Modern Cryptography
Bachelor Computer Science, University of Amsterdam, 2017/18
TEACHER: Christian Schaffner, TA: Jan Czajkowski, Christian Majenz

Problem Set 5

We will work on the following exercises together during the work sessions on Tuesday, 26 September 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

Problem 1: not PRFs

Let us assume that k and x are n-bit strings. For all of the following constructions, explain why they are not PRFs. Give an explicit description of an efficient attacker that distinguishes the given function from a uniform function $f \in \mathsf{Func}_n$.

(a) Let $F_k(x)$ output k.

(b) Let $F_k(x)$ output x.

(c) Let $F_k(x)$ output $x \oplus k$.

Problem 2: Basic properties of PRFs

The set of all functions from n bits to ℓ bits is denoted by

$$\mathsf{Func}_{n,\ell} := \left\{ f : \{0,1\}^n \to \{0,1\}^\ell \right\}.$$

Note that with this definition, we have that Func_n as defined on page 77 of [KL] is equal to $\mathsf{Func}_{n,n}$.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\ell$ be a pseudorandom function.

(a) How many functions are there in $\mathsf{Func}_{n,\ell}$?

(b) How many functions $F_k : \{0,1\}^n \to \{0,1\}^\ell$ are there if you vary k?

(c) Let $h(n,\ell)$ denote the fraction of functions F_k among all functions in $\mathsf{Func}_{n,\ell}$. Argue that $h(n,\ell)$ is a negligible function in n. Argue that $h(n,\ell)$ is also negligible in ℓ.

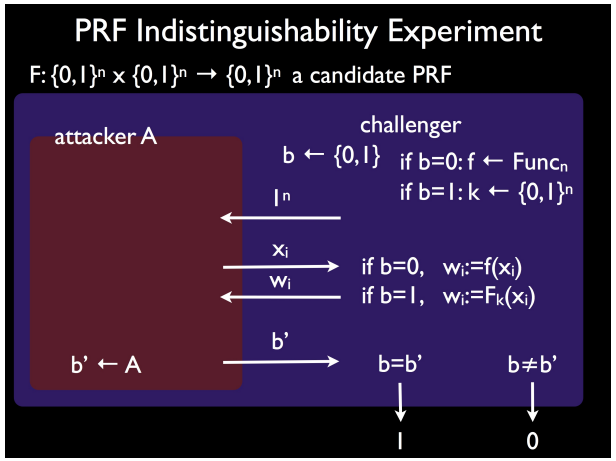

Figure 1: The $\mathsf{PRF}_{\mathcal{A},F}(n)$ experiment

Problem 3: Exercise 3.12

Let F be a keyed function and consider the following experiment:

The PRF indistinguishability experiment $\mathsf{PRF}_{\mathcal{A},F}(n)$**:**, see also Figure 1:

1. *A uniform bit $b \in \{0,1\}$ is chosen. If $b = 1$ then choose uniform $k \in \{0,1\}^n$.*

2. *$\mathcal{A}$ is given 1^n for input. If $b = 0$ then $\mathcal{A}$ is given access to a uniform function $f \in \mathsf{Func}_n$. If $b = 1$ then $\mathcal{A}$ is instead given access to $F_k(\cdot)$.*

3. *$\mathcal{A}$ outputs a bit b'.*

4. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.*

Define pseudorandom functions using this experiment, and prove that your definition is equivalent to Definition 3.25.

Problem 4: Exercise 3.14 from [KL]

Argue that if F is a length-preserving pseudorandom function, then $G(s) := F_s(1)\|F_s(2)\|\cdots\|F_s(\ell)$ is a pseudorandom generator with expansion factor $\ell \cdot n$.

Problem 5: Exercise 3.9 from [KL]

Prove *unconditionally* the existence of a pseudorandom function $F : \{0,1\}^{n^2} \times \{0,1\}^{\log(n)} \to \{0,1\}^n$.

Hint: Implement a uniform function with logarithmic input length.

★ Problem 6: Exercise 3.16 from [KL]

Prove Proposition 3.27: *If F is a pseudorandom permutation and additionally $\ell_{in}(n) \geq n$, then F is also a pseudorandom function.*

Hint: Use the results of Appendix A.4.