QUANTUM CRYPTOGRAPHY

Master of Logic, University of Amsterdam, 2018

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 Canvas no later than **Friday June 23, 20:00h**.

Problem 1: Injective functions are collapsing

Show that an injective function is collapsing, i.e. give a proof of Lemma 4 of our recent paper. You can ignore the oracles $\mathcal{O}$ in the statement of Lemma 4 and in Definition 3.

Problem 2: XOR-universal hash functions

A family $\mathscr{F} = \{f_y : \{0,1\}^n \mapsto \{0,1\}^m\}$ is *XOR universal* if for all $x \neq x'$ and all z,

$$P_y[f_y(x) \oplus f_y(x') = z] = \frac{1}{2^m}.$$

In words, the XOR of any pair of function values is uniformly distributed over the output space.

(a) Show that if a function family $\mathscr{F}$ is 2-universal, then it is XOR-universal.

(b) Show that the converse of the previous subexercise does not hold by showing that there exists a function that is XOR-universal, but not 2-universal. (**Hint:** start with an arbitrary 2-universal function and alter it slightly, so that it is not 2-universal anymore.)

(c) In the lecture notes, it is shown that a 2-universal function family $\mathscr{F}$ can be used to construct a strong seeded randomness extractor (see Theorem 4.3.1; the leftover hash lemma). Is the proof (for the case with no side information) still valid if a XOR-universal function family is used to build the extractor?

Problem 3: 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 4: SARG04 Quantum Key Distribution Protocol

A protocol propose in 2004 is a seemingly innocent variation to BB84 protocol, but has some advantages in realistic implementation in QKD. A again sends randomly one of four states used in BB84, and B measures randomly in either horizontal-vertical or diagonal basis. However, instead of revealing the basis at the sifting stage, A announces publicly one of four pairs $\{|0\rangle, |+\rangle\}$, $\{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$, $\{|1\rangle, |-\rangle\}$. The announced pair contains a state send by A but it is not revealed which one. The convention is that $|+\rangle$, $|-\rangle$ are assigned logical value 0 while $|0\rangle$, $|1\rangle$ logical value 1. To understand how secret key can be generated consider situation in which A sends $|1\rangle$ and announces the pair $\{|1\rangle, |+\rangle\}$, with probability $1/2$ B measures in the computational basis and he gets $|1\rangle$. He is not sure, however which state from the announced pair caused this results so he discard it. With probability $1/2$ he measures in the Hadamard basis in which case half of the times he gets $|+\rangle$ and half of the time he gets $|-\rangle$. Only in this last case he is sure that the state send by A was $|1\rangle$ and he writes down the bit value 0. What portion of the bits is discarded. Analyze the security of the protocol under random basis attacks. If the pairs of states had been announced before sending the qubit, could E perform a more powerful intercept and resend attack?

Problem 5: Intermediate-basis attack

Analyse the intercept-and-resend attack on the BB48 protocol in which Eve measures in the basis intermediate between the computational and Hadamard bases.