Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2018/12/11

Cryptography – Questionnaire 2

Name: _____

Matr.: _____

"One/Two-liners" – 5P

Exercise 2.1 **2P**

How many *injective* functions $f : \{0,1\}^n \to \{0,1\}^{2n}$ are there? Give a closed-form expression!

Answer: _____

Exercise 2.2 **1P**

State the name of a computationally secret fixed-length ES such that every PPT-algorithm $\mathcal{A}$, which, on input 1^n and ciphertext c, tries to compute the parity of the original message m, succeeds with probability exactly $1/2$. (The parity of a message $x_1||\ldots||x_n \in \{0,1\}^n$ is just the xor of all bits $\bigoplus_i x_i$)

Answer: _____

Exercise 2.3 **2P**

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a DPT-computable function such that f is a permutation on $\{0,1\}^n$ for all n.

Show that $G : \{0,1\}^n \to \{0,1\}^{2n}$ with $G(x) = f(x)||x \oplus f(x)$ is never a PRG of stretch $l(n) = 2n$. To this end, briefly describe a PPT distinguisher, and (roughly) estimate its success probability.

Questions—1P each = 5P

	true	false
$f\colon \mathbb{N} \to \mathbb{R}$ is negligible with $f(n) := \begin{cases} \frac{1}{2^n} & \text{if } n \text{ is even,} \\ \frac{1}{\log_2(n)} & \text{otherwise.} \end{cases}$.	☐	☐
Let $f\colon \mathbb{N} \to \mathbb{N}$ and $g\colon \mathbb{N} \to \mathbb{N}$. If $(f \circ g)$ is negligible, then f and g are both negligible.	☐	☐
If $\varepsilon : \mathbb{N} \to \mathbb{R}^+$ is negligible, then $f : \mathbb{N} \to \mathbb{R}^+$ with $f(n) := \varepsilon(\lceil \log n \rceil)$ is also negligible.	☐	☐
Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a computationally secret fixed-length PPT-ES. Every PPT-algorithm $\mathcal{A}$, which, on input 1^n and ciphertext c, tries to compute the parity of the original message m, succeeds with probability exactly $1/2$.	☐	☐
There exists a PRG G with strech $l(n) > n$ such that $\Pr\left[\mathsf{Win}_{n,G}^{\text{IndPRG}}(\mathcal{D})\right] = \frac{1}{2}$ for every probabilistic exponential time distinguisher $\mathcal{D}$ and all $n \in \mathbb{N}$.	☐	☐