An evolution of GPT cryptosystem

Pierre Loidreau

DGA MI and IRMAR, Université de Rennes 1

ACCT 2016, June 21st, Albena

Motivations

- Post-Quantum cryptography
  - Multivariate primitives
  - Lattice Based primitives
  - Code based primitives
- Rank metric
  - Smaller keys for a given security target
  - Another alternative to Hamming metric or Euclidian metric based primitives.

Rank metric, [Gab85]

Definition

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

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

- A $[n, k, d]_r$ code: $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, k-dimensional, where $d = \min_{\mathbf{c} \neq \mathbf{0} \in \mathcal{C}} \mathrm{Rk}(\mathbf{c})$
- Singleton property $d - 1 \leq n - k$ (if $n \leq m$)
- $\mathrm{Rk}(\mathbf{e}) = t \Leftrightarrow \exists \mathcal{V} \subset \mathbb{F}_{q^m}$, s.t. $\dim_q(\mathcal{V}) = t$ and $e_i \in \mathcal{V}$, $\forall i$

Principle of rank metric code based cryptography

Key generation

- Private-key
  - $\mathcal{C}$ a $[n, k, d]_r$ t-rank error decodable code over $\mathbb{F}_{q^m}$
  - $L : \mathbb{F}_{q^m}^n \mapsto \mathbb{F}_{q^m}^n$, s.t.
    - L is vector-space isomorphism
    - L is a rank isometry
- Public-key: $\mathcal{C}_{pub} = L^{-1}(\mathcal{C})$.

Process

- Encryption: $\mathbf{y} = \mathbf{c} \in \mathcal{C}_{pub} + \mathbf{e}$, where $\mathrm{Rk}(\mathbf{e}) \leq t$
- Decryption: $L(\mathbf{y}) = L(\mathbf{c}) \in \mathcal{C} + L(\mathbf{e}) \overset{Decode}{\Rightarrow} \mathbf{c}$

Decoding complexities

Consider a *random* $[n, Rn]_r$-code over $\mathbb{F}_{q^m}$, $m \geq n$

- Decoding errors of rank δn, [GRS12]:

$$m^3 q^{\delta R n^2}$$

- Decoding errors of Hamming weight δn:

$$\text{Lee-Brickell} \quad : \quad n^3 \frac{\binom{n}{k}}{\binom{n-\delta n}{k}}$$

For $R < 1/2$, $\approx n^3 q^{n \log_2(q)[H(R)-H(R-\delta)]}$

$\Rightarrow$ Rank metric provides better security/size tradeoff

Gabidulin codes, [Gab85]

Definition (Gabidulin codes)

Let $\mathbf{g} = (g_1, \ldots, g_n) \in (\mathbb{F}_{q^m})^n$, $\mathbb{F}_q$*-l.i.*, $[i] \stackrel{def}{=} q^i$. *Generator matrix of* $Gab_k(\mathbf{g})$ *of the form*

$$\mathbf{G} = \begin{pmatrix} g_1 & \cdots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}$$

- Properties of $\text{Gab}_k(\mathbf{g})$
  - Optimal $[n, k, d]_r$ codes for rank metric: $n - k = d - 1$
  - P-time quadratic decoding up to $t = \lfloor (n-k)/2 \rfloor$
- *Sufficiently* scrambled $\Rightarrow$ McEliece-like cryptosystems.

Rise and fall of GPT system - [GPT91, Ksh07, RGH11, OKN16]

- Linear rank preserving isometries of $\mathbb{F}_{q^m}^n$: $\mathbf{P} \in M_n(\mathbb{F}_q)$
- Since $\mathrm{Gab}_k(\mathbf{g})\mathbf{P} = \mathrm{Gab}_k(\mathbf{gP}) \Rightarrow$ Necessity of scrambling
- But
  1. For any published reparation, always possible to write

$$\mathbf{G}_{pub} = \mathbf{S}_1(\mathbf{X}_1 \mid \underbrace{\mathbf{G}_1}_{Gab_k(\mathbf{g}_1)})\mathbf{P}^*, \ \mathbf{P}^* \in M_n(\mathbb{F}_q)$$

  2. $\Rightarrow$ Stability through Frobenius, for all i,

$$(\mathbf{G}_{pub})^{[i]} = \mathbf{S}_1^{[i]} \left(\mathbf{X}_1^{[i]} \mid \mathbf{G}_1^{[i]}\right) \mathbf{P}^*$$

  3. $\Rightarrow$ Apply Overbeck's like attacks

How to mend it ?

- Find less structured codes for rank metric
  - Use of subfield subcodes ? Not sufficient !
- Find a new way to mask the structure

A novel idea: LRPC codes, [GMRZ13]

- Let $\mathcal{V} \subset \mathbb{F}_{q^m}$ a λ dimensional $\mathbb{F}_q$-subspace
- Let $\mathcal{L} \subset \mathbb{F}_{q^m}^n$, $[n, k, d]_r$-code with parity-check $\mathbf{H}$ of low rank:

$$\mathbf{H} \in \mathcal{V}^{(n-k)\times n} \subset \mathbb{F}_{q^m}^{(n-k)\times n}$$

- Decoding $\mathbf{y} = \mathbf{c} + \mathbf{e}$, $\mathbf{e} \in \mathcal{E}^n$ where $\dim_q(\mathcal{E}) \leq t$
  1. Since $\mathbf{e} \in \mathcal{E}^n \Rightarrow \mathbf{y}\mathbf{H}^t = \mathbf{e}\mathbf{H}^t \subset (\mathcal{E} \cdot \mathcal{V})^{n-k}$
  2. $(\mathcal{E} \cdot \mathcal{V}) \overset{def}{=} < \alpha\beta,\ \alpha \in \mathcal{E},\ \beta \in \mathcal{V} > \Rightarrow \dim_q(\mathcal{E} \cdot \mathcal{V}) \leq t\lambda$
  3. If $t\lambda \leq n - k$, knowing $\mathcal{V} \Rightarrow$ recovers $\mathcal{E}$ from $(\mathcal{E} \cdot \mathcal{V})$

$\Rightarrow$ LRPC based cryptosystem was designed

Mixing the ideas

Weaknesses and strengths

- Gabidulin codes:
  - Advantages: efficient deterministic decoding
  - Drawbacks: too much structured
- LRPC codes:
  - Advantages: not structured
  - Drawbacks: probabilistic decoding with failure $q^{-(n-k-\lambda t)}$

$\Rightarrow$ use rank multiplication to scramble structure of Gabidulin codes

The new cryptosystem

Proposition

Let $\mathcal{V} \subset \mathbb{F}_{q^m}$ *with* $\dim_q(\mathcal{V}) = \lambda$*, and let* $\mathbf{P} \in M_n(\mathcal{V})$*, then*

$$\forall \mathbf{x} \in \mathbb{F}_{q^m}^n, \ \mathrm{Rk}(\mathbf{xP}) \leq \lambda \, \mathrm{Rk}(\mathbf{x})$$

- Private-key:
  - $\mathrm{Gab}_k(\mathbf{g})$
  - $\mathcal{V} =< \alpha_1, \dots, \alpha_\lambda >_q$, λ-dimensional
  - $\mathbf{P} \in M_n(\mathcal{V})$
- Public-key: $\mathcal{C}_{pub} = \mathrm{Gab}_k(\mathbf{g})\mathbf{P}^{-1}$
- Encryption: $\mathbf{y} = \mathbf{c} \in \mathcal{C}_{pub} + \mathbf{e}$, where $\mathrm{Rk}(\mathbf{e}) \leq \lfloor (n-k)/(2\lambda) \rfloor$
- Decryption: $\mathbf{yP} = \mathbf{cP} \in \mathcal{C} + \mathbf{eP}$, where $\mathrm{Rk}(\mathbf{eP}) \leq \lfloor (n-k)/2 \rfloor$

Security arguments

- $\mathrm{Gab}_k(\mathbf{g})\mathbf{P}^{-1} \neq \mathrm{Gab}_k(\mathbf{g}\mathbf{P}^{-1})$: $\mathcal{V}$ not q-stable
- $\mathcal{C}_{pub}$ and $\mathcal{C}_{pub}^{[i]}$, behave independently
- Complexity evaluation: reduce to the difficulty of finding $\mathcal{V}$. Since w.l.o.g. suppose $1 \in \mathcal{V} \to$ loose 1 dimension. Therefore, complexity of finding $\lambda - 1$ dimensional subspaces:

$$\approx q^{m(\lambda-1)-(\lambda-1)^2}$$

Proposition of parameters

q	m	n	k	t	λ	Bits.Struc.Sec	Bits.Dec.Sec	Size
2	96	64	40	4	3	206	139	11.5 KBytes
2	64	64	22	8	3	142	130	7.4 KBytes

- Key-size for classical McEliece: 1 MByte for 128 bits security
- Key-size factor gain: ≈ 90

Perspectives

- Reducing key-size by some structural property
- Thorough study of the security of the system
- Designing additional cryptographic services

References I

E. M. Gabidulin.
Theory of codes with maximal rank distance.
Problems of Information Transmission, 21:1–12, July 1985.

E. M. Gabidulin, A. V. Paramonov and O. V. Tretjakov.
Ideals over non-commutative rings and their application in cryptology.
EUROCRYPT'91.

E. M. Gabidulin, H. Rashwan and B. Honary.
On improving security of GPT cryptosystems.
ISIT 2009.

References II

A. Kshevetskiy.
Security of GPT-like public-key cryptosystems based on linear rank codes.
3rd International Workshop on Signal Design and Its Applications in Communications, 2007. IWSDA 2007.

A. Otmani, H. T. Kalashi and S. Ndjeya.
Improved cryptanalysis of rank metric schemes based on Gabidulin codes.
http://arxiv.org/abs/1602.08549v1.

P. Gaborit, G. Murat, O. Ruatta and G. Zémor.
Low Rank Parity-check codes and their application to cryptography.
International Workshop on Coding and Cryptography, WCC 2013.

P. Gaborit, O. Ruatta and J. Schrek.
On the complexity of rank syndrome decoding problem.
IEEE Trans. on Inf. Theo., 62(2), pages 1006–1019.

References III

H. Rashwan, E. M. Gabidulin and B. Honary.
Security of the GPT cryptosystem and its applications to cryptography.
Security and Communication Networks, 4(8):937-946, 2011.

M. Bianchi, F. Chiaraluce, J. Rosenthal and D. Schipani.
Enhanced Public Key Security for the McEliece Cryptosystem.
Journal of Cryptology, 29(1):1-27, 2016.

A. Couvreur, A. Otmani, J.-P. Tillich and V. Gauthier-Umaña.
A Polynomial-Time Attack on the BBCRS Scheme.
http://arxiv.org/pdf/1501.03736.pdf.