TD 7: Asymmetric Encryptions (corrected version)

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.

   ☞ Let us consider the following adversary $\mathcal{A}$. On input the public key pk, it chooses two messages $m_0 \neq m_1$ uniformly chosen over the message space $\mathcal{M}$ as its challenge query. It gets c. It computes $c_b = \mathsf{Enc}(\mathsf{pk}, m_b)$ and returns b such that $c_b = c$. Since the scheme is deterministic, there exists such a $b \in \{0,1\}$. Moreover, by correctness, the probability that $c_0 = c_1$ is negligible. Its advantage is close to one.

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 mod 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 $f(a,b) = (1+N)^a \cdot b^N \bmod N^2$.

   ☞ First, $N = pq$ with p and q prime, $\varphi(N) = (p-1)(q-1)$. Since p and q have the same bit-size, p cannot divide $q-1$ and q cannot divide $p-1$.

   Second, $(1+N)^a = \sum_{k=0}^{a} \binom{k}{a} N^k = 1 + aN + \sum_{k=2}^{a} \binom{k}{a} N^k$ and $\sum_{k=2}^{a} \binom{k}{a} N^k = 0 \bmod N^2$.

   Third, $(1+N)^N = 1 + N \cdot N = 1 \bmod N^2$.
   And for all $0 < a < N$, $(1+N)^a = 1 + aN \neq 1 \bmod N^2$.

   Fourth, we first verify that f is well-defined and has values in $(\mathbb{Z}/N^2\mathbb{Z})^\star$:

   - $\gcd(1+N, N^2) = 1$ so that $1+N$ is invertible,
   - $b \in (\mathbb{Z}/N\mathbb{Z})^\star$ so that $\gcd(b, N) = 1$, and $\gcd(b, N^2) = 1$, and finally $\gcd(b^N, N^2) = 1$: b^N is invertible.

   Second, f is a group homomorphism: $f(a_1+a_2, b_1b_2) = (1+N)^{a_1+a_2}(b_1b_2)^N \bmod N^2 = f(a_1,b_1)f(a_2,b_2) \bmod N^2$, with $(1+N)$ of order N so that we can reduce $(a_1+a_2) \bmod N$ (and of course $(b_1b_2 + kN)^N = (b_1b_2)^N \bmod N$).

   Considering the cardinalities of the groups, we have $|(\mathbb{Z}/N^2\mathbb{Z})^\star| = \varphi(N^2) = p(p-1)q(q-1) = |(\mathbb{Z}/N\mathbb{Z})||(\mathbb{Z}/N\mathbb{Z})^\star|$, since $|(\mathbb{Z}/N\mathbb{Z})| = pq$ and $|(\mathbb{Z}/N\mathbb{Z})^\star| = \varphi(N) = (p-1)(q-1)$. Therefore it is enough to prove that f is injective, or in other words, that $f(a,b) = 1$ implies $(a,b) = (0,1)$.

   Suppose that $f(a,b) = 1$. Then, we have $(1+N)^a b^N = 1 \bmod N^2$ and taking the power $\varphi(N)$ in this identity gives $(1+N)^{a\varphi(N)} b^{N\varphi(N)} = 1 \bmod N^2$, with $N\varphi(N) = \varphi(N^2)$.

   Then, from the theorem of Fermat, since $\gcd(b, N^2) = 1$ we have $b^{\varphi(N^2)} = 1 \bmod N^2$, hence $(1+N)^{a\varphi(N)} = 1 \bmod N^2$. Since the order of $(1+N)$ is N, we have $N | a\varphi(N)$, and $\gcd(N, \varphi(N)) = 1$ implies $N|a$, that is, $a = 0$ in $\mathbb{Z}/N\mathbb{Z}$.

   In particular, $b^N = 1 \bmod N^2$ and thus $b^N = 1 \bmod N$. Besides, $\gcd(b, N) = 1$ implies $b^{\varphi(N)} = 1 \bmod N$ (Fermat). Now, $\gcd(N, \varphi(N)) = 1$ so there are integers α, β such that $\alpha N + \beta\varphi(N) = 1$, and therefore $b = b^{\alpha N + \beta\varphi(N)} = 1 \bmod N$. This proves that $b = 1$ in $(\mathbb{Z}/N\mathbb{Z})^\star$, which concludes the proof.

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

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

   ☞ Taking any $y \in (\mathbb{Z}/N^2\mathbb{Z})^\star$ with $y \leftrightarrow (a,b)$ and raising it to the power N gives

$$y^N \bmod N^2 \leftrightarrow (a,b)^N = (Na \mod N, b^N \mod N) = (0, b^N \mod N).$$

Now, we consider $x \leftrightarrow (0, b)$ and we show that x is a residue. Indeed, defining $d = N^{-1} \bmod \phi(N)$ (which exists since $\gcd(N, \phi(N)) = 1$) we have for any $a \in \mathbb{Z}/N\mathbb{Z}$,

$$(a, b^d \bmod N)^N = (Na \bmod N, b^{dN} \bmod N) = (0, b) \leftrightarrow x.$$

Remark: we note that the number of N-th roots of any residue is exactly N, so that computing N-th powers is an N-to-1 function. As a consequence, if $r \in (\mathbb{Z}/N^2\mathbb{Z})^\star$ is chosen uniformly at random, then $r^N \bmod N^2$ is a uniformly distributed element of the set of residues.

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.

☞ If an adversary knows the factorization of $N = pq$, he can compute $\phi(N) = (p-1)(q-1)$. We recall that $\phi(N^2) = N\phi(N)$, so that for any $x \in (\mathbb{Z}/N^2\mathbb{Z})^\star$, we have $x^{N\phi(N)} = 1 \bmod N^2$.

Writing $x \leftrightarrow (a, b)$, it is easy to check that $x^{\phi(N)} = 1 \bmod N^2 \Leftrightarrow \phi(N)a = 0 \bmod N$, which is equivalent to $a = 0 \bmod N$ since $\phi(N)$ is invertible modulo N. In other words, $x^{\phi(N)} = 1 \bmod N^2$ if and only if x is a residue, that is, of the form $r^N \bmod N^2$.

Then, when receiving $x \in (\mathbb{Z}/N^2\mathbb{Z})^\star$, the adversary simply computes $x^{\phi(N)} \bmod N^2$, and outputs "residue" if the result is 1, "not residue" otherwise. The adversary fails only when the uniformly sampled $r \in (\mathbb{Z}/N^2\mathbb{Z})^\star$ happened to be a residue; this happens with negligible probability.

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.

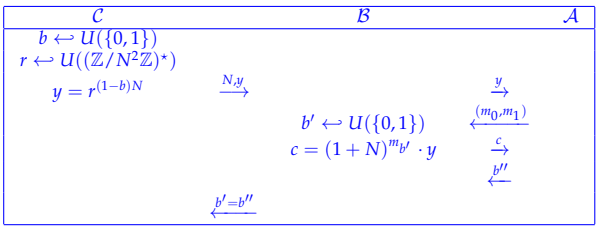
☞ On input a private key $N, \phi(N)$ and a ciphertext c, the decryption function outputs

$$\mathrm{Dec}(c) = \frac{[c^{\phi(N)} \bmod N^2] - 1}{N} \cdot \phi(N)^{-1} \mod N.$$

Indeed, writing $c = (1+N)^m r^N \bmod N^2$, we have $c^{\phi(N)} = (1+N)^{m\phi(N) \bmod N} \bmod N^2$. Then, thanks to question 1.2 we get $c^{\phi(N)} = 1 + (m\phi(N) \bmod N)N \bmod N^2$, so that (computing over the integers) we have $([c^{\phi(N)} \bmod N^2] - 1)/N = m\phi(N) \bmod N$, and finally multiplying by $\phi(N)^{-1} \bmod N$ we get the decryption m.

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

☞ Let $\mathcal{A}$ be an adversary against the CPA-security of Paillier's encryption scheme with non negligible advantage. We build the following adversary $\mathcal{B}$ against the DCR problem:



Two claims: if $b = 0$ then $\mathcal{A}$'s view is perfectly simulated. If $b = 1$, then c is independent of b' and $\Pr(b' = b'' | b = 1) = 1/2$. Thus $\mathrm{Adv}(\mathcal{B}) = \frac{1}{2}\mathrm{Adv}(\mathcal{A})$.

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?

☞ Indeed, for two plaintexts m_1 and m_2, we have $\mathrm{Enc}(m_1 + m_2) = \mathrm{Enc}(m_1) \cdot \mathrm{Enc}(m_2)$ (where $m_1 + m_2$ is considered modulo N). This also means that

$$\mathrm{Dec}[\mathrm{Enc}(m_1) \cdot \mathrm{End}(m_2)] = m_1 + m_2 \bmod N.$$

That is an interesting property in practice; for example, this allows to conceive a cryptographic voting scheme as follows:

- an authority generates a public key N for Pailler's scheme
- the voter i encrypts its vote v_i (0 or 1) into c_i using Pailler's encryption
- all ℓ voters broadcast their vote c_i, which are publicly aggregated by computing $c = \prod_{1 \leqslant i \leqslant \ell} c_i \mod N^2$
- the authority (which didn't observe previous steps) receives c and decrypts it, obtaining the total number of votes $v = \sum_{1 \leqslant i \leqslant \ell} v_i \mod N$; if N is sufficiently large, the identity $v = \sum_{1 \leqslant i \leqslant \ell} v_i$ holds over the integers.

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

☞ Let $(\mathbb{G}, q, g, h)$ be the public key in the ElGamal encryption scheme. Recall that the plaintexts are elements of G and the ciphertexts elements of $\mathbb{G} \times \mathbb{G}$; if $m_1, m_2 \in \mathbb{G}$ are two messages, their encryptions are $\langle g^{y_1}, h^{y_1} m_1 \rangle$ and $\langle g^{y_2}, h^{y_2} m_2 \rangle$ for random y_1 and y_2 in $\mathbb{Z}/q\mathbb{Z}$. Then, in $\mathbb{G} \times \mathbb{G}$ we have the product

$$\langle g^{y_1}, h^{y_1} m_1 \rangle \langle g^{y_1}, h^{y_1} m_1 \rangle = \langle g^{y_1+y_2}, h^{y_1+y_2} m_1 m_2 \rangle,$$

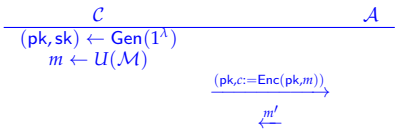
which is a valid encryption for the plaintext $m_1 m_2$.

Exercise 3. *One-way Security*

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 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 $\mathcal{M} = \{0,1\}$?

☞ Define the following game:

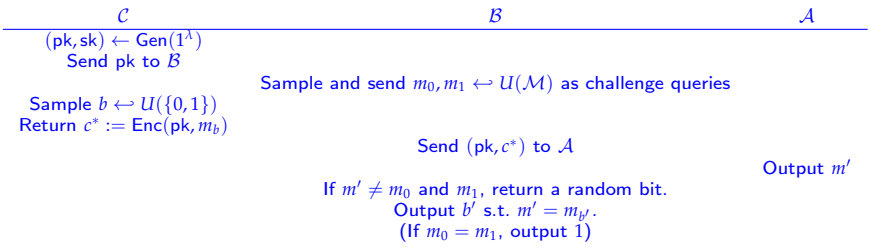


The advantage of the adversary is defined as $\mathsf{Adv}(\mathcal{A}) := \Pr(m' = m)$. A PKE scheme is OW-CPA secure if no ppt adversary has non-negligible advantage.

An adversary guessing uniformly which message was encrypted has advantage $1/|\mathcal{M}|$. As such, if the message space does not have cardinality such that $1/|\mathcal{M}| = \mathsf{negl}(\lambda)$, the scheme is trivially not OW-CPA secure.

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.

☞ Assume that the scheme is IND-CPA secure, but not OW-CPA secure. Let $\mathcal{A}$ be an adversary with non-negligible advantage in the OW-CPA game. We build the following adversary against the IND-CPA security:



Since m_b is uniformly sampled, adversary $\mathcal{A}$'s view is exactly the same as in the OW-CPA game. As such, it outputs m_b with probability $\mathsf{Adv}(\mathcal{A})$.

It holds that $\Pr(b' = 1 | b = 1) = \frac{1}{2} \Pr(m' \neq m_0 \wedge m' \neq m_1) + \Pr(m' = m_1 | b = 1)$: the second term is the probability of the random bit being right, if we output a random bit, and the second term is actually the advantage of $\mathcal{A}$.

Moreover, $\Pr(b' = 1 | b = 0) = \frac{1}{2} \Pr(m' \neq m_0 \wedge m' \neq m_1) + \Pr(m' = m_1 | b = 0)$. All that is left is to estimate the quantity $\Pr(m' = m_1 | b = 0)$.

Note that in the case $b = 0$, m' and m_1 are two independent random variables. As such, whatever the value of m', the message m_1 has probability $\frac{1}{|\mathcal{M}|}$ of being equal to it, and thus gives $\Pr(m' = m_1 | b = 0) = \frac{1}{|\mathcal{M}|}$ (this can be seen by using the law of total probabilities on the possible values of m').

Then the advantage of $\mathcal{B}$ is:

$$\mathsf{Adv}(\mathcal{B}) = \left| \mathsf{Adv}(\mathcal{A}) - \frac{1}{|\mathcal{M}|} \right|.$$

However, recall that in the first question we have proven that if the size of the message space is polynomial in λ then the notion of $OW - CPA$ does not exist. As such, we restrict our reduction to the case where $\frac{1}{|\mathcal{M}|} = \mathsf{negl}(\lambda)$, and this concludes the reduction.

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.

☞ **First method:** determinizing the scheme.

As we have already done a few times, let us assume that Enc uses ℓ bits of uniform randomness, and we make them explicit: there exists some deterministic algorithm Enc' such that $\mathsf{Enc}'(\mathsf{pk}, m, S)$ behaves exactly as $\mathsf{Enc}(\mathsf{pk}, m)$ when S is uniformly sampled over $\{0,1\}^\ell$. We simply choose to put the seed S as a part of the message: the new message space is $\mathcal{M}' = \mathcal{M} \times \{0,1\}^\ell$.

No adversary in the OW-CPA setting sees any difference, as the seed is uniformly sampled (as the rest of the message): $(\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec})$ is still OW-CPA secure.

However, no scheme with deterministic encryption is IND-CPA secure, proving that this scheme is not IND-CPA secure.

Second method: Let m be a fixed message and choose any ciphertext c. Then set $\mathsf{Enc}'(pk, m) = c$ for any pk, and do the following (to keep perfect correctness):

$$\forall pk, m' \mathsf{Enc}'(pk, m') = \begin{cases} \mathsf{Enc}(pk, m') & \text{if } \mathsf{Enc}(pk, m') \neq c \\ \mathsf{Enc}(pk, m) & \text{if } \mathsf{Enc}(pk, m') = c \end{cases}$$

Then since we only changed, for a fixed public key, at most two ciphertexts ($\mathsf{Enc}(pk, \cdot)$ is injective if we have perfect correctness), an OW-CPA adversary only sees a difference with probability $1/2|\mathcal{M}|$, which is negligible: the scheme is still OW-CPA secure.

However, an IND-CPA challenger can specifically give as challenge (m, m') and return 0 iff $c^\star = c$, where $c^\star$ is the challenger ciphertext: it has an advantage of 1. This scheme is not IND-CPA secure.

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?

☞ In the lecture, we fixed $Q = 1$.

2. Show that these two definitions are equivalent.

☞ With what was previously stated, we already see that many-CPA-secure implies CPA-secure. Let us define the following hybrid games: in game H_i, the challenger returns $\mathsf{Enc}(pk, m_0^{(j)})$ for the first i queries, and $\mathsf{Enc}(pk, m_1^{(j)})$ for the following ones. Experiment 0 is H_Q and experiment 1 is H_0. Let us assume that there exists an encryption scheme which is CPA-secure but not many-CPA-secure. This means that there exists an adversary able to distinguish between hybrids H_0 and H_Q with non-negligible probability. In particular, there exists some index i where this adversary has non-negligible advantage in distinguishing H_i and H_{i+1} by the hybrid argument:

$$\mathsf{Adv}(\mathcal{A}) \leq \sum_{i=0}^{Q-1} |\Pr(\mathcal{A} \xrightarrow{H_i} 1) - \Pr(\mathcal{A} \xrightarrow{H_{i+1}} 1)|.$$

However, the distringuishing game between H_i and H_{i+1} can be simulated by a (one time) CPA adversary: it encrypts the first i and last $n-1-i$ queries itself, and chooses query $i+1$ as its challenge query. Finally it returns the same bit that the simulated adversary returns, and they both have the same advantage, thus breaking the CPA security.

Then these two notions are equivalent.

3. Do we have a similar equivalence in the secret-key setting? ☞ No, recall the one-time pad, which is insecure as soon as two message challenges are allowed. Notably, what fails in the previous proof is that now, the adversary in the middle cannot encrypt by itself.