Algebraic Cryptanalysis: Tools and Applications

Luk Bettale

Advisors: Jean-Charles Faugère et Ludovic Perret

LIP6 - SALSA
UPMC, CNRS, INRIA Paris-Rocquencourt

3 Octobre 2011

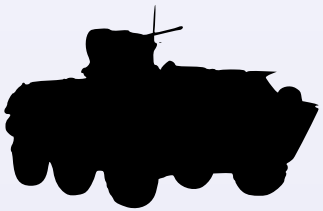
PhD defense, UPMC

Motivations

Goals of Cryptography

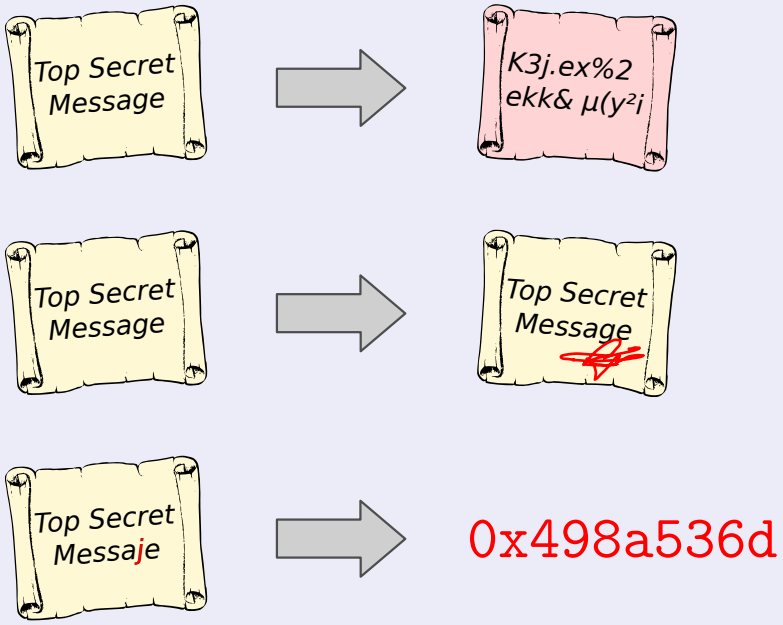
Protect data and communications

- Confidentiality
- Integrity
- Authentication
- ...



Cryptographic Primitives

- Encryption
  (DES, AES, RSA, . . .)
- Signature
  (RSA, DSA, . . .)
- Hashing
  (MD5, SHA-1, . . .)
- ...



Security of Cryptographic Primitives

Cryptanalysis

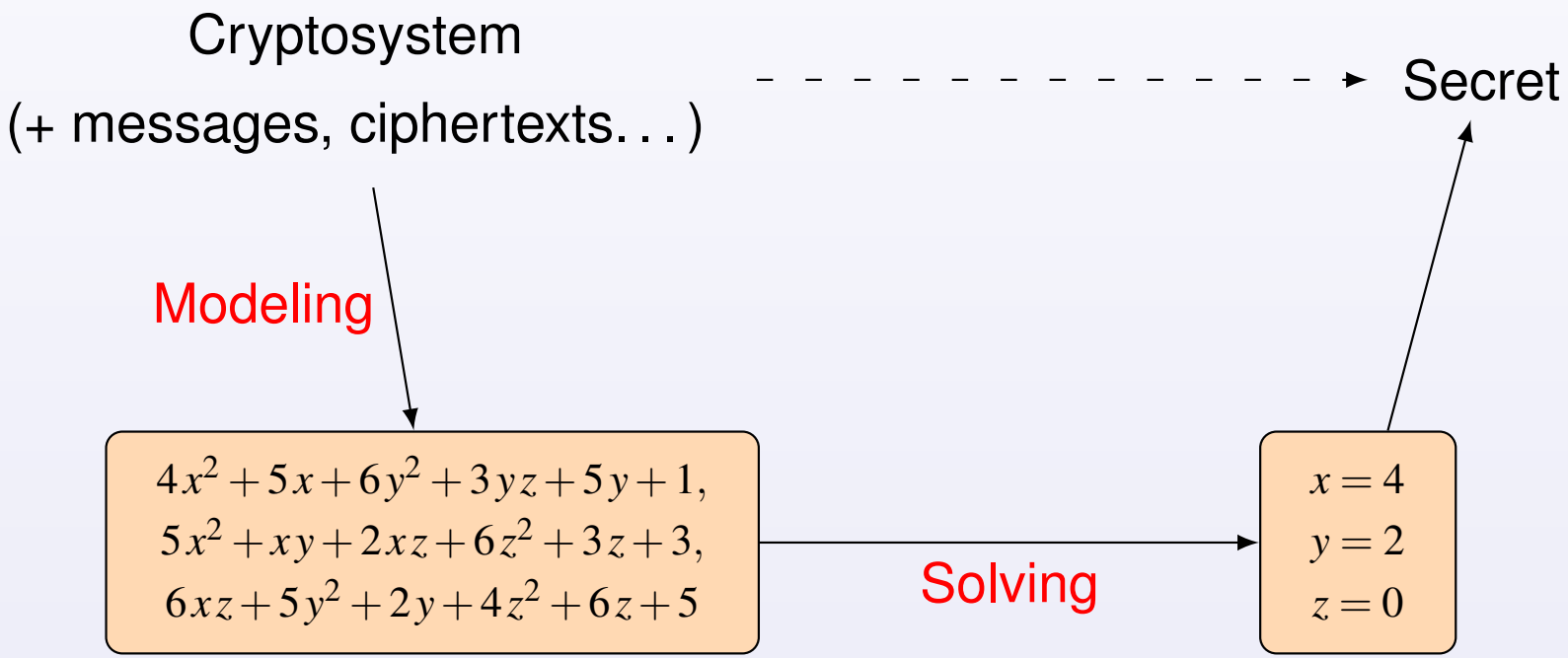
- Test the strength
- Hardness $\Rightarrow$ Complexity.

General cryptanalysis methods

- Linear cryptanalysis
- Differential cryptanalysis
- Lattice cryptanalysis
- Algebraic cryptanalysis
- ...

A General Method for Cryptanalysis

security of a cryptosystem $\Rightarrow$ hardness of solving a related multivariate polynomial system.



Polynomial System Solving (PoSSo)

q, size of field n, nb. of variables m, nb. of equations

PoSSo Problem

Let $\{f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)\} \subset \mathbb{F}_q[x_1,\ldots,x_n]$, we want $(z_1,\ldots,z_n) \in \mathbb{F}_q^n$ such that:

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

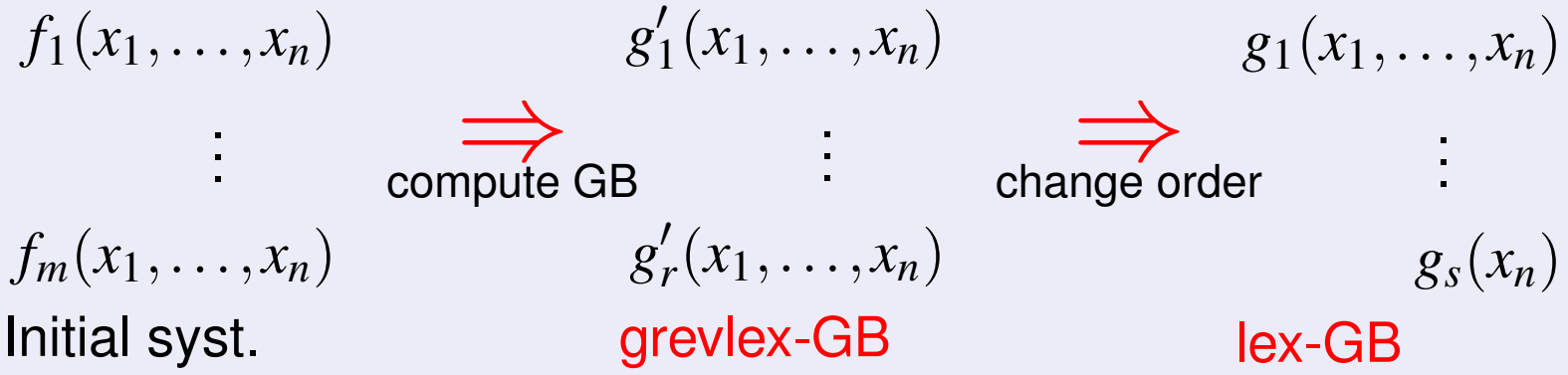
- PoSSo is NP-hard
- Complexity well mastered for "*generic*" polynomials.

Crypto Specificity

- Finite field $\rightsquigarrow$ exhaustive search
- Zero-dimensional systems (finite number of solutions).

Solving a Polynomial System

Gröbner Bases (zero-dimensional systems)



Algorithms

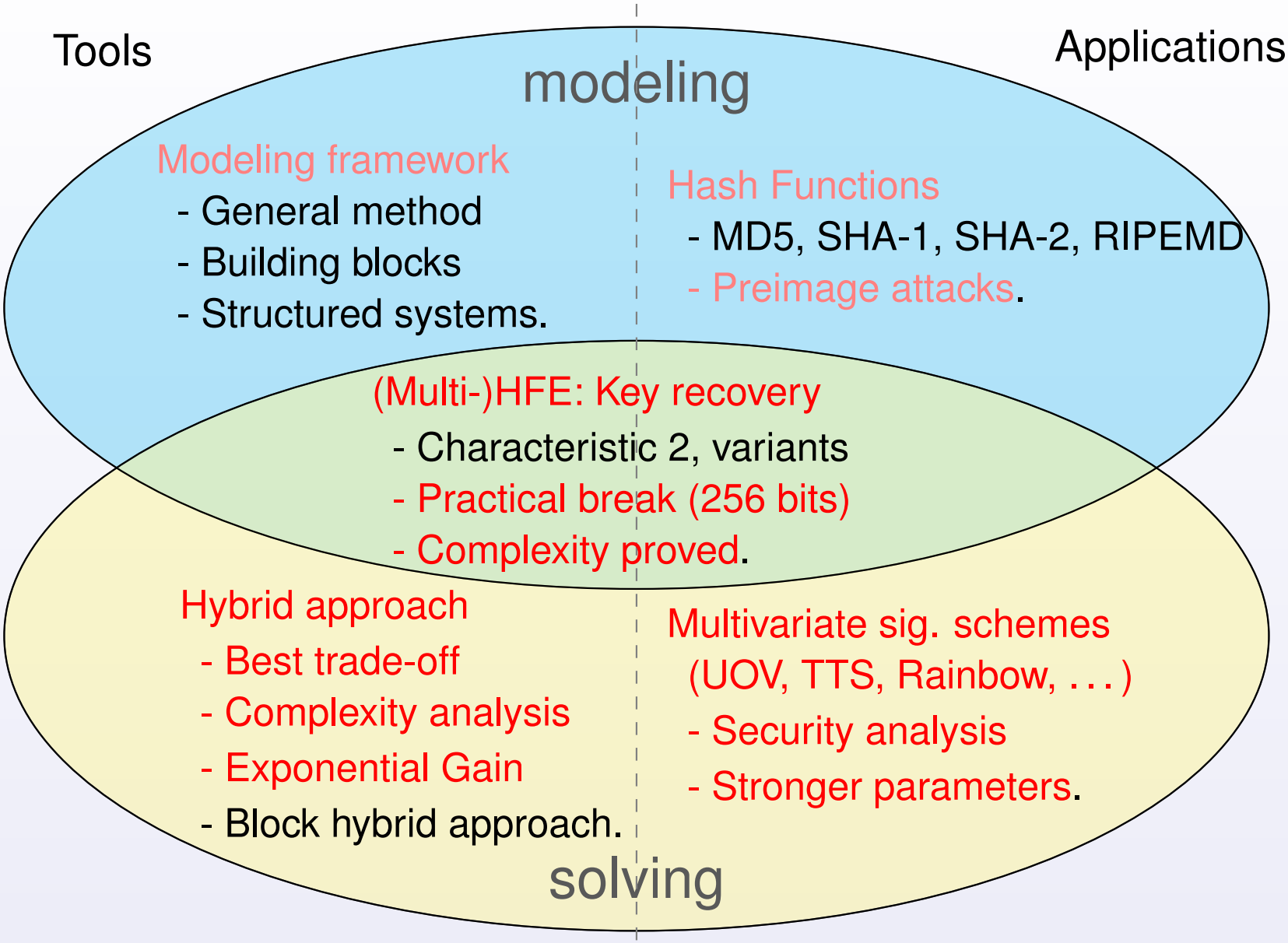
Gröbner bases

- Buchberger: historical algo. (1965)
- F_4: linear algebra (1999)
- F_5: criterion, complexity (2002)

Change ordering

- FGLM: zero-dim. (1993)

Contributions



Outline

Hybrid Approach

- Algorithm
- Complexity Analysis

Security of Multivariate Cryptosystems

- Presentation of Multivariate Cryptography
- Application of the Hybrid Approach

Cryptanalysis of HFE and Multi-HFE

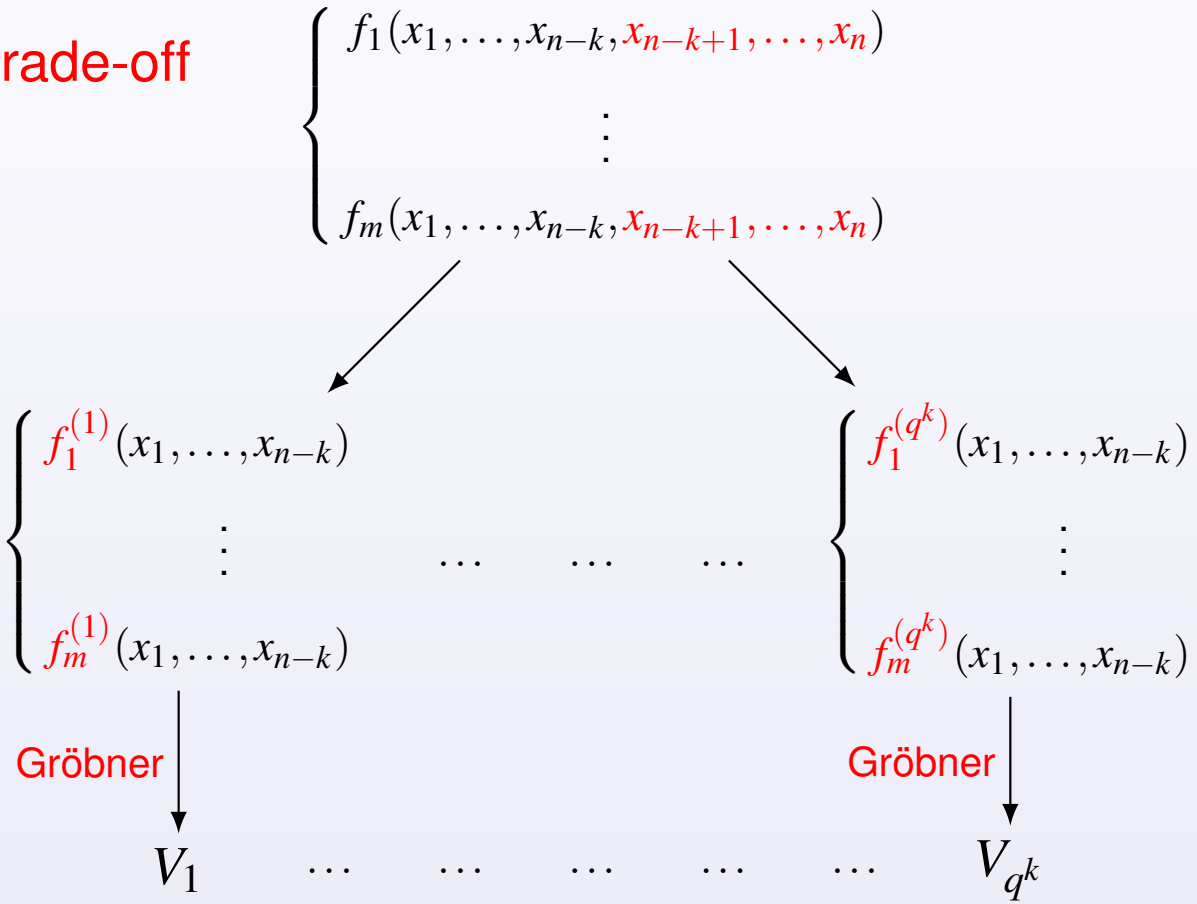
- Description of HFE / Multi-HFE
- New Attack on HFE
- Generalization to Multi-HFE

Hybrid Approach

Goal

$$V_{\mathbb{F}_q} = \left\{(z_1, \ldots, z_n) \in \mathbb{F}_q^n \mid f_1(z_1, \ldots, z_n) = \cdots = f_m(z_1, \ldots, z_n) = 0\right\}$$

k is the trade-off



compute GB,
F_5: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$,
with $2 \leqslant \omega \leqslant 3$,

change order.
FGLM: $\mathcal{O}\left(n \cdot D^{\omega}\right)$,
and D, the number of solutions in $\overline{\mathbb{F}_q}$.

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 $\deg(g \cdot f_i) \leqslant d_{reg}$.
  d_{reg} known a priori.
- More equations $\Rightarrow$ lower d_{reg}.
  (*e.g.* for quadratic systems)
  $m : n \to n+1$ $\qquad$ $d_{reg} : n+1 \to \lceil \frac{n+1}{2} \rceil$

Degree of regularity of a semi-regular system: $\mathrm{d_{reg}}(n, m, d)$.

Strong semi-regularity

k-Strong Semi-Regularity

Let $\{f_1, \ldots, f_m\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ semi-regular,

$$\{f_1(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k), \ldots, f_m(x_1, \ldots, x_{n-k}, v_1, \ldots, v_k)\}$$

is semi-regular for each vector $(v_1, \ldots, v_k) \in \mathbb{F}_q^k$.

- Matches for $k \leqslant \beta\, n$ with $\beta < 1$
- When $k > \beta\, n$, d_{reg} is smaller $\Rightarrow$ bound on d_{reg}.

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

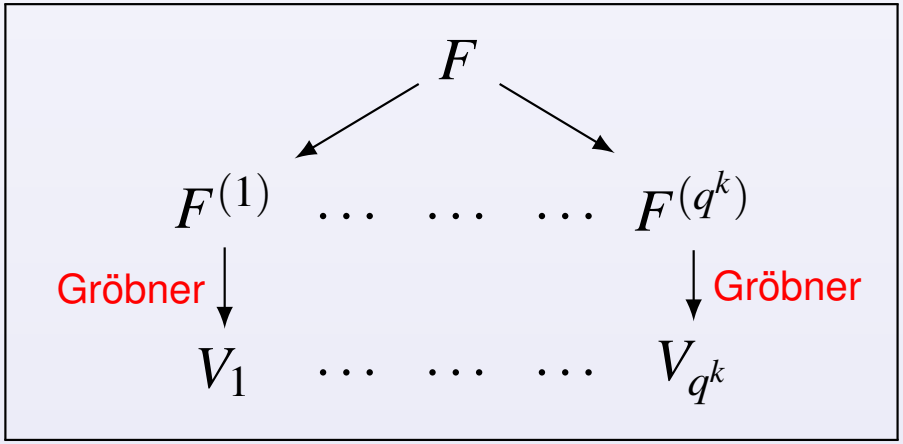
Proposition

Let $\{f_1, \ldots, f_m\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a semi-regular system of n degree d equations. Complexity of the hybrid approach:

$$\underbrace{\min_{0 \leqslant k \leqslant \beta n}}_{\text{trade-off}} \left(\underbrace{q^k}_{\text{ex. srch}} \underbrace{\mathcal{O}\left(\binom{n-k+\mathrm{d_{reg}}(n-k,m,d)}{\mathrm{d_{reg}}(n-k,m,d)}^{\omega} \right)}_{F_5} \right),$$

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

- Asymptotic trade-off ?
- Asymptotic complexity ?



Asymptotic d_{reg} (quadratic systems) for α constant

$$\mathrm{d_{reg}}\left(n, \alpha n, 2\right) = n\left(\alpha - \frac{1}{2} - \sqrt{\alpha\left(\alpha - 1\right)}\right) + \mathcal{O}\left(n^{1/3}\right).$$

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.

Best Asymptotic Trade-Off

Best trade-off: minimum of $C_{\mathrm{hyb}}(k) \Rightarrow k_0$ s.t. $C'_{\mathrm{hyb}}(k_0) = 0$

$k_0 \sim \mathrm{Const} \cdot n$, when $n \to \infty$.

Square systems:

$$k_0 \sim \frac{22.61\,\omega^2}{\left(8.66\log_2(q) + 2.75\,\omega\right)^2} \cdot n,$$

when $q \to \infty, \quad n \to \infty, \quad n > \log_2(q)$.

Asymptotic Complexity ($n \to \infty$)

Complexity of the Hybrid Approach

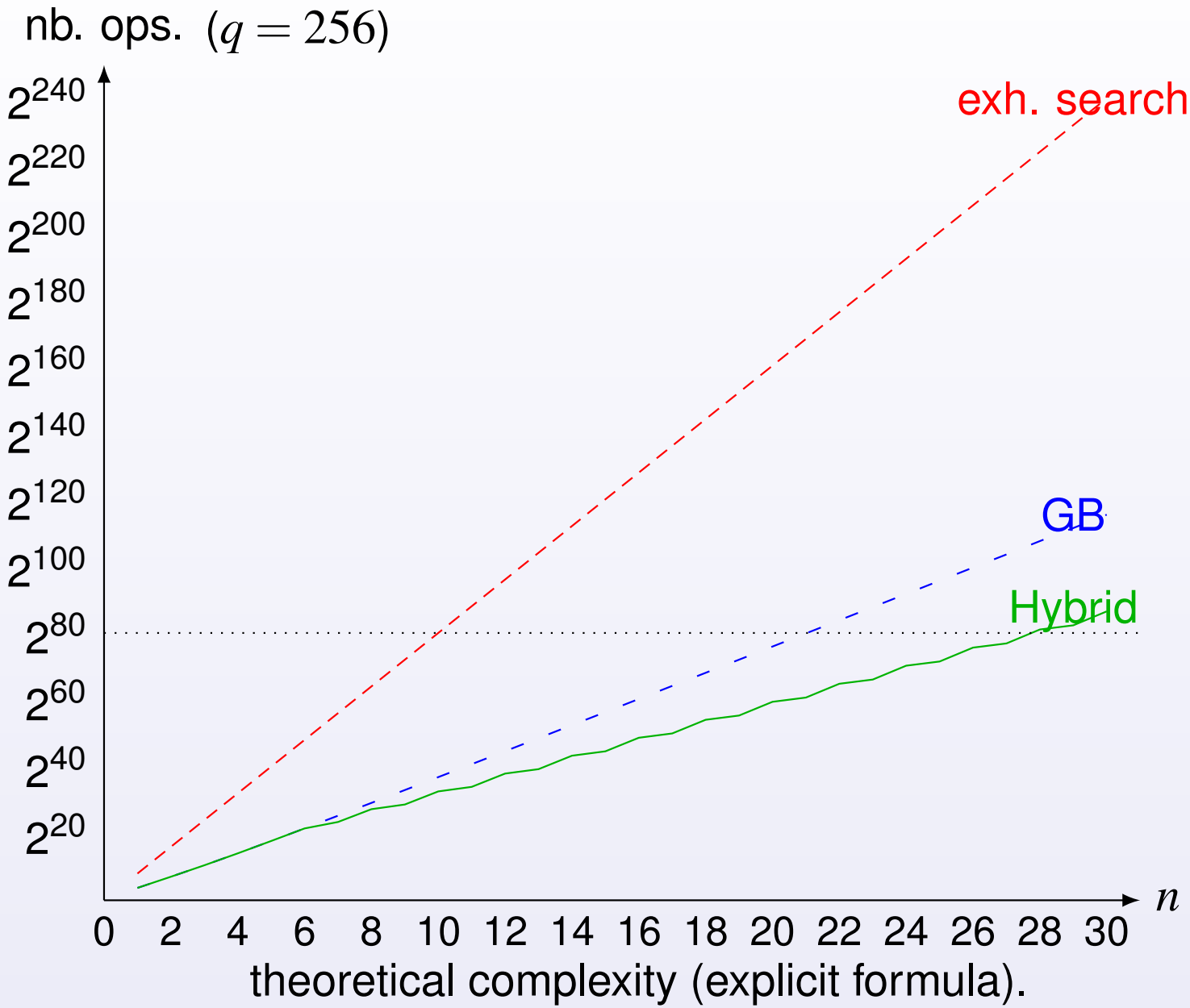
When $q \to \infty, \quad n \to \infty, \quad n > \log_2(q)$:

$$C_{\text{hyb}} \sim 2^{\left(1.38\,\omega - 0.44\,\omega^2\,\log_2(q)^{-1}\right) n},$$

direct GB: $\sim 2^{2\,\omega\,n}$ exh. search: $\sim 2^{\log_2(q)\,n}$

Exponential gain over direct GB: $2^{0.62\,\omega\,n}$.

Comparison Solving Methods (fixed $q = 256$)



Summary

Advantages of the Hybrid Approach

- An exponential gain over direct Gröbner bases
- Explicit computation of the best trade-off
- Asymptotic estimation of the best trade-off

Applications: security of multivariate cryptosystems.

Multivariate Cryptography: Motivations

Tsutomu Matsumoto and Hideki Imai.
Public quadratic polynomial-tuples for efficient signature-verification and message-encryption.
EUROCRYPT '88.

Multivariate Public Key Cryptosystems

- Based on PoSSo
- Fast encryption, small signatures
- Alternative to RSA and ECC
- Long term security (Post-Quantum cryptography).

- Many proposals (HFE$^-$, ~~HFE$_2$~~, UOV, ~~SFLASH~~, ~~Rainbow~~, ~~IP~~ ...)
- A lot of cryptanalysis.

(Billet, Bouillaguet, Ding, Dubois, Gilbert, Faugère, Fouque, Joux, Kipnis, Patarin, Perret, Shamir, Stern, Wolf ...)

Encryption.

Private Key

$\mathscr{F} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n).$$

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

Decrypt:

$\underline{m} = \mathscr{S}^{-1} \circ \mathscr{F}^{-1} \circ \mathscr{T}^{-1}(\underline{c})$.

Public Key

$\mathscr{G} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$g_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$\vdots$$
$$g_n(x_1, \ldots, x_n).$$

$\mathscr{G} = \mathscr{T} \circ \mathscr{F} \circ \mathscr{S}$.

Encrypt:

$\underline{c} = \mathscr{G}(\underline{m})$.

Signature.

Private Key

$\mathscr{F} : (\mathbb{F}_q)^{n+r} \mapsto (\mathbb{F}_q)^{n+r}$

$$f_1(x_1, \ldots, x_{n+r}),$$
$$\vdots$$
$$\vdots$$
$$f_{n+r}(x_1, \ldots, x_{n+r}).$$

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

Sign:

$\underline{z} = \mathscr{S}^{-1} \circ \mathscr{F}^{-1} \circ \mathscr{T}^{-1}(\underline{m} \mid \underline{v})$.

Public Key

$\mathscr{G} : (\mathbb{F}_q)^{n+r} \mapsto (\mathbb{F}_q)^{n}$

$$g_1(x_1, \ldots, x_{n+r}),$$
$$\vdots$$
$$g_n(x_1, \ldots, x_{n+r}).$$

$\mathscr{G} = \pi \circ \mathscr{T} \circ \mathscr{F} \circ \mathscr{S}$.

Verify:

$\underline{m} =? \mathscr{G}(\underline{z})$.

Multivariate Schemes Faster than ECC

	q	n	$n+r$	signature length	Pubkey size
UOV_{30}	2^8	10	30	80 bits	4.8 kB
UOV_{60}	2^8	20	60	160 bits	36.8 kB
enTTS	2^8	20	28	160 bits	8.5 kB
Rainbow	2^8	24	42	192 bits	22.1 kB
amTTS	2^8	24	34	192 bits	14.7 kB

Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf
Time-Area Optimized Public-Key Engines: MQ-Cryptosystems as Replacement for Elliptic Curves?
CHES 2008.

Signature Forgery

Let $\underline{m} = (m_1, \ldots, m_n) \in \mathbb{F}_q^n$ be a message, find a signature $\underline{z} = (z_1, \ldots, z_{n+r}) \in \mathbb{F}_q^{n+r}$ such that $\mathcal{G}(\underline{z}) = \underline{m}$.

Solve the system

$$\begin{cases} g_1(x_1, \ldots, x_n, v_1, \ldots, v_r) - m_1 = 0 \\ \vdots \qquad \text{No structure} \Rightarrow \text{semi-regular system} \\ g_n(x_1, \ldots, x_n, v_1, \ldots, v_r) - m_n = 0\,. \end{cases}$$

Typical parameters (TRMS) : $q = 2^8, n = 20$ (160 bits).

Hybrid Approach: $2^{160} \to 2^{60} \sim 51$ h $\times$ 65536 proc.


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


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

Size of field $q = 2^8$.

	n	exh. search	Gröbner basis ($k = 0$)	hybrid approach	mem.	practical attack
UOV_{30}	10	2^{80}	2^{37}	2^{33} ($k = 1$)	2.6 MB	0.5s $\times$ 256
UOV_{60}	20	2^{160}	2^{76}	2^{59} ($k = 1$)	213 GB	
enTTS				2^{60} ($k = 2$)	16 GB	51h $\times$ 65536
Rainbow	24	2^{192}	2^{92}	2^{70} ($k = 1$)	15 TB	
amTTS				2^{71} ($k = 2$)	1.2 TB	

Minimal Parameters

Table: The minimal value of n below which the parameters are unsafe (complexity below 2^{80}).

q	n	k	C_{hyb}	sig. length	pub. key size
2^{32}	22	0	2^{84}	864 bits	28.55 kB
2^{16}	26	1	2^{84}	528 bits	25.57 kB
2^{8}	28	1	2^{81}	288 bits	16.41 kB
2^{4}	33	7	2^{80}	174 bits	13.74 kB
2^{2}	47	24	2^{80}	129 bits	17.41 kB
2	82	53	2^{80}	123 bits	38.79 kB

Hybrid approach $\Rightarrow$ calibrate parameters of multivariate schemes.

History of Hidden Field Equations (HFE)

- Generalization of Matsumoto-Imai's C* (EUROCRYPT '88)
- Encryption/Signature.

Jacques Patarin.
Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms.
EUROCRYPT '96.

Known Attacks

- Message recovery attack [Faugère, Joux 2003]
  - First HFE challenge broken in 2002 (80 bits security)
  - efficient in char 2
  - Theoretical degree of regularity.
- Key recovery attack [Kipnis, Shamir 1999]
  - not practical
  - complexity conjectured.
- Weak keys [Bouillaguet, Fouque, Joux, Treger 2011]
  - practical key recovery.

Generalization of HFE: Multi-HFE

[BPS08] Olivier Billet, Jacques Patarin, and Yannick Seurin.
Analysis of Intermediate Field Systems.
SCC 2008.

[CCDWY08] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang.
Odd-char multivariate Hidden Field Equations.
Cryptology ePrint Archive, 2008.

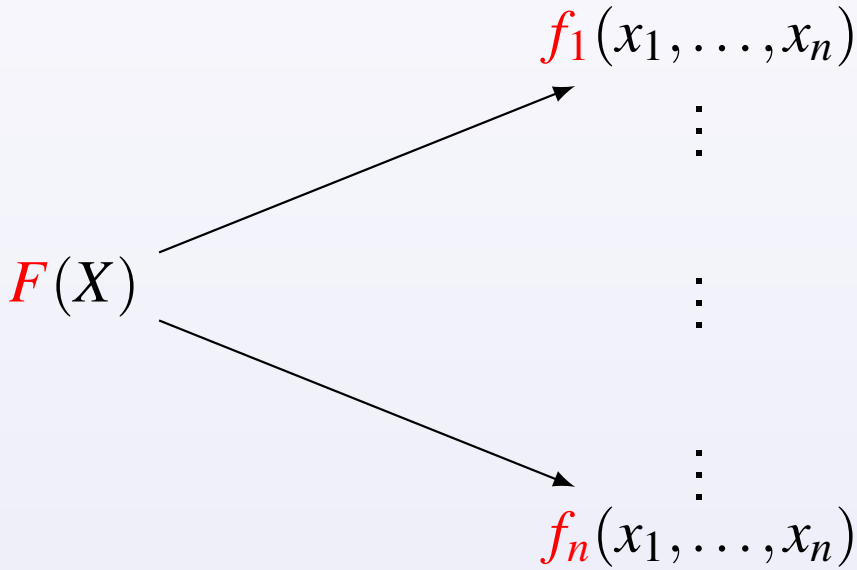
- Use odd-characteristic field to prevent [FJ03] attack
- Various additional variants (minus, embedding).
- No known attacks
- Efficient implementations.

Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang.
SSE implementation of multivariate PKCs on modern x86 CPUs.
CHES 2009.

HFE Shape

$F(X) \in \mathbb{F}_{q^n}[X]$, $D \in \mathbb{N}$

$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j < n \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i < n \\ q^i \leqslant D}} B_i X^{q^i} + C.$$



with $F\left(\sum_{i=1}^n \theta_i x_i\right) = \sum_{i=1}^n \theta_i f_i(x_1, \ldots, x_n)$ where $(\theta_1, \ldots, \theta_n) \in (\mathbb{F}_{q^n})^n$ is a basis of the $\mathbb{F}_q$-vector space $(\mathbb{F}_q)^n$.

Multi-HFE Trapdoor

Multi-HFE Shape

$F_1(X_1,\ldots,X_N),\ldots,F_N(X_1,\ldots,X_N) \in (\mathbb{F}_{q^d}[X_1,\ldots,X_N])^N, \quad n = Nd$

$$F_k(X_1,\ldots,X_N) = \sum_{1\leqslant i\leqslant j\leqslant N} A_{k,i,j} X_i X_j + \sum_{1\leqslant i\leqslant N} B_{k,i} X_i + C_k \quad \text{for } 1 \leqslant k \leqslant N.$$

$q = 7, 11, 31, \ldots$

$$\begin{array}{ccc} & & f_1(x_1,\ldots,x_n) \\ & \nearrow & \vdots \\ F_1(X_1,\ldots,X_N) & & \\ & \searrow & f_d(x_1,\ldots,x_n) \\ \vdots & & \vdots \\ F_N(X_1,\ldots,X_N) & \longrightarrow & f_{n-d+1}(x_1,\ldots,x_n) \\ & \searrow & \vdots \\ & & f_n(x_1,\ldots,x_n) \end{array}$$

with $F_k\left(\sum_{i=1}^d \theta_i x_i,\ldots,\sum_{i=1}^d \theta_i x_{(k-1)d+i}\right) = \sum_{i=1}^d \theta_i f_{(k-1)d+i}(x_1,\ldots,x_n)$
for $1 \leqslant k \leqslant N$ where $(\theta_1,\ldots,\theta_n) \in (\mathbb{F}_{q^d})^d$ is a basis of $(\mathbb{F}_q)^d$.

Table: Status of HFE and Multi-HFE variants.

construction	message recovery	key recovery
HFE (q odd)	[FJ03] (if $q < 7$)	[KS99] theoretical $\rightarrow$ improved [KS99] attack
HFE ($q = 2$)	[FJ03]	[KS99] theoretical ? $\rightarrow$ extended [KS99] attack
Multi-HFE ($q = 2$)	[FJ03] + [BPS08]	new attack
Multi-HFE (q odd)	–	new attack
(Multi-)HFE$^-$	–	new attack (if $N > 1$)
(Multi-)HFE w/ emb.	–	new attack
(Multi-)HFEv	–	–

Matrix Representation (Odd Characteristic)

Matrix Representation (non-standard quadratic form)

$$F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{F}\underline{X}^t,$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

$$\begin{pmatrix} f_{1,1} & \ldots & f_{1,\ell} & 0 & \ldots & 0 \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ f_{\ell,1} & \ldots & f_{\ell,\ell} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

$$\mathrm{rank}(\mathbf{F}) = \log_q\left(\deg\left(F(X)\right)\right).$$

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
CRYPTO '99.

Use the quadratic forms of $(g_1, \ldots, g_n)$.

Matrix Representation of Quadratic Form

$$g_1(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_1}\,\underline{x}^t$$

$$\vdots$$

$$g_n(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_n}\,\underline{x}^t,$$

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

Linear change of basis between $(x_1, \ldots, x_n)$ and $(X^{q^0}, \ldots, X^{q^{n-1}})$.
$\Rightarrow$ Low rank linear combination of the $\mathbf{G_i}$'s.

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret.
Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants.
PKC 2011.

Improvement of Kipnis-Shamir's Attack

Let $\mathbf{M}_n$ a change basis matrix between $(x_1, \ldots, x_n)$ and $(X^{q^0}, \ldots, X^{q^{n-1}})$, $g_k(\underline{x}) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$, $\mathbf{T}^{-1}\mathbf{M}_n = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\,\mathbf{M}_n = \mathbf{W}$.

Fundamental Equation

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{WFW}^t.$$

Find a vector $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^n})^n$ such that

$$\operatorname{rank}\left(\sum_{k=1}^{n} \lambda_k \mathbf{G_k}\right) = \log_q(D).$$

- The MinRank problem on matrices over $\mathbb{F}_q \rightsquigarrow$ faster solving
- Standard quadratic form representation
- Clean description as matrix/vector operations.

Kipnis-Shamir Attack vs. New Attack on HFE ($N = 1$)

Table: Comparison between KS attack and new attack on HFE with parameters $q = 31$, $N = 1$, $D = 31^2 + 31 = 992$ from 60 to 80 bits security.

d	12	13	14	15	16
KS attack (in sec.)	374	1305	1790	2719	14763
new attack (in sec.)	3.2	6.7	12.9	26.1	54.9
ratio	170	195	139	104	269

Using MAGMA (V2.17-1) on a 2.93 GHz Intel® Xeon® CPU.

MinRank solved using Gröbner bases.

Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret.
Cryptanalysis of MinRank.
Crypto 2008.

Let $\mathbf{M}_{N,d} = \mathrm{Diag}(\mathbf{M}_d, \ldots \mathbf{M}_d)$, $g_k(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$,
$\mathbf{T}^{-1}\mathbf{M}_{N,d} = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\mathbf{M}_{N,d} = \mathbf{W}$.

Fundamental Equations

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_1}\mathbf{W}^t, \ldots, \sum_{k=0}^{n-1} u_{k,N}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_N}\mathbf{W}^t.$$

Find N vectors $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^d})^n$ such that

$$\mathrm{rank}\left(\sum_{k=0}^{n-1} \lambda_k \mathbf{G_k}\right) = N \log_q(D).$$

N MinRank relations "equivalent up to Frobenius transforms"
$\Rightarrow$ only one to be solved.

Proposed Parameters Practically Broken

Table: Proposed parameters of Multi-HFE [CCDWY08]. Broken on a 2.93 GHz Intel Xeon CPU.

using MAGMA (V2.16-10).

q	N	d	D	security	time (MAGMA)	mem (MAGMA)	d_{reg}
31	2	15	2	150 bits	2 m 27 s	434 MB	3
31	3	10	2	150 bits	1 h 38 m	1.5 GB	3
31	3	15	2	192 bits	2 d 1 h	12 GB	3
31	3	18	2	256 bits	9 d 16 h	33 GB	3

using FGb.

q	N	d	D	security	time (FGb)	mem (FGb)	d_{reg}
31	2	15	2	150 bits	21.1 s	276 MB	3
31	3	10	2	150 bits	24 m 56 s	1.6 GB	3

Explicit method to compute d_{reg}.

Theorem

For a MinRank coming from Multi-HFE with parameters q, N, d, D

$$d_{reg} \leqslant \psi(q, N, d, D)$$

where $\psi(q, N, d, D)$ can be computed for explicit values of q, N, d, D.

Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer
Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology.
ISSAC 2010.

Theorem

Proved for all parameters with $N \log_q(D) < 11$

$$\psi(q, N, d, D) = N \log_q(D) + 1.$$

Formula conjectured for all parameters.

Proposition

Complexity of solving the Multi-HFE MinRank with Gröbner bases:

$$\mathscr{O}\left(d^{(N\log_q(D)+1)\,\omega}\right)$$

when $d \to \infty$, *with* $2 \leqslant \omega \leqslant 3$ *the linear algebra constant.*

- The complexity is polynomial in d, the degree of the extension
- For equally sized keys, Multi-HFE is less secure than HFE.

$$\text{Complexity}_{\text{attack}}(N,d) < \text{Complexity}_{\text{attack}}(1,n), \quad \text{when} \quad n = Nd.$$

Software

Available at `http://www-salsa.lip6.fr/~bettale/`

- Hybrid approach: MAGMA package
- (Multi-)HFE key recovery: MAGMA implementation
- Hash Functions: Framework for algebraic preimage.

Algebraic Preimage Attacks on Hash Functions

- Hash functions building blocks (MAGMA)
- Built-in modelings of MD5, SHA-1, SHA-2, RIPEMD (MAGMA)
- Semi-automatic preimage attack (BASH)
- Automatic statistics generation (BASH)
- ANF to CNF converter (C)
- Operates with Gröbner bases / SAT-solver (C).

Algebraic Modeling of Hash Functions

MD5, SHA-1, RIPEMD-128, RIPEMD-160, SHA-256, SHA-512.

Features of the modeling

- Coefficients in $\mathbb{F}_2 \Rightarrow$ boolean systems
- Equations of degree at most 2
- Structured systems w.r.t. ordering $\Rightarrow$ Gröbner bases.

Preimage Attack

1. Fix some variables (hybrid approach)
2. Solve the system (GB or SAT)
3. Estimate the complexity.

Algebraic Preimage Attacks on Hash Functions

	nb. rounds	ref.	other works	this thesis
MD5	64 (full)	EUROCRYPT '09	$2^{123.4}$	$2^{122.97}$
SHA-1	48	CRYPTO '09	$2^{159.3}$	$2^{154.17}$
SHA-1	80 (full)	–	–	$2^{153.53}$
RIPEMD-128	29	ISPEC '09	$2^{115.2}$	$2^{123.09}$
RIPEMD-128	64 (full)	–	–	$2^{122.36}$
RIPEMD-160	80 (full)	–	–	$2^{153.14}$
SHA-256	46	ASIACRYPT '09	$2^{254.9}$	$2^{251.56}$
SHA-256	64 (full)	–	–	$2^{250.71}$
SHA-512	43	ASIACRYPT '09	$2^{511.5}$	$2^{506.99}$
SHA-512	80 (full)	–	–	$2^{506.45}$

Ready for SHA-3 finalists !

Perspectives

What else to be done ?

- Modeling/Attack on SHA-3 finalists
- Extension of the framework (collision attacks).

Work in progress:

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret
Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic.
submitted to Designs, Codes and Cryptography.

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret
Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach.
to be submitted.

Luk Bettale, Jean-Charles Faugère, and Ludovic Perret
Algebraic Preimage Attacks on Hash Functions.
to be submitted.