Slide 1

Cryptanalysis of the TTM Cryptosystem

Triangle Plus Minus cryptosystems (TPM)

The MinRank problem

http://www.minrank.org/ttm/

Louis Goubin
Bull Smart Cards and Terminals, Louveciennes, France
L.Goubin@frlv.bull.fr

Nicolas T. Courtois
Paris 6 University, Toulon University
and INRIA Rocquencourt, France
courtois@minrank.org

Slide 2

Contents

1. Multivariate Cryptography
2. **T**riangular quadratic systems (**T**)
3. General **M**ultivariate **Q**uadratic systems (**MQ**)
4. **T**riangle **P**lus **M**inus (**TPM**)
5. TPM in cryptography
6. Breaking TPM in signature due to small u
7. Breaking TPM in encryption due to small rank r
8. The MinRank problem
9. TTM vs. TPM
10. Conclusion

Slide 3

Multivariate Cryptography.

- In 1983-88 Fell and Diffie and Matsumoto-Imai proposed several public-key cryptosystems using multivariate polynomials
  $(x_1, \ldots, x_n) \quad \mapsto \quad (P_1(x), \ldots, P_n(x))$
- The idea of birational polynomials [Fell and Diffie, Crypto'85]:

  Both the function and the inverse has a bounded degree,

  Open Pb: How to make it secure maintaining a public key of realistic size ?
- At Cypto 93 Adi Shamir proposed **sequentially solved** equations:

  Only a part of the inverse has a small degree.

  Some equations are removed to avoid attacks on it.

  Not injective, no encryption, signature only.

Slide 4

A triangle (T) and it's inverse

$$F \quad : \begin{cases} y_1 = x_1 \\ y_2 = x_2 + g_2(x_1) \\ y_3 = x_3 + g_3(x_1, x_2) \\ y_3 = x_3 + g_3(x_1, x_2, x_3) \\ \vdots \\ y_n = x_n + g_n(x_1, x_2, x_3, \ldots, x_n) \end{cases}$$

$$F^{-1} \quad : \begin{cases} x_1 = y_1 \\ x_2 = y_2 - g_2(x_1) \\ x_3 = y_3 - g_3(x_1, x_2) \\ x_3 = y_3 - g_3(x_1, x_2, x_3) \\ \vdots \\ x_n = y_n - g_n(x_1, x_2, x_3, \ldots, x_n) \end{cases}$$

Slide 5

Solving **M**ultivariate **Q**uadratic equations (**MQ**)

Find (one) solution to a system of **m** quadratic equations with **n** variables in a filed K.

$$f: \begin{cases} b_k = \sum_{i=0}^{n} \sum_{j=i}^{n} \lambda_{ijk}\ a_i a_j \\ \text{with } k = 1..m, \quad \mathbf{a_0 = 1} \end{cases}$$

Theory: MQ is NP-complete for **any field** K [Garey,Johnson], [Patarin, Goubin].

Solving MQ

Case $m = \varepsilon \frac{n^2}{2}$**:** Expected to be **polynomial**. Claimed at Crypto 99 [Shamir, Kipnis].

Improved algorithm XL [Shamir, Patarin, Courtois and Klimov, Eurocrypt 2000].

Case $m \approx n$**:** MQ might be subexponential, FXL algorithm [Eurocrypt 2000], no real proof.

State of the Art

Solving **n** multivariate equations with **n** variables over a very small finite field and $n \approx 100$
$\rightsquigarrow$ no method is substantially better than the exhaustive search !

Design goal in Multivariate Cryptography

A *good multivariate trapdoor function* on **n**-bit should have the security close to $\mathbf{2^n}$.

Apparently such functions exist: HFE, Quartz, Flash.

Slide 6

TPM (Triangle Plus Minus)

$$F: \begin{cases} y_1 = x_1 + g_1(x_{n-r+1}, \ldots, x_n;) \\ y_2 = x_2 + g_2(x_{n-r+1}, \ldots, x_n; x_1) \\ y_3 = x_3 + g_3(x_{n-r+1}, \ldots, x_n; x_1, x_2) \\ y_4 = x_4 + g_4(x_{n-r+1}, \ldots, x_n; x_1, x_2, x_3) \\ \vdots \\ y_{n-r} = x_{n-r} + g_{n-r}(x_{n-r+1}, \ldots, x_n; x_1, \ldots, x_{n-r-1}) \\ y_{n-r+1} = g_{n-r+1}(x_1, \ldots, x_n) \\ \vdots \\ y_{n-r+u} = g_{n-r+u}(x_1, \ldots, x_n) \end{cases}$$

Slide 7

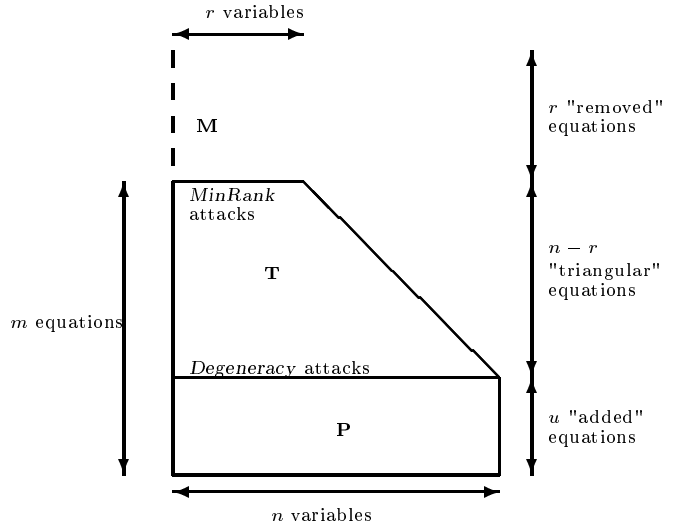

Figure 1: General view of the TPM scheme – The two classes of attacks

Slide 8

TPM in cryptography

Let F be a **TPM** system.

Let s, t - two invertible linear (affine) variable changes.

Public Key $G = t \circ F \circ s$, rewritten as **M**ultivariate **Q**uadratic polynomials.

Secret Key s, t and F.

Decryption

Guess r variables. Complexity $\mathcal{O}(q^r)$.

Then solve sequentially, as with triangular system (**T**).

Goal of TTM: use "tricks" that allows to compute these r variables.

Signature

Pick **any** random values for the r variables and solve the **T**riangle-**M**inus part TM.

With probability q^{-u} also the added equations (**P**) are true. Complexity $\mathcal{O}(q^u)$.

Important: F must be surjective, therefore we have $u < r$.

Slide 9

Basic linear algebra

The homogenous part of a quadratic equation y_i
$\rightsquigarrow$ a symmetric matrix M_i.

In T we have matrices of rank

$$0, 1, 2, \ldots, n-1.$$

In TPM we have matrices of rank

$$r, r+1, r+2, \ldots, n-1; \quad n, \ldots, n.$$

Effect of s and t

The rank is invariant under the initial transformation s.

The transformation t correspond to linear combinations over $GF(q)$ of the M_i.

Slide 10

Degeneracy Attack on signature schemes

- The linear space of equations that are of rank $n-1$ is of dimension $n-r$ and co-dimension u.
- If we chose a random linear combination of the equations/matrices, with probability q^{-u} it is degenerated, i.e. has rank $n-1$.
- By repeating the attack we determine a basis of the **TM** part, then remove the **P** part.
- In the **TM** part we determine any basis of a subspace of matrices that have rank $n-2$, we restrict to this space.
- Thus we removed a linear combination of $n-1$ which is y_{n-r} (or equivalent).
- Now all the matrices has a common nullspace that identifies x_{n-r}.
- We restrain to any complementary space of $\{x_{n-r}\}$.
- We repeat until we recovered completely s, and t (an equivalent one).

Attacks on encryption

In encryption we have u big, the Degeneracy attack fails.

Example in TTM 2.1. $u = 36$, $q^u \approx 2^{208}$.

TPM: Decryption is possible when q^r is small.

TTM vs TPM

Slide 11

TPM: We construct special polynomials that decrypt even if q^r big.

- The first two equations are written as a polynomial (of e.g. degree 8) in the algebraic basis composed by the added (**P**lus) equations: $y_{n-r}, \ldots$.
- Still they rewrite as a quadratic polynomial in the x_i.

It is not obvious to find such polynomials and many of them probably introduce additional weaknesses to the system. To be explored.

We cryptanalysed it as a general TPM.

Example of "TTM trick"

Let Q_8 be

$$Q_8(q_1, \ldots, q_{30}) = q_1^8 + q_{29}^4 + q_{30}^2 + [q_2^4 + q_3^2 q_8^2 + q_4^2 q_5^2 + q_6^2 q_{12}^2 + q_7^2 q_{13}^2]$$
$$\times [q_9^4 + (q_{10}^2 + q_{14} q_{15} + q_{18} q_{19} + q_{20} q_{21} + q_{22} q_{24})(q_{11}^2 + q_{16} q_{17} + q_{23} q_{28} + q_{25} q_{26} + q_{13} q_{27})].$$

We substitute the $q_{1..30}$ with:

Slide 12

$q_1 = t_1 + t_2 t_6$	$q_2 = t_2^2 + t_3 t_7$	$q_3 = t_3^2 + t_4 t_{10}$	$q_4 = t_3 t_5$
$q_5 = t_3 t_{11}$	$q_6 = t_4 t_7$	$q_7 = t_4 t_5$	$q_8 = t_7^2 + t_5 t_{11}$
$q_9 = t_6^2 + t_8 t_9$	$q_{10} = t_8^2 + t_{12} t_{13}$	$q_{11} = t_9^2 + t_{14} t_{15}$	$q_{12} = t_7 t_{10}$
$q_{13} = t_{10} t_{11}$	$q_{14} = t_{12}^2 + t_7 t_8$	$q_{15} = t_{13}^2 + t_{11} t_{16}$	$q_{16} = t_{14}^2 + t_{10} t_{12}$
$q_{17} = t_{15}^2 + t_{11} t_{17}$	$q_{18} = t_{12} t_{16}$	$q_{19} = t_{11} t_{12}$	$q_{20} = t_8 t_{13}$
$q_{21} = t_7 t_{13}$	$q_{22} = t_8 t_{16}$	$q_{23} = t_{14} t_{17}$	$q_{24} = t_7 t_{11}$
$q_{25} = t_{12} t_{15}$	$q_{26} = t_{10} t_{15}$	$q_{27} = t_{12} t_{17}$	$q_{28} = t_{11} t_{14}$
$q_{29} = t_{18} + t_1^2$	$q_{30} = t_{19} + t_{18}^2$		

Then

$$Q_8(q_1, \ldots, q_{30}) = t_{19}^2$$

Slide 13

The problem MinRank

MinRank(n , n , m , r , $GF(q)$)

Given: **m** matrices $\mathbf{n} \times \mathbf{n}$ over $GF(\mathbf{q})$: $M_1, \ldots M_m$.

Find a linear combination α of M_i of rank $\leq r$ such that:

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

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

A very hard problem:

Contains syndrome decoding problem for linear error correcting codes and rank-distance error correcting codes by Gabidulin.

MinRank can encode any set of multivariate equations.

Slide 14

Cryptographic importance of MinRank

Rump session of Crypto'2000:

A new practical Zero-knowledge scheme

based on hard instances of MinRank.

See: **http://www.minrank.org**.

Solving MinRank

Four algorithms for MinRank are known for either r small, either m big.

See PhD thesis, Nicolas Courtois, Paris 6 University, to appear soon.

We present one of them that applies in case r small, q not too big.

Slide 15

The Kernel Attack

We call M the matrix of rank r we try to find.

$$M = \sum_i \alpha_i M_i$$

$Ker(M)$ has dimension $n - r$ and co-dimension r.

We pick up a random vector

$$x \in GF(q)^n$$

The probability that $x \in Ker(M)$ is q^{-r}. In this case we have

$$\vec{0} = M \cdot x = \sum_i \alpha_i \ (M_i x)$$

It gives n linear equations with m variables α_i.

We want **m** equations $\rightsquigarrow$ guessing $\lceil \frac{m}{n} \rceil$ such vectors x.

The complexity of the attack is

$$(q^r)^{\lceil \frac{m}{n} \rceil} \cdot m^3 = q^{r \lceil \frac{m}{n} \rceil} \cdot m^3.$$

Slide 16

Must r always be small ?

In TPM r is small, because it can only be decrypted if q^r is small.

In TTM papers published so far we have $r = 2$, plus other weaknesses.

In the 1000$ TTM 2.1. challenge we broke, r was 2, and it was partly linear over $GF(2)$. Our program managed to solve the TTM 2.1. challenge in 3 minutes on PC. The solution is:

"Tao TTP way BCKP of living hui mountain wen river moon love pt"

Since U.S. Data Security desactivated it, renamed "Learner's challenge II", introduced a different challenge TTM 2.2., and never paid the 1000$.

The U.S. Data Security challenge 2.3. for 5000 $ has been deactivated since and we could not try if we could break it.

We could not break the U.S. Data Security contest TTM 1.7.

Slide 17

The general strategy of attacks on encryption

We solve the MinRank problem to recover the smallest side of the hidden triangle **T**.

Example for TTM 2.1. with rank $r = 2$

The MinRank is solved in $q^{r\lceil \frac{m}{n} \rceil} \cdot m^3 \approx 2^{52}$.

How to continue.

Remove the nullspace of the Matrix, $\rightsquigarrow$ an easy **T**riangle-**P**lus to solve.

Possible problems with TTM

Additional properties (small ranks of other components, if any) should be eliminated. Each of them willl be recovered seperately by MinRank and by exhaustive tries one of them will allow to continue. What if covered several times different small ranks ?

A TTM that would resist to attacks by MinRank is still to be proposed.

N.B. Papers about TTM use vague statements about details of cryptosystems.

Slide 18

Conclusion

The cryptosystems of the TPM family are broken both in signature and in encryption due to small values of respectively r and u.

TTM attempts to construct such systems with a slightly bigger r.

The 1000$ challenge TTM 2.1. with $r = 2$ would be broken as a TPM in 2^{52}.

It takes only 3 minutes to break, because of the presence of additional linearities.

Possible improved TTM cryptosystems

TTM uses very special polynomials, and there is no convincing general construction. Their special algebraical structure might add more weaknesses.

Better versions of TTM may be proposed in the future, but thay will be probably have $r << n$.

Then it will be broken much faster than the exhaustive search.

Unlike such multivariate cryptosystems as HFE, Quartz.