Homework 6: 26 October 2017
Traitement Quantique de l'Information

Exercise 1 *Bennett 1992 Protocol for quantum key distribution*

The analysis of BB84 shows that the important point is the use of non-orthogonal states. BB92 retains this characteristic but simply uses two states instead of four.

Encoding by Alice: Alice generates a random sequence $e_1, \ldots, e_N$ of bits that she keeps secret. She sends to Bob the quantum bits $|0\rangle$ if $e_i = 0$ and $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ if $e_i = 1$. The state of the quantum bit sent by Alice is thus $H^{e_i}|0\rangle$.

Decoding by Bob: Bob generates a random sequence $d_1, \ldots, d_N$ of bits that he keeps secret. He measures the received quantum bit $H^{e_i}|0\rangle$ in the basis $\{|0\rangle, |1\rangle\}$ (Z basis) or in the basis $\{H|0\rangle, H|1\rangle\}$ (X basis) according to the value $d_i = 0, 1$. So the measurement basis of Bob is $\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}$. He registers $y_i = 0$ if the outcome is $H^{d_i}|0\rangle$ (i.e. if it is $|0\rangle$ or $H|0\rangle$) and $y_i = 1$ if the outcome is $H^{d_i}|1\rangle$ (i.e. if it is $|1\rangle$ or $H|1\rangle$).

Public discussion phases: Bob announces on a public channel his measurement outcome $y_1, \ldots, y_N$.

Secret key generation: You will propose it in question 3).

1) Prove that just after Bob's measurements:

$$P(y_i = 0|e_i = d_i) = 1 \qquad P(y_i = 1|e_i = d_i) = 0$$
$$P(y_i = 0|e_i \neq d_i) = \frac{1}{2} \qquad P(y_i = 1|e_i \neq d_i) = \frac{1}{2}$$

2) Deduce that $P(e_i = 1 - d_i|y_i = 1) = 1$.
Hint: You can convince yourself that this is necessarily the case from the above probabilities; but you can also prove it more in detail by using Bayes' rule $P(A|B) = \frac{P(A \cup B)}{P(B)} = \frac{P(B|A)P(A)}{P(B)}$.

3) Based on the result in 2) propose a secret key generation scheme. Show that the secret key has length $\approx N/4$ (discuss with your neighbors).

4) Propose a security check (discuss with your neighbors).

5) Suppose that Eve performs the following attack: she captures a photon and makes a measurement in a random basis Z or X. Let $E_i = 0, 1$ denote her choice Z or X for the measurement basis.
– If Eve chooses $E_i = 0$ her resulting state after the measurement is $|0\rangle$ or $|1\rangle$. When she gets $|0\rangle$ she decides to send $|0\rangle$ to Bob; but when she gets $|1\rangle$ she decides to send $H|0\rangle$ to Bob (because she knows Alice never sent $|1\rangle$).

– If Eve chooses $E_i = 1$ her resulting state after the measurement is $H|0\rangle$ or $H|1\rangle$. When she gets $H|0\rangle$ she decides to sends $H|0\rangle$ to Bob; but when she gets $H|1\rangle$ she decides to send $|0\rangle$ to Bob (because she knows Alice never sent $H|1\rangle$).
Prove that in the presence of Eve we always have

$$P(e_i = 1 - d_i | y_i = 1) = \frac{3}{4}$$

Hints:

- Use Bayes' rule

$$P(e_i = 1 - d_i | y_i = 1) = \frac{P(y_i = 1 | e_i = 1 - d_i) P(e_i = 1 - d_i)}{P(y_i = 1)}.$$

- Use

$$\begin{aligned} P(y_i = 1 | e_i = 1 - d_i) = P(y_i = 1 | e_i = 1 - d_i, E_i = e_i) P(E_i = e_i) \\ + P(y_i = 1 | e_i = 1 - d_i, E_i \neq e_i) P(E_i \neq e_i) \end{aligned}$$

  and a similar method to compute $P(y_i = 1)$.

- You will also need the following equation (discuss it with your neighbors and justify it)

$$\begin{aligned} &P(y_i = 1 | d_i, e_i, E_i) \\ &\quad = P\big(y_i = 1 | \text{Eve's meas is } H^{E_i}|0\rangle\big) \cdot P\big(\text{Eve's meas is } H^{E_i}|0\rangle \, | d_i, e_i, E_i\big) \\ &\qquad + P\big(y_i = 1 | \text{Eve's meas is } H^{E_i}|1\rangle\big) \cdot P\big(\text{Eve's meas is } H^{E_i}|1\rangle \, | d_i, e_i, E_i\big). \end{aligned}$$

  Write down each probability in bra-ket notation according to the measurement postulate (or the Born rule).