

Problem Set 1

*Lecturer: Daniele Micciancio***Due:** *Tue October 6, 2026*

This is a review homework, based on background knowledge from (introductory cryptography) courses which are assumed as a prerequisite. If you have any difficulty understanding or solving these problems, you may miss the necessary background, and you should consult with the instructor and/or TA.

IND-CPA security

Recall that a public key encryption scheme with message space $\mathcal{M}$ is a triple of (probabilistic polynomial time) algorithms $(\text{Gen}, \text{Enc}, \text{Dec})$ such that

$$\text{Dec}(\text{sk}, \text{Enc}(\text{pk}, m)) = m$$

for all messages $m \in \mathcal{M}$ and keys $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(\kappa)$, where $\kappa \in \mathbb{N}$ is the security parameter. The standard notion of security (under passive attacks) for a public key encryption scheme is that of *INDistinguishability under Chosen Plaintext Attack* (*IND-CPA*), which is defined as follows.

Definition 1 (IND-CPA security) *An encryption scheme $\mathbf{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ is (t, ϵ) IND-CPA secure if any (probabilistic, stateful) adversary $\mathcal{A}$ running in time at most t , has advantage $\text{Adv}(\mathcal{A}) = |\Pr\{\mathcal{D}_1(\mathcal{A}) = 1\} - \Pr\{\mathcal{D}_0(\mathcal{A}) = 1\}|$ at most ϵ in the following game $\mathcal{D}_b$ parametrized by a bit $b \in \{0, 1\}$:*

1. $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(\kappa)$ are chosen at random
2. $(m_0, m_1) \leftarrow \mathcal{A}(\text{pk})$ selects a pair of (equal length) messages $m_0, m_1 \in \{0, 1\}^\ell$
3. The adversary is given a ciphertext $c \leftarrow \text{Enc}(\text{pk}, m_b)$ and outputs a bit $b' \leftarrow \mathcal{A}(c)$. The output of the game is $\mathcal{D}_b(\mathcal{A}) = b'$.

Consider the following variant of the IND-CPA security definition, where the adversary outputs only one message m , and it is given either the encryption of m or the encryption of a random string.

Definition 2 (IND-CPA' security) *An encryption scheme $\mathbf{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ is (t, ϵ) IND-CPA' secure if any (probabilistic, stateful) adversary $\mathcal{A}'$ running in time at most t , has advantage $\text{Adv}'(\mathcal{A}') = |\Pr\{\mathcal{D}'_1(\mathcal{A}') = 1\} - \Pr\{\mathcal{D}'_0(\mathcal{A}') = 1\}|$ at most ϵ in the following game $\mathcal{D}'_b$ parametrized by a bit $b \in \{0, 1\}$:*

1. $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(\kappa)$ are chosen at random
2. $m_1 \leftarrow \mathcal{A}'(\text{pk})$ selects a message $m_1 \in \{0, 1\}^\ell$, and $m_0 \leftarrow \{0, 1\}^\ell$ is chosen uniformly at random among all messages of the same length ℓ .
3. The adversary is given a ciphertext $c \leftarrow \text{Enc}(\text{pk}, m_b)$ and outputs a bit $b' \leftarrow \mathcal{A}'(c)$. The output of the game is $\mathfrak{D}'_b(\mathcal{A}') = b'$.

Notice that IND-CPA' is different from the RND-CPA security definition presented in class: in RND-CPA security, the adversary is given either the encryption of the $c_1 \leftarrow \text{Enc}(\text{pk}, m)$ of its chosen message $m \leftarrow \mathcal{A}'(\text{pk})$, or a ciphertext $c_0 \leftarrow \{0, 1\}^m$ chosen uniformly at random from all strings of the same length $m = |c_1|$.

In this assignment, you are asked to prove that IND-CPA and IND-CPA' are equivalent security definitions.

(a) Prove that any scheme **PKE** that satisfies IND-CPA security is also IND-CPA' secure. More specifically, assume that **PKE** is (t, ϵ) IND-CPA secure for some given t and ϵ . Prove that the same scheme **PKE** is also (t', ϵ') IND-CPA' secure, for some $t' \approx t$ and $\epsilon' \approx \epsilon$ related to the original parameters. (Determining appropriate t', ϵ' is part of the assignment.)

As you should recall, this is done by showing that any adversary $\mathcal{A}'$ running in time t' and achieving advantage $\text{Adv}'(\mathcal{A}') \geq \epsilon'$ in the IND-CPA' game $\mathfrak{D}'$, can be transformed into an adversary $\mathcal{A}$ against the IND-CPA game $\mathfrak{D}$ with similar running time $t \approx t'$ and achieving advantage ϵ .

(b) Similar to part (a), but in the opposite direction. Prove that any scheme **PKE** that satisfies IND-CPA' security is also IND-CPA secure.

This time you will have to show that any adversary $\mathcal{A}$ against IND-CPA, can be transformed into a similarly effective adversary against IND-CPA'. The relation between (t, ϵ) and (t', ϵ') may be different from the previous part.