

## 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: XOR-universal hash functions

A family  $\mathcal{F} = \{f_y : \{0, 1\}^n \mapsto \{0, 1\}^m\}$  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  $\mathcal{F}$  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  $\mathcal{F}$  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 2: 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:

$$H_{\min}(X|E) \geq H_{\min}(X) - \log |E|.$$

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

### Problem 3: Intermediate-basis attack

Analyze the intercept-and-resend attack on BB84 protocol in which Eve measures in the basis intermediate between the computational and Hadamard bases, i.e.  $\{|\frac{\pi}{4}\rangle, |\frac{5\pi}{4}\rangle\}$ , where  $|\frac{\pi}{4}\rangle := \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ , and  $|\frac{5\pi}{4}\rangle := -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$ . What is the error rate this attack induces?

### Problem 4: SARG04 Quantum Key Distribution Protocol (Exercise 4.3.4 from [the lecture notes to Quantum Information 1/2](#))

A protocol proposed in 2004 is a seemingly innocent variation to BB84 protocol, but has some advantages in realistic implementation of QKD. Alice again sends randomly one of four states used in BB84, and Bob measures randomly in either computational or Hadamard basis. However, instead of revealing the basis, Alice announces publicly one of four pairs  $\{|0\rangle, |+\rangle\}$ ,  $\{|0\rangle, |-\rangle\}$ ,  $\{|1\rangle, |+\rangle\}$ ,  $\{|1\rangle, |-\rangle\}$ . The announced pair contains the state sent by Alice 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 Alice sends  $|1\rangle$  and announces the pair  $\{|1\rangle, |+\rangle\}$ , with probability  $1/2$  Bob measures in the computational basis and he gets  $|1\rangle$ . He is not sure, however, which state from the announced pair caused this result so he discards it. With probability  $1/2$  he measures in the Hadamard basis in which case half of the time he gets  $|+\rangle$  and half of the time he gets  $|-\rangle$ . Only in the latter case he is sure that the state sent by A was  $|1\rangle$  and he writes down the bit value 1. What portion of the bits is discarded. Analyze the security of the protocol under random basis intercept-and-resend attack. If the pairs of states had been announced before sending the qubit, could Eve perform a more powerful intercept-and-resend attack? In realistic implementations of QKD we want to send single photons in polarization states, production of single photons is rather hard though. One dangerous thing that might happen is that Alice, instead of one, sends two photons in the same state, giving Eve a copy of the sent state. Explain how does using SARG04 help with this issue.

**Problem 5: 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.