On the cryptographic applications of Gröbner bases and Lattice Theory

University of Maria Curie-Sklodowska
Faculty of Mathematics, Physics and Computer Science
Lublin, 2-14 December 2012

Jaime Gutierrez
University of Cantabria
Santander
This course will give a general introduction to the Gröbner basis and Lattice Theory, and cover the main applications to both cryptography and cryptanalysis. The main goal of this course is to show interactions between Cryptology and Symbolic Computation; the two important tools are lattices and Gröbner bases.

- The most famous example of such an interaction is probably the so called Lenstra, Lenstra, and Lovász (LLL) lattice basis reduction algorithm, it was a key ingredient to solve a computer algebra problem (factoring polynomials over the rational numbers); since then, it was used in numerous attacks in cryptology. Informally speaking a lattice is a set of points in n-dimensional space with a periodic structure. Historically, lattices were investigated since the late 18th century by mathematicians such as Lagrange, Gauss, and later Minkowski. More recently, lattices have become an active topic of research in computer science. At the beginning lattice reduction techniques were were used in cryptography principally to prove cryptographic insecurity. We will cover several of these negative results in particular:
  - breaking of knapsack-based cryptosystems
  - breaking the linear congruential pseudorandom generator.
  - breaking the security of padded RSA

The lectures will be primarily focused on the algorithmic aspects of the lattice theory, which lattice problem can be solved in polynomial time, and which problems seems to be intractable. And also, presenting applications to predicting pseudorandom number generators and integer factoring.

- The second important symbolic computation tool is the theory of Gröbner basis. A Gröbner basis is a set of multivariate polynomials that has desirable algorithmic properties. Every set of polynomials can be transformed into a Gröbner basis. This process generalizes three familiar techniques: Gaussian elimination for solving linear systems of equations, the Euclidean algorithm for computing the greatest common divisor of two univariate polynomials, and the Simplex Algorithm for linear programming. It is a powerful technique for solving problems in algebraic geometry that was introduced by Bruno Buchberger, who named them after his advisor Wolfgang Gröbner. Gröbner bases provide a uniform approach for solving problems that can be expressed in terms of systems of multivariate polynomial equations. It happens that many practical problems, can be transformed into sets of polynomials, thus solved using Gröbner bases method. For instance, in cryptology the ciphers are rewritten to systems of multivariate equations that are solved for variables representing, for example, key bits. Algebraic attacks apply to a variety of ciphers, ranging from
  - blockciphers, like AES and Serpent,
  - streamciphers, like Toyocrypt and BlueTooth,
  - Asymmetric cryptosystems, like Hidden Field Equation (HHE),
  - hash functions, like multivariate polynomial for hashing.

The course will give a short theoretical and algorithmic background on Gröbner bases, including the Buchberger’s algorithm for computing a such basis, and then shows several applications to cryptology, including the asymmetric cryptographic primitives based on multivariate polynomials over finite fields. Those schemes are often considered to be good candidates for post-quantum cryptography, once quantum computers can break the current schemes.
On the cryptographic applications of Gröbner bases and Lattice Theory

University of Maria Curie-Sklodowska.
Faculty of Mathematics, Physics and Computer Science.
Lublin, 2-14 December 2012

Jaime Gutierrez (University of Cantabria)
Gröbner bases:
- Affine varieties and ideals
- Division algorithm
- Buchberger’s Algorithm. Extensions F4 and F5
- Elimination theory: How to solve system of equations
- Common cryptosystems and Algebraic cryptanalysis
- AES (Advanced Encryption Standard)
- HFE (Hidden Field Equations)
- Stream Ciphers: Trivium, Bivium

Lattices:
- Definitions
- Minkowski theorem.
- Computational problems: SVP, CVP
- LLL Reduced Lattice Basis
- Knapsack-based cryptosystems and Lattice-based cryptanalysis.
- Small roots of integers polynomials:
  - Predicting pseudorandom number generators
  - Security of RSA with small decryption exponent


**Sage: Open Source Mathematics Software**

University of Maria Curie-Sklodowska. Faculty of Mathematics, Physics and Computer Science. Lublin, 2-14 December 2012

On the cryptographic applications of Gröbner bases and Lattice Theory
- Cryptography
  - Private Key
  - Public key

- Cryptanalysis
C.E. Shannon (1916 – 2001)


“AS MUCH WORK AS SOLVING A SYSTEM OF SIMULTANEOUS EQUATIONS IN A LARGE NUMBER OF UNKNOWNS OF A COMPLEX TYPE.”
Gröbner bases in public key cryptography

University of Maria Curie-Sklodowska.
Faculty of Mathematics, Physics and Computer Science.
Lublin, 2-14 December 2012

Jaime Gutierrez (University of Cantabria)
The public key is a set of polynomial equations over a finite field $\mathbb{K}$

$$
\begin{align*}
  y_1 &= f_1(x_1, \ldots, x_n), \\
  y_2 &= f_2(x_1, \ldots, x_n), \\
  &\vdots \\
  y_n &= f_n(x_1, \ldots, x_n).
\end{align*}
$$

- **Encryption**: Evaluating the polynomials $f_i$ in: plaintext $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$, $\rightarrow$ ciphertext $y = (y_1, \ldots, y_n) \in \mathbb{K}^n$

- **Attacking**: Solving the system of equations.

**Theorem**

*Deciding if an arbitrary system of multivariate, quadratic equations over a finite field is solvable is NP-complete.*
\( \mathbb{K} = \mathbb{F}_q \) a finite field of characteristic a prime number \( p \).

- HFE polynomial:
  
  \[
  f(x) = \sum_{i,j} \beta_{i,j} x^{q^{\theta_{i,j}}} + \sum_{l} \alpha_{l} x^{q^{\phi_{l}}} + \mu \in \mathbb{F}_q^n[x]
  \]

  \( \beta_{i,j}, \alpha_{l}, \mu \in \mathbb{F}_q^n \) and \( \theta_{i,j}, \phi_{i,j}, \epsilon_{l} \in \mathbb{N} \)

- For an irreducible polynomial \( g(x) \in \mathbb{K}[x] \):
  
  \[ \mathbb{K}[x]/\langle g(x) \rangle \cong \mathbb{F}_q^n \]

  The elements of \( \mathbb{F}_q^n \) are represented as \( n \)-tuples over \( K \).

  \( f(x_1, \ldots, x_n) = (p'_1(x_1, \ldots, x_n), p'_2(x_1, \ldots, x_n \ldots, p'_n(x_1, \ldots, x_n)) \)

  \( p'_i(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n] \) are quadratic polynomials.

- Two affine bijections \( s \) and \( t \) as vector spaces: \( \mathbb{K}^n \rightarrow \mathbb{K}^n \).

  \[
  t(f(s(x_1, \ldots, x_n))) = (p_1(x_1, \ldots, p_n(x_1, \ldots, x_n))
  \]

University of Maria Curie-Sklodowska. Faculty of Mathematics, Physics and Computer Science. Lublin, 2-14 December 2012

Gröbner bases in public key cryptography
The protocol

- **Public key:** \( \mathbb{K}, n \) and \( p_i(x_1, \ldots, x_n) \).
- **Private key:** \( f, s, t \) and the representation of \( \mathbb{F}_{q^n} \) over \( \mathbb{K} \).

- **Encrypt:** Plaintext \( x = (x_1, \ldots, x_n) \) compute the ciphertext \( y = (y_1, \ldots, y_n) \):

\[
y = p_1(x_1, \ldots, p_n(x_1, \ldots, x_n))
\]

- **Decrypt:** Find all solutions to the equation

\[
f(z) = t^{-1}(y)
\]

and \( x' = s^{-1}(z) \)

- Encryption and Decryption can be computed efficiently:
  - Public transformation: $O(n^5)$
  - Private: $O(n^4(n + \log n))$
- The inverse quadratic polynomial map may have a much higher degree.
- Algebraic Cryptanalysis
SK:

- Three affine bijections $r, s, t : \mathbb{K}^n \to \mathbb{K}^n$
- Two applications $\psi, \phi : \mathbb{K}^n \to \mathbb{K}^n$

PK: $h_1, \ldots, h_u, \ldots, h_n \in \mathbb{K}[x_1, \ldots, x_n]$ describing:

$$h = \underbrace{t \circ \psi \circ s \circ \phi \circ r}_{f, g} : \mathbb{K}^n \to \mathbb{K}^n.$$

$2R^-$ schemes: some polynomials of the PK are removed
Input: \( h = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u. \)

Find:

- \( f = (f_1, \ldots, f_u) \neq h \in \mathbb{K}[x_1, \ldots, x_n]^u, \) and
- \( g = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n, \)

such that:

\[
    h = (f \circ g) = (f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)).
\]
References

Lattices in Algorithmic and Cryptography

Jaime Gutierrez

Algorithmic Mathematics and Cryptography

University of Cantabria
Organization

- Lattices.
- Cryptographic Knapsack Scheme
- RSA and integer factoring with extra information.
- Pseudorandom number generators over Elliptic curves.
- Ideal decomposition and intermediate subfields.
- Cayley graphs of cyclic groups.
LATTICES
LATTICES

\[ B = [b_1 | \cdots | b_n], \text{ l.i.} \]

\[ \mathcal{L}(B) := \{Bx \mid x \in \mathbb{Z}^n\} \]
\( b_1, \ldots, b_n \in \mathbb{R}^m, \text{l.i.} \)

\[ \mathcal{L} = \mathcal{L}([b_1| \cdots |b_n]) = \]

\[ = \left\{ \sum_{i=1}^{n} \lambda_i b_i \bigg| \lambda_i \in \mathbb{Z} \right\}. \]

\( B = (b_1, \ldots, b_n) \) is a basis of \( \mathcal{L} \).

\[ \mathcal{L}([(1, 0), (0, 1)]) = \]

\[ \mathcal{L}([(2006, 1), (2007, 1)]) = \mathbb{Z}^2 \]

\[ \mathcal{L}([(3, 1), (2, 4)]) = \]

\[ \{(x, y) \in \mathbb{Z}^2 : 3x + y \equiv 0 \mod 10\} \]

[LAGRANGE, GAUSS, MINSKOWSKI]
DISCRETE SUBGROUPS

In general, \( \mathcal{L}(B) \) is not a lattice:

\[
B := (2, \sqrt{2})
\]

\[
\sqrt{2} 2
\]

Lattices are discrete subgroups.

\[
\lambda_1 := \min \{ \|v\| / v \in \mathcal{L} \setminus \{0\} \}
\]
The volume of a lattice

Fundamental Parallelepiped
(associated to a basis)

\[ \text{vol} \mathcal{L} = \sqrt{|B^t B|} \]
**Main Bounds**

- **Norm $\ell_\infty$:**
  \[ \lambda_1 \leq (\text{vol } \mathcal{L})^{1/n} \]

- **Norm $\ell_1$:**
  \[ \lambda_1 \leq (n! \text{vol } \mathcal{L})^{1/n} \]

- **Norm $\ell_2$:**
  \[ \lambda_1 \leq \sqrt{\gamma_n (\text{vol } \mathcal{L})^{1/n}} \]
  \[ \frac{n}{2e\pi} + o(n) \leq \gamma_n \leq \frac{1'744}{e\pi} n + o(n) \]

**Gauss Heuristic**
MAIN PROBLEMS

- SVP
  \[ \min\{\|v\| \mid v \in \mathcal{L}\backslash\{0\} \} \]

  NP hard ??

- CVP
  \[ \min\{\|v - t\| \mid v \in \mathcal{L} \} \]

  NP hard

Fixed \( n \) is polynomial: [KANNAN (1987)]

Approximation: [LLL = A. LENSTRA, H. LENSTRA, L. LOVÁCS (1982)],
[T. BABAI (1986)], [M. AJTAI (1998)]
LLL-reduction

\[ B = [b_1| \cdots |b_n] \text{ is a } \delta \text{-LLL reduced basis of } \mathcal{L} \text{ if} \]

1. \(|\mu_{i,j}| \leq 1/2\)
2. \(\delta \|b_i^*\| \geq \|\mu_{i+1,i} b_i^* + b_{i+1}^*\|,\)

where \(1/4 < \delta < 1\) and \(b_1^*, \ldots, b_n^*\) is the Gram-Schmidt orthogonal basis:

\[ b_i^* := b_i - \sum_{j<i} \mu_{ij} b_j, \mu_{i,j} := \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}. \]

\[ \|b_1\| \leq \left( \frac{1}{\delta - 1/4} \right)^{\frac{n-1}{2}} \lambda_1 \]

LLL-algorithm is polynomial in \(M = \max\{n, \log(\max_i \|b_i\|)\}\).
OUR LATTICES

\( \mathcal{L} \) consist of integer solutions \( x = (x_0, \ldots, x_{s-1}) \in \mathbb{Z}^s \) of a system of congruences

\[
\sum_{i=0}^{s-1} a_{ij} x_i \equiv 0 \pmod{q_j}, \quad j = 1, \ldots, m,
\]

modulo the integers \( q_1, \ldots, q_m \).

- Typically, \( \text{vol}(\mathcal{L}) = Q = q_1 \cdots q_m \).
- SVP and CVP are polynomials in \( \log Q \).
CRYPTOGRAPHIC KNAPSACK SCHEME
THE KNAPSACK PROBLEM

\((a_1, a_2, \ldots, a_n)\) a finite sequence of positive integers (the weights)

Given a natural \(s\) compute, if it exists, \(x_1, x_2, \ldots, x_n\), where \(x_i \{0, 1\}\) such that

\[
s = x_1a_1 + x_2a_2 + \cdots + x_na_n
\]

NP-complete problem
SUPER-INCREASING SEQUENCES

The sequence \((a_1, a_2, \ldots, a_n)\) is super-increasing if satisfies:

\[ a_i > a_1 + a_2 + \cdots + a_{i-1} \]

Example:

\[ a_i := k^i \]

In this case it is simple
THE MERKLE-HELLMAN CRYTOSYSTEM

- A \((b_1, b_2, \ldots, b_n)\) super-increasing sequence
- Two co-prime positive integers \(U\) and \(V\) such that
  \[
  U > \sum_{i=1}^{n} b_i, \quad V < U.
  \]
- \(a_i = b_i V \mod U.\)

- PUBLIC KEY: \((a_1, a_2, \ldots, a_n)\)
- PRIVATE KEY: \((b_1, b_2, \ldots, b_n, U, V)\)
THE MERKLE-HELLMAN CRYPTOSYSTEM

ENCRYPTION:
The plaintext $x, 0 \leq x < 2^n$

- $x = [x_1, \ldots, x_n]$ binary representation
- The cipher text is $y = \sum_{i=1}^{n} x_i a_i$

DECRIPTION.
The ciphertext $y, 0 \leq y < 2^n$

- Compute $s = y V^{-1} \mod U = \sum x_i b_i$
- $x = \sum_{i=1}^{n} x_i 2^{i-1}$
The Merkle-Hellman Cryptosystem

- Several variations of this scheme.
- It is easy to implement.
- It is faster than RSA
- Broken by Shamir in 1982
- Chor-Rivest Scheme
LLL AND MERKLE-HELLMAN CRYPTOGRAPHY

Given a knapsack problem with coefficients \((c_1, c_2, \ldots, c_n)\) and \(s\). Let \(\mathcal{L}\) be the lattice generated by \(A\):

\[
A = \begin{pmatrix}
-a_1 & a_2 & \ldots & -a_n & s \\
1 & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & 0 \\
\end{pmatrix} \in \mathbb{Z}^{(n+1) \times (n+1)},
\]

If \(x = (x_1, \ldots, x_n) : \sum_{i}^{n} x_i c_i = s \rightarrow \) vector \(v \in \mathcal{L}\) is small:

\[
v = (0, x_1, \ldots, x_n).
\]
Integers factorization

THE PROBLEM

INPUT: \( N = PQ \) and the high-order \( h \) bits of \( P \).
**Integers factorization**

**THE PROBLEM**

**INPUT:** \( N = PQ \) and the high-order \( h \) bits of \( P \).

**OUTPUT:** The factorization of \( N \), i.e, \( P \) and \( Q \).
Integers factorization

Why study this problem?
Integers factorization

Why to study this problem?

because I like it,
Integers factorization

**WHY TO STUDY THIS PROBLEM?**

- because I like it,
- RSA
  - loss of the equipment that generated $P$ and $Q$,
  - explicit release of partial extra information as part of a protocol, for instance exchange of secret,
  - timing measurements,
  - routine usage of $P$ and $Q$ to decrypt mail, sign messages, etc.,
  - poor physical security to guard $P$ and $Q$,
  - any other heuristic attack . . .

FORMALIZATION AND NOTATION

DEFINITION. We say that an integer \( w \) is a \( \Delta \)-approximation to the integer \( u \) when \( |w - u| \leq \Delta \).

We can build a \( \Delta \)-approximation \( P_0 \) to \( P \), by taking the \( h \) high-order bits of \( P \) and \( \lceil \log P \rceil + 1 - h \) zeroes. In this case, \( \Delta = 2^\lceil \log P \rceil + 1 - h - 1 \), that is,

\[
P - P_0 \leq \Delta \simeq \frac{P}{2^h}.
\]

By dividing \( N \) into \( P_0 \), we obtain a \( \Delta_1 \)-approximation \( Q_0 \) to \( Q \):

\[
|Q - Q_0| \leq \Delta_1 \simeq \frac{Q\Delta}{P}.
\]
Integers factorization and attacking RSA

FORMALIZATION AND NOTATION

Let $\varepsilon_0 = P - P_0$ and $\varepsilon_1 = Q - Q_0$. From $N = PQ$ we obtain:

$$f(\varepsilon_0, \varepsilon_1) = 0,$$

where

$$f(\varepsilon_0, \varepsilon_1) = (P_0 + \varepsilon_0)(Q_0 + \varepsilon_1) - N.$$

And with

$$|\varepsilon_0| \leq \Delta, \quad |\varepsilon_1| \leq \Delta_1.$$

The main objective is to find small roots of this innocent polynomial $f(\varepsilon_0, \varepsilon_1)$. 
The Coppersmith’s Result

**Theorem.** [D. Coppersmith (1997)]

Let $p(\varepsilon_0, \varepsilon_1)$ be an irreducible polynomial in two variables over $\mathbb{Z}$, of maximum degree $\delta$ in each variable separately. Let $\Delta, \Delta_1$ be bounds on the desired solutions $x_0, y_0$. Define $p^*(\varepsilon_0, \varepsilon_1) = p(\varepsilon_0 \Delta, \varepsilon_1 \Delta_1)$ and let $W$ be the absolute value of the largest coefficient of $p^*(\varepsilon_0, \varepsilon_1)$. If

$$\Delta \Delta_1 \leq W^{2/(3\delta)} - \epsilon 2^{-14\delta/3},$$

then in polynomial time in $(\log W, \delta, 1/\epsilon)$ we can find all integer pairs $(x_0, y_0)$ with $p(x_0, y_0) = 0$ bounded by $|x_0| \leq \Delta, |y_0| \leq \Delta_1$. 

Integers factorization

Adapting Coppersmith’s Result

We suppose that we know \( N = PQ \) and the high-order \( h = \frac{1}{4} \log_2 N \) bits of \( P \). We apply the previous result to polynomial \( f(\varepsilon_0, \varepsilon_1) \) and take:

\[
|\varepsilon_0| < P_0 N^{-1/4} = \Delta,
|\varepsilon_1| < Q_0 N^{-1/4} = \Delta_1,
\delta = 1, \quad W = N^{3/4}.
\]

Corollary. [D. Coppersmith (1997)]

In polynomial time we can find the factorization of \( N = PQ \) if we know the high-order \( \left( \frac{1}{4} \log_2 N \right) \) bits of \( P \).
**Integers factorization**

**Two Iteration Technique**

\[(P_0 + \varepsilon_0)(Q_0 + \varepsilon_1) = N,\]

\[|\varepsilon_0| \leq \Delta, \quad |\varepsilon_1| \leq \Delta_1\]

\[(P_0 Q_0 - N)\Delta_1 \Delta + Q_0 \Delta x_1 + P_0 \Delta_1 x_2 + x_3 = 0,\]

\[x_1 \equiv 0 \mod \Delta,\]

\[x_2 \equiv 0 \mod \Delta_1.\]
**Integers factorization**

**TWO ITERATIONS TECHNIQUE**

- $e = (\Delta_1 \varepsilon_0, \Delta \varepsilon_1, \varepsilon_0 \varepsilon_1)$.
- $f$ solution of the CVP. Check if $e = f$, otherwise:

  - $u, v$ LLL reduced basis of lattice:

    $Q_0 \Delta x_1 + P_0 \Delta_1 x_2 + x_3 = 0,$
    
    $x_1 \equiv 0 \bmod \Delta,$
    
    $x_2 \equiv 0 \bmod \Delta_1.$

- $f = (\Delta_1 f_1, \Delta f_2, f_3),$  
- $u = (\Delta_1 u_1, \Delta u_2, u_3),$  
- $v = (\Delta_1 v_1, \Delta v_2, v_3).$
TWO ITERATIONS TECHNIQUE

\[
e = f + \alpha u + \beta v
\]

\[
\Downarrow
\]

\[
\varepsilon_0 = f_1 + \alpha u_1 + \beta v_1,
\]

\[
\varepsilon_1 = f_2 + \alpha u_2 + \beta v_2,
\]

\[
\varepsilon_0 \varepsilon_1 = f_3 + \alpha u_3 + \beta v_3,
\]

\[
\Downarrow
\]

\[
(f_1 + \alpha u_1 + \beta v_1)(f_2 + \alpha u_2 + \beta v_2) = f_3 + \alpha u_3 + \beta v_3
\]

This is a new equation in \(\alpha, \beta\)
**Two iterations result**

**Theorem.** [D. Gómez and J. G. and A. Ibeas (2006)]

For a prime $P$ and natural numbers $\Delta$, $\Delta_1$, there is a set $\mathcal{V}(\Delta, \Delta_1) \subset \mathbb{Z}_P$ of cardinality

$$\# \mathcal{V}(\Delta, \Delta_1) = O\left(\frac{(\Delta^7 \Delta_1^4)}{P^3}\right)$$

with the following property. Given $N$, $P_0$, $Q_0$, $\Delta_1$ and $\Delta$, where $N = PQ$, $P_0$ is a $\Delta$-approximation of $P$ and $Q_0$ a $\Delta_1$-approximation of $Q$ then if $Q \notin \mathcal{V}(\Delta, \Delta_1)$ there is an algorithm such that recover $P$ and $Q$ in polynomial time in the size of $N$. 
**PRACTICAL APPLICATION: TWO ITERATIONS**

\[ P \equiv Q \equiv \sqrt{N}, \text{ then } O\left(\frac{(\Delta_7 \Delta_{41})}{P^3}\right) < P \text{ implies } 3/10 \log N < h \]

\[ P, Q \equiv 2^{1000} \]

- This method requires :636 bits of \( P \).
- The dimension of the lattice is 8.
- For the same known bits, Coppersmith method requires a lattice of dimension 199.
Integers factorization

**NUMERICAL RESULTS**

<table>
<thead>
<tr>
<th>Bits of P</th>
<th>Bits of Q</th>
<th>Bits known</th>
<th>Iterations</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>100</td>
<td>66</td>
<td>1</td>
<td>3.675 sec</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>60</td>
<td>2</td>
<td>10.271 sec</td>
</tr>
<tr>
<td>512</td>
<td>512</td>
<td>306</td>
<td>2</td>
<td>11.392 sec</td>
</tr>
<tr>
<td>512</td>
<td>512</td>
<td>300</td>
<td>3</td>
<td>14.025 sec</td>
</tr>
<tr>
<td>512</td>
<td>512</td>
<td>292</td>
<td>3</td>
<td>15.339 sec</td>
</tr>
<tr>
<td>1024</td>
<td>1024</td>
<td>624</td>
<td>2</td>
<td>7.240 sec</td>
</tr>
<tr>
<td>1024</td>
<td>1024</td>
<td>600</td>
<td>3</td>
<td>29.357 sec</td>
</tr>
<tr>
<td>1024</td>
<td>1024</td>
<td>580</td>
<td>3</td>
<td>1 m. 35 sec</td>
</tr>
</tbody>
</table>
LINEAR GENERATOR
over
ELLIPTIC CURVES
Linear generators over elliptic curves

STREAM CIPHERS

Insecure channel

\[ m \rightarrow m \oplus k \] ......... \[ m \oplus k \rightarrow m \]

\[ k = \begin{array}{ccccccc}
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\end{array} \]

\[ \ldots \]
**Linear congruential generator**

\[
a \in \mathbb{F}_p^*, \quad c \in \mathbb{F}_p
\]

\[
u_0 \in \mathbb{F}_p \text{ (seed)}
\]

\[
u_{n+1} \equiv_p aun + c
\]
LINEAR GENERATOR ON ELLIPTIC CURVES

This generator employs the usual abelian group operation \( \oplus \) on the set of points of an elliptic curve:

- A prime \( p \).
- An elliptic curve \( \mathbb{E} : Y^2 = X^3 + AX^2 + B \) over \( \mathbb{F}_p \).
- The seed \( U_0 \in \mathbb{E} \).
- The parameter \( G \in \mathbb{E} \), which we call composer.

\[ U_{n+1} = U_n \oplus G, \forall n \geq 0. \]
Toy example with a 7-periodic generator in an elliptic curve with 35 points over $\mathbb{F}_{31}$.

$E: Y^2 = X^3 - X^2 + 1$

$U_{n+1} = n(5, 11) \oplus (8, 3)$
CRYPTOGRAPHICALLY SECURE GENERATOR

A PRBG is cryptographically secure if there is no polynomial time algorithm which on input of the first $l$ bits of an output sequence $s$ can predict the $(l + 1)^{st}$ bit of $s$ with probability significant greater than $1/2$.

[YAO (1982)], [BLUM AND BLUM AND SHUB (1998)]
A PRBG is cryptographically secure if there is no polynomial time algorithm which on input of the first \( l \) bits of an output sequence \( s \) can predict the \((l + 1)^{st}\) bit of \( s \) with probability significant greater than \(1/2\).

[Yao (1982), Blum and Blum and Shub (1998)]

\[ k = \begin{array}{cccccccccccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \cdots \\
\end{array} \]

[Blackburn and Gómez and J. G. and I. Shparlinski (2005)]

Linear generators over elliptic curves

**METHOD SKETCH**

We assume access to:

- Approximations $W_0, W_1$ to the first two values $U_0, U_1$:
  - $U_i = (x_i, y_i), W_i = (\alpha_i, \beta_i)$,
  - $x_i = \alpha_i + e_i, y_i = \beta_i + f_i, |e_i|, |f_i| \leq \Delta$.
- The composer $G = (x_G, y_G)$.

From $U_0 \oplus G = U_1$ when $U_0 \not\in \{G, -G\}$, we obtain (over $\mathbb{F}_p$):

$$x_G^3 + x_1 x_G^2 - x_0 x_G^2 - 2x_1 x_G x_0 - x_G x_0^2 + x_0^3 + 2y_G y_0 + x_1 = 0,$$

$$y_1 x_G - y_1 x_0 - y_G x_0 + y_G x_1 - y_0 x_1 + y_0 x_G = 0.$$
METHOD SKETCH

- Translate previous equations into a linear system in the approximation errors $e_0, e_1, f_0, f_1$.
- Find the smaller integer solution to the system (CVP)
- Check if the obtained solution is valid.

THEOREM. [J. G. AND A. IBEAS (2007)]

If the algorithm outputs a wrong solution, the first coordinate $x_0$ of the first value must satisfy a certain equation. This leads to the bound $O(\Delta^6)$ for the possibilities for $x_0$ in a failure example. So, when $\Delta < p^{1/6}$ we can expect with high probability the success of the guessing algorithm.
Linear generators over elliptic curves

UNKNOWN COMPOSER

We take three approximations \( W_i = (\alpha_i, \beta_i) \) to any three values (consecutive or not): \( U_i = (x_i, y_i) \)

\[
y_i^2 = x_i^3 + Ax_i + B, \quad i = 0, 1, 2.
\]

Eliminating the curve parameters \( A, B \) and assuming that \( U_0 \notin \{U_1, -U_1\} \) (that is, \( x_0 \neq x_1 \)), we obtain the following equation:

\[
-y_2^2 x_1 + y_2^2 x_0 + x_2^3 x_1 - x_2^3 x_0 - x_2 y_0^2 + x_2 x_0^3 + x_2 y_1^2 - x_2 x_1^3 - y_1^2 x_0 + x_1 x_0^3 + x_1 y_0^2 - \]

Substituting \( x_i = \alpha_i + e_i, \quad y_i = \beta_i + f_i \) for \( i = 0, 1, 2 \), we obtain a threshold of \( p^{1/46} \) for the tolerance below which we can expect successful guessing.
**Theorem.** [J. G. (2007)]

There exists an algorithm with the following properties. Let $p$ be a prime number and $\Delta$ a positive integer such that $p > \Delta \geq 1$. Let $f(X, Y) = \sum_{i=0,j=0}^{m_1,m_2} a_{i,j} X^i Y^j \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of degree $m_1 \geq 2$ in $X$ and degree $m_2 \geq 2$ in $Y$ over $\mathbb{F}_p$.

The algorithm, when given $f$ and $\Delta$-approximations $w_0, w_1$ to $v_0, v_1$ where $f(v_0, v_1) \equiv 0 \mod p$, recovers $v_0, v_1$ in time polynomial in $m_1, m_2$ and $\log q$ provided that $v_0$ does not lie in a certain set $\mathcal{V}(f) \subseteq \mathbb{F}_p$ of cardinality:

$$\mathcal{V}(f) = (2\sqrt{(m_1 + 1)(m_2 + 1)\lambda(m_1+1)(m_2+1)})^{(m_1+1)(m_2+1)} \Delta^{\omega_{m_1,m_2}}$$

$$\omega_{m_1,m_2} = \frac{m_1^2}{2}(2m_2 + 1) + \frac{m_2^2}{2}(2m_1 + 1) + m_1m_2.$$
IDEAL DECOMPOSITION
and
INTERMEDIATE FIELDS
Ideal decomposition and intermediate fields

THE PROBLEM

Given:

\( f(x) \) polynomial in \( \mathbb{Q}[x] \)

Find:

\( g(x), h(x), \bar{f}(x) \in \mathbb{Q}[x] \) verifying

\[ f(x)\bar{f}(x) = g(h(x)), \]

\( 1 < \deg g, \deg h < \deg f. \)
POLYNOMIAL DECOMPOSITION AND RATIONAL SUBFIELDS

If \( \deg \bar{f} = 0 \), then

\[
f(x) = g(h(x)).
\]

Lüroth’s Theorem. [A. Schinzel (1982)]

Let \( F \) be a field such that \( K \subset F \subset K(x_1, \ldots, x_n) \) and \( \text{tr.deg.}(F/K) = 1 \). Then there exists \( h \in K(x_1, \ldots, x_n) \) such that \( F = K(h) \). Also, if the field contains a polynomial, then a polynomial generator exists.

\[
\{[(g, h)] : f = g(h)\} \leftrightarrow \{F : K(f) \subset F \subset K(x)\}
\]

\[
[(g, h)] \leftrightarrow F = K(h).
\]

Ideal decomposition and intermediate fields

**ALGEBRAIC SUBFIELDS**

If \( f(x) \) is irreducible and \( f(\alpha) = 0 \), then the following statements are equivalent:

- \( f \) is an ideal decomposable.
- \( \text{Gal}_{\mathbb{Q}}(f) \) acts imprimitively on the roots of \( f \).
- A proper subfield, \( \mathbb{Q}(\beta) \), exists with
  \[ \mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha). \]

\[
[(\bar{f}, g, h)] : f \bar{f} = g(h) \quad \leftrightarrow \quad \{ F : \mathbb{Q} \subset F \subset \mathbb{Q}(\alpha) \}
\]

\[
[(\bar{f}, g, h)] \quad \leftrightarrow \quad F = \mathbb{Q}(h(\alpha)).
\]

[S. Landau and G. Miller (1985)], [J. Klüners and M. Pohst (1997)]
[J. G. and D. Sevilla (2006)]

---

LATTICES IN ALGORITHMIC AND CRYPTOGRAPHY. University of Maria Curie-Sklodowska, Lublin 3-14 December 2012. – p.51/72
Ideal decomposition and intermediate fields

THE ALGORITHM

We divide the problem into two parts:

1. Compute candidates polynomial $h(x)$.
2. Given $f(x)$ and $h(x)$, compute (if it exists) $\bar{f}(x)$, $g(x)$:

   $$f(x)\bar{f}(x) = g(h(x))$$

- Compute $\bar{f}(x)$, $g(x)$ from $f(x)$ and $h(x)$ is solving a linear system of equations.
- The hard part is compute $h(x)$. 
Ideal decomposition and intermediate fields

THE BASIC IDEA

From

\[ f(x) \bar{f}(x) = g(h(x)), \]

There are two distinct roots of \( f(x) \), say \( \alpha_i \) and \( \alpha_j \) for which

\[ h(\alpha_i) = h(\alpha_j) \]

\[ h(x) = \sum_{k=1}^{s} h_k x^k \in \mathbb{Z}[x] \text{ for some } s \text{ with: } 1 < s < \deg f \]

Find the coefficients \( h_1, h_2, \ldots, h_s \) in \( \mathbb{Z} \) satisfying

\[ h_1(\alpha_i - \alpha_j) + h_2(\alpha_i^2 - \alpha_j^2) + \cdots + h_s(\alpha_i^s - \alpha_j^s). \]
Ideal decomposition and intermediate fields

INTEGER RELATIONS

A nonzero vector $h = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ is called an INTEGER RELATION for the real numbers $\gamma_1, \ldots, \gamma_s$ if

$$h_1 \gamma_1 + \cdots + h_s \gamma_s = 0.$$ 

Given $\bar{\gamma}_1, \ldots, \bar{\gamma}_s$ complex numbers approximating to the algebraic numbers $\gamma_1, \ldots, \gamma_s$, and a parameter $\epsilon$,

- either finds an integer relation for $\gamma_1, \ldots, \gamma_s$ or
- proves that no relation of Euclidean length shorter than $1/\epsilon$ exists.
Ideal decomposition and intermediate fields

INTEGER RELATIONS AMONG ALGEBRAIC NUMBERS

\[ \mathcal{L}([b_1| \cdots |b_s]) \subset \mathbb{Q}^{s+2} \] the lattice spanned

\[ \begin{align*}
  b_1 &= (1, 0, \ldots, 0, C \cdot Re(\bar{\gamma}_1), C \cdot Im(\bar{\gamma}_1)) \\
  & \vdots \\
  b_s &= (0, \ldots, 0, 1, C \cdot Re(\bar{\gamma}_s), C \cdot Im(\bar{\gamma}_s))
\end{align*} \]

\( C \) is a large integer depend on \( \epsilon \), the height of \((\gamma_1, \ldots, \gamma_s)\) and \([\mathbb{Q}(\gamma_1, \ldots, \gamma_s) : \mathbb{Q}]\).

- Let \( b \) be the first vector of the LLL-basis:
  \[ b = (m_1, \ldots, m_s, C \cdot \sum_{i=1}^{s} m_i Re(\bar{\gamma}_i), C \cdot \sum_{i=1}^{s} m_i Im(\bar{\gamma}_i)). \]
- If \( \|b\| < 2^n/\epsilon^2 \), then \((m_1, \ldots, m_s)\) is a solution. Otherwise, no solution shorter than \(1/\epsilon\) exists.

[J. HÅSTAD AND B. JUST AND J. LAGARIAS AND C. SCHNORR (1989)]

LATTICES IN ALGORITHMIC AND CRYPTOGRAPHY. University of Maria Curie-Sklodowska, Lublin 3-14 December 2012. – p.55/72
**Ideal decomposition and intermediate fields**

**Bounds on the coefficients of** $h(x)$

Given a non-trivial ideal decomposition of polynomial $f \in \mathbb{Z}[x]$, i.e.

$$f(x) \bar{f}(x) = g(h(x))$$

find an upper bound on the height $Ht(h(x))$ of $h(x)$.

- **Polynomial Decomposition**, i.e., $\bar{f}(x) = 1$, then
  $$Ht(h(x)) < C Ht(f(x)).$$

- If $f(x)$ is irreducible: [J. Dixon (1990)], [J. McKay (1996)],
  $$Ht(h(x)) < C Ht(f(x))^\deg f,$$
  where $C$ is a constant

- In general, ???

---

*Lattices in Algorithmic and Cryptography.* University of Maria Curie-Sklodowska, Lublin 3-14 December 2012. – p.56/72
Cayley graphs of cyclic groups

**CIRCULANT DI-GRAPHS**

- **Vertices:** $G = (\mathbb{Z}_N, +)$
- **Edges - Set of jumps:** $H = \{j_1, \ldots, j_r\}$

$(x, x + j_i \mod N), \quad x \in \mathbb{Z}_N, \ 1 \leq i \leq r$

$N = 10$

$H = \{1, 3\}$

Connected graph: $\gcd(j_1, \ldots, j_r, N) = 1$
Cayley graphs of cyclic groups

**ADJACENCY MATRIX**

Circulant Matrix:

\[
R_N = \begin{pmatrix}
0 & 1 \\
1 & 0 \\
\vdots & \vdots \\
1 & 0
\end{pmatrix}
\]

\[
C_N(j_1, \ldots, j_r), \quad \sum_{i=1}^{r} R_N^{j_i}
\]

**Undirected:** \( C_N(\pm j_1, \ldots, \pm j_r) \)
**DISTRIBUTED LOOP COMPUTER NETWORKS**

- Application to distributing an parallel computation.
- A extremely simple description.
- \( O(r \log N) \)
- small diameter.
- Routing algorithms and fault tolerance.
- The two jump case is widely studied.

[C. K. WONG AND D. COPPERSMITH (1974)]

[J.C. BERMOND AND F. COMELLAS AND D. F. HSU (1995)]
Cayley graphs of cyclic groups

Paths in a circulant

\[ x = (x_1, \ldots, x_r) \in \mathbb{N}^r \]

\[ x = (x_1, \ldots, x_r) \in \mathbb{Z}^r \]
**Cayley graphs of cyclic groups**

**The lattice of a circulant graph**

Given the jumps $j_1, \ldots, j_r$ and the number of nodes $N$:

$$\mathcal{L}_C = \{(x_1, \ldots, x_r) \in \mathbb{Z}^r : j_1 x_1 + \cdots + j_r x_r \equiv 0 \text{ mod } N.\}$$

A shortest path from node $\alpha$ to node $\beta$:

- **Undirected**: $x = (x_1, \ldots, x_r) \in \mathcal{L}_C$ (with minimal $\|x\|_1$).
- **Directed**: $x = (x_1, \ldots, x_r) \in \mathcal{L}_C \cap \mathbb{N}^r$ (with minimal $\|x\|_1$)

$$\sum_{i=1}^{r} x_i j_i \equiv \alpha - \beta \text{ mod } N.$$
Cayley graphs of cyclic groups

SHORTEST PATH FOR TWO JUMPS
Cayley graphs of cyclic groups

PATH DESCRIPTION

\[ C_N(a, b) \]
\[ w = (x_1, x_2) / ax_1 + bx_2 \equiv c \mod N \]

\[ L := \{ x \in \mathbb{Z}^2 / ax_1 + bx_2 \equiv 0 \mod N \} \]
\[ CA(c) = w + L \]

The total amount of jumps of the path \( w \) is \( \|w\|_1 \).
Cayley graphs of cyclic groups

**THE COMPLEXITY THEOREM.** [D. GÓMEZ AND J. G. AND A. IBEAS (2005)]

**INPUT:** $a, b, N, c$

- Description of the set of paths $CA(c)$.
  $$w + \mathbb{Z} < u, v >$$
  $O(\log N)$

- Reduction of the basis $L$.
  $$w + \mathbb{Z} < u, v >$$
  $O(\log N)$

- Iterative reduction.
  $$w'$$
  $O(\log N)$

- Discrete searching.
  $$w''$$
  $O(1)$

$$O(\log^2 N \log \log N \log \log \log N))$$
THE POLYNOMIAL IDEAL OF A LATTICE

\[ I_\mathcal{L} := ( x^{a^+} - x^{a^-} : a \in \mathcal{L} ) \subset K[X_1, \ldots, X_r]. \]

\[ a = a^+ - a^- = (a_1, \ldots, a_r) \in \mathbb{Z}^r, \quad a^+ = (a_1^+, \ldots, a_r^+), \]
\[ a_i^+ = \max\{a_i, 0\}, \quad a^- = (a_1^-, \ldots, a_r^-), \quad a_i^- = \max\{-a_i, 0\}. \]

[B. Sturmfels and R. Weismantel and G. M. Ziegler (1995)]

THEOREM. [J. G. and A. Ibeas (2006)]

\[ I_{\mathcal{L}_C} = ( x_1^N x_2^N \cdots x_r^N - 1, \quad x^{a^+} - x^{a^-}, (a \in S) ), \]

\[ S = \{(N\alpha_1, \ldots, N\alpha_r), (\alpha_1 j_1 - 1, \alpha_2 j_2, \ldots, \alpha_r j_r), \]
\[ (\alpha_1 j_1, \alpha_2 j_2 - 1, \ldots, \alpha_r j_r), \ldots, (\alpha_1 j_1, \ldots, \alpha_{r-1} j_{r-1} \alpha_r j_r - 1)\}. \]
\[ \alpha_i \in \mathbb{Z}, \quad (i = 1, \ldots, r), \quad 1 = \alpha_1 j_1 + \cdots + \alpha_r j_r + \beta N \]
**Groebner Bases and Routing Theorem.** [J. G. and A. Ibeas (2006)]

Fixed any grade monomial ordering $\prec$:
Let $G$ be a Gröbner basis of $I_{LC}$ with respect $\prec$ and $c$ a path from 0 to $j \in \mathbb{Z}_N$.

The normal form of $x^c - 1$ with respect $G$ is $x^d - 1$, where $d$ is a shortest path.
GROEBNER BASES
and
LLL-REDUCED BASES
Groebner Bases and LLL-reduced bases

**Groebner Basis versus LLL-reduced Basis**

**Definition** Let $I$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. 
$G = \{g_1, \ldots, g_s\} \subset I$ is a Groebner Basis if and only if $\forall f \in I$ 

\[
f = \sum_{i=1}^{s} f_i g_i \text{ with } f_i \in \mathbb{K}[x_1, \ldots, x_n], g_i \in G \text{ and } \ \text{lm}(f) \geq \text{lm}(f_i g_i)
\]
Groebner Bases and LLL-reduced bases

**Groebner Basis versus LLL-reduced Basis**

**Definition** Let $I$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

$G = \{g_1, \ldots, g_s\} \subset I$ is a Groebner Basis if and only if $\forall f \in I$

\[
f = \sum_{i=1}^{s} f_i g_i \text{ with } f_i \in \mathbb{K}[x_1, \ldots, x_n], g_i \in G \text{ and } \text{lm}(f) \geq \text{lm}(f_i g_i)
\]

**Definition** Let $\mathcal{L}$ be a lattice of $\mathbb{Z}^n$. $G = \{b_1, \ldots, b_s\} \subset \mathcal{L}$ is a G-Reduced Basis if and only if $\forall v \in \mathcal{L}$

\[
x = \sum_{i=1}^{s} \alpha_i b_i \text{ with } \alpha_i \in \mathbb{Z}, b_i \in G \text{ and } ||x|| \geq ||\alpha_i b_i||
\]
**GROEBNER BASIS VERSUS LLL-REDUCED BASIS**

**Definition** Let $I$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.  
$G = \{g_1, \ldots, g_s\} \subset I$ is a Groebner Basis if and only if $\forall f \in I$ 
\[
f = \sum_{i=1}^{s} f_i g_i \text{ with } f_i \in \mathbb{K}[x_1, \ldots, x_n], g_i \in G \text{ and } \text{lm}(f) \geq \text{lm}(f_i g_i) \]

**Definition** Let $\mathcal{L}$ be a lattice of $\mathbb{Z}^n$. $G = \{b_1, \ldots, b_s\} \subset \mathcal{L}$ is a G-Reduced Basis if and only if $\forall v \in \mathcal{L}$ 
\[
x = \sum_{i=1}^{s} \alpha_i b_i \text{ with } \alpha_i \in \mathbb{Z}, b_i \in G \text{ and } \|x\| \geq \|\alpha_i b_i\| \]

**LLL-Reduced $\not\Rightarrow$ G-reduced**
Groebner Bases and LLL-reduced bases

**Groebner basis versus LLL-reduced basis**

**Theorem** [D. Gómez (2005)]

Let \(\{b_1, \ldots, b_s\}\) be a LLL reduced basis of a lattice \(\mathcal{L}\) with respect to \(\delta\), \(1/4 < \delta < 1\). Let \(x \in \mathcal{L}\) such that:

\[
x = \alpha_1 b_1 + \cdots + \alpha_s b_s,
\]

then we have the following inequality:

\[
\|\alpha_i b_i\| \leq 2^{3s} \|x\|,
\]

for all \(i = 1, \ldots, s\).