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

Exercise 1 *Bennett 1992 Protocol for quantum key distribution*

1) When $d_i = e_i$, Bob measures the qubit in the same basis as the preparation basis used by Alice. In other words if $e_i = d_i = 0$ the transmitted qubit state is $|0\rangle$ and the measurement is in the Z-basis then this yields a measurement result $|0\rangle$ with probability 1. A similar argument holds if $e_i = d_i = 1$ and the transmitted qubit is $H|0\rangle$ and the measurement is in the X-basis which yields a measurement result $H|0\rangle$ with probability 1. Thus when $d_i = e_i$ we certainly have $y_i = 0$. So

$$P(y_i = 0|e_i = d_i) = 1, \qquad P(y_i = 1|e_i = d_i) = 0.$$

When $d_i \neq e_i$ then, for example $e_i = 1$ and $d_i = 0$, the transmitted state is $|\psi\rangle = H|0\rangle$ but the measurement is done in the Z-basis which results in $|0\rangle$ or $|1\rangle$ with equal probability because $|\langle 0|\psi\rangle|^2 = |\langle 1|\psi\rangle|^2 = (1/\sqrt{2})^2 = 1/2$. So

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

2) We observe from the above analysis that $y_i = 1$ only when $d_i \neq e_i$. Indeed if $y_i = 1$ then Alice and Bob know that $e_i = 1 - d_i$ for sure, i.e.

$$P(e_i = 1 - d_i|y_i = 1) = 1.$$

This can be proved more formally from Bayes' rule:

$$P(e_i = 1 - d_i|y_i = 1) = \frac{P(y_i = 1|e_i = 1 - d_i)P(e_i = 1 - d_i)}{P(y_i = 1)} = \frac{\frac{1}{2} \times \frac{1}{2}}{\frac{1}{4}} = 1$$

where for the denominator we used

$$\begin{aligned} P(y_i = 1) &= P(y_i = 1|e_i = d_i)P(e_i = d_i) + P(y_i = 1|e_i \neq d_i)P(e_i \neq d_i) \\ &= 0 \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}. \end{aligned}$$

Here we have assumed that $P(e_i \neq d_i) = P(e_i = d_i) = \frac{1}{2}$.

3) The secret key is then generated as follows: Alice and Bob reveal the y_i's and keep the $e_i = 1 - d_i$ such that $y_i = 1$ as their secret bits. The other e_i and d_i are discarded. The length of the resulting secret key is around $N \times P(y_i = 1) = N/4$, a quarter of the length of the main sequence.
We observe a few differences with respect to BB84. First the common secret bits are here constituted from a subset of the encoding and decoding bits. Second the length of the secret key is halved with respect to BB84. However the main advantage of BB92 over BB84 is that in BB92 we manipulate only two non-orthogonal states instead of four in BB84.

4) Alice and Bob can do a security check by exchanging a small fraction $\epsilon N/4$, $0 < \epsilon \ll 1$of the secure bits via public channel. If the test is successful they keep the rest of the common substring secure: thus they have succeeded in generating a common secure string. If there is no attack from Eve's side and the transmission channel is perfect, then as we explained we have $e_i = 1 - d_i$ whenever $y_i = 1$. The test should check that

$$P(e_i = 1 - d_i | y_i = 1) = 1.$$

In practice Alice and Bob check that

$$\#(i \text{ such that } e_i = 1 - d_i \text{ given that } y_i = 1) = \epsilon N/4$$

which means that the empirical probability is one.

5) Let us summarize the attack in other words: Alice sends $H^{e_i} |0\rangle$ and Eve gets $H^{E_i} |z_i\rangle$ upon measurement with probability $|\langle z_i| H^{E_i+e_i} |0\rangle|^2$; Eve then sends $H^{E_i+z_i} |0\rangle$ and Bob gets $H^{d_i} |y_i\rangle$ upon measurement with probability $|\langle y_i| H^{d_i+E_i+z_i} |0\rangle|^2$. Hence, we have

$$\begin{aligned} P(y_i|d_i, e_i, E_i) &= \sum_{z_i=0,1} P\big(y_i|d_i, \text{Eve's meas is } H^{E_i}|z_i\rangle\big) \cdot P\big(\text{Eve's meas is } H^{E_i}|z_i\rangle|d_i, e_i, E_i\big) \\ &= \sum_{z_i=0,1} |\langle y_i| H^{d_i+E_i+z_i} |0\rangle|^2 \cdot |\langle z_i| H^{E_i+e_i} |0\rangle|^2. \end{aligned} \tag{1}$$

Since Eve has no information on e_i and d_i (the Bernoulli choices by Alice and Bob), we shall assume that Eve's choice of E_i is independent of e_i and d_i so that $P(E_i = e_i) = P(E_i \neq e_i) = 1/2$ and $P(E_i = d_i) = P(E_i \neq d_i) = 1/2$.

Using Bayes' rule

$$\begin{aligned} P(e_i = 1 - d_i | y_i = 1) &= \frac{P(y_i = 1|e_i = 1 - d_i) P(e_i = 1 - d_i)}{P(y_i = 1)} \\ &= \frac{P(y_i = 1|e_i = 1 - d_i) \times \frac{1}{2}}{P(y_i = 1)} \end{aligned}$$

We expand the denominator into

$$\begin{aligned} P(y_i = 1) = {} & P(y_i = 1|d_i = E_i, E_i = e_i) P(d_i = E_i) P(E_i = e_i) \\ & + P(y_i = 1|d_i \neq E_i, E_i = e_i) P(d_i \neq E_i) P(E_i = e_i) \\ & + P(y_i = 1|d_i = E_i, E_i \neq e_i) P(d_i = E_i) P(E_i \neq e_i) \\ & + P(y_i = 1|d_i \neq E_i, E_i \neq e_i) P(d_i \neq E_i) P(E_i \neq e_i) \\ = {} & \frac{1}{4}\big(P(y_i = 1|d_i = E_i, E_i = e_i) + P(y_i = 1|d_i \neq E_i, E_i = e_i) \\ & + P(y_i = 1|d_i = E_i, E_i \neq e_i) + P(y_i = 1|d_i \neq E_i, E_i \neq e_i)\big). \end{aligned}$$

From (1), we have

$$P(y_i = 1 | d_i = E_i, E_i = e_i) = \sum_{z_i=0,1} |\langle 1| H^{z_i} |0\rangle|^2 \cdot |\langle z_i|0\rangle|^2 = 0,$$

$$P(y_i = 1 | d_i \neq E_i, E_i = e_i) = \sum_{z_i=0,1} |\langle 1| H^{1+z_i} |0\rangle|^2 \cdot |\langle z_i|0\rangle|^2 = \frac{1}{2}, \tag{2}$$

$$P(y_i = 1 | d_i = E_i, E_i \neq e_i) = \sum_{z_i=0,1} |\langle 1| H^{z_i} |0\rangle|^2 \cdot |\langle z_i| H |0\rangle|^2 = \frac{1}{4}, \tag{3}$$

$$P(y_i = 1 | d_i \neq E_i, E_i \neq e_i) = \sum_{z_i=0,1} |\langle 1| H^{1+z_i} |0\rangle|^2 \cdot |\langle z_i| H |0\rangle|^2 = \frac{1}{4}$$

and thus we continue to write

$$P(y_i = 1) = \frac{1}{4}\big(0 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4}\big) = \frac{1}{4}.$$

For the numerator, we expand $P(y_i = 1 | e_i = 1 - d_i)$ into

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

and reuse the results (2) and (3) to see that

$$P(y_i = 1 | e_i = 1 - d_i) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{3}{8}.$$

Putting these results all together we obtain:

$$P(e_i = 1 - d_i | y_i = 1) = \frac{P(y_i = 1 | e_i = 1 - d_i) \times \frac{1}{2}}{P(y_i = 1)} = \frac{\frac{3}{8} \times \frac{1}{2}}{\frac{1}{4}} = \frac{3}{4}.$$