An integrated heterogeneous superconducting-silicon-photonic platform for measurement-device-independent quantum key distribution

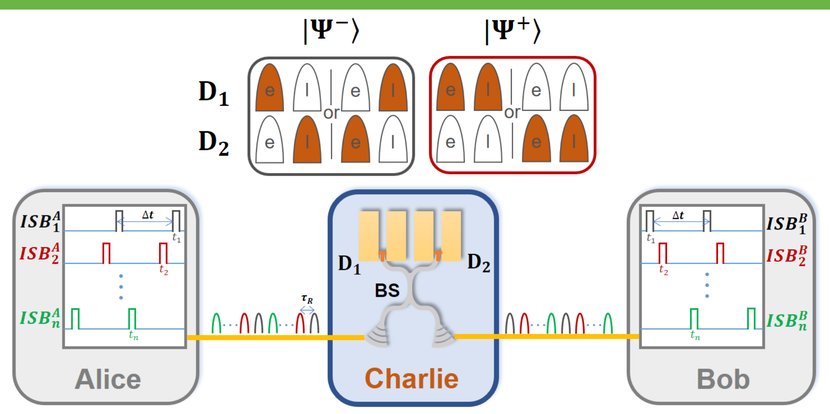
Xiaodong Zheng[1], Peiyu Zhang[1], Renyou Ge[2], Liangliang Lu[1], Guanglong He[1], Fangchao Qu[1], Labao Zhang[1], Xinlun Cai[2], Yanqing Lu[1], Shining Zhu[1], Peiheng Wu[1],Xiaosong Ma[1]

1. National Laboratory of Solid-State Microstructures, Collaborative Innovation Center of Advanced Microstructures, Research Institute of superconducting electronics, Nanjing University, Nanjing 210093, China.

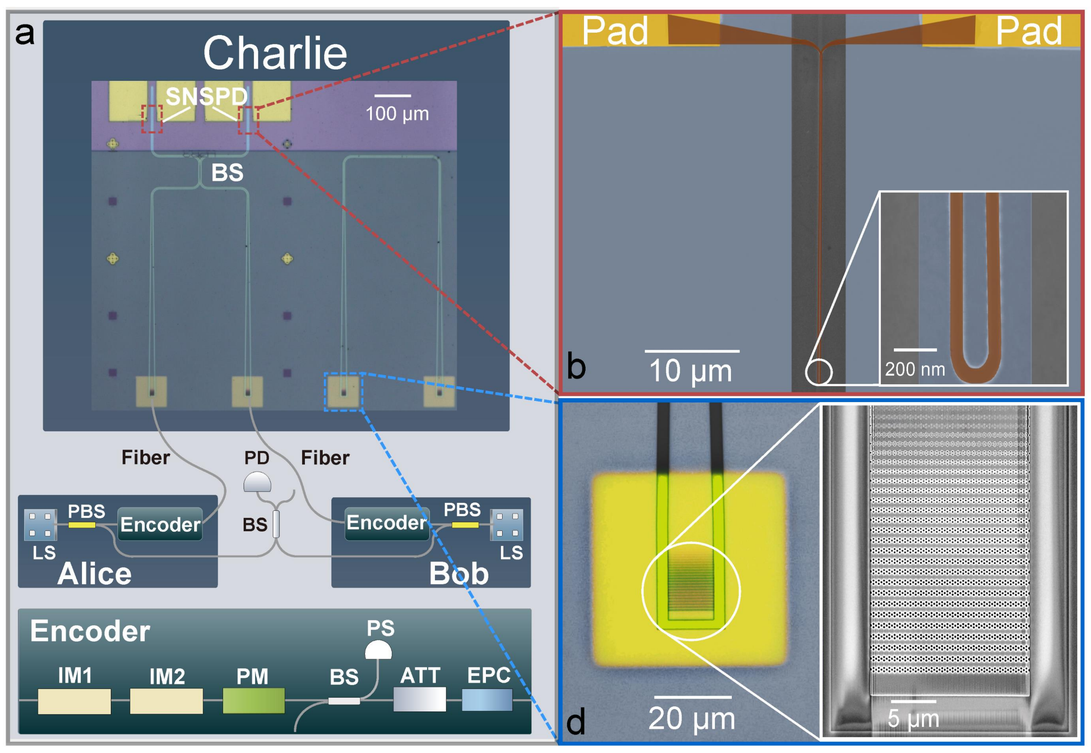
2. State Key Laboratory of Optoelectronic Materials and Technologies, School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510000, China

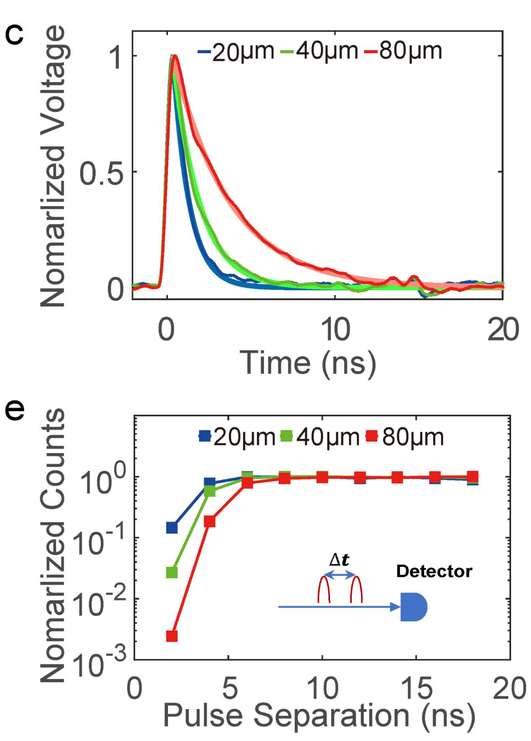
Introduction

Measurement-device-independent quantum key distribution (MDI-QKD) removes all detector side attacks. Here we realize a server for MDI-QKD based on a heterogeneous superconducting-silicon-photonics. The unique design of the waveguide integrated superconducting nanowire single-photon detector enables an ultra-short recovery time, allowing us to perform time-bin-encoded two-outcome Bell state measurements (BSM). Together with the time multiplexing, we obtain a secure key rate of 6.166 kbps over 24.0 dB loss with a 125 MHz clock rate, which is comparable to the state-of-the-art MDI-QKD experimental results with GHz clock rate.



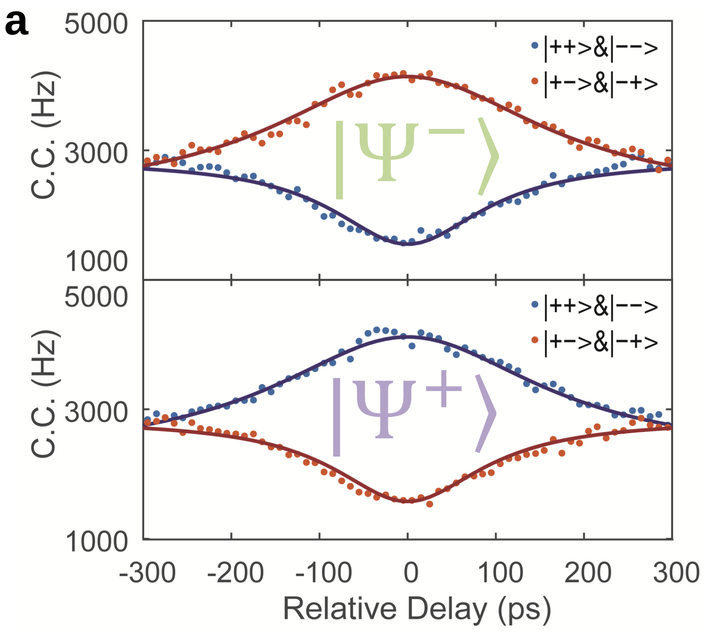
Experiment



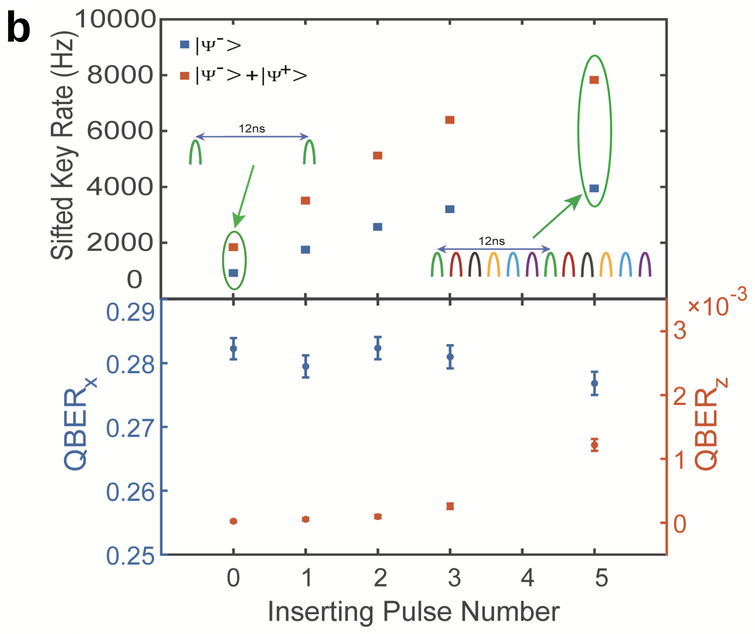


a. Schematic of the experimental setup. **b.** Scanning electron micrograph of the SNSPD with a 80 nm-wide, 80 um-long U-shaped nanowire which is connected with two golden pads and integrated on 500 nm-wide silicon waveguide. **c.** Response pulses of the SNSPD with same width but different length. **d.** Optical microscopy and scanning electron microscopy (SEM) pictures for the high-efficiency photonic-crystal grating coupler with back-reflected mirror. **e.** Normalized counts of the event that detector can detect both early and late pulse continuously as a function of time separation.

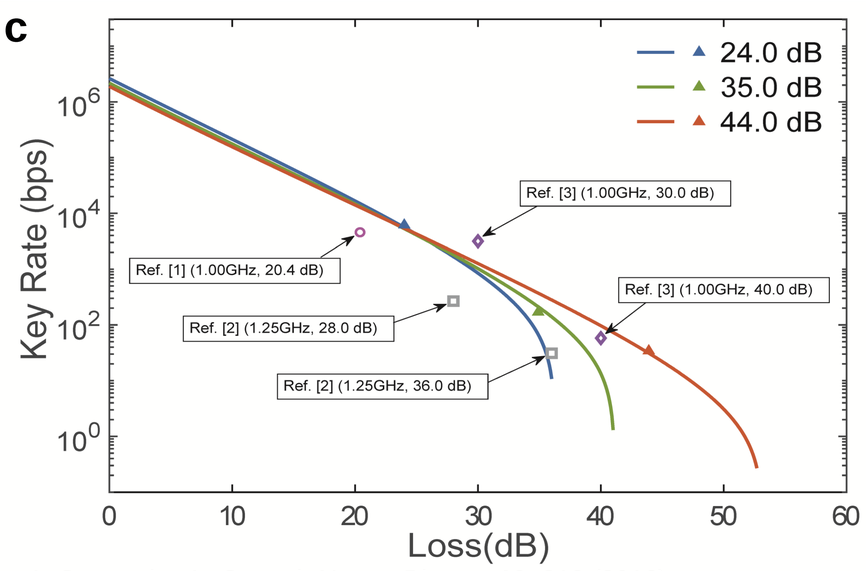
Results



a. The two-photon coincidence counts with BSM as a function of relative electronic delays between Alice's and Bob's pulse sequence.



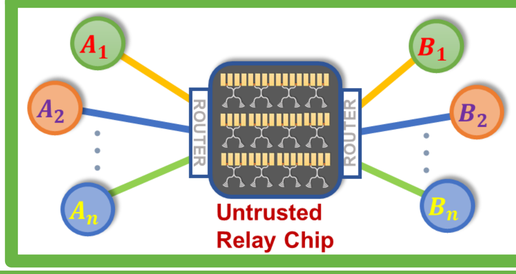
b. Sifted key rate with only Ψ^- measurement or two Bell state measurement versus inserting pulse number and the measured QBER in X-basis or Z-basis versus inserting pulse number.



1. Comandar, L. C. et al. *Nature Photon.* **10**, 312 (2016).
2. Wei, K. et al. *Phys. Rev. X* **10**, 031030 (2020).
3. Woodward, R.I., Lo, Y.S., Pittaluga, M. et al. *npj Quantum Inf* **7**, 58 (2021).

c. Finite-key secret rate versus different channel loss with 125 MHz system frequency and the comparison with the state of the art MDI-QKD experiments.

Outlook



By using more advanced waveguide-integrated SNSPDs, one can further scale the integrated server. Combined with transmitter chip, a fully chip-based, scalable and high-key-rate MDI-QKD metropolitan quantum network should be realized in the near future.

Acknowledgement

NSFC
National Natural Science Foundation of China
中华人民共和国科学技术部
NANJING UNIVERSITY