Quiz 5

Name: ______________________________ Date: _______________________ I participated today: _____

1. One of the reasons why quantum communication protocols are interesting is that they seem to provide stronger security guarantees than classical information security. In what sense is this true, and in what sense might it be misleading?

2. In a particular (incorrect) implementation of the QKD scheme discussed in lecture (BB84), suppose that the second party (Bob) generates his public bit and sends it to the first party (Alice) before receiving the qubit, and that a third party (Eve) intercepts both public bits and the qubit. How might Eve use this information to eavesdrop on Alice and Bob, i.e., obtain a copy of their shared secret?

3. Give an example (besides those discussed in lecture) where error correction is fundamental to the universality of a phenomenon, process, or technology, or where the lack of error correction limits its reach.

4. Suppose a single-qubit state $a|0\rangle + b|1\rangle$ is encoded using the bit-flip code, producing the state $a|000\rangle + b|111\rangle$. Then, some quantum-mechanical process occurs that flips exactly one of the qubits, resulting in a superposition of each possible outcome given below:

$$x(a|100\rangle + b|011\rangle) + y(a|010\rangle + b|101\rangle) + z(a|001\rangle + b|110\rangle)$$

   (Here, x, y, and z are arbitrary amplitude values.) Can this error be corrected? That is, can the original encoded state $a|000\rangle + b|111\rangle$ be recovered?

5. The Steane code provides bit-flip and phase-flip protection on a single-qubit state across 7 physical qubits. Suppose in a particular quantum computer, whenever an operation is applied, it has a 1% chance of causing a single bit or phase flip. Assuming an implementation of the Steane code requires 4 operations on each qubit, how likely is the error correction to work, that is, not introduce an error itself?