On the Security of MinRank

Ludovic Perret
(Jean-Charles Faugère and Françoise Levy-dit-Vehel)

SALSA
LIP6, Université Paris 6 & INRIA Paris-Rocquencourt
Jean-Charles.Faugere@grobner.org, ludovic.perret@lip6.fr

ENSTA/UMA/ALI
levy@ensta.fr

Journées C2 – 2008

Outline

1. MinRank and Related Problems
   - Complexity issues
   - Solving MinRank
2. A Fresh look at Kipnis-Shamir's attack
3. Conclusion and open problems

The MinRank problem

MR

Input : $N, n, k \in \mathbb{N}^*$, $M_0, \ldots, M_k \in \mathcal{M}_{N\times n}(\mathbb{F}_q)$, $r \in \mathbb{N}^*$.
Question : decide if there exists $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ such that :

$$\mathrm{Rk}\left(M_0 - \sum_{i=1}^{k} \lambda_i M_i\right) \leq r.$$

Theorem (Courtois 01)

MR *is NP-Complete.*

Related Problems

Rank decoding over $\mathbb{F}_{q^N}$:

RD: *Input :* $N, n, k \in \mathbb{N}^*,\ G \in \mathcal{M}_{k\times n}(\mathbb{F}_{q^N}),\ y \in \mathbb{F}_{q^N}^n,\ r \in \mathbb{N}^*$.
Question : is there a vector $\mathbf{m} \in \mathbb{F}_{q^N}^k$, such that $e = y - \mathbf{m}G$ has rank $\mathrm{Rk}(e \,|\, \mathbb{F}_q) \leq r$?

Here $\mathrm{Rk}(e \,|\, \mathbb{F}_q) = \mathrm{Rk}(\mathrm{mat}_{\mathcal{B}}(e)),\ \mathcal{B}$ a basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$.

Maximum likelihood decoding over $\mathbb{F}_q$:

MLD: *Input :* $n, k \in \mathbb{N}^*,\ G \in \mathcal{M}_{k\times n}(\mathbb{F}_q)$, $y \in \mathbb{F}_q^n$, and $w \in \mathbb{N}^*$.
Question : is there $\mathbf{m} \in \mathbb{F}_q^k$ s. t. weight of $y - \mathbf{m}G$ is $\leq w$?

Complexity issues

Open Question

RD is NP-Complete ?

A natural reduction

By reduction from MR, i.e. f:

$$\mathrm{MR}(N, n, k, M_0, M_1, \ldots, M_k, w) \mapsto \mathrm{RD}(N, n, k, G, y, w),$$

with :

- $L_i = \mathrm{vect}_{\mathcal{B}}(M_i) \in (\mathbb{F}_{q^N})^n$, for all $i, 1 \leq i \leq k$
- $G = {}^t(L_1, \ldots, L_k)$
- $y = \mathrm{vect}_{\mathcal{B}}(M_0) \in (\mathbb{F}_{q^N})^n$.

The Kernel Attack (Courtois, Goubin)

We consider $\mathrm{MR}(n, k, M_0, \ldots, M_k, r)$, i.e. find $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ such that :

$$\mathrm{Rk}\left(M_0 - \sum_{i=1}^{k} \lambda_i M_i\right) = r.$$

- Set $E_\lambda = M_0 - \sum_{j=1}^{k} \lambda_j M_j$, we have :

  $\dim(\mathrm{Ker} E_\lambda) = n - r \Rightarrow \Pr\{X \in_R \mathbb{F}_q^n \text{ belongs to } \mathrm{Ker} E_\lambda\} = q^{-r}$.
- Choose m vectors $X^{(i)} \in_R \mathbb{F}_q^n,\ i, 1 \leq i \leq m$.
- Solve the system of $m \cdot n$ equations for $(\mu_1, \ldots, \mu_k) \in \mathbb{F}_q^k$,

$$\left(M_0 - \sum_{j=1}^{k} \mu_j M_j\right) X^{(i)} = \mathbf{0}_n,\ \forall i, 1 \leq i \leq m.$$

  if $m = \lceil \frac{k}{n} \rceil$, essentially "only one solution" $\lambda = (\lambda_1, \ldots, \lambda_k)$.
- Complexity : $\mathcal{O}(q^{\lceil \frac{k}{n} \rceil r} k^3)$.

Kipnis-Shamir's attack

Idea

Model MR *as an* MQ *problem.*

- Set $E_\lambda = M_0 - \sum_{j=1}^{k} \lambda_j M_j$, where $(\lambda_1, \ldots, \lambda_k)$ is a solution of MR.
- $\mathrm{Rk}\, E_\lambda = r \;\Leftrightarrow\; \exists (n-r)$ independent vectors in $\mathrm{Ker} E_\lambda$.
- Look for such vectors of the form : $x^{(i)} = (e_i, x_1^{(i)}, \ldots, x_r^{(i)})$, where $e_i \in \mathbb{F}_q^{n-r}$ and $x_j^{(i)}$s are variables. Then :

$$\left(M_0 - \sum_{j=1}^{k} y_j M_j \right) x^{(i)} = \mathbf{0}_n, \ \forall 1 \leq i \leq n-r,$$

  is a quadratic system of $(n-r)n$ equations in $r(n-r)+k$ unknowns.
- We shall call $\mathcal{I}_{\mathrm{KS}}$ the ideal generated by these equations.

The minors method

- Set $E_\lambda = M_0 - \sum_{j=1}^{k} \lambda_j M_j$ and $E_\lambda^{(r')}$ an $r' \times r'$ submatrix of E_λ.
- Write that all $\det(E_\lambda^{(r')}) = 0$, $r' = r + 1$.
- We get a system of $\left(\begin{array}{c} n \\ r' \end{array} \right)$ eqs. of degree r'.

Outline

Properties of KS equations

Theorem

Let $(n, k, M_0, M_1, \ldots, M_k, r)$ be an instance of MinRank. There is a one-to-one correspondence between $\mathcal{S}ol(n, k, M_0, M_1, \ldots, M_k, r)$ – the set of solutions of MinRank – and :

$$V_{\mathbb{F}_q}(\mathcal{I}_{\mathrm{KS}}) = \{\mathbf{z} \in \mathbb{F}_q^{r\cdot(n-r)+k} : f(\mathbf{z}) = 0, \text{for all } f \in \mathcal{I}_{\mathrm{KS}}\}.$$

Properties of KS equations

Proposition

We will suppose that $\mathcal{I}_{\mathrm{KS}}$ is radical, i.e. :

$$\sqrt{\mathcal{I}_{\mathrm{KS}}} = \{f \in \mathbb{F}_q[y_1, \ldots, y_m] : \exists r > 0 \text{ s. t. } f^r \in \mathcal{I}_{\mathrm{KS}}\} = \mathcal{I}_{\mathrm{KS}}.$$

Set $E(y_1, \ldots, y_m) = \sum_{i=1}^{k} y_i M_i - M_0$. Then all the minors of $E(y_1, \ldots, y_m)$ of degree $r' > r$ lie in $\mathcal{I}_{\mathrm{KS}}$.

Proof.

It is clear that all the minors vanish on $V_{\mathbb{F}_q}(\mathcal{I}_{\mathrm{KS}})$. By Hilbert's Strong Nullstellensatz, we get that all the minors of rank $r' > r$ lie in the radical of $\mathcal{I}_{\mathrm{KS}}$. This ideal being radical, it turns out that all those minors lie in $\mathcal{I}_{\mathrm{KS}}$. $\square$

Courtois' authentication scheme

- 3-pass zero-knowledge authentication protocol
- Based on MR
- Provably secure: breaking the scheme is equivalent to either finding a collision for the hash function or solving the underlying instance of MR.
- Communication complexity: 1075 bits/round for $n = 6$, $q = 65521$. (then, PK: 735 bits, SK: 160 bits).
- Security: best attack on MR : 2^{106}.

Zero-dim solving

- Compute a DRL Gröbner basis
  - Buchberger's algorithm (1965)
  - F_4 (J.-C. Faugère, 1999)
  - F_5 (J.-C. Faugère, 2002)

  $\Rightarrow$ For a zero-dim system :

$$\mathcal{O}\left(m^{3 \cdot d_{reg}}\right),$$

d_{reg} being the max. degree reached during the computation.

- Compute a LEX Gröbner basis by a FGLM change of ordering

Courtois' Authentication Scheme – Challenges

- A : $\mathbb{F}_{65521}, k = 10, n = 6, r = 3$ (18 eq., and 18 variables)
  - F_5+ FGLM : 1 minute (30 s.+30 s.), nb_sol= 982, $d_{reg} = 5$
- B : $\mathbb{F}_{65521}, k = 10, n = 7, r = 4$ (21 eq., and 21 variables)
  - F_5+ FGLM : $3764s.+2580s.$, nb_sol= 4116, $d_{reg} = 6$
- C : $\mathbb{F}_{65521}, k = 10, n = 11, r = 8$ (33 eq., and 33 variables)
- D : $\mathbb{F}_2, k = 81, n = 11, r = 10$

Theoretical Complexity

Remark

The ideal $\mathcal{I}_{\mathrm{KS}}$ is bi-homogeneous.

Theorem

Let $r' = n - r$ is constant, we can solve in polynomial time the minRank $\left(k = r'^2, n, r = n - r'\right)$ problem using Gröbner bases computation; a bound for the number of solutions in the algebraic closure of $\mathbb{K}$ is given by $\#\mathcal{S}ol \le \binom{n}{r'}^{r'}$; a complexity bound of the attack is given by

$$\mathcal{O}\left(n^{3\,r'^2}\right).$$

(k, n, r)	$(9, 6, 3)$	$(9, 7, 4)$	$(9, 11, 8)$
$\#\mathcal{S}ol$ (MH Bezout bound)	8000	42875	$2^{22.1}$
Complexity bound $(\#Sol)^3$	$2^{38.9}$	$2^{46.2}$	$2^{66.3}$

Conclusion and open problems

- Find alternative/better modellings for MinRank by means of eq. systems.
- How to exploit MR for coding theory pbs.?