QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, 2017
TEACHERS: Jan Czajkowski, Yfke Dulek, and Christian Schaffner

Homework problem set 2

Please hand in your solutions to these exercises in digital form (typed, or scanned from a neatly hand-written version) through Moodle no later than **Friday June 23, 20:00h**.

Problem 1: Min-Entropy Chain rule for cq-states

Let $\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x$ be a cq-state. Prove the following chain rule:

$$\mathrm{H}_{\min}(X|E) \geq \mathrm{H}_{\min}(X) - \log|E| \, .$$

Hint: Use the fact that $0 \leq \rho_E^x \leq \mathbb{1}$.

Problem 2: 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 $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ 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 $\mathrm{Ext}(x, y) = f_y(x)$. Do you think this is a good idea? How does Eve's guessing probability change after extraction?