Improvement of Algebraic attacks for solving superdetermined Minrank instances

Magali Bardet, Manon Bertin

LITIS, University of Rouen Normandie, France

PQCrypto 2022,
September 29, 2022

MinRank

DAGS

Conclusion

The MinRank problem in general

Computational MinRank

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant r.$$

- This is exactly the decoding problem for matrix codes,
- NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.

Modeling MR: $\text{Rank}(M_{\vec{x}}) \leqslant r$ with $M_{\vec{x}} = \sum_{i=1}^{K} x_i M_i$

- Kipnis-Shamir modeling 1999 (hyp: last r columns of $M_{\vec{x}}$ are independent)

$$M_{\vec{x}} \begin{pmatrix} I_{n-r} \\ -R \end{pmatrix} = 0_{m\times(n-r)}, \qquad R \in \mathbb{F}_q^{r\times(n-r)} \qquad \text{(KS)}$$

- Minors modeling (Analysis by Faugère-Safey El Din-Spaenlehauer 2010)

$$\text{Minors}_{r+1}(M_{\vec{x}}) = 0 \qquad \text{(Minors)}$$

Hyp: it is sufficient to consider $|M_{\vec{x}}|_{J,T} = 0$ with $\{n-r+1..n\} \subset T$.

- Support Minors modeling 2020, $\vec{m}_j = (M_{\vec{x}})_{j,*}$

$$\text{Minors}_{r+1}\begin{pmatrix} & \vec{m}_j \\ R & I_r \end{pmatrix} = 0 \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

Ideals and Algebraic varieties

Links between the 3 modelings? (no hypothesis on the parameters)

Proposition

$$\langle \mathrm{KS} \rangle = \langle \mathrm{SM} \rangle$$
$$\langle \mathrm{Minors} \rangle \subseteq \langle \mathrm{KS} \rangle \cap \mathbb{F}_q[\vec{\boldsymbol{x}}]$$

Ideals and Algebraic varieties

Lemma

KS is included in SM.

Proof.

For all $j \in \{1..m\}$, $\ell \in \{1..n-r\}$ we have (Laplace expansion along the first row):

$$\left|\begin{pmatrix} & \vec{\boldsymbol{m}}_j \\ \boldsymbol{R} & \boldsymbol{I}_r \end{pmatrix}\right|_{*,\{\ell\}\cup\{n-r+1..n\}} = (\boldsymbol{M}_{\vec{\boldsymbol{x}}})_{j,\ell} - \sum_{i=1}^{r} (\boldsymbol{M}_{\vec{\boldsymbol{x}}})_{j,i+n-r} \boldsymbol{R}_{i,\ell} = \left(\boldsymbol{M}_{\vec{\boldsymbol{x}}} \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} \right)_{j,\ell}.$$

□

Lemma

$\langle KS \rangle$ contains Minors.

Proof.

- We write any $\boldsymbol{A} = \begin{pmatrix} \overset{n-r}{\leftrightarrow} & \overset{r}{\leftrightarrow} \\ \boldsymbol{A}^1 & \boldsymbol{A}^2 \end{pmatrix}$
- $vec_{col}(\boldsymbol{A})$ is a vector formed by all columns of $\boldsymbol{A}$ put one after the other,
- $\vec{\boldsymbol{v}}\boldsymbol{A}\vec{\boldsymbol{e}}^{\mathsf{T}} = \vec{\boldsymbol{v}}\left(\sum_i e_i \boldsymbol{A}_{*,i}\right) = (\vec{\boldsymbol{e}} \otimes \vec{\boldsymbol{v}})vec_{col}(\boldsymbol{A})$

Let $\boldsymbol{V}_J(\boldsymbol{M_{\vec{x}}}^2) = (\underbrace{0}_{j \notin J}, \dots, \underbrace{\left|\boldsymbol{M_{\vec{x}}}^2\right|_{J \setminus \{j\},*}}_{j \in J})_{j=1..m}$ for any $J \subset \{1..m\}$ of size $r+1$.

Then $\boldsymbol{V}_J(\boldsymbol{M_{\vec{x}}}^2)\vec{\boldsymbol{a}}^{\mathsf{T}} = \left|\vec{\boldsymbol{a}}^{\mathsf{T}}\boldsymbol{M_{\vec{x}}}^2\right|_{J,*}$ for any $\vec{\boldsymbol{a}}$, hence $\boldsymbol{V}_J(\boldsymbol{M_{\vec{x}}}^2)\boldsymbol{M_{\vec{x}}}^2 = 0$.

For any $1 \leqslant i \leqslant n-r$ we get

$$\vec{\boldsymbol{e}}_i \otimes \boldsymbol{V}_J(\boldsymbol{M_{\vec{x}}}^2) \underbrace{vec_{col}\left(\boldsymbol{M_{\vec{x}}}\begin{pmatrix}\boldsymbol{I}_{n-r} \\ -\boldsymbol{R}\end{pmatrix}\right)}_{=vec_{col}(\boldsymbol{M_{\vec{x}}}^1 - \boldsymbol{M_{\vec{x}}}^2\boldsymbol{R}) \in \mathrm{KS}} = \underbrace{\boldsymbol{V}_J(\boldsymbol{M_{\vec{x}}}^2)\boldsymbol{M_{\vec{x}}}^1\vec{\boldsymbol{e}}_i^{\mathsf{T}}}_{=\left|\boldsymbol{M_{\vec{x}}}\right|_{J,\{i\}\cup\{n-r+1..n\}}} - \underbrace{\boldsymbol{V}_J(\boldsymbol{M_{\vec{x}}}^2)\boldsymbol{M_{\vec{x}}}^2}_{=0}\boldsymbol{R}\vec{\boldsymbol{e}}_i^{\mathsf{T}}$$

Lemma

$\langle KS \rangle$ contains SM.

Proof.

- $(\vec{e}_\ell \otimes \boldsymbol{Y}) vec_{row}(\boldsymbol{X}) = vec_{row}(\vec{e}_\ell \boldsymbol{X} \boldsymbol{Y}^\mathsf{T}) = vec_{row}(\boldsymbol{X}_{\ell,*} \boldsymbol{Y}^\mathsf{T})$
- $\vec{a} \boldsymbol{V}_J(\boldsymbol{M}^\mathsf{T})^\mathsf{T} = \left| \begin{pmatrix} \vec{a} \\ \boldsymbol{M} \end{pmatrix} \right|_{J,*}$ for any $\vec{a}$

For any $1 \leqslant \ell \leqslant m$ and $J \subset \{1..n-r\}$ of size $r+1$ we get

$$(\vec{e}_\ell \otimes \boldsymbol{V}_J(\boldsymbol{R}^\mathsf{T})) \underbrace{vec_{row}\left(\boldsymbol{M}_{\vec{x}} \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix}\right)}_{\in \mathrm{KS}} = (\boldsymbol{M}_{\vec{x}})_{\ell,*} \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} \boldsymbol{V}_J(\boldsymbol{R}^\mathsf{T})^\mathsf{T}$$

$$= \left| \begin{pmatrix} (\boldsymbol{M}_{\vec{x}}{}^1)_{\ell,*} \\ \boldsymbol{R} \end{pmatrix} \right|_{*,J}$$

$\square$

Lemma
$\langle KS \rangle$ contains SM.

Proof.
- $(\vec{\boldsymbol{e}}_\ell \otimes \boldsymbol{Y})vec_{row}(\boldsymbol{X}) = vec_{row}(\vec{\boldsymbol{e}}_\ell \boldsymbol{X}\boldsymbol{Y}^\top) = vec_{row}(\boldsymbol{X}_{\ell,*}\boldsymbol{Y}^\top)$
- $\vec{\boldsymbol{a}}\boldsymbol{V}_J(\boldsymbol{M}^\top)^\top = \left|\begin{pmatrix}\vec{\boldsymbol{a}}\\ \boldsymbol{M}\end{pmatrix}\right|_{J,*}$ for any $\vec{\boldsymbol{a}}$

For any $1 \leqslant \ell \leqslant m$ and $J \subset \{1..n-r\}$ of size $d+1$ and $T \subset \{1..r\}, \#T = d$, $J' = J \cup ((\{1..r\} \setminus T) + n - r)$, $\#J' = r+1$ we get

$$(\vec{\boldsymbol{e}}_\ell \otimes \boldsymbol{V}_J({\boldsymbol{R}^\top}_{*,T}))\underbrace{vec_{row}\left(\boldsymbol{M}_{\vec{\boldsymbol{x}}}\begin{pmatrix}\boldsymbol{I}_{n-r}\\ -\boldsymbol{R}\end{pmatrix}\right)}_{\in \mathrm{KS}} = (\boldsymbol{M}_{\vec{\boldsymbol{x}}})_{\ell,*}\begin{pmatrix}\boldsymbol{I}_{n-r}\\ -\boldsymbol{R}\end{pmatrix}\boldsymbol{V}_J({\boldsymbol{R}^\top}_{*,T})^\top$$

$$= \left|\begin{pmatrix}(\boldsymbol{M}_{\vec{\boldsymbol{x}}})_{\ell,*}\\ \boldsymbol{R} \quad \boldsymbol{I}_r\end{pmatrix}\right|_{*,J'}$$

□

Computational point of view

KS and SM produce the same ideal, not the same computations.

Gröbner basis computation on KS with the Normal selection strategy

- Eq. SM are produced from KS by multiplying by $\boldsymbol{R}$ variables at degree $(1, r+1)$ in $\vec{\boldsymbol{x}}, \boldsymbol{R}$ after a degree fall.

Gröbner basis computation on SM with the Normal selection strategy

- Eq. KS are included in SM, $\rightarrow$ many syzygies when multiplying by monomials in $\boldsymbol{R}$.
- When multiplying by monomials in $\vec{\boldsymbol{x}}$ of degree r, we have degree falls and equations of degree $(r+1, 0)$ (Minors).

$\rightarrow$ compute with SM, but multiply only by $\vec{\boldsymbol{x}}$ variables. Expect regular behavior up to degree $r+1$.

Solving SM with the Plücker coordinates

Equations, $0 \leqslant d \leqslant r$, $\#\mathscr{E}(d) = m\binom{n-r}{d+1}\binom{r}{d}$

$$\mathscr{E}(d) \triangleq \left\{ E_{J,T,\ell} \triangleq \vec{\boldsymbol{e}}_\ell \boldsymbol{M}_{\vec{\boldsymbol{x}}} \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{R} \end{pmatrix} \boldsymbol{V}_J(\boldsymbol{R}_{T,*})^\mathsf{T} : \begin{smallmatrix} \forall J \subset \{1..n-r\}, \#J = d+1, \\ \forall T \subset \{1..r\}, \#T = d, \\ \forall \ell \in \{1..m\} \end{smallmatrix} \right\}.$$

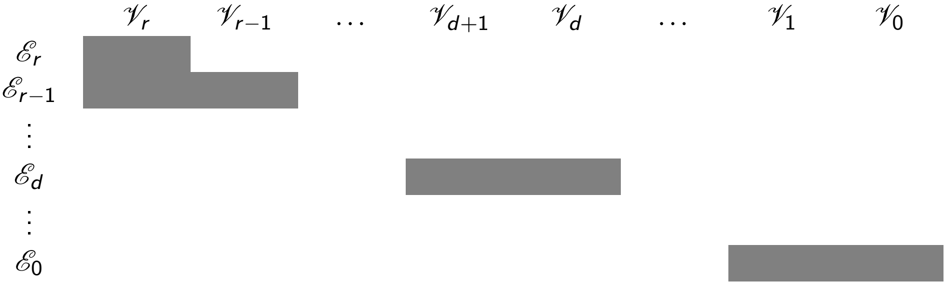
$$E_{J,T,\ell} = \left| \begin{pmatrix} \vec{\boldsymbol{m}}_\ell \\ \boldsymbol{R} \ \boldsymbol{I}_r \end{pmatrix} \right|_{*,T'} \quad \text{with } T' = J \cup (\{n-r+1..n\} \setminus (T+n-r)) \subset \{1..n\}$$

$$= \sum_{s \notin T} \left(\sum_{i=1}^{K} (\boldsymbol{M}_i^2)_{\ell,s} x_i \right) |\boldsymbol{R}|_{T \cup \{s\}, J} + \sum_{j \in J} \left(\sum_{i=1}^{K} (\boldsymbol{M}_i^1)_{\ell,j} x_i \right) |\boldsymbol{R}|_{T, J \setminus \{j\}}.$$

Variables, $0 \leqslant d \leqslant r$, $\#V(d) = K\binom{n-r}{d}\binom{r}{d}$

$$\mathscr{V}(d) \triangleq \{x_i |\boldsymbol{R}|_{T,J}\}_{i=1..K, \#J=d, \#T=d}, \qquad \mathscr{V}(r+1) \triangleq \emptyset.$$

Linearization: shape of the Macaulay matrix



- Degree fall: whenever $\#\mathscr{E}_d \geqslant \#\mathscr{V}_{d+1}$, i.e. $m(d+1) \geqslant K(r-d)$. $\rightarrow$ superdetermined MinRank instances
- End of computation (1 sol): whenever $\#\mathscr{E}_d \geqslant \#\mathscr{V}_{d+1} + \#\mathscr{V}_d - 1$.
- End of computation (1 sol): whenever $\sum_{d=0}^{r} \#\mathscr{E}_d \geqslant \sum_{d=0}^{r} \#\mathscr{V}_d - 1$, i.e. $m\binom{n}{r+1} \geqslant K\binom{n}{r} - 1$. Almost $m(n-r) \geqslant K(r+1)$
- Better linear exponent than for a random matrix.

Improvements

When linearization works too well:

- if $m\binom{n}{r+1} \gg K\binom{n}{r} - 1$, consider "punctured" codes (i.e. $n' < n$ columns) (but keep 1 solution).

When linearization does not work: $m\binom{n}{r+1} < K\binom{n}{r} - 1$, almost $m(n-r) < K(r+1)$

- use hybrid approach:
  - perform exhaustive search on k variables $\vec{\boldsymbol{x}}$ to get $m\binom{n}{r+1} \geqslant (K-k)\binom{n}{r}$,
  - perform exhaustive search on a columns of $\boldsymbol{R}$ to get $m\binom{n-a}{r+1} \geqslant (K-ma)\binom{n-a}{r} - 1$, almost $m(n-r) \geqslant K(r+1) - mar$ (we also get ma linear equations in $\vec{\boldsymbol{x}}$, see `https://arxiv.org/abs/2208.05471`!)
- Solve SM at higher degree b (multiplication by $\vec{\boldsymbol{x}}$ only).

Numerical values compared to Verbel et all, PQCrypto 2019

m	n	K	r	$\frac{m(n-r)}{K(r+1)}$	n_{eq}	n_{vars}	n_{rows} in PQcrypto 19
10	10	10	2	2.6	1,200	450	1,530
10	5	10	2	1	100	100	
10	10	10	3	1.75	2,100	1,200	20,240
10	7	10	3	1	350	350	
10	10	10	4	1.2	2,520	2,100	38,586
10	9	10	4	1	1,260	1,260	
10	10	10	5	**0.8**	2,100	2,520	341,495
10	10	10	5	$b=2$	14,400	13,860	
10	10	10	6	$b=6$	427,350	420,420	$> 2,035,458$

Table: Size of matrices on SM for a minrank instance with $K=10$ matrices of size $m \times n$, for various r. n can be decreased by puncturing the matrices to get a speedup. The results at $b=1$ have been verified experimentally on random instances.

Attack on DAGS by Barelli and Couvreur 2018

Magali Bardet, Manon Bertin

MinRank
DAGS
Conclusion

DAGS Scheme

- KEM,
- quasi-dyadic alternant codes,
- submitted to the first round of the NIST PQ standardization process,
- attack by Barelli and Couvreur (Asiacrypt 2018): finding a secret code,
- it's a Minrank problem!

DAGS attack as a Minrank problem

Find a sub-code of the invariant public code such that:

$$\begin{pmatrix} \boldsymbol{I}_d & \boldsymbol{U} \end{pmatrix} \boldsymbol{G}_{inv} \star \boldsymbol{H}_{pub} \cdot \boldsymbol{V}^{\mathsf{T}} = 0.$$

with

- $\boldsymbol{U} \in \mathbb{F}^{(k_0-c)\times c}$,
- $\boldsymbol{G}_{inv} = (\boldsymbol{I}_{k_0} \; \boldsymbol{G}) \otimes \mathbb{1}_{2^\gamma}$ and $\boldsymbol{G} \in \mathbb{F}_{q^2}^{k_0\times(n_0-k_0)}$ public invariant matrix,
- $\boldsymbol{H}_{pub} = \begin{pmatrix} * & \boldsymbol{I}_{n_0-k_0} \otimes (1, 0_{2^\gamma}) \end{pmatrix}$ is a compact form of the public parity-check matrix,
- $\boldsymbol{V} = \vec{\tau} \otimes \mathbb{1}_{2^\gamma} + \sum_{i=1}^{\gamma-1} b_i \mathbb{1}_{n_0} \otimes \vec{\boldsymbol{e}}_i \in \mathbb{F}^{2^\gamma(n_0)}$ is a vector of unknowns $\vec{\tau} = (\tau_1, \dots, \tau_{n_0})$ and $(b_1, \dots, b_{\gamma-1})$.

Minrank version

$$\left(\sum_{i=1}^{k_0} \tau_i \boldsymbol{M}_i + \sum_{j=k_0+1}^{n_0-1} \tau_j \boldsymbol{M}_j + \sum_{i=1}^{\gamma-1} b_i \boldsymbol{H}_i\right) \begin{pmatrix} \boldsymbol{I}_{k_0-c} \\ \boldsymbol{U}^\mathsf{T} \end{pmatrix} = 0 \qquad (1)$$

$$\text{with } \boldsymbol{M}_i = \begin{pmatrix} 0_{i-1} & (\boldsymbol{G}_{\{i\},*})^\mathsf{T} & 0_{k_0-i} \end{pmatrix} \; \forall 1 \leqslant i \leqslant k_0$$

$$\boldsymbol{M}_{j+k_0} = \begin{pmatrix} 0_{j-1} \\ (\boldsymbol{G}_{*,\{j\}})^\mathsf{T} \\ 0_{n_0-k_0-j} \end{pmatrix} \; \forall 1 \leqslant j \leqslant n_0 - k_0$$

$$\boldsymbol{H}_i = \left(\boldsymbol{H}_{pub}(\boldsymbol{I}_{n_0} \otimes \vec{\boldsymbol{e}}_i{}^\mathsf{T})\right)_{*,\{1..k_0\}} \; \forall 1 \leqslant i \leqslant \gamma - 1$$

Non generic matrices

Proposition

For the DAGS minrank modeling, the part of the Macaulay matrix associated to rows $\mathscr{E}(d)$ and columns $\mathscr{V}(d+1)$ has

- $(n_0 - k_0)\binom{k_0-c}{d+1}\binom{c}{d}$ *rows,*
- $(n_0 - k_0 - 1 + c + \gamma - 1)\binom{k_0-c}{d+1}\binom{c}{d+1}$ *columns,*
- *rank* $\min\left(N_{rows}, \binom{k_0-c}{d+1}\left((n_0-k_0)\binom{c-1}{d} + \binom{c}{d+1}d\right)\right)$.

Reducing the number of variables: puncturing the code on a_0 columns $\rightarrow$ k_0 replaced by $k_0 - a_0$

Optimal attack on DAGS parameters

Security Level	q	n_0	k_0	γ	c	$k_0 - a_0 - c$	Matrix size	Rank	Time
DAGS_1 (128)	2^5	52	26	4	4	4	1456×2520	1322	3.5s
DAGS_3 (192)	2^6	38	16	4	4	5	2772×4284	2540	8.8s
DAGS_5 (256)	2^6	33	11	2	2	3	220×310	194	0.0s

Table: DAGS original sets of parameters, optimal attack, SM modeling

Conclusion

- better understanding of the algebraic systems associated to the MinRank problem, and why SM can perform better than KS or Minors,
- Plücker coordinates $r_T \leftrightarrow |\boldsymbol{R}|_{*,J}$,
- It is possible to use Minrank to attack cryptosystems in Hamming code-based crypto!

Acknowledgments

This work was supported by the project:

CBCRYPT
(ANR-17-CE39-0007)