Solving multivariate polynomial systems over finite fields : Hybrid approach

Luk Bettale[1], Jean-Charles Faugère, Ludovic Perret

LIP6 - SALSA
UPMC, CNRS, INRIA Paris-Rocquencourt

Journées Nationales du Calcul Formel
Luminy, Mai 2010

[1]author partially supported by DGA/MRIS (french secretary of defense)

Outline

Motivations

- Algebraic cryptanalysis
- General algorithms
- Design of cryptographic schemes.

Given $f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n)$ of $\mathbb{F}_q[x_1,\dots,x_n]$, does there exist $z_1,\dots,z_n \in \mathbb{F}_q^n$ such that:

$$\begin{cases} f_1(z_1,\dots,z_n) = 0 \\ \vdots \\ f_m(z_1,\dots,z_n) = 0 \end{cases}$$

Polynomial System Solving

Given $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)$ of $\mathbb{F}_q[x_1,\ldots,x_n]$, does there exist $z_1,\ldots,z_n \in \mathbb{F}_q^n$ such that:

$$\begin{cases} f_1(z_1,\ldots,z_n) = 0 \\ \qquad\vdots \\ f_m(z_1,\ldots,z_n) = 0 \end{cases}$$

- Polynomial System Solving is NP-hard
- Hard in practice for generic polynomials.

Known methods

- Exhaustive search
- Gröbner bases
- Gröbner bases with field equations

- Exhaustive search
- Gröbner bases
- Gröbner bases with field equations

Gröbner bases algorithms

Algorithms

- Buchberger : the historical algorithm
- F_4 : linear algebra on matrices
- F_5 : no useless computations for semi-regular systems

Jean-Charles Faugère.
A new efficient algorithm for computing Gröbner bases (F_4).
Journal of Pure and Applied Algebra 139, June 1999.

Jean-Charles Faugère.
A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5).
ISSAC 2002, July 2002.

Algorithms

- Buchberger : the historical algorithm
- F_4 : linear algebra on matrices
- F_5 : no useless computations for semi-regular systems

$$\mathrm{F}_5 : \mathcal{O}\left(\left(m \cdot \binom{n+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}\right)^{\omega}\right), \quad \mathrm{FGLM} : \mathcal{O}\left(n \cdot D^{w}\right),$$

with $2 \leqslant \omega \leqslant 3$, D the number of solutions in $\overline{\mathbb{K}}$.

Magali Bardet, Jean-Charles Faugère, Bruno Salvy and Bo-Yin Yang.
Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.
MEGA 2005.

Gröbner bases algorithms

Algorithms

- F_5 : no useless computations for semi-regular systems

$$F_5 : \mathcal{O}\left(\left(m \cdot \binom{n+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}\right)^{\omega}\right), \quad \mathrm{FGLM} : \mathcal{O}\left(n \cdot D^{w}\right),$$

with $2 \leqslant \omega \leqslant 3$, D the number of solutions in $\overline{\mathbb{K}}$.

Semi-regular systems

- A system of unrelated polynomials
- The degree of regularity (d_{reg}) can be known a priori
- The more equations we have, the more d_{reg} decrease.

  (e.g. for quadratic systems)
  $m : n \rightarrow n+1$ $\qquad$ $d_{reg} : n+1 \rightarrow \lceil \frac{n+1}{2} \rceil$

Algorithms

- F_5 : no useless computations for semi-regular systems

$$\mathrm{F}_5 : \mathcal{O}\left(\left(m \cdot \binom{n+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}\right)^{\omega}\right), \quad \mathrm{FGLM} : \mathcal{O}\left(n \cdot D^{w}\right),$$

with $2 \leqslant \omega \leqslant 3$, D the number of solutions in $\overline{\mathbb{K}}$.

Semi-regular systems

- A system of unrelated polynomials $\approx$ a random system
- The degree of regularity (d_{reg}) can be known a priori
- The more equations we have, the more d_{reg} decrease.

  (e.g. for quadratic systems)
  $m : n \to n+1$ $d_{reg} : n+1 \to \lceil \frac{n+1}{2} \rceil$

Solving a system – General approach

$f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ for $1 \leqslant i \leqslant n$

$$\left\{ \begin{array}{c} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_n(x_1, \ldots, x_n) = 0 \end{array} \right.$$

Solving a system – General approach

$f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ for $1 \leqslant i \leqslant n$

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

Specificity ($m = n$)

- Random systems $\Rightarrow d_{reg} = n(d-1)+1$
- Square systems $\Rightarrow d^n$ solutions in the algebraic closure.
- $\mathbb{F}_q$ is finite and rather big (no field equations).

Solving a system – Hybrid approach

Solution

We specialize k variables of the system (exhaustive search)
$\Rightarrow$ the system becomes over-defined

+ The degree of regularity decreases
+ The number of solutions is 0 or 1
- We have to compute q^k Gröbner bases.

Luk Bettale, Jean-Charles Faugère and Ludovic Perret.
Hybrid approach for solving multivariate systems over finite fields.
In Journal of Mathematical Cryptology, Volume 3, issue 3. Sep 2009.

Solving a system – Hybrid approach

Solution

We specialize k variables of the system (exhaustive search)
$\Rightarrow$ the system becomes over-defined

+ The degree of regularity decreases
+ The number of solutions is 0 or 1
- We have to compute q^k Gröbner bases.

Luk Bettale, Jean-Charles Faugère and Ludovic Perret.
Hybrid approach for solving multivariate systems over finite fields.
In Journal of Mathematical Cryptology, Volume 3, issue 3. Sep 2009.

A tradeoff between exhaustive search and Gröbner bases computation.

Proposition

Let $\mathbb{F}_q$ be a finite field and $\{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular system of equations of degree d.

$$\mathcal{O}\left(\underbrace{\min_{0 \leqslant k \leqslant n}}_{\text{tradeoff}} \left(\underbrace{q^k}_{\text{exh. search}} \underbrace{\left(n \cdot \binom{n-k-1+\mathrm{d_{reg}}(n-k,n,d)}{\mathrm{d_{reg}}(n-k,n,d)}\right)^{\omega}}_{F_5} \underbrace{+n \cdot D^{\omega}}_{FGLM} \right)\right),$$

where $2 \leqslant \omega \leqslant 3$.

$\mathrm{d_{reg}}(n, m, d)$ is the d_{reg} of a semi-regular system of m equations of degree d in n variables.

Proposition

Let $\mathbb{F}_q$ be a finite field and $\{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular system of equations of degree d.

$$\mathcal{O}\left(\underbrace{\min_{0 \leqslant k \leqslant n}}_{\text{tradeoff}}\left(\underbrace{q^k}_{\text{exh. search}}\underbrace{\left(n \cdot \binom{n-k-1+\mathrm{d_{reg}}(n-k,n,d)}{\mathrm{d_{reg}}(n-k,n,d)}\right)^{\omega}}_{F_5}\underbrace{+n \cdot D^{\omega}}_{FGLM}\right)\right),$$

where $2 \leqslant \omega \leqslant 3$.

$\mathrm{d_{reg}}(n, m, d)$ is the d_{reg} of a semi-regular system of m equations of degree d in n variables.

The degree of regularity can be computed exactly.

Complexity analysis

Proposition

Let $\mathbb{F}_q$ be a finite field and $\{f_1,\ldots,f_n\} \subset \mathbb{F}_q[x_1,\ldots,x_n]$ be a semi-regular system of equations of degree d.

$$\mathcal{O}\left(\underbrace{\min_{1\leqslant k\leqslant n}}_{\text{tradeoff}}\left(\underbrace{q^k}_{\text{exh. search}}\underbrace{\left(n\cdot\binom{n-k-1+\mathrm{d_{reg}}(n-k,n,d)}{\mathrm{d_{reg}}(n-k,n,d)}\right)^{\omega}}_{F_5}\right)\right),$$

where $2 \leqslant \omega \leqslant 3$.

$\mathrm{d_{reg}}(n,m,d)$ is the d_{reg} of a semi-regular system of m equations of degree d in n variables.

The degree of regularity can be computed exactly.

Asymptotic analysis $(d = 2)$

Approximation of $\mathrm{d}_{\mathrm{reg}}(n-k,n,2)$

$$d_{reg} \sim \frac{n+k}{2} - \sqrt{nk} + \mathcal{O}((n-k)^{1/3})$$

when $n \to \infty$.

Magali Bardet

Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.

Ph.D. thesis, Université de Paris VI, 2004.

Approximation of the complexity

$$C_{Hyb} = \mathcal{O}\left(q^k \left(\frac{n}{\sqrt{2\pi}}\right)^{\omega} \left(\frac{\left(\frac{3n-k}{2} - 1 - \sqrt{nk}\right)^{(3n-k-1)/2-\sqrt{nk}}}{(n-k-1)^{(n-k-1/2)} \left(\frac{n+k}{2} - \sqrt{nk}\right)^{(n+k+1)/2-\sqrt{nk}}} \right)^{\omega} \right)$$

when $n \to \infty$.

Finding the best tradeoff $(d=2)$

Find the best tradeoff by solving $\dfrac{\partial \log(C_{Hyb})}{\partial k} = 0.$

$$
\begin{aligned}
&\log(q) + \omega\left(\log(n-k-1) + \frac{1}{2(n-k-1)}\right) \\
&-\frac{\omega}{2}(1+\sqrt{n/k})\left(\log\left(\frac{3n-k}{2} - 1 - \sqrt{nk}\right) + \frac{1}{2\left(\frac{3n-k}{2} - 1 - \sqrt{nk}\right)}\right) \\
&-\frac{\omega}{2}(1-\sqrt{n/k})\left(\log\left(\frac{n+k}{2} - \sqrt{nk}\right) + \frac{1}{2\left(\frac{n+k}{2} - \sqrt{nk}\right)}\right) = 0.
\end{aligned}
$$

Find the best tradeoff by solving $\dfrac{\partial \log(C_{Hyb})}{\partial k} = 0.$

$$k \approx \frac{n}{c^2}$$

$$8\,q\,(c-1)^{3\,c-3}\,e^{-3/2\,c\ln((3\,c+1)(c-1))}\,(c-1)^3\,(c+1)^3$$
$$-((3\,c+1)\,(c-1))^{3/2} = 0$$

q	2	16	256	65521	2^{32}	2^{64}	2^{80}
c^2	1.23	3.07	9.15	37.13	160.37	678.32	1073.1

Borderline case ($d = 2$)

Classical approach

($d_{reg} = n + 1$)

$$\mathcal{O}\left(\left(n \cdot \binom{2n}{n-1}\right)^{\omega}\right).$$

Hybrid approach with $k = 1$

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

$$\mathcal{O}\left(q\left(n \cdot \binom{3(n-1)/2}{n-2}\right)^{\omega}\right).$$

Best tradeoff > 0

$$\log_2(q) \leq 0.6226 \cdot \omega \cdot n + \mathcal{O}(\log_2(n))$$

when $n \to \infty$.

Borderline case $(d = 2)$

Classical approach

$(d_{reg} = n+1)$

$$\mathcal{O}\left(\left(n \cdot \binom{2n}{n-1}\right)^{\omega}\right).$$

Hybrid approach with $k = 1$

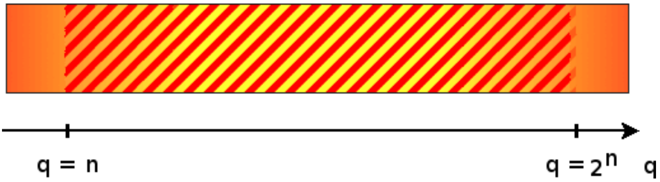
$(d_{reg} = \lceil \frac{n+1}{2} \rceil)$

$$\mathcal{O}\left(q\left(n \cdot \binom{3(n-1)/2}{n-2}\right)^{\omega}\right).$$

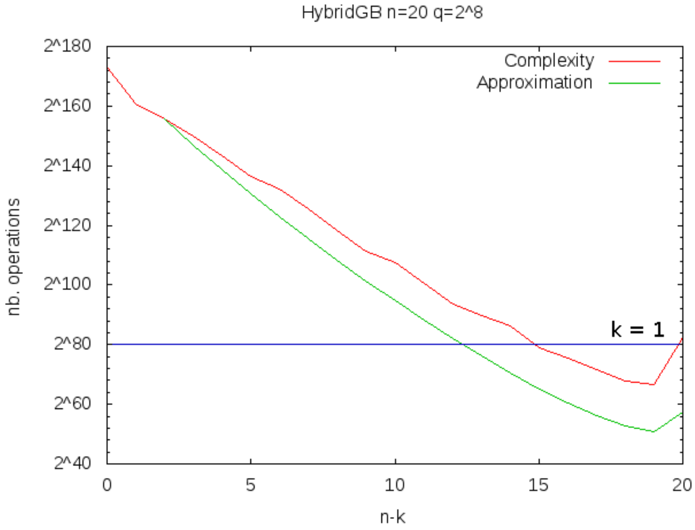
Best tradeoff > 0

$$\log_2(q) \leq 0.6226 \cdot \omega \cdot n + \mathcal{O}(\log_2(n))$$

when $n \to \infty$.

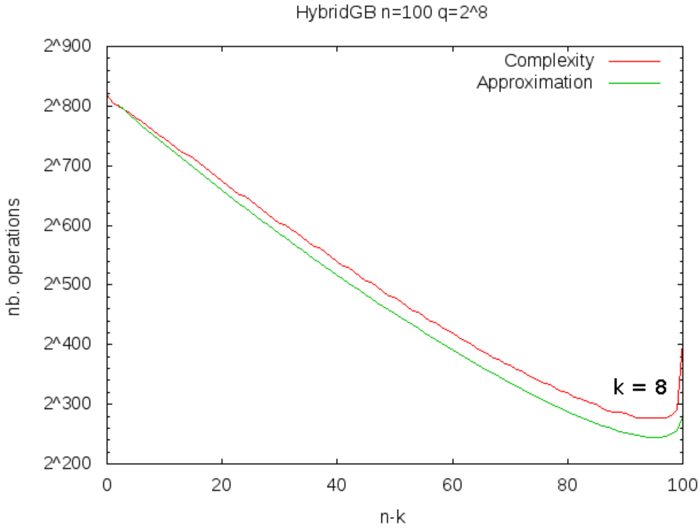


Comparison

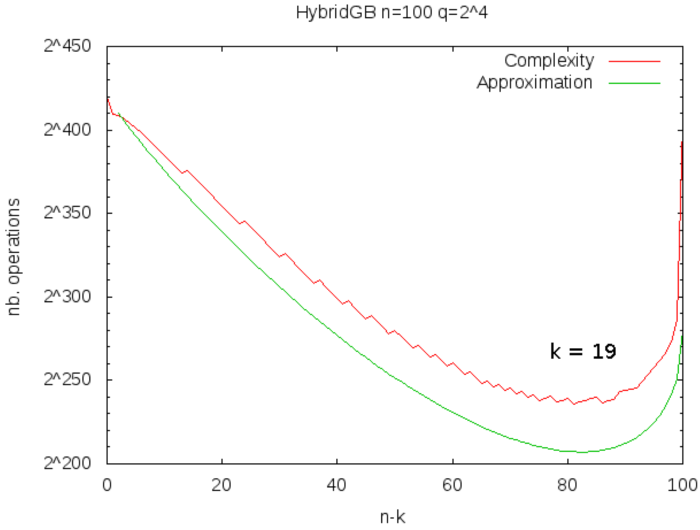


HybridGB n=20 q=2^8
Complexity
Approximation
k = 1
2^180
2^160
2^140
2^120
2^100
2^80
2^60
2^40
nb. operations
0
5
10
15
20
n-k

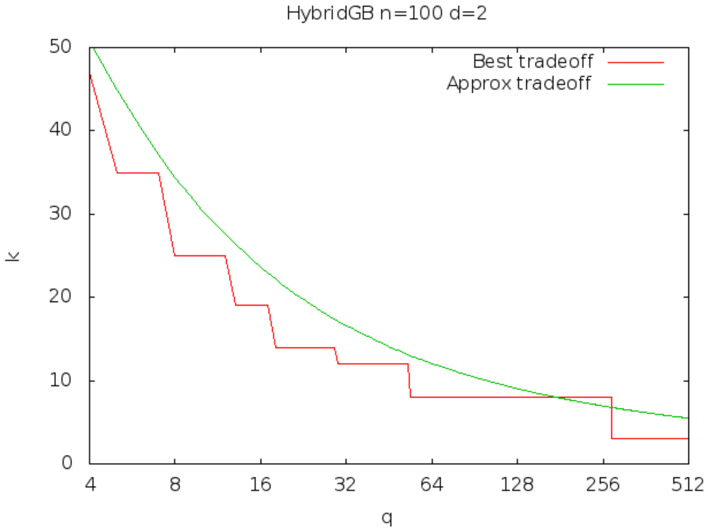
Comparison


HybridGB n=100 q=2^8
Complexity
Approximation
nb. operations
2^900
2^800
2^700
2^600
2^500
2^400
2^300
2^200
k = 8
0
20
40
60
80
100
n-k

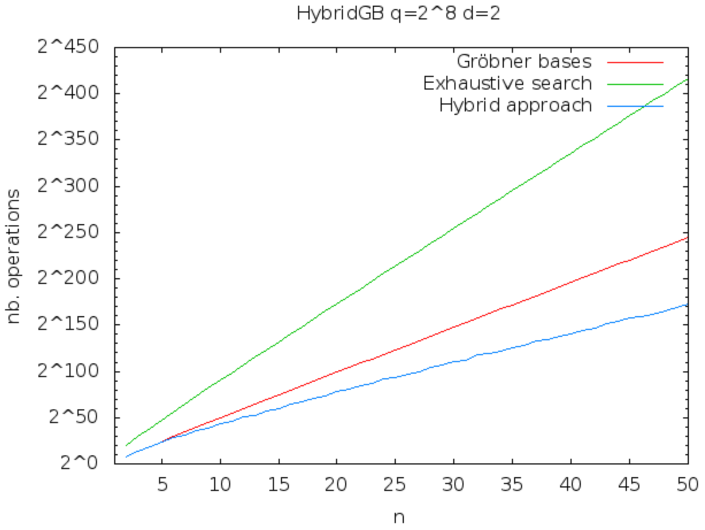
Comparison


HybridGB n=100 q=2^4
Complexity
Approximation
nb. operations
2^450
2^400
2^350
2^300
2^250
2^200
0
20
40
60
80
100
n-k
k = 19

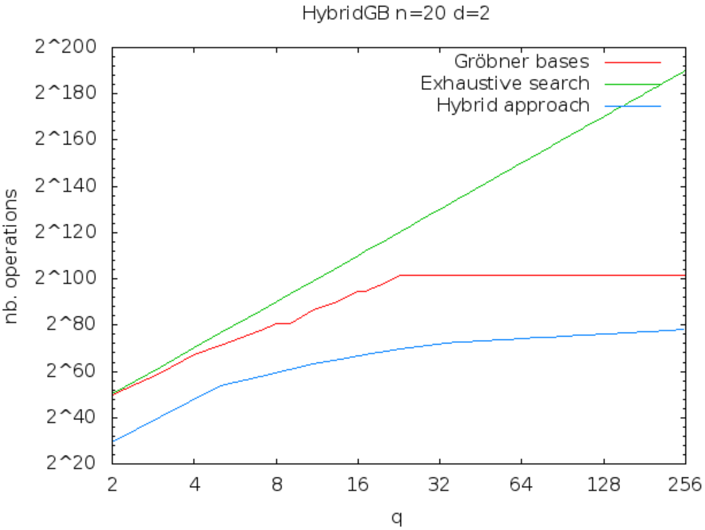
The best tradeoff



Overall


HybridGB q=2^8 d=2
2^450
2^400
2^350
2^300
2^250
2^200
2^150
2^100
2^50
2^0
nb. operations
5
10
15
20
25
30
35
40
45
50
n
Gröbner bases
Exhaustive search
Hybrid approach

Overall



HybridGB n=20 d=2
Gröbner bases
Exhaustive search
Hybrid approach
nb. operations
2^200
2^180
2^160
2^140
2^120
2^100
2^80
2^60
2^40
2^20
2
4
8
16
32
64
128
256
q

Input: $\mathbb{K}$ is finite, $\{f_1, \ldots, f_m\} \subset \mathbb{K}[x_1, \ldots, x_n]$ is zero-dimensional, $k \in \mathbb{N}$.

Output: $\mathcal{S} = \{(z_1, \ldots, z_n) \in \mathbb{K}^n : f_i(z_1, \ldots, z_n) = 0, 1 \leq i \leq m\}$.

$\mathcal{S} := \emptyset$

for all $(v_1, \ldots, v_k) \in \mathbb{K}^k$ **do**

Find the set of solutions $\mathcal{S}' \subset \mathbb{K}^{(n-k)}$ of

$$\begin{cases} f_1(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k) = 0 \end{cases}$$

using the zero-dim solving strategy.

$\mathcal{S} := \mathcal{S} \cup \{(z'_1, \ldots, z'_{n-k}, v_1, \ldots, v_k) : (z'_1, \ldots, z'_{n-k}) \in \mathcal{S}'\}$.

end for

return $\mathcal{S}$.

Algorithm (MAGMA)

```
function HybridSolving(F,k)
    R := Universe(F); K := BaseRing(R); n := Rank(R);
    Rp<[x]> := PolynomialRing(K,n-k);
    Kev := VectorSpace(K,k);
    S := [ ];
    for e in Kev do
        v := Eltseq(e);
        fp := [ Evaluate(f,x cat v) : f in F ];
        Sp := VarietySequence(Ideal(fp));
        S cat:= [ s cat v : s in Sp ];
    end for;
    return S;
end function;
```

http://www-salsa.lip6.fr/~bettale/hybrid.html

Multivariate cryptography

Properties

- The public key is a quadratic system
- Very efficient (hardware)
- Resist quantum computers.

Examples

- C^*, HFE
- UOV, SFLASH
- ...

Unbalanced Oil and Vinegar

Secret key

$$\begin{array}{rcl} \mathbf{F}: \quad \mathbb{F}_q^{n+r} & \rightarrow & \mathbb{F}_q^n \\ (x_1,\ldots,x_{n+r}) & \rightarrow & (f_1(x_1,\ldots,x_{n+r}),\ldots,f_n(x_1,\ldots,x_{n+r})) \end{array}$$

Easy to invert

$T \in \mathrm{GL_{n+r}}(\mathbb{F}_q)$

Public key

$$\begin{array}{rcl} \mathbf{G}: \quad \mathbb{F}_q^{n+r} & \rightarrow & \mathbb{F}_q^n \\ (x_1,\ldots,x_{n+r}) & \rightarrow & (g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)) \end{array}$$

$\mathbf{G} = \mathbf{F} \circ T = \mathbf{F}(\mathbf{x} \cdot T)$.

$\mathrm{Verify}_{\mathbf{G}}(\mathbf{x})$: Evaluate $\mathbf{G}(\mathbf{x})$

Unbalanced Oil and Vinegar

Secret key

$$\begin{array}{rcl} \mathbf{F}: \quad \mathbb{F}_q^{n+r} & \to & \mathbb{F}_q^n \\ (x_1,\ldots,x_{n+r}) & \to & (f_1(x_1,\ldots,x_{n+r}),\ldots,f_n(x_1,\ldots,x_{n+r})) \end{array}$$

Easy to invert

$$f_k = \sum_{x_i\in O, x_j\in V} a_{i,j}^{(k)} x_i x_j + \sum_{x_i,x_j\in V} a_{i,j}^{(k)} x_i x_j + \sum_{x_i\in O\cup V} a_i^{(k)} x_i$$

$T \in \mathrm{GL_{n+r}}(\mathbb{F}_q)$

Public key

$$\begin{array}{rcl} \mathbf{G}: \quad \mathbb{F}_q^{n+r} & \to & \mathbb{F}_q^n \\ (x_1,\ldots,x_{n+r}) & \to & (g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)) \end{array}$$

$\mathbf{G} = \mathbf{F} \circ T = \mathbf{F}(\mathbf{x} \cdot T)$.

$\mathrm{Verify}_{\mathbf{G}}(\mathbf{x})$: Evaluate $\mathbf{G}(\mathbf{x})$

Signature of a message $\mathbf{m} = (m_1, \ldots, m_n)$

1. Pick $(v_1, \ldots, v_r) \in \mathbb{F}_q^r$
2. Solve the linear system

$$\begin{cases} f_1(x_1, \ldots, x_n, v_1, \ldots, v_r) - m_1 = 0 \\ \vdots \\ f_n(x_1, \ldots, x_n, v_1, \ldots, v_r) - m_n = 0 \end{cases}$$

3. $\mathbf{s} = (z_1, \ldots, z_n, v_1, \ldots, v_r) \cdot T^{-1}$

Verification of the signature $\mathbf{s} = (s_1, \ldots, s_{n+r})$

$$\mathbf{m} = (g_1(s_1, \ldots, s_{n+r}), \ldots, g_n(s_1, \ldots, s_{n+r}))$$

Unbalanced Oil and Vinegar

Signature of a message $\mathbf{m} = (m_1, \ldots, m_n)$

1. Pick $(v_1, \ldots, v_r) \in \mathbb{F}_q^r$
2. Solve the linear system

$$\begin{cases} f'_1(x_1, \ldots, x_n) - m_1 = 0 \\ \vdots \\ f'_n(x_1, \ldots, x_n) - m_n = 0 \end{cases}$$

3. $\mathbf{s} = (z_1, \ldots, z_n, v_1, \ldots, v_r) \cdot T^{-1}$

Verification of the signature $\mathbf{s} = (s_1, \ldots, s_{n+r})$

$$\mathbf{m} = (g_1(s_1, \ldots, s_{n+r}), \ldots, g_n(s_1, \ldots, s_{n+r}))$$

Signature forgery attack

Given a message $\mathbf{m} = (m_1, \ldots, m_n)$, find a signature $(s_1, \ldots, s_{n+r})$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{m}$.

Signature forgery attack

Given a message $\mathbf{m} = (m_1, \ldots, m_n)$, find a signature $(s_1, \ldots, s_{n+r})$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{m}$.

Solve the system

$$\begin{cases} g_1(x_1, \ldots, x_{n+r}) - m_1 = 0 \\ \vdots \\ g_n(x_1, \ldots, x_{n+r}) - m_n = 0 \end{cases}$$

Signature forgery attack

Given a message $\mathbf{m} = (m_1, \ldots, m_n)$, find a signature $(s_1, \ldots, s_{n+r})$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{m}$.

Solve the system

$$\begin{cases} g_1(x_1, \ldots, x_n, y_1, \ldots, y_r) - m_1 = 0 \\ \vdots \\ g_n(x_1, \ldots, x_n, y_1, \ldots, y_r) - m_n = 0 \end{cases}$$

Signature forgery attack

Given a message $\mathbf{m} = (m_1, \ldots, m_n)$, find a signature $(s_1, \ldots, s_{n+r})$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{m}$.

Solve the system

$$\begin{cases} g'_1(x_1, \ldots, x_n) - m_1 = 0 \\ \vdots \\ g'_n(x_1, \ldots, x_n) - m_n = 0 \end{cases}$$

Signature forgery attack

Given a message $\mathbf{m} = (m_1, \ldots, m_n)$, find a signature $(s_1, \ldots, s_{n+r})$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{m}$.

Solve the system

$$\begin{cases} g'_1(x_1,\ldots,x_n) - m_1 = 0 \\ \vdots \\ g'_n(x_1,\ldots,x_n) - m_n = 0 \end{cases}$$

Parameters: $q = 2^4, n = 16$.

An Braeken, Bart Preneel, and Christopher Wolf
A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes
CT-RSA 05.

q	n	k	T_{F_5}	mem. (MB)	Nop_{F_5}	Nop
2^4	16	1	$\approx$ 1 h	3532	$2^{36.9}$	$2^{40.9}$
		2	126 s	270	$2^{32.3}$	$2^{40.5}$
		3	9.41 s	38	$2^{28.7}$	$2^{40.7}$

Best tradeoff : $k = 2$. Broken in $\leqslant$ 9h.

Jean-Charles Faugère, and Ludovic Perret.
On the security of UOV.
SCC 2008.

Analysis of several multivariate schemes

	n	q	expected security	Gröbner basis ($k=0$)	hybrid approach		mem.
UOV_{30}	10	2^8	2^{80}	2^{41}	2^{37}	($k=1$)	2 MB
UOV_{60}	20	2^8	2^{160}	2^{82}	2^{66}	($k=1$)	139 GB
enTTS					2^{67}	($k=2$)	12 GB
Rainbow	24	2^8	2^{192}	2^{98}	2^{78}	($k=1$)	10 TB
amTTS					2^{79}	($k=2$)	816 GB

Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf
Time-Area Optimized Public-Key Engines: MQ-Cryptosystems as Replacement for Elliptic Curves?
CHES '08: Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems

Analysis of several multivariate schemes

	n	q	expected security	Gröbner basis $(k=0)$	hybrid approach	mem.
UOV_{30}	10	2^8	2^{80}	2^{41}	2^{37} $(k=1)$	2 MB
UOV_{60}	20	2^8	2^{160}	2^{82}	2^{66} $(k=1)$	139 GB
enTTS					2^{67} $(k=2)$	12 GB
Rainbow	24	2^8	2^{192}	2^{98}	2^{78} $(k=1)$	10 TB
amTTS					2^{79} $(k=2)$	816 GB

Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf
Time-Area Optimized Public-Key Engines: MQ-Cryptosystems as Replacement for Elliptic Curves?
CHES '08: Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems

Applications in cryptography

- A general tool for solving random systems over finite field
- Reevaluate parameters of multivariate cryptosystems
- Natural generalization : Block hybrid approach
- Implementation in MAGMA.
  `http://www-salsa.lip6.fr/~bettale/hybrid.html`