Rank Analysis of Cubic Multivariate Cryptosystems

John Baena[1] Daniel Cabarcas[1] Daniel Escudero[2] Karan Khathuria[3] Javier Verbel[1]

April 10, 2018

[1]Universidad Nacional de Colombia, Colombia

[2]Aarhus University, Denmark

[3]University of Zurich, Switzerland

Motivation

HFE Cryptosystem

- $\mathbb{F}$ a finite prime field of size q.
- $\mathbb{K}$ field extension of degree n of $\mathbb{F}$.
- $\phi : \mathbb{K} \to \mathbb{F}^n$ vector space isomorphism.
- $\mathcal{F}(X) = \sum \alpha_{i,j} X^{q^i + q^j} \in \mathbb{K}[X]$
- S, T linear transformations $\mathbb{F}^n \to \mathbb{F}^n$.

Secret Key

$\mathcal{F}$, S and T.

Public Key

$P = T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$, which is given by multivariate **quadratic** polynomials $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$.

Encryption Evaluation at these polynomials

Decryption Inverting P ($\mathcal{F}$ is taken as a low degree polynomial)

Min-Rank Attack (in a nutshell)

1. A symmetric matrix $(\alpha_{i,j})_{i,j}$ can be associated to $\mathcal{F}$
2. This matrix has low rank due to the fact that $\mathcal{F}$ has low degree
3. This rank defect is reflected in P as an instance of the so-called Min-Rank problem
4. This instance can be solved by practical means
5. The solution yields valuable information that can be used to recover an equivalent secret key.

- It has been proven that this vulnerability also has a negative impact in the degree of regularity of the system.

The attack seems to require a quadratic setting

- Otherwise no symmetric matrix could be associated to $\mathcal{F}$

Countermeasure?

Take the same construction, but with

$$\mathcal{F}(X) = \sum_{0 \le i \le j \le k \le n-1} \alpha_{i,j,k} X^{q^i + q^j + q^k}.$$

(low degree is still needed for decryption!)

Now the public key is given by **cubic** multivariate polynomials $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$.

Differential attack

Consider the differential $D_{\mathbf{a}}P(\mathbf{x}) = P(\mathbf{x}+\mathbf{a}) - P(\mathbf{x}) - P(\mathbf{a})$.

- This differential is composed of quadratic multivariate polynomials. Let P' be the quadratic homogeneous part.
- We have that $P' = T \circ \phi \circ \mathcal{F}' \circ \phi^{-1} \circ S$, where $\mathcal{F}'$ is the quadratic homogeneous part of $D_a\mathcal{F}(X)$.

The bad news

$\mathcal{F}'$ has the same (low) degree as $\mathcal{F}$, so P' is an instance of quadratic HFE, with the same S and T, which is vulnerable to the Min-Rank attack.

Our Contributions

- We introduce a cubic version of the Min-Rank problem and show how to solve it using natural extensions from the KS modelling.
- We show, experimentally, that taking differentials does not necessarily make the problem easier (as it did in cubic HFE).
- We discuss the implications of a cubic rank defect in the direct algebraic attack.
- We show that cubic big field constructions with a low-rank central polynomial are vulnerable to the cubic Min-Rank attack.

Related work

- Moody, Perlner, and Smith-Tone do a rank analysis of the cubic ABC scheme.[1][2]
  - Taking differentials reduces the rank significantly, which allows for a quadratic Min-Rank attack.
  - Their work avoids discussing the rank of cubic polynomials by focusing on the differentials

[1] Dustin Moody, Ray Perlner, and Daniel Smith-Tone. "Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme". In: *Selected Areas in Cryptography – SAC 2016*. 2017.

[2] Dustin Moody, Ray Perlner, and Daniel Smith-Tone. "Improved Attacks for Characteristic-2 Parameters of the Cubic ABC Simple Matrix Encryption Scheme". In: *Post-Quantum Cryptography*. 2017.

Cubic Min-Rank Attack

Definition

Let $A \in \mathbb{F}^{n\times n\times n}$ be a three-dimensional matrix, we define the **rank** of A as the minimum number of summands r required to write A as

$$A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i \otimes \mathbf{w}_i,$$

where $\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}_i \in \mathbb{F}^n$. We denote this number by $\mathrm{Rank}(A)$.

- The matrix $\mathbf{u} \otimes \mathbf{v} \otimes \mathbf{w}$ is defined so that its entry (i, j, k) is given by $u_i v_j w_k$.

- Generalizes the concept of rank for two-dimensional matrices
- It is not trivial to determine the rank of a three-dimensional matrix
    - In fact, the problem is NP-hard, along with many other problems related to three-dimensional rank
- It is not easy to generate three-dimensional matrices with a desired rank
- Determining the maximum rank attainable by a $n \times n \times n$ matrix remains an open question
    - It is known that this maximum lies between $\frac{n^2}{3}$ and $\frac{3n^2}{4}$

Definition (Cubic Min-Rank Problem)

Given $M_1, \ldots, M_\kappa \in \mathbb{F}^{n \times n \times n}$, determine whether there exist $\lambda_1, \ldots, \lambda_\kappa \in \mathbb{F}$ such that the rank of $\sum_{i=1}^{\kappa} \lambda_i M_i$ is less or equal to r.

- Same definition as in the two-dimensional case but with three-dimensional matrices and using the extended concept of rank.

Solving the cubic Min-Rank problem

Theorem (Characterization of rank[3])

The rank of a matrix $A \in \mathbb{F}^{n \times n \times n}$ *is the minimal number* r *of rank one matrices* $S_1, \ldots, S_r \in \mathbb{F}^{n \times n}$*, such that, for all slices*[4] $A[i, \cdot, \cdot]$ *of* A*,* $A[i, \cdot, \cdot] \in \mathrm{span}(S_1, \ldots, S_r)$*.*

- Analog in two-dimensional case: the rank is the minimum number of vectors required to span the row space (or the column space).
    - This is the characterization of rank used in the quadratic KS modelling.

[3] Joseph M Landsberg. *Tensors: geometry and applications*.

[4] $A[i, \cdot, \cdot]$ is the two-dimensional matrix whose entry (j, k) is given by $A[i, j, k]$

Generalization of KS modelling

- Let $A = \sum_{i=1}^{\kappa} \lambda_i M_i$.
- Write $S_i = \mathbf{u}_i \mathbf{v}_i^T$ for some *unknown* vectors $\mathbf{u}_i, \mathbf{v}_i \in \mathbb{F}^n$.
- We force the property $A[i, \cdot, \cdot] \in \mathrm{span}(S_1, \ldots, S_r)$:

$$\sum_{j=1}^{r} \alpha_{ij} \mathbf{u}_j \mathbf{v}_j^T = A[i, \cdot, \cdot], \text{ for } i = 1, \ldots, n.$$

- We get a system of cubic equations

Variables $r(2n) + rn + \kappa$ (entries of the vectors above + linear combination coefficients + λ_i)

Equations n^3 (n equations of $n \times n$ matrices)

If $r \ll n$ we can do much better

- It is very likely that $A[1,\cdot,\cdot],\dots,A[r,\cdot,\cdot]$ are linearly independent, so

$$\operatorname{span}(S_1,\dots,S_r) = \operatorname{span}(A[1,\cdot,\cdot],\dots,A[r,\cdot,\cdot]).$$

- We force the condition $A[i,\cdot,\cdot] \in \operatorname{span}(A[1,\cdot,\cdot],\dots,A[r,\cdot,\cdot])$ by

$$\sum_{j=1}^{r} \alpha_{ij} A[j,\cdot,\cdot] = A[i,\cdot,\cdot], \text{ for } i = r+1,\dots,n.$$

- We get a system of $n^2(n-r)$ quadratic equations in $(n-r)r+\kappa$ variables
  - Easier system than the system obtained with the quadratic KS modelling.

Differentials

Differentials

What is the expected rank of the quadratic part of the differential $D_{\mathbf{a}} f(\mathbf{x}) = f(\mathbf{x} + \mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a})$, where $f \in \mathbb{F}[\mathbf{x}]$ is a random homogeneous cubic polynomial of rank r?

Main problem

How to generate random polynomials of a specific rank r?

Definition

We define the symmetric rank of $S \in \mathbb{F}^{n \times n \times n}$ as the minimum number of summands s required to write S as

$$S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i,$$

where $\mathbf{u}_i \in \mathbb{F}^n$, $t_i \in \mathbb{F}$. We denote this number by $\mathrm{SRank}(S)$.

- It is clear that, in general, $\mathrm{Rank}(S) \leq \mathrm{SRank}(S)$.
- $\mathrm{SRank}(S) < \infty$ if $|\mathbb{F}| \geq 3$.

Proposition

Let $f \in \mathbb{F}[\mathbf{x}]$ be a homogeneous cubic polynomial. If g is the quadratic homogeneous part of $Df_{\mathbf{a}}(\mathbf{x})$, then $\mathrm{Rank}(g) \leq \mathrm{SRank}(f)$.

Proof.

If $f(\mathbf{x}) = \sum_{i=1}^{r} t_i u_i(\mathbf{x}) u_i(\mathbf{x}) u_i(\mathbf{x})$, then for any $\mathbf{a} \in \mathbb{F}^n$ the quadratic part of $Df_{\mathbf{a}}(\mathbf{x})$ is $\sum_{i=1}^{r} 3 t_i u_i(\mathbf{a}) u_i(\mathbf{x}) u_i(\mathbf{x})$. □

Kruskal Rank

$\text{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_m)$: maximum integer k such that any subset of $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ of size k is linearly independent.

Theorem (Kruskal Theorem)

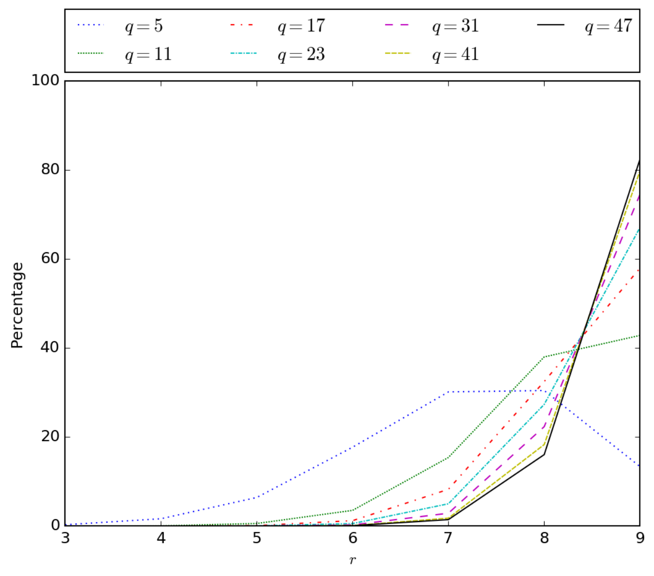
If $A = \sum_{i=1}^{r} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$ *and*

$$2r + 2 \leq \text{KRank}(t_1\mathbf{u}_1, \ldots, t_r\mathbf{u}_r) + 2 \cdot \text{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_r),$$

then $\text{Rank}(A) = r$.

- To generate matrices of rank r, pick $\mathbf{u}_1, \ldots, \mathbf{u}_r \in \mathbb{F}^n$ and $t_1, \ldots, t_r \in \mathbb{F} - \{0\}$ at random.

r = 9, n = 20



$q = 5$
$q = 11$
$q = 17$
$q = 23$
$q = 31$
$q = 41$
$q = 47$
Percentage
100
80
60
40
20
0
3
4
5
6
7
8
9
r

Algebraic Attack

The complexity of performing a direct algebraic attack (via Groebner bases) is upper bounded by

$$O\left(n^{\omega\frac{r(q-1)+5}{2}}\right),$$

where $2 \leq \omega \leq 3$ is a linear algebra constant.

- Polynomial in n if r and q are constant.
- Super-polynomial in n if r grows with n.[5]

[5] This is still an upper bound on the complexity of the attack!

Low rank big field constructions

- Let $\mathcal{F} \in \mathbb{K}[X]$ be a homogeneous weight 3 polynomial given by

$$\mathcal{F}(X) = \sum_{1 \leq i,j,k \leq n} \alpha_{i,j,k} X^{q^{i-1}+q^{j-1}+q^{k-1}}$$

- Consider the matrix $A = (\alpha_{i,j,k})_{i,j,k} \in \mathbb{F}^{n \times n \times n}$.
- Suppose that A has low rank r (e.g. HFE-like construction).
- Let A_i be the three-dimensional matrix representing the i-th polynomial of the public key $T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$.

- Consider the trilinear form $\mathcal{T} : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ given by

$$\mathcal{T}(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1 \le i,j,k \le n} \alpha_{i,j,k} \cdot (\beta_i \delta_j \gamma_k).$$

Theorem

There exist $\lambda_i \in \mathbb{K}$ such that $\sum_{i=1}^{n} \lambda_i A_i = A'$, where A' is the three-dimensional matrix representing the trilinear form $\mathcal{T} \circ (\Delta S)$.[6]

- We can prove that $\text{Rank}(A') \le \text{Rank}(A)$
- We obtain an instance of the cubic Min-Rank problem
- Equivalent secret keys

[6] $\Delta \in \mathbb{K}^{n \times n}$ is a matrix associated to the field extension $\mathbb{K}$ over $\mathbb{F}$

Conclusions

- Rank weaknesses are still present in the cubic setting
- Instances of the cubic Min-Rank problem can be solved
    - More efficiently than in the quadratic setting for $r \ll n$.
    - Solving a cubic system for $r \geq n$.
- Taking differentials does not allow, in general, to transform the problem into a quadratic one that is easier.
- Low, fixed rank constructions cannot be secure
    - The system is distinguishable from random
    - Succeptible to Min-Rank attack (obtaining equivalent secret keys)
    - Makes direct algebraic attack polynomial

Future Work

- Finding other algorithms to solve the cubic Min-Rank problem (e.g. generalization of minors modelling)
- Solving the Min-Rank problem in the setting of characteristic 2 and 3
- Developing new encryption/signature schemes with low enough rank to allow decryption/signing but large enough rank to avoid the Min-Rank attack
- Using the hardness of three-dimensional rank problems as a security assumption

Thanks