TD 6: Provable cryptography - cryptographic assumptions

Margot Catinaud margot.catinaud@lmf.cnrs.fr

A function $f : \mathbb{N}^* \longrightarrow [0,1]$ is *negligible*[1] when we have :

$$\forall\, P \in \mathbb{R}[X],\ \exists\, n_P \in \mathbb{N}^*,\ \forall\, n \geqslant n_P,\ 0 \leqslant f(n) \leqslant \frac{1}{|P(n)|}.$$

Exercise 1 ($\mathtt{IND-CPA}$ and advantage definitions)

The goal of this exercise is to present different ways to define the advantage of an adversary against a cryptographic game. We will illustrate those on the $\mathtt{IND-CPA}$ security game for asymmetric encryption with only one challenge[2]. For a security parameter $\eta \in \mathbb{N}^*$, we define the *set of random tapes* Ω_η to be a pair of two random tape sets $\Omega_\eta \stackrel{\text{def}}{=} \left(\Omega^{\mathtt{h}}_\eta, \Omega^{\mathtt{a}}_\eta\right) \subset \{0,1\}^* \times \{0,1\}^*$ where

- The set $\Omega^{\mathtt{h}}_\eta$ of *honest random tapes* is defined by

  $$\Omega^{\mathtt{h}}_\eta \stackrel{\text{def}}{=} \{0,1\}^{\mathtt{poly}(\eta)} \quad \text{such that} \quad \forall\, \rho_h \in \Omega^{\mathtt{h}}_\eta,\ \exists\, P_{\rho_h} \in \mathbb{R}[X],\ \mathsf{len}(\rho_h) \leqslant |P(\eta)|.$$

  Said otherwise, $\Omega^{\mathtt{h}}_\eta$ is the set of honest random tapes of length polynomial in the security parameter η. Besides, we suppose that all random values generated with the honest random tape ρ_h are *independent and chosen uniformly at random*:

  $$n \xleftarrow{\rho_h} \mathcal{N} \stackrel{\text{def}}{\Longleftrightarrow} n \xleftarrow{\$} \mathcal{N}.$$

  Where $\cdot \xleftarrow{\$} \mathcal{N}$ denote the uniform distribution on $\mathcal{N}$.

- The set $\Omega^{\mathtt{a}}_\eta$ of *adversarial random tapes* is defined by

  $$\Omega^{\mathtt{a}}_\eta \stackrel{\text{def}}{=} \{0,1\}^{\mathtt{poly}(\eta)}.$$

  Besides, no constraints are made on an adversarial random tape ρ_a, meaning that $\cdot \xleftarrow{\rho_a} \mathcal{N}$ follows any probability distribution the adversary choose to use. In particular, any random value computed with the random tape ρ_a can depend of any previously generated values.

The $\mathtt{IND-CPA}$ security game for an asymmetric encryption scheme $\mathbb{AES} = (\mathsf{keygen}_{\mathbb{AES}}, \mathsf{aenc}_{\mathbb{AES}}, \mathsf{adec}_{\mathbb{AES}})$ with randomness set $\mathcal{R}_{\mathbb{AES}}$ is defined as follows in Game 1.

$\mathtt{IND-CPA}^{\mathcal{A}}_{\mathbb{AES}}(\eta, (\rho_h, \rho_a)\,;\, \beta)$ – $\mathtt{IND-CPA}$ **game for the** $\mathbb{AES}$ **scheme**
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{keygen}_{\mathbb{AES}}(\eta)$;
$(m_0, m_1, \mathtt{st}_1) \leftarrow \mathcal{A}(\eta, \mathsf{pk}\,;\, \rho_a)$;
$r \xleftarrow{\rho_h} \mathcal{R}_{\mathbb{AES}}$;
$c_\beta \leftarrow \mathsf{aenc}_{\mathbb{AES}}(\mathsf{pk}, m_\beta\,;\, r)$;
$b \leftarrow \mathcal{A}(c_\beta\,;\, \rho_a,\, \mathtt{st}_1)$;
return b.

Game 1: **IND**istinguishability under **C**hosen **P**laintext **A**ttack cryptographic game

Now, we defines some variants of the *advantage of $\mathcal{A}$ against the* $\mathtt{IND-CPA}$ *game* as follows.

- ***(find-then-guess* model)** Given an asymmetric encryption scheme $\mathbb{AES}$, the *advantage of $\mathcal{A}$ against the* $\mathtt{IND-CPA}$ *game for* $\mathbb{AES}$ in the *find-then-guess* model is given by :

  $$\forall\, \eta \in \mathbb{N}^*,\ \mathbf{Adv}_{\mathbb{AES}}\left[\mathtt{IND-CPA} \mid \mathcal{A}\right](\eta) \stackrel{\text{def}}{=} \left| 2 \cdot \mathbb{P}\mathsf{r}_{(\rho_h,\rho_a)\in\Omega_\eta}\left[\, \beta \leftarrow_{\mathcal{G}} \mathtt{IND-CPA}^{\mathcal{A}}_{\mathbb{AES}}(\eta, \rho\,;\, \beta) \;\middle|\; \beta \xleftarrow{\rho_h} \{0,1\} \,\right] - 1 \right|$$

[1] Notice that all polynomial function $P \in \mathbb{R}[X]$ have a **finite** set of roots. Thus, we implicitly suppose that $n_P \in \mathbb{N}^*$ is such that

$$n_P > \max\left\{x \in \mathbb{R}\ |P(x) = 0\right\}.$$

[2] Notice that there exists also a multiple challenges definition of the $\mathtt{IND-CPA}$ game, but we will not consider this multiple challenges to make this exercise easier. For the multiple challenges definition, we need to state the $\mathtt{IND-CPA}$ game with a challenge oracle which can be called multiple times by the adversary.

- **(*left-or-right* model)** Given an asymmetric encryption scheme $\mathbb{AES}$, the *advantage of* $\mathcal{A}$ *against the* $\mathtt{IND-CPA}$ *game for* $\mathbb{AES}$ in the *left-or-right* model is given by :

$$\forall\,\eta \in \mathbb{N}^*,\ \mathbf{Adv}_{\mathbb{AES}}\big[\mathtt{IND-CPA} \mid \mathcal{A}\big](\eta) \overset{\text{def}}{=} \left| \begin{array}{r} \mathbb{P}\mathsf{r}_{\rho\in\Omega_\eta}\Big[\ 0 \leftarrow_{\mathcal{G}} \mathtt{IND-CPA}^{\mathcal{A}}_{\mathbb{AES}}\big(\eta,\rho\,;\,\beta=0\big)\ \Big] \\ -\mathbb{P}\mathsf{r}_{\rho\in\Omega_\eta}\Big[\ 0 \leftarrow_{\mathcal{G}} \mathtt{IND-CPA}^{\mathcal{A}}_{\mathbb{AES}}\big(\eta,\rho\,;\,\beta=1\big)\ \Big] \end{array} \right| .$$

- **(*real-or-random* model)** In this model, we redefine the $\mathtt{IND-CPA}$ game as follows :

$\mathtt{IND-CPA-RoR}^{\mathcal{A}}_{\mathbb{AES}}\big(\eta,(\rho_h,\rho_a)\,;\,\beta\big)$ – ***Real-or-random*** $\mathtt{IND-CPA}$ **game**
$(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{keygen}_{\mathbb{AES}}(\eta)$;
$(m_0,\mathtt{st}_1) \leftarrow \mathcal{A}(\eta,\mathsf{pk}\,;\,\rho_a)$;
$r \overset{\rho_h}{\twoheadleftarrow} \mathcal{R}_{\mathbb{AES}}$; $m_1 \overset{\rho_h}{\twoheadleftarrow} \{0,1\}^{\mathsf{len}(m_0)}$;
$c_\beta \leftarrow \mathsf{aenc}_{\mathbb{AES}}(\mathsf{pk},m_\beta\,;\,r)$;
$b \leftarrow \mathcal{A}(c_\beta\,;\,\rho_a,\,\mathtt{st}_1)$;
return b.

Game 2: $\mathtt{IND-CPA}$ cryptographic game in the case of the *real-or-random* model

Then, the *advantage of* $\mathcal{A}$ *against the* $\mathtt{IND-CPA-RoR}$ *game for* $\mathbb{AES}$ in the *real-or-random* model is given by :

$$\forall\,\eta \in \mathbb{N}^*,\ \mathbf{Adv}_{\mathbb{AES}}\big[\mathtt{IND-CPA-RoR} \mid \mathcal{A}\big](\eta) \overset{\text{def}}{=} \left| \begin{array}{r} \mathbb{P}\mathsf{r}_{\rho\in\Omega_\eta}\Big[\ 0 \leftarrow_{\mathcal{G}} \mathtt{IND-CPA-RoR}^{\mathcal{A}}_{\mathbb{AES}}\big(\eta,\rho\,;\,\beta=0\big)\ \Big] \\ -\mathbb{P}\mathsf{r}_{\rho\in\Omega_\eta}\Big[\ 0 \leftarrow_{\mathcal{G}} \mathtt{IND-CPA-RoR}^{\mathcal{A}}_{\mathbb{AES}}\big(\eta,\rho\,;\,\beta=1\big)\ \Big] \end{array} \right| .$$

Let $\eta \in \mathbb{N}^*$ be a security parameter. We say that the adversary $\mathcal{A}$ *wins the* $\mathtt{IND-CPA}$ *game* when

$$\forall\,\rho \in \Omega_\eta,\ \forall\,\beta \in \{0,1\},\ \beta = \mathtt{IND-CPA}^{\mathcal{A}}_{\mathbb{AES}}\big(\eta,\rho\,;\,\beta\big)\,.$$

1. *Show that the encryption scheme must be randomized : otherwise, there exists an attacker that wins with probability* 1.
2. *Prove that there exists an attacker that wins with probability* $\dfrac{1}{2}$.
3. *Show that the definitions of advantage for the* find-then-guess *and the* left-or-right *models are equal.*
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 (Hardness assumptions on cyclic groups)

The goal of this exercise is to present a bunch of cryptographic assumptions over cyclic groups. Consider a (multiplicative) cyclic group $\mathbb{G}_p$ of prime order $p \in \mathbb{P}$ and a fixed *public* generator $g \in \mathbb{G}_p$ of $\mathbb{G}_p$. In provable security, we can suppose several cryptographic assumptions over a cyclic group to prove security of larger cryptographic constructions (such as asymmetric encryption schemes or signature schemes) or protocols.
For two cryptographic games $\mathcal{G}_1$ and $\mathcal{G}_2$, we define a binary relation $\preccurlyeq_{\mathcal{G}}$ on games to be :

$$\mathcal{G}_1 \preccurlyeq_{\mathcal{G}} \mathcal{G}_2 \overset{\text{def}}{\iff} \mathcal{G}_1 \text{ is } \textit{at least} \text{ as hard as } \mathcal{G}_2.$$

More formally, $\mathcal{G}_1 \preccurlyeq_{\mathcal{G}} \mathcal{G}_2$ means that, by contraposition, if an adversary $\mathcal{A}$ *breaks* (*i.e.* wins) the game $\mathcal{G}_1$ then there exists another adversary $\mathcal{B}(\mathcal{A})$, built over adversary $\mathcal{A}$, that breaks the $\mathcal{G}_2$ game.

1. *Give, for each hardness problem* $\mathtt{HP}$ *of fig. 3, a corresponding cryptographic game* $\mathcal{G}_{\mathtt{HP}}\big[\mathbb{G}_p\big]$.
2. *Show the following relations between hardness assumptions over cyclic groups:*

$$\boxed{\mathcal{G}_{\mathtt{DL}}\big[\mathbb{G}_p\big] \preccurlyeq_{\mathcal{G}} \mathcal{G}_{\mathtt{CDH}}\big[\mathbb{G}_p\big] \preccurlyeq_{\mathcal{G}} \left\{ \begin{array}{l} \mathcal{G}_{\mathtt{DDH}}\big[\mathbb{G}_p\big] \\ \mathcal{G}_{\mathtt{GDH}}\big[\mathbb{G}_p\big] \end{array} \right.}$$

Problem 1: Discrete Logarithm (DL)

problem Discrete Logarithm for group $\mathbb{G}_p$ **is:**
- **given** $y \in \mathbb{G}_p$.
- **computes** $x \in \mathbb{F}_p$ **such that** $y = g^x$.

Problem 2: Computational Diffie-Hellman (CDH)

problem Computational DH for group $\mathbb{G}_p$ **is:**
- **given** $\left(\alpha \stackrel{\text{def}}{=} g^a, \beta \stackrel{\text{def}}{=} g^b\right) \in \mathbb{G}_p^2$.
- **computes** $\gamma \in \mathbb{G}_p$ **such that** $\gamma = g^{ab}$.

Problem 3: Decisional Diffie-Hellman (DDH)

problem Decisional DH for group $\mathbb{G}_p$ **is:**
- **given** $\left(\alpha \stackrel{\text{def}}{=} g^a, \beta \stackrel{\text{def}}{=} g^b, \gamma \stackrel{\text{def}}{=} g^c\right) \in \mathbb{G}_p^3$.
- **decides whether** $\gamma = g^{ab}$.

Problem 4: Gap Diffie-Hellman (GDH)

problem Gap DH for group $\mathbb{G}_p$ **is:**
- **given** $\left(\alpha \stackrel{\text{def}}{=} g^a, \beta \stackrel{\text{def}}{=} g^b\right) \in \mathbb{G}_p^2$.
- **computes** $\gamma \in \mathbb{G}_p$ **such that** $\gamma = g^{ab}$
- **with oracle access to** $\mathcal{O}_{\texttt{DDH}}$ solving the DDH problem.

Figure 3: Bunch of hardness assumptions over cyclic groups.

Exercise 3 (A zoo of cryptographic games)

For the next description of security games, try to write it down properly. Be careful to the case where the adversary $\mathcal{A}$ can do an arbitrary number of challenges : we need oracles[3].

1. ***INDistinguishability under Chosen-Plaintext Attacks*** ($\texttt{IND}-\texttt{CPA}$) Give the multiple challenges version of the $\texttt{IND}-\texttt{CPA}$ game.
2. ***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.
3. ***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 her 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.
4. ***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 her if a given bitstring is a valid ciphertext or not.
5. ***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 her before the call to the challenge oracle.
6. ***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 her. Be careful, some restrictions must occur to avoid trivial wins for the adversary.

Exercise 4 (Hardness relations between $\texttt{IND}-\texttt{CPA}$, $\texttt{IND}-\texttt{CCA1}$ and $\texttt{IND}-\texttt{CCA2}$ games)

In this exercise, we will try to give security relationship between $\texttt{IND}-\texttt{CPA}$, $\texttt{IND}-\texttt{CCA1}$ and $\texttt{IND}-\texttt{CCA2}$ games[4]. Recall the $\preccurlyeq_{\mathcal{G}}$ relations between games see in exercise 2. We say that a game $\mathcal{G}$ is *secure* when, for all adversary $\mathcal{A}$ (modelled as Probabilistic Polynomial-time Turing Machine), we have:

$$\eta \longmapsto \mathbf{Adv}\left[\mathcal{G} \mid \mathcal{A}\right](\eta) \text{ is negligible in } \eta.$$

1. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two cryptographic games such that $\mathcal{G}_1 \preccurlyeq_{\mathcal{G}} \mathcal{G}_2$. In this question, we will show the following property:
$$\boxed{\mathcal{G}_2 \text{ is secure} \implies \mathcal{G}_1 \text{ is also secure.}} \qquad (\Sigma)$$
To do so, we proceed by contraposition. Suppose that $\mathcal{G}_1$ is not secure: meaning that there exists an adversary $\mathcal{A}$ such that the function $\mathbf{Adv}\left[\mathcal{G}_1 \mid \mathcal{A}\right]$ is *non-negligible* in η.
Using $\mathcal{G}_1 \preccurlyeq_{\mathcal{G}} \mathcal{G}_2$, show that $\mathcal{G}_2$ is not secure.
2. *Give and prove relations between games* $\texttt{IND}-\texttt{CPA}$, $\texttt{IND}-\texttt{CCA1}$ *and* $\texttt{IND}-\texttt{CCA2}$ *for the relation* $\preccurlyeq_{\mathcal{G}}$ *using the property eq.* (Σ).

[3] **Note:** Do not hesitate to ask how we write cryptographic games in the case of arbitrary number of calls to oracles.
[4] To learn more about hierarchy between indistinguishability security notions in the case of *Fully Homomorphic Encryption* (FHE) schemes, see the thesis of Marc Renard:

https://theses.hal.science/tel-05421880v1/file/157007_RENARD_2025_archivage.pdf

3. *Do we have relations in the opposite direction?*

Exercise 5 (About the RSA encryption scheme)

The RSA encryption scheme $\mathbb{RSA} = (\mathsf{keygen}_{\mathbb{RSA}}, \mathsf{aenc}_{\mathbb{RSA}}, \mathsf{adec}_{\mathbb{RSA}})$ is defined as follows:

- $\mathsf{keygen}_{\mathbb{RSA}}(\eta)$ takes as input a security parameter $\eta \in \mathbb{N}^*$. Computes two random primes $p, q \in \mathbb{P}$ such that $\log_2 p \geqslant \eta$ and $\log_2 q \geqslant \eta$. Then, computes $n = pq$ and $\phi(n) = (p-1)(q-1)$ (the Euler function). Chooses some exponent $e \in \mathbb{Z}_n$ such that $e \wedge \phi(n) = 1$ and $e \leqslant \phi(n)$. Finally, outputs $(\mathsf{sk}, \mathsf{pk})$ where $\mathsf{sk} \stackrel{\text{def}}{=} e^{-1} \mod [\phi(n)]$ is the secret key and $\mathsf{pk} \stackrel{\text{def}}{=} (n, e)$ is the public key.
- $\mathsf{aenc}_{\mathbb{RSA}}\big(m, \mathsf{pk} = (n, e)\big)$ returns $m^e \mod [n]$ on inputs a message $m \in \mathbb{Z}_n$ and a public key $\mathsf{pk} \in \mathbb{N} \times \mathbb{Z}_n$.

1. *Find the decryption algorithm* $\mathsf{adec}_{\mathbb{RSA}}$.
2. *Prove that this encryption scheme verifies the functional correctness property*[5].

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

Problem 5: `RSA` assumption

problem RSA for group $\mathbb{Z}_n$ **is:**

given $\left(n \stackrel{\text{def}}{=} pq, e, y\right) \in \mathbb{N} \times \mathbb{N} \times \mathbb{Z}_n^*$ **such that** $p, q \in \mathbb{P}$ **and** $e \wedge \phi(n) = 1$.

computes $x \in \mathbb{Z}_n$ **such that** $y = x^e \mod [n]$.

3. *Is* $\mathbb{RSA}$ $\mathtt{OW-CPA}$*-secure under the* `RSA` *assumption?*
4. *Is* $\mathbb{RSA}$ $\mathtt{OW-PCA}$*-secure under the* `RSA` *assumption?*
5. *Is* $\mathbb{RSA}$ $\mathtt{IND-CPA}$*-secure under the* `RSA` *assumption?*

Exercise 6 (About the El-Gamal encryption scheme)

For all security parameter η, let $\mathbb{G}_{p_\eta}$ be a cyclic group of prime order $p_\eta \in \mathbb{P}$ such that $\log_2 p_\eta \geqslant \eta$ and let $g_\eta \in \mathbb{G}_{p_\eta}$ be a generator of this group. The family of pairs $\mathfrak{G} \stackrel{\text{def}}{=} \left(\mathbb{G}_{p_\eta}, g_\eta\right)_{\eta \in \mathbb{N}^*}$ of group and generator are considered to be public knowledge. The *El-Gamal encryption scheme* $\mathbb{EG} \stackrel{\text{def}}{=} (\mathsf{keygen}_{\mathbb{EG}}, \mathsf{aenc}_{\mathbb{EG}}, \mathsf{adec}_{\mathbb{EG}})$ for the public parameters $\mathfrak{G}$ is defined as follows:

- $\mathsf{keygen}_{\mathbb{EG}}(\eta)$ takes as input a security parameter $\eta \in \mathbb{N}^*$ and generates a key pair $(\mathsf{pk}, \mathsf{sk}) \in \mathbb{G}_{p_\eta} \times \mathbb{F}_{p_\eta}$ such that $\mathsf{pk} \stackrel{\text{def}}{=} g_\eta^{\mathsf{sk}}$;
- $\mathsf{aenc}_{\mathbb{EG}}\big(\mathsf{pk}, m\,;\,r\big)$ takes as input a public key $\mathsf{pk} \in \mathbb{G}_{p_\eta}$, a message $m \in \mathbb{G}_{p_\eta}$ and a random value $r \in \mathbb{F}_{p_\eta}$. Then, outputs a ciphertext pair $\left(g^r, m \cdot \mathsf{pk}^r\right) \in \mathbb{G}_{p_\eta}^2$. Notice that we can also write $\mathsf{aenc}_{\mathbb{EG}}(\mathsf{pk}, m)$ which implies that this algorithm generates uniformly at random a public coin $r \in \mathbb{F}_{p_\eta}$ and becomes this way probabilistic.

1. *Find the decryption algorithm* $\mathsf{adec}_{\mathbb{EG}}$.
2. *Prove that this encryption scheme verifies the functional correctness property.*
3. *Prove that, for all public key* $\mathsf{pk} \in \mathbb{G}_{p_\eta}$*, the following function is a group homomorphism:*

$$\varphi_{\mathsf{pk}} : \begin{array}{ccc} \mathbb{G}_{p_\eta} & \longrightarrow & \mathbb{G}_{p_\eta}^2 \\ m & \longmapsto & \mathsf{aenc}_{\mathbb{EG}}(\mathsf{pk}, m) \end{array}$$

   Thus, we say that the El-Gamal encryption scheme is *homomorphic*[6].

4. *Prove that* $\mathbb{EG}$ *is* $\mathtt{OW-CPA}$*-secure under the* `CDH` *assumption.*
5. *Prove that* $\mathbb{EG}$ *is* $\mathtt{IND-CPA}$*-secure under the* `DDH` *assumption.*
6. *Is* $\mathbb{EG}$ $\mathtt{IND-CCA1}$*-secure?*

[5] The functional correctness property for an asymmetric encryption scheme $(\mathsf{aenc}, \mathsf{adec})$ is given by:

$$\mathsf{adec}(\mathsf{aenc}(\mathsf{pk}(\mathsf{sk}), m, r), \mathsf{sk}) = m.$$

[6] In this exercise, $\mathbb{EG}$ is a multiplicative homomorphic encryption scheme. We can also make this scheme additively homomorphic. When a homomorphic encryption scheme $\mathbb{HS}$ is simultaneously multiplicative and additve, we say that $\mathbb{HS}$ is *fully homomorphic.*