The MinRank problem

by Nicolas T. Courtois
Bull CP8 / Paris 6 University /Toulon University

www.minrank.org

courtois@minrank.org

A problem that arose at Crypto'99 [Shamir, Kipnis]:

$\boxed{\text{Given}}$

Given a field K. Let $m, n \in \mathbb{N}$, $r < n$
We consider m matrices $n \times n$ over K.

$$M_1, \ldots, M_m$$

$\boxed{\text{The MinRank Problem}}$

Find a linear combination $\alpha \in K^m$ of small rank:

$$Rank(\sum_i \alpha_i M_i) \leq r.$$

MinRank is NP-complete

[Shallit, Frandsen, Buss 1996]
http://www.brics.dk/RS/96/33/
An effective method to encode **any** system of multivariate equations !

MinRank is very difficult in practice.

Degenerated MinRank

Special Case: all matrices are diagonal:
The **Minimal Weight Problem** of Error Correcting Codes.
Equivalent to **Syndrome Decoding**.
Studied a lot for 20 years now...
[Berlekamp,McEliece,Gabidulin,Stern, Chabaud,Canteaut,Véron,...]
All known algorithms for this problem are **exponential**.

Algorithms for full MinRank

We proposed 4 algorithms. See:

- Nicolas Courtois, Louis Goubin:
  "The Cryptanalysis of TTM", Asiacrypt 2000.
- My PhD thesis April-Mai 2001, Paris 6 University

Hard instances AD 2000

Let p=65521, the biggest prime $< 2^{16}$
Given 10 matrices 6×6, over $\mathbb{Z}_p$. Rank $r = 3$.
Best known attack is in 2^{106}.

A new Zero-knowledge scheme MinRank

The public key: $M_1, \ldots, M_m$.

The secret key: $\alpha \in GF(p)^n$, such that

$$M = \sum \alpha_i \cdot M_i$$

$$Rank(M) = r < n.$$

The main idea:

Consider two random non-singular matrices S and T.

Consider the probability distribution of

$$TMS$$

Just a random matrix of rank r !

The Prover setup

A uniformly chosen random combination β_1 of M_i:

$$N_1 = \sum \beta_{1i} \cdot M_i$$

Let $\beta_2 = \alpha + \beta_1$. Remark: β_2 is just random.

$$N_2 = \sum \beta_{2i} \cdot M_i$$

$$N_2 - N_1 \ = \ M$$

One round of identification

Prover — **V**erifier

$\beta_1, \beta_2, S, T, X$

$$\xrightarrow[H(X),\ H(TN_1S+X),\ H(TN_2S+X),\ H(S,T)]{\qquad\qquad\qquad\qquad}$$

?

$$\xleftarrow[q \in \{0,1,2\}]{\qquad\qquad\qquad\qquad}$$

Case $\mathbf{q} = \mathbf{0}$:

$$\xrightarrow[(TN_1S+X),\ (TN_2S+X)]{\qquad\qquad\qquad\qquad}$$

Checks commitments and the rank of

$$(TN_2S+X)-(TN_1S+X) \ = \ TN_2S-TN_1S \ = \ TMS.$$

Case $\mathbf{q} = \mathbf{1}, \mathbf{2}$:

$$\xrightarrow[X,\ S,\ T,\ \beta_q]{\qquad\qquad\qquad\qquad}$$

That relate the committed values to the M_i.

- **It is Black-box Zero-knowledge.**
- **Cheating probability $\frac{2}{3}$ in 3 moves.**