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: injective functions are collapsing

Show that an injective function is collapsing, i.e. give a proof of Lemma 2 of our recent paper. You can ignore the oracles $\mathcal{O}$ in the statement of Lemma 2 and in Definition 1.

Problem 3: 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) Show that the family $\mathscr{F} = \{f_y\}$ is not 2-universal.

(c) 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 $0 \leq k \leq n$? Is this extractor useful?

(d) Alice and Bob have a k-source X for some $k < n$. They are impressed by the parameters in the previous subexercise, and decide to use $\mathscr{F}$ to build a strong seeded randomness extractor as well. They know they should not expect to securely extract more than k bits of key, so they define $\mathrm{Ext}(x,y) := (x_1 \oplus y_1, ..., x_k \oplus y_k)$, that is, the first k bits of $f_y(x)$. (From the exercise session, they know how to show that this set of functions is still 1-universal). Do you think this is a good idea? Give a lower bound to Eve's probability of guessing the key.