Universität Leipzig
Institute of Computer Science
Winter term 2026/2027

Andreas Maletti

Exercises for the lecture

Cryptography

Exercise Sheet 5

for the exercise on November 20th, 2026

Exercise 5.1

Decrypt the ciphertext available on my website. (will not be done during exercise)

Exercise 5.2

Is $\equiv_{\mathsf{PPT}}$ (§4.6) an equivalence relation? Prove your answer. (If you do not want to work with ensembles, then prove that the asymptotic almost equality $\simeq$ is an equivalence relation.)

Exercise 5.3

Let G_1 and G_2 be pseudorandom generators with expansions p_1 and p_2. Is G given for all $s \in \{0,1\}^*$ by

$$G(s) = G_2\big(G_1(s)\big)$$

again a pseudorandom generator?
(In other words, can we chain pseudorandom generators to extend pseudorandom sequences arbitrarily?)

Exercise 5.4

Let G be a pseudorandom generator with expansion polynomial $p = 4x + 2$. For $n \in \mathbb{N}$ and $s = s_1 \cdots s_n$ with $s_1, \ldots, s_n \in \{0,1\}$ let

$$s_{\mathsf{o}} = \begin{cases} s_1 s_3 s_5 \cdots s_{n-2} & \text{if } n \text{ is odd} \\ s_1 s_3 s_5 \cdots s_{n-3} & \text{otherwise} \end{cases} \quad \text{and} \quad s_{\mathsf{e}} = \begin{cases} s_2 s_4 s_6 \cdots s_{n-2} & \text{if } n \text{ is even} \\ s_2 s_4 s_6 \cdots s_{n-1} & \text{otherwise} \end{cases}$$

be the words of length $\lfloor \frac{n}{2} \rfloor$ consisting of the suitable number of odd (respectively, even) positions in s. Additionally, let $\mathrm{prefix}(s, \ell)$ be the prefix of s of length ℓ. Determine whether the following function G' is a pseudorandom generator. For every $s \in \{0,1\}^*$

$$G'(s) = \mathrm{prefix}\big(G(s_{\mathsf{o}}) \oplus G(s_{\mathsf{e}}), 2\,|s|\big) \ .$$

Exercise 5.5

Let G be a pseudorandom generator with expansion polynomial $p = 3x$. For $n \in \mathbb{N}$ and $s = s_1 \cdots s_{2n}$ with $s_1, \ldots, s_n \in \{0,1\}$ let

$$s_{\mathsf{L}} = s_1 \cdots s_n \qquad \text{and} \qquad s_{\mathsf{R}} = s_{n+1} \cdots s_{2n}$$

be the left- and right-half of s, respectively. Determine whether the following functions are pseudorandom generators, where we assume that they are defined for even length inputs only. For every $s \in \{0,1\}^{2n}$

(a) $G'(s) = G(s_{\mathsf{L}}) \oplus G(s_{\mathsf{R}})$

(b) $G''(s) = s_{\mathsf{L}} \cdot G\big((s_{\mathsf{L}} \oplus s_{\mathsf{R}}) \cdot s_{\mathsf{R}}\big)$, where $\cdot$ is concatenation.