Cryptanalysis of the TRMS Signature Scheme of PKC'05

Luk Bettale, Jean-Charles Faugère and Ludovic Perret

SALSA
LIP6, Université Paris 6 & INRIA Paris-Rocquencourt
luk.bettale@free.fr, Jean-Charles.Faugere@inria.fr,
ludovic.perret@lip6.fr

Outline

Outline

Multivariate Public Key Cryptography (MPKC)

General Idea (Matsumoto–Imai, 88/83)

Let $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]^m$ be s. t. $\forall \mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{K}^m$:

$$V_{\mathbb{K}}\big(f_1 - c_1, \ldots, f_m - c_m\big) = \{\mathbf{z} \in \mathbb{K}^n : f_1(\mathbf{z}) - c_1 = 0, \ldots, f_m(\mathbf{z}) - c_m = 0\},$$

can be computed efficiently.

Secret key

$$(S, U) \in GL_n(\mathbb{K}) \times GL_n(\mathbb{K}) \,\&\, \mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]^m.$$

Public key

$$\mathbf{p}(\mathbf{x}) = \big(p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})\big) = \big(f_1(\mathbf{x} \cdot S), \ldots, f_m(\mathbf{x} \cdot S)\big)\, U = \mathbf{f}(\mathbf{x} \cdot S) \cdot U,$$

with $\mathbf{x} = (x_1, \ldots, x_n)$.

Encryption

- To encrypt $\mathbf{M} \in \mathbb{K}^n$:

$$\mathbf{c} = \mathbf{p}(\mathbf{M}) = \big(p_1(\mathbf{M}), \ldots, p_m(\mathbf{M})\big).$$

- To decrypt, compute $\mathbf{M}' \in \mathbb{K}^n$ s.t. :

$$\mathbf{f}(\mathbf{M}') = \mathbf{c} \cdot U^{-1}.$$

We then have $\mathbf{M} = \mathbf{M}' \cdot S^{-1}$, if $\#V_{\mathbb{K}}\big(\mathbf{f} - \mathbf{c} \cdot U^{-1}\big) = 1$.

Proof.

$$\mathbf{p}(\mathbf{M}' \cdot S^{-1}) = \mathbf{f}(\mathbf{M}' \cdot S^{-1} \cdot S) \cdot U = \mathbf{c} \cdot U^{-1} \cdot U = \mathbf{c}.$$

□

Signature

- To verify the signature $\mathbf{s} \in \mathbb{K}^n$ of a digest $\mathbf{H} \in \mathbb{K}^m$:

$$\mathbf{p}(\mathbf{s}) = \mathbf{H}.$$

- To generate $\mathbf{s} \in \mathbb{K}^n$ from a digest $\mathbf{H} \in \mathbb{K}^m$, we apply the decryption process to $\mathbf{H}$, i.e. we compute $\mathbf{s}' \in \mathbb{K}^n$ s.t. :

$$\mathbf{f}(\mathbf{s}') = \mathbf{H} \cdot U^{-1}.$$

The signature is then $\mathbf{s} = \mathbf{s}' \cdot S^{-1}$.

Proof.

$$\mathbf{p}(\mathbf{s}) = \mathbf{f}(\mathbf{s}' \cdot S^{-1} \cdot S) \cdot U = \mathbf{H} \cdot U^{-1} \cdot U = \mathbf{H}.$$

□

"Historical" MPKC

- T. Matsumoto, and H. Imai.
  Public Quadratic Polynomial-tuples for Efficient Signature-Verification and Message-Encryption.
  EUROCRYPT 1988.
  IECE, 1983 (Japanese).
- J. Patarin.
  Hidden Fields Equations (HFE) and Isomorphism of Polynomials (IP): two new families of Asymmetric Algorithms.
  EUROCRYPT 1996.
- N. Courtois, L. Goubin, and J. Patarin.
  SFLASH, a Fast Symmetric Signature Scheme for low-cost Smartcards – Primitive Specification and Supporting documentation.
  Available at `www.minrank.org/sflash-b-v2.pdf`.

MPKC under Attack

Underlying hard problem

Given $\mathbf{H} \in \mathbb{K}^m$, find $\mathbf{z} \in \mathbb{K}^n$ such that :

$$p_1(\mathbf{z}) - H_1 = 0, \ldots, p_m(\mathbf{z}) - H_m = 0.$$

- J.-C. Faugère, and A. Joux.
  Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases.
  CRYPTO 2003.
- V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern.
  Practical Cryptanalysis of SFLASH.
  CRYPTO 2007.

Outline

Tractable Rationale Maps

Principle

The set $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]^m$ is constructed as follows.

$$
\begin{aligned}
f_1 &= r_1(x_1) \\
f_2 &= r_2(x_2) \cdot \frac{g_2(x_1)}{q_2(x_1)} + \frac{h_2(x_1)}{s_2(x_1)} \\
&\vdots \\
f_m &= r_m(x_m) \cdot \frac{g_m(x_1, \ldots, x_{m-1})}{q_m(x_1, \ldots, x_{m-1})} + \frac{h_m(x_1, \ldots, x_{m-1})}{s_m(x_1, \ldots, x_{m-1})}
\end{aligned}
$$

C.-Y. Chou, Y.-H. Hu, F.-P. Lai, L.-C. Wang, and B.-Y. Yang.
Tractable Rational Map Signature.
PKC'05.

Previous Security Result

C.-Y. Chou, Y.-H. Hu, F.-P. Lai, L.-C. Wang, and B.-Y. Yang.
Tractable Rational Map Signature.
PKC'05.

A. Joux, S. Kunz-Jacques, F. Muller, and P.-M. Ricordel.
Cryptanalysis of the Tractable Rational Map Cryptosystem.
PKC'05.

Recommended Values for TRMS (PKC'05)

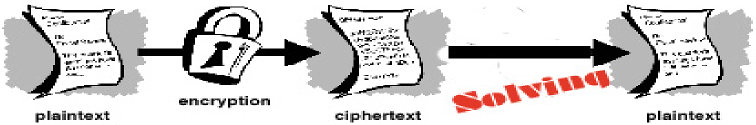
- $\mathbb{K} = \mathbb{F}_{2^8}$
- $n = 28$ and $m = 20$

Algebraic Cryptanalysis

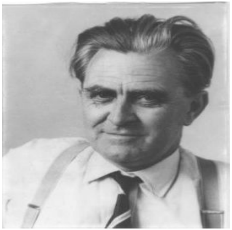
- differential cryptanlysis
- linear cryptanlysis

Principle

- Model a cryptosystem as a set of algebraic equations
- Try to solve this system (or estimate the difficulty of solving)



Outline



W. Gröbner

B. Buchberger

Gröbner basis

- $\mathbb{K}$ is a field, $\mathbb{K}[x_1, \ldots, x_n]$ a polynomial ring in n variables.

Linear Systems

$$\begin{cases} \ell_1(x_1, \ldots, x_n) = 0 \\ \ell_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ \ell_m(x_1, \ldots, x_n) = 0 \end{cases}$$

- $V = \mathrm{Vect}_{\mathbb{K}}(\ell_1, \ldots, \ell_k)$
- Triangular/diagonal basis of V

Polynomial Systems

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

- ideal $\mathcal{I} = \langle f_1, \ldots, f_k \rangle =$

$$\left\{ \sum_{i=1}^{k} f_k u_k : u_i \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

- Gröbner basis of $\mathcal{I}$

Gröbner basis

Definition (Buchberger 1965/1976)

$G \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis of a polynomial ideal $\mathcal{I}$, if :

$$\forall f \in \mathcal{I}, \exists g \in G \text{ s. t. } \mathrm{LM}(g) \text{ divides } \mathrm{LM}(f).$$

Remark

- depends of the monomial ordering

FGLM

Property

A LEX Gröbner basis of a zero-dimensional system is :

$$\{g_1(x_1), g_2(x_1,x_2), \ldots, g_{k_2}(x_1,x_2), g_{k_2+1}(x_1,x_2,x_3), \ldots, \ldots\}$$

Computing LEX directly is much slower than computing DRL directly

J.-C. Faugère , P. Gianni, D. Lazard, T. Mora.
Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symb. Comp., 1993.

Fact

Let D the nb. of zeroes (with multiplicities) of $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$. FGLM computes a LEX Gröbner basis of $\mathcal{I}$ from a DRL Gröbner basis of $\mathcal{I}$ in $\mathcal{O}(nD^3)$.

Zero-dim solving : a two steps process

- Compute a DRL Gröbner basis
  - Buchberger's algorithm (1965)
  - F_4 (J.-C. Faugère, 1999)
  - F_5 (J.-C. Faugère, 2002)

  ⇒ For a zero-dim system :

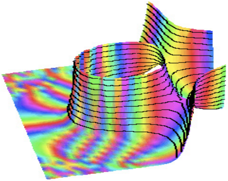
$$\mathcal{O}\left(n^{3 \cdot d_{reg}}\right),$$

  d_{reg} being the max. degree reached during the computation.
  - If $m = n$, d_{reg} is gen. equal to $n + 1$.
- Compute a LEX Gröbner basis using FGLM
- Automatically done in almost all computer algebra systems
  - For instance : Variety in Magma

Complexity of F_5

For a *semi-regular* system of $m\,(> n)$ quadratic equations over $\mathbb{K}[x_1, \ldots, x_n]$ the degree of regularity is given by :

$$\sum_{i \geq 0} a_i z^i = \frac{(1-z^2)^m}{(1-z)^n}.$$



M. Bardet, J-C. Faugère, B. Salvy and B-Y. Yang.
Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.
MEGA 2005.

- If $m = n + 1$, $d_{reg} \sim_{n \to \infty} \left\lceil \frac{(n+1)}{2} \right\rceil$.

Complexity of F_5

For a *semi-regular* system of $m\,(> n)$ quadratic equations over $\mathbb{K}[x_1, \ldots, x_n]$ the degree of regularity is given by :

$$\sum_{i \geq 0} a_i z^i = \frac{(1 - z^2)^m}{(1 - z)^n}.$$

- If $m = n + 1$:

$$d_{reg} = \left\lceil \frac{(n+1)}{2} \right\rceil.$$

A. Szanto.
Multivariate Subresultants using Jouanolou's Resultant Matrices.
Journal of Pure and Applied Algebra.

Outline

Signature Forgery Attack

Specific Context

Given $\mathbf{H} \in \mathbb{K}^m$, find $\mathbf{z} \in \mathbb{K}^n$ such that :

$$p_1(\mathbf{z}) - H_1 = 0, \ldots, p_m(\mathbf{z}) - H_m = 0.$$

A Zero level attack

J.-C. Faugère, and A. Joux.
Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases.
CRYPTO 2003.

- nb. of polynomials (m) is smaller than nb. of variables (n)
- $\mathbb{K} = \mathbb{F}_{2^8} \Rightarrow$ we have not included the field equ. $(x_i^{2^8} - x_i)$
  - DRL-GB difficult to compute
  - complexity of FGLM very high

Specifying Variables – (I)

You can randomly fix $n - m$ variables .

Working Hypothesis

new system behaves like a (semi-)regular system.

- $d_{reg} = m + 1\,(21)$
- $V_{\mathbb{K}}(.) \approx 2^m$ (Bezout's bound)

Specifying Variables – (II)

Obviously, you can randomly fix $n - m - r$ variables $(r > 0)$.

- decrease the degree of regularity $(r = 1, d_{reg} = \lceil \frac{m}{2} \rceil)$
- decrease the size of the variety
- increase the number of Gröbner bases to compute $(\#\mathbb{K})^r$

Experimental Results

m	$m-r$	r	d_{reg} (theoretical)	d_{reg} (observed)
20	19	1	10	
20	18	2	9	9
20	17	3	8	8
20	16	4	7	7
20	15	5	6	6

m	$m-r$	r	$(\#\mathbb{K})^r$	$\mathrm{T}_{\mathrm{F}_5}$	Mem	$\mathrm{Nop}_{\mathrm{F}_5}$	T
20	18	2	2^{16}	51h	42 Gbytes	2^{41}	2^{57}
20	17	3	2^{24}	2h45min.	4 Gb	2^{37}	2^{61}
20	16	4	2^{32}	626 sec.	912 Mb	2^{34}	2^{66}
20	15	5	2^{40}	46 sec.	368 Mb.	2^{30}	2^{70}

Conclusion and Future Works

- Evaluation of the complexity of the attack for different values of the parameters
- A systematic method (quasi automatic) for evaluating the security of multivariate systems

Jean-Charles Faugère, and L. Perret.
On the Security of UOV.
First International Conference on Symbolic Computation and Cryptography (SCC'08).