Technische Universität München (I7) **Winter term 2018/2019**
Dr. M. Luttenberger / S. Jaax **2018/11/13**

Cryptography – Homework 2

Discussed on Tuesday, 20th November, 2018.

Exercise 2.1 Negligible Functions

(a) Show that the following two definitions are equivalent:

i) $\varepsilon(n)$ is negligible if and only if $\forall a \in \mathbb{N} \exists N \in \mathbb{N} \forall n > N : \varepsilon(n) < n^{-a}$.

ii) $\varepsilon(n)$ is negligible if and only if $\forall$polynomials q $\exists N \in \mathbb{N} \forall n > N : \varepsilon(n) < \frac{1}{|q(n)|}$

(b) Let $\varepsilon_1 : \mathbb{N} \to \mathbb{R}^+, \varepsilon_2 : \mathbb{N} \to \mathbb{R}^+$ be negligible functions and let $p : \mathbb{N} \to \mathbb{R}^+$ be a polynomial in $\mathbb{R}$. Show that $f : \mathbb{N} \to \mathbb{R}^+$ with $f(n) = \varepsilon_1(n) + \varepsilon_2(n)$ and $g : \mathbb{N} \to \mathbb{R}^+$ with $g(n) = p(n) \cdot \varepsilon_1(n)$ are also negligible functions.

(c) Prove: If $\varepsilon_0, \varepsilon_1, \ldots$ is a family of negligible functions $\varepsilon_i \colon \mathbb{N} \to \mathbb{R}^+$ and $p \colon \mathbb{N} \to \mathbb{N}$ is a polynomial, then f with $f(n) := \sum_{i=0}^{n} \varepsilon_i(n)$ need not be negligible anymore.

Exercise 2.2 Pseudorandom Generators

- Let $f \colon \{0,1\}^* \to \{0,1\}$ be any DPT-computable function.

  Show that $G_f(x) = x||f(x)$ is no PRG.
- Use a similar argument to show that also the follwing is not a PRG:

  Let $m \in \mathbb{N}$ and $a, c \in \mathbb{Z}_m$.

  – For simplicity, let $m = 2^n$ so that we may identify $\mathbb{Z}_m$ with $\{0,1\}^n$.

  For $x \in \{0,1\}^n$, let $f(x) = (a \cdot x + c) \bmod m$, and $G(x, 1^{n \cdot s}) = f(x)||f(f(x))|| \ldots ||f^s(x)$.

Exercise 2.3 Pseudorandom Generators II

Let G be a PRG of stretch $l(n) = 2n$.

(a) Show that there exists an *exponential time* distinguisher $\mathcal{D}$ with:

$$\left| \Pr_{x \overset{u}{\in} \{0,1\}^n}[\mathcal{D}(1^n, G(x)) = 1] - \Pr_{y \overset{u}{\in} \{0,1\}^{2n}}[\mathcal{D}(1^n, y) = 1] \right| \geq 1 - 2^{-n}$$

(b) Determine the success probability of the following $\mathcal{D}$:

- Input: $y \in \{0,1\}^{l(n)}$ and 1^n.
- Generate $x' \overset{u}{\in} \{0,1\}^n$.
- Compute $y' = G(x')$.
- Return 1 if $y = y'$; else return 0.

Exercise 2.4

(a) Show that PRFs with $l_{\text{out}}(n) \cdot 2^{l_{\text{in}}(n)} \leq n$ exist (unconditionally!).

(b) Let G be a PRG of stretch $l_G(n) = 2n$.

Split $G(k) =: G_0(k)||G_1(k)$ into two n bit strings.

Set $F_k^{(1)}(0) := G_0(k)$ and $F_k^{(1)}(1) := G_1(k)$. Show: $F^{(1)}$ is a PRF with $l_{\text{in}}(n) = 1$ and $l_{\text{out}}(n) = n$.