Cryptography: A Challenge for Efficient Computation of Gröbner Bases

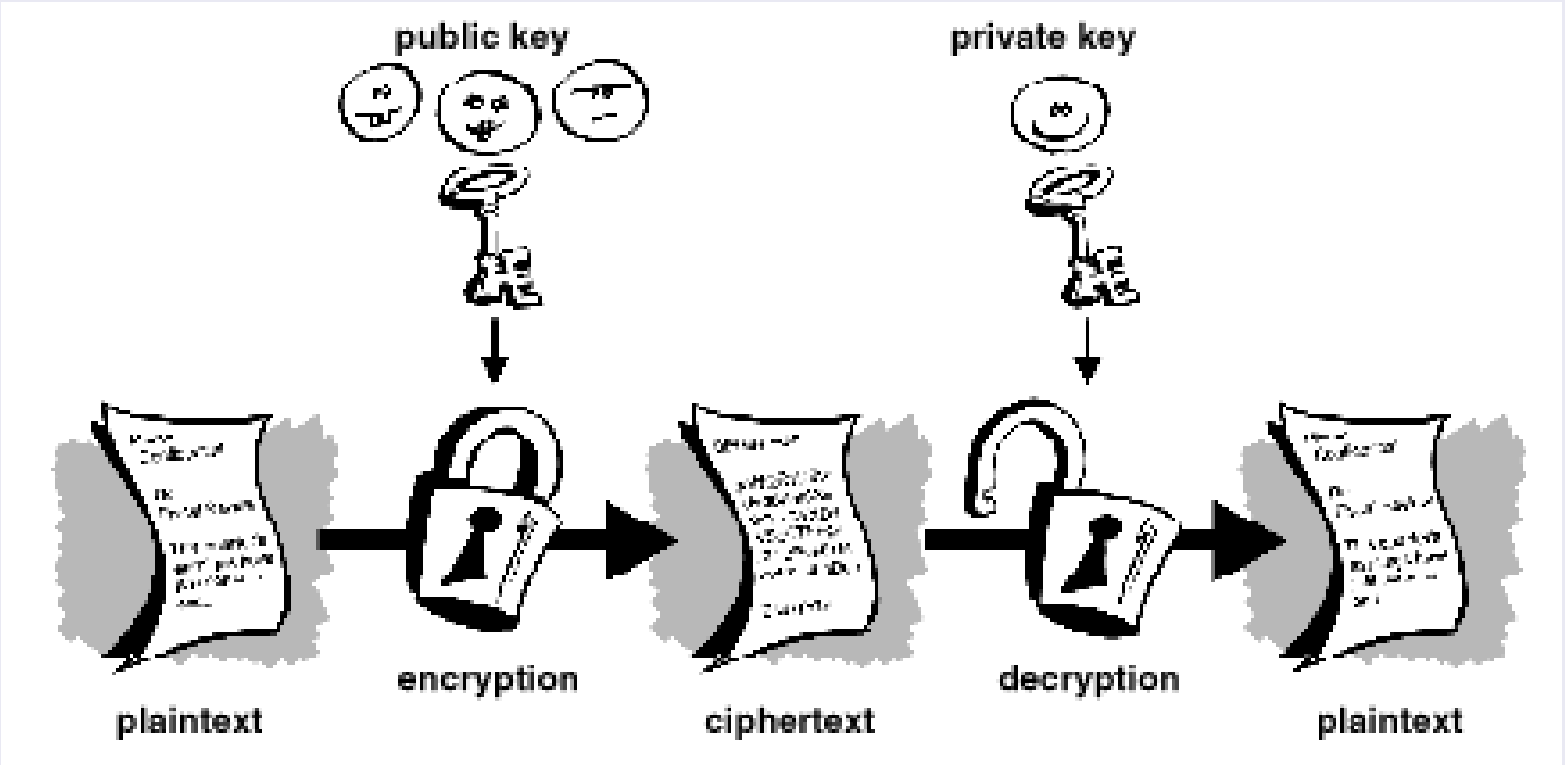
Ludovic Perret

UCL Crypto Group
Louvain-la-Neuve, BELGIUM
ludovic.perret@uclouvain.be

Workshop on Efficient Computation of Gröbner Bases
Linz, Austria

Public Key Cryptograhy : Principle

Diffie & Hellman, 1976



Trapdoor One-Way Functions

An informal definition

A function:

$$f : x \longmapsto f(x),$$

is a *trapdoor one-way function* if:

- given x, it is easy to compute $f(x)$.
- given $f(x) = y$, it is *computationally impossible* to recover x, without an additional knowledge called the *trapdoor*.

Existing Constructions

- The *discrete logarithm problem*: given a finite field $\mathbb{F}_q$, a primitive element $g \in \mathbb{F}_q^*$, and $y \in \mathbb{F}_q^*$, find $0 \leq x \leq q-1$ such that:
$$g^x = y.$$
- The *factorization problem*: given an integer n, find prime numbers $p_1, \ldots, p_k$, and positive integers $e_1, \ldots, e_k$ s. t.:
$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

Algebraic Crypanalysis

- Construct an algebraic system whose zeroes correspond to solutions of the problem considered

  a particular attention to the way of constructing the system

  we have to exploit all the properties of the problem

- Try to solve this system (using Gröbner bases)

  System Solving is NP-Hard

  but, this only provides intractability of the worst-case

Perfect knowledge of the problem considered and of Gröbner bases algorithms is required.

Algebraic Crypanalysis

- Construct an algebraic system whose zeroes correspond to solutions of the problem considered

  a particular attention to the way of constructing the system

  we have to exploit all the properties of the problem

- Try to solve this system (using Gröbner bases)

  System Solving is NP-Hard

  but, this only provides intractability of the worst-case

Perfect knowledge of the problem considered and of Gröbner bases algorithms is required.

Algebraic Crypanalysis

- Construct an algebraic system whose zeroes correspond to solutions of the problem considered
  - a particular attention to the way of constructing the system
    - we have to exploit all the properties of the problem
- Try to solve this system (using Gröbner bases)
  - System Solving is NP-Hard
    - but, this only provides intractability of the worst-case

Perfect knowledge of the problem considered and of Gröbner bases algorithms is required.

Algebraic Crypanalysis

- Construct an algebraic system whose zeroes correspond to solutions of the problem considered
  - a particular attention to the way of constructing the system
    - we have to exploit all the properties of the problem
- Try to solve this system (using Gröbner bases)
  - System Solving is NP-Hard
    - but, this only provides intractability of the worst-case

Perfect knowledge of the problem considered and of Gröbner bases algorithms is required.

Outline

1. Introduction
2. A First Attempt
3. The 2PLE Algorithm
4. Conclusion

History of 2PLE

The C^* scheme [T. Matsumoto & H. Imai, 88]

Secret key: $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$.
Public data: $\underline{a} = \big(a_1(\underline{x}), \ldots, a_n(\underline{x})\big) \in \mathbb{F}_q[\underline{x}]^u$.
Public key:

$$\big(b_1(\underline{x}), \ldots, b_n(\underline{x})\big) = \big(a_1(\underline{x}S), \ldots, a_n(\underline{x}S)\big)U,$$

with $\underline{x} = (x_1, \ldots, x_n)$.
Encryption: To encrypt a message $\underline{m} \in \mathbb{F}_q^n$, we compute:

$$\underline{c} = \big(b_1(\underline{m}), \ldots, b_n(\underline{m})\big).$$

Decryption: Compute $\underline{m'} \in \mathbb{F}_q^n$ verifying $\underline{a}(\underline{m'}) = \underline{c}U^{-1}$, and then recover the plaintext by $\underline{m} = \underline{m'}S^{-1}$.

Underlying Hard Problem

2PLE

Given: $\underline{a} = (a_1, \ldots, a_u)$, and $\underline{b} = (b_1, \ldots, b_u) \in \mathbb{F}_q[x_1, \ldots, x_n]^u$.
Question: Find – if any – $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, s. t.:

$$\big(b_1(\underline{x}), \ldots, b_n(\underline{x})\big) = \big(a_1(\underline{x}S), \ldots, a_n(\underline{x}S)\big)U,$$

denoted by $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, with $\underline{x} = (x_1, \ldots, x_n)$.

- Introduced by J. Patarin at Eurocrypt'96

A First Attempt

Evaluation

Let D be the maximal total degree of the polynomials of $\underline{a}$.
If $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, for $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, then:

$$\underline{b}(\underline{p})U^{-1} = \underline{a}(\underline{p}S), \text{ for all } \underline{p} \in \mathbb{F}_q^n.$$

- $O(u \cdot q^n)$ algebraic equations of degree D
- $n^2 + u^2$ unknowns

Linearization

- $O(u \cdot q^n)$ linear equations
- $C_{n^2+D}^{D} + u^2 \approx O(n^{2D})$ unknows (w.l.o.g. $u \leq n$)

Why can linearization not be used – (I)

Lemma

Let $\underline{y} = (y_{1,1}, \ldots, y_{1,n}, \ldots, y_{n,1}, \ldots, y_{n,n})$, $\underline{z} = (z_{1,1}, \ldots, z_{1,u}, \ldots, z_{u,1}, \ldots, z_{u,u})$. *For each* $i, 1 \leq i \leq u$, *there* $\exists S_i \subset \mathbb{F}_q^n$, *and* $p_{\alpha_i} \in \mathbb{F}_q[\underline{y}, \underline{z}]$, *s. t.:*

$$\left(\underline{b}(\underline{x})U^{-1} - \underline{a}(\underline{x}S)\right)_i = \sum_{\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,n}) \in S_i} p_{\alpha_i}(S, U^{-1}) x_1^{\alpha_{i,1}} \cdots x_n^{\alpha_{i,n}},$$

with:

$$p_{\alpha_i}(S, U^{-1}) = p_{\alpha_i}(s_{1,1}, \ldots, s_{n,n}, u'_{1,1}, \ldots, u'_{u,u}).$$

Why can linearization not be used – (II)

Let $\underline{p} = (p_1, \ldots, p_n) \in \mathbb{F}_q^n$, and $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, s.t. $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, then $\forall i, 1 \leq i \leq u : \left(\underline{b}(\underline{p})U^{-1} - \underline{a}(\underline{p}S)\right)_i =$

$$\sum_{\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,n}) \in S_i} p_{\alpha_i}(S, U^{-1}) p_1^{\alpha_{i,1}} \cdots p_n^{\alpha_{i,n}} = 0,$$

with D denoting max. total degree of the poly. of $\underline{a}$:

- $u \cdot C_{n+D}^D \approx O(u \cdot n^D)$ linearly independent equations
- number of unknowns is $O(n^{2D})$

Basic Idea – (I)

Proposition [J.-C. Faugère & L. Perret, 2006]

Let $\mathcal{I} = \langle p\alpha_i : \forall i, 1 \leq i \leq u, \text{ and } \forall \alpha_i \in S_i \rangle \subset \mathbb{F}_q[\underline{y}, \underline{z}]$, *and:*

$$V(\mathcal{I}) = \left\{ \underline{s} \in \mathbb{F}_q^{n^2+u^2} : p\alpha_i(\underline{s}) = 0, \forall 1 \leq i \leq u, \text{ and } \forall \alpha_i \in S_i \right\}.$$

If $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, *for some* $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, *then:*

$$\left(\phi_1(S), \phi_2(U^{-1})\right) \in V(\mathcal{I}),$$

with:

$$\phi_1 : S = \{s_{i,j}\}_{1 \leq i,j \leq n} \mapsto (s_{1,1}, \ldots, s_{1,n}, \ldots, s_{n,1}, \ldots, s_{n,n}), \text{ and}$$
$$\phi_2 : U^{-1} = \{u'_{i,j}\}_{1 \leq i,j \leq u} \mapsto (u'_{1,1}, \ldots, u'_{1,u}, \ldots, u'_{u,1}, \ldots, u'_{u,u}).$$

Basic Idea – (II)

Proof.

If $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, for some $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, then for all $i, 1 \leq i \leq u$: $\left(\underline{b}(\underline{p})U^{-1} - \underline{a}(\underline{p}S)\right)_i =$

$$\sum_{\alpha_i=(\alpha_{i,1},\ldots,\alpha_{i,n})\in S_i} p_{\alpha_i}(S, U^{-1}) p_1^{\alpha_{i,1}} \cdots p_n^{\alpha_{i,n}} = 0.$$

Thus, for all $i, 1 \leq i \leq u$, and for all $\alpha_i \in S_i$:

$$p_{\alpha_i}(S, U^{-1}) = 0.$$

□

Basic Idea – (III)

Let D be the max. total degree of the poly. of $\underline{a}$. We obtain an algebraic system of:

- $u \cdot C_{n+D}^{D} \approx O(u \cdot n^{D})$ equations of degree at most D
- $n^2 + u^2$ unknowns

A Structural Property – (I)

Property

If $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, *for some* $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, *then:*

$$\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U \iff \underline{b}^{(d)}(\underline{x}) = \underline{a}^{(d)}(\underline{x}S)U, \forall d, 0 \leq d \leq D.$$

- $a_i^{(d)}$ *(resp.* $b_i^{(d)}$*) being the homogeneous component of degree* d *of* a_i *(resp.* b_i*)*
- D *being the max. total degree of the polynomials of* $\underline{a}$

A Structural Property – (II)

Lemma

Let d be a positive integer, and $\mathcal{I}_d \subset \mathbb{F}_q[\underline{y}, \underline{z}]$ be the ideal generated by the polynomials $p\alpha_i$ of maximal total degree smaller than d. Let also $V(\mathcal{I}_d)$ be the variety associated to $\mathcal{I}_d$. If $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$, for some $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, then:

$$\left(\phi_1(S), \phi_2(U^{-1})\right) \in V(\mathcal{I}_d), \text{ for all } d, 0 \leq d \leq D,$$

with:

$$\phi_1 : S = \{s_{i,j}\}_{1 \leq i,j \leq n} \mapsto (s_{1,1}, \ldots, s_{1,n}, \ldots, s_{n,1}, \ldots, s_{n,n}), \text{ and}$$
$$\phi_2 : U^{-1} = \{u'_{i,j}\}_{1 \leq i,j \leq u} \mapsto (u'_{1,1}, \ldots, u'_{1,u}, \ldots, u'_{u,1}, \ldots, u'_{u,u}).$$

The 2PLE algorithm

Input : $(\underline{a}, \underline{b}) \in \mathbb{F}_q[\underline{x}]^u \times \mathbb{F}_q[\underline{x}]^u$
Output : $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$, s.t. $\underline{b}(\underline{x}) = \underline{a}(\underline{x}S)U$

Let $d_0 = \min\{d > 1 : \underline{a}^{(d)} \neq \underline{0}_u\}$

- **Construct** the $p\alpha_i s$ of max. total degree smaller than d_0 associated to $(\underline{a}, \underline{b})$
- **Compute** $V(\mathcal{I}_{d_0})$
- **Find** an element of $V(\mathcal{I}_{d_0})$ corresponding to a solution of 2PLE
- **Return** this solution

Analysis

- Computing a variety $\approx$ computing a Gröbner basis
  - Buchberger's algorithm
  - F_4 algorithm [J.C. Faugère, 99]
  - F_5 algorithm [J.C. Faugère, 02]

We solve algebraic systems of:

- $O(n^{d_0})$ equations of degree at most $d_0 (= 2$ in practice$)$
- $n^2 + u^2$ unknowns

Analysis

- Computing a variety $\approx$ computing a Gröbner basis
  - Buchberger's algorithm
  - F_4 algorithm [J.C. Faugère, 99]
  - F_5 algorithm [J.C. Faugère, 02]

We solve algebraic systems of:

- $O(n^{d_0})$ equations of degree at most $d_0 (= 2$ in practice$)$
- $n^2 + u^2$ unknowns

Analysis

- Computing a variety $\approx$ computing a Gröbner basis
  - Buchberger's algorithm
  - F_4 algorithm [J.C. Faugère, 99]
  - F_5 algorithm [J.C. Faugère, 02]

We solve algebraic systems of:

- $O(n^{d_0})$ equations of degree at most $d_0 (= 2$ in practice$)$
- $n^2 + u^2$ unknowns

Analysis

- Computing a variety $\approx$ computing a Gröbner basis
  - Buchberger's algorithm
  - F_4 algorithm [J.C. Faugère, 99]
  - F_5 algorithm [J.C. Faugère, 02]

We solve algebraic systems of:

- $O(n^{d_0})$ equations of degree at most $d_0 (= 2$ in practice)
- $n^2 + u^2$ unknowns

Experimental Results – Random instances

$u = n$, and $deg = 2$

n	$\#unk.$	q	T_{Gen}	T_{F_5}	T_{F_4/F_5}	T	$q^{n/2}$
8	128	2^{16}	0.3s.	0.1s.	6	0.4s.	2^{64}
10	200	2^{16}	1.6s.	0.6s.	10	2.2s.	2^{80}
12	288	2^{16}	7.3s.	2.1s.	16	9.4s.	2^{96}
15	450	2^{16}	48s.	10s.	23	58s.	2^{120}
17	578	2^{16}	137.2s.	27.9s.	31	195.1s.	2^{136}
20	800	2^{16}	569.1s.	91.5s.	41	660.6s.	2^{160}
10	200	65521	1.2s.	0.4s.	10	1.6s.	2^{80}
15	450	65521	35.5s.	8s.	23	43.5s.	2^{120}
20	800	65521	434.9s.	69.9s.	41	504.8s.	2^{160}
23	1058	65521	1578.6s.	235.9s.		1814s.	2^{184}

Experimental Results – C^* Instances

$u = n$

n	$\#unk.$	q	deg	T_{Gen}	T_{F_5}	T_{F_4/F_5}	T	$q^{n/2}$
5	50	2^{16}	4	0.2 s.	0.13 s.	45	0.33 s.	2^{80}
6	72	2^{16}	4	0.7s.	1s.	64	1.7s.	2^{96}
7	98	2^{16}	4	1.5s.	6.1s.	90	7.6s.	2^{112}
8	128	2^{16}	4	3.8s.	54.3s.	112	58.1s.	2^{128}
9	162	2^{16}	4	5.4s.	79.8s.	145	85.2s.	2^{144}
10	200	2^{16}	4	12.9s.	532.3s.	170	545.2s.	2^{160}

Challenges for Gröbner Bases

Cryposystem	$\#unk.$	$\#Sys.$	solved ?
HFE (solved)	80	80	J.-C. Faugère, 2002
Khazad	4800	6000	N
Mysti1	1848	1845	N
Kasumi	2000	2000	N
Camelia-128	1664	4304	N
Rinjdael-128	1600	4600	N
Serpent-128	8320	9360	N

[Biryukov - De Cannière, 03]

History of 2PLE

The C^* scheme [T. Matsumoto & H. Imai, 88]

Secret key: $(S, U) \in GL_n(\mathbb{F}_q) \times GL_u(\mathbb{F}_q)$.
Public data: $\underline{a} = \big(a_1(\underline{x}), \ldots, a_n(\underline{x})\big) \in \mathbb{F}_q[\underline{x}]^u$.
Public key:

$$\big(b_1(\underline{x}), \ldots, b_n(\underline{x})\big) = \big(a_1(\underline{x}S), \ldots, a_n(\underline{x}S)\big)U,$$

with $\underline{x} = (x_1, \ldots, x_n)$.
Encryption: To encrypt a message $\underline{m} \in \mathbb{F}_q^n$, we compute:

$$\underline{c} = \big(b_1(\underline{m}), \ldots, b_n(\underline{m})\big).$$

Decryption: Compute $\underline{m'} \in \mathbb{F}_q^n$ verifying $\underline{a}(\underline{m'}) = \underline{c}U^{-1}$, and then recover the plaintext by $\underline{m} = \underline{m'}S^{-1}$.

Conclusion

Others problems related to Gröbner bases:

- Ideal membership
- Finding low-degree relations
- Change of ordering
- Computing the quotient of an ideal