Problem Set 3

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.

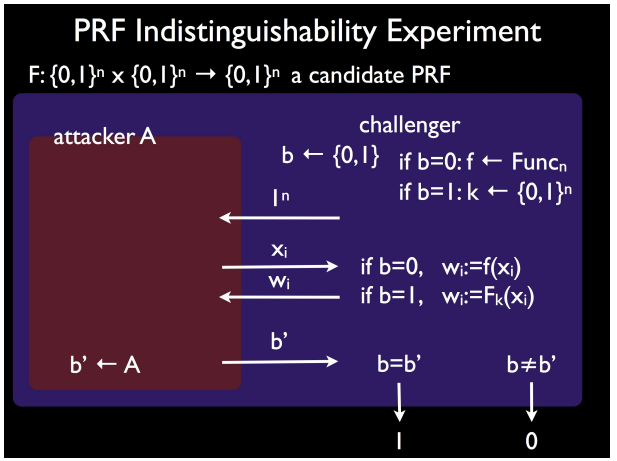

Figure 1: The $\mathsf{PRF}_{\mathcal{A},F}(n)$ experiment

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 3.20 from [KL]

Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather

than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

Problem 5: Exercise 3.28 from [KL]

Show that the CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption schemes (regardless of F). Consider encryptions and decryptions of only single block messages.

Problem 6: Exercise 3.29 from [KL]

Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one is CPA-secure (but you don't know which one). Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Provide a full proof of your solution.

Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one reveals nothing about the original plaintext, but knowledge of both enables the original plaintext to be computed.

★ Problem 7: 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 8: 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 9: 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.

★ Problem 10: Exercise 3.26 from [KL]

For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}()$ to be a probabilistic oracle that, on input 1^n, chooses uniform $r \in \{0,1\}^n$ and returns $\langle r, g(r)\rangle$. A keyed function F is a *weak pseudorandom function* if for all PPT algorithms D, there exists a negligible function negl such that:

$$\left|\Pr[D^{F_k^{\$}(\cdot)}(1^n) = 1] - \Pr[D^{f^{\$}(\cdot)}(1^n) = 1]\right| < \mathsf{negl}(n), \tag{1}$$

where $k \in \{0,1\}^n$ and $f \in \mathsf{Func}_n$ are chosen uniformly.

(a) Prove that if F is pseudorandom then it is weakly pseudorandom.

(b) Let F' be a pseudorandom function, and define

$$F_k(x) := \begin{cases} F'_k(x) & \text{if } x \text{ is even} \\ F'_k(x+1) & \text{if } x \text{ is odd.} \end{cases} \tag{2}$$

Prove that F is weakly pseudorandom, but *not* pseudorandom.

(c) Is CTR-mode encryption using a weak pseudorandom function necessarily CPA-secure? Does it necessarily have indistinguishable encryptions in the presence of an eavesdropper? Prove your answers.

Hint: Consider CTR-mode using F defined above, show an attack on this encryption scheme.

(d) Prove that Construction 3.30 is CPA-secure if F is a weak pseudorandom function.