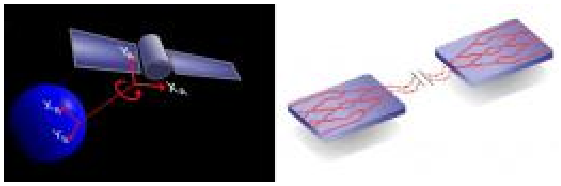
PHYS.ORG

Quantum cryptography protocol doesn’t require shared reference frames (Update)

March 9 2010, by Lisa Zyga



Two scenarios that could use a quantum key distribution protocol that is reference-frame-independent are (left) earth-to-satellite quantum communication and chip-to-chip quantum communication. Image credit: Laing, et al.

(PhysOrg.com) -- Quantum cryptography, which enables two parties to communicate with each other with unconditional security, has begun to be implemented by some governments, banks, and other corporations with high-security requirements. However, certain applications of quantum cryptography, such as satellite links, have proved to be challenging, partly due to a key requirement of quantum key distribution: that the two parties must have a shared reference frame.

But in a new study, physicists Anthony Laing and coauthors from the University of Bristol and the National University of Singapore have developed a protocol that is reference-frame-independent. By generating a secure quantum key between two parties without the need for aligning their reference frames, the new protocol could extend the advantages of quantum cryptography into new domains. Possibilities include earth-to-satellite quantum communication, in which the satellite is rotating and orbiting the Earth, as well as chip-to-chip quantum communication inside a computer and between different computers.

The new protocol requires the two parties, Alice and Bob, to share many pairs of entangled particles. The correlations between particles provide the secret shred key; the trick of the protocol is that the correlations also allow Alice and Bob to measure the purity of their entanglement. Too much impurity alerts them to the possible presence of an eavesdropper, Eve. The useful property of this kind of safeguard against Eve is that the purity should be quite robust in a reference frame that is unknown or even one that varies slowly compared with repetition rate of the quantum signals. This key advantage gives the protocol an edge in other situations such as an environment of intermittent rapid fluctuation where the key is exchanged during the periods of relative stability without the need to realign the reference frame.

As the physicists explain, the new technique greatly simplifies secure quantum encryption in situations that involve moving objects. For example, a beam that connects a satellite and a ground station may encode information in circular polarization, which remains stable. But if the satellite is rotating with respect to the ground station, the linear polarizations will vary, making it difficult to establish a shared reference frame. Similarly, the microchips inside electronic devices are constantly moving around relative to the wavelength of light, and would benefit from a protocol that doesn't require a shared reference frame.

Citation: Quantum cryptography protocol doesn't require shared reference frames (Update) (2010, March 9) retrieved 20 March 2024 from https://phys.org/news/2010-03-quantum-cryptography-protocol-doesnt-require.html