Assignment 2

Due: Tuesday, February 13, 2024 11:30 pm (Eastern Standard Time)

Time left Hide

13 days, 3 hours

Submit your assignment

Help

After you have completed the assignment, please save, scan, or take photos of your work and upload your files to the questions below. Crowdmark accepts PDF, JPG, and PNG file formats.

Q1 (10 points)

Show that for a lattice L with basis B, if B^* is the Gram-Schmidt orthogonalized basis from B, then $\lambda_1(L) \geq \min_i\{\|b_i^*\|\}$.

Q2 (10 points)

The problem of γ-CVP asks: given a lattice basis B and a vector t in the real span of B, find $v \in \mathcal{L}(B)$ such that

$$\|v - t\| \leq \gamma \min\{\|t - w\| : w \in \mathcal{L}(B)\} \tag{1}$$

a) (5 points) Suppose $v \in \mathcal{L}(B)$ is a shortest vector in $\mathcal{L}(B)$, with $v = \sum_{i=1}^{n} a_i b_i$. Fix some index i, and let B' be formed by setting $b'_j = b_j$ for all $j \neq i$, and $b'_i = 2b_i$. Show that if a_i is odd, then if we solve γ-CVP for $\mathcal{L}(B')$ given input vector b_i, we can efficiently obtain a vector $w \in \mathcal{L}(B)$ such that $\|w\| \leq \gamma\lambda_1(\mathcal{L}(B))$.

b) (5 points) Reduce γ-SVP to γ-CVP (that is: given a program to solve γ-CVP, use it to solve γ-SVP).

Q3 (10 points)

Give an algorithm to multiply two degree-one polynomials $a_1 + a_2 X$ and $b_1 + b_2 X$ in $\mathbb{Z}_q[X]/p(X)$ for $p(X) = X^2 - \zeta$ (for some ζ), which uses only four multiplications modulo q (hint: use Karatsuba!).

Q4 (6 points)

Given a polynomial $r(X) \in R_q = \mathbb{Z}_q[X]/p(X)$, with $r(X) = r_0 + r_1 X + \cdots + r_{d-1} X^{d-1}$, we can evaluate r on any element $\omega \in \mathbb{Z}_q$ by computing

$$r(\omega) := r_0 + r_1 \omega + r_2 \omega^2 + \cdots + r_{d-1} \omega^{d-1} \tag{2}$$

a) (3 points) Show that in a ring LWE-scheme where the public key is $(a(x), b(x) = a(x)s(x) + e(x))$ in R_q, we have that $b(\omega) \equiv a(\omega)s(\omega) + e(\omega) \mod q$ if ω is a root of $p(x)$.

b)(3 points) Does the same equality hold if ω is not a root of $p(x)$, and why or why not?

Q5 (10 points)

Let $R_q = \mathbb{Z}_q[X]/(X^{256} + 1)$. Suppose we use $q = 7681 = 2^9 \cdot 15 + 1$, so that there is an element $\zeta \in \mathbb{Z}_q$ such that

$$X^{256} + 1 = \prod_{i=0}^{255} (X - \zeta^{2i+1}) \mod q. \tag{3}$$

That is, $X^{256} + 1$ splits completely.

Show that a uniformly randomly selected $a(x) \in R_q$ is invertible with probability

$$\left(1 - \frac{1}{q}\right)^{256}. \tag{4}$$

Hint: use Sun's theorem (the Chinese Remainder Theorem).

Q6 (10 points)

Let q and be a prime, and let $\varphi(n)$ be the Euler-Phi function. In this question we prove a restricted case of Sun's Theorem, more or less (aka the Chinese Remainder Theorem).

a) (8 points) Let $f(x) \in \mathbb{Z}_q[x]$ be a polynomial of degree $\varphi(n) - 1$. Show that the list $\hat{f} := (f(\zeta_1), f(\zeta_2), \ldots, f(\zeta_{\varphi(n)}))$, where ζ_i are all distinct elements of $\mathbb{Z}_q$ of order n, is a unique representation of f.

b) (2 points) Show that $\widehat{f(x)g(x)}$ is the same as $\hat{f} \star \hat{g}$, where $\star$ is the component-wise product.