Quantum Key Distribution

Abstract: Quantum Key Distribution (QKD) uses quantum physics to enable secure communication and information transfer. In the recently completed Beijing-Shanghai quantum network random keys can be securely shared between two users to encrypt large volumes of data. The security of the distribution relies on information being stored as the polarization states of photons.

Introduction

The Shanghai-Beijing integrated space-to-ground quantum network makes use of two different approaches to quantum key distribution [1]. Both relying on the information being saved as the polarization of photons. The first and principle one employed in the backbone and metropolitan-area fiber networks is the Bennett-Brassard protocol (BB84).

For ground-to-space distribution, two photons are entangled in the superposition of the two polarization basis states $|H\rangle$ and $|V\rangle$, corresponding to horizontal and vertical polarization, respectively [2].

The Bennett-Brassard Protocol

The quantum mechanical measurement projects the polarization state of the photon onto one eigenstate of the measurement basis. Thus the information of the polarization is only faithfully transmitted if the polarization is measured in the right basis.

Alice, the first party, uses four laser diodes (LD) and beam splitters (BS) to send signal pulses of diagonal or rectilinear polarization through one quantum channel to Bob, the receiving party.

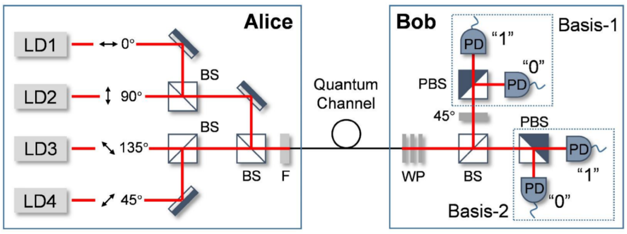

Fig. 1: A typical system for BB84 QKD based on polarization encoding [3].

In Fig. 1, it is shown how Bob randomly splits up the signals to be measured either in Basis-1 or Basis-2. Due to the quarter-wave plate (45°), the polarization of the signals measured in Basis-2 is turned by 45°. Thus the vertically-placed polarizing beam splitter (PBS) effectively projects the incoming signal onto a diagonal polarization basis. Correspondingly, Basis-1 is then the rectilinear measurement basis [3].

After the transfer, Bob saves which photon detector (PD) measured the signal, and publicly sends to Alice the detection bases. Comparison of the bases reveals which signal was send and measured in the same basis, i.e. which signal transmitted the correct polarization and bit of information [4].

The laser diodes do not emit single photons but rather coherent pulses with Poissonian distributed photon numbers. Thus an eavesdropper has the chance to siphon off single photons from the signal and gain information about the transmitted state. A countermeasure to this photon number-splitting (PNS) attack is the splicing of decoy states in-between the signals [5].

Because the decoy states have lower average photon numbers, they are unproportionally more likely to be lost from the channel due to a PNS attack. The different loss statistics of the decoy states would then reveal an eavesdropper.

Entanglement Distribution

The ground-to-space based QKD was first described by Artur Eckert and uses the properties of a Bell-state of two photons [6]. In the satellite, one initial photon travels through a nonlinear optical medium and, through harmonic down-conversion, two entangled photons in the state

$$|\Psi\rangle = [|V\rangle_A |H\rangle_B + e^{i\phi} |H\rangle_A |V\rangle_B]/\sqrt{2} \qquad (1)$$

are produced [7]. The photons are entangled and each are sent to one of the two ground stations to be measured in one of the two basis states $|H\rangle_i$ or $|V\rangle_i$.

The polarization measured by one of the ground stations also determines the state of the other photon. The two-photon state is the secret information, only created at measurement, when the wavefunction collapses [8].

The Beijing-Shanghai Network

The recently completed Chinese quantum network spans over 4,600 km and connects four quantum metropolitan-area networks. It is the first example of commercial use of this technology. On the ground, the network can serve up to 150 users at rates between 11 and 26 kilobits per second (kbps). Its space-to-ground capabilities make the extension to ultralong quantum links feasible and test the non-locality of quantum mechanics on a space scale [2].

References

[1] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science* 560 (2014), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

[2] Yu-Ao Chen et al. “An integrated space-to-ground quantum communication network over 4,600 kilometres”. In: *Nature* 589 (2021), pp. 214–219. DOI: 10.1038/s41586-020-03093-8.

[3] Phichai Youplao and Sukhum Julajaturasiraratn. “A Simulation of Quantum Key Distribution Protocol with Enhancing Ability to Against PNS Attack”. In: *Proceedings of International Conference on Mechanical, Electrical and Medical Intelligent System* (2017).

[4] Won-Young Hwang. “Quantum Key Distribution with High Loss: Toward Global Secure Communication”. In: *Phys. Rev. Lett.* 91 (2003), p. 057901. DOI: 10.1103/PhysRevLett.91.057901.

[5] Xiongfeng Ma et al. “Practical decoy state for quantum key distribution”. In: *Phys. Rev. A* 72 (2005), p. 012326. DOI: 10.1103/PhysRevA.72.012326.

[6] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Phys. Rev. Lett.* 67 (1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

[7] Juan Yin et al. “Satellite-based entanglement distribution over 1200 kilometers”. In: *Science* 356 (2017), pp. 1140–1144. DOI: 10.1126/science.aan3211.

[8] Kevin Günthner et al. “Quantum-limited measurements of optical signals from a geostationary satellite”. In: *Optica* 4 (2017), pp. 611–616. DOI: 10.1364/OPTICA.4.000611.

[9] Sergio L. Castro. “Towards a global space-based QKD network”. In: *Master thesis* Delft University of Technology, Delft The Netherlands (2019).