Tractable Rational Map Signature

Lih-Chung Wang,
Yuh-Hua Hu,
Feipei Lai,
Chun-Yen Chou,
Bo-Yin Yang

Jan. 26, 2005

Digital signature

- It is useful for electronic commerce
- It relies on Public key cryptosystems
- Most well-known number-theoretical signature systems are based on
  - modular exponentiation RSA
  - discrete logarithms problem ElGamal/DSA/ECC

Introduction to Multivariate Schemes

Multivariate schemes:

1. using polynomials in stead of big numbers
2. Advantage: high performance
3. Disadvantage: big public key,

TRMS:

1. multivariate digital signature
2. based on Tractable Rational Maps
3. Similar to TTS
4. 1000 times faster than RSA

Introduction to Multivariate Schemes

Multivariate schemes:

1. using polynomials in stead of big numbers
2. Advantage: high performance
3. Disadvantage: big public key,

TRMS:

1. multivariate digital signature
2. based on Tractable Rational Maps
3. Similar to TTS
4. 1000 times faster than RSA

Design Philosophy of Multivariate Cryptosystem

1. solving general multivariate equations is NP
2. solving general quadratic multivariate equations is NP (MQ problem)
3. finding some quadratic polynomial map with trapdoor

Mathematical Background

Let L be the finite Galois field $GF(p^n)$ with p^n elements.

Lemma

Every function f from L^n to L is an n-variable polynomial function.

Proposition

Every map f from L^n to L^m is a polynomial map.

The above proposition shows that:
the category of polynomial maps is as big as the category of maps.

Mathematical Background

Let L be the finite Galois field $GF(p^n)$ with p^n elements.

Lemma

Every function f from L^n to L is an n-variable polynomial function.

Proposition

Every map f from L^n to L^m is a polynomial map.

The above proposition shows that:
the category of polynomial maps is as big as the category of maps.

permutation polynomial

Definition

A polynomial $f(x) \in L[x]$ is called a permutation polynomial of L if the associated polynomial function from L to L is a one-to-one and onto function.

Examples:

1. Frobenius map $x \longrightarrow x^p$
2. If L is a field extension of a field K, then any invertible affine transformation of L over K is a permutation polynomial map.

permutation polynomial

Definition

A polynomial $f(x) \in L[x]$ is called a permutation polynomial of L if the associated polynomial function from L to L is a one-to-one and onto function.

Examples:

1. Frobenius map $x \longrightarrow x^p$
2. If L is a field extension of a field K, then any invertible affine transformation of L over K is a permutation polynomial map.

Tractable Rational Map

A tractable rational map is an invertible affine transformation or, after a permutation of indices if necessary, a rational map of the following form

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_j \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_j(x_j) \cdot \frac{p_j(x_1,x_2,\ldots,x_{j-1})}{q_j(x_1,x_2,\ldots,x_{j-1})} + \frac{f_j(x_1,x_2,\ldots,x_{j-1})}{g_j(x_1,x_2,\ldots,x_{j-1})} \\ \vdots \\ r_n(x_n) \cdot \frac{p_n(x_1,x_2,\ldots,x_{n-1})}{q_n(x_1,x_2,\ldots,x_{n-1})} + \frac{f_n(x_1,x_2,\ldots,x_{n-1})}{g_n(x_1,x_2,\ldots,x_{n-1})} \end{pmatrix}$$

where f_j, g_j, p_j and q_j are polynomials and r_j are permutation polynomials of the finite field L.

Why in Rational Form

Note that, by Lagrange interpolation, any map over a finite field is a polynomial map. There are both computational and categorical reasons that we put our maps in rational form.

For computational reasons, it is faster to compute the division between two function values by low degree polynomial maps than to compute a single function value by a much higher degree polynomial map. For example, it is much easier to compute $\frac{1}{x}$ than to compute x^{254} over $GF(256)$.

And categorically, even given a tractable rational map without denominator, by the direct computation above, the inverse of that map is most naturally described as a rational map. Therefore we choose to put the map in the rational form. For details, see [35].

Theorem

Given a tractable rational map $\phi : S \to L^n$ of the following form.

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_j \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_j(x_j) \cdot \frac{p_j(x_1,x_2,\ldots,x_{j-1})}{q_j(x_1,x_2,\ldots,x_{j-1})} + \frac{f_j(x_1,x_2,\ldots,x_{j-1})}{g_j(x_1,x_2,\ldots,x_{j-1})} \\ \vdots \\ r_n(x_n) \cdot \frac{p_n(x_1,x_2,\ldots,x_{n-1})}{q_n(x_1,x_2,\ldots,x_{n-1})} + \frac{f_n(x_1,x_2,\ldots,x_{n-1})}{g_n(x_1,x_2,\ldots,x_{n-1})} \end{pmatrix}$$

where $S = \{(x_1, \ldots, x_n) \mid \prod_{j=2}^{n}(p_j q_j g_j)(x_1, x_2, \ldots, x_{j-1}) \neq 0\}$. Then ϕ is one-to-one. Furthermore, given an image point, we can get the pre-image constructively with the recursive algorithm.

Proof

Given a image point $(y_1, \ldots, y_n)$. We can solve the following system of equations inductively.

$$\begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_j(x_j) \cdot \frac{p_j(x_1,x_2,\ldots,x_{j-1})}{q_j(x_1,x_2,\ldots,x_{j-1})} + \frac{f_j(x_1,x_2,\ldots,x_{j-1})}{g_j(x_1,x_2,\ldots,x_{j-1})} \\ \vdots \\ r_n(x_n) \cdot \frac{p_n(x_1,x_2,\ldots,x_{n-1})}{q_n(x_1,x_2,\ldots,x_{n-1})} + \frac{f_n(x_1,x_2,\ldots,x_{n-1})}{g_n(x_1,x_2,\ldots,x_{n-1})} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_j \\ \vdots \\ y_n \end{pmatrix}$$

Proof (continued)

First, we get $x_1 = r_1^{-1}(y_1)$ from the first equation. Suppose we know $x_1, \ldots, x_{j-1}$. Substitute $x_1, \ldots, x_{j-1}$ into the j-th equation.

$$r_j(x_j) \cdot \frac{p_j(x_1, x_2, \ldots, x_{j-1})}{q_j(x_1, x_2, \ldots, x_{j-1})} + \frac{f_j(x_1, x_2, \ldots, x_{j-1})}{g_j(x_1, x_2, \ldots, x_{j-1})} = y_j$$

Then we obtain

$$x_j = r_j^{-1}\left(\frac{q_j(x_1, x_2, \ldots, x_{j-1})}{p_j(x_1, x_2, \ldots, x_{j-1})} \cdot \left(y_j - \frac{f_j(x_1, x_2, \ldots, x_{j-1})}{g_j(x_1, x_2, \ldots, x_{j-1})}\right)\right).$$

Corollary

If we assume g_j, p_j and q_j in the above form be non-vanishing polynomials, then $S = L^n$ and ϕ is a bijection of L^n.

Proof (continued)

First, we get $x_1 = r_1^{-1}(y_1)$ from the first equation. Suppose we know $x_1, \ldots, x_{j-1}$. Substitute $x_1, \ldots, x_{j-1}$ into the j-th equation.

$$r_j(x_j) \cdot \frac{p_j(x_1, x_2, \ldots, x_{j-1})}{q_j(x_1, x_2, \ldots, x_{j-1})} + \frac{f_j(x_1, x_2, \ldots, x_{j-1})}{g_j(x_1, x_2, \ldots, x_{j-1})} = y_j$$

Then we obtain

$$x_j = r_j^{-1}\left(\frac{q_j(x_1, x_2, \ldots, x_{j-1})}{p_j(x_1, x_2, \ldots, x_{j-1})} \cdot \left(y_j - \frac{f_j(x_1, x_2, \ldots, x_{j-1})}{g_j(x_1, x_2, \ldots, x_{j-1})}\right)\right).$$

Corollary

If we assume g_j, p_j and q_j in the above form be non-vanishing polynomials, then $S = L^n$ and ϕ is a bijection of L^n.

TRMS and its Implementation

We show an implement scheme of TRMS.

It can be seen that there are a variety of schemes of TRMS which are all based on tractable rational maps.

Let $\mathbb{K} = GF(2^8)$. We will construct 3 maps $\varphi_1 : \mathbb{K}^{28} \to \mathbb{K}^{28}$, $\varphi_2 : \mathbb{K}^{28} \to \mathbb{K}^{20}$, $\varphi_3 : \mathbb{K}^{20} \to \mathbb{K}^{20}$ where φ_1, φ_3 are invertible affine transformations, $\varphi_2 = \pi \circ \widetilde{\varphi_2} \circ i$ with π a projection, i an imbedding, and $\widetilde{\varphi_2}$ identified as a tractable rational map over some extension field over $\mathbb{K}$.

Public key: $\varphi_3 \circ \varphi_2 \circ \varphi_1$
Private key: $(\varphi_1^{-1}, \varphi_2, \varphi_3^{-1})$

TRMS and its Implementation

We show an implement scheme of TRMS.

It can be seen that there are a variety of schemes of TRMS which are all based on tractable rational maps.

Let $\mathbb{K} = GF(2^8)$. We will construct 3 maps $\varphi_1 : \mathbb{K}^{28} \to \mathbb{K}^{28}$, $\varphi_2 : \mathbb{K}^{28} \to \mathbb{K}^{20}$, $\varphi_3 : \mathbb{K}^{20} \to \mathbb{K}^{20}$ where φ_1, φ_3 are invertible affine transformations, $\varphi_2 = \pi \circ \widetilde{\varphi_2} \circ i$ with π a projection, i an imbedding, and $\widetilde{\varphi_2}$ identified as a tractable rational map over some extension field over $\mathbb{K}$.

Public key: $\varphi_3 \circ \varphi_2 \circ \varphi_1$
Private key: $(\varphi_1^{-1}, \varphi_2, \varphi_3^{-1})$

Sign and Verify

To sign a message M, first find its hash $\mathbf{z} = H(M) \in \mathbb{K}^{20}$ by a publicly agreed hash function. Then do $\mathbf{y} = \varphi_3^{-1}(\mathbf{z})$, where the indices of $\mathbf{y}$ is starting at 9. Then choose 8 nonzero random numbers $r_1, r_2, \ldots, r_8$. Then get $\mathbf{x}$ by identifying it with $(\widetilde{\varphi_2} \circ i)^{-1}(r_1, r_2, \ldots, r_8, \mathbf{y})$ which is computed by a sequence of substitutions. Then get the signature $\mathbf{w} = \varphi_1^{-1}(\mathbf{x})$.

To verify a signature $\mathbf{w}$, simply check if $V(\mathbf{w}) = (\varphi_3 \circ \varphi_2 \circ \varphi_1)(\mathbf{w}) = (\varphi_3 \circ \pi \circ \widetilde{\varphi_2} \circ i)(\mathbf{x}) = (\varphi_3 \circ \pi)(r_1, r_2, \ldots, r_8, \mathbf{y}) = \varphi_3(\mathbf{y}) = \mathbf{z} = H(M)$.

Sign and Verify

To sign a message M, first find its hash $\mathbf{z} = H(M) \in \mathbb{K}^{20}$ by a publicly agreed hash function. Then do $\mathbf{y} = \varphi_3^{-1}(\mathbf{z})$, where the indices of $\mathbf{y}$ is starting at 9. Then choose 8 nonzero random numbers $r_1, r_2, \ldots, r_8$. Then get $\mathbf{x}$ by identifying it with $(\widetilde{\varphi_2} \circ i)^{-1}(r_1, r_2, \ldots, r_8, \mathbf{y})$ which is computed by a sequence of substitutions. Then get the signature $\mathbf{w} = \varphi_1^{-1}(\mathbf{x})$.

To verify a signature $\mathbf{w}$, simply check if $V(\mathbf{w}) = (\varphi_3 \circ \varphi_2 \circ \varphi_1)(\mathbf{w}) = (\varphi_3 \circ \pi \circ \widetilde{\varphi_2} \circ i)(\mathbf{x}) = (\varphi_3 \circ \pi)(r_1, r_2, \ldots, r_8, \mathbf{y}) = \varphi_3(\mathbf{y}) = \mathbf{z} = H(M)$.

Details of φ_2

Decompose $(x_1, x_2, \ldots, x_{28}) \in \mathbb{K}^{28}$ into five groups: $X_1 = (x_1, x_2, \ldots, x_8)$, $X_2 = (x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14})$, $X_3 = (x_{15}, x_{16})$, $X_4 = (x_{17}, x_{18}, x_{19})$ and $X_5 = (x_{20}, x_{21}, \ldots, x_{28})$.
Let $\widetilde{\varphi_2} : \mathbb{L}^5 \to \mathbb{L}^5$ be a tractable rational map of the following form.

$$\begin{cases} R_1 &= X_1 \\ Y_2 &= X_2\ p_2(X_1) + f_2(X_1) \\ Y_3 &= r_3(X_3) + f_3(X_1, X_2) \\ Y_4 &= X_4\ p_4(X_1, X_2, X_3) + f_4(X_1, X_2, X_3) \\ Y_5 &= X_5\ p_5(X_1, X_2, X_3, X_4) + f_5(X_1, X_2, X_3, X_4) \end{cases}$$

Details of φ_2 (continued)

$R_1 = X_1$ induces $(r_1, r_2, \ldots, r_8) = (x_1, x_2, \ldots, x_8)$.

$Y_2 = X_2\ p_2(X_1)\ +\ f_2(X_1)$ induces

$$\begin{pmatrix} y_9 \\ y_{10} \\ \vdots \\ y_{14} \end{pmatrix} = \begin{pmatrix} x_9 \\ x_{10} \\ \vdots \\ x_{14} \end{pmatrix} *_6 \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_6 \end{pmatrix} + \begin{pmatrix} c_1 x_3 x_4 \\ c_2 x_4 x_5 \\ \vdots \\ c_6 x_8 x_1 \end{pmatrix} + \begin{pmatrix} c_7 x_3 \\ c_8 x_4 \\ \vdots \\ c_{12} x_8 \end{pmatrix}$$

where c_i's are constant parameters of user's choice and $\mathbf{u} *_n \mathbf{v}$ denotes first identifying $\mathbf{u}, \mathbf{v} \in \mathbb{K}^n$ in the extension field with degree n then carrying out the multiplication there.

Details of φ_2 (continued)

$Y_3 = r_3(X_3) + f_3(X_1, X_2)$ induces

$$\begin{pmatrix} y_{15} \\ y_{16} \end{pmatrix} = \begin{pmatrix} x_{15} \\ x_{16} \end{pmatrix}^2 + \begin{pmatrix} c_{13}x_1x_2 + c_{14}x_3x_4 + \cdots + c_{19}x_{13}x_{14} + c_{27}x_1 \\ c_{20}x_{14}x_1 + c_{21}x_2x_3 + \cdots + c_{26}x_{12}x_{13} + c_{28}x_2 \end{pmatrix}$$

where $\begin{pmatrix} x_{15} \\ x_{16} \end{pmatrix}^2 = \begin{pmatrix} x_{15} \\ x_{16} \end{pmatrix} *_2 \begin{pmatrix} x_{15} \\ x_{16} \end{pmatrix}$ and c_i's are constant parameters of user's choice.

$Y_4 = X_4\ p_4(X_1, X_2, X_3) + f_4(X_1, X_2, X_3)$ induces

$$\begin{pmatrix} y_{17} \\ y_{18} \\ y_{19} \end{pmatrix} = \begin{pmatrix} x_{17} \\ x_{18} \\ x_{19} \end{pmatrix} *_3 \begin{pmatrix} x_7 \\ x_8 \\ x_9 \end{pmatrix} + \begin{pmatrix} c_{29}x_4x_{16} + c_{32}x_9 \\ c_{30}x_5x_{10} + c_{33}x_{10} \\ c_{31}x_{15}x_{16} + c_{34}x_{11} \end{pmatrix}$$

where c_i's are constant parameters of user's choice.

Details of φ_2 (continued)

$Y_5 = p_5(X_1, X_2, X_3, X_4)\ X_5 \ + \ f_5(X_1, X_2, X_3, X_4)$ induces

$$\begin{pmatrix} y_{20} \\ y_{21} \\ \vdots \\ y_{28} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} x_{19} \\ x_{18} \\ x_{17} \end{pmatrix} & \begin{pmatrix} x_{16} \\ x_{15} \\ x_{14} \end{pmatrix} & \begin{pmatrix} x_{13} \\ x_{12} \\ x_{11} \end{pmatrix} \\ \begin{pmatrix} x_{10} \\ x_9 \\ x_8 \end{pmatrix} & \begin{pmatrix} x_7 \\ x_6 \\ x_5 \end{pmatrix} & \begin{pmatrix} x_4 \\ x_3 \\ x_2 \end{pmatrix} \\ \begin{pmatrix} x_1 \\ x_{19} \\ x_{18} \end{pmatrix} & \begin{pmatrix} x_{17} \\ x_{16} \\ x_{15} \end{pmatrix} & \begin{pmatrix} x_{14} \\ x_{13} \\ x_{12} \end{pmatrix} \end{pmatrix} *_3 \begin{pmatrix} x_{20} \\ x_{21} \\ \vdots \\ x_{28} \end{pmatrix} +$$

Details of φ_2 (continued)

$$\begin{pmatrix} c_{35}x_{18}x_{19} + c_{44}x_1 \\ c_{36}x_{17}x_{13} + c_{45}x_2 \\ c_{37}x_{16}x_{14} + c_{46}x_3 \\ c_{38}x_{12}x_{13} + c_{47}x_4 \\ c_{39}x_{15}x_{14} + c_{48}x_5 \\ c_{40}x_{19}x_{12} + c_{49}x_6 \\ c_{41}x_{18}x_{10} + c_{50}x_7 \\ c_{42}x_{12}x_6 + c_{51}x_8 \\ c_{43}x_{13}x_5 + c_{52}x_9 \end{pmatrix}$$

where c_i's are constant parameters of user's choice.

Performance of TRMC

Test Platform: CPU: P4 2.4GHz; RAM: 1024MB; OS: Linux + gcc 3.3;
ARG: gcc -O3 -march=pentium4 -fomit-frame-pointer

Scheme Name	Signature size (byte)	Public Key Size (byte)	Private Key Size (byte)	Sign (μs)	Verify (μs)	Key Generation (ms)
TTS(20,28)	28	8680	1399	7	20	2.2
TRMS(20,28)	28	8680	396	4.8	20	1.2

Table: NESSIE signature report, TTS and TRMS tested as above

Unit: { Signature/key size:Bytes, Sign/Verify/Key Generation: cycles/invocation

Scheme Name	Signature size	Public Key Size	Private Key Size	Sign	Verify	Key Generation
ECDSA	48	48	24	1971K	5415K	1758K
ESgin	144	145	96	4434K	936K	269M
RSA-PSS	128	128	320	82M	1587K	3206M
$SFLASH_{v2}$	37	$\approx$ 15K	$\approx$ 28K	5106K	765K	2929M
SQARTZ	16	$\approx$ 71K	$\approx$ 4K	6261M	144K	3167M
ACESign	425	620	748	26M	20M	9645M
TTS(20,28)	28	$\approx$ 8.7K	$\approx$ 1.4K	16.8K	48K	5.28M
TRMS(20,28)	28	$\approx$ 8.7K	396	11.4K	48K	2.67M

Security Analysis

For brevity, we fix the following notations for our TRMS example:

- $m = 20$ denotes the dimension of the hash space.
- $n = 28$ denotes the dimension of the signature space.
- $q = 2^8$ denotes the size of the base field $GF(256)$.
- $r = 12$ denotes the minimal rank.
- $k_1 = 6$ denotes the number of the linear combinations of the components of φ_2 which reach the minimal rank.
- $u = 9$ denotes the minimal number of appearances in φ_2 for any variable x_i.
- $k_2 = 9$ denotes the maximum size of the set of oil variables.

Security Analysis (continued)

There are several known attacks for multivariate cryptosystems.

Attack	Complexity	Note
Rank Attack	2^{101} 3DES units	$q^r \cdot \frac{(m^2(\frac{n}{2}-\frac{m}{6})+mn^2)}{k_1}$
Dual Rank Attack	2^{80} 3DES units	$q^u(un^2+\frac{n^3}{6})$
UOV Attack	2^{80} 3DES units	$k_2^4 q^{n-2k_2-1}$
Patarin Relation Attack	Not Applicable	no Patarin relation
Affine Parts Distillation	Not Applicable	not homogeneous
XL Family & Gröbner Basis	2^{74} 3DES units	F$\mathbf{F_5}$ if $O(n^{2+\varepsilon})$ timing can be achieved
Finding Minus and Vinegar Variables	Not Applicable	with non-constant central parts
Patarin's IP Approach	Not Applicable	variable parameters in the middle map
Search Methods	2^{120} 3DES units	not small finite fields

Thank you for your attention!

Rank Attack

Goubin and Courtois shows that the MinRank attack for Triangular-Plus-Minus systems. Yang and Chen generalized the idea to Rank attack for multivariate systems in [37]. The complexity of the Rank attack is about $q^r \cdot \frac{(m^2(\frac{n}{2} - \frac{m}{6}) + mn^2)}{k}$ multiplications, where k is the number of linear combinations of the components of φ_2 which reach the minimal rank r. The minimal rank for our example is at least 12, and k is 6. Therefore the complexity is about 2^{107} multiplications or 2^{101} 3DES units (1 unit of 3DES $\approx 2^6$ multiplications).

Dual Rank Attack

Yang and Chen proposed the Dual Rank attack for multivariate systems in [37]. The complexity of the Dual Rank attack is about $q^u(un^2 + \frac{n^3}{6})$ multiplications where u is the minimal number of appearances in φ_2 for any variable x_i. When $u = 9$ for our sample scheme, the complexity is about 2^{86} multiplications or 2^{80} 3DES units.

Unbalanced Oil and Vinegar Attack

As in [37], Let an "oil-set" be any set of independent variables x_i, such that any of their cross-products never appears in any equation in φ_2. Suppose the maximum size of an oil set is k, then then we may determine in time $k^4 q^{n-2k-1}$ the "vinegar" and the "oil" subspaces. After that, several possible techniques may be used to find a solution. If case $k = 9$, so the time taken to identify the vinegar and oil subspaces is about 2^{80} 3DES units.

Patarin Relations Attack for C^* family

In φ_2 of our TRMS example, there is no Patarin relation, which means the attack for C^* family is not feasible for our system.

Affine Parts Distillation

Geiselmann et al. in [18, 19] pointed out the possibility that if the middle portion of any multivariate system is homogeneous of degree two, then it is possible to find the constant parts of both affine mappings easily. The φ_2 in our TRMS example is not homogeneous.

XL Family and Gröbner Bases

Courtois et al proposed the XL method for solving overdetermined quadratic system (which can be viewed as a refinement of the relinearization method by Kipnis-Shamir, [23]) and its variant FXL in [10]. Faugère ([14, 15]) have been improving algorithms for computing Gröbner Bases, and the current state-of-the art variant is $\mathbf{F_5}$, which was used as the critical equation solver in breaking the HFE challenge 1 ([16]).
The consensus of current research ([1, 2, 3, 12, 38, 39]) is that Gröbner/XL-like equation solvers on generic equations are exponential in the number of variables. The best variant will be F$\mathbf{F_5}$ if $O(n^{2+\varepsilon})$ timing can be achieved, and FXL otherwise. The time complexity for the two methods on a system with $m = 20$ equations will be respectively 2^{74} and 2^{76} 3DES units, still better than RSA-1024 (see [28]). If $m = 24$, then we would get 2^{80} and 2^{81} respectively.

Remark

The speed estimates on nongeneric equations are still being debated, but the converse to Moh's lemma was proved in [38], which shows that it is likely that all Gröbner/XL-like equation solvers will run into trouble if the dimension of the projective solution set at infinity (denoted $\dim H_\infty$) is non-zero. It is not very easy to benefit from this, however, because the UOV attack means that the last stage of our sample TRMS scheme or something similar cannot be too large, and the dual rank attack dictates that it cannot be too small! Thus for $m = 20$, we cannot benefit $\dim H_\infty > 0$, because the last stage is forced to be 9 variables. For larger TRMS schemes, say $m = 28$ upwards, we can start to do better with optimal selection of parameters.

Finding Minus and Vinegar Variables

These are very specialized methods designed against what is generally called "Big-Field" multivariate schemes such as C^{*--}. They do not work against tame-like multivariates with non-constant central parts.

Patarin's IP approach

Patarin et al proposed an attack method for fixed middle map schemes in [30, 31]. Since there are variable parameters in the middle map, the IP attack is not applicable.

Search Methods

Courtois et al proposed some search methods at PKC 2002 in [6]. However, they are mainly designed for small finite fields, and we may follow the computations of [4] to find a complexity of 2^{120} 3DES units.

Time line

- 1996/8 TTM (patent application)
- 2002/6 TTS (IWAP 2002)
- 2002/10 TRMC and TRMS (patent application)
- 2003/8 TTS/2 and TTS/4 (eprint)
- 2004/2/18 TRMC and TRMS with field extensions (eprint)
- 2004/2/22 Enhanced TTS (eprint)

[1] G. Ars and J.-C. Faugère, *Comparison of XL and Gröbner Bases Algorithms over Finite Fields*, preprint. Will appear as one half of an article at Asiacrypt 2004 and LNCS.

[2] M. Bardet, J.-C. Faugère, and B. Salvy, *Complexity of Gröbner Basis Computations for Regular Overdetermined Systems*, INRIA Rapport de Recherche No. 5049; a slightly modified preprint is accepted by the International Conference on Polynomial System Solving.

[3] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang, *Asymptotic Complexity of Gröbner Basis Algorithms for Semi-regular Overdetermined Systems over Large Fields*, manuscript in preparation.

[4] J.-M. Chen and B.-Y. Yang, *Tame Transformations Signatures With Topsy-Turvy Hashes*, proc. IWAP 2002, Taipei.

[5] J.-M. Chen and B.-Y. Yang, *A More Secure and Efficacious TTS Scheme*, ICISC 2003, LNCS v. 2971, pp. 320-338; full version at `eprint.iacr.org/2003/160`.

[6] N. Courtois, L. Goubin, W. Meier, and J. Tacier, *Solving Underdefined Systems of Multivariate Quadratic Equations*, PKC 2002, LNCS v. 2274, pp. 211-227

[7] N. Courtois, *Generic Attacks and the Security of Quartz*, PKC 2003, LNCS v. 2567, pp. 351-364.

[8] N. Courtois, *Algebraic Attacks over GF*(2^k)*, Cryptanalysis of HFE Challenge 2 and SFLASH*^{v2}, accepted for PKC 2004.

[9] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, EUROCRYPT 2000, LNCS v. 1807, pp. 392-407.


[10] N. Courtois and J. Patarin, *About the XL Algorithms over GF(2)*, CT-RSA 2003, LNCS v. 2612, pp. 141-157.


[11] N. Courtois, L. Goubin, and J. Patarin, *SFLASH^{v3}, a Fast Asymmetric Signature Scheme*, preprint


[12] C. Diem, *The XL-algorithm and a Conjecture from Commutative Algebra*, preprint (to appear Asiacrypt 2004 and LNCS) and private communication.


[13] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Trans. Info. Theory, vol. IT-22, no. 6, pp. 644-654.


[14] J.-C. Faugére, *A New Efficient Algorithm for Computing Gröbner Bases (F4)*, Journal of Pure and Applied Algebra, 139 (1999), pp. 61–88.


[15] J.-C. Faugère, *A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5)*, Proc. ISSAC 2002, pp. 75-83, ACM Press 2002.


[16] J.-C. Faugère and A. Joux, *Algebraic Cryptanalysis of Hidden Field Equations (HFE) Cryptosystems Using Gröbner Bases*, Crypto 2003, LNCS v. 2729, pp. 44-60.


[17] M. Garey and D. Johnson, *Computers and Intractability, A Guide to the Theory of NP-completeness*, 1979, p. 251.


[18] W. Geiselmann, R. Steinwandt, and T. Beth, *Attacking the Affine Parts of SFLASH*, 8th International IMA Conference on Cryptography and Coding, LNCS v. 2260, pp. 355-359.


[19] W. Geiselmann, R. Steinwandt, and T. Beth, *Revealing the 441 Key Bits of SFLASH^{v2}*, Third NESSIE Workshop, 2002.


[20] L. Goubin and N. Courtois, *Cryptanalysis of the TTM cryptosystem*, Asiacrypt 2000, LNCS v. 1976, pp. 44-57.


[21] A. Kipnis and A. Shamir, *Cryptanalysis of the Oil and Vinegar Signature Scheme*, Crypto'98, LNCS v. 1462, pp. 257-266

[22] A. Kipnis, J. Patarin, and L. Goubin, *Unbalanced Oil and Vinegar Sigature Schemes*, Crypto'99, LNCS v. 1592, pp. 206-222

[23] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, Crypto'99, LNCS v. 1666, pp. 19-30

[24] T. Matsumoto and H. Imai, *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, EUROCRYPT'88, LNCS v. 330, pp. 419-453.

[25] T. Moh, *A Public Key System with Signature and Master Key Functions, Communications in Algebra*, 27 (1999), pp. 2207-2222.

[26] T. Moh and J. -M. Chen, *On the Goubin-Courtois Attack on TTM*, published electronically by Cryptology ePrint Archive (2001/072).


[27] *New European Schemes for Signatures, Integrity, and Encryption*, project homepage at http://www.cryptonessie.org.


[28] *Performance of Optimized Implementations of the NESSIE primitives, version 2.0* http://www.cryptonessie.org.


[29] J. Patarin, *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, Crypto'95, LNCS v. 963, pp. 248-261.


[30] J. Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) Two New Families of Asymmetric Algorithms*, EUROCRYPT'96, LNCS v. 1070, pp. 33-48.


[31] J. Patarin, L. Goubin, N. Courtois, *Improved Algorithm for Isomorphisms of Polynomials*, EUROCRYPT'98, LNCS v. 1403, pp. 184-200.


[32] J. Patarin, N. Courtois, and L. Goubin, *QUARTZ, 128-Bit Long Digital Signatures*, CT-RSA 2001, LNCS v. 2020,

pp. 282-297. Updated version available at http://www.cryptonessie.org.


[33] J. Patarin, N. Courtois, and L. Goubin, FLASH, *a Fast Multivariate Signature Algorithm*, CT-RSA 2001, LNCS v. 2020, pp. 298-307. Updated version available at http://www.cryptonessie.org.


[34] A. Shamir and E. Tromer, *Factoring Large Numbers with the TWIRL Device*, Crypto 2003, LNCS v. 2729, pp. 1-26.


[35] Lih-Chung Wang and Fei-Hwang Chang, *Tractable Rational Map Cryptosystem*, available at http://eprint.iacr.org/2004/046.


[36] C. Wolf, *Efficient Public Key Generation for Multivariate Cryptosystems, preprint*, available at http://eprint.iacr.org/2003/089.

[37] B.-Y. Yang and J.-M. Chen, *Rank Attacks and Defence in Tame-Like Multivariate PKC's*, see `http://eprint.iacr.org/2004/061`.

[38] B.-Y. Yang and J.-M. Chen, *All in the XL Family: Theory and Practice*, to appear at ICISC 2004 and LNCS.

[39] B.-Y. Yang, J.-M. Chen, and N. Courtois, *On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis*, ICICS 2004, LNCS v. 3269, pp. 401-413.