Cryptographic applications of codes in rank metric

Pierre Loidreau

CELAr and Université de Rennes
Pierre.Loidreau@m4x.org

June 16th, 2009

Introduction

- Rank metric and cryptography
- Gabidulin codes and linearized polynomials
- McEliece type cryptosystems
- AF-like cryptosystems

Rank metric and cryptography

History of Cryptographic applications

- Encryption schemes, [Gabidulin-Paramonov-Tretjakov 91]
  $\longrightarrow$ Trapdoor: Difficulty of decoding in rank metric.
- Authentification codes, [Johannson95]
- ZK-identification scheme, [Chen96]
- Hash functions for MAC, [Savafi-Naini-Charnes 05]

Rank metric

Definition (Rank of a vector)

- $\gamma_1, \ldots, \gamma_m$, *a basis of* $\mathbb{F}_{q^m}/\mathbb{F}_q$,
- $\mathbf{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{q^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

$$\forall \mathbf{e} \in \mathbb{F}_{q^m}, \quad \mathrm{Rk}(\mathbf{e}) \stackrel{def}{=} \mathrm{Rk} \begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

Definition

$\mathcal{C} \subset \mathbb{F}_{q^m}^n$ is a $(n, M, d)_r$-code if

- $M = |\mathcal{C}|$
- *Min. rank distance:* $d = \min_{\mathbf{c_1} \neq \mathbf{c}_2 \in \mathcal{C}} \mathrm{Rk}(\mathbf{c_1} - \mathbf{c}_2)$

Bounds in rank metric

- Volume of sphere: $q^{(m+n-1)t-t^2} \leq \mathcal{S}_t \leq q^{(m+n+1)t-t^2}$
- Volume of ball: $q^{(m+n-1)t-t^2} \leq \mathcal{B}_t \leq q^{(m+n+1)t-t^2+1}$

Classical Bounds

- Singleton: $M \leq q^{\min(m(n-d+1),n(m-d+1))} \longrightarrow$ MRD codes
- Sphere-packing: $M\mathcal{B}_{\lfloor (d-1)/2 \rfloor} \leq q^{mn} \longrightarrow$ perfect codes
- GV-like: $M\mathcal{B}_{d-1} < q^{mn} \Longrightarrow \exists (n, M+1, d)_r$ code

- Singleton: $M \leq q^{\min(m(n-d+1),n(m-d+1))} \longrightarrow$ MRD codes
- Sphere-packing: $M\mathcal{B}_{\lfloor (d-1)/2 \rfloor} \leq q^{mn} \longrightarrow$ perfect codes
- GV-like: $M\mathcal{B}_{d-1} < q^{mn} \Longrightarrow \exists (n, M+1, d)_r$ code

Proposition ([L.06])

- *No perfect codes exist*
- *For $\mathcal{C}$ on GV: if $mn \geq \log_q M = o(n)(m+n)$*

$$\frac{d}{m+n} \overset{n \to +\infty}{\sim} \frac{1}{2} - \frac{\sqrt{\log_q M}}{m+n} \sqrt{1 + \frac{(m-n)^2}{4 \log_q M}},$$

Decoding problems for linear codes

Parameters

- $\mathcal{C}$ generated by matrix $\mathbf{G}$
- $\mathbf{y} \in \mathbb{F}_{q^m}^n$, received vector
- t an integer

Problems

- MDD: Find $\mathbf{x}$, s.t. $\mathrm{Rk}(\mathbf{y} - \mathbf{xG}) = \min_{\mathbf{c} \in \mathcal{C}}(\mathrm{Rk}(\mathbf{y} - \mathbf{c}))$
- BDD: Find, if exists, $\mathbf{x}$, s.t. $\mathrm{Rk}(\mathbf{y} - \mathbf{xG}) \leq t$
- LD: Find all $\mathbf{x}$ such that $\mathrm{Rk}(\mathbf{y} - \mathbf{xG}) \leq t$

Are these search problems NP-hard ?

Solving BDD(t) for $t \leq \lfloor (d-1)/2 \rfloor$

- Principle: Find min. rank codewords in code generated by

$$\mathbf{G}' = \begin{pmatrix} \mathbf{G} \\ \mathbf{y} \end{pmatrix} = \mathbf{S}\,(\mathbf{I}_{k+1} \mid \mathbf{R})$$

- System: $(\beta_1, \ldots, \beta_t)\,(\mathbf{U}_2 - \mathbf{U}_1\mathbf{R}) = \mathbf{0}$
- Methods
  - Try and solve, [Chabaud-Stern 96, Ourivski-Johannson 02]

Algo. type	Complexity
Basis enumeration	$\leq (k+t)^3 q^{(t-1)(m-t)+2}$
Coordinates enumeration	$\leq (k+t)^3 t^3 q^{(t-1)(k+1)}$

  - Projection on base field and use of Groebner bases techniques, [Levy-Perret 06]

Why use rank metric for cryptographic applications

Complexities of solving BDD(t) for a $[n, k, d]$ code over $\mathbb{F}_{2^m}$

- IS Decoding:

$$\sim M(\mathbb{F}_{2^m}) n^3 2^{n(H_2(t/n)-(1-R)H_2(t/((1-R))n))} = m^2 n^3 2^{\alpha n}$$

- Coord. Enum.:

$$\leq (k+t)^3 t^3 2^{(\alpha_1 n-1)(\alpha_2 n+1)}$$

Use of smaller public-keys in McEliece type system.

Gabidulin codes and linearized polynomials

Gabidulin codes

Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}$, where a_i's are l.i. over $\mathbb{F}_q$. Consider

$$\mathbf{G} = \begin{pmatrix} a_1 & \cdots & a_n \\ \vdots & \ddots & \vdots \\ a_1^{[k-1]} & \cdots & a_n^{[k-1]} \end{pmatrix}, \text{ where } [i] \stackrel{def}{=} q^i \qquad (1)$$

Definition ([Gabidulin85])

The code generated by $\mathbf{G}$ *is denoted* $Gab_k(\mathbf{a})$.

Properties of the codes

- They are MRD codes (implies also MDS codes)
- Dual of $Gab_k(\mathbf{a})$ is a $Gab_{n-k}(\mathbf{h})$
- Rank distribution is known
- Permutation group trivial, [Berger 03]

Decoding algorithms

Algorithm	Complexity (mult. in $\mathbb{F}_{q^m}$)	
Ext. Euclidean	$2t(n+5t)$	[Gabidulin85]
Linear system solving	$2t(n+t^2/2)$	[Gabidulin91] [Roth91]
BM-like	$2t(n+3t+t^2/4)$	[Richter-Plass 05]
WB-like	$2t(4n-t)$	[L.05]

Table: Decoding rank $t = \lfloor (d-1)/2 \rfloor$ errors in $Gab_{n-d+1}(\mathbf{g})$ code

McEliece like cryptosystems

Description

- Parameters
  - $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}$
- Private key
  - $\mathbf{G}$ generates $Gab_k(\mathbf{g})$, correcting rank t errors
  - $\mathbf{T}$ isometry of rank metric
  - $\mathbf{Z}$ size $k \times t_1$ over $\mathbb{F}_{q^m}$
- Public-key

$$\mathbf{G}_{\text{pub}} = \mathbf{S}(\mathbf{G} \mid \underbrace{\mathbf{Z}}_{t_1 \ cols})\mathbf{T} \tag{2}$$

Encryption

$$\mathbf{y} = \mathbf{x}\mathbf{G}_{\text{pub}} + \mathbf{e},\ \text{Rk}(\mathbf{e}) \leq t - t_1$$

Decryption

- Compute $\mathbf{y}\mathbf{T}^{-1} = \mathbf{x}(\mathbf{G} \mid \mathbf{Z}) + \mathbf{e}\mathbf{T}^{-1}$
- Puncture on last t_1 positions and decode

Security assumption: BDD(t) difficult

Properties in rank metric

Advantages

- Fast in Encryption-Decryption
- Enables small keys ($\leq$ 50 000 bits)
- Security against reaction attacks

Drawbacks

- Not optimal transmission rate
- Weakness against message resend attacks
- ONLY ONE family of decodable codes is known
  $\longrightarrow$ Mandatory to scramble the structure

History of systems

- $\mathbf{G}$, $\mathbf{G}_1$, $\mathbf{G}_2$, generator matrices of Gabidulin codes
- $\mathbf{H}$, parity-check matrix of Gabidulin codes

Scrambling matrix	$\mathbf{G}_{pub} = \mathbf{SG} + \mathbf{X}$	[Gabidulin-Paramonov-Tretjakov91]
Right scrambler	$\mathbf{G}_{pub} = \mathbf{S}(\mathbf{G}\|\mathbf{Z})\mathbf{T}$	[Gabidulin-Ourivski 01]
Subcodes	$\mathbf{H}_{pub} = \mathbf{S}\begin{pmatrix}\mathbf{H}\\ \mathbf{A}\end{pmatrix}$	[Berger-L. 02]
Reducible Rank codes	$\mathbf{G}_{pub} = \mathbf{S}\begin{pmatrix}\mathbf{G}_1 & \mathbf{0}\\ \mathbf{A} & \mathbf{G}_2\end{pmatrix}\mathbf{T}$	[Ourivski-Gabidulin-Honary-Ammar03] [Berger-L. 04]

Structural attacks [Overbeck06]

Principle for $\mathbf{G}_{pub} = \mathbf{S}(\mathbf{G}|\mathbf{Z})\mathbf{T}$

- Quasi-stability under action of Frobenius: $\alpha \mapsto \alpha^q \stackrel{def}{=} \alpha^{[1]}$

$$Gab_k(\mathbf{g}) \cap [Gab_k(\mathbf{g})]^{[1]} = Gab_{k-1}\left(\mathbf{g}^{[1]}\right)$$

- Use public-key $\mathbf{G}_{pub} = \mathbf{S}(\mathbf{G}|\mathbf{Z})\mathbf{T}$ and compute

$$\underbrace{\begin{pmatrix} \mathbf{G}_{pub} \\ \vdots \\ \mathbf{G}_{pub}^{[n-k-1]} \end{pmatrix}}_{\mathcal{G}_{pub}} = \underbrace{\begin{pmatrix} \mathbf{S} & \cdots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{S}^{[n-k-1]} \end{pmatrix}}_{\mathcal{S}} \underbrace{\left(\begin{array}{c|c} \mathbf{G} & \mathbf{Z} \\ \vdots & \vdots \\ \mathbf{G}^{[n-k-1]} & \mathbf{Z}^{[n-k-1]} \end{array}\right)}_{(\mathcal{G} \mid \mathcal{Z})} \mathbf{T},$$

Proposition

If $\dim\left(\ker_r(\mathcal{G}_{pub})\right) = 1 \rightarrow$ *a decoder for public-code can be recovered in polynomial-time*

Proof.

In that case

$$\ker_r(\mathcal{G}_{\text{pub}}) = \{\mathbf{T}^{-1}(\alpha\mathbf{h} \mid \mathbf{0})^T \ , \ \alpha \in \mathbb{F}_{q^m}\},$$

□

- For security: Choose $\mathbf{Z}$ so that $\dim\left(\ker_r(\mathcal{G}_{pub})\right) > 1$

Proposition

If $1 \leq \mathrm{Rk}(\mathbf{Z}) \leq (t_1 - \ell)/(n-k)$, *then* $\dim\left(\ker_r(\mathcal{G}_{pub})\right) \geq 1 + \ell$

- Possible parameters

$m = n$	k	$\mathrm{Rk}(\mathbf{Z})$	ℓ	t_1	Key size	Decoding	k/n	Rate Improv.
24	12	3	4	40	14 976	$> 2^{83}$	19%	35%
24	12	4	4	52	18 432	$> 2^{83}$	15.8%	33%

- Same problem with Reducible Rank Codes

Modifications imply increased public-key size

AF-like systems

q-polynomials

Definition ([Øre33])

$$P(z) = \sum_{i=0}^{t} p_i z^{q^i}, \ p_i \in \mathbb{F}_{q^m}$$

If $p_t \neq 0$, $deg_q(P) \stackrel{def}{=} t$ *is the* q*-degree of* P*.*

Properties

- Non-commutative ring with $+, \circ$
- Euclidean algorithms on the left and on the right
- P. Time interpolation and root finding algorithms

Reconstruction problem

- Parameters
  - $\mathbf{g} \in \mathbb{F}_{q^m}^n$ support vector
  - $\mathbf{y} \in \mathbb{F}_{q^m}^n$,
  - k, t integers
- PR: Find P of q-degree $\leq k$ s.t. $\mathrm{Rk}(P(\mathbf{g}) - \mathbf{y}) \leq t$
- Link with other problems:
  - if $t \leq \lfloor (n-k)/2 \rfloor$, equivalent to decode $Gab_k(\mathbf{g})$
  - if $t > \lfloor (n-k)/2 \rfloor$, supposed to be difficult
    $\Rightarrow \mathrm{LD}(\mathbf{y}, t)$ is difficult

Description of the cryptosystem

- Parameters
  - $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}$, k
- Private key:
  - $\mathbf{E} = (E_1, \ldots, E_n)$ of rank $W > (n-k)/2$.
    $\Rightarrow$ exists $\mathbf{Q} \in GL_n(\mathbb{F}_q)$ such that $\mathbf{EQ} = (\underbrace{\mathbf{0}}_{n-W \text{ coords}} \mid \mathbf{E}')$
  - q-polynomial P of q-degree $k-1 \leq n-W$ over $\mathbb{F}_{q^m}$.
- Public-key:
  - $\mathbf{K} = \underbrace{P(\mathbf{g})}_{\in Gab_k(\mathbf{g})} + \mathbf{E}$

Security assumption: PR$(\mathbf{K}, W)$ difficult

Encryption and decryption

- Encryption: $\mathbf{y} = x(\mathbf{g}) + \alpha\mathbf{K} + \mathbf{e}$, where
  - x has q-degree $k - 2 \leq n - W$
  - $\mathbf{e}$ of rank $t \leq (n - k - W)/2$
  - $\alpha \in \mathbb{F}_{q^m}^*$ random

- Decryption: Let $\mathbf{v} \overset{def}{=} (\overbrace{\widetilde{\mathbf{v}}}^{n-W} | \mathbf{V}')$
  - We have

$$\mathbf{yQ} = \left(x(\widetilde{\mathbf{gQ}}) + \alpha P(\widetilde{\mathbf{gQ}}) + \widetilde{\mathbf{eQ}} \mid \mathbf{Y}' \right)$$

  - Decode $\widetilde{\mathbf{yQ}}$ in $Gab_k(\widetilde{\mathbf{gQ}}) \Rightarrow (x + \alpha P)(\widetilde{\mathbf{gQ}})$
  - Since $deg_q(x) < deg_q(P) \Rightarrow \alpha$
  - Since $k - 1 \leq n - W \Rightarrow x$

Security assumption: BDD$(x(\mathbf{g}) + \alpha\mathbf{K}, t)$ in some code is difficult

Possible attacks

Solving the system

$$\begin{cases} V(y_i) = (V \circ x)(g_i) + V(\alpha K_i), \quad \forall\ i = 1, \ldots, n, \\ deg_q(V) \leq t \end{cases}$$

Linearization: Solve

$$\begin{cases} V(y_i) = N(g_i) + U(K_i), \quad \forall\ i = 1, \ldots, n, \\ deg_q(V) \leq t \\ deg_q(N) \leq k + t - 2 \\ deg_q(U) \leq t \end{cases}$$

Linear system of $k + 3t + 1$ unknowns and n equations

Evolution of the system (I)

- Parameters
  - $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}$, k
- Private key:
  - $\mathbf{E}_i \in \mathbb{F}_{q^m}^W$, $i = 1, \ldots, u$ of rank $W > (n-k)/2$.
  - $\mathbf{Q} \in GL_n(\mathbb{F}_\mathbf{q})$
  - P_i, $i = 1, \ldots, u$ of q-degree $k - 1 \leq n - W$ over $\mathbb{F}_{q^m}$.
- Public-key:

$$\begin{cases} \mathbf{K}_1 = P_1(\mathbf{g}) + (\mathbf{0}|\mathbf{E}_1)\mathbf{Q}^{-1}, & \mathrm{Rk}(\mathbf{E}_1) = W > (n-k)/2 \\ \vdots \\ \mathbf{K}_u = P_u(\mathbf{g}) + (\mathbf{0}|\mathbf{E}_u)\mathbf{Q}^{-1}, & \mathrm{Rk}(\mathbf{E}_u) = W > (n-k)/2 \end{cases}$$

Evolution of the system (II)

- Encryption: $\mathbf{y} = x(\mathbf{g}) + \sum_{i=1}^{u} \alpha_i \mathbf{K}_i + \mathbf{e}$, where
  - x has q-degree $k - u - 1$
  - $\mathbf{e}$ of rank $t \leq (n - k - W)/2$
  - $\alpha_i \in \mathbb{F}_{q^m}^*$ random for all $i = 1, \ldots, u$
- Decryption:
  - We have

$$\mathbf{yQ} = \left(x(\widetilde{\mathbf{gQ}}) + \sum_{i=1}^{u} \alpha_i P_i(\widetilde{\mathbf{gQ}}) + \widetilde{\mathbf{eQ}} \mid \mathbf{Y}' \right)$$

  - Decode $\widetilde{\mathbf{yQ}}$ in $Gab_k(\widetilde{\mathbf{gQ}}) \Rightarrow (x + \sum_i \alpha_i P_i)(\widetilde{\mathbf{gQ}})$
  - Since $deg_q(x) < k - 1 - u \Rightarrow (\alpha_1, \ldots, \alpha_u)$
  - Since $k - u \leq n - W \Rightarrow x$

Possible attacks

- Decoding attacks: solve system

$$V(\mathbf{y}) = V \circ X(\mathbf{g}) + \sum_{i=1}^{u} V(\alpha_i \mathbf{K}_i), \quad \begin{cases} deg_q(V) = \mathrm{Rk}(\mathbf{e}) \\ deg_q(x) = k - u - 1 \\ \alpha_i \in \mathbb{F}_{q^m} \end{cases}$$

- Structural attacks:
  - Set

$$\mathbf{K} = \begin{pmatrix} \mathbf{K}_1 \\ \vdots \\ \mathbf{K}_u \end{pmatrix} = \begin{pmatrix} P_1(\mathbf{g}) \\ \vdots \\ P_u(\mathbf{g}) \end{pmatrix} + \left(\begin{array}{c|c} \mathbf{0} & \begin{matrix} \mathbf{E}_1 \\ \vdots \\ \mathbf{E}_u \end{matrix} \end{array} \right) \mathbf{Q}^{-1}$$

  - Under some conditions one can apply Overbeck's approach to recover the secret elements

Parameters

Compromise between attacks $\Rightarrow$ not many choices for u

u	$n = m$	k	W	$\mathrm{Rk}(\mathbf{e})$	key size	Rate
3	56	28	16	6	9408	44%
3	54	32	13	4	11664	44%

Open problems

- Are the discussed problems really *NP*-hard ?
- How to improve arithmetic complexity of q-polynomials ?
- Johnson bound for Gabidulin codes and list-decoder ?
- How construct new decodable families of rank metric codes ?
- What changes the use of skew polynomials instead of q-polynomials ?