CS191 – Fall 2014
Homework 5 solutions

1. ***The six state protocol.*** Let the tuple (a, b, e) represent the basis that Alice, Bob and Eve measure/prepare in. After sifting the only events that are kept (out of the 27 possible events) have one of the following combinations of measurements and preparations:

$$(Z,Z,Z),(X,X,X),(Y,Y,Y),(Z,Z,Y),(Z,Z,X),(X,X,Z),(X,X,Y),(Y,Y,X),(Y,Y,Z)$$

Out of these, the occurrence of any of the first three cannot be detected by Alice and Bob in the error rate estimation step. Therefore, the probability of having a detectable intervention by Eve is $p_1 = 6/9$. Then, the probability of creating a disagreement is $p_2 = 1/2$ since even if Eve measured in the wrong basis and sent a state orthogonal to the one Alice sent, Bob will still have probability $1/2$ of getting a measurement outcome that is the same as the state Alice sent. Therefore the error rate that Alice and Bob will estimate in this case where Eve attacks every qubit individually with the intercept resend attack is $\epsilon = p_1 \times p_2 = 1/3$.

2. ***Entanglement-based protocol.***

   (a) To write $|\Psi\rangle$ in the new basis, we write each $|0\rangle_i = \frac{1}{\sqrt{2}}(|+\rangle_i + |-\rangle_i$ and each $|1\rangle_i = \frac{1}{\sqrt{2}}(|+\rangle_i - |-\rangle_i$, for $i = A, B$. Then combining terms and canceling, we get:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle_A \otimes |+\rangle_B + |-\rangle_A \otimes |-\rangle_B)$$

   (b) Note that both Alice's measurement result and Bob's measurement result are random events if they measure in different bases. If Alice and Bob measure in the same basis, the outcome is still random, but they are guaranteed to get the same outcome. I've made random choices in cases where the outcome is random and so the following table may not be exactly the same as yours.

Alice basis choice	σ_z	σ_x	σ_x	σ_z	σ_z	σ_z	σ_x	σ_z	σ_x	σ_z
Bob basis choice	σ_x	σ_z	σ_x	σ_x	σ_z	σ_x	σ_z	σ_z	σ_x	σ_z
Alice measurement result	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$
Alice bit value	0	0	1	0	1	1	1	0	0	1
Bob measurement result	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$
Bob bit value	0	0	1	1	1	0	0	0	0	1
Keep after sifting?	No	No	Yes	No	Yes	No	No	Yes	Yes	Yes

   (c) Now Alice and Bob get a non-ideal, or noisy, state

$$\rho = \frac{p}{4} I_4 + (1-p)\,|\Psi\rangle\langle\Psi|\,,$$

   Then we are told that Alice measures in the σ_x basis and gets the result $|+\rangle$. To calculate the possible results that Bob will get we need to calculate the post-measurement state after Alice's result. Recall that the post-measurement state is determined as:

$$\rho^{PM} = \frac{P_i \rho P_i}{\mathrm{tr}\,(P_i \rho P_i)},$$

   where P_i is a projector onto the eigenspace corresponding to the measurement result that was obtained. In this question $P_i = |+\rangle^A\langle+| \otimes I^B$, which is a projector onto the $|+\rangle$ state on Alice's qubit (since this is the result she got) and the identity on Bob's qubit indicates that nothing is done on it. Calculating the numerator for the post measurement state,

$$\begin{aligned}
& (|+\rangle^A\langle+| \otimes I^B)\rho(|+\rangle^A\langle+| \otimes I^B) \\
= \; & \frac{p}{4}(|+\rangle^A\langle+| \otimes I^B) I_4 (|+\rangle^A\langle+| \otimes I^B) + (1-p)(|+\rangle^A\langle+| \otimes I^B)\,|\Psi\rangle\langle\Psi|\,(|+\rangle^A\langle+| \otimes I^B) \\
= \; & \frac{p}{4}\,|+\rangle^A\langle+| \otimes I^B + \frac{(1-p)}{2}\,|+\rangle^A\langle+| \otimes |+\rangle^B\langle+|\,, \qquad (1)
\end{aligned}$$

where the second term was arrived at by expanding $|\Psi\rangle\langle\Psi|$ as

$$\begin{aligned}|\Psi\rangle\langle\Psi| \;=\; \frac{1}{2}\Big(&|+\rangle^A\langle+|\otimes|+\rangle^B\langle+| \\ &+|+\rangle^A\langle-|\otimes|+\rangle^B\langle-| \\ &+|-\rangle^A\langle+|\otimes|-\rangle^B\langle+| \\ &+|-\rangle^A\langle-|\otimes|-\rangle^B\langle-|\Big).\end{aligned}$$

Having done this it should be clear that only one of those components (the first one) will survive when we project with P_i from the left and right.
So Eq. (1) is the numerator for the post measurement state. To normalize it we need to find the denominator, which is the trace of Eq. (1). Some useful properties of the trace to keep in mind are:

$$\begin{array}{lll}\mathrm{tr}\,(ABC) = \mathrm{tr}\,(CAB) = \mathrm{tr}\,(BCA) & & \text{Cyclic property}\\ \mathrm{tr}\,(A+B) = \mathrm{tr}\,(A) + \mathrm{tr}\,(B) & & \text{Linearity}\\ \mathrm{tr}\,(A\otimes B) = \mathrm{tr}\,(A)\mathrm{tr}\,(B) & & \text{Behavior under tensor product}\end{array}$$

Using these,

$$\begin{aligned}&\mathrm{tr}\,(\frac{p}{4}|+\rangle^A\langle+|\otimes I^B + \frac{(1-p)}{2}|+\rangle^A\langle+|\otimes|+\rangle^B\langle+|)\\ =\;& \frac{p}{4}\mathrm{tr}\,(|+\rangle^A\langle+|\otimes I^B) + \frac{(1-p)}{2}\mathrm{tr}\,(|+\rangle^A\langle+|\otimes|+\rangle^B\langle+|)\\ =\;& \frac{p}{2} + \frac{(1-p)}{2} = \frac{1}{2}\end{aligned}$$

Therefore the post measurement state is:

$$\rho^{PM} = \frac{p}{2}|+\rangle^A\langle+|\otimes I^B + (1-p)|+\rangle^A\langle+|\otimes|+\rangle^B\langle+| \tag{2}$$

Now we can answer the questions about Bob's possible outcomes.

i. Suppose Bob also measures in the σ_x basis. What are the probabilities of his possible outcomes? We know his outcomes are $|+\rangle$ or $|-\rangle$. To find their probabilities we recall that the probability of a particular outcome with projector P_i, given a state ρ, is:

$$\mathrm{tr}\,(P_i\rho) = \mathrm{tr}\,(P_i\rho P_i).$$

(Why are these equal? You should make sure you understand why). This time we are asking for probabilities for Bob's measurement outcomes, so the relevant P_i are

$$\begin{aligned}P_+ &= I^A\otimes|+\rangle^B\langle+|\\ P_- &= I^A\otimes|-\rangle^B\langle-|.\end{aligned}$$

Therefore,

$$\begin{aligned}\Pr\{+\} \;&=\; \mathrm{tr}\,(P_+\rho^{PM}) = \frac{p}{2}\mathrm{tr}\,(|+\rangle^A\langle+|\otimes|+\rangle^B\langle+|) + (1-p)\mathrm{tr}\,(|+\rangle^A\langle+|\otimes|+\rangle^B\langle+|) = \frac{p}{2}+(1-p)\\ &=\; 1-\frac{p}{2},\\ \Pr\{-\} \;&=\; \mathrm{tr}\,(P_-\rho^{PM}) = \frac{p}{2}\mathrm{tr}\,(|+\rangle^A\langle+|\otimes|-\rangle^B\langle-|) + (1-p)(0)\\ &=\; \frac{p}{2}.\end{aligned}$$

Note that due to the noise in the state (proportional to p), Bob's result is not guaranteed to be perfectly correlated to Alice's any longer.

ii. Now suppose Bob measures in the σ_z basis. What are the probabilities for his possible outcomes? In this case his outcomes are $|0\rangle$ or $|1\rangle$, and the relevant measurement operators are

$$P_0 = I^A \otimes |0\rangle^B \langle 0|,$$
$$P_1 = I^A \otimes |1\rangle^B \langle 1|.$$

Therefore,

$$\begin{aligned}
\Pr\{0\} &= \mathrm{tr}\left(P_0 \rho^{PM}\right) = \frac{p}{2}\mathrm{tr}\left(|+\rangle^A \langle +| \otimes |0\rangle^B \langle 0|\right) + (1-p)\mathrm{tr}\left(|+\rangle^A \langle +| \otimes |0\rangle^B \langle +| \langle 0|+\rangle\right) \\
&= \frac{p}{2} + (1-p)\frac{1}{2} = \frac{1}{2}, \\
\Pr\{1\} &= \mathrm{tr}\left(P_1 \rho^{PM}\right) = \frac{p}{2}\mathrm{tr}\left(|+\rangle^A \langle +| \otimes |1\rangle^B \langle 1|\right) + (1-p)\mathrm{tr}\left(|+\rangle^A \langle +| \otimes |1\rangle^B \langle +| \langle 1|+\rangle\right) \\
&= \frac{p}{2} + (1-p)\frac{1}{2} = \frac{1}{2}.
\end{aligned}$$

So if Alice and Bob choose the wrong basis, the noise in the entangled state doesn't affect the probabilities of measurement outcome results.

3. ***Universal hashing for privacy amplification.*** Alice and Bob share the binary string $\mathbf{x} = (1,0,0,1,1,1,0,1,0,0)^\mathsf{T}$, and decide on the Topelitz hashing matrix:

$$\begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}.$$

(a) Alice and Bob's privacy amplified bit string is

$$\begin{aligned}
\mathbf{y} &= T\mathbf{x} \\
&= (0,1,1,0,1,1,0)^\mathsf{T}
\end{aligned}$$

(b) Suppose Eve's bit string she has eavesdropped is $\mathbf{x}' = (1,1,0,1,0,1,1,1,1,0)^\mathsf{T}$. We've flipped four random bits of $\mathbf{x}$ to get this. If Eve were to hash this eavesdropped string, she would get

$$\begin{aligned}
\mathbf{y}' &= T\mathbf{x}' \\
&= (1,1,0,0,1,1,1)^\mathsf{T}
\end{aligned}$$

The hamming distance between $\mathbf{y}$ and $\mathbf{y}'$ is 3.

(c) Now we will flip fewer bits in Eve's bit string to give her more information about the string Alice and Bob share.

i. $l = 3$: $\mathbf{x}' = (0,0,0,1,0,1,0,1,1,0)^\mathsf{T} \Rightarrow \mathbf{y}' = T\mathbf{x}' = (0,0,0,0,0,0,1)^\mathsf{T}$. The hamming distance between $\mathbf{y}$ and $\mathbf{y}'$ in this case is 5.

ii. $l = 2$: $\mathbf{x}' = (1,0,0,1,1,0,1,1,0,0)^\mathsf{T} \Rightarrow \mathbf{y}' = T\mathbf{x}' = (0,1,1,1,0,0,1)^\mathsf{T}$. The hamming distance between $\mathbf{y}$ and $\mathbf{y}'$ in this case is 4.

iii. $l = 1$: $\mathbf{x}' = (1,0,0,0,1,1,0,1,0,0)^\mathsf{T} \Rightarrow \mathbf{y}' = T\mathbf{x}' = (0,0,1,1,1,1,0)^\mathsf{T}$. The hamming distance between $\mathbf{y}$ and $\mathbf{y}'$ in this case is 2.

We see that even when one bit is flipped, it is difficult for Eve to have full knowledge of the privacy amplified bit string. Of course, note that if you flip different bits to obtain $\mathbf{x}'$ in each of the cases above you may compute different hamming distances. But the chance that $\mathbf{y}$ and $\mathbf{y}'$ have zero hamming distance will be very small.