Prof. Dr. Johannes Blömer
Nils Löken

May 20th, 2016
submission due: May 31st, 2016: 11 a.m.

Cryptography - Provable Security

SS 2016

Handout 7

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

Exercise 1:
Prove that if there exists a pseudorandom generator, then there exists a 1-way function (Theorem 5.18 from the lecture).

Hint: Prove that a PRG with expansion factor $2n$ is a 1-way function.

Exercise 2 (4 points)**:**
(**) Consider Theorem 7.5 from the lecture and the corresponding multiple messages eavesdropping game $\mathrm{PubK}^{\mathrm{mult}}_{\mathcal{A},\Pi}(n)$. Extend at first the experiment to the CCA setting in an appropriate way. Next, assume that the underlying public-key encryption scheme Π is CCA-secure. Does it necessarily have multiple indistinguishable encryptions under a chosen ciphertext attack? Prove your answer formally.

Exercise 3:
Consider the hybrid encryption scheme defined in the lecture. Let Π be a CCA-secure public-key encryption scheme (define an appropriate experiment for this) and Π' be a CCA-secure private-key encryption scheme. Is the hybrid construction Π^{hyb} instantiated using Π and Π' also CCA-secure? Prove your answer formally. I. e., does an analogue for Thoerem 7.11 hold for CCA security?

Exercise 4 (4 points)**:**
(**) Let $G = G_0 \times G_1$ be a pseudorandom generator with expansion factor $2n$ such that for all $x \in \{0,1\}^n$

$$G(x) = (G_0(x) \| G_1(x)) \quad \text{and} \quad |x| = |G_0(x)| = |G_1(x)|.$$

Prove that

$$\tilde{G}(x) = (G_0(G_0(x)) \| G_0(G_1(x)) \| G_1(G_0(x)) \| G_1(G_1(x)))$$

is a pseudorandom generator with expansion factor $4n$.