# Lattices III – Babai's CVP algorithm and lattice based signature cryptosystems

Milan Boháček

In this talk we will introduce Babai's nearest plane algorithm for solving $\text{CVP}_\gamma$. Then we will introduce GGH signature scheme and its implementation NTRUSign signature scheme. Practical attack on GGH will be sketched.

## 1 Babai's nearest plane algorithm

**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 $\|x - t\| \leq 2^{n/2}\text{dist}(t, \mathcal{L}(B))$

```
procedure CVP(a, b)
    B̃ ← δ − LLL on B with δ = 3/4                ▷ B̃ = (b̃_1, ··· , b̃_n)
    b ← t
    for j = n to 1 do
        c_j ← ⌈⟨b, b̃_j⟩/⟨b̃_j, b̃_j⟩⌋
        b ← b − c_j b̃_j
    end for
    return t − b
end procedure
```

## 2 The GGH Signature Scheme

Every signature scheme consists of (Key generation algorithm, Signing algorithm, Verification algorithm). In case of GGH these are:

- KGA: Choose a lattice with some good basis (= private key) and bad basis (= public key).
- SA: Given a message and a private key: map message to point in space and use CVP to find nearest lattice point (= signature).
- VA: Given message, signature and public key, verify that signature is lattice point and is close to the message.

## 3 The NTRUSign Signature Scheme

Is essentially same as GGH Signature scheme for lattice of dimension $2N$ for some $N$ but uses clever techiques to cut down storage and computational costs. All operations are done in ring of convolution polynomials $R = \mathbb{Z}[x]/(x^N - 1)$.

*Note*: This means that product of polynomials is simply their convolution.

**Definition 1.** Convolution $*$ of two polynomials $f$ and $g$ is defined by taking the coefficient of $x^k$ in $f * g$ to equal

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

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

**Definition 2.** 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

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

**Lemma 3.** *Convolution modulo lattice has a rotational invariance property: If* $(u, v) \in L_h$, *then*

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

**Definition 4.** We write $R * (u, v)$ for the sublattice of $L_h$ generated by $(u, v)$, and all of its rotations.

**Definition 5.** 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 $L_h^{\mathrm{NT}}$.

**Definition 6.** Key generation for NTRUSign

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

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

(4) $f$, $g$, $G$, $H$ is private key.
(5) $h$ is public key.

**Lemma 7.** *Rotations of* $(f, g)$ *and* $(F, G)$ *form a basis of* $L_h$.

**Definition 8.** Signing with NTRUSign

(1) Hash digital document to create a random vector $(m_1, m_2)$ mod $q$.
(2) 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

$$s \equiv \quad f * B + F * b \qquad (\text{mod } q).$$

**Definition 9.** Verification of NTRUSign signature

(1) Compute $t \equiv s * h \pmod{q}$

(2) Verify that $\|s - m_1\|^2 + \|t - m_2\|$ is small.