Prof. Dr. Johannes Blömer
Nils Löken, Peter Günther

April 22th, 2016
submission due: May 3rd, 2016: 11 a.m.

Cryptography - Provable Security

SS 2016

Handout 3

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

Exercise 1:
Let G be a pseudorandom generator with expansion factor $l(n)$. Fix a family $\{S_n\}_{n\in\mathbb{N}}$ of sets such that for every $n \in \mathbb{N}$ it holds $S_n \subset \{0,1\}^n$ and $|S_n| = 2^{\lceil \frac{n}{2} \rceil}$ and consider the following construction:

$$\tilde{G}(s) := \begin{cases} 0^{l(|s|)} & \text{if } s \in S_{|s|} \\ G(s) & \text{otherwise} \end{cases}$$

Prove that $\tilde{G}$ is a pseudorandom generator.

Exercise 2 (4 points)**:**
(**) Let G be a pseudorandom generator where $|G(s)| > 2 \cdot |s|$. Consider the following construction:

$$G_1(s) := G(s||0^{|s|}).$$

Is G_1 necessarily a pseudorandom generator?
Hint: Exercise 1 might be helpful to argue about G_1.

Exercise 3:
Let M be a $l \times n$ matrix over the field $\mathbb{Z}_2$ with $l > n$. We treat bit strings as column vectors over $\mathbb{Z}_2$ and vice versa. Consider the function

$$\begin{array}{rccc} G_M: & \{0,1\}^n & \to & \{0,1\}^l \\ & s & \mapsto & M \cdot \vec{s} \end{array}$$

Is G_M a pseudorandom generator? Prove your answer.

Exercise 4 (4 points)**:**
(*) Let $n \geq 1$ be an integer. Fix $X_1, X_2, Y_1, Y_2 \in \{0,1\}^n$ with $X_1 \neq X_2$,. Compute probabilities

$$\Pr_{f\leftarrow \mathrm{Func}_n}[f(X_1) \oplus f(X_2) = Y_1 \oplus Y_2], \quad \Pr_{f\leftarrow \mathrm{Func}_n}[f(X_1) \oplus Y_1 = Y_2], \quad \Pr_{f\leftarrow \mathrm{Func}_n}[f(X_1 \oplus X_2) = f(0^n)].$$

Here f is chosen uniformly at random from the set Func_n. Explain your answers.

Exercise 5 (4 points)**:**
(**) Let $n \geq 1$ be an integer. Fix $X_1, X_2, Y_1, Y_2 \in \{0,1\}^n$ with $X_1 \neq X_2$,. Compute probabilities

$$\Pr_{\pi\leftarrow P_n}[\pi(X_1) = Y_1 \wedge \pi(X_2) = Y_2], \qquad \Pr_{\pi\leftarrow P_n}[\pi(X_1) \oplus \pi(X_2) = Y_1].$$

Here π is chosen uniformly at random from the set P_n of all permutations on $\{0,1\}^n$.

Exercise 6:
Let G be a pseudorandom generator and define $G'(s)$ to be the output of G truncated to $|s|$ bits. Prove that the keyed function $F_k(x)$ given by

$$F_k(x) := G'(k) \oplus x,$$

where $k \leftarrow \{0,1\}^{|x|}$, is not pseudorandom.

Exercise 7:
Let G be a pseudorandom generator with expansion factor $l(n) = n+1$ and F a pseudorandom function. For each of the following encryption schemes, state whether the scheme is cpa-secure. In each case, the shared key is a random $k \leftarrow \{0,1\}^n$:

- To encrypt $m \in \{0,1\}^{2n+2}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$ and compute

$$\mathrm{Enc}_k(m) := \langle G(k) \oplus m_1, G(k+1) \oplus m_2 \rangle .$$

- To encrypt $m \in \{0,1\}^{n+1}$, choose a random $r \leftarrow \{0,1\}^n$ and compute

$$\mathrm{Enc}_k(m) := \langle r, G(r) \oplus m \rangle .$$

- To encrypt $m \in \{0,1\}^n$ compute

$$\mathrm{Enc}_k(m) := m \oplus F_k(0^n).$$

- To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose $r \leftarrow \{0,1\}^n$ and compute

$$\mathrm{Enc}_k(m) := \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle .$$

Exercise 8 (4 points)**:**
(**) Consider the following keyed function $F_k(x) : \{0,1\}^{n^2+n} \times \{0,1\}^n \to \{0,1\}^n$, where the key and the input are interpreted as follows. The first n^2 bits of k describe a $n \times n$ matrix M over $\mathbb{Z}_2$. The last n bits of k as well as the input are interpreted as vectors $\vec{v}$ and $\vec{x}$ over $\mathbb{Z}_2$ respectively. The function value is then computed as

$$F_k(\vec{x}) := M \cdot \vec{x} + \vec{v}.$$

Prove that this function is not a pseudorandom fuction.