An algebraic approach to the Rank Support Learning problem

Magali BARDET, Pierre BRIAUD

PQCrypto 2021, July 20-22

Code-based cryptography

Decoding problem = decoding a random linear code ...

- In the Hamming metric
  - Well-established encryption schemes (classic McEliece, BIKE).
  - Difficult to construct evolved primitives (Wave : hash-and-sign).
- In the rank metric
  - Encryption (NIST candidates ROLLO, RQC).
  - Seems more flexible.

RSL for more applications in the rank metric

- IBE scheme (broken). [Gab+17]
- Durandal signature scheme. [Ara+19]
  - Adapting Schnorr-Lyubashevsky to the rank metric.

Both based on RSL = generalization of the decoding problem.

[Gab+17] Gaborit et al. "Identity-based Encryption from Rank Metric". CRYPTO 2017.

[Ara+19] Aragon et al. "Durandal: a rank metric based signature scheme". EUROCRYPT 2019.

$\mathbb{F}_{q^m}$-linear codes

$\mathbb{F}_{q^m}/\mathbb{F}_q$ finite field extension of degree m, basis $\mathcal{B} := (\beta_1, \ldots, \beta_m)$.

$\mathbb{F}_{q^m}$-linear code

- $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, dim. k.
- Words $\leftrightarrow$ Matrices in $\mathbb{F}_q^{m \times n}$.

$$\boldsymbol{c} := (c_1, \ldots, c_n) \leftrightarrow \mathbf{Mat}_{\boldsymbol{c}} = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \cdots & c_{m,n} \end{pmatrix}, \text{ where } c_i := \sum_{j=1}^{m} c_{j,i}\beta_j.$$

Support and rank weight for $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$

$$\boxed{\mathrm{Supp}(\boldsymbol{c}) := \langle c_1, \ldots, c_n \rangle_{\mathbb{F}_q}.}$$

$$\boxed{\omega(\boldsymbol{c}) := \dim_{\mathbb{F}_q}(\mathrm{Supp}(\boldsymbol{c})) = \mathrm{rk}\,(\mathbf{Mat}_{\boldsymbol{c}}).}$$

The Rank Decoding problem (RD)

Fixed weight decoding

Given $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ full-rank, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$, find $x \in \mathbb{F}_{q^m}^n$ s.t.

$$\omega(\boldsymbol{y} - \boldsymbol{x}\boldsymbol{G}) := \omega(\boldsymbol{e}) = r, \text{ where } \boldsymbol{e} \text{ is an error.}$$

Syndrome decoding

Given $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ full-rank, a syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and $r \in \mathbb{N}$, find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ s.t.

$$\boldsymbol{e}\boldsymbol{H}^T = \boldsymbol{s} \text{ and } \omega(\boldsymbol{e}) = r.$$

Rank Support Learning problem (RSL)

Rank Support Learning (RSL)

Input: $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ full-rank, N syndromes $\boldsymbol{s}_i \in \mathbb{F}_{q^m}^{(n-k)}$ s.t.

$$\forall i, \exists \boldsymbol{e}_i \in \mathbb{F}_{q^m}^{n}, \ (\boldsymbol{e}_i \boldsymbol{H}^{\mathsf{T}} = \boldsymbol{s}_i, \ \mathrm{Supp}(\boldsymbol{e}_i) = \mathcal{V}),$$

where $\dim_{\mathbb{F}_q}(\mathcal{V}) = r$.

Output: the common support $\mathcal{V}$

This is RD when $N = 1$. How easier when $N \nearrow$?

Previous cryptanalysis

Known attacks

- $\mathbf{N} \geq \mathbf{nr}$: polynomial (linear algebra, [Gab+17]).
- $\mathbf{N} \geq \mathbf{kr}$: subexponential (GB, very overdetermined system, [DAT18]).
- Any RD solver on 1 syndrome . . . the best so far when $N < kr$ (!)

$\rightarrow$ This talk : an attack for any $N < kr$.

[Gab+17] Gaborit et al. "Identity-based Encryption from Rank Metric". CRYPTO 2017.

[Ara+19] Aragon et al. "Durandal: a rank metric based signature scheme". EUROCRYPT 2019.

[DAT18] Debris-Alazard and Tillich. "Two attacks on rank metric code-based schemes: RankSign and an Identity-Based-Encryption scheme". ASIACRYPT 2018.

RSL-Minors modeling

$\forall i,\ \boldsymbol{y}_i \boldsymbol{H}^\mathsf{T} = \boldsymbol{s}_i$ (no weight constraint on $\boldsymbol{y}_i$).

$$\mathcal{C}_{aug} := \mathcal{C} + \langle \boldsymbol{y}_1, \ldots, \boldsymbol{y}_N \rangle_{\mathbb{F}_q} = \mathcal{C} + \langle \boldsymbol{e}_1, \ldots, \boldsymbol{e}_N \rangle_{\mathbb{F}_q} := \mathcal{C} + \mathcal{E} \subset \mathbb{F}_{q^m}^n.$$

Strategy ([Gab+17])

Target : $\boldsymbol{e} \in \mathcal{C}_{aug}, w(\boldsymbol{e}) := w \leq r$ ($\approx q^N$ such words).

$\Rightarrow$ MinRank with $km + N$ matrices, rank w.

$$\boldsymbol{e} := \boldsymbol{x}\boldsymbol{G} + \sum_{i=1}^{N} \lambda_i \boldsymbol{y}_i = (\beta_1, \beta_2, \ldots, \beta_m)\mathbf{Mat}_{\boldsymbol{e}} := (\beta_1, \beta_2, \ldots, \beta_m)\boldsymbol{C}\boldsymbol{R}.$$

(Unknowns $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$, $\lambda_i \in \mathbb{F}_q$, $\boldsymbol{C} \in \mathbb{F}_q^{m \times w}$ and $\boldsymbol{R} \in \mathbb{F}_q^{w \times n}$).

[Gab+17] Gaborit et al. "Identity-based Encryption from Rank Metric". CRYPTO 2017.

RSL-Minors modeling

Multiply by $\boldsymbol{H}^\top$ to remove the $\boldsymbol{xG}$ term:

$$\boldsymbol{eH}^\top := \boldsymbol{s} = \sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i := (\beta_1, \beta_2, \ldots, \beta_m)\boldsymbol{CRH}^\top.$$

The matrix $\boxed{\Delta_{\boldsymbol{H}} := \underbrace{\left(\sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i\right)}_{\boldsymbol{RH}^\top} = \underbrace{\left(\sum_{i=1}^{N} \lambda_i \boldsymbol{y}_i\right)}_{\boldsymbol{R}} \boldsymbol{H}^\top}$

has rank $\leq w$!

System over $\mathbb{F}_{q^m}$ (variables over $\mathbb{F}_q$)

$$\mathcal{F} := \left\{ f = 0 \middle| f \in \mathrm{MaxMinors}(\Delta_{\boldsymbol{H}}) \right\}.$$

$$\#\text{eqs over } \mathbb{F}_{q^m} = \binom{n-k}{w+1}.$$

RSL-Minors modeling

Degree ?

Bilinear in λ_i and in the maximal minors of $\boldsymbol{R}$ ($r_T = |\boldsymbol{R}|_{*,T}$).

$\rightarrow$ Sum of products $\left| \underbrace{\sum_{i=1}^{N} \lambda_i \boldsymbol{y}_i}_{\boldsymbol{R}} \right|_{*,I} \times \left| \boldsymbol{H} \right|_{J,I}$ (Cauchy-Binet formula).

$\rightarrow$ Compute left factors by Laplace expansion along the first row.

RSL-Minors system

$$\mathcal{F}_{ext} := \mathrm{Exp}_{\mathcal{B}}(\mathcal{F}) := \{[\beta_i]f = 0 \mid i \in \{1..m\},\ f \in \mathcal{F}\}.$$

$$\#\text{eqs over } \mathbb{F}_q = m\binom{n-k}{w+1} \quad \#\{\text{monomials } \lambda_i r_T\} = N\binom{n}{w}.$$

Solving the system

1. Restrict the number of solutions !
   $\rightarrow$ Decrease $w \leq r$ and/or shorten $\mathcal{C}_{aug}$.

2. Multiply by monomials in λ_i + linearize at bi-degree $(b, 1)$. (as in [Bar+20])
   $\rightarrow$ Find b ? How many independent eqs ? Syzygies ?

3. Solve the linear system with Strassen/Wiedemann.
   $\rightarrow$ Very few sols, easy to recover the true RSL ones.

[Bar+20] Bardet et al. "Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems". ASIACRYPT 2020.

At bi-degree $(b, 1)$ over $\mathbb{F}_{q^m}$ (system $\mathcal{F}$)

Assumption 1 (cheap)

Let $\boldsymbol{S} := \left(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_N\right) \in \mathbb{F}_{q^m}^{(n-k)\times N}$. We assume that

$$\boxed{\mathrm{Rank}(\boldsymbol{S}_{\{1..n-k-w\},*}) = n - k - w.}$$

Under Assumption 1, leading terms at bi-degree $(1, 1)$ are known.

$\Rightarrow$ Then construct a basis at higher bi-degree.

Theorem 1 (under Assumption 1)

Let $b \geq 1$ and $\mathcal{N}_b := \#\{\text{Lin. Indep. bi-degree } (b, 1)\}$. One has

$$\boxed{\mathcal{N}_b := \sum_{d=2}^{n-k-w+1} \binom{n-k-d}{w-1} \sum_{j=1}^{d-1} \binom{N-j+1+b-2}{b-1}.}$$

Expanding over $\mathbb{F}_q$ (system $\mathcal{F}_{ext}$)

To be solved: $\mathcal{F}_{ext} = \mathrm{Ext}_{\mathcal{B}}(\mathcal{F})$, eqs, sols $\in \mathbb{F}_q$.

Assumption 2

Applying $\mathrm{Ext}_{\mathcal{B}}(.)$ does not add extra linear relations.

When $q = 2$, field equations affect the analysis for $b \geq 2$, i.e.

$$\mathcal{N}_b^{\mathbb{F}_2} := \#\{\text{Lin. Indep. bi-degree } (b,1)\} < \mathcal{N}_b.$$

- Theorem 1 + Assumption 2:
  $\Rightarrow$ Find b to solve by linearization at bi-degree $(b, 1)$.
- Dominant cost : final linear system over $\mathbb{F}_q$.
  $\Rightarrow$ Sparse linear algebra when b large enough.

Cryptographic impact

128-bit parameters constructed w.r.t. Durandal reqs. + [Bar+20].

(m, n, k, r)	Best so far (RD)	$N = k(r-2)$	$N = k(r-1)$
$(277, 358, 179, 7)$	130	**126**	**125**
$(281, 242, 121, 8)$	159	170	**128**
$(293, 254, 127, 8)$	152	172	**125**
$(307, 274, 137, 9)$	339	**187**	**159**

- Improves key-recovery on Durandal.
- The harder the RD instance, the more we might gain ?

Conclusion

- Attack to be considered to design future parameters.
- Precise complexity analysis:
  - #{Lin. Indep. Eqs} is proven (contrary to [Bar+20]).
- Further work:
  - Dealing with the $q = 2$ case.
  - Broader comparison to RD attacks.