Hybrid Approach: a Tool for Multivariate Cryptography

Luk Bettale\(^1\)  Jean-Charles Faugère  Ludovic Perret

LIP6 - SALSA
UPMC, CNRS, INRIA Paris-Rocquencourt

Workshop on Tools for Cryptanalysis 2010
Royal Holloway University of London
June 2010

\(^1\)author partially supported by DGA/MRIS (french secretary of defense)
Algebraic Cryptanalysis

General analysis (such as linear, differential)

- Modeling
- Solving (or estimate difficulty)
**Algebraic Cryptanalysis**

General analysis (such as linear, differential)
- Modeling
- **Solving** (or estimate difficulty)
Introduction

Algebraic Cryptanalysis

General analysis (such as linear, differential)
- Modeling
- **Solving** (or estimate difficulty)

Setting parameters of multivariate cryptosystems.
**Properties**
- The public key is a quadratic system
- Very efficient (hardware)
- Resist quantum computers.

**Examples**
- C*, HFE
- UOV, SFLASH
- ...
**Multivariate signature**

### Secret key

\[ \mathbf{F} : \mathbb{F}_q^{n+r} \rightarrow \mathbb{F}_q^n \]
\[ (x_1, \ldots, x_{n+r}) \rightarrow (f_1(x_1, \ldots, x_{n+r}), \ldots, f_n(x_1, \ldots, x_{n+r})) \]

Easy to invert

\[ S, T \in \text{GL}_{n+r}(\mathbb{F}_q) \times \text{GL}_n(\mathbb{F}_q) \]

### Public key

\[ \mathbf{G} : \mathbb{F}_q^{n+r} \rightarrow \mathbb{F}_q^n \]
\[ (x_1, \ldots, x_{n+r}) \rightarrow (g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)) \]

\[ \mathbf{G} = T \circ \mathbf{F} \circ S = \mathbf{F}(x \cdot S) \cdot T. \]

\[ \text{Verify}_\mathbf{G}(s, m): \text{Evaluate } \mathbf{G}(s) = m \]
Signature forgery attack

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

$$
\begin{align*}
    g_1(x_1, \ldots, x_n, y_1, \ldots, y_r) - m_1 &= 0 \\
    \vdots \\
    g_n(x_1, \ldots, x_n, y_1, \ldots, y_r) - m_n &= 0
\end{align*}
$$
Attacks on multivariate signature schemes

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

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

An Braeken, Bart Preneel, and Christopher Wolf.  
A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes.  
*CT-RSA 05.*
Attacks on multivariate signature schemes

**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

\[
\begin{aligned}
g'_1(x_1, \ldots, x_n) - m_1 &= 0 \\
&\vdots \\
g'_n(x_1, \ldots, x_n) - m_n &= 0
\end{aligned}
\]

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

Tractable Rational Map Signature.
*PKC 05.*

**TRMS:** \( q = 2^8, n = 20 \).
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:

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

\[
\begin{align*}
  f_1(z_1, \ldots, z_n) &= 0 \\
  & \vdots \\
  f_m(z_1, \ldots, z_n) &= 0
\end{align*}
\]

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

- Exhaustive search
- Gröbner bases with/without field equations
- ...

Luk Bettale

Introduction
Known methods

- Exhaustive search
- Gröbner bases with/without field equations
- ...

$q = n$
Gröbner bases algorithms

Algorithms

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

GB: $\mathcal{O}\left(m \cdot \left(n + \frac{d_{\text{reg}}}{d_{\text{reg}} - 1}\right)^\omega\right)$, 
FGLM: $\mathcal{O}(n \cdot D^\omega)$,

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

Jean-Charles Faugère.
A new efficient algorithm for computing Gröbner bases ($F_4$).

Jean-Charles Faugère.
A new efficient algorithm for computing Gröbner bases without reduction to zero ($F_5$).
Semi-regular systems

- \( g \cdot f_i \in \langle f_1, \ldots, f_{i-1} \rangle \Rightarrow g \in \langle f_1, \ldots, f_{i-1} \rangle \) if \( \deg(g \cdot f_i) \leq d_{\text{reg}} \).
- Random system \( \Rightarrow \) semi-reg.
- The degree of regularity \( (d_{\text{reg}}) \) can be known \textit{a priori}.
- The more equations we have, the more \( d_{\text{reg}} \) decrease (e.g. for quadratic systems):
  \[
m = n \quad \Rightarrow \quad d_{\text{reg}} = n + 1
  \]
  \[
m = n + 1 \quad \Rightarrow \quad d_{\text{reg}} = \left\lceil \frac{n+1}{2} \right\rceil
  \]

---

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.
Solving a system

\[ f_i \in \mathbb{F}_q[x_1, \ldots, x_n] \quad \text{for } 1 \leq i \leq n \]

\[
\begin{align*}
    f_1(x_1, \ldots, x_n) &= 0 \\
    \vdots \\
    f_n(x_1, \ldots, x_n) &= 0
\end{align*}
\]
Solving a system

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

\[
\begin{align*}
  f_1(x_1, \ldots, x_n) &= 0 \\
  \vdots \\
  f_n(x_1, \ldots, x_n) &= 0
\end{align*}
\]

Specificity \((m = n)\)

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

Hypotheses

- Regular system \(\Rightarrow d_{reg} = n(d - 1) + 1\)
- Semi-regular sub-systems.
**Solution**

We specialize $k$ variables of the system (exhaustive search) 
⇒ 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. 
Solving a system – Hybrid approach

Solution

We specialize $k$ variables of the system (exhaustive search)
⇒ 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.

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 $d$.

\[
\mathcal{O} \left( \min_{0 \leq k \leq n} \left( \frac{q^k}{\text{exh. search}} \frac{n \cdot (n-k-1 + d_{\text{reg}}(n-k,n,d))^{\omega}}{d_{\text{reg}}(n-k,n,d)} \right) + n \cdot D^\omega \right),
\]

where $2 \leq \omega \leq 3$.

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

$$
\mathcal{O} \left( \min_{0 \leq k \leq n} \left( \frac{q^k}{\text{exh. search}} \right) \left( n \cdot (n-k-1 + d_{\text{reg}}(n-k,n,d)) \right)^\omega + n \cdot D^\omega \right),
$$

where $2 \leq \omega \leq 3$.

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

The degree of regularity can be computed exactly.
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 $d$.

$$O \left( \min_{1 \leq k \leq n} \left( \left( q^k \right)^{\frac{n \cdot (n-k-1+d_{reg}(n-k,n,d))}{d_{reg}(n-k,n,d)}} \right)^\omega \right),$$

where $2 \leq \omega \leq 3$.

$d_{reg}(n,m,d)$ 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 \(d_{\text{reg}}(n-k,n,2)\)**

\[
d_{\text{reg}} \sim \frac{n+k}{2} - \sqrt{n}k + O((n-k)^{1/3})
\]

when \(n \to \infty\).

---

**Magali Bardet**

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


---

**Approximation of the complexity**

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

when \(n \to \infty\).
Borderline case \( (d = 2) \)

Classical approach 
\[
(d_{\text{reg}} = n + 1) \quad \mathcal{O} \left( \left( n \cdot \left( \frac{2^n}{n-1} \right) \right)^\omega \right)
\]

Hybrid approach with \( k = 1 \) 
\[
(d_{\text{reg}} = \lceil \frac{n+1}{2} \rceil) \quad \mathcal{O} \left( q \left( n \cdot \left( \frac{3(n-1)/2}{n-2} \right) \right)^\omega \right)
\]

**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

\[ (d_{\text{reg}} = n + 1) \]

\[ \mathcal{O}\left(\left(n \cdot \left(\frac{2^n}{n-1}\right)\right)^\omega\right) \]

Hybrid approach with \( k = 1 \)

\[ (d_{\text{reg}} = \lceil \frac{n+1}{2} \rceil) \]

\[ \mathcal{O}\left(q \left(n \cdot \left(\frac{3(n-1)/2}{n-2}\right)\right)^\omega\right) \]

**Best tradeoff > 0**

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

when \( n \to \infty \).
Finding the best tradeoff ($d = 2$)

Find the best tradeoff by solving

$$\frac{\partial \log(C_{Hyb})}{\partial k} = 0.$$ 

$$\log(q) + \omega \left( \log(n - k - 1) + \frac{1}{2(n - k - 1)} \right)$$ 

$$- \frac{\omega}{2} \left( 1 + \sqrt{n/k} \right) \left( \log \left( \frac{3n - k}{2} - 1 - \sqrt{nk} \right) + \frac{1}{2 \left( \frac{3n - k}{2} - 1 - \sqrt{nk} \right)} \right)$$ 

$$- \frac{\omega}{2} \left( 1 - \sqrt{n/k} \right) \left( \log \left( \frac{n + k}{2} - \sqrt{nk} \right) + \frac{1}{2 \left( \frac{n + k}{2} - \sqrt{nk} \right)} \right) = 0.$$
Finding the best tradeoff \((d = 2)\)

Find the **best tradeoff** by solving

\[
\frac{\partial \log(C_{Hyb})}{\partial k} = 0.
\]

\[
k \approx \frac{n}{c^2}
\]

\[
8q(c-1)^3 c^{-3} e^{-3/2 c \ln((3c+1)(c-1))} (c-1)^3 (c+1)^3
\]

\[
- ((3c+1)(c-1))^{3/2} = 0
\]

<table>
<thead>
<tr>
<th>(q)</th>
<th>2</th>
<th>16</th>
<th>256</th>
<th>65521</th>
<th>(2^{32})</th>
<th>(2^{64})</th>
<th>(2^{80})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c^2)</td>
<td>1.23</td>
<td>3.07</td>
<td>9.15</td>
<td>37.13</td>
<td>160.37</td>
<td>678.32</td>
<td>1073.1</td>
</tr>
</tbody>
</table>
Comparison

$q = 256, n = 20, D = 2$

![Graph showing complexity and approximation](chart.png)

- Complexity
- Approximation
- $2^{80}$

$n-k$

nb. operations

$k = 1$
Comparison

$q = 256, n = 100, D = 2$

![Graph showing the comparison between complexity and approximation for a hybrid approach with parameters $q = 256$, $n = 100$, $D = 2$. The graph plots the number of operations ($y$-axis) against $n-k$ ($x$-axis) for different values of $k$. The red line represents the complexity, and the green line represents the approximation. The graph shows a significant reduction in operations for the approximation compared to the complexity.]
Comparison

\[ q = 16, \ n = 100, \ D = 2 \]

Graph showing the complexity and approximation for \( n-k \) with \( q = 16 \) and \( n = 100 \), indicating a decrease in nb. operations as \( n-k \) increases.

- Complexity: Red line
- Approximation: Green line

Points highlighted:
- \( k = 19 \)
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: $S = \{(z_1, \ldots, z_n) \in \mathbb{K}^n : f_i(z_1, \ldots, z_n) = 0, 1 \leq i \leq m\}$.

$S := \emptyset$

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

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

\[
\begin{align*}
    f_1(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k) &= 0 \\
    & \vdots \\
    f_m(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k) &= 0
\end{align*}
\]

using the zero-dim solving strategy.

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

end for

return $S$. 
Algorithm (MAGMA)

```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;

```
### TRMS: Experimental results

<table>
<thead>
<tr>
<th>$q$</th>
<th>$n$</th>
<th>$k$</th>
<th>$T_{F_5}$</th>
<th>mem. (MB)</th>
<th>$Nop_{F_5}$</th>
<th>$Nop$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$2^8$</td>
<td>20</td>
<td>2</td>
<td>51h</td>
<td>41940</td>
<td>$2^{41}$</td>
<td>$2^{57}$</td>
</tr>
<tr>
<td>3</td>
<td>2h45</td>
<td>4402</td>
<td></td>
<td></td>
<td>$2^{37}$</td>
<td>$2^{61}$</td>
</tr>
<tr>
<td>4</td>
<td>626s</td>
<td>912</td>
<td></td>
<td></td>
<td>$2^{34}$</td>
<td>$2^{66}$</td>
</tr>
</tbody>
</table>

Practical tradeoff: $k = 2$. Broken in $< 51h$ on $2^{16}$ proc.

---

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of the TRMS Signature Scheme of PKC'05. *AFRICACRYPT 2008.*
Analysis of several multivariate schemes

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

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

<table>
<thead>
<tr>
<th>Scheme</th>
<th>$n$</th>
<th>$q$</th>
<th>expected security</th>
<th>$k=0$</th>
<th>$k=1$ hybrid</th>
<th>mem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UOV$_{30}$</td>
<td>10</td>
<td>$2^8$</td>
<td>$2^{80}$</td>
<td>$2^{41}$</td>
<td>$2^{37}$</td>
<td>2 MB</td>
</tr>
<tr>
<td>UOV$_{60}$</td>
<td>20</td>
<td>$2^8$</td>
<td>$2^{160}$</td>
<td>$2^{82}$</td>
<td>$2^{66}$</td>
<td>139 GB</td>
</tr>
<tr>
<td>enTTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$2^{67}$</td>
<td>12 GB</td>
</tr>
<tr>
<td>Rainbow</td>
<td>24</td>
<td>$2^8$</td>
<td>$2^{192}$</td>
<td>$2^{98}$</td>
<td>$2^{78}$</td>
<td>10 TB</td>
</tr>
<tr>
<td>amTTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$2^{79}$</td>
<td>816 GB</td>
</tr>
</tbody>
</table>

Block hybrid approach: Motivations

High degree polynomials

Semaev polynomials

Solving DLP on curves

Pierrick Gaudry.
Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem.
Previous approaches

Field equations

\[ \langle f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n), x^q_1 - x_1, \ldots, x^q_n - x_n \rangle \]

\[ x^q - x = \prod_{i=1}^{d} (x - e_{1,i}) \ldots \prod_{i=1}^{d} (x - e_{l,i}) \]

Hybrid approach

\[ \mathcal{I} = \langle f_1(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k), \ldots, f_m(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k) \rangle \]

\[ \mathcal{J} = \langle f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n), x_{n-k+1} - v_1, \ldots, x_n - v_k \rangle \]

\[ \mathcal{I} = \mathcal{J} \cap \mathbb{K}[x_1, \ldots, x_{n-k}] \]
**Principle**

\[
\langle f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n), \prod_{i=1}^{d_i} (x_1 - e_{1,i}), \ldots, \prod_{i=1}^{d_k} (x_k - e_{k,i}) \rangle
\]

We have to compute \((q/d)^k\) Gröbner bases.

**Complexity**

\[
O \left( \min_{0 \leq k \leq n} \left\lfloor \frac{q}{d} \right\rfloor^k \cdot C_{F_5} \left( n, \{d_1, \ldots, d_m, d, \ldots, d_k \} \right) \right)
\]
Applications in cryptography

- A general tool for solving random systems over finite field
- Reevaluate parameters of multivariate cryptosystems
- Block hybrid approach for high degree equations
- Implementation in MAGMA.