TD 7: Asymmetric Encryptions

Exercise 1. *Deterministic Encryption*

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

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

Exercise 2. *Paillier Encryption Scheme*

Let $N = pq$ with p and q primes of identical bit-size, and ϕ be the Euler function. We first want to study the algebraic structure of $(\mathbb{Z}/N^2\mathbb{Z})^\star$.

1. Show the following propositions:

1. $\gcd(N, \phi(N)) = 1$.
2. For any $a \in (\mathbb{Z}/N\mathbb{Z})$, $(1+N)^a = (1+aN) \bmod N^2$.
3. As a consequence, $(1+N)$ has order $N \bmod N^2$.
4. $(\mathbb{Z}/N^2\mathbb{Z})^\star$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^\star$ with the following function $f(a,b) = (1+N)^a \cdot b^N \bmod N^2$.

2. We say that an element x of $(\mathbb{Z}/N^2\mathbb{Z})^\star$ is a *residue* if it can be written as N-th power (that is, $x = y^N \bmod N^2$ for some $y \in (\mathbb{Z}/N^2\mathbb{Z})^\star$). Show that the set of residues of $(\mathbb{Z}/N^2\mathbb{Z})^\star$ is isomorphic to

$$\{(a,b) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^\star \mid a = 0\}.$$

We define the Decisional Composite Residue problem (DCR) as follows: the goal of an adversary $\mathcal{A}$ is to distinguish with non-negligible advantage between $r^N \bmod N^2$ and $r \bmod N^2$, where r is sampled uniformly in $(\mathbb{Z}/N^2\mathbb{Z})^\star$.

3. Show that if an adversary knows the factorisation of N, then he can solve the DCR problem.

We now define the Paillier's Encryption scheme. The public key of the scheme is $N = pq$ with p and q prime, and the private key is $\phi(N)$ and $\phi(N)^{-1} \bmod N$. For a message $m \in (\mathbb{Z}/N\mathbb{Z})$, the encryption algorithm picks $r \in (\mathbb{Z}/N\mathbb{Z})^\star$ at random and returns:

$$\mathrm{Enc}(m) = (1+N)^m \cdot r^N \bmod N^2.$$

4. Give a decryption function.

5. Show that if the DCR problem is hard, then Paillier's encryption is CPA-secure.

6. Show that this scheme is additively homomorphic, i.e., that given the public key and the encryptions of two messages m_1 and m_2, one can compute a valid ciphertext for $m_1 + m_2$. Is it an interesting property?

7. Show a similar property for the ElGamal encryption scheme.

Exercise 3. *One-way Security*

Let (Gen, Enc, Dec) be a public-key encryption scheme. The One-Wayness against Chosen Plaintext Attack (OW-CPA) security notion is the following. The challenger samples $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$, 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 $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure and has exponential message space, then it is OW-CPA secure.

3. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure encryption scheme with message space $\mathcal{M}$ such that it has cardinality $|\mathcal{M}| = 2^\lambda$, where λ is the security parameter. Show that a small modifiction of the scheme leads to an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ that is OW-CPA secure but not IND-CPA secure anymore.

Exercise 4. *Many Challenges*

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

$$\mathsf{Exp}_b^{\text{many-CPA}}$$

$\mathcal{C}$		$\mathcal{A}$
$(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$		
	$\xrightarrow{pk}$	
		Choose adaptively $(m_0^{(i)}, m_1^{(i)})_{i=1}^Q$
	$\xleftarrow{(m_0^{(i)}, m_1^{(i)})_{i=1}^Q}$	
$(c_i = \mathsf{Enc}(pk, m_b^{(i)}))_{i=1}^Q$		
	$\xrightarrow{(c_i)_{i=1}^Q}$	
		Output $b' \in \{0,1\}$

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

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

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?