Practical passive state preparation for quantum key distribution

Y Kurochkin[1], M Papadovasilakis[1], R Piera[1], and J A Grieve[1]

[1] *Quantum communications, TII, PO Box: 9639 Masdar City, Abu Dhabi, United Arab Emirates*
Contact Email: yury.kurochkin@tii.ae

Quantum key distribution is one of the best ways to protect information from future "save now, decrypt later" hacking strategies. One of the biggest challenges pointed out by the US [1] and EU [2] certification authorities is the high cost of quantum key distribution (QKD) equipment and the challenges of side-channel testing. One of the reasons for these problems is the complexity of state preparation. According to the BB84 protocol, random states should be selected from four possible states. The randomness should have a quantum nature to be unpredictable. To realize the BB84 high-speed protocol, one needs to prepare a large number of random quantum states, measure them, amplify the detector output, and digitize them. Next you need to perform high-speed post-processing and use 2-5 bits of randomness to prepare a quantum state. If the rate of state preparation is on the order of GHz, one needs high-speed digital-to-analog converters, amplifiers, and ∼10 GHz electro-optic modulators. This chain makes it challenging to reduce the cost of QKD and offers the possibility of attacks such as the Trojan attack or the inter-symbol correlation side channel.

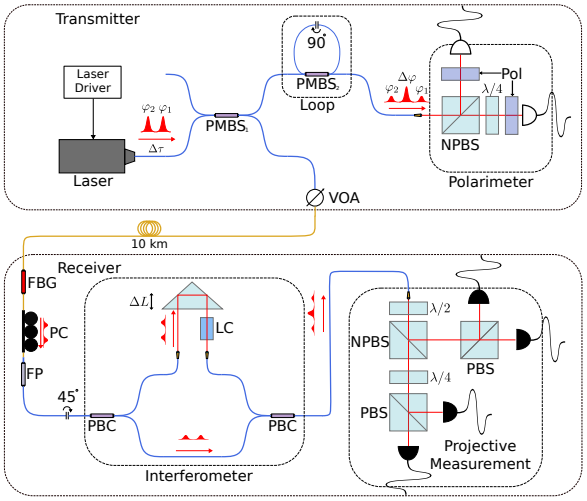

Figure 1: Experimental setup: A DFB laser produces a pulse pair with random phases φ_1 and φ_2 sent through a PMF (Blue Line). A Polarization-maintaining fiber Beamsplitter ($PMBS_1$) splits the signal into two outputs, one sent to the Polarimeter through the tomography channel (top output) and the other sent through the quantum channel (bottom output). In the Tomography channel, the random phase difference $\Delta\varphi = \varphi_1 - \varphi_2$ is mapped to a polarization state utilizing a loop consisting of $PMBS_2$ and 90° rotator connecting the two principal axes of fiber. A free space polarimeter splits signal using a nonpolarizing beamsplitter (NPBS) and measures circular (diagonal) output polarization with (without) a quarter wave plate $\lambda/4$ followed by polarizer (Pol) and amplified detector (represented by a white semicircle). In the Quantum Channel, the light is attenuated by a VOA to a small fraction of the signal and then sent to the receiver through 10 km lengths SMF (yell)

The alternative approach is passive state preparation. It was proposed in 2010 [3] and recently investigated for security aspects [4]. Gain-switch laser phase randomness is well tested and commonly used in quantum random number generators. We use it to prepare a random phase in a time bin qubit. Such a pair of consecutive pulses is a ready-to-use qubit. The main difference from widely used devices is that the random phase can take any value between 0 and 2π. To detect the state prepared by the transmitter, we measure the classical light with the local tomography system, while a small part of the coherent state is attenuated to less than one photon per pulse and sent to the receiver. In this way, we can simplify Alice's device (transmitter) considerably.

The experimental setup is shown in Fig. 1. To generate a quantum state, the laser is driven with a pair of consecutive pulses from a table-top pulse generator. The time delay Δt is sufficient (more than 2 ns) for the phase diffusion process to randomize the phase difference. Four phase states can be distinguished by converting it to polarization state. Two polarization detectors that use maximum and minimum voltage discriminators distinguish four BB84 states. The outputs of the tomography detectors are connected to a time tagger with adjustable threshold voltage. By adjusting the threshold criteria, prepared quantum states can be postselected with the required precision. It means that with some probability tomography

indicates successfull preparation of one of four BB84 states. Otherwise the state is discarded. Without a decoy state, this QKD system is well suited for the "last mile" of a star-shaped quantum network with a loss budget of up to 10 dB. We demonstrate a practical QBER of less than 6%, which opens a possibility for simple and low-cost QKD devices for urban networks. Finally, we use asymptotic key analysis to generate a secret key with passive state preparation over a 10 km routed fiber and a spool fiber (3 and 7 dB loss points in Fig.4) to obtain 10-100 bps of secret keys [5].

In a star-shaped network, such a receiver can operate simultaneously with multiple transmitters that are multiplexed by time to maximize the utilization of the central node.

References

[1] $https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/$

[2] $https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/QuantumPositionspapier.pdf$

[3] M Curty, X Ma, H-K Lo and N Lütkenhaus, Phys. Rev. A **82**, 052325 (2010)

[4] W Wang, R Wang, V Zapatero, L Qian, B Qi, M Curty and H-K Lo, arXiv:2207.05916v1 (2022)

[5] Y Kurochkin, M Papadovasilakis, A Trushechkin, R Piera and J A Grieve, arXiv:2405.08481v1 (2024)