Prof. Dr. Johannes Blömer
Nils Löken

May 5th, 2017
submission due: May 16th, 2017: 11 a.m.

Cryptography - Provable Security

SS 2017

Handout 4

Exercises marked (*) will be checked by tutors.

Exercise 1:
Let $l : \mathbb{N} \to \mathbb{N}$ be a polynomial with $l(n) > n$ and let G be a deterministic polynomial-time algorithm such that for every $x \in \{0,1\}^n$ algorithm G outputs a string of length $l(n)$. We call G an almost-random generator if for every ppt algorithm $\mathcal{A}$ there exists a negligible function μ such that $\mathcal{A}$ wins the following game $\text{Guess}_{\mathcal{A},G}(n)$ with probability at most $\frac{1}{2} + \mu(n)$.

Distribution guessing game $\text{Guess}_{\mathcal{A},G}(n)$

- A bit $b \leftarrow \{0,1\}$ is chosen uniformly at random.
- If $b = 1$, then choose $x \leftarrow \{0,1\}^{l(n)}$ uniformly at random. If $b = 0$, then choose $s \leftarrow \{0,1\}^n$ and compute $x := G(s)$. The string x is given to $\mathcal{A}$.
- $\mathcal{A}$ outputs a bit $b' \leftarrow \mathcal{A}(1^n, x)$.
- $\mathcal{A}$ wins the game if and only if $b = b'$.

Show that every pseudorandom generator is an almost-random generator.

Exercise 2 (4 points)**:**
(*) Consider almost-random generators from exercise 1. Show that every almost-random generator G is a pseudorandom generator.

Exercise 3:
Prove that every pseudorandom permutation is a pseudorandom function.

Exercise 4 (4 points)**:**
(*) Let F be a pseudorandom permutation. Consider the fixed-length encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$. $\text{Gen}(1^n)$ outputs $k \leftarrow \{0,1\}^n$. $\text{Enc}_k(m)$, for input $m \in \{0,1\}^{n/2}$, picks $r \leftarrow \{0,1\}^{n/2}$ and outputs $F_k(r||m)$.
Construct algorithm Dec. Prove that Π is cpa-secure. Compare Π to Construction 3.6 from the lecture, discuss advantages and disadvantages of the schemes.

Exercise 5:
Consider the construction of a Feistel cipher for some arbitrary round function

$$f : \{0,1\}^l \times \{0,1\}^t \to \{0,1\}^t$$

with block length $2t$ and r rounds. Let $m \in \{0,1\}^{2t}$ be a message and let c be the encryption of m with round keys $k_1, k_2, \ldots, k_r$ for arbitrary $k_i \in \{0,1\}^l$. Prove, that the *encryption* of c with the round keys $k_r, k_{r-1}, \ldots, k_1$ leads to the message m.
Hint: Remember the difference of the last round.

Exercise 6:
What kind of influence do the following modifications of AES imply:

- We extend the last round of AES in such a way, that it does not differ from the other $r-1$ rounds.
- We remove the SubBytes operation from the algorithm.