Homework 3

1 Problem 1

Consider the following scheme for signing single-bit messages. The scheme will be built from a one-way function F. The secret key is x_0, x_1, two inputs to F. The public key is $y_0 = F(x_0), y_1 = F(x_1)$.

To sign a message b using the secret key, simply output x_b. To verify, simply apply F to x_b, and check that the result is y_b.

Your goal will be to show that this signature scheme is secure in the following sense: the adversary is given y_0, y_1, and is allowed to make a single quantum query to the signing function. That is, it sends $\sum_{b,z} \alpha_{b,z}|b, z\rangle$ and gets in return $\sum_{b,z} \alpha_{b,z}|b, z \oplus x_b\rangle$. Then, it must produce valid signatures on two distinct messages. Since messages are only single bits, this means that the adversary must produce $(0, x_0'), (1, x_1')$ such that $F(x_0') = y_0$ and $F(x_1') = y_1$. (Notice that there many be multiply valid signatures for any message, and we allow the adversary to produce any of them).

Show that if there exists an adversary A that breaks the security of this signature scheme, then there is an adversary B that can break the security of the one-way function F. The probability B wins must be at least 1/4 the probability A wins.

Hint: consider a hybrid experiment where the b registers of A's query is measured.

2 Problem 2

Recall the basic quantum money scheme seen in class: a banknote is the state $|\phi_{a,b}\rangle$, where $|\phi_{0,b}\rangle = |b\rangle$ and $|\phi_{1,b}\rangle = \frac{1}{\sqrt{2}}(|0\langle + (-1)^b|1\rangle)$. The serial number is (a, b). To verify a supposed banknote $|\psi\rangle$ given the serial number (a, b), simply perform the projective measurement in the basis $|\phi_{a,0}\rangle, |\phi_{a,1}\rangle$, and check that the result is b.

Prove that the probability of cloning $|\phi_{a,b}\rangle$ is at most $3/4$

Care is needed in the proof, since invalid states will still pass verification with non-zero probability. For example, if the adversary produces 2 copies of $|0\rangle$ but the serial number is $(1, 0)$, then the adversary will pass both verifications simultenously with probability $1/4$. Moreover, the two states the adversary produces could be entangled. For example, it could produce $\frac{1}{\sqrt{2}}(|0, 0\rangle + |1, 1\rangle)$.

So precisely, your goal is to prove the following. The adversary is defined by a unitary U over two qubits. The adversary is given $|\phi_{a,b}\rangle|0\rangle$ for a random choice of a, b. It then applies U. Finally, the resulting state is measured in the basis $\{|\phi_{a,0}\rangle \otimes |\phi_{a,0}\rangle, |\phi_{a,0}\rangle \otimes |\phi_{a,1}\rangle, |\phi_{a,1}\rangle \otimes |\phi_{a,0}\rangle, |\phi_{a,1}\rangle \otimes |\phi_{a,1}\rangle\}$ to obtain two bits (b', b''). The adversary wins if $b = b' = b''$. Show that for any U, the probability of winning is at most $3/4$.

3 Problem 3

- Suppose instead of getting a single copy of $|\phi_{a,b}\rangle$, you actually are given two copies $|\phi_{a,b}\rangle \otimes |\phi_{a,b}\rangle$, and now your goal is to produce 3 copies of the state. Design a cloner with the best success probability you can in this setting.
- Now suppose you are given n copies, and your goal is to produce $n + 1$. Devise an algorithm whose success probability approaches 1 as n goes to infinity.
- Show that, for any $n < \infty$, no algorithm can succeed with probability exactly 1.