COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 8

This exercise sheet is designed to help you review the concepts discussed in the lecture and explore some additional interesting results that were not covered in the lecture. Exercises marked with * will have solutions provided after the exercise session, while those marked with ⧫ will be the main focus during the exercise session. You are encouraged to discuss with other students, and ask for help if you get stuck for too long.

1. (⧫, $*$) **Thinking adversarially**
   Let's imagine that we are Eve and we observe someone trying to implement a QKD protocol. Because QKD is hard they might try to cut corners in their implementations. In this problem we present three "candidate" protocols for key distribution. It is your job to try to break them! For each protocol, choose the step in which there is a mistake which allows you to break security.
   Protocol 1:

   (a) Alice generates bit strings x, θ.

   (b) Alice prepares the bits x encoded in the basis θ, and sends the resulting qubits to Bob.

   (c) Alice announces the basis string θ.

   (d) Bob measures in the bases corresponding to θ and obtains x.

   Protocol 2:

   (a) Alice generates bit strings x, θ.

   (b) Alice generates 2-qubit states $|x_i\rangle\,|\theta_i\rangle$ with the first qubit in the standard basis and the second in the Hadamard basis.

   (c) Alice send the 2-qubit states to Bob.

   (d) Bob announces receipt of the states.

   (e) Bob generates a string $\hat{\theta}$ and measures the second qubit in either the standard or Hadamard basis depending on $\hat{\theta}$, getting an output string χ.

   (f) Alice and Bob announce θ and χ over an authenticated channel.

   (g) If $\chi_i = \theta_i$ then Bob measures the corresponding first qubit in the standard basis, obtaining a bit $\hat{x}_i$.

   (h) Alice and Bob discard all data where $\chi_i \neq \theta_i$, and now share the string $\hat{x}$.

   Protocol 3:

   (a) Alice creates a string of EPR pairs and sends one half of each to Bob.

(b) Bob generates a string θ and measures his half of each pair according to the value of θ.

(c) Alice generates a string $\hat{\theta}$ and similarly measures her half of the EPR pairs.

(d) Bob announces over an authenticated channel that he received and measured his qubits

(e) Alice and Bob compare θ and $\hat{\theta}$ over an authenticated channel

(f) Alice and Bob use the measurement results obtained for each $\theta_i = \hat{\theta}_i$ as their key.

2. (*) **Generating key using using an anonymous message board**
Imagine that Alice and Bob have discovered an anonymous message board in the hallway. It allows both Alice and Bob to post messages in such a way that no adversary can ever find out who the message came from. In particular, Alice and Bob each have a one-way secret channel for transmitting messages to the board. They can ask the board to erase all messages, or to publish in a random order the messages it has received that have not been erased. In other words, when asked to publish the messages, the board simply creates in a random order a list of messages that has sent to it and has not been erased, without indicating a sender, and announces it publicly (so that any eavesdropper Eve can also see the announcement). Alice and Bob come up with the following candidate protocols.

- Protocol I
  - Both Alice and Bob send a random bit to the board, and Alice tells Bob that she has done the first step in a classical authenticated channel (CAC).
  - After receiving Alice's confirmation that the first step is done, Bob asks the board to publish the messages.
  - If Alice's bit is the same as Bob's bit, then Bob asks the board to erase the messages and then tells Alice to restart from the first step in a CAC.
  - If Alice's bit is different than Bob's bit then both Alice and Bob set Alice's bit as the next bit of their key. Alice asks the board to erase the bits and tells Bob to repeat from the first step until they have n bits of key in a CAC.
- Protocol II
  - Alice starts by asking the board to erase the messages and then sending two fresh random bits on the board, and asks the board to publish the messages.
  - If the second bit on the board is 0 they take the first bit as a key bit and they repeat step 1.
  - If the second bit on the board is 1 they take the XOR of the two bits as a key bit and start from step 1 but now Bob writes instead of Alice.
  - Alice or Bob execute this alternating protocol until they have n bits of key.

At the end of the day, we want that Alice and Bob both share an n-bit key (correctness), but Eve is ignorant about the key (security).

(a) Is Protocol I is perfectly correct? Is Protocol II is perfectly correct?

(b) Which of the protocols is secure?

(c) Can you come up with a different protocol that generates key?