Lattice based cryptography

Milan Boháček

MFF UK

March 23, 2012 / Spring school of algebra

Babai's Nearest Plane Algorithm

- Developed by L. Babai in 1986.
- Solves CPV_γ for $\gamma = 2^{\frac{n}{2}}$
- Given a basis $B \in \mathbb{Z}^{m \times n}$ and a point $t \in \mathbb{Z}^m$, find a point $x \in \mathcal{L}(B)$ such that $\|x - t\| \leq 2^{\frac{n}{2}} \text{dist}(t, \mathcal{L}(B))$.

Algorithm 1 Babai's algorithm

Input: Basis $B \in \mathbb{Z}^{m \times n}$, $t \in \mathbb{Z}^m$

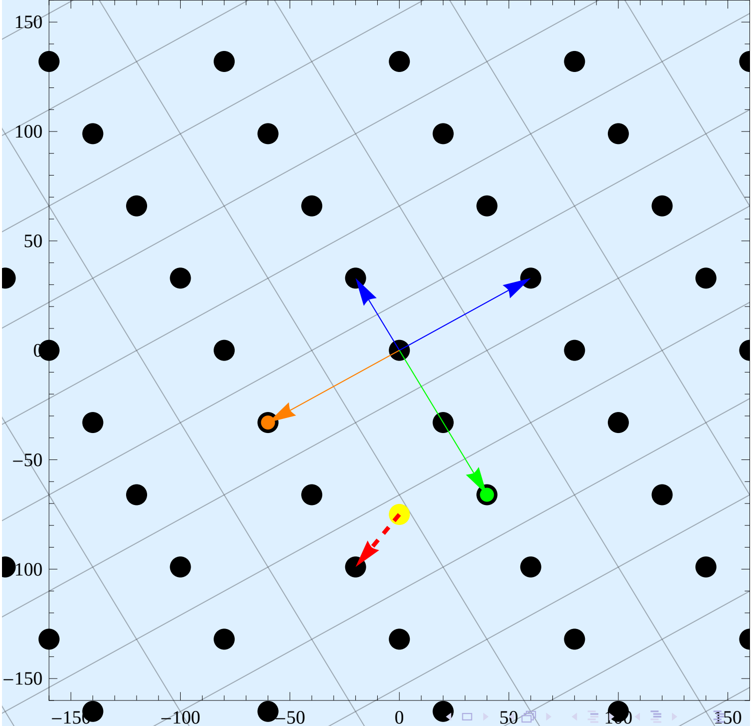
Output: A vector $x \in \mathcal{L}(B)$ such that $\|x - t\| \leq 2^{\frac{n}{2}} \mathrm{dist}(t, \mathcal{L}(B))$

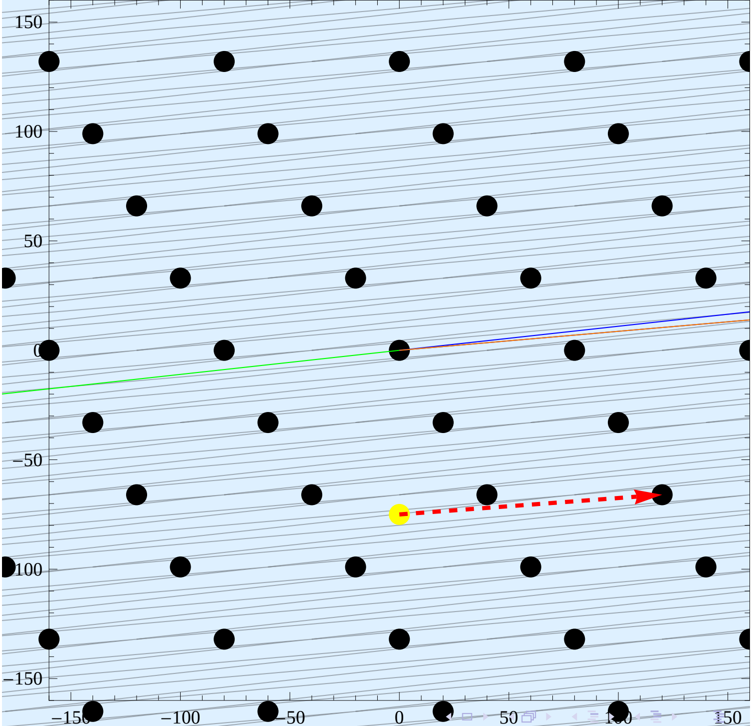
1: $\tilde{B} \leftarrow \mathrm{LLL}_\delta(B)$ with $\delta = \frac{3}{4}$ $\qquad \triangleright\ \tilde{B} = (\tilde{b}_1, \cdots, \tilde{b}_n)$

2: $t = \alpha_1 \tilde{b}_1 + \alpha_2 \tilde{b}_2 + \ldots + \alpha_n \tilde{b}_n$

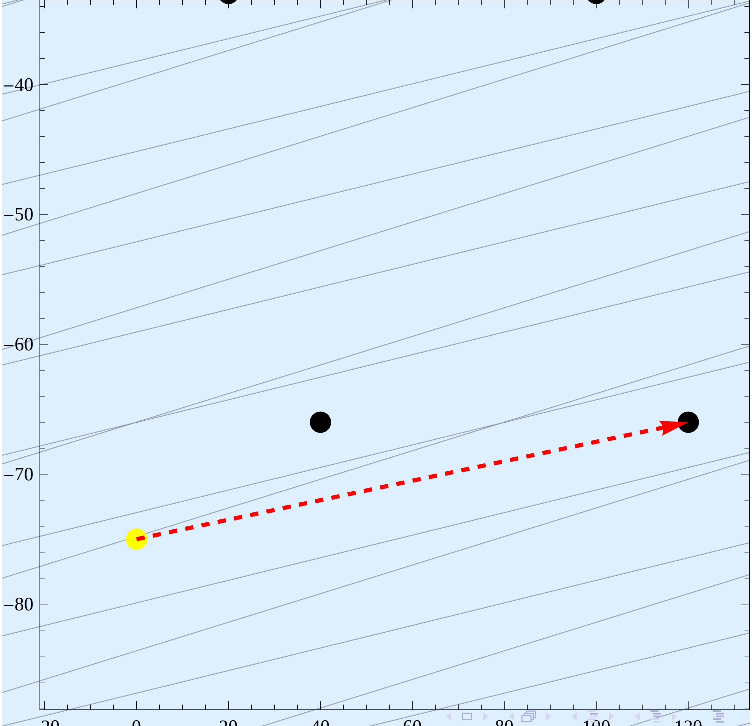
3: **return** $\lceil \alpha_1 \rfloor \tilde{b}_1 + \lceil \alpha_2 \rfloor \tilde{b}_2 + \ldots + \lceil \alpha_n \rfloor \tilde{b}_n$

- Running time is polynomial in the input size.
- LLL is polynomial and the rest is just n times some polynomial operations.
- Mathematica demo1 (but images on next 3 slides first)!


150
100
50
0
−50
−100
−150
−150
−100
−50
0
50
100
150



150
100
50
0
−50
−100
−150
−150
−100
−50
0
50
100
150

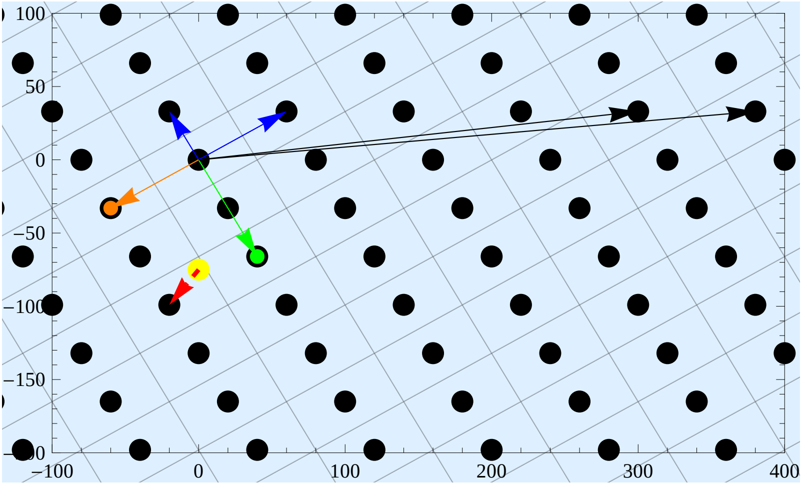

−40
−50
−60
−70
−80

The GGH Signature

- Suggested by O. Goldreich, S. Goldwasser and S. Halevi in 1997.
- 
- Without security proof.
- Idea: CVP is hard. But easy with good basis.

The GGH Signature Scheme

- Key generation algorithm
  - Choose a lattice with some good basis
  - Private key = good basis
  - Public key = bad basis
- Signing algorithm: given a message and a private key
  - Map message to a point in space
  - Apply Babai's algorithm with good basis to obtain the signature
- Verification algorithm: given (message, signature) and a public key, verify
  - Signature is a lattice point
  - Signature is close to the message


100
50
0
−50
−100
−150
−200
−100
0
100
200
300
400

The NTRUSign Signature

- GGH based signature scheme
- by J. Hoffstein, N. Howgrave-Graham, J.Pipher, J.H. Silverman and William Whyte in 2003
- 
- under consideration for standardization by the IEEE P1363 working group.
- uses $2N$ dimensional Convolution Modular Lattices
- All operations are done in ring of convolution polynomials $R = \mathbb{Z}[x]/(x^N - 1)$.

Convolution

- Convolution $*$ of two polynomials f and g is defined by taking the coefficient of x^k in $f * g$ to equal

$$(f * g)_k \equiv \sum_{i+j \equiv k \pmod{N}} f_i \cdot g_j \qquad (0 \leq k \leq N)$$

  If coefficients of the polynomials are reduced modulo q for some q we will refer to the convolution as being *modular*.

- Product of polynomials is simply their convolution in case of NTRUSign (recall $R = \mathbb{Z}[x]/(x^N - 1)$).
- Proof: $x^k \equiv x^{k \mod N}$

Convolution Modular Lattice L_h

Definition

- The *Convolution Modular Lattice* L_h associated to the polynomial

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{N-1} x^{N-1} \in R$$

is set of vectors $(u, v) \in R \times R \cong \mathbb{Z}^{2N}$ satisfying

$$v(x) = h(x) * u(x) \pmod{q}.$$

Example

- $h(x) = h(x) * 1 \pmod{q} \ldots (1, h) \in L_h$
- $q = h(x) * 0 \pmod{q} \ldots (0, q) \in L_h$

Lemma

Convolution modular lattice has a rotational invariance property: If $(u, v) \in L_h$, then

$$(x^i * u, x^i * v) \in L_h \quad \forall\, 0 \leq i < N.$$

Proof.

- We have $v(x) = h(x) * u(x) \pmod{q}$
- multiply both sides by x^i.
- $(x^i * v(x)) = h(x) * (x^i * u(x)) \pmod{q}$
- so $(x^i * u, x^i * v) \in L_h$

$\square$

NTRU Lattice L_h^{NT}

Definition

- If the polynomial h has a decomposition of the form $h \equiv f^{-1} * g \pmod q$ with polynomials f and g having small coefficients, then we say that L_h is and *NTRU Lattice* and denote it by L_h^{NT}.

The NTRUSign Signature Scheme - KG

- Key generation algorithm
  - Select a (prime) dimension N, modulus q, key size parameters $\deg(f)$ and $\deg(g)$.
  - Choose polynomials (f, g) and computes $h \equiv f^{-1} * g \pmod{q}$.
  - Compute polynomials F,G satisfying

$$f * G - g * F = q.$$

  - f, g, G, H is private key.
  - h is public key.

The NTRUSign Signature Scheme

- Signing algorithm: given a message and a private key
  - Hash digital document to create a random vector $(m_1, m_2) \bmod q$.
  - Write

$$\begin{aligned} G * m_1 - F * m_2 &= A + qB, \\ -g * m_1 + f * m_2 &= a + qb \end{aligned}$$

    where A and a have coefficients between $-q/2$ and $q/2$. The signature is the polynomial s given by

$$s \equiv \quad f * B + F * b \pmod{q}.$$

- Verification algorithm: given (message, signature) and a public key, verify
  - Compute $t \equiv s * h \pmod{q}$
  - Verify that $\|s - m_1\|^2 + \|t - m_2\|$ is small.

Lemma

Rotations of (f, g) and (F, G) forms a basis of L_h.

Proof.

- We want to show that

$$H \begin{pmatrix} f & g \\ F & G \end{pmatrix} = \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix}$$

  For some unimodular matrix H i.e. $\det(H) = \pm 1$ and H has entries in $R = \mathbb{Z}[x]/(x^N - 1)$.
- F and G were chosen so that $f * G - g * F = q = \det \begin{pmatrix} f & g \\ F & G \end{pmatrix} = \det \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} = q$.
- So $\det(H) = 1$

Proof cont.

- Now we must prove that $H \in R^{2,2}$
- $f * h \equiv g \pmod{q}$ and $q \nmid f$, $q \nmid g$
- So there must be $F_1 \in R$ and $G_1 \in R$ such that $qF_1 = F$ and $qG_1 = G$

$$\begin{aligned}
H &= \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} \begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1} = \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} \begin{pmatrix} f & g \\ qF_1 & qG_1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} \begin{pmatrix} G_1 & -g/q \\ -F_1 & f/q \end{pmatrix} \\
&= \begin{pmatrix} G_1 - F_1 * h & (-g + f * h)/q \\ -qF_1 & f \end{pmatrix} \in R^{2,2}
\end{aligned}$$

- So H is indeed unimodular.

$\square$

- Suggested by Phong Q. Nguyen at Eurocrypt 2006.
- 
- Inherited security flaw in GCH-based signature schemes.
- Attack recovers the private key.
- Demonstrated practical attack on:
- GGH
  - Up to dimension 400
- NTRUSign
  - Up to dimension 502
  - Applies to half of the parameter sets in P1363.
  - Only 400 signatures needed!
- Running time is few minutes on a 2GHz/2GB PC.

Attack outline

- Collect as many signatures as you can.
- Mathematica demo3.
- Now you have fundamental parallelepiped approximation.

Attack outline

- Morph parallelepiped into unit centered hypercube.
- All of our samples x can be written as $x = Ry$ where y is chosen uniformly from $[-1, 1]^n$ and R is some matrix.
- $E[xx^\mathsf{T}] = E[Ry(Ry)^\mathsf{T}] = E[Ryy^\mathsf{T}R^\mathsf{T}]$
- $= RE[yy^\mathsf{T}]R^\mathsf{T} = RR^\mathsf{T}/3$
- So we can can have an approximation of $S = RR^\mathsf{T}$.
- Then $S^{-1/2}.R = I$ and so we can squeze parallelepiped into hypercube.
- Mathematica demo3.

Attack outline

- Use the fourth moment to find hypercube's face vector.
- Morph discovered vectors back.
- For unit vector u and random samples x from unit hypercube define Kurtosis (fourth moment) as:
- $Kur(u) = E_x[\langle u, x\rangle^4]$
- Then the global minimum of $Kur(u)$ over the unit sphere of R^n is $1/5$ and this minimum is obtained at direction of faces of hypercube. There are no other local minima.
- Mathematica demo4.

Thank you for your attention!