

Cryptosystems based on hard lattice problems

Let $\{v_1, \dots, v_n\} \subseteq \mathbb{R}^n$ be a set of linearly independent vectors. The *lattice* L generated by these vectors is $L = \{a_1v_1 + \dots + a_nv_n : a_i \in \mathbb{Z}\}$. A *basis* for L is any set of independent vectors that generate L ; any two such sets have the same number of elements, which we call the *dimension*.

1. Show that if $V = \{v_1, \dots, v_n\}$ and $W = \{w_1, \dots, w_n\}$ are two bases for a lattice L , and M_V and M_W are the related matrices (i.e., matrices whose columns are v_i 's and w_j 's respectively), then there exists a matrix A over \mathbb{Z} with determinant ± 1 such that $M_W = AM_V$.

Let L be a lattice of dimension n and let $V = \{v_1, \dots, v_n\}$ be a basis for L . The *fundamental domain* for L wrt to V is $\mathcal{F}(v_1, \dots, v_n) = \{t_1v_1 + \dots + t_nv_n : 0 \leq t_i < 1\}$.

2. Every $w \in \mathbb{R}^n$ can be written as $w = t + v$ where t is a *unique* vector in \mathcal{F} and v is a *unique* vector in L .

The volume of \mathcal{F} is called the *determinant* of L , and denoted $\det(L)$. Assuming $L \subseteq \mathbb{R}^n$ and L itself is of dimension n , then $\det(L) = |\det(M_V)|$, i.e., the usual determinant of the matrix whose columns (alternatively, rows) are the vectors of V .

3. Explain that $\det(L)$ is well defined, i.e., independent of the particular basis.

Define the the following indicator $H(V) = \left(\frac{\det(L)}{\|v_1\| \dots \|v_n\|} \right)^{\frac{1}{n}}$, where $V = \{v_1, \dots, v_n\}$ and $\|v\|$ is the usual Euclidean norm in \mathbb{R}^n .

The closest vector problem (CVP) is defined as follows: given $w \in \mathbb{R}^m$ that is not in L , find a vector $v \in L$ that is closest to w , i.e., find a vector $v \in L$ such that $\|w - v\|$ is minimized.

Consider the following algorithm that attempts to solve CVP: write $w = t_1v_1 + \dots + t_nv_n$ with $t_i \in \mathbb{R}$. Let $a_i = \lfloor t_i \rfloor$, i.e., a_i is t_i rounded. Let $v = a_1v_1 + \dots + a_nv_n$.

4. Use this algorithm to solve CVP on the following two inputs:

(i) $V = \{v_1 = (137, 312), v_2 = (215, -187)\}$ and $w = (53172, 81743)$, and (ii) same w but $V' = \{v'_1 = (1975, 438), v'_2 = (7548, 1627)\}$.

5. Compare the quality of the two solutions; discuss the difference in quality in terms of $H(V)$ and $H(V')$. Conjecture the “meaning” of the indicator H . Discuss “good” and “bad” bases for L , and how to use H to tell them apart.

Lattice based cryptosystem: Alice chooses a good basis V and an integer matrix U with $\det(U) = \pm 1$. Then Alice computes a bad basis $W = UV$. Alice publishes W . Now Bob

wants to send $m = (m_1, \dots, m_n)$; Bob chooses a random r , and computes $e = m_1 w_1 + \dots + m_n w_n + r$ and sends e to Alice. Alice uses our algorithm above to compute $v \in L$ closest to e , and then computes vW^{-1} to get back m .

6. Discuss how this lattice based cryptosystem is related to CVP. Conjecture a good dimension for which the system appears hard (but not too big so that encryption/decryption are still feasible).

7. Suppose that Bob sends the same message m twice, using different random perturbations r and r' . Explain what sort of information Eve can deduce from the ciphertexts $e = mW + r$ and $e' = mW + r'$.

8. For example, suppose that $n = 5$ and that random perturbations are chosen with coordinates in the set $\{-2, -1, 0, 1, 2\}$. This means that there are 5^5 possibilities for r . Suppose further that Eve intercepts two ciphertexts

$$e = (-9, -29, -48, 18, 48) \quad e' = (-6, -26, -51, 20, 47)$$

having the same plaintext. With this information, how many possibilities are there for r ?

9. Suppose that Bob is lazy and uses the same perturbation to send two different messages. Explain what sort of information Eve can deduce from the ciphertexts $e = mW + r$ and $e' = m'W + r$.