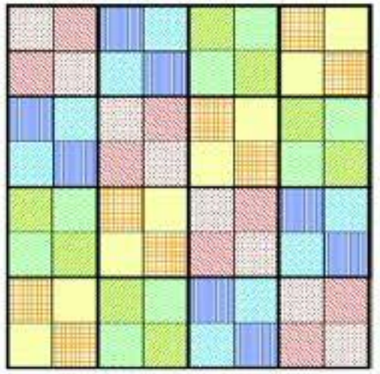
Structured Codes (cont.)

Quasi-Dyadic Codes (Misoczki, Barreto '09).



Structured Codes (cont.)

Quasi-Dyadic Codes (Misoczki, Barreto '09).



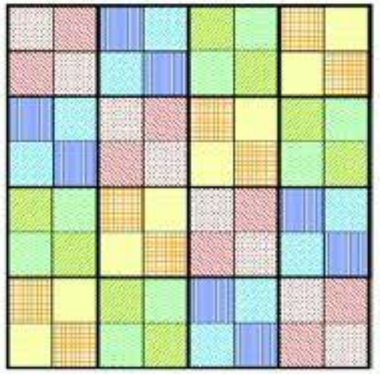
Several families admit QC/QD description:
GRS, Goppa, Generalized Srivastava (P. '11).

Problem: extra structure = extra info for attacker.

Critical algebraic attack (Faugère, Otmani, Perret, Tillich '10).

Structured Codes (cont.)

Quasi-Dyadic Codes (Misoczki, Barreto '09).



Several families admit QC/QD description:
GRS, Goppa, Generalized Srivastava (P. '11).

Problem: extra structure = extra info for attacker.

Critical algebraic attack (Faugère, Otmani, Perret, Tillich '10).

After a few years of fixes and new attacks: keys getting bigger, confidence getting smaller.

Part III

Sparse-matrix Codes

Sparse-matrix Codes

Family of codes characterized by very sparse parity-check matrix.

Definition 1 (LDPC Code)

An $[n, k]$ binary linear code which admits a parity-check matrix of constant row weight $w \in O(1)$.

If we write $H = (H_0 \mid H_1)$ resp. $r \times k$ and $r \times r$ then $G = (I_k \mid H_0^T H_1^{-T})$.

The non-trivial block is dense, so this is a natural choice of public key for McEliece.

Sparse-matrix Codes

Family of codes characterized by very sparse parity-check matrix.

Definition 1 (LDPC Code)

An $[n, k]$ binary linear code which admits a parity-check matrix of constant row weight $w \in O(1)$.

If we write $H = (H_0 \mid H_1)$ resp. $r \times k$ and $r \times r$ then $G = (I_k \mid H_0^T H_1^{-T})$.

The non-trivial block is dense, so this is a natural choice of public key for McEliece.

Decodable with very efficient probabilistic "bit flipping" algorithm (Gallager, '63), small decoding failure rate (DFR) $\approx 10^{-9}$.

Security

Distinguish public matrix $\approxeq$ look for low-weight codewords in the dual.

This is also a decoding problem! So we have just one assumption.

Best attacks: generic "search" algorithms like Information-Set Decoding (ISD).

MDPC: "relaxed" version of LDPC (Misoczki, Tillich, Sendrier and Barreto '12).

Change weight w from very low (≈ 10) to "moderate" ($O(\sqrt{n})$).

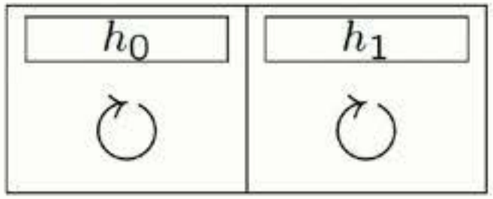
Still decodable (worse) but gain in security makes tradeoff worth it.

Structured Sparse-matrix Codes

Using "plain" LDPC/MDPC is not practical due to long code lengths.

Possible to build QC-LDPC/MDPC codes and have compact keys.

Correspond to ideals of $\mathcal{R} = \mathbb{F}_2[x]/(x^k - 1)$: describe using ring arithmetic.



QC property alone does not provide a structural attack. Still:

Possible ISD speed-up (DOOM attack).

Can mount reaction attacks.

Part IV

Reproducibility

Reproducibility

Reproducible Matrix

For $A \in \mathbb{F}_q^{k \times n}$ let $\mathcal{R}$ be the set of rows and $2^{\mathcal{R}}$ be its power set. A is reproducible if can be entirely described as $\mathcal{F}(a)$, where $a \in 2^{\mathcal{R}}$, $|a| = m < k$, and $\mathcal{F} = \{\sigma_0, \sigma_1, \cdots, \sigma_\ell\}$ is a family of linear functions acting on elements of $\mathbb{F}_q^{m \times n}$.

Reproducibility

Reproducible Matrix

For $A \in \mathbb{F}_q^{k \times n}$ let $\mathcal{R}$ be the set of rows and $2^{\mathcal{R}}$ be its power set. A is reproducible if can be entirely described as $\mathcal{F}(a)$, where $a \in 2^{\mathcal{R}}$, $|a| = m < k$, and $\mathcal{F} = \{\sigma_0, \sigma_1, \cdots, \sigma_\ell\}$ is a family of linear functions acting on elements of $\mathbb{F}_q^{m \times n}$.

The set a is called signature set.

Reproducibility

Reproducible Matrix

For $A \in \mathbb{F}_q^{k \times n}$ let $\mathcal{R}$ be the set of rows and $2^{\mathcal{R}}$ be its power set. A is reproducible if can be entirely described as $\mathcal{F}(a)$, where $a \in 2^{\mathcal{R}}$, $|a| = m < k$, and $\mathcal{F} = \{\sigma_0, \sigma_1, \cdots, \sigma_\ell\}$ is a family of linear functions acting on elements of $\mathbb{F}_q^{m \times n}$.

The set a is called signature set.

Quasi-Reproducible Matrix

For $A_{i,j} \in \mathbb{F}_q^{k_{i,j} \times n_{i,j}}$ reproducible, defined by (resp.) $a_{i,j} \in \mathbb{F}_q^{m_{i,j} \times n_{i,j}}$ and $\mathcal{F}_{i,j}$. Let A be obtained using $A_{i,j}$ as building blocks; then, A is quasi-reproducible.

Reproducibility

Reproducible Matrix

For $A \in \mathbb{F}_q^{k \times n}$ let $\mathcal{R}$ be the set of rows and $2^{\mathcal{R}}$ be its power set. A is reproducible if can be entirely described as $\mathcal{F}(a)$, where $a \in 2^{\mathcal{R}}$, $|a| = m < k$, and $\mathcal{F} = \{\sigma_0, \sigma_1, \cdots, \sigma_\ell\}$ is a family of linear functions acting on elements of $\mathbb{F}_q^{m \times n}$.

The set a is called signature set.

Quasi-Reproducible Matrix

For $A_{i,j} \in \mathbb{F}_q^{k_{i,j} \times n_{i,j}}$ reproducible, defined by (resp.) $a_{i,j} \in \mathbb{F}_q^{m_{i,j} \times n_{i,j}}$ and $\mathcal{F}_{i,j}$. Let A be obtained using $A_{i,j}$ as building blocks; then, A is quasi-reproducible.

Linear codes described by (quasi-)reproducible generator and/or parity-check matrices are in (quasi-)reproducible form.

Reproducible Pseudo-Rings

Special case: $\mathcal{F} = \left\{\sigma_0, \sigma_1, \cdots, \sigma_{\frac{p}{m}-1}\right\}$, σ_i is $p \times p$ matrix ($\sigma_0 = I_p$).

Consider the set $\mathcal{M}_q^{\mathcal{F},m}$ of all reproducible matrices defined by $\mathcal{F}$. Then:

- $(\mathcal{M}_q^{\mathcal{F},m}, +)$ is abelian group.
- Multiplication is distributive.

Moreover, we have the following result.

Theorem 1

$(\mathcal{M}_q^{\mathcal{F},m}, \cdot)$ is semigroup iff for all matrices $B \in \mathcal{M}_q^{\mathcal{F},m}$ and for all $\sigma_i \in \mathcal{F}$ we have $\sigma_i B = B\sigma_i$.

Reproducible Pseudo-Rings

Special case: $\mathcal{F} = \left\{\sigma_0, \sigma_1, \cdots, \sigma_{\frac{p}{m}-1}\right\}$, σ_i is $p \times p$ matrix ($\sigma_0 = I_p$).

Consider the set $\mathcal{M}_q^{\mathcal{F},m}$ of all reproducible matrices defined by $\mathcal{F}$. Then:

- $(\mathcal{M}_q^{\mathcal{F},m}, +)$ is abelian group.
- Multiplication is distributive.

Moreover, we have the following result.

Theorem 1

$(\mathcal{M}_q^{\mathcal{F},m}, \cdot)$ is semigroup iff for all matrices $B \in \mathcal{M}_q^{\mathcal{F},m}$ and for all $\sigma_i \in \mathcal{F}$ we have $\sigma_i B = B\sigma_i$.

Reproducible Pseudo-Ring

We call $\mathcal{M}_q^{\mathcal{F},m}$ the reproducible pseudo-ring induced by $\mathcal{F}$.

Permutation Pseudo-Rings

Special case: $m = 1$ and σ_i are permutations.

Associate $\sigma_i \leftrightarrow f_{\sigma_i}$ bijection such that $f_{\sigma_i}(v) = z$ iff $\sigma_i(v, z) = 1$.

Then $\sigma_i^{-1} \leftrightarrow f_{\sigma_i}^{-1}$ and $\sigma_i\sigma_j \leftrightarrow f_{\sigma_i} \circ f_{\sigma_j}$ and we have the following.

Theorem 2

Let $\mathcal{F} = \{\sigma_0 = I_p, \sigma_1, \cdots, \sigma_{p-1}\}$ permutations. Then in $\mathcal{M}_q^{\mathcal{F},1}$ it must be

$$\sigma_j\sigma_i = \sigma_{f_{\sigma_i}(j)}$$

for all $0 \leq i, j \leq p - 1$.

Corollary 1

$\mathcal{F}$ has the following properties

- $f_{\sigma_i}(0) = i, \ \ \forall i;$
- $\forall i \ \ \exists j \ \ s.t. \ \ f_{\sigma_i} \circ f_{\sigma_j} = id.$

Permutation Pseudo-Rings (cont.)

Corollary 2

$\mathcal{M}_q^{\mathcal{F},1}$ is a ring and the invertible elements form a multiplicative group.

Theorem 3

If $f_{\sigma_j}^{-1}(i) = f_{\sigma_v}^{-1}(0), \quad v = f_{\sigma_i}^{-1}(j), \quad \forall i,j \;\; s.t. \;\; 0 \leq i,j \leq p-1$ then $\mathcal{M}_q^{\mathcal{F},1}$ is closed under transposition.

If $\mathcal{M}_q^{\mathcal{F},1}$ verifies all the previous theorems, we have a particular condition on its elements.

Consider A block matrix with blocks in $\mathcal{M}_q^{\mathcal{F},1}$. Then $det(A) \in \mathcal{M}_q^{\mathcal{F},1}$.

Since $A^{-1} = det(A)^{-1} adj(A)$ and $adj(A)$ also has blocks in $\mathcal{M}_q^{\mathcal{F},1}$ then A^{-1} has same reproducible structure as A.

Permutation Pseudo-Rings (cont.)

Corollary 2

$\mathcal{M}_q^{\mathcal{F},1}$ is a ring and the invertible elements form a multiplicative group.

Theorem 3

If $f_{\sigma_j}^{-1}(i) = f_{\sigma_v}^{-1}(0), \quad v = f_{\sigma_i}^{-1}(j), \quad \forall i,j \;\; s.t. \;\; 0 \leq i,j \leq p-1$ then $\mathcal{M}_q^{\mathcal{F},1}$ is closed under transposition.

If $\mathcal{M}_q^{\mathcal{F},1}$ verifies all the previous theorems, we have a particular condition on its elements.

Consider A block matrix with blocks in $\mathcal{M}_q^{\mathcal{F},1}$. Then $det(A) \in \mathcal{M}_q^{\mathcal{F},1}$.

Since $A^{-1} = det(A)^{-1} adj(A)$ and $adj(A)$ also has blocks in $\mathcal{M}_q^{\mathcal{F},1}$ then A^{-1} has same reproducible structure as A.

All previous results can be generalized to $m > 1$.

Known Examples

The most famous case of reproducible matrices is circulant matrices.

Signature set is just first row, and we have $\sigma_i = \pi^i$ where π is given by

$$\pi_{l,j} = \begin{cases} 1 & \text{if } l+1 \equiv j \mod p \\ 0 & \text{otherwise} \end{cases}$$

to which corresponds $f_\pi(v) = v + 1 \mod p$. Then

$$f_{\sigma_i}(v) = f_{\pi^i}(v) = \underbrace{f_\pi \circ f_\pi \cdots \circ f_\pi}_{i \text{ times}}(v) = v + i \mod p$$

and therefore $\pi^p = I_p$ and $\pi^i \pi^j = \pi^{i+j \mod p}$.

It follows that $\sigma_i \sigma_j = \pi^{i+j \mod p} = \sigma_{i+j \mod p} = f_{\sigma_i}(j)$ as per Theorem 2.

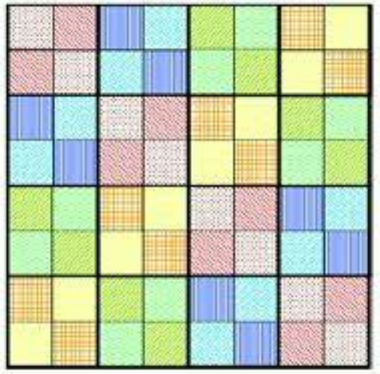
Theorem 3 is also satisfied, and multiplication is commutative.

Known Examples (cont.)

Another important example is given by dyadic matrices.

Here $p = 2^\ell$, signature is again first row and $\mathcal{F}$ given by permutations.

Define matrix as $A_{i,j} = a_{i \oplus j}$, that is $f_{\sigma_i}(v) = v \oplus i \mod p$.



Then $f_{\sigma_i} \circ f_{\sigma_j}(v) = (v \oplus j) \oplus i = v \oplus (i \oplus j) = f_{\sigma_{i \oplus j}}(v)$.

Since $f_{\sigma_i}(j) = i \oplus j$, it follows that $\sigma_i \sigma_j = f_{\sigma_i}(j)$ as per Theorem 2.

Again, Theorem 3 is also satisfied, and multiplication is commutative.

In particular, dyadic matrices are symmetric.

Part V

Codes in Reproducible Form

Construction: Sufficient Conditions

Many possibilities for constructing codes with compact matrices.

Generalize further: abandon pseudo-ring, work on generator matrix.

Theorem 4

Let G be reproducible, with signature $g_0 \in \mathbb{F}_q^{m \times n}$ and family $\mathcal{F} = \left\{\sigma_0 = I_n, \sigma_1, \cdots, \sigma_{\frac{k}{m}-1}\right\}$. Let H be such that $g_0 H^T = 0_{m \times r}$ and $s \mid r$, call h_i subset of rows of H in pos. $\{is, is+1, \cdots, (i+1)s-1\}$. If we can define a function $f(x_0, x_1) : [0, \frac{k}{m} - 1] \times [0, \frac{r}{s} - 1] \subset \mathbb{N}^2 \to [0, \frac{r}{s} - 1] \subset \mathbb{N}$ such that:

$$h_j \sigma_i^T = h_{f(i,j)}$$

then G and H are orthogonal.

Natural candidates for generator/parity-check (need to have full rank).

Construction: Householder Matrices

Definition 2

A Householder matrix is orthogonal and symmetric.

Consider a set of Householder matrices $\psi_0, \psi_1, \cdots, \psi_{v-1}$ and two sets of 2^v distinct binary v-tuples

$$\left\{ a^{(i)} \,\middle|\, 0 \leq i \leq 2^v - 1,\ a^{(i)} \in \mathbb{F}_2^v,\ \forall i\ \nexists j \text{ s.t. } a^{(i)} = a^{(j)} \right\},$$
$$\left\{ b^{(i)} \,\middle|\, 0 \leq i \leq 2^v - 1,\ b^{(i)} \in \mathbb{F}_2^v,\ \forall i\ \nexists j \text{ s.t. } b^{(i)} = b^{(j)} \right\}.$$

which are identical up to order. Set $a^{(0)} = 0_{1\times v}$. Then can define

$$\sigma_i = \prod_{l=0}^{v-1} \psi_l^{a_l^{(i)}} \text{ and } h_j = h_0 \left(\prod_{l=0}^{v-1} \psi_l^{b_l^{(j)}} \right)^T.$$

Form g_0 selecting m codewords and build repr. generator using $\mathcal{F}$.

Code parameters n, $k = m2^v$, $r = s2^v$, rate close (or equal) to 1/2.

Construction: Powers of a Single Function

Take an $n \times n$ matrix π such that $\pi^b = I_n$, for some integer b.

Can build a family $\mathcal{F}$ containing b/v functions as $\sigma_i = \pi^{vz_i}$

Form a parity-check matrix H using an $s \times n$ matrix h_0 and setting

$$H = \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{\frac{b}{v}-1} \end{bmatrix} = \begin{bmatrix} h_0 \\ h_0(\pi^{b-v})^T \\ h_0(\pi^{b-2v})^T \\ \vdots \\ h_0(\pi^{v})^T \end{bmatrix}.$$

Again obtain generator forming g_0 with m codewords, and using $\mathcal{F}$.

Code parameters n, $k = m\frac{b}{v}$, $r = s\frac{b}{v}$.

Building Code-based Schemes

Have to guarantee sparsity to be able to decode.

Building Code-based Schemes

Have to guarantee sparsity to be able to decode.

Form H choosing appropriately sparse $\mathcal{F}$ and signature.

Niederreiter public key is $H' = SH$ for a random dense matrix S.

Building Code-based Schemes

Have to guarantee sparsity to be able to decode.

Form H choosing appropriately sparse $\mathcal{F}$ and signature.

Niederreiter public key is $H' = SH$ for a random dense matrix S.

From Theorem 1, the entries of H' belong to $\mathcal{M}_q^{\mathcal{F},m}$, and so maintain the same reproducible structure defined by $\mathcal{F}$.

Building Code-based Schemes

Have to guarantee sparsity to be able to decode.

Form H choosing appropriately sparse $\mathcal{F}$ and signature.

Niederreiter public key is $H' = SH$ for a random dense matrix S.

From Theorem 1, the entries of H' belong to $\mathcal{M}_q^{\mathcal{F},m}$, and so maintain the same reproducible structure defined by $\mathcal{F}$.

If $m = 1$ and $\mathcal{F}$ is permutations, then can set $H = [H_0, H_1, \cdots, H_{n_0-1}]$, with $H_i \in \mathcal{M}_q^{\mathcal{F},1}$ as private key and $H' = H_0^{-1}H$ as public key.

If $\mathcal{F}$ satisfies Theorem 3, we can obtain a generator matrix, and use McEliece.

Choose $H = [H_0, H_1]$, then $G = S[H_1^T, -H_0^T]$, with $H_i, S \in \mathcal{M}_q^{\mathcal{F},1}$.

This is actually BIKE-1.

Part VI

Defeating Attacks and Explicit Constructions

Reaction attacks

Reaction attacks recover private key by exploiting decoding failures.
(Guo, Johansson and Stankovski '16)

Attacker aims at recovering distance spectrum (set of all distances).

Reaction attacks

Reaction attacks recover private key by exploiting decoding failures.
(Guo, Johansson and Stankovski '16)

Attacker aims at recovering distance spectrum (set of all distances).

In QC codes distances are computed cyclically, and all rows have same distance spectrum.

Reaction attacks

Reaction attacks recover private key by exploiting decoding failures.
(Guo, Johansson and Stankovski '16)

Attacker aims at recovering distance spectrum (set of all distances).

In QC codes distances are computed cyclically, and all rows have same distance spectrum.

This is not true in general for reproducible codes.

Thus, we remove the basis for building reaction attacks.

May be impossible for opponent to recover distance spectrum.

DOOM

"Decoding One Out of Many", technique to speed up ISD (Sendrier '11).

Exploit multiple instances of SDP with same solution.

DOOM

"Decoding One Out of Many", technique to speed up ISD (Sendrier '11).

Exploit multiple instances of SDP with same solution.

Gives a speed up of $\approx \sqrt{N}$, where N is number of syndromes.

In the QC case multiple instances obtained via cyclic shifts of initial syndrome.

For general reproducible codes, this can be prevented.

For example abandoning cyclic permutations, one can force opponent to consider multiple instances having higher (3x) Hamming weight.

This means no gain in applying DOOM.

QD-MDPC

Quasi-Dyadic reproducible structure less “obvious” than circulant.

Still allows for efficient arithmetic (Banegas, Barreto, P. and Santini ’18).

QD-MDPC

Quasi-Dyadic reproducible structure less "obvious" than circulant.

Still allows for efficient arithmetic (Banegas, Barreto, P. and Santini '18).

Easy to design McEliece "a-la" BIKE -1, $G = S[H_1^T, -H_0^T]$.

For systematic form (e.g. BIKE-2): caution.

In fact, dyadic matrices are symmetric and orthogonal.

This means density of inverse is not guaranteed.

Use 2×2 block matrices (quasi-dyadic), rather than fully dyadic.

Caution required with ring homomorphisms.

Block-wise Circulant

Generalize the idea of circulant matrix to $m > 1$.

Take m independent rows and functions π^{im}.

This gives "p by p" reproducible matrix.

We again obtain a reproducible pseudo-ring.

Lose the property about distances typical of circulant matrices.

This means reaction attacks are hindered, as explained before.

Construction proposed in literature for first time.

Thank you