COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 8

1. **Thinking adversarially**

   Protocol 1: Alice makes a mistake in step (c). Because she announces her basis to Bob (and Eve) before Bob tells her that he received and measured his states, Eve can intercept all Alice's qubits, measure them in the right bases (because she has θ) and then re-prepare qubits in the same bases (or even re-use the same qubits, since measurement in the correct basis doesn't change the eigenstate), and send them to Bob.

   Protocol 2: The protocol fails at step (c). Because the bases in which Alice prepares her qubits are known in advance, Eve can intercept them upon transmission, measure them (discovering the strings x, θ), and then re-prepare the states correctly to pass them to Bob. Then Eve has the same information as Alice over the system and hence can easily reproduce the key.

   Protocol 3: This protocol is not secure. It fails in step (f) because Alice and Bob do not check what fraction of their measurement results coincide. This allows Eve to perform the following attack: She intercepts Alice's qubits, and then creates another string of EPR pairs of which she sends one half of each to Bob. After Alice and Bob measure in bases $\theta, \hat{\theta}$ and announce these bases, Eve measures her halves of the pairs she shares with Alice in θ and the halves of the pairs she shares with Bob in $\hat{\theta}$. Because she also knows when $\theta_i = \hat{\theta}_i$ she now shares a key with Bob and a key with Alice, both of whom think they share a key with each other. Note that the protocol is also not correct since Alice and Bob both hold completely uncorrelated bit strings.

2. **Generating key using using an anonymous message board**

   (a) Both protocols are perfectly correct. In Protocol I, because Alice and Bob each know their own bit, they can set the key as described. In Protocol II, when the board publishs the messages, both party can see it, and thus they can set the key as describes.

   (b) Protocol I is secure. Because if the two bits on the board are different, Eve does not know which one is Alice's and hence her best possible stratergy is to just pick one of the two bits as a potential key bit, on average she guesses the correct bit 50% of the time. This makes the protocol secure. Protocol II is not secure because Eve also sees the two bits when the board publishs the messages.

   (c) You can try a lot of interesting things, for example, you can let both Alice and Bob send a random bit to the board, and ask the board to publish the messages. If the two bits are different, they know their own bit, so they know if Alice's bit is the first bit. They can set the key according to whether Alice's bit is the first bit.