The MinRank problem over finite fields and Zero-knowledge authentication

http ://www.cryptosystem.net/minrank/

Nicolas T. Courtois
courtois@minrank.org
http ://www.nicolascourtois.net

Road map

♢ "Usual cryptography" vs. multivariate cryptography with NP-complete problems

♢ The decoding problems and MinRank problem

♢ Attacks on MinRank problem

♢ Relevance to other known cryptosystems

♢ The new Zero-knowledge authentication scheme

♢ Comparison to other schemes based on NP-hard problems

♢ Multi-user setting, anonymous group authentication, ring signatures

Good cryptography

The security should be **provably** reduced to some **difficult problem** (and will be).

Multivariate vs. "usual" P.K. cryptography

Main stream PK-cryptography basic problems :
♢ defined using **univariate** or **bivariate** polynomial/exponentiation over **big** finite fields/rings
♢ usually not known to be NP-complete, many subexponential algorithms ⇒ **huge** blocks (e.g. 1024 bits).

Multivariate cryptography basic problems :
♢ **Many multivariate** polynomial equations over **small** finite fields/rings
♢ NP-hard problems, especially those that seem hard on average and are **exponential** to solve ⇒ **small** blocks of 80..160 bits.

Zero-knowledge Authentication schemes :

[Goldwasser, Micali, Rackoff 1985]
Provably secure entity authentication based on a difficult problem.

Known solutions

The best practical Zero-knowledge protocols are arithmetical :
Fiat-Shamir, Guillou-Quisquater, Schnorr.

Still, there are **practical** schemes based on a NP complete problem :
- PKP [Shamir]
- CLE [Stern]
- PPP [Pointcheval]
- Schemes related to coding [Harari, Girault, Veron, Stern, Chen].

New algorithm in this branch - MinRank.

Famous decoding (closest codeword) problems in cryptography

→ CVP problem in lattices :
decoding **group codes** over $\mathbb{R}$ with **Euclidian** distance.
→ Syndrome Decoding (SD) :
decoding **linear codes** over K with **Hamming** distance.
→ MinRank problem :
decoding **group codes** over K with **Rank** distance :

The problem MinRank$(\eta \times n, m, r, K)$

Given : $1 + m$ matrices $\eta \times n$ over a field K : $M_0; M_1, \ldots M_m$.
Find an linear combination α of M_i [+ constant M_0] of small rank.

$$Rank(M_0 + \sum_i \alpha_i M_i) \leq r.$$

The hardness of MinRank

Fact : MinRank is NP-complete [Shallit, Frandsen, Buss 1996].

Proof 1 : MinRank can encode any set of multivariate equations. NP-complete already for quadratic, MQ problem [Eurocrypt'00].

Proof 2 : MinRank contains syndrome decoding. Also trivial reduction from rank-distance syndrome decoding.

These problems are known as hard on average, not only worst case.
All known attacks on these problems are exponential...
expect the same for MinRank !

MinRank attacks

- ♢ First put $m := Min(m,\ \eta n + r^2 - (\eta + n)r + 1)$
  Exceptions : constructed small number of solutions.
- ♢ If $\eta < n$, transpose all matrices. Now $\eta \geq n$.
- ♢ **Brute force attack** $WF \approx q^m$.
- ♢ **Random square MinRank r≈n** [Schnorr] Let $n = r - s$, then $m := Min(m,\ s^2)$, broken in q^{s^2}. Fails for rectangular matrices.
- ♢ **Sub-matrices Attack r≪n** [Coppersmith-Stern-Vaudenay, C'93]. All the sub-matrices $(r+1)$x$(r+1)$ are singular. $WF \approx m^{\omega r}$.
- ♢ **MinRank → overdefined MQ r≪n** [Shamir-Kipnis, Crypto'99] Express the fact that columns $r+1..n$ are dependent. $WF \approx n^{\omega r}$
- ♢ **The Kernel Attack** [Goubin, Asiacrypt 2000] Guess the kernel of the matrix. The best attack for small q, $WF \approx q^{\lceil \frac{m}{\eta} \rceil r}$.
- ♢ **The Big m Attack m≫n** [Courtois], $WF \approx q^{Max(0, \eta(n-r)-m)}$.
- ♢ **The Syndrome Attack m≫n** [Gabidulin, Courtois]. Uses syndromes and linearity. $WF \approx q^{Max(\frac{\eta n - m - 1}{2}, (\eta+n)r/2 - m - r^2/4)}$

$\Rightarrow$ All attacks are exponential

MinRank in cryptanalysis of other known PK cryptosystems

- ♢ Shamir-Kipnis attack on Patarin's Hidden Field Equations HFE scheme [Crypto'99], reduction from HFE to MinRank.
- ♢ Improved by Courtois [RSA'01], now the best known structural attack for all HFE family of cryptosystems and also for C^* Matsumoto-Imai family.
- ♢ Cryptanalysis of TPM and TTM by Goubin and Courtois [Asiacrypt'00].
- ♢ Cryptanalysis of Shamir's birational signature scheme by Coppersmith, Stern and Vaudenay [Crypto'93].
- ♢ MinRank used for decoding rank distance codes : Chen and GPT family cryptosystems. For some parameters the best attack known for Chen [preprint].

What's new ? Another cryptosystem, based directly on any instance of MinRank problem.

Protocol settings

Simplification : square matrices $\eta = n$ and $M_0 = 0$.

The public key : m matrices $n \times n$ over $GF(q)$: $M_1, \ldots, M_m$.

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

$$Rank(\sum \alpha_i \cdot M_i) = r \quad \text{and} \quad r < n.$$

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

Key generation : All but 1 matrices are random, let M be a random matrix of rank r ; now choose random $\alpha_1, .., \alpha_m$ with $\alpha_m \neq 0$ and compute $M_m = (M - \sum_{i=1}^{m-1} \alpha_i \cdot M_i)/\alpha_m$.

Proposed instances of MinRank.

Field K	matrices m	size n	rank r	Best Attack complexity
GF(2)	121	21	10	2^{81}
GF(2)	190	29	15	2^{128}
GF(65521)	10	6	3	2^{106}
GF(65521)	10	7	4	2^{122}

[online] entity authentication / proof of identity

An interactive protocol between the **P**rover and the **V**erifier.
Goal : At the end of interaction **V** says *Accept* or *Refuse*.

The Prover computations

P chooses :
– two random non-singular matrices S and T.
– a random $n \times n$ matrix X.
– a random combination β_1 of M_i :

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

P uses the expression of M to get an expression of $N_2 = M + N_1$ as :

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

Each of them is a random combination with $N_2 - N_1 = M$.

One round of identification

$$\longrightarrow$$

$$H(X),\ H(TN_1S+X),\ H(TN_2S+X),\ H(S,T)$$

$$\longleftarrow$$

$$q \in \{0,1,2\}$$

If $q = 0$ the prover reveals :

$$\longrightarrow$$

$$(TN_1S+X),\ (TN_2S+X)$$

If $q = 1, 2$ the prover reveals :

$$\longrightarrow$$

$$S,\ T,\ \beta_q, X$$

Why it works :

Principle : $(TN_2S + X) - (TN_1S + X) \ = \ T(N_2 - N_1)S \ = \ TMS.$

1. If q=1 or 2 only random variables are disclosed.

2. Given two random non-singular matrices S and T.
TMS gives no information on M, just a random matrix of rank r !

3. To disclose $(TN_1S + X)$ and $(TN_2S + X)$ is equivalent to disclosing of $(TN_1S + X)$ that is random and uniform and $(TN_2S + X) - (TN_1S + X) \ = \ TMS.$

The security of an authentication scheme

The **strongest possible** security for an authentication scheme :

1. Adversarial **objective** : Obtain any information form the **P**rover that the **V**erifier cannot compute himself.
2. Adversarial **ressources** : Probabilistic Turing machine in time $T(n)$ and success probability $\varepsilon(n)$; $n =$ security parameter. Here we will be able to have $T(n)/\varepsilon(n) =$ exponential expression in n. Both asymptotic and concrete security !
3. **Access** to the system (i.e. initial penetration). Adaptive Verifier with unlimited interactions.

The security proof

Proof technique : Prove that it is a Zero-knowledge scheme.

Proof of Zero-knowledge

Black-box Zero-knowledge [Goldwasser, Micali, Rackoff 1985].

- **Correctness** An honest Prover is always accepted.
- **Soundness** No one can impersonate the Prover with an overwhelming probability.
- **Zero-knowledge** An (even malicious) verifier cannot extract from the Prover any information about Prover's secret knowledge (or ability) that he can't find out himself.

My scheme : If an adversary can answer all possible 3 questions, then **either he found a solution to MinRank either he found a collision for H**.

$T(n)/\varepsilon(n) \geq$ exponential for both problems.

Performances of the scheme

Simple scheme : cheating probability $\frac{2}{3}$ in 3 moves. 35 rounds necessary to achieve the impersonation probability of 10^{-6}.

Improved scheme : cheating probability $\frac{1}{2}$ in 3 moves. 20 rounds are enough. Requires an additional assumption (MQ).

I used several other tricks to improve the communications of the scheme.

My best version requires for a security of 2^{SF} to transmit the following number of bits :

$$2SF + \left(4SF + 9 + \frac{n\eta + m}{2} \log_2 q\right) \cdot \#\text{rounds}.$$

	PKP Shamir	SD Stern	Chen Chen	CLE Stern	PPP Pointcheval	MinRank Courtois
matrix	16x34	256x512	32x16	24x48	101x117	6x6
field	$\mathbb{F}_{251}$	$\mathbb{F}_2$	$\mathbb{F}_{65535}$	$\mathbb{F}_{257}$	$\mathbb{F}_2$	$\mathbb{F}_{65521}$
passes	5	3	5	3/5	3/5	3
impersonation probability	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{1}{2}$	$\frac{2}{3}/\frac{1}{2}$	$\frac{3}{4}/\frac{2}{3}$	$\frac{2}{3}/\frac{1}{2}$
rounds	20	35	20	35/20	48/35	35/20
impersonation global	10^{-6}	10^{-6}	10^{-6}	10^{-6}	10^{-6}	10^{-6}
public key [bits]	272	256	256	80	149	735
secret key [bits]	128	512	512	80	117	160
best attack	2^{60}	2^{70}	2^{53}	2^{73}	2^{61}	$\mathbf{2^{106}}$
bits send/round	665	954	1553	940/824	896/1040	1075/694
global [Kbytes]	**1.62**	4.08	3.79	4.01/**2.01**	5.25/4.44	4.6/**1.94**

Multiple user setting

Each user has one solution to MinRank and no information about other solutions :

Pick $1+m$ [pseudo-]random matrices $M_0; M_1, \ldots, M_m$.

Each user $i \in$ group G chooses for a random matrix M of rank r and a random combination $\sum \beta_i M_i$. His [part of] public key is : $U_i = M_0 + \sum \beta_i M_i + M$.

Then the set of matrices :
$M_0; M_1, \ldots, M_m$; with the $\{U_i | i \in G\}$ is the public key for any subgroup G.

Now any member can use the MinRank authentication scheme to **anonymously** prove his membership for any subgroup $G' \subseteq G$ to which he belongs.

Easy setup, unlimited updates, no trusted parties and fully public key (no shared secrets).

Ring Signatures with MinRank

Transform MinRank authentication into a signature scheme [FS heuristics] + the multi-user setting :

$\Rightarrow$ anonymous group signature scheme known as **a ring signature scheme** [Rivest, Shamir, Tauman, Asiacrypt 2001].

Conclusion :

Another successful application of MinRank in cryptography.

Here is a new provably secure authentication scheme in the strongest sense I know.

It can be used to prove the knowledge of a solution to any system of multivariate equations over a finite field. It can be also used for anonymous group authentication and ring signatures.

There are good reasons to hope that all the attacks for MinRank are be exponential.

Remark : MinRank is easy to implement and **royalty-free !**