# 高效能單光子光源和單光子偵測器之開發與絕對安全通訊之應用

## Highly Efficient Single-Photon Source and Single-Photon Detector for Unconditionally Secure Communication

**Chih-Sung Chuu[1,2*]**

*[1]Department of Physics, National Tsing Hua University, Hsinchu 30013, Taiwan*
*[2]Center for Quantum Technology, Hsinchu 30013, Taiwan*
*E-mail: cschuu@phys.nthu.edu.tw*

Quantum key distribution (QKD), which was proposed nearly 60 years ago [1,2], promises unconditionally (theoretically) secure communication as granted by the laws of physics. Today, a variety of the QKD protocols and systems have been demonstrated in free space and optical fibers. Among these demonstrations, the weak coherent pulses (WCP) are widely used for the light sources due to their simple realization. Compared to the WCP sources, the quantum light sources such as the single- or entangled- photon sources are more challenging to achieve the high performance but can definitely benefit the QKD. For example, the use of single photons in QKD can tolerate higher photon loss [3,4] or higher quantum bit error rate (QBER) [5]. The use of entangled photons can also extend the distance of QKD via the quantum repeaters [6].

Recently, Liu et. al [7] showed that the key creation efficiency (KCE) of QKD can be enhanced to 66% by using single photons with long coherence time. However, the emission wavelength (795 nm) and the complexity of their single-photon source, which is based on the cold atom system, are not suitable for practical uses. To realize the long-distance QKD in fiber transmission system, the telecommunication band is advantageous for minimizing the transmission loss of photons. Therefore, single photons with long coherence time at 1550 nm, which has lower propagation loss compared to the other wavelengths, will be essential for realizing highly efficient QKD. In this work we demonstrate a miniature 1550-nm single-photon source based on the monolithic doubly resonant parametric down-conversion [8]. The telecommunication wavelength of the single photons allows us to implement the QKD in long optical fibers, while the long coherence time and narrow bandwidth enable the high KCE and low QBER [9], respectively. In addition, we show that the double-exponential waveform of the single photons plays a key role to further enhance the KCE. By shaping each photon into 50 equally spaced time bins, we demonstrate the field test of the QKD using an inter-university optical fiber (Fig. 1) with 97% KCE and a QBER below the threshold level of unconditional security [10]. Our work shows that the single photons with long coherence time and controlled waveforms are feasible for practical quantum communication.

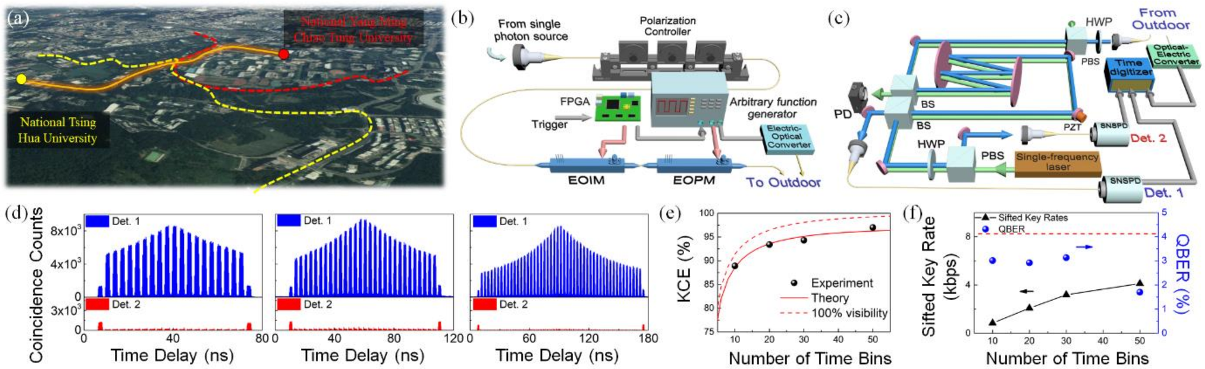


Fig. 1 (a) The field test of the QKD exploits an inter-university optical fiber (orange line) between the General II Building (yellow dot) at NTHU (bounded by the yellow dash line) and the IT Service Center (red dot) at NYCU (bounded by the red dash line). The sender’s and receiver's setup are illustrated in (b) and (c), respectively. The abbreviations stand for half-wave plate (HWP), beamsplitter (BS), polarizing beamsplitter (PBS), piezoelectric actuator (PZT), photodiode (PD), and superconducting nanowire single-photon detector (SNSPD). (d) The time-resolved interference of single photons prepared in 20, 30, and 50 time bins (from the left to right). The integration time and coincidence time bin are 600 s and 0.2 ns, respectively. (e) The key creation efficiency (dots) versus the number of time bins. The solid and dash curves correspond to the theory considering realistic and 100% interference visibility, respectively. (f) The sifted key rates and QBERs versus the number of time bins. The dash line indicates the threshold level of unconditional security.

**References**


[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptology 5, 3 (1992).

[3] N. Lutkenhaus, Phys. Rev. A 61, 052304 (2000).

[4] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, Phys. Rev. Lett. 100, 090501 (2008).

[5] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nature Photonics 9, 832 (2015).

[6] H.-J. Briegel, W. D• ur, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. 81, 5932 (1998).

[7] C. Liu, S. Zhang, L. Zhao, P. Chen, C. H. F. Fung, H. F. Chau, M. M. T. Loy, and S. Du, Opt. Express 21, 9505 (2013).

[8] C.-S. Chuu and S. E. Harris, Phys. Rev. A 83, 061803(R) (2011).

[9] T. Honjo, T. Inoue, and K. Inoue, Optics Communications 284, 5856 (2011).

[10] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. 103, 170503 (2009).