Problem sheet 8 for Course 02231, 2025

These practice problems have the purpose of helping you understand the material better and learning the skills that are necessary to analyze cryptographic constructions, and sometimes to prepare you for the next class. All answers should be supported by a written justification. To gauge whether a justification is sufficient, ask yourself if your peers would be convinced by it without additional explanations.

We denote vectors as $\vec{x} \in \{0,1\}^\lambda$. By $\vec{x}[i]$ we denote the ith index of $\vec{x}$, where $i \in \{1,\ldots,\lambda\}$. As in the lecture, we write $k \leftarrow K$ if k is sampled from the set K such that it can be each element from K with equal probability $1/|K|$. For two strings x, y we use $x|y$ to denote the string obtained from concatenating x with y. Throughout this problem sheet, let p be a prime.

Recall the definition of the discrete Gaussian probability distribution

$$q_\sigma(z) = \frac{d_\sigma(z)}{\nu_\sigma},$$

where

$$d_\sigma(z) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{z^2}{2\sigma^2}}$$

is the probability density of the normal distribution $\mathcal{N}(0,\sigma^2)$ with mean 0 and variance σ^1, and

$$\nu_\sigma = \sum_{z\in\mathbb{Z}} d_\sigma(z).$$

Some helpful facts about the discrete Gaussian distribution:

1. $\nu_\sigma \geq 1 - d_\sigma(0)$
2. For a random variable $X \sim q_\sigma$ the following tail bound holds. For any integer $x > 1$,

$$\Pr[X \geq x] \leq \frac{\sigma}{\nu \cdot (x-1) \cdot \sqrt{2\pi}} e^{-\frac{(x-1)^2}{2\sigma^2}}.$$

For convenience, we quickly recap the Regev public-key encryption scheme:

Keygen()**:**

1. Sample $\mathbf{A} \leftarrow \mathbb{Z}_p^{\ell\times n}$ and $\mathbf{s} \leftarrow \mathbb{Z}_p^n$ uniformly at random.
2. Let $\mathbf{e} \in \mathbb{Z}_p^\ell$ where each e_i is distributed according to q_σ.
3. Set $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod p$.
4. Output $pk = (\mathbf{A}, \mathbf{b})$ as public key and $sk = (\mathbf{s})$ as private key.

Enc(pk, m)**:** To encrypt the message $m \in \{0,1\}$ using public key $pk = (\mathbf{A}, \mathbf{b})$:

1. Let $\mathbf{r} \in \{0,1\}^\ell$ be uniformly random.
2. Set $\mathbf{c}_0 \leftarrow \mathbf{r}^\top \mathbf{A} \bmod p$ and $c_1 = \mathbf{r}^\top \mathbf{b} + m \cdot \frac{p-1}{2}$

3. Output $c = (\mathbf{c}_0, c_1)$.

Dec(sk, c)**:** To decrypt a ciphertext $c = (\mathbf{c}_0, c_1)$ using private key $sk = (\mathbf{s})$:

1. Compute $m' = \lfloor \frac{2(c_1 - \mathbf{c}_0^\top \mathbf{s}) \bmod p}{p} \rceil$
2. Output m'.

Exercise 1. (**Decryption failure probability**)

In this exercise, we derive a bound on the probability that the encryption algorithm of Regev's encryption scheme, on input a message m produces a ciphertext c such that the decryption algorithm decrypts c to a different message m'. Assume that $\sigma \leq \frac{\epsilon p}{\ell}$ for some small $\epsilon > 0$.

1. Derive a lower bound for the probability

$$\Pr\left[e_i \leq \frac{p}{4\ell} \forall i = 1, \ldots, \ell\right]$$

using the facts given above and a union bound.

2. What does this lower bound mean for the probability of decryption failure, i.e. for the probability that encrypting a message m and decrypting it again returns $m' \neq m$?

Note: Our analysis is quite loose here, it suffices to pick $\sigma = \frac{\epsilon q}{\sqrt{\ell}}$, but it is slightly harder to show that.

Exercise 2. (**Broken variants of Regev's encryption scheme**)

In this exercise, you will find attacks against insecure modifications of Regev's encryption scheme. For each attack, give a detailed argument why it works.

1. Describe how to break Regev's encryption scheme for $\sigma = 0$, i.e. in the case where it always holds that $e_i = 0$ for all i. More precisely, describe an algorithm that given a public key pk and a ciphertext $c = \mathsf{Enc}_{pk}(m)$, recovers the plaintext m.
2. Describe how to break Regev's encryption scheme where instead of picking the r_i at random, $r_i = 1$ for all i.
3. Let σ be chosen such that $\Pr_{x \leftarrow q_\sigma}[x \neq 0 \bmod p] = \frac{1}{2\ell}$. Describe how to break Regev's encryption scheme in that case.

Exercise 3. (Towards homomorphic encryption from LWE)

Consider the following symmetric-key encryption scheme for messages $m \in \{0, 1, ..., \ell - 1\}$.

- Key generation: choose uniform $\mathbf{s} \in \mathbb{Z}_p^n$.
- Encryption of message $m \in \{0, 1, \dots \ell - 1\}$: Choose uniform $c_0 = \mathbf{a} \in \mathbb{Z}_p^n$ and $e \leftarrow q_\sigma$. Output (c_0, c_1) with $c_1 = \mathbf{a}^\top \cdot \mathbf{s} + e + \left\lfloor \frac{m(p-1)}{\ell} \right\rceil$.

1. Describe a decryption algorithm that gets as input a secret key $\mathbf{s}$ and a ciphertext $c = (c_0, c_1)$ and outputs a plaintext, and show that your decryption algorithm is correct if σ is small enough.
2. Let $c = (c_0, c_1)$ and $c' = (c'_0, c'_1)$ be ciphertexts obtained by encrypting messages m and m'. consider $c'' = (c''_0, c''_1)$ given by $c''_i = c_i + c'_i$ for $i = 0, 1$. Apply the decryption algorithm you described in 1) to c''. Under which condition do you get $m + m' \bmod \ell$?