Prof. Dr. Johannes Blömer
Nils Löken

May 26th, 2017
submission due: June 6th, 2017: 11 a.m.

Cryptography - Provable Security

SS 2017

Handout 7

Exercises marked (*) will be checked by tutors.

Exercise 1:
Prove that if pseudorandom generators exist, then one-way functions exist (Theorem 6.18 from the lecture).

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

Exercise 2 (4 points)**:**
(*) Consider Theorem 7.5 from the lecture and the corresponding multiple messages eavesdropping game $\mathrm{PubK}_{A,\Pi}^{\mathrm{mult}}(n)$.

a) Extend the experiment to the CCA setting (Def. 3.8) in an appropriate and meaningful way.

b) 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 $4n$.