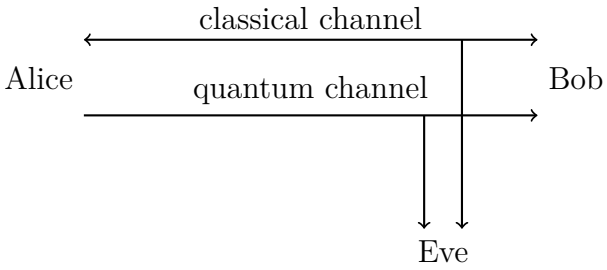
**Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He**

# Exercise 12
# - Proposed Solution -

Friday, February 2, 2018

## Solution of Problem 1

Before we solve the problem at hand, we take a look at our scenario: man-in-the-middle attack. In general this means that an evesdropper can monitor messages into a communication channel. Here, we have two channels.




The classical channel is authenticated, i.e., Eve can listen to this channel, but cannot change the messages. Eve *can* listen to the quantum channel and inject qubits.

The quantum channel has the following properties. An evesdropper Eve must perform measurements in order to observe the photon transmissions between Alice and Bob. Eve will introduce errors in the data, because they have the state that Eve used for the measurement. If Bob uses the correct basis to perform his measurements there will be a 25% chance that he will have measured the wrong value.

As an example, let us consider that Alice sends a photon corresponding to $|\rightarrow\rangle$ and Bob uses the same basis $+$. If Eve uses $+$, then the photon is passed through correctly and Bob measures the photon correctly. However, if Eve uses $\times$, then she will measure $|\nwarrow\rangle$ and $|\nearrow\rangle$ equally likely. The photons that pass to Bob will have one of these orientations and will therefore half the time be measured correctly as $|\rightarrow\rangle$ and half the time incorrectly. Combining the two possible choices of basis that Eve has, causes Bob to have a 25% chance of measuring the incorrect value. Any eavesdropping introduces a higher error rate in the communication between Alice and Bob. If Alice and Bob test their data for discrepancies over the conventional channel, they will detect any eavesdropping.

**a)** Bob's and Alice's selected bases must be equal. Look at the table and read the one-time pad of 16 bits as

$$0011\,1001\,1100\,1001\,.$$

Bob sends his chosen bases to Alice, and Alice tells Bob which ones were chosen correctly. Alternatively Alice tells Bob which bases she used for preparation of the qubits.

**b)** Eight useful qubits are sent over the classical channel, and thereby sacrified, in order to check if there is an eavesdropper. This step must be authenticated, but needs not to be encrypted. Suppose they were all intercepted, so there would be a probability of 25% for each qubit that it gave the wrong measurement for Bob. Hence, the probability of no discrepancies, i.e. the probability that Eve was lucky, is $\left(\frac{3}{4}\right)^8 \approx 0.1$. In practice Alice and Bob would want to use more bits to get a better estimate of the risk, but if they went ahead with these their eight non-sacrifice qubits (the even numbered ones) would give a one-time pad of

$$0101\,1001\,.$$

**c)** For $n$ check qubits, the probability that Eve will not be detected for any of them is $\left(\frac{3}{4}\right)^n$. For the 99.9% certainty we are looking for $n$ large enough that $\left(\frac{3}{4}\right)^n < 0.001 \;\Rightarrow\; n \geq 25$. It follows that Alice and Bob need 45 *useful* qubits: 20 for the pad and 25 sacrificed for detecting interceptions. Since on average only half the qubits are useful, they need 90 qubits altogether.

**d)** If Eve intercepts more than 10%, then on average at least 2.5% of the qubits will show a discrepancy. The probability of no discrepancy in $n$ check qubits is $0.975^n$, so for 95% certainty we want $0.975^n < 0.05$.

$$n > \frac{\log 0.05}{\log 0.975} \approx 120\,.$$

For 140 useful qubits (20 for the pad, 120 to check), Alice and Bob need 280 qubits.