QUANTUM CRYPTOGRAPHY

Master of Logic, University of Amsterdam, June 2022
TEACHERS: Christian Schaffner, Florian Speelman and Sebastian Zur

Practice problem set 4

You do not have to hand in these exercises, they are for practicing only.

Problem 1: A pretty good measurement

You are given one of three states $\rho_0 = |0\rangle\langle 0|$, $\rho_1 = \frac{1}{2}\mathbb{I}$, and $\rho_2 = |1\rangle\langle 1|$, each with equal probability.

- (a) What is the probability of correctly identifying which state you were given (1, 2 or 3) if you use the pretty-good-measurement?
- (b) Can you find a measurement that will give you a better success probability?

Problem 2: Negligible functions

A function $f: \mathbb{N} \to \mathbb{R}$ is called negligible if for any $c \in \mathbb{N}_+$, there exists an integer n_c such that for all $n > n_c$ we have

$$|f(n)| < \frac{1}{n^c}.$$

- (a) Show that $f(n) = 2^{-(\log(n))^2}$ is negligible.
- **(b)** Show that if f(n) and g(n) are negligible, then so is h(n) = f(n) + g(n).
- (c) Similarly, show that if f(n) is negligible, and $g(n) = O(n^d)$ for some $d \in \mathbb{N}$, then so is $h(n) = f(n) \cdot g(n)$. Can you see why negligible functions are useful to bound the success probability of an adversary?

Problem 3: 2-universality

Let $\mathscr{F} = \{f_y : \{0,1\}^n \to \{0,1\}^m\}$ be a 2-universal family of hash functions. For some m' < m, define $\mathscr{F}' = \{f_y' : \{0,1\}^n \to \{0,1\}^{m'}\}$ by $f_y'(x) = f_y(x)_{|m'}$, that is, the first m' bits of $f_y(x)$. Show that \mathscr{F}' is also 2-universal.

Problem 4: A weak seeded extractor

For any $y \in \{0,1\}^n$, define $f_y : \{0,1\}^n \to \{0,1\}^n$ by $f_y(x) = x \oplus y$. Here, \oplus represents the bitwise parity (e.g., $11 \oplus 01 = 10$).

- (a) Show that the family $\mathscr{F} = \{f_y\}$ is 1-universal.
- (b) How could you use \mathscr{F} to build a (k,0)-weak seeded randomness extractor Ext : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ for any k. Is this extractor useful?
- (c) Alice and Bob are impressed by the parameter $\epsilon=0$ in the previous exercise. They decide that if \mathscr{F} can be used for a (k,0)-weak seeded randomness extractor, then certainly it can reasonably be used as a **strong** seeded randomness extractor as well. They define $\operatorname{Ext}(x,y)=f_y(x)$. Do you think this is a good idea? How does Eve's guessing probability change after extraction?

Problem 5: Deterministic extractors on bit-fixing sources

In the lectures, you learned that no deterministic function can serve as an extractor for all random sources of a given length. This doesn't rule out the possibility that a deterministic extractor can work on some restricted class of sources. Consider Alice holding an n-bit source X that fixes t < n bits. These t bits represent the bits that Eve learns about X, and that are therefore not usable by Alice anymore for her cryptographic tasks.

- (a) If Alice knows which t positions are fixed by X, how much randomness can she extract from X?
- (b) Now suppose Alice does not know which bits are compromised (but she does know t). She decides to extract randomness from X by taking the XOR of all of her bits, producing just one output bit. For which values of t is this secure?
- (c) Alice now wants to extract more than one bit of randomness from X (still without knowing which positions are fixed). Her idea is to take subsets of the bits of X, and to treat each subset as its own bit-fixing source. What is the largest number of independent subsources she can take (in terms of n and t), such that it is possible to securely extract a bit of randomness from each subsource?