Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 4

will be discussed on November 24, 2020

Exercise 4.1

Is $\equiv_{\text{PPT}}$ an equivalence relation (see §4.6 of the lecture)?

Exercise 4.2

Let G_1 and G_2 be pseudorandom generators (PRG). Is G given by

$$G(s) = G_2(G_1(s)) \text{ for all } s \in \{0,1\}^*$$

again a pseudorandom generator?

Exercise 4.3

Let G be a pseudorandom generator with polynomial $p(n) = 3n$. For $s \in \{0,1\}^{2n}$ define $s_L = s_1 \dots s_n$ and $s_R = s_{n+1} \dots s_{2n}$, the left and right half of s.

(a) Is G' defined by $G'(s) = G(s_L) \oplus G(s_R)$ a pseudorandom generator?

(b) Is G' defined by $G'(s) = s_L \mid\mid G((s_L \oplus s_R) \mid\mid s_R)$ a pseudorandom generator?

Assume that G' is only defined for even n.