Intro Quantum Computing
CSCI/PHYS 3090
CU Boulder Spring 2020
HW 4 Solutions

Problem 1

A

No, the onetime pad scheme should not be modified. As long as the pad y is randomly selected, then $m \oplus y$ is also random. Eve does not know the pad y, so for $y = 0^l$, $m \oplus y = m \oplus 0^l = m$, the ciphertext will appear random from Eve's perspective. In fact, it would weaken the scheme to exclude 0^l as this lowers your randomness and actually provides Eve with (slightly) more information, since she *knows* that 0^l is not possible as a pad.

B

Though $Pr_y[y = 0^l] = \frac{1}{2^l} > 0$, it is exponentially low with respect to the size l and so not a realistic exploit against this scheme. Although the output ciphertext is identical to the message, the one-time pad encryption scheme could have produced this ciphertext from any possible message of the same length and so someone trying to decipher the message would not learn much by knowing the ciphertext without knowing the key.

Problem 2

Assume without loss of generality that Alice and Bob both use type-1. With probability $1 - p$, Eve does nothing and does not affect Bob's measurement. With probability p, Eve *does* measure, but half the time she will measure in the type-1 basis and does not mess up Bob's qubit. The other half of the time, Eve measures in the type-H basis and if she does, there is a 50 % chance that she messes up Bob's qubit. This is because whether Eve ends up projecting the state into $|+\rangle$ or $|-\rangle$, the following is true:

$$|\langle 0|+\rangle|^2 = |\langle 1|+\rangle|^2 = |\langle 0|-\rangle|^2 = |\langle 1|-\rangle|^2 = \frac{1}{2}$$

This means that Bob still has a 50 % chance of measuring whichever state Alice initially sent. In summary, Eve messes up Bob's measurement with probability $p/4$ and thus the probability that Bob's measurement equals Alice's bit is $1 - p/4$.

Problem 3

$Pr[\text{Bob chooses wrong basis } l \text{ times}] = \frac{1}{2^l}$, which can be seen from two somewhat different perspectives:

Counting: There are 2^l ways that Bob can choose the l basis choices. Only 1 of these is the string that always disagrees with Alice. Thus $1/2^l$.

Probability: For $1 \leq i \leq l$, we have Pr[Bob measures qubit i incorrectly] $= 1/2$. Each decision is independent so Pr[Bob measures qubit all incorrectly] is the product of the probability of getting each individual decision incorrectly, thus $(1/2)^l = 1/2^l$.
In this case $l = 100$ so we have that the probability p that Bob measures in the wrong basis every time is

$$p = \left(\frac{1}{2}\right)^{100} \approx 8 \times 10^{-31}$$

Problem 4

Suppose that Bob would like to differentiate between states $|0\rangle$ and $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ using the orthogonal basis $\{|\phi_0\rangle, |\phi_1\rangle\}$. In order that Bob have absolute certainty that Alice prepared state $|\psi\rangle$ when he measures the state $|\phi_1\rangle$, then the conditions $\langle\phi_1|0\rangle = 0$ and $\langle\phi_1|\psi\rangle \neq 0$ must hold. Generically we can express the state as $|\phi_1\rangle = c|0\rangle + d|1\rangle$, but then $\langle\phi_1|0\rangle = 0 \implies c\langle 0|0\rangle + d\langle 0|1\rangle = c = 0$. In order for $|\phi_1\rangle$ to be normalized, we require that $|d| = 1$, and so that requires that $|\phi_1\rangle = |1\rangle$. However, for $\langle\phi_1|\phi_0\rangle = 0$, as required by the orthogonal basis convention, then we have that the state $|\phi_0\rangle$ is fixed to be $|0\rangle$. Therefore, we find that $\langle\phi_0|\psi\rangle = \alpha \neq 0$, which means that Bob can measure the state $|\phi_0\rangle$ when Alice prepares the state $|\psi\rangle$. It is therefore not possible for Bob to construct any orthogonal basis such that he can distinguish perfectly between Alice preparing state $|0\rangle$ and $|\psi\rangle$.