On the Generalizations of the Rank Metric Over Finite Chain Rings

Hermann Tchatchiem Kamche & **Hervé Talé Kalachi**

AFRICACRYPT 2024

15th International Conference on Cryptology

July 11, 2024

Introduction

Linear code

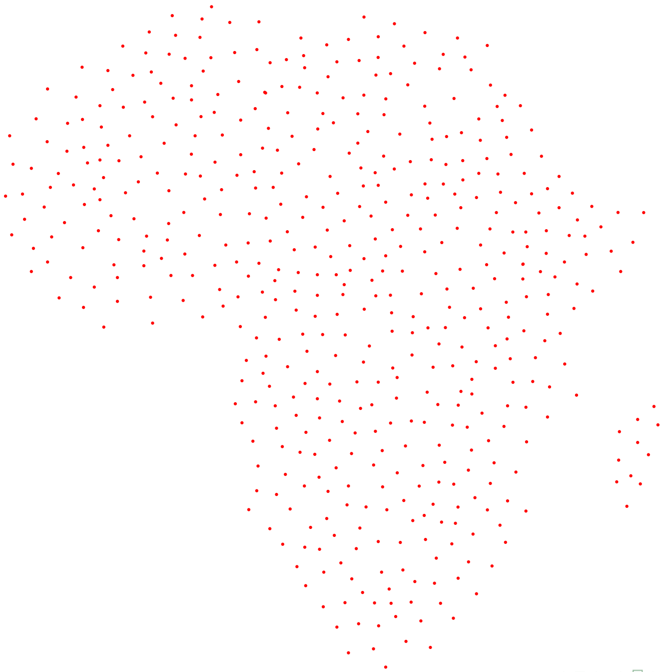
1. $(\mathrm{R}^n, \|\cdot\|)$, R a finite field/ring and $\|\cdot\|$ a norm
2. Linear code $\mathscr{C}$ = free.sm of $(\mathrm{R}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathrm{R}\ \vec{v}_i$$

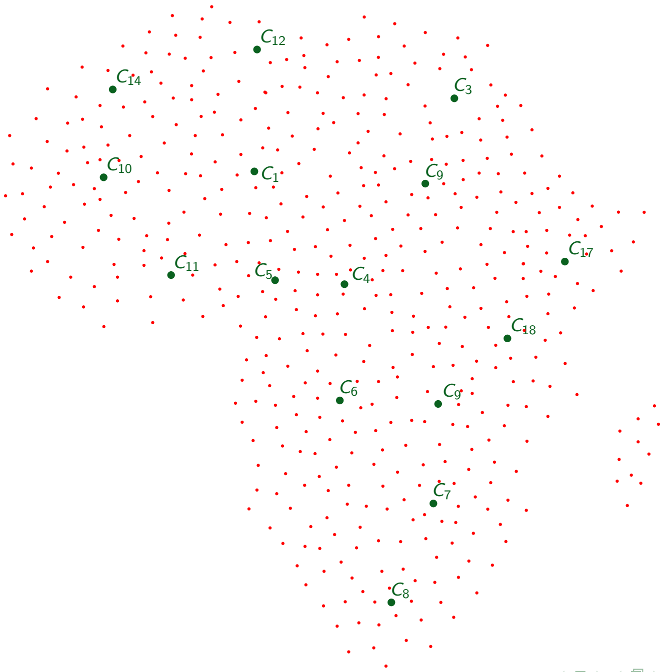
   where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$
4. Decoding a word $\vec{w} \in \mathrm{R}^n$ = solving the closest vector problem (CVP)

General Decoding Problem = Closest Vector Problem (CVP)



General Decoding Problem = Closest Vector Problem (CVP)



Rank-Based Cryptography

First Rank-Metric Encryption Scheme

- First proposal from at Eurocrypt'91 : GPT Cryptosystem
- Broken by Overbeck at Mycrypt'05

Recent Proposals

- New proposal at WCC'13 based on LRPC codes
- Submission to the NIST PQ competition (ROLLO, RQC)
  - ROLLO : Analogue of NTRU, uses LRPC codes
  - RQC : Security relying only on the CVP in the rank metric
  - Shorter public keys

Solving the decoding problem in the rank metric

1.
- Combinatorial attacks
- Aragon-Gaborit-Hautville-Tillich '18

$$2^{tn+o(1)}$$

2.
- New algebraic attack
- By Bardet et al. Eurocrypt'20

$$2^{O(t\log_2(n))}$$

Consequenses

- Drastic reduction of security levels
- ROLLO−I−128/192/256 ⇝ ROLLO−I−71/87/151
- RQC−256 ⇝ RQC−188
- Elimination of ROLLO and RQC from the NIST competition

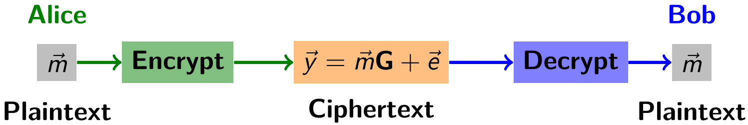
Excerpt from the NIST Report on the Second Round of the PQCS

"... Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth... " [1]

[1] Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, **July 2020**

Starting Point for all Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}-$code generated by $\boldsymbol{G}$



Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)-$code generated by

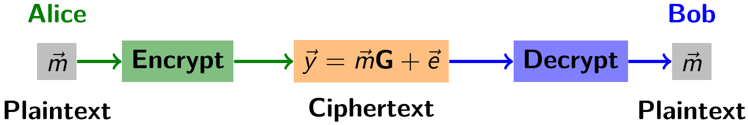
$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$ is a good candidate

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n, k)_{\mathbb{F}_{q^m}}$ −code generated by $\boldsymbol{G}$



Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)$−code generated by

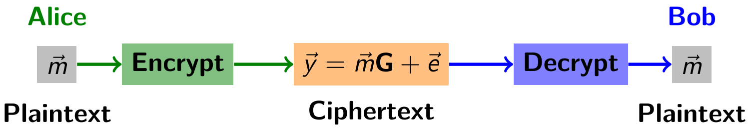
$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_{\mathbb{F}_q}(\vec{c}') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in \mathbb{F}^*_{q^m}$ is a good candidate

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n, k)_S$−code generated by $\boldsymbol{G}$



Ourivski-Johansson's Modelling

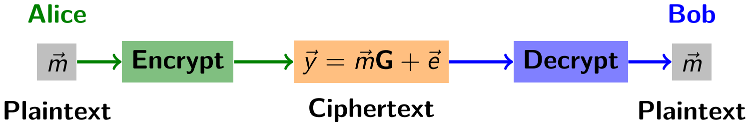
- $\mathscr{C}_{ext}$ the $(n, k+1)$−code generated by

$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_S = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_S$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_R(\vec{c}') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in S^*$ is a good candidate ?

- $\mathscr{C}$ is a $(n, k)_S-$code generated by $\boldsymbol{G}$



Ourivski-Johansson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)-$code generated by

$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_S = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_S$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathtt{Rank}_R(\vec{c}') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in S^*$ is a good candidate ?

Rank-Metric Code-Based Cryptography over Finite Rings

- Ourivski-Johansson's modelling is not applicable[2]
- All known algebraic attacks/costs are not applicable
- The (rank) metric need to be clarified

Rank Metric : Finite Fields Vs Finite Rings

Let S/R , $\vec{x} = (x_1 \cdots x_n) \in S^n$ and $\mathscr{V} =< x_1, \cdots, x_n >_R$

1. **Finite Fields :**
   - $\|\vec{x}\|_R =$ Min. numb. of gen. of $\mathscr{V}$
   - $\log_{|R|}(|\mathscr{V}|)$
   - Max. len. for chains of s.s. of $\mathscr{V}$
2. **Finite Rings :**
   - $\|\vec{x}\|_g =$ Min. numb. of gen. of $\mathscr{V}$, d_g
   - $\|\vec{x}\|_c = \log_{|R|}(|\mathscr{V}|)$, d_c
   - $\|\vec{x}\|_l =$ Max. len. for chains of s.s. of $\mathscr{V}$, d_l

$$\{0\} \subsetneq \mathscr{V}_1 \subsetneq \cdots \subsetneq \mathscr{V}_k = \mathscr{V}$$

[2] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. *AMC'23*

Example 1

- $R = \mathbb{Z}_8$
- $\mathscr{V} =< (2,4) >_R = \{\lambda(2,4),\ \lambda \in \mathbb{Z}_8\}$
  1. the Min. numb. of gen. of $\mathscr{V}$ is 1.
  2. $\log_{|R|}(|\mathscr{V}|) = \frac{2}{3}$.
  3. the length of the longest chain of subspaces $\mathscr{V}$ is 2: $\{0\} \subsetneq 2\mathscr{V} \subsetneq \mathscr{V}$.

$$\text{Let } S/R\ ,\ \vec{x} = (x_1 \cdots x_n) \in S^n \text{ and } \mathscr{V} =< x_1, \cdots, x_n >_R$$

- $\|\vec{x}\|_g$ = Min. numb. of gen. of $\mathscr{V}$, d_g — Kamche & Mouaha'19
- $\|\vec{x}\|_c = \log_{|R|}(|\mathscr{V}|)$, d_c — Epelde & Rúa'22
- $\|\vec{x}\|_l$ = Max. len. for chains of s.m. of $\mathscr{V}$, d_l — Gorla & Ravagnani'17

Generalizations of the Rank Metric over Finite Rings

- $\|\vec{x}\|_g$ = Min. numb. of gen. of $\mathscr{V}$, d_g — Kamche & Mouaha'19
- $\|\vec{x}\|_c = \log_{|R|}(|\mathscr{V}|)$, d_c — Epelde & Rúa'22
- $\|\vec{x}\|_l$ = Max. len. for chains of s.m. of $\mathscr{V}$, d_l — Gorla & Ravagnani'17

Our contribution

1. Relationship between these three metrics
2. Code-based crypto. comparison of these metrics

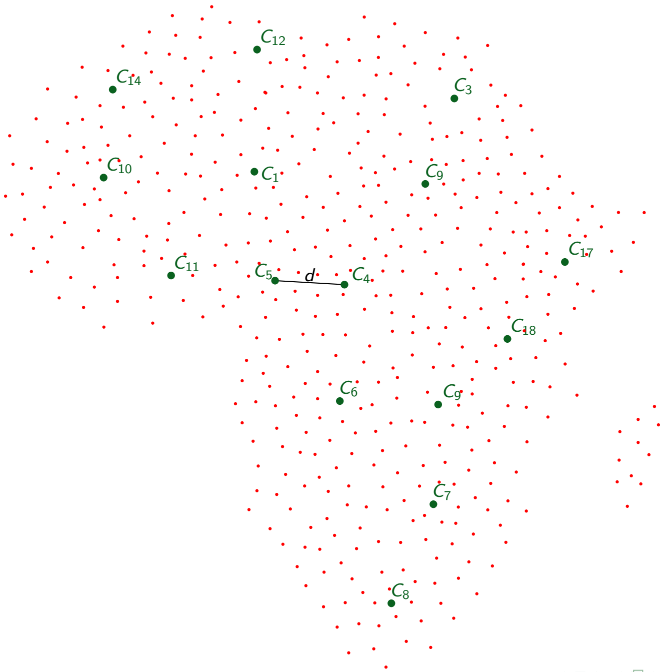
Outline

Next

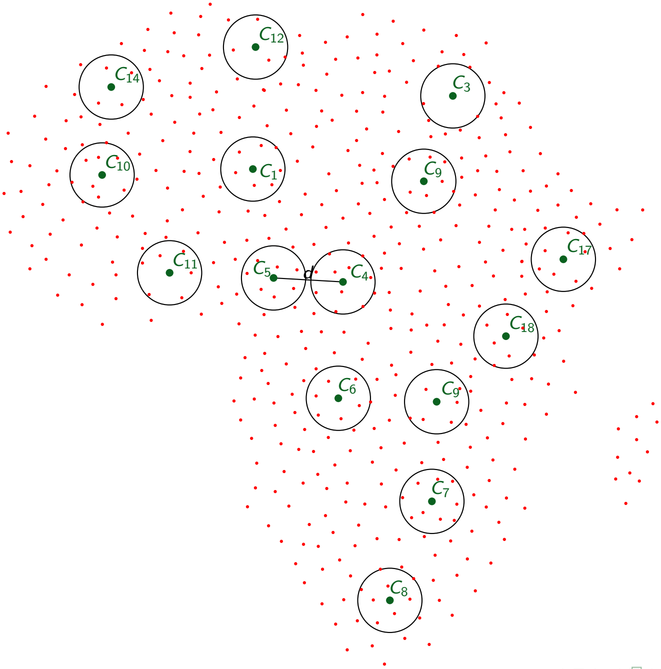
Notations

- R is a finite commutative chain ring with maximal ideal $\mathfrak{m}$
- $\mathbb{F}_q = R/\mathfrak{m}$ is the residue field of R
- π is a generator of $\mathfrak{m}$
- ν the nilpotency index of π, i.e., the smallest positive integer such that $\pi^\nu = 0$
- $S = R[X]/(h)$ is a Galois extension of R of degree m

Minimum Distance & Packing Radius



Minimum Distance, Packing Radius & Balls



Decoding Equivalence

Definition 2 (Decoding equivalence)

- $\mathscr{V}$ is a given set (e.g. R^n or $\mathbb{F}_{q^m}^n$)
- d_1 and d_2 are distances on $\mathscr{V}$

If for any subset $\mathscr{C}$ of $\mathscr{V}$ and any $\vec{y}$ in $\mathscr{V}$,

$$\text{argmin}\{d_1(\vec{x},\vec{y}) : \vec{x} \in \mathscr{C}\} = \text{argmin}\{d_2(\vec{x},\vec{y}) : \vec{x} \in \mathscr{C}\},$$

we say that d_1 and d_2 are **decoding equivalent**

Proposition 1

- *$\mathscr{C} \subset R^n$ is a linear code*
- *d_1 and d_2 are distances on R^n s.t. $d_2 = \alpha d_1$ with $\alpha \in \mathbb{R}$*

*Then, d_1 and d_2 are **decoding equivalent** and we have*

$$d_2(\mathscr{C}) = \alpha d_1(\mathscr{C}) \text{ and } R_{d_2}(\mathscr{C}) = \alpha R_{d_1}(\mathscr{C}).$$

Next

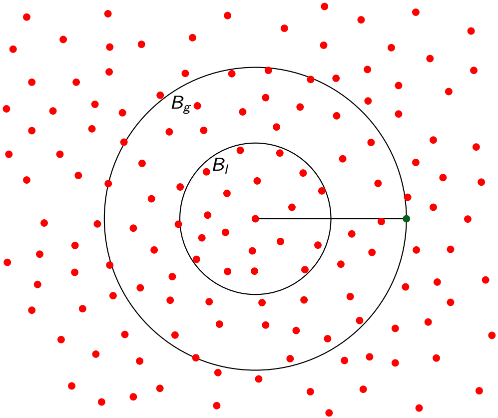
Main Results on Minimum distances and Packing Radii

- R is a finite chain ring of the nilpotency index ν.
- $\mathscr{C}$ is a linear code over a Galois extension of R.

Metrics	Generators d_g	Longest Chain d_l	Log of Cardinality d_c
Relation on Metrics	$d_c \leqslant d_g \leqslant d_l = \nu d_c$		
Minimum Distances	$d_g(\mathscr{C})$	$d_l(\mathscr{C})$	$d_c(\mathscr{C})$
Relation on Minimum Distances	$d_g(\mathscr{C}) = d_l(\mathscr{C}) = \nu\ d_c(\mathscr{C})$		
Packing Radii	$t_g = \lfloor (d_g(\mathscr{C}) - 1)/2 \rfloor$	$t_l = \lfloor (d_l(\mathscr{C}) - 1)/2 \rfloor$	$t_c = \lfloor (\nu\ d_c(\mathscr{C}) - 1)/2 \rfloor / \nu$

Results on balls with radii the Packing radii

$$B_c = B_l \subset B_g$$



Consequence

Up to the error correction capacity:

- $(\mathscr{C}, d_g)$ corrects more errors than $(\mathscr{C}, d_l)$ and $(\mathscr{C}, d_c)$.

Next

1. Notations and Preliminaries
2. Relations Between the Metrics
3. Cryptographic Consequenses

Key generation.

- Choose $(\mathscr{C}, d)$ a $(n, k)-$code over a FC-Rings S (e.g. LRPC code)
- $t_d = R_d(\mathscr{C})$ the packing radius of $\mathscr{C}$
- $\boldsymbol{H}_{\text{pub}} \in S^{r\times n}$ the parity check matrix of $\mathscr{C}$ in systematic form
- $\Gamma_{\mathscr{C}}$ an efficient decoding algorithm of $\mathscr{C}$
- Public Key
$$\text{pk} = (\boldsymbol{H}_{\text{pub}}, t_d)$$
- Secret Key
$$\text{sk} = \Gamma_{\mathscr{C}}$$

A Canonical Code-Based Encryption Scheme over FC-Rings

Encryption.

- Input : $\vec{e} \in S^n$ with $d(\vec{e}, \vec{0}) \leqslant t_d$.
- Output the syndrome $\vec{s} = \vec{e}\boldsymbol{H}_{\text{pub}}^{\top}$

Decryption. Uses $\Gamma_{\mathscr{C}}$ to find $\vec{e}$.

Security.

- Given $\vec{s} = \vec{e}\boldsymbol{H}_{\text{pub}}^{\top}$ and $\boldsymbol{H}_{\text{pub}}^{\top}$,

An attacker must solve the SD-Problem with the metric d.

Definition 3 (Syndrome Decoding Problem)

- $\mathbf{H} \in S^{(n-k)\times n}$,
- $\mathbf{s} \in S^{n-k}$ and $t_d \in \mathbb{N}^*$

The *Syndrome Decoding Problem* is to find $\mathbf{e}$ in S^n such that

$$\mathbf{s} = \mathbf{e}\mathbf{H}^{\top} \tag{1}$$

with $d(\mathbf{e}, \mathbf{0}) \leqslant t_d$.

A Canonical Code-Based Encryption Scheme over FC-Rings

Encryption.

- Input : $\vec{e} \in S^n$ with $d(\vec{e}, \vec{0}) \leqslant t_d$.
- Output the syndrome $\vec{s} = \vec{e}\boldsymbol{H}_{\text{pub}}^{\top}$

Decryption. Uses $\Gamma_{\mathscr{C}}$ to find $\vec{e}$.

Security.

- Given $\vec{s} = \vec{e}\boldsymbol{H}_{\text{pub}}^{\top}$ and $\boldsymbol{H}_{\text{pub}}^{\top}$,

An attacker must solve the SD-Problem with the metric d.

Definition 3 (Syndrome Decoding Problem)

- $\mathbf{H} \in S^{(n-k)\times n}$,
- $\mathbf{s} \in S^{n-k}$ and $t_d \in \mathbb{N}^*$

The *Syndrome Decoding Problem* is to find $\mathbf{e}$ in S^n such that

$$\mathbf{s} = \mathbf{e}\mathbf{H}^{\top} \tag{1}$$

with $d(\mathbf{e}, \mathbf{0}) \leqslant t_d$.

Best Algorithm.

- Error Support Attack[3] [4]
- Idea :
  1. guess a free s.m. $F \subset S$ of rank $u = \lfloor (n-k)m/n \rfloor$ and s.t. $\text{supp}(\vec{e}) \subset F$
  2. Solve a linear system for each guess
- Complexity :

$$\mathcal{O}\left(m\left(n-k\right)u^2n^2/P_d\right)$$

P_d being the probability that $\text{supp}(\mathbf{e}) \subset F$

Complexities Comparison

Metrics	d_g	d_l
$1/P_d$	$\approx q^{\nu r(m-u)}$	$\approx q^{r(m-u)}$
Complexities	$\mathcal{O}\left(m\left(n-k\right)u^2n^2q^{\nu r(m-u)}\right)$	$\mathcal{O}\left(m\left(n-k\right)u^2n^2q^{r(m-u)}\right)$

With $r = t_g = t_l$.

[3] Gaborit, Ruatta & Schrek. On the complexity of the rank syndrome decoding problem. *IEEE IT'16*

[4] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. *AMC'23*

Complexities Comparison

Table: Average Complexities of the Error Support Attack for $m = n = 32,\ k = 16,\ r = 4$.

q	2	2	2	2	4	4
ν	1	2	3	4	1	2
$Cost_{d_l}$	91	91	91	91	155	155
$Cost_{d_g}$	91	155	219	283	155	283

Table: Key sizes comparison for d_g and d_l

Metrics	m	n	k	r	q	ν	Public Key sizes	Security Levels
d_g	34	34	17	3	2	2	2.4 KB	128
	38	40	20	3	2	4	7.6 KB	256
d_l	58	58	24	4	2	2	11.8 KB	128
	80	87	40	6	2	4	75.2 KB	256

- Public Key sizes 100 times smaller than Classic McEliece for d_g
- 2 to 4 times smaller than LowMS

Complexities Comparison

Table: Average Complexities of the Error Support Attack for $m = n = 32,\ k = 16,\ r = 4$.

q	2	2	2	2	4	4
ν	1	2	3	4	1	2
$Cost_{d_l}$	91	91	91	91	155	155
$Cost_{d_g}$	91	155	219	283	155	283

Table: Key sizes comparison for d_g and d_l

Metrics	m	n	k	r	q	ν	Public Key sizes	Security Levels
d_g	34	34	17	3	2	2	2.4 KB	128
	38	40	20	3	2	4	7.6 KB	256
d_l	58	58	24	4	2	2	11.8 KB	128
	80	87	40	6	2	4	75.2 KB	256

- Public Key sizes 100 times smaller than Classic McEliece for d_g
- 2 to 4 times smaller than LowMS

Complexities Comparison

Table: Average Complexities of the Error Support Attack for $m = n = 32,\ k = 16,\ r = 4$.

q	2	2	2	2	4	4
ν	1	2	3	4	1	2
$Cost_{d_l}$	91	91	91	91	155	155
$Cost_{d_g}$	91	155	219	283	155	283

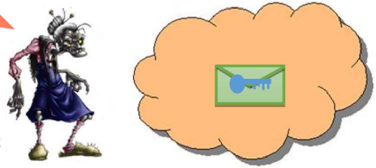
Table: Key sizes comparison for d_g and d_l

Metrics	m	n	k	r	q	ν	Public Key sizes	Security Levels
d_g	34	34	17	3	2	2	2.4 KB	128
	38	40	20	3	2	4	7.6 KB	256
d_l	58	58	24	4	2	2	11.8 KB	128
	80	87	40	6	2	4	75.2 KB	256

- Public Key sizes 100 times smaller than Classic McEliece for d_g
- 2 to 4 times smaller than LowMS

An important open question

Algebraic Attacks ?



Combinatorial Attacks over Finite Rings

Talé & Tchatchiem ‘23