A 4-Photon Entangled State for a Truly Reference-Frame-Independent Quantum Key Distribution Protocol

S. L. Slimani [a], K. Raslan [a], and J. Q. Quach [a]

[a] *Institute for Photonics and Advanced Sensing (IPAS) and School of Physical Sciences, The University of Adelaide, Adelaide SA 5005, Australia.*

Quantum key distribution (QKD) protocols allow for the secure transfer of information between two parties, commonly denoted Alice and Bob, via the generation of a secret key. The security of information transfer in entanglement-based protocols such as the Ekert 91 protocol can be determined by the quantum correlations between the measurements performed by Alice and Bob. Similar to the entanglement-based protocols, prepare and measure protocols such as the BB84 protocol also require a reference frame to be shared between Alice and Bob for the transfer of qubits and subsequent generation of the secret key. Recent research has proposed a reference-frame-independent quantum key distribution (RFI-QKD) protocol to overcome such limitations [1].

Satellite communication offers the advantage of covering a wider terrain than ground-based territories. In 2017, entangled photons were sent from the Micius satellite to a receiver station located 1200 km away [2]. Consequently, entangled photons could be used as a means of providing secure information transfer via earth-to-satellite links for secure long-distance communication. However, current RFI-QKD protocols assume the reference frame shared between Alice and Bob to be fixed or slowly varying with time. Furthermore, a jamming attack, whereby a magnetic field is introduced, can alter the polarization of the photon states received by Alice and Bob. Here we will present a true RFI-QKD protocol which operates at any angle between Alice and Bob's reference frame. We also show that the 4-photon entangled qubit utilized in this protocol is both globally and rotationally invariant thus making our RFI-QKD protocol unaffected by a jamming attack. Our RFI-QKD protocol operates at the Tsirelson bound therefore making it easier for the presence of an eavesdropper to be detected compared to previous entanglement-based QKD protocols.

Figure 1 RFI-QKD protocol utilizing a 4-photon entangled state $|\Psi\rangle$. The state is both locally and globally and rotationally invariant thus making it unaffected by a Faraday rotation.

[1] A. Laing, V. Scarani, J. G. Rarity *et al. Phys. Rev. A* **82**, 1 (2010).

[2] J.Yin, Y. Cao, S-K Liao *et al. Science* **356**, 6343 (2017).