

**TD 8: Public Key Encryption**

**Exercise 1.**

Let  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  be a correct public-key encryption scheme. Let us assume moreover that  $\text{Enc}$  is deterministic.

1. Show that this scheme is not CPA-secure.

**Exercise 2.**

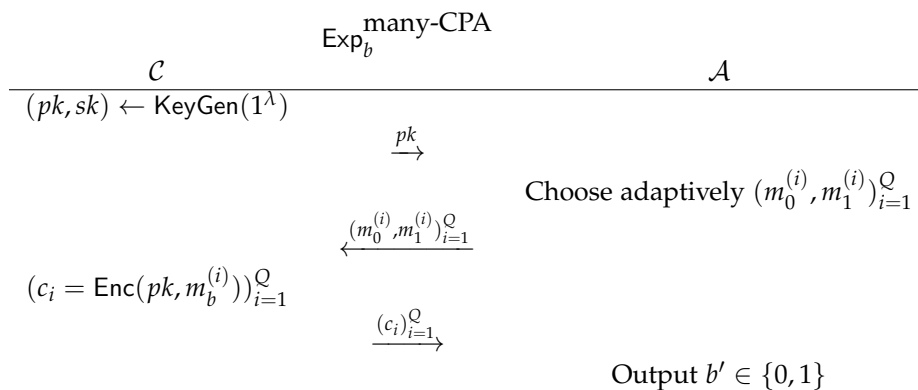
Let  $(\text{Gen}, \text{Enc}, \text{Dec})$  be a public-key encryption scheme. The One-Wayness against Chosen Plaintext Attack (OW-CPA) security notion is the following. The challenger samples  $(pk, sk) \leftarrow \text{Gen}(1^\lambda)$  and  $ct \leftarrow \text{Enc}(pk, m)$ , where  $m \leftarrow U(\mathcal{M})$  and  $\mathcal{M}$  is the message space. The adversary wins if it outputs a message  $m'$  such that  $m = m'$ .

A scheme is said OW-CPA secure if no ppt adversary wins with non-negligible probability.

1. Write a formal definition of the OW-CPA security. Can a scheme be OW-CPA secure if the message space is  $\mathcal{M} = \{0, 1\}$ ?
2. Show that if  $(\text{Gen}, \text{Enc}, \text{Dec})$  is IND-CPA secure and has exponential message space, then it is OW-CPA secure.
3. Let  $(\text{Gen}, \text{Enc}, \text{Dec})$  be an IND-CPA secure encryption scheme with message space  $\mathcal{M}$  such that it has cardinality  $|\mathcal{M}| = 2^\lambda$ , where  $\lambda$  is the security parameter. Show that a small modification of the scheme leads to an encryption scheme  $(\text{Gen}, \text{Enc}', \text{Dec}')$  that is OW-CPA secure but not IND-CPA secure anymore.

**Exercise 3.**

Let  $(\text{Gen}, \text{Enc}, \text{Dec})$  be a Public-Key encryption scheme. Let us define the following experiments for  $b \in \{0, 1\}$  and  $Q = \text{poly}(\lambda)$ .



The advantage of  $\mathcal{A}$  in the many-time CPA game is defined as

$$\text{Adv}^{\text{many-CPA}}(\mathcal{A}) = |\Pr(\mathcal{A} \xrightarrow{\text{Exp}_1^{\text{many-CPA}}} 1) - \Pr(\mathcal{A} \xrightarrow{\text{Exp}_0^{\text{many-CPA}}} 1)|.$$

1. Recall the definition of CPA-security that was given during the lecture. What is the difference?
2. Show that these two definitions are equivalent.
3. Do we have a similar equivalence in the secret-key setting?