Prof. Dr. Johannes Blömer
Nils Löken

May 13th, 2016
submission due: May 24th, 2016: 11 a.m.

Cryptography - Provable Security

SS 2016

Handout 6

Exercises marked (*) and (**) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1:
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 2 (8 points)**:**
(**) Consider the construction of pseudorandom generators with arbitrary polynomial expansion factors $p(n)$ from PRGs with expansion factor $n+1$. In the lecture you have shown that for the special case $p(n) = n+2$ hybrid distributions H_n^0, H_n^2 are indistinguishable by probabilistic polynomial time distinguishers. Now, prove that

a) hybrid distributions H_n^0 and H_n^1 are indistinguishable by probabilistic polynomial time distinguishers, and

b) hybrid distributions H_n^1 and H_n^2 are indistinguishable by probabilistic polynomial time distinguishers.

Exercise 3:
Prove or refute: the counter mode of operations employing a pseudorandom function has indistinguishable encryptions under chosen-ciphertext attacks (Definition 3.8).

Exercise 4 (4 points)**:**
(**) Assume a public-key encryption scheme for single-bit messages with no decryption error. Show that, given pk and a ciphertext $c \leftarrow \mathrm{Enc}(b)$, it is possible for an unbounded adversary to determine b 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 $|\mathrm{Enc}(b)| = \omega(\log n)$ for any $b \in \{0,1\}$).

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