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.