conferenceseries.com

J Laser Opt Photonics 2017, 4:3(Suppl)
DOI: 10.4172/2469-410X-C1-015

2nd International Conference on

Quantum Physics and Quantum Technology

September 25-26, 2017 Berlin, Germany

Time-bin code multi-qubit QKD

June-Koo Kevin Rhee
KAIST, S. Korea

Quantum key distribution (QKD) is a cryptography method for two authenticated parties to share the same random key over a quantum channel. This key is proved to be unconditionally secure that can be used for symmetric encryption such as in a one-time pad encryption. The performance measure can be how fast the keys are generated over how far distance. Recently, a protocol for encoding multi-qubit information in a single photon has been proposed by a modification from BB84. However, there are only few schemes to implement the multi-qubit QKD. In fact, there has been no report that demonstrated more than two-qubit QKD. We proposed an N qubit scheme with a single photon, in which single-photon wave packets are distributed over multiple time bins as shown in the figure below. The wave packets of single photons can represent for separable states that are denoted by the tensor product of the single qubit states. As an example of a two-qubit single photon case, Alice uses two asymmetric Mach-Zehnder interferometers (MZI) with different delays to distribute a single photon wave packet over four time bins. Bob also uses two matched asymmetric MZI to measure Alice's signal with random choice of basis such as in BB84. After the transmission of the quantum state is complete, Alice and Bob compare the transmission bases and the measurement bases of two qubits to extract the secure key. This method can be extended to transmit N-qubit states through N asymmetric MZI. As a result, in situations where the photon counting rate of a single photon detector (SPD) is limited, typically due to the dead time of the single photon avalanche photo detectors, our proposed scheme of the N-qubit protocol in Fig. 1(b) provides a N-fold higher secure key rate than the conventional one-qubit system. In addition, the tolerable qubit error rate (QBER) is increased by use of N qubit protocol, which effectively extends the distribution distance.

rhee.jk@kaist.edu