Practice Exam Solutions

1. These questions are to some extent ambiguous to me (I have little time to write this up so don't have a chance to ask for clarification) but the idea of this BB84 protocol is clear. It is provably secure. You can just focus on what happens during the protocol instead of the questions below.

   (a) All qubits are collapsed to Z eigenstates. Expected: among all qubits, Bob choose the right basis for 1/2 of them (1/2 can be check qubits); 1/2 of these are originally X eigenstates (but now Z eigenstate because of Eve). Bob measures them in X basis so only 1/2 outcomes match. In conclusion: 1/8 (of the total number of qubits) differ from the proper value.

   (b) I don't understand the problem statement.

   (c) Again I'm not sure what the question means. The probability that Eve is undetected is exponentially small in the total number of qubits (Chernoff bound) no matter what α is. One mismatch means Eve is listening in (given that the quantum channel is noiseless).

2. (a) Denote encoded $|0\rangle$ as $|\tilde{0}\rangle$ and $|1\rangle$ as $|\tilde{1}\rangle$. Denote $e^{-i\theta Z/2} = Z_\theta$.

   Notice that $Z^{\otimes 4}|\tilde{0}\rangle = |\tilde{0}\rangle, Z^{\otimes 4}|\tilde{1}\rangle = |\tilde{1}\rangle$. So the encoded state is invariant under $Z^{\otimes 4}$.

   Recall that $Z_\theta = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z$, so $Z_\theta|0\rangle = e^{-i\theta/2}|0\rangle, Z_\theta|1\rangle = e^{i\theta/2}|1\rangle$. Notice that every term in the code has equal number of 0 and 1: phases cancel out. So the encoded state is also invariant under $Z_\theta^{\otimes 4}$.

   (b) It is not hard to observe that these two codewords have the following property: if you rewrite them in X basis the form keeps the same (just $|0\rangle \to |+\rangle, |1\rangle \to |-\rangle$). This means they are also invariant under $X_\theta^{\otimes 4}$, according to (a).

   (c) Same for Y.

   (d) Invariant.

   This means the given encoding protects against collective Pauli rotations.

3. (a) Pauli operators anticommute. $S^2 = \frac{1}{4}(4I\otimes I + \{X,Y\}\otimes\{X,Y\} + \text{other anticommutators}) = I \otimes I$.

   (b) $S|00\rangle = |00\rangle, S|01\rangle = |10\rangle, S|10\rangle = |01\rangle, S|11\rangle = |11\rangle$. Define $|\phi\rangle \equiv a|0\rangle + b|1\rangle, |\psi\rangle \equiv c|0\rangle + d|1\rangle$. $S|\phi\rangle \otimes |\psi\rangle = S(ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle) = ac|00\rangle + ad|10\rangle + bc|01\rangle + bd|11\rangle = |\psi\rangle \otimes |\phi\rangle$. S swaps tensor producted qubits.

   (c) $S|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) = -|\Psi\rangle$. Singlet is a -1 eigenstate of S.

   (d) Does nothing. Triplets are +1 eigenstates of S.

   (e) Recall that singlet and triplets span the two-qubit Hilbert space. Any pure two-qubit state $|\psi\rangle = \alpha|t\rangle + \beta|\Psi\rangle$ where $|t\rangle$ is its projection onto the triplet space. By (c) and (d), $S|\psi\rangle = \alpha|t\rangle - \beta|\Psi\rangle$. So $\frac{S+I}{2}|\psi\rangle = \alpha|t\rangle, \frac{S-I}{2}|\psi\rangle = \beta|\Psi\rangle$. That is, the projectors onto the singlet and triplet spaces are respectively $\frac{S-I}{2}$ and $\frac{S+I}{2}$.