Proofs of Security

TUT n°5 — Foundations of symmetric cryptography

M2-SIF, M2-CRYPTO

Léo Ackermann

Answer all ▸ questions before looking at ⋆ questions.

Shannon's theorem

The goal of this exercise is to prove the following result from Shannon.

> **Theorem 1** *Let* (KeyGen, Enc, Dec) *be an encryption scheme such that* $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$. *The scheme is perfectly secure if and only if:*
>
> 1. *Every key* $k \in \mathcal{K}$ *is chosen with (equal) probability* $1/|\mathcal{K}|$ *by* Gen.
> 2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$, *there is a unique key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}(m, k)$ *outputs* c.

First, we justify that the hypothesis made on spaces is reasonable: the considered encryption schemes can be seen as the optimal ones.

▸ **Question 1.** *Show that Perfect Secrecy requires* $|\mathcal{K}| \geqslant |\mathcal{M}|$.

▸ **Question 2.** *Show that Correctness requires* $|\mathcal{C}| \geqslant |\mathcal{M}|$.

Now the proof. You may consider that Enc is deterministic, as this can be done without loss of generality here.

▸ **Question 3.** *Show that verifying conditions (1) and (2) suffices to be perfectly secure. You may consider the following equivalent definition of Perfect Secrecy:*

$$\forall m, m' \in \mathcal{M}, \forall c \in \mathcal{C}, \Pr_K(\mathsf{Enc}(m, K) = c) = \Pr_K(\mathsf{Enc}(m', K) = c).$$

▸ **Question 4.** *Show the remaining direction.*

Extending PRF range

We are given a PRF $F : (\{0,1\}^k)^2 \to \{0,1\}^k$ and we wants to build a PRF G with range twice as big.

▸ **Question 5.** *Let* $G(K, x) = F(K, x) || F(K, \overline{x})$. *Is* G *a PRF? If so, prove it. Otherwise, give an attack.*

▸ **Question 6.** *Same as (1), but with* $G(K, x) = \texttt{let } y_1 \leftarrow F(K, x) \texttt{ in: } \; y_1 || F(K, y_1)$.

▸ **Question 7.** *Same as (1), but with* $G(K, x) = \texttt{let } L \leftarrow F(K, x) \texttt{ in: } \; F(L, 0^k) || F(L, 1^k)$.

Increasing PRG expansion factor

We recall that the advantage $\mathrm{Adv}_{\mathcal{A}}^{PRG}[G]$ of an algorithm $\mathcal{A}$ against a PRG (pseudo-random generator) $G : \{0,1\}^k \to \{0,1\}^n$ is the difference of the probabilities that $\mathcal{A}$ returns 1 when it is given $G(x) \in \{0,1\}^n$ for x uniformly sampled in $\{0,1\}^k$, and when it is given u uniformly sampled in $\{0,1\}^n$. We say that G is a secure PRG if for all probabilistic polynomial-time $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in k, i.e., $\mathrm{Adv}_{\mathcal{A}}^{PRG}[G] \leqslant k^{-\omega(1)}$.

In this exercise, we assume we are given a pseudo-random generator $G : \{0,1\}^k \to \{0,1\}^{k+1}$.

▸ **Question 8.** *Consider* $G^{(1)} : \{0,1\}^k \to \{0,1\}^{k+2}$ *defined as follows. On input* $x \in \{0,1\}^k$, $G^{(1)}$ *first evaluates* $G(x)$ *and obtains* $(x^{(1)}, y^{(1)}) \in \{0,1\}^k \times \{0,1\}$ *such that* $G(x) = x^{(1)} \parallel y^{(1)}$. *It then evaluates* G *on* $x^{(1)}$ *and eventually returns* $G(x^{(1)}) \parallel y^{(1)}$. *Show that if* G *is a secure PRG, then so is* $G^{(1)}$.

▸ **Question 9.** *Let* $n \geqslant 1$. *Propose a construction of a PRG* $G^{(n)} : \{0,1\}^k \to \{0,1\}^{k+n+1}$ *based on* G. *Show that if* G *is a secure PRG, then so is* $G^{(n)}$.

Feistel networks

We start by recalling the definition of Fesitel networks.

Let $G : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a family of functions, and let $d \geqslant 1$ be an integer. The Feistel network of depth d associated to G is the family of functions $F^{(d)} : \{0,1\}^{kd} \times \{0,1\}^{2l} \to \{0,1\}^{2l}$, defined as follows:

$F^{(d)}((K_i)_{i \in [\![1,d]\!]}, x)$

```
L_0||R_0 ← x
For i ∈ [[1, d]] do
L_i ← R_{i−1}; R_i ← G(K_i, R_{i−1}) ⊕ L_{i−1}
Return L_d||R_d
```

▸ **Question 10.** *Draw a representation of a Feistel network of depth 3.*

▸ **Question 11.** *Show that a Feistel network is invertible, even if the family of functions G is not.*

▸ **Question 12.** *Show that neither $F^{(1)}$ nor $F^{(2)}$ is a secure PRF.*

Feistel networks are a way of constructing an efficiently invertible permutation from a set of pseudorandom functions: it suffices to consider $F^{(3)}$. In the rest of this exercise, we suppose G to be a family of pseudorandom functions.

▸ **Question 13.** *Show that "collision at R_1", i.e. $R_1^i = R_1^j$ for two different queries i and j made by the adversary, only occurs with negligible probability.*

▸ **Question 14.** *Similarly show that, conditionned on "no collision at R_1", the probability of having a "collision at R_2" is negligible. Conclude.*

★ **Question 15.** *Show that $F^{(3)}$ is not a strong pseudorandom permutation, i.e. $(F^{(3)}, (F^{(3)})^{-1})$ is not indistinguishable from (ρ, ρ^{-1}) where ρ is a random function, but that $F^{(4)}$ does.*