1 Negligible Functions

A non-negative function $\nu : \mathbb{N} \to \mathbb{R}$ is negligible if it decreases faster than the inverse of any polynomial; More precisely, for each polynomial P with coefficients in $\mathbb{R}$, there exists some $N \in \mathbb{N}$ such that $\nu(n) < 1/P(n)$ for $n > N$. Otherwise, we say that ν is non-negligible. We use $\mathsf{negl}(n)$ to denote some arbitrary negligible function and $\mathsf{poly}(n)$ for some arbitrary polynomial in n with non-negative leading coefficient.

1. (2 points) Show that ν is negligible if and only if for every fixed sufficiently large integer c, we have
$$\lim_{n\to\infty} \nu(n) \cdot n^c = 0.$$
2. (1 point) Is $\nu(n) = 1/2^{100 \log n}$ negligible or non-negligible? Give a brief justification.
3. (1 point) Is $\nu(n) = n^{-\log\log\log n}$ negligible or non-negligible? Give a brief justification.

2 Security Definitions

2.1 Alternative CPA-Security Definition for PKE

Recall in class we define the syntax, correctness and CPA-security of a PKE scheme. Consider an alternative CPA-security definition of PKE. The security experiment between adversary and challenger is described as follows:

- The challenger sets up a PKE scheme as $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and sends pk to adversary $\mathcal{A}$.
- Upon receiving pk, the adversary $\mathcal{A}$ sends a random message m to the challenger.
- The challenger flips a coin $b \in \{0, 1\}$. If $b = 0$, the challenger computes $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$. Otherwise, compute $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, r)$, where r is a random message of equal length of m. The challenger sends ct to the adversary.
- The adversary $\mathcal{A}$ outputs guess b'.

The advantage of adversary and security notion can be defined similarly. (4 points) Is the definition equivalent to the IND-CPA security? Prove your answer or construct a counter-example.

2.2 Security of Parallel Repetition of 1-bit PKE

Suppose we have a PKE scheme Π for single-bit messages. We can construct a new PKE scheme Π' for message space $\{0, 1\}^\ell$, by defining the encryption algorithm Enc' as

$$\mathsf{Enc}'(\mathsf{pk}, \vec{m}) = \mathsf{Enc}(\mathsf{pk}, m_1)||\cdots||\mathsf{Enc}(\mathsf{pk}, m_\ell),$$

where $\boldsymbol{m} = (m_1, \ldots, m_\ell) \in \{0, 1\}^\ell$ and $\ell = \mathsf{poly}(\lambda)$.

1. (3 points) Show that if Π is IND-CPA secure, so is Π'.
2. (3 points) show that the IND-CCA security of Π' does not hold even if Π is IND-CCA secure.

3 Lattices

3.1 Gram-Schmidt Orthogonalization

Recall the Gram-Schmidt orthogonalization process of vectors. Let $\mathbf{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) \in \mathbb{R}^d$ and $\tilde{\mathbf{B}}$ be the input and output of Gram-Schmidt orthogonalization process respectively. Let $\mathcal{L}(\mathbf{B})$ be the lattice generated by $\mathbf{B}$.

1. (4 points) Show that the output of Gram-Schmidt orthogonalization $(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n)$ is pairwise orthogonal.

2. (4 points) Show that the norm of the Gram-Schmidt vectors provides a bound on the minimum distance of a lattice as
$$\lambda_1(\mathcal{L}(\mathbf{B})) \geq \min_{i \in [n]} \|\tilde{\boldsymbol{b}}_i\|.$$

3.2 Leftover Hash Lemma

Recall the statement of the lemma as

Theorem 3.1. *Let $n, m, q \in \mathbb{N}$ and $\epsilon \in (0, 1)$ be parameters satisfying $m \geq n \log q + 2\log(1/\epsilon) + 1$. Let $\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}$ be a uniformly random matrix over $\mathbb{Z}_q^{m \times n}$ and $\boldsymbol{r} \leftarrow \{0,1\}^m$. Then the distribution of $(\mathbf{A}, \boldsymbol{r}^\mathsf{T}\mathbf{A})$ is ϵ-close to the uniformly distribution.*

1. (3 points) Show that for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_q^m$, such that $\boldsymbol{x} \neq \boldsymbol{y}$, we have
$$\mathbf{Pr}_{\mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}}[\boldsymbol{x}^\mathsf{T}\mathbf{A} = \vec{y}^\mathsf{T}\mathbf{A}] \leq \frac{1}{q^n}.$$

2. (4 points) For a discrete random variable X, define the collision probability of X to be the probability that two independent samples of X taking the same value. More specifically, define $\mathsf{CP}(X) := \mathbf{Pr}[X = X']$, where X' denotes an independent copy of X. Show that
$$\mathsf{CP}(\mathbf{A}, \boldsymbol{r}^\mathsf{T}\mathbf{A}) \leq \frac{1}{q^{mn}} \cdot (\frac{1}{2^m} + \frac{1}{q^n}).$$

3. (4 points) Let X be a random variable with support size N. It is known that if X has collision probability $\mathsf{CP}(X) \leq (1 + \epsilon^2)/N$, then X is ϵ-close to the uniform distribution over its support. Use this fact and (1) to prove the lemma.

3.3 CCA-security

1. (3 points) Prove that Regev's PKE scheme is not IND-CCA secure.

2. (4 points) Show that any FHE is not CCA-secure.