Hybrid lattices and the NTWO cryptosystem *

Emmanuela Orsini
Dipartimento di Matematica
Università di Pisa, Italy

Primo Workshop di Crittografia "BunnyTN", March 10, 2011
Dipartimento di Matematica, Università di Trento

(*joint work with Carlo Traverso)

Outline

Lattices

A **lattice** in $\mathbb{Z}^n$ is the set of all integer linear combination of (linearly indipendent) basis vectors $(b_1, \ldots, b_n)$:

$$\mathcal{L} = \sum_{i=1}^{n} b_i \cdot \mathbb{Z} = \left\{ Bx \mid x_i \in \mathbb{Z}, b_i \in \mathbb{Z}^n \right\}.$$

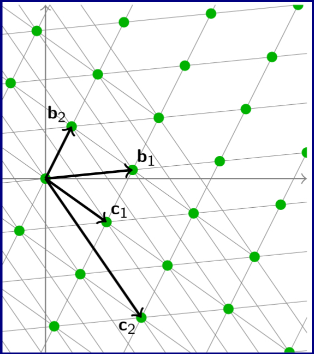
Lattices

A **lattice** in $\mathbb{Z}^n$ is the set of all integer linear combination of (linearly indipendent) basis vectors $(b_1, \ldots, b_n)$:

$$\mathcal{L} = \sum_{i=1}^{n} b_i \cdot \mathbb{Z} = \{Bx \mid x_i \in \mathbb{Z}, b_i \in \mathbb{Z}^n\}.$$

- $B = [b_1, \ldots, b_n] \in \mathbb{Z}^{n \times n}$
- The same lattice has many bases

$$\mathcal{L} = \sum_{i=1}^{n} c_i \cdot \mathbb{Z}$$



Definition (Lattice)

A discrete additive subgroup of $\mathbb{Z}^m$

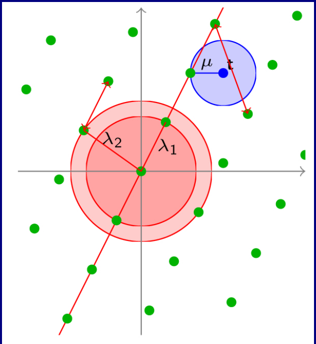
Minimum Distance

- **Minimum distance:**

$$\lambda_1 = min_{x,y \in \mathcal{L}, x \neq y} \|x - y\|$$
$$min_{x \in \mathcal{L}, x \neq 0} \|x\|$$

- **Distance function:**

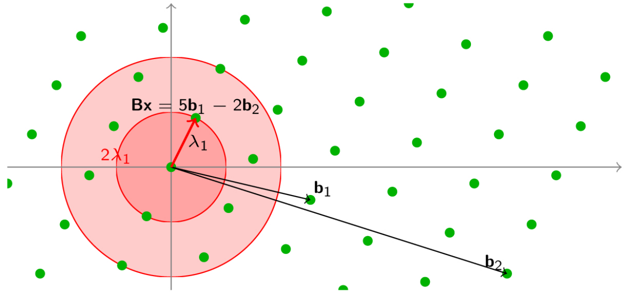
$$\mu(t, \mathcal{L}) = min_{x \in \mathcal{L}} \|t - x\|$$



Lattice problems: SVP

Definition (SVP, Shortest Vector Problem)

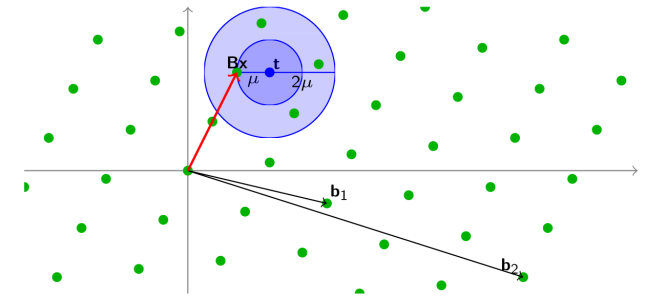
Given a basis $B \in \mathbb{Z}^{n \times n}$ of $\mathcal{L}$, find a nonzero lattice vector Bx (with $x \in \mathbb{Z}^n / \{0\}$) of length at most $\|Bx\| \leq \lambda_1$.



Lattice problems: CVP

Definition (CVP, Closest Vector Problem)

Given a basis $B \in \mathbb{Z}^{n \times n}$ and a target vector $t \in \mathbb{Z}^n$, find a lattice vector Bx closest to the target t, i.e., find an integer vector $x \in \mathbb{Z}^n$ such that $\|Bx - t\| \leq \mu$.



Lattice problems: SVP and CVP

We consider the following problem (equivalent CVP):

SMALLEST RESIDUE PROBLEM (SRP)

`Input`: $L \subseteq \mathbb{Z}^n$, $v \in \mathbb{Z}^n$
`Question`: the smallest $v' \in \mathbb{Z}^n$ s.t. $v - v' \in L$

Lattice problems: SVP and CVP

We consider the following problem (equivalent CVP):

SMALLEST RESIDUE PROBLEM (SRP)

`Input`: $L \subseteq \mathbb{Z}^n$, $v \in \mathbb{Z}^n$
`Question`: the smallest $v' \in \mathbb{Z}^n$ s.t. $v - v' \in L$

- The exact version of these problems is NP-hard.
- Reduction algorithms (LLL, BKZ)

Lattice problems: SVP and CVP

We consider the following problem (equivalent CVP):

SMALLEST RESIDUE PROBLEM (SRP)

`Input`: $L \subseteq \mathbb{Z}^n$, $v \in \mathbb{Z}^n$
`Question`: the smallest $v' \in \mathbb{Z}^n$ s.t. $v - v' \in L$

- The exact version of these problems is NP-hard.
- Reduction algorithms (LLL, BKZ)

Lattices and codes

- **Lattices** $\longrightarrow \mathbb{Z}^n$, Euclidean distance

Let $w = (w_1, \ldots, w_n) \in \mathbb{N}^n$ be *weight vector*, $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$:

$$||wa||_2 = \sqrt{\sum w_i a_i^2}.$$

Instead of l_2 one can choose a different norm l_r, $1 \leq r \leq \infty$.

- **Codes** $\longrightarrow \mathbb{K}^n$, Hamming distance

Let $x, y \in \mathbb{K}^n$, $d_H(x, y) = \#$ of coordinates on which x and y differ.

- $\mathbb{K} = \mathbb{Z}/p$: $C \subseteq (\mathbb{Z}/p)^n \longrightarrow L \subseteq \mathbb{Z}^n$; the CVP in L is equivalent to the MLD (Maximum Likelihood Decoding).
- $\mathbb{K} = \mathbb{Z}/2$ (binary codes): no substantial difference between Hamming distance and Euclidean distance;
- the situation is different when $p > 2$

Hybrid lattices

A **hybrid lattice** is a subgroup $L \subseteq \mathbb{Z}^n$ with a mixed distance.

- Reordering the variables we may assume to have a block with Euclidean distance and another block with Hamming distance.
- A hybrid lattice with only the Hamming block is called a *Hamming lattice*.
- A hybrid lattice with only the Euclidean block will be called a *standard lattice*.
- **q-ary lattices** : $q\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$, for a suitable $q \in \mathbb{N}$ (possible prime).
  - the membership of a vector $x \in \mathbb{Z}^n$ in L is determined by $x \bmod q$;
  - these lattices are in one-one correspondence with linear code in $\mathbb{Z}_q^n$.

SRP in hybrid lattices. Example

Let $q = 131$ and $I = (1, 4, 17, 53)$ **(q-interpolators)**.
$\forall m \in \mathbb{Z}_q$, we can compute the length of the smallest integer vector (a, b, c, d) **(multipliers)** such that

$$m \equiv 1a + 4b + 17c + 53d \mod q$$

This length is $\leq \sqrt{7}$ and in average is 1.89.

SRP in hybrid lattices. Example

Let $q = 131$ and $I = (1, 4, 17, 53)$ **(q-interpolators)**.
$\forall m \in \mathbb{Z}_q$, we can compute the length of the smallest integer vector (a, b, c, d) **(multipliers)** such that

$$m \equiv 1a + 4b + 17c + 53d \mod q$$

This length is $\leq \sqrt{7}$ and in average is 1.89.

$23 = 4 - 2 \cdot 17 + 53,$ $(0, 1, -2, 1)$

$41 = 1 + 4 - 17 + 53,$ $(1, 1, -1, 1)$

$43 \equiv -1 - 2 \cdot 17 - 53$ $(-1, 0, -2, -1)$

SRP in hybrid lattices. Example

Let $q = 131$ and $I = (1, 4, 17, 53)$ **(q-interpolators)**.
$\forall m \in \mathbb{Z}_q$, we can compute the length of the smallest integer vector (a, b, c, d) **(multipliers)** such that

$$m \equiv 1a + 4b + 17c + 53d \mod q$$

This length is $\leq \sqrt{7}$ and in average is 1.89.

Let $L \subseteq \mathbb{Z}^n$ be an Hamming lattice, $q\mathbb{Z}^n \subseteq L$; $L' \subseteq \mathbb{Z}^{5n}$ be the standard lattice:

$$L' = \begin{pmatrix} L & 0 & 0 & 0 & 0 \\ I & I & 0 & 0 & 0 \\ 4I & 0 & I & 0 & 0 \\ 17I & 0 & 0 & I & 0 \\ 53I & 0 & 0 & 0 & I \end{pmatrix}$$

Let $a \in \mathbb{Z}^n$ and b the shortest residue of a modulo L. Then we define $a' = [a, 0, 0, 0, 0], b' = [b, 0, 0, 0, 0] \in \mathbb{Z}^{5n}$. Let $\overline{b}$ be the SR of a'.

We have $\|\overline{b}\|_2 \leq \sqrt{7}\ \mathrm{d}_H(b', 0)$ and $b_1 + 4b_2 + 17b_3 + 53b_4$ is $\equiv a \mod L$.

NTRU (Hoffstein, Pipher, Silverman (1998))

Notation and parameters

- $A = \mathbb{Z}[x]/(x^n - 1)$
- p, q prime numbers, $p \neq q$, p very small $(2, 3)$
- Small polynomial: small coefficients (uniquely represented mod p), few monomials: small Euclidean and Hamming weight.

Private and public keys

Private key: $f, g \in A$, f invertible (mod q, p). f and g small.
Public key: $h = g/f \in A/(q)$

Encryption

$c = phr + m$, $r \in A$ random small polynomial, m small

Decryption

$fc = pgr + fm$ (mod q) (moderate), and then lifting to $\phi \in A$, then reducing mod p, $\phi \equiv fm$ (mod p), and dividing by f mod p.

The Coppersmith-Shamir (or NTRU) lattice

NTRU can be seen as a lattice cryptosystem:

- $A = \mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}^n$ as abelian group;
- In A^2, L_{CS} generated by $(q, 0)$ and $(h, 1)$ is a full-dimensional lattice

$$L_{CS} = \begin{pmatrix} qI & 0 \\ H & I \end{pmatrix} = \begin{pmatrix} q & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & q & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & q & 0 & 0 & \dots & 0 \\ h_0 & h_1 & \dots & h_{N-1} & 1 & 0 & \dots & 0 \\ h_{N-1} & h_0 & \dots & h_{N-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

The Coppersmith-Shamir (or NTRU) lattice

NTRU can be seen as a lattice cryptosystem:

- $A = \mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}^n$ as abelian group;
- In A^2, L_{CS} generated by $(q, 0)$ and $(h, 1)$ is a full-dimensional lattice

$$L_{CS} = \begin{pmatrix} qI & 0 \\ H & I \end{pmatrix} = \begin{pmatrix} q & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & q & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & q & 0 & 0 & \dots & 0 \\ h_0 & h_1 & \dots & h_{N-1} & 1 & 0 & \dots & 0 \\ h_{N-1} & h_0 & \dots & h_{N-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

▷ **Key attacks:** $(g, f) \in L_{CS}$ and it is with high probability the SV

▷ **Message attack:** $[m, pr]$ is presumably the shortest residue of $[c, 0]$.

NTWO: Notation

M. Caboara, F. Caruso, C. Traverso. *Gröbner Bases in Public Key Cryptography.*, Proc. ISSAC '08, ACM (2008), pp. 315–323.

NTWO: Notation

M. Caboara, F. Caruso, C. Traverso. *Gröbner Bases in Public Key Cryptography.*, Proc. ISSAC '08, ACM (2008), pp. 315–323.

- $A = \mathbb{Z}[X]/(X^N - 1) = \mathbb{Z}[x_1, \ldots, x_k]/(x_1^{n_1} - 1, \ldots, x_k^{n_k} - 1)$ (multivariate polynomial algebra)
- p, q prime numbers such that $p = 2, 3$ and $q \neq p$
- $n_i \mid (q - 1)$, for each n_i

$k = 2$ and $n_1 = n_2 = n$, so that $A = \mathbb{Z}[x, y]/(x^n - 1, y^n - 1)$

NTWO: Key preparation

- $A = \mathbb{Z}[x, y]/(x^n - 1, y^n - 1)$

- $\mathcal{Q} = \{(\omega^i, \omega^j) \mid \omega$ is a primitive n-th root of $1\}$
  $= \{$ roots of $(x^n - 1, y^n - 1)\}$
- $E \subset \mathcal{Q}$ small; $\alpha \in A/q$ a polynomial having support E
- $f, g \in A$ small polynomials:
  - f invertible $\pmod p$ (f_p^{-1}) and $\pmod \alpha$ $(f' \in A/q$ s.t. $ff' \equiv 1 \pmod \alpha)$
  - g invertible $\pmod \alpha$

NTWO: Key preparation

- $A = \mathbb{Z}[x, y]/(x^n - 1, y^n - 1)$

- $\mathcal{Q} = \{(\omega^i, \omega^j) \mid \omega$ is a primitive n-th root of $1\}$
  $= \{$ roots of $(x^n - 1, y^n - 1)\}$
- $E \subset \mathcal{Q}$ small; $\alpha \in A/q$ a polynomial having support E
- $f, g \in A$ small polynomials:
  - f invertible $\pmod{p}$ (f_p^{-1}) and $\pmod{\alpha}$ $(f' \in A/q$ s.t. $ff' \equiv 1 \pmod{\alpha})$
  - g invertible $\pmod{\alpha}$

Public key

$h = gf' + \alpha \in A/q.$

Private key

$f, g, J = (\alpha, q) \subseteq A$; J is the **private ideal**

NTWO: encryption and decryption

Encryption

$c = phr + m$, $r \in A$ random small polynomial, m small

Decryption

$$fc = phr + fm \Rightarrow fc = pgr + fm + \beta$$

where $\beta \in J$ is unknown to the receiver.
We can conjecture that β is the closest vector to fc.
So if we have a "good" basis of J we can correctly identify β.
We have $pgr + fm$ and we can continue like in NTRU. If $pgr + fm$ is a moderate polynomial ϕ in A, then we reduce ϕ modulo p and then we multiply by f_p^{-1}.

- The case $k = 1$ and $J = (q)$ is just the NTRU cryptosystem.

The Lagrange basis

For each point (a, b) of $\mathcal{Q}$ define a Lagrange interpolator

$$\lambda_{a,b} = \frac{ab(x^n - 1)(y^n - 1)}{n^2(x - a)(y - b)}$$

being a polynomial vanishing everywhere in $\mathcal{Q}$ except (a, b), where its value is 1. The $\lambda_{a,b}$ are a basis of A/q (the **Lagrange basis**).

J (as a vector subspace of A/q) has a basis composed of the $\lambda_{a,b}$ such that $(a, b) \in E$. As ideal, it is generated by $\sum_{(a,b)\in E} \lambda_{a,b}$, or by any other polynomial not vanishing in E (every ideal is generated by polynomials having the same support of the ideal).

The Lagrange-Coppersmith-Shamir lattice

NTWO can be seen as a lattice cryptosystem:

- $A = \mathbb{Z}[x, y]/(x^n - 1)(y^n - 1) \cong \mathbb{Z}^{n^2}$ as abelian group;
- In A^3, L_{LCS} generated by $(q, 0, 0)$, $(h, 1, 0)$ and $(1, 0, 1)$ is a full-dimensional lattice

$$L_{LCS} = \begin{pmatrix} qI & 0 & 0 \\ H & I & 0 \\ L & 0 & I \end{pmatrix}$$

The Lagrange-Coppersmith-Shamir lattice

NTWO can be seen as a lattice cryptosystem:

- $A = \mathbb{Z}[x, y]/(x^n - 1)(y^n - 1) \cong \mathbb{Z}^{n^2}$ as abelian group;
- In A^3, L_{LCS} generated by $(q, 0, 0)$, $(h, 1, 0)$ and $(1, 0, 1)$ is a full-dimensional lattice

$$L_{LCS} = \begin{pmatrix} qI & 0 & 0 \\ H & I & 0 \\ L & 0 & I \end{pmatrix}$$

The Lagrange-Coppersmith-Shamir lattice

NTWO can be seen as a lattice cryptosystem:

- $A = \mathbb{Z}[x, y]/(x^n - 1)(y^n - 1) \cong \mathbb{Z}^{n^2}$ as abelian group;
- In A^3, L_{LCS} generated by $(q, 0, 0)$, $(h, 1, 0)$ and $(1, 0, 1)$ is a full-dimensional lattice

$$L_{LCS} = \begin{pmatrix} qI & 0 & 0 \\ H & I & 0 \\ L & 0 & I \end{pmatrix}$$

▷ **Key attacks:** $(g, f, \alpha) \in L_{LCS}$

▷ (g, f, α) is with high probability the SV (Euclidean + Hamming)

Expanded NTWO lattice

Find a small set of interpolators $(c_1, \ldots, c_m)$ of elements of $\mathbb{Z}/q$, such that every $a \in \mathbb{Z}/q$ can be represented as $\sum a_i c_i$, with $(a_1, \ldots, a_m)$ of small Euclidean norm.

$$\begin{pmatrix} qI & 0 & 0 & 0 & \ldots & 0 \\ H & I & 0 & 0 & \ldots & 0 \\ c_1 L & 0 & I & 0 & \ldots & 0 \\ c_2 L & 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_m L & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

- We can map the expanded lattice to the LCS lattice:

$$(x, y, a_1, \ldots, a_m) \longmapsto (x, y, \sum a_i c_i)$$

- Elements of small Hamming weight are represented by elements of (slightly larger) Euclidean weight.
- Attack to the NTWO key, but the increase in dimension makes the problem much harder.

Expanded NTWO lattice

Find a small set of interpolators $(c_1, \ldots, c_m)$ of elements of $\mathbb{Z}/q$, such that every $a \in \mathbb{Z}/q$ can be represented as $\sum a_i c_i$, with $(a_1, \ldots, a_m)$ of small Euclidean norm.

$$\begin{pmatrix} qI & 0 & 0 & 0 & \ldots & 0 \\ H & I & 0 & 0 & \ldots & 0 \\ c_1 L & 0 & I & 0 & \ldots & 0 \\ c_2 L & 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_m L & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

- We can map the expanded lattice to the LCS lattice:

$$(x, y, a_1, \ldots, a_m) \longmapsto (x, y, \sum a_i c_i)$$

- Elements of small Hamming weight are represented by elements of (slightly larger) Euclidean weight.
- Attack to the NTWO key, but the increase in dimension makes the problem much harder.

Expanded NTWO lattice

Find a small set of interpolators $(c_1, \ldots, c_m)$ of elements of $\mathbb{Z}/q$, such that every $a \in \mathbb{Z}/q$ can be represented as $\sum a_i c_i$, with $(a_1, \ldots, a_m)$ of small Euclidean norm.

$$\begin{pmatrix} qI & 0 & 0 & 0 & \ldots & 0 \\ H & I & 0 & 0 & \ldots & 0 \\ c_1 L & 0 & I & 0 & \ldots & 0 \\ c_2 L & 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_m L & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

- We can map the expanded lattice to the LCS lattice:

$$(x, y, a_1, \ldots, a_m) \longmapsto (x, y, \sum a_i c_i)$$

- Elements of small Hamming weight are represented by elements of (slightly larger) Euclidean weight.
- Attack to the NTWO key, but the increase in dimension makes the problem much harder.

Parameters for n, p, q

We experimented mainly $p = 2$, and

$$
\begin{array}{ll}
n = 7 & q = 29, 43 \\
n = 9 & q = 19, 37, 73 \\
n = 11 & q = 67, 89 \\
n = 13 & q = 53, 79, 131, 157 \\
n = 17 & q = 103, 137, 239 \\
n = 19 & q = 191, 229 \\
n = 23 & q = 47, 139, 277, 461 \\
n = 29 & q = 59, 233, 349, 523
\end{array}
$$

$n = 3, 5$ have been used for toy examples.
Cracking a key is easy up to $n = 7$, it can be done sometimes with $n = 9$, it has been impossible with 3 days of computation for $n = 11$. No message has ever been cracked with $n = 13$ or more.

Conclusions and further work

- We have shown that CVP in hybrid lattices can be useful as a hardcore problem for the construction of cryptosystems.

  NTWO has a much more involved decryption, but it seems to allow considerably shorter keys (f, g) and slightly larger r and m, making the attacks to the messages more difficult.

- Prepare an efficient production implementation.
  Extensive tests with different q, p and n (and smallnes bounds).
- Discover what properties (of the private ideal especially) produce keys that
  - make decoding easy and reliable;
  - make breaking messages harder
- Study alternatives to hybrid lattice reduction

Conclusions and further work

- We have shown that CVP in hybrid lattices can be useful as a hardcore problem for the construction of cryptosystems.

  NTWO has a much more involved decryption, but it seems to allow considerably shorter keys (f, g) and slightly larger r and m, making the attacks to the messages more difficult.

- Prepare an efficient production implementation.
  Extensive tests with different q, p and n (and smallnes bounds).
- Discover what properties (of the private ideal especially) produce keys that
  - make decoding easy and reliable;
  - make breaking messages harder
- Study alternatives to hybrid lattice reduction

Conclusions and further work

- We have shown that CVP in hybrid lattices can be useful as a hardcore problem for the construction of cryptosystems.

  NTWO has a much more involved decryption, but it seems to allow considerably shorter keys (f, g) and slightly larger r and m, making the attacks to the messages more difficult.

- Prepare an efficient production implementation.
  Extensive tests with different q, p and n (and smallnes bounds).
- Discover what properties (of the private ideal especially) produce keys that
  - make decoding easy and reliable;
  - make breaking messages harder
- Study alternatives to hybrid lattice reduction