TD 4: Computational model and security assumptions

Margot Catinaud margot.catinaud@lmf.cnrs.fr
Théo Vignon theo.vignon@lmf.cnrs.fr

December 6, 2024

Exercise 1: $\texttt{IND}-\texttt{CPA}$ and Advantage defintions

There are three main ways to write down the advantage of an adversary.
We will illustrate those on the $\texttt{IND}-\texttt{CPA}$ security game for asymmetric encryption.

Definition: $\texttt{IND}-\texttt{CPA}$ security game

The attacker must distinguish between two scenarios (the variations between those two scenarios are parametrized by a boolean b).

- First, we compute a key pair $(\mathsf{pk}, \mathsf{sk})$ from $\mathcal{K}$.
- Then, the adversary gets pk and access to an oracle $\mathcal{O}^b_{\texttt{IND}-\texttt{CPA}}$ and returns a boolean b'. This oracle is defined as such (with r being some fresh randomness at every call)

$$\mathcal{O}^b_{\texttt{IND}-\texttt{CPA}}(m_0, m_1) = \begin{cases} \{m_b\}^r_{\mathsf{pk}} & \text{if } |m_0| = |m_1| \\ \textbf{error} & \text{otherwise} \end{cases}$$

The adversary wins if $b' = b$

Definition: find-then-guess model

Given an asymmetric encryption scheme $(\mathcal{K}, \mathcal{E}, \mathcal{D})$,
The advantage of an adversary $\mathcal{A}$ against the $\texttt{IND}-\texttt{CPA}$ game is

$$\mathbf{Adv}^{\eta}_{\texttt{IND}-\texttt{CPA}}(\mathcal{A}) = \left| 2\ \mathbf{Pr}_{b,r}\begin{bmatrix} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\eta); (m_0, m_1, s) \leftarrow \mathcal{A}_0(\mathsf{pk}); \\ c = \mathcal{O}^b_{\texttt{IND}-\texttt{CPA}}(m_0, m_1) : \mathcal{A}_1(\mathsf{pk}, m_0, m_1, c, s) = b \end{bmatrix} - 1 \right|$$

Definition: left-or-right model

Given an asymmetric encryption scheme $(\mathcal{K}, \mathcal{E}, \mathcal{D})$,
The advantage of an adversary $\mathcal{A}$ against the $\texttt{IND}-\texttt{CPA}$ game is

$$\mathbf{Adv}^{\eta}_{\texttt{IND}-\texttt{CPA}}(\mathcal{A}) = \left| \begin{array}{r} \mathbf{Pr}_r\left[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\eta) : \mathcal{A}^{\mathcal{O}^0_{\texttt{IND}-\texttt{CPA}}}(\mathsf{pk}) = 0\right] \\ -\mathbf{Pr}_r\left[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\eta) : \mathcal{A}^{\mathcal{O}^1_{\texttt{IND}-\texttt{CPA}}}(\mathsf{pk}) = 0\right] \end{array} \right|$$

1. Show that the encryption scheme must be randomized (i.e. if the encryption isn't randomized, there exists an attacker that wins with probability 1.)
2. Prove that there exists an attacker that wins with probability $\frac{1}{2}$
3. Show that the definitions of advantage for the find-then-guess and the left-or-right models with one call to oracle by the adversary are equal.

Exercise 1: $\texttt{IND}-\texttt{CPA}$ and Advantage defintions

Definition: real-or-random model

We redefine the "challenge" oracle as such (with r and m_1 being some fresh randomness at every call)

$$\mathcal{O}^b_{\texttt{IND}-\texttt{CPA}}(m_0) = \begin{cases} \{m_b\}^r_{\mathsf{pk}} & \text{if } |m_0| = |m_1| \\ \textbf{error} & \text{otherwise} \end{cases}$$

Given an asymmetric encryption scheme $(\mathcal{K}, \mathcal{E}, \mathcal{D})$,
The advantage of an adversary $\mathcal{A}$ against the $\texttt{IND}-\texttt{CPA}$ game is

$$\mathbf{Adv}^{\eta}_{\texttt{IND}-\texttt{CPA}}(\mathcal{A}) = \left| \begin{array}{l} \mathbf{Pr}_r\left[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\eta) : \mathcal{A}^{\mathcal{O}^0_{\texttt{IND}-\texttt{CPA}}}(\mathsf{pk}) = 0\right] \\ -\mathbf{Pr}_r\left[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\eta) : \mathcal{A}^{\mathcal{O}^1_{\texttt{IND}-\texttt{CPA}}}(\mathsf{pk}) = 0\right] \end{array} \right|$$

4. Show that the definitions of advantage for the left-or-right and the real-or-random models are related by a factor at most 2.

Exercise 2: A zoo of cryptographic games

For the next description of security games, try to write it down properly.

1. *one-wayness under chosen-plaintext attacks* $\texttt{OW}-\texttt{CPA}$: Here, the adversary wants to recover the whole plaintext from just the ciphertext and the public key
2. *one-wayness under plaintext-checking attacks* $\texttt{OW}-\texttt{PCA}$: Same as $\texttt{OW}-\texttt{CPA}$ but additionally, it now has access to an oracle that tell him if a given ciphertext c is the encryption of a message m. Be careful, some restrictions must occur to avoid trivial wins for the adversary.
3. *indistinguishability under validity-checking attacks* $\texttt{IND}-\texttt{VCA}$: Same as $\texttt{IND}-\texttt{CPA}$. Additionally, it now has access to an oracle that tells him if a given bitstring is a valid ciphertext or not.
4. *indistinguishability under non-adaptive chosen-ciphertext attacks* $\texttt{IND}-\texttt{CCA1}$: Same as $\texttt{IND}-\texttt{CPA}$ but additionally, it now has access to an oracle that decrypts ciphertext for him before the call to the challenge oracle.
5. *indistinguishability under adaptive chosen-ciphertext attacks* $\texttt{IND}-\texttt{CCA2}$: Same as $\texttt{IND}-\texttt{CPA}$ but additionally, it now has access to an oracle that decrypts ciphertext for him. Be careful, some restrictions must occur to avoid trivial wins for the adversary.

Exercise 3: Relation between security notions

In this exercise, we want to prove some relation between the various security notions of the previous exercises. First, we are interested in implication result, where a security notion implies another (and is therefore at least as strong as).

1. Show that $\mathtt{OW-PCA}$ implies $\mathtt{OW-CPA}$. i.e. if you have an attacker against $\mathtt{OW-CPA}$ then you can build an attacker against $\mathtt{OW-PCA}$.
2. Show that $\mathtt{IND-CPA}$ implies $\mathtt{OW-CPA}$
3. Show that $\mathtt{IND-VCA}$ implies $\mathtt{IND-CPA}$
4. Show that $\mathtt{IND-CCA1}$ implies $\mathtt{IND-VCA}$
5. Show that $\mathtt{IND-CCA2}$ implies $\mathtt{IND-CCA1}$

We now want to show that we haven't defined the same thing multiple times and therefore, that the converse implications don't hold.

6. Build an encryption scheme that is $\mathtt{IND-CPA}$ but not $\mathtt{IND-CCA1}$
   Hint: you can start by assuming that you have an $\mathtt{IND-CPA}$ or $\mathtt{IND-CCA1}$ encryption scheme and build another one upon this one.

Exercise 4: Hardness assumptions on cyclic groups

Consider a (multiplicative) cyclic group $\mathcal{G}$ of prime order p with a generator g of $\mathcal{G}$.
We can define multiple problems that we can suppose hard to prove security notions on primitives.

Definition: Discrete logarithm (DL)

Given $\mathsf{y} \in \mathcal{G}$, compute $x \in \mathbb{Z}_p$ such that $\mathsf{y} = \mathsf{g}^x$

Definition: Computational Diffie-Hellman (CDH)

Given $\mathsf{a} = \mathsf{g}^a$ and $\mathsf{b} = \mathsf{g}^b$. Compute $\mathsf{c} = g^{ab}$

Definition: Decisional Diffie-Hellman (DDH)

Given $\mathsf{a} = \mathsf{g}^a, \mathsf{b} = \mathsf{g}^b$ and $\mathsf{c} = g^c$. Decide if $\mathsf{c} = g^{ab}$

Definition: Gap Diffie-Hellman (GDH)

Given $\mathsf{a} = \mathsf{g}^a$ and $\mathsf{b} = \mathsf{g}^b$. Compute $\mathsf{c} = g^{ab}$ with access to an oracle that solves the $\mathtt{DDH}$ problem.

1. Show that $\mathtt{DL}$ is at least as hard as $\mathtt{CDH}$
2. Show that $\mathtt{CDH}$ is at least as hard as $\mathtt{DDH}$ and $\mathtt{GDH}$

Exercise 5: the RSA encryption scheme

Let's define the RSA encryption scheme

Definition: RSA

- $\mathcal{K}(1^\eta)$: get two random prime p, q with η bits, compute $n = pq$ and $\phi(n) = (p-1)(q-1)$, choose some exponent e prime to $\phi(n)$ and smaller than $\phi(n)$, the secret key is $e^{-1} \bmod \phi(n)$ and the public key is (n, e)
- $\mathcal{E}(m, \mathsf{pk} = (n, e))$: return $m^e \bmod n$

1. Find the decryption algorithm

The security of the RSA encryption scheme relies on a specific assumption called the RSA assumption.

Definition: RSA assumption

Given $n = pq$ product of two large primes of similar size and e an integer prime to $\phi(n)$. For a given $y \in \mathcal{Z}_n^*$, it is hard to compute x such that $y = x^e \bmod n$.

2. is RSA $\texttt{OW} - \texttt{CPA}$ under the RSA assumption?
3. is RSA $\texttt{OW} - \texttt{PCA}$ under the RSA assumption?
4. is RSA $\texttt{IND} - \texttt{CPA}$ under the RSA assumption?

Exercise 6: the El-Gamal encryption scheme

Let's define the El-Gamal encryption scheme

Definition: El-Gamal cryptosystem

Let $\mathbb{G}$ be a *cyclic* group of order q and let $g \in \mathbb{G}$ be a generator of this group. Both group $\mathbb{G}$ and generator g are considered to be public knowledge. The *El-Gamal cryptosystem* $\mathcal{EG}$ is defined by three algorithms $\mathcal{EG} = (\mathcal{EG}.\textsc{KeyGen}, \mathcal{EG}.\textsc{Enc}, \mathcal{EG}.\textsc{Dec})$ given by

- $\mathcal{EG}.\textsc{KeyGen}$ generates the public/secret key pair given by $(\mathsf{pk} = g^{\mathsf{sk}}, \mathsf{sk}) \leftarrow \mathcal{EG}.\textsc{KeyGen}()$ where $\mathsf{pk} \in \mathbb{G}$ and $\mathsf{sk} \in \mathbb{Z}$;
- $\mathcal{EG}.\textsc{Enc}$ encrypts a message $m \in \mathbb{G}$ and returns the pair $(g^r, m \cdot \mathsf{pk}^r) \leftarrow \mathcal{EG}.\textsc{Enc}(m, \mathsf{pk})$ where $r \in \mathbb{Z}_q$ is chosen uniformly at random in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. Sometimes, we explicit the random coin $r \in \mathbb{Z}_q$ in the definition of the algorithm $\mathcal{EG}.\textsc{Enc}$ with the notation $c \leftarrow \mathcal{EG}.\textsc{Enc}(m, \mathsf{pk}\,;\, r)$;

1. Find the decryption algorithm
2. Prove that this encryption scheme verifies the correctness property
3. Prove that this encryption scheme is $\texttt{OW} - \texttt{CPA}$ under the $\texttt{CDH}$ assumption
4. Prove that this encryption scheme is $\texttt{IND} - \texttt{CPA}$ under the $\texttt{DDH}$ assumption