Prof. Dr. Johannes Blömer
Nils Löken

May 19th, 2017
submission due: May 30th, 2017: 11 a.m.

# Cryptography - Provable Security

SS 2017

Handout 6

*Exercises marked (*) will be checked by tutors.*

**Exercise 1:**
Prove or refute: the counter mode of operations employing a pseudorandom function has indistinguishable encryptions under chosen-ciphertext attacks (Definition 3.8).

**Exercise 2:**
Let $p(n)$ be a polynomial. Prove that if there exists a pseudorandom function $F$ that, using a key of length $n$, maps $p(n)$-bit inputs to single-bit outputs, then there exists a pseudorandom function that maps $p(n)$-bit inputs to $n$-bit outputs. (Here $n$, as usual, denotes the security parameter.) Give a direct construction, that does not rely on the results from the lecture.

**Hint:** Use a key of length $n^2$, and prove that your construction is secure using a hybrid argument.

**Exercise 3** (8 points)**:**
(*) Given a pseudorandom generator with expansion factor $n+7$, construct a pseudorandom generators with expansion factor $2n$. Prove that your construction is correct and secure.

**Exercise 4** (4 points)**:**
(*) Assume a public-key encryption scheme without decryption errors for single-bit messages. Show that, given $pk$ and a ciphertext $c \leftarrow \mathrm{Enc}_{pk}(m)$, it is possible for an unbounded adversary to determine the message $m$ with probability 1. This shows that perfectly secret public-key encryption is impossible.

**Exercise 5:**
Show that for any CPA-secure public-key encryption scheme, the size of the ciphertext after encrypting a single bit is superlogarithmic in the security parameter. (That is, for $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$ it must hold that $|\mathrm{Enc}_{pk}(b)| = \omega(\log n)$ for any $b \in \{0,1\}$).

**Hint:** If not, the range of possible ciphertexts is only polynomial in size.