Lattice cryptography

October 08, 2018

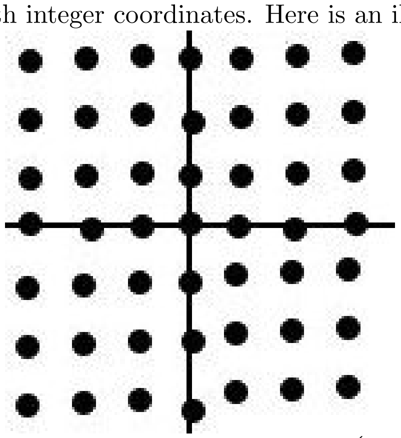
Definition: Post-Quantum Cryptography – classically computed protocols secure against quantum adversaries.

1 Lattices

A lattice is a grid of dots, not necessarily aligned with the coordinate axes. It is always > 2 dimensions. (usually n-dimensional where $n \approx 100$)

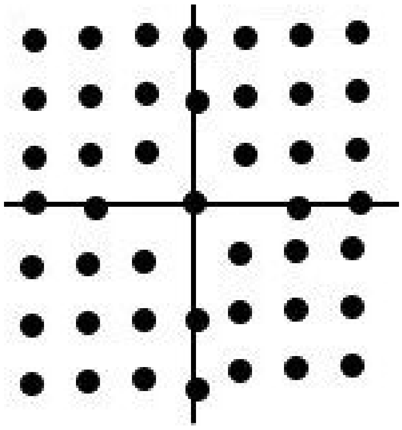
Formally, a lattice falls under either of two definitions:
(1) Any discrete subgroup of $\mathbb{R}^n$
(2) Let $B = \{b1, ..., b_k\}$ be a linearly independent subset of $\mathbb{R}^n$. The lattice is the set $L(B) = \left\{ \sum_{i=1}^{k} x_i b_i | x_i \in \mathbb{Z} \right\}$

For example, the lattice $L(B)$ where $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Is the grid of all points with integer coordinates. Here is an illustration:



The lattice $L(B)$ where $B = \begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix}$, is the same lattice as before.

The lattice $L(B)$ where $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, is the same lattice as before, except the points $(1, 0), (0, 1), (-1, 0), (0, -1)$ are not in the lattice, as in the illustration below.



The set $B = \begin{pmatrix} 1 & \sqrt{2} \end{pmatrix}$ does not form a lattice, since the elements are not linearly independent.

Thought not formally required, usually a full rank lattice is used.

2 Hardness assumptions

Cryptography relies on hardness assumptions. For lattices, these are:

(1) Shortest Vector Problem (SVP): Given $B \in \mathbb{Z}^{n \times n}$ find $v \in L(B)$
$\{0\}$ s.t. $|v|$ is minimized.

(2) Closest vector problem (CVP): Given $B \in \mathbb{Z}^{n \times n}, u \in \mathbb{Z}^n$ find $v \in L(B)$
$\{0\}$ s.t. $|v - u|$ is minimized.

These problems are easy in dimension 2 but harder in higher dimensions.

3 Approximation

Unfortunately, these problems are NP hard in the exact case. Instead, we use approximate variations of the problems, SVP_γ and CVP_γ, which are correct to within a gamma factor of optimal.

4 Decisional variants

We also define decision SVP and CVP problems. The decisional variant of SVP is called gap-SVP_γ, outputs "yes" if, given (B, S), the shortest vector is of length at most s, and outputs "no" if, given (B, S), the shortest vector is of length at most γs. The behavior for shortest vectors between lengths s and γs is undefined. gap-CVP_γ is defined similarly.

5 Complexity landscape

The complexity landscape of SVP_γ is as follows:

1. $1 < \gamma < 2^{(\log n)^{1-\epsilon}}$: NP-hard
2. $\sqrt{n} < \gamma < n$: NP $\cap$: Co-NP

3. $n < \gamma < 2^{n^{\frac{\log \log n}{\log n}}}$: Acceptable for cryptography
4. $\gamma > 2^{n^{\frac{\log \log n}{\log n}}}$: Easy

6 Trapdoors

Observe: not all bases are created equal. This lets us create trapdoor functions.

For example, we can use Lattice Rounding to solve CVP_γ.

Suppose all entries are bounded by δ. Then we can solve $v = B\lceil B^{-1}u \rfloor$, and $|v - u| = \left|B\left(\lceil B^{-1}u\rfloor - (B^{-1}u)\right)\right| \leq n^{\frac{3}{2}}\delta$

7 Encryption

Scheme for encryption:
Secret Key: A "good" basis B
Public Key: A "bad" basis B' s.t. $L(B) = L(B')$
$Enc(pk, m)$: Map m onto $L(B')$, add some small error to get ciphertext c
$Decr(sk, m)$: Solve CVP_γ to find m.

8 Signatures

In general, signatures have 2 functions:
Sign(sk,m) $\rightarrow \sigma$
Ver(pk,m,σ) $\rightarrow$ "Yes", if σ corresponds to m. "No" otherwise.
It also must hold that given just (pk,m), it is hard to find σ.

For lattices, our scheme is:
Secret Key: A "good" basis B
Public Key: A "bad" basis B' s.t. $L(B) = L(B')$
Sign(sk,m): Map $m \rightarrow \mathbb{R}^n$, then use CVP_γ to find the closest vector on the lattice, σ.
Ver(pk,m,σ): Test that $|m - \sigma|$ is sufficiently small and that σ is in $L(B')$

9 Short integer solutions

Special lattices that make cryptography easier.

A short integer solution lattice $SIS_{n,m,q,b}$ is defined s.t. $m >> n, b \approx \sqrt{m}$. Choose a random $A \in \mathbb{Z}_{||}{}^{n \times m}$. Then it is hard to find $x \in Z^m$ s.t. $|x| < b, x \neq 0, A \cdot x = 0 \mod q$.

It turns out this is a special case of SVP$_\gamma$, with the lattice $\Lambda(A) = \{x \in \mathbb{Z}_m | A \cdot x = 0 \mod q\}$. In particular, the hardness of the worst case of SVP implies the hardness of the average case of SIS.

10 Collision-resistant hashing

Using SIS, we can construct collision resistant hashing.

Let D be the short integer vectors in $\mathbb{Z}^m$. Then let $h_A : D \rightarrow \mathbb{Z}_q^n$ be a hash function such that $h_A(x) = A \cdot x \mod q$. To show collision resistance, assume we find a collision x_0, x_1 i.e. $A \cdot x_0 \mod q = A \cdot x_1 \mod q$. Then we find a short vector $(x_0 - x_1) \neq 0$ s.t. $A \cdot (x_0 - x_1) = 0 \mod q$, violating the SIS hardness assumption.