COM-440 reading assignment #2

Due Tuesday December 2nd at 23:59pm.

Micius

For the second reading we fast-track ourselves into the modern age: the quantum space race! The reading is very short, but I encourage you to spend time browsing online resources in order to form a personal opinion on the questions below.

Your complete answer should be at most 2 pages (with standard formatting).

1. Can you guess what "linked quantum state" the researchers "beamed" 1200km apart?

2. Consider the paragraph starting with "Quantum communication is secure because…"? Read carefully the description of the "BB84 protocol" and the "E91" protocol on the Wikipedia page for quantum key distribution. Which of these protocols do you think the article is referring to? Explain why.

3. The article claims "In theory, entangled particles should remain linked at any separation. That can be checked using a classic experiment called a Bell test." Give an example of a "Bell test" using the language from class, and use it to justify the claim made in the article. (You way look up the Wikipedia page for "Bell test".)

4. Give at least two technological challenges that are faced by the implementation of quantum key distribution over large distances, using satellites or otherwise. Which of these challenges do you think will be overcome in the future? (It's ok if the answer is "neither" or "both". Justify your answer.)

5. Form your own opinion about the prospects for quantum key distribution (QKD) to become a widespread technology. Do you think this will ever happen? If so, in what timeframe? Can you give an example of a compelling "use case" for QKD, i.e. a scenario where there could be a real advantage to using QKD over classical cryptographic methods?