Cryptography for Computer Scientists 2018/19 — Oct 10, 2018

Exercises 2

Stefan Dziembowski — MIM UW

Exercise 1: Semantically-secure encryption implies that P≠NP

Prove that if semantically-secure encryption exists then P≠NP.

Exercise 2: One-way functions

Let f and g be one-way functions that are *length preserving*, i.e., for every $x \in \{0,1\}^*$ we have that $|f(x)| = |g(x)| = |x|$. For h_i's defined as below decide if they are one-way functions (if the answer is "yes" then give a proof, and otherwise provide a counterexample).

1. $h_1(x) := f(x) \oplus g(x)$,
2. $h_2(x_1||x_2) = f(x_1)||g(x_2)$ (where $|x_1| = |x_2|$),
3. $h_3(x) = f(x)||g(x)$, and
4. $h_4(x) := f(g(x))$.

Exercise 3: PRG output extension

Let G be a pseudorandom generator that extends its input by one bit (i.e. it has expansion factor ℓ' such that $\ell'(n) = n + 1$). Let ℓ be any polynomial such that for every $n \in \mathbb{N}$ we have $\ell(n) > n$. Define $H : \{0,1\}^* \to \{0,1\}^*$ by the following procedure (for any $t \in \mathbb{N}$):

on input $(x_1^0, \ldots, x_t^0) \in \{0,1\}^t$:
for $i = 1, \ldots, \ell(t)$ **do**
  $(x_1^i, \ldots, x_{t+1}^i) := G(x_1^{i-1}, \ldots, x_t^{i-1})$
return $\left(x_{t+1}^1, \ldots, x_{t+1}^{\ell(t)}\right)$

Prove that G is a pseudorandom generator.

Hint: Use the *hybrid argument*[1].

[1] `https://en.wikipedia.org/wiki/Hybrid_argument_(Cryptography)`