Problem sheet 11 for Course 01410, 2023

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.

Recall Regev's encryption scheme (all arithmetic is modulo q except when specified otherwise):

- Secret key: $sk = \mathbf{s} \in \mathbb{Z}_q^n$
- Public key: pick $\mathbf{a}_i \in \mathbb{Z}_q^n$ independently uniformly at random and $e_i \leftarrow D_{\mathbb{Z}^1,\sigma}$, for $i = 1, ..., m$, and set $b_i = \mathbf{a}_i \cdot \mathbf{s} + e_i$ ($\mathbf{x} \cdot \mathbf{y}$ for vectors $\mathbf{x}$ and $\mathbf{y}$ denotes the inner product). The public key is $pk = (\mathbf{a}_i, b_i)_{i=1}^m$.
- Encryption Enc: To encrypt message $\mathsf{m} \in \{0, 1\}$, sample random bits $\iota_i \in \{0, 1\}$ for $i = 1, ..., m$ and set

  $$\mathbf{c}_0 = \sum_{i=1}^m \iota_i \mathbf{a}_i, \qquad c_1 = \frac{m(q-1)}{2} + \sum_{i=1}^m \iota_i b_i.$$

  The ciphertext is $c = (\mathbf{c}_0, c_1)$.
- Decryption Dec: To decrypt a ciphertext $c = (\mathbf{c}_0, c_1)$ using secret key $sk = \mathbf{s}$, compute $\mathsf{m}' = \left\lceil \frac{2(c_1 - \mathbf{s} \cdot \mathbf{c}_0)}{q} \right\rfloor$ (This computation is done regarding all involved numbers as reals).

Exercise 11.1 In lattice-based cryptography, rounded Gaussian distributions play an important role. The rounded version of a Gaussian random variable X with mean 0 and variance σ^2 is defined as $Y = \lceil X \rfloor$, where $\lceil \cdot \rfloor$ denotes the standard rounding operation. We denote the probability distribution of Y by $D_{\mathbb{Z}^1,\sigma}$, as in the book.

For the Gaussian random variable X the following tail bound holds. For any $x \in \mathbb{R}$ with $x > 0$,

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

Suppose that in Regev's decryption scheme, $\sigma \leq \frac{\epsilon q}{m}$ for some small $\epsilon > 0$.

1. Derive a lower bound for the probability

   $$\Pr\left[e_i \leq \frac{q}{4m} \forall i = 1, ..., m\right].$$

   Solution: We first observe that the random variables e_i are independent and identically distributed, therefore we have

   $$\Pr\left[e_i \leq \frac{q}{4m} \forall i = 1, ..., m\right] = \Pr\left[e_1 \leq \frac{q}{4m}\right]^m.$$

   we proceed by deriving a lower bound for $\Pr\left[e_1 \leq \frac{q}{4m}\right]$ by upper-bounding $\Pr\left[e_1 > \frac{q}{4m}\right]$. The random variable e_1 is a rounded Gaussian, $e_1 \sim D_{\mathbb{Z}^1,\sigma}$, so we can define a random variable X such that $e_1 = \lceil X \rfloor$. The difference between a number and its rounded version is clearly at most 1/2, so we can conclude that the implication $e_1 > \frac{q}{4m} \implies X > \frac{q}{4m} - \frac{1}{2}$. We can therefore bound

$$\Pr\left[e_1 > \frac{q}{4m}\right] \leq \Pr\left[X > \frac{q}{4m} - \frac{1}{2}\right].$$

For the case where $q \leq 4m$, we cannot use Equation (1). Otherwise, we get

$$\Pr\left[X > \frac{q}{4m} - \frac{1}{2}\right] \leq \frac{\sigma}{\left(\frac{q}{4m} - \frac{1}{2}\right) \cdot \sqrt{2\pi}} e^{-\frac{\left(\frac{q}{4m} - \frac{1}{2}\right)^2}{2\sigma^2}} = \frac{1}{\sqrt{2\pi} y} e^{-\frac{y^2}{2}}$$

where we have defined $y = \frac{\frac{q}{4m} - \frac{1}{2}}{\sigma}$. We observe that the right hand side of the above inequality is decreasing in y, i.e. $y \leq z$ implies $\frac{1}{\sqrt{2\pi} y} e^{-\frac{y^2}{2}} \geq \frac{1}{\sqrt{2\pi} z} e^{-\frac{z^2}{2}}$. We bound

$$y = \frac{\frac{q}{4m} - \frac{1}{2}}{\sigma} \geq \frac{\frac{q}{4m} - \frac{1}{2}}{\frac{\epsilon q}{m}} = \epsilon^{-1} \left(\frac{1}{4} - \frac{m}{2q}\right) =: \epsilon^{-1} \cdot C,$$

where we defined the constant $C = \left(\frac{1}{4} - \frac{m}{2q}\right) > 0$. We therefore get

$$\frac{1}{\sqrt{2\pi} y} e^{-\frac{y^2}{2}} \leq \frac{\epsilon}{\sqrt{2\pi} C} e^{-\frac{C^2}{2\epsilon^2}}.$$

Combining the inequalities we get

$$\Pr\left[e_1 > \frac{q}{4m}\right] \leq \frac{\epsilon}{\sqrt{2\pi} C} e^{-\frac{C^2}{2\epsilon^2}}$$

and thus

$$\Pr\left[e_i \leq \frac{q}{4m} \forall i = 1, ..., m\right] = \Pr\left[e_1 \leq \frac{q}{4m}\right]^m = \left(1 - \Pr\left[e_1 > \frac{q}{4m}\right]\right)^m \geq \left(1 - \frac{\epsilon}{\sqrt{2\pi} C} e^{-\frac{C^2}{2\epsilon^2}}\right)^m$$

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 $\mathsf{m}' \neq \mathsf{m}$?

   Solution: By making ϵ small enough, we can make sure that the probability $\Pr\left[e_i \leq \frac{q}{4m} \forall i = 1, ..., m\right]$ is very close to 1. But in that case, the "error" term when decrypting, $\sum_{i=1}^m \iota_i e_i$, is small enough to ensure correct decryption.

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

Exercise 11.2 In this exercise, you will find attacks against insecure modifications of Regev's encryption scheme.

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 $c = \mathsf{Enc}_{pk}(\mathsf{m})$, recovers the plaintext m.

   Solution: If there is no error we can do the following. We have the public key $pk = (\mathbf{a}_i, b_i)_{i=1}^m$, so we can solve the linear system given by the equations $\mathbf{a}_i \cdot \mathbf{s} = b_i$ for $i = 1, ..., m$ using Gaussian elimination. We can then use the computed private key $\mathbf{s}$ to decrypt.

2. Describe how to break Regev's encryption scheme where instead of picking the ι_i at random, $\iota_i = 1$ for all i.

   Solution: This was in some sense a trick question! We don't need to use any specifics about Regev's scheme here. We can just observe that Regev's scheme for $\sigma = 0$ is deterministic and can thus be broken by the generic CPA attack against deterministic schemes: Use the public key to encrypt 0 and 1, and then use the two resulting ciphertexts to decrypt any given ciphertext by comparing.