Hybrid approach for solving multivariate polynomial systems over big finite fields

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

SALSA
LIP6 UPMC INRIA Paris-Rocquencourt, France

Jounrées Codage et Cryptographie 2009



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

Outline

Introduction

Polynomial system solving

- Gröbner bases
- Algorithms and complexity

Hybrid approach

- Presentation of the hybrid approach
- Complexity analysis
- Security analysis of multivariate signature schemes

Conclusion

Motivations

- Algebraic cryptanalysis
- Multivariate signature
- Design of multivariate schemes.

Multivariate cryptography (Matsumoto-Imai, Patarin, ...)

Secret key

$$\begin{array}{rccc} \mathbf{F}: & \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (x_1,\ldots,x_n) & & \to & (f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)) \end{array}$$

$(S,T) \in \mathrm{GL_n}(\mathbb{F}_q) \times \mathrm{GL_n}(\mathbb{F}_q)$.

Public key

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

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

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

Multivariate cryptography (Matsumoto-Imai, Patarin, ...)

Secret key

$$\begin{array}{rccc} \mathbf{F}: & \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (x_1,\ldots,x_n) & \to & (f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)) \end{array}$$

Easy to invert

$(S,T) \in \mathrm{GL_n}(\mathbb{F}_q) \times \mathrm{GL_n}(\mathbb{F}_q)$.

Public key

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

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

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

Multivariate cryptography (Matsumoto-Imai, Patarin, ...)

Secret key

$$\begin{array}{rccc} \mathbf{F}: & \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (x_1,\ldots,x_n) & \to & (f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)) \end{array}$$

Easy to invert

$(S,T) \in \mathrm{GL_n}(\mathbb{F}_q) \times \mathrm{GL_n}(\mathbb{F}_q)$.

Public key

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

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

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

$\mathbf{G}$ should look like a random polynomial system.

Multivariate signature (UOV,SFLASH,...)

Secret key

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

Easy to invert

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

Public key

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

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

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

$\mathbf{G}$ should look like a random polynomial system.

Message recovery attack

Given a ciphertext $\mathbf{z} = (z_1, \ldots, z_n)$, find a message $(x_1, \ldots, x_n)$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{z}$.

Message recovery attack

Given a ciphertext $\mathbf{z} = (z_1, \ldots, z_n)$, find a message $(x_1, \ldots, x_n)$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{z}$.

Solve the system

$$\begin{cases} g_1(x_1, \ldots, x_n) - z_1 = 0 \\ \qquad\qquad \vdots \\ g_n(x_1, \ldots, x_n) - z_n = 0 \end{cases}$$

Message recovery attack

Given a ciphertext $\mathbf{z} = (z_1, \ldots, z_n)$, find a message $(x_1, \ldots, x_n)$ such that $\mathbf{G}(\mathbf{x}) = \mathbf{z}$.

Solve the system

$$\begin{cases} g_1(x_1, \ldots, x_n) - z_1 = 0 \\ \qquad\qquad \vdots \\ g_n(x_1, \ldots, x_n) - z_n = 0 \end{cases}$$

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

Definition

A set $G \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis w.r.t. a monomial ordering $\prec$ of a polynomial ideal $\mathcal{I}$ if :
$\forall f \in \mathcal{I}, \exists g \in G$ such that $LM_{\prec}(g)$ divide $LM_{\prec}(f)$.

About Gröbner bases

Definition

A set $G \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis w.r.t. a monomial ordering $\prec$ of a polynomial ideal $\mathcal{I}$ if :
$\forall f \in \mathcal{I}, \exists g \in G$ such that $LM_{\prec}(g)$ divide $LM_{\prec}(f)$.

Property

*A Gröbner basis for the lexicographic order of a **zero-dimensional** system has the following shape :*

$$\begin{cases} g_1(x_1), \\ g_2(x_1, x_2), \\ \quad \vdots \\ g_{k_2}(x_1, x_2), \\ g_{k_3}(x_1, x_2, x_3), \\ \quad \vdots \\ g_{k_n}(x_1, \ldots\ldots, x_n) \end{cases}$$

Definition

A set $G \subset \mathbb{K}[x_1, \ldots, x_n]$ is a Gröbner basis w.r.t. a monomial ordering $\prec$ of a polynomial ideal $\mathcal{I}$ if :
$\forall f \in \mathcal{I}, \exists g \in G$ such that $LM_{\prec}(g)$ divide $LM_{\prec}(f)$.

Property

*A Gröbner basis for the lexicographic order of a **zero-dimensional** system has the following shape :*

$$\begin{cases} g_1(x_1), \\ g_2(x_1, x_2), \\ \quad \vdots \\ g_{k_2}(x_1, x_2), \\ g_{k_3}(x_1, x_2, x_3), \\ \quad \vdots \\ g_{k_n}(x_1, \ldots\ldots, x_n) \end{cases}$$

Zero-dim solving strategy:

1. *Compute a DRL Gröbner basis.*
2. *Compute a lex Gröbner basis with a change ordering algorithm (FGLM).*

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

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

Complexity of F_5 : $\mathcal{O}\left(\left(m \cdot \binom{n+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}\right)^{\omega}\right)$, with $2 \leqslant \omega \leqslant 3$.

Magali Bardet, Jean-Charles Faugère, and Bruno Salvy.

On the complexity of Gröbner basis computation of semi-regular over-defined algebraic equations.

Proc. ICPSS.

Algorithms

- F_5 : no useless computations for semi-regular systems

Complexity of F_5 : $\mathcal{O}\left(\left(m \cdot \binom{n+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}\right)^{\omega}\right)$, with $2 \leqslant \omega \leqslant 3$.

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.

Well studied for $\mathbb{F}_2$ with field equations.

Algorithms

- F_5 : no useless computations for semi-regular systems

Complexity of F_5 : $\mathcal{O}\left(\left(m \cdot \binom{n+d_{\mathrm{reg}}-1}{d_{\mathrm{reg}}}\right)^{\omega}\right)$, with $2 \leqslant \omega \leqslant 3$.

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.

Well studied for $\mathbb{F}_2$ with field equations.

Solving a system – Naive approach

System

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

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

Solving a system – Naive approach

System

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

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

Specificity

- $\mathbb{K}$ is finite
- Square systems and no field equations $\Rightarrow 2^n$ solutions
- Random systems $\Rightarrow d_{reg} = n + 1$.

Solving a system – Naive approach

System

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

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

Specificity

- $\mathbb{K}$ is finite
- Square systems and no field equations $\Rightarrow 2^n$ solutions
- Random systems $\Rightarrow d_{reg} = n + 1$.

Cannot be solved directly.

Solving a system – Hybrid approach

Solution

We specialize k variables of the system (random guess)

$\Rightarrow$ the system becomes over-defined

- $+$ The degree of regularity decreases
- $+$ The number of solutions is 0 or 1
- $-$ We have to compute $|\mathbb{K}|^k$ Gröbner bases.


Luk Bettale, Jean-Charles Faugère, and Ludovic Perret.
Cryptanalysis of the TRMS signature scheme of PKC'05.
AFRICACRYPT 2008.


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


Luk Bettale, Jean-Charles Faugère, and Ludovic Perret.
Security analysis of Multivariate Polynomials for Hashing.
INSCRYPT 2008.

Solving a system – Hybrid approach

Solution

We specialize k variables of the system (random guess)

$\Rightarrow$ the system becomes over-defined

+ The degree of regularity decreases
+ The number of solutions is 0 or 1
– We have to compute $|\mathbb{K}|^k$ Gröbner bases.

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret.
Cryptanalysis of the TRMS signature scheme of PKC'05.
AFRICACRYPT 2008.

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

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret.
Security analysis of Multivariate Polynomials for Hashing.
INSCRYPT 2008.

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. The complexity of solving the system with an hybrid approach, is bounded from above by:

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

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

We note $\mathrm{d_{reg}}(n, m, d)$ the degree of regularity 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. The complexity of solving the system with an hybrid approach, is bounded from above by:

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

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

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

The degree of regularity can be computed exactly.

Finding the best tradeoff

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

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

when $n \longrightarrow \infty$.

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 $n \longrightarrow \infty$.

Finding the best tradeoff

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

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

when $n \longrightarrow \infty$.

Magali Bardet

Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.
Ph.D. thesis, Université de Paris VI, 2004.

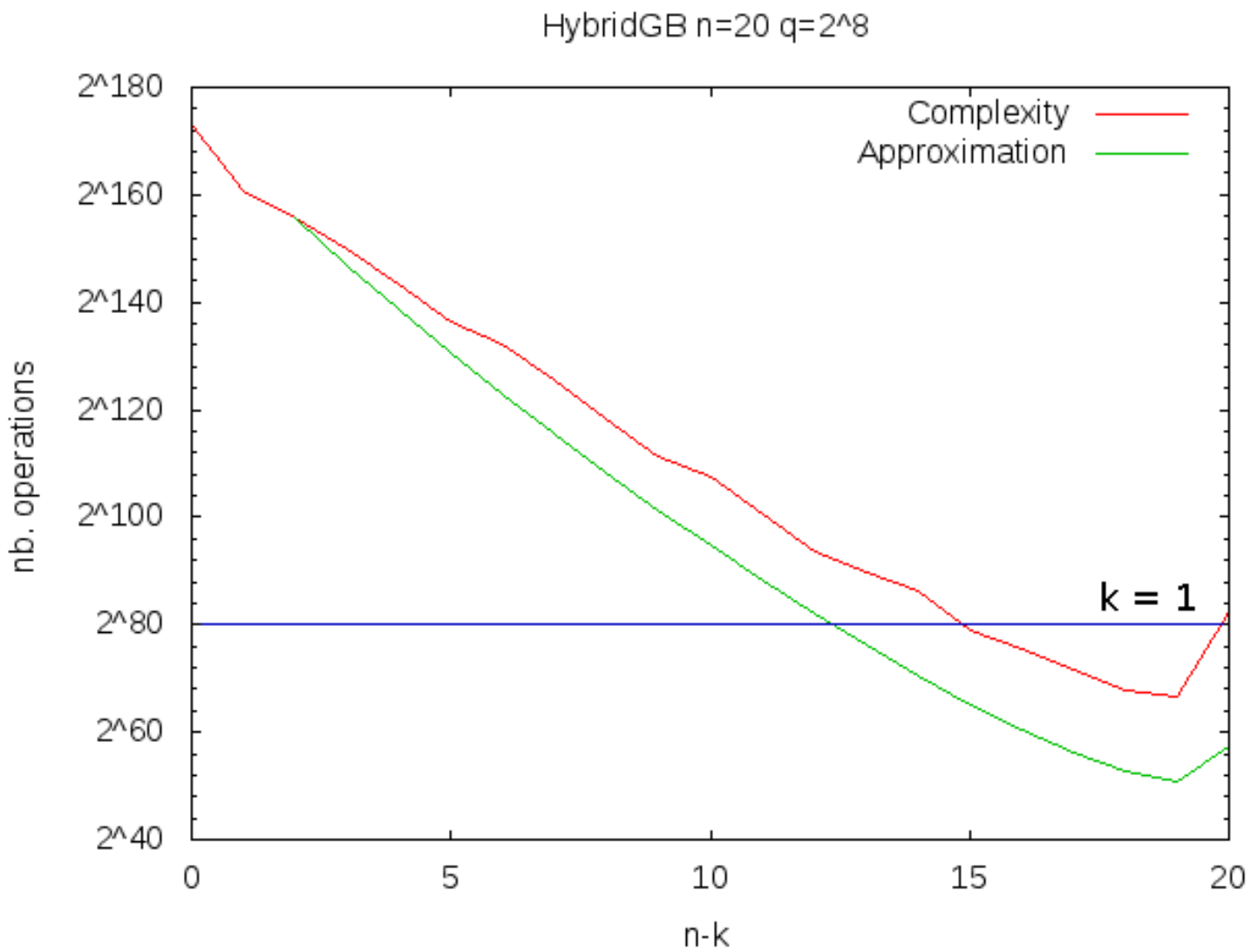
Approximation of the complexity

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

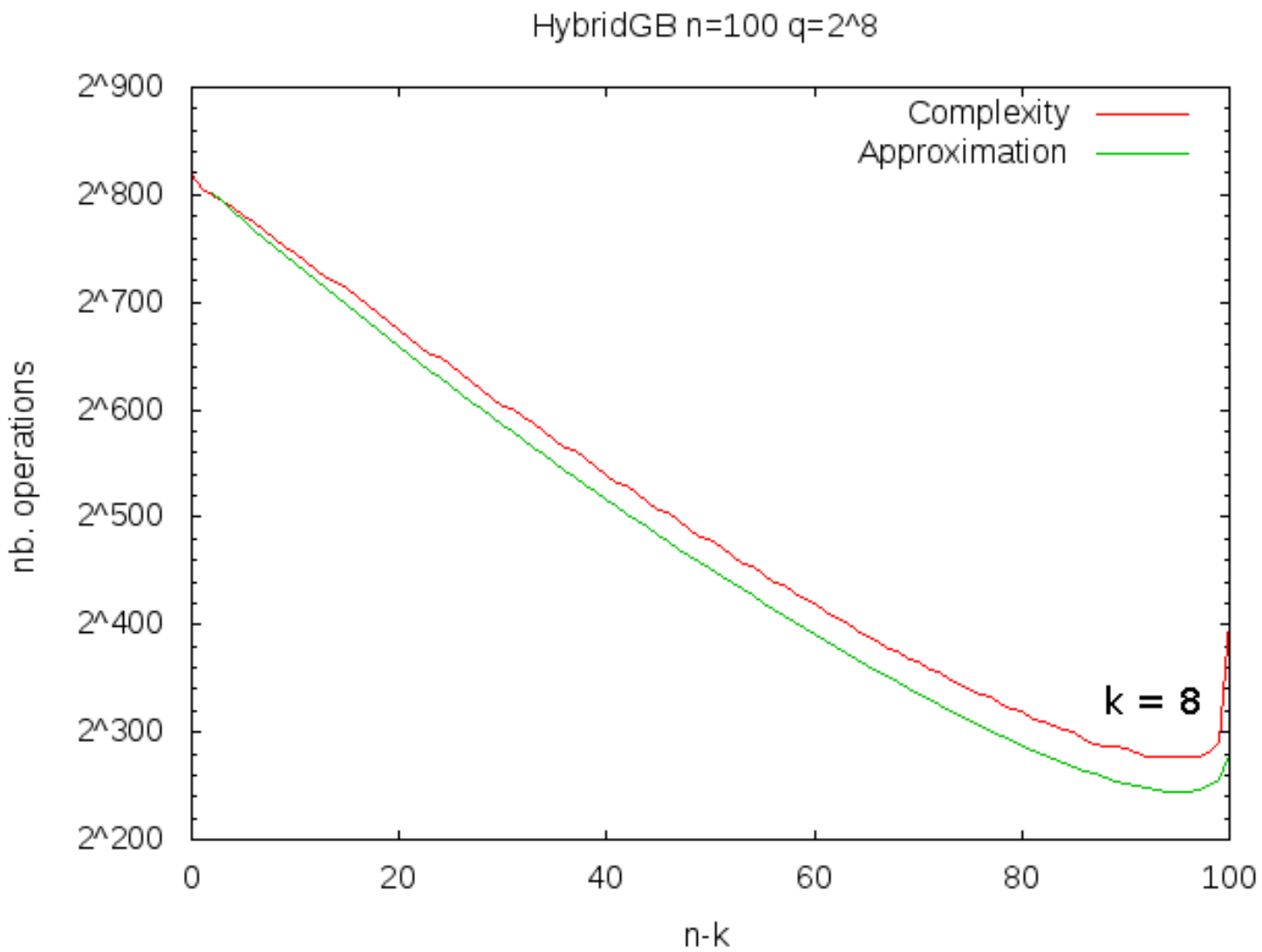
when $n \longrightarrow \infty$.

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

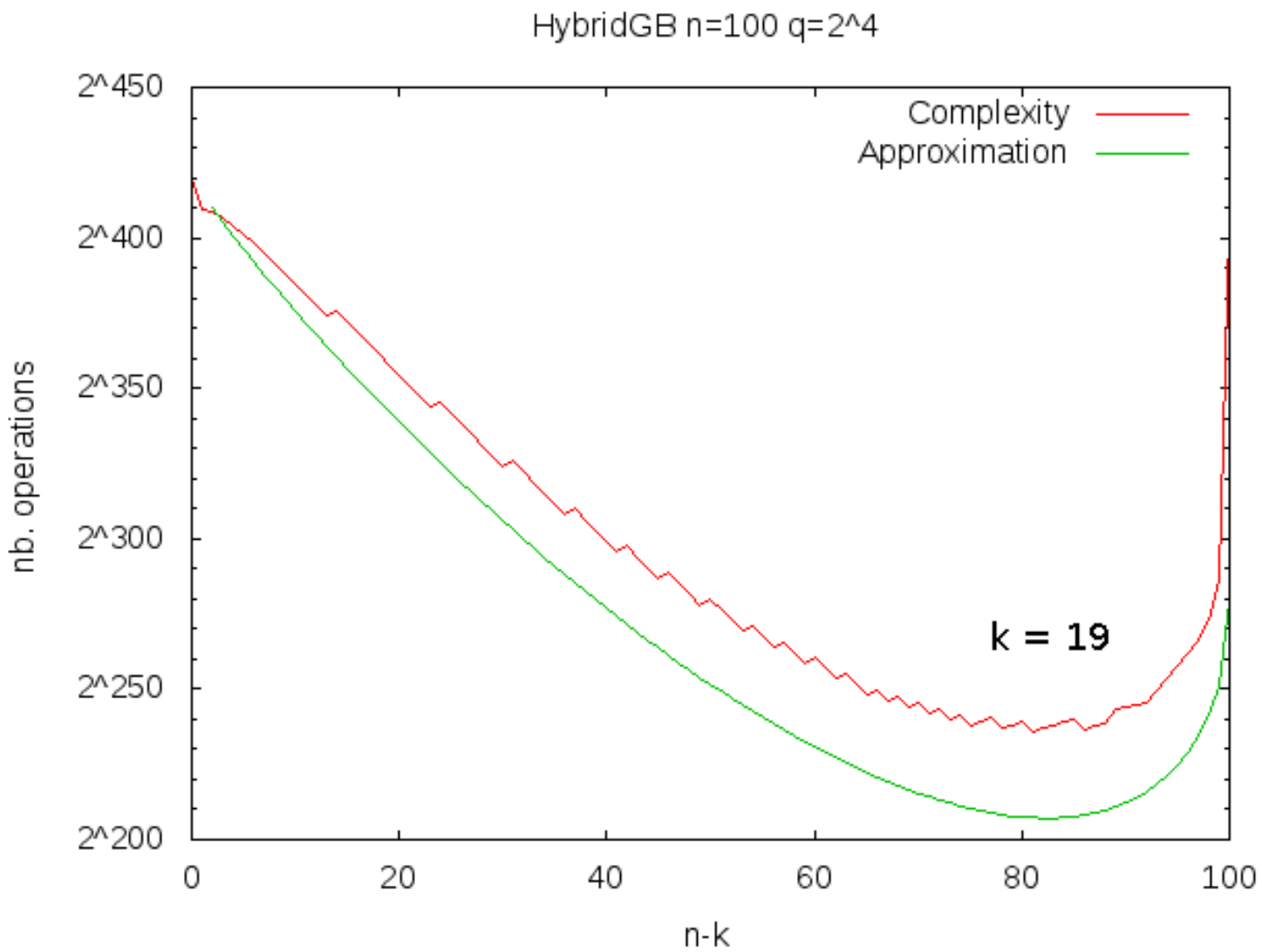
Comparaison



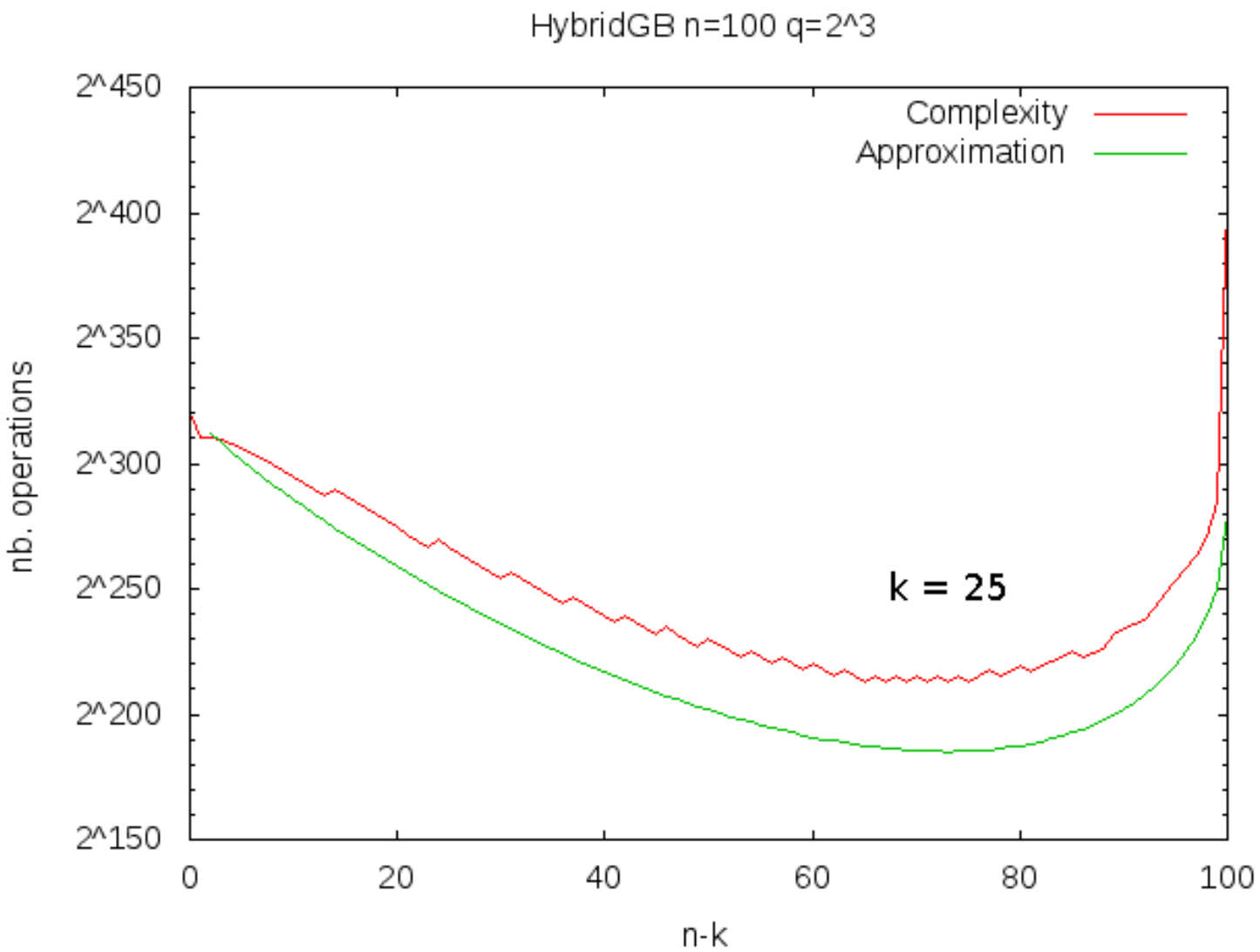
Comparaison



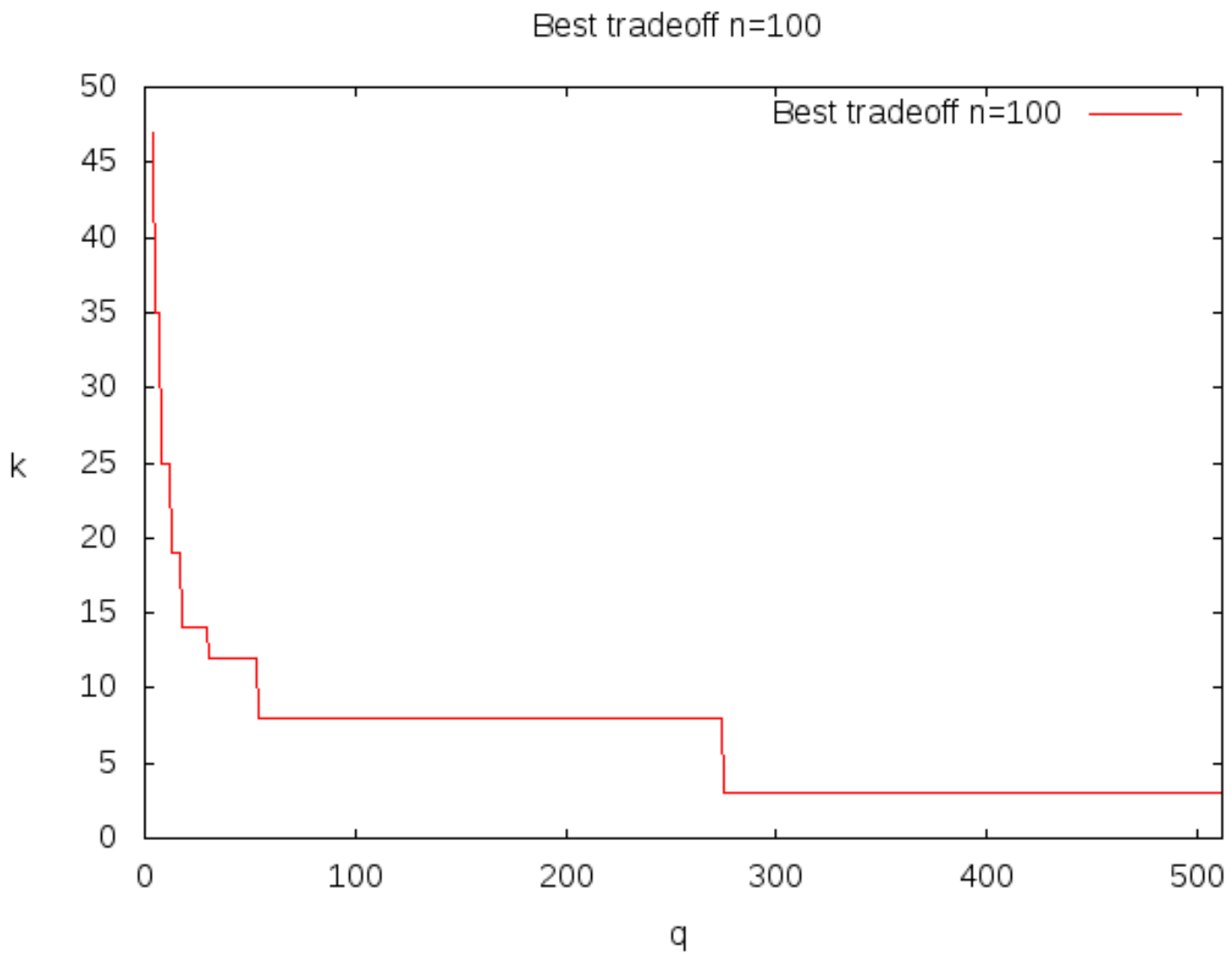
Comparaison



Comparaison



The best tradeoff



Analysis of several multivariate schemes

	n	$\lvert\mathbb{K}\rvert$	expected security	Gröbner basis ($k=0$)
UOV_{30}	10	2^8	2^{80}	2^{41}
UOV_{60} enTTS	20	2^8	2^{160}	2^{82}
Rainbow amTTS	24	2^8	2^{192}	2^{98}

Table: Analysis of several multivariate schemes

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, 2008

Analysis of several multivariate schemes

	n	$\lvert\mathbb{K}\rvert$	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} enTTS	20	2^8	2^{160}	2^{82}	2^{66} $(k=1)$	139 GB
					2^{67} $(k=2)$	12 GB
Rainbow amTTS	24	2^8	2^{192}	2^{98}	2^{78} $(k=1)$	10 TB
					2^{79} $(k=2)$	816 GB

Table: Analysis of several multivariate schemes

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, 2008

Minimal recommended parameters

Key size computed with $\frac{3n}{2}$ variables.

$\lvert\mathbb{K}\rvert$	n	k	T	signature length	public key size
2^{32}	20	0	2^{82}	960 bits	39 kB
2^{16}	23	1	2^{81}	560 bits	29 kB
2^{8}	26	1	2^{83}	312 bits	21 kB
2^{4}	30	7	2^{83}	180 bits	16 kB

Table: Minimal recommended parameters

Conclusion

Applications in cryptography

- Reevaluate parameters of cryptosystems
- A general tool to solve random systems over finite field
- Implementation in MAGMA.