Quiz 5

Name: _*Solution*_____ 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?

   The security guarantees of the quantum information channel in a quantum communication protocol are derived from the principles of quantum mechanics. That is, the security is (theoretically) a physical property of the system, rather than a mathematical property of an algorithm. This is the sense in which the security guarantees seem to be stronger; they are derived from the laws of physics as we know them. In practice however, problems in information security (and in general) are inevitable, so we should not expect systems implementing quantum communication protocols to be "unhackable", or any similar claim.

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?

   In a nutshell, Eve could imitate Bob in the protocol. In cases where the public bits agree, she could decode the secret bit and then re-encode it using the same strategy Alice used before forwarding it to Bob. (It is worth noting that, even without this mistake in the implementation, BB84 is not secure without an authenticated classical channel. If Eve can intercept and freely modify the public bits without Alice and Bob knowing, she can manipulate the protocol to obtain a copy of the 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.

   A very interesting example of error correction being fundamental is in political philosophy. Karl Popper argued that the success of a political system is based not its ability to answer the question, "who should rule?", but that of "how do we remove bad leaders without violence?".

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?

Yes, the error can be corrected in the normal way. The syndrome measurement will find that the first qubit is flipped with probability $|x|^2$, the second with $|y|^2$, and the third with $|z|^2$. After the measurement, the state of the system is now fully described by the case that was observed, and an X gate can be applied to the qubit that was flipped. For example, if the syndrome measurement finds that the second qubit was flipped, the state is $a|010\rangle + b|101\rangle$; applying X to the second qubit gives $a|000\rangle + b|111\rangle$.

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?

A good way to think about this is that each operation has a 99% chance of success. If Steane error correction takes $7 \times 4 = 28$ operations to work, then the overall chance of success is $\frac{99}{100}^{28} \approx 74.5\%$. Obviously, this is not good enough for reliable error correction.