Experimental demonstration of a quantum key distribution without signal disturbance monitoring

Shuang Wang,1 Zhen-Qiang Yin,1 Wei Chen,1 De-Yong He,1
Xiao-Tian Song,1 Hong-Wei Li,1 Li-Jun Zhang,1 Zheng Zhou,1
Guang-Can Guo,1 and Zheng-Fu Han1,†

1 Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
and Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

I Schemes of the variable-delay interferometer

The variable-delay interferometer is the core part of Bob’s setup. We propose four typical schemes to implement the variable-delay interferometer as an example, three schemes are shown in Fig. 1. The passive scheme is based on a $1 \times 64$ BS, followed by 64 FMIs (see Fig. 1a), of which the delays are \{1,2,\ldots,64\}. Each interferometer uses one PZT cylinder to achieve better precision and compensate for the phase shift. All 64 interferometers are completely independent. The passive scheme has the advantage of high speed but requires an excessive number of SPDs. Fig. 1b and Fig. 1c show two active schemes based on the Mach-Zehnder interferometer structure. The simple scheme shown in Fig. 1b uses a $2 \times 2$ OS with $\log_2(L - 1)$ separate delays, and the balanced scheme shown in Fig. 1c uses a $1 \times N$ OS with $2N = 2\sqrt{(L - 1)}$ separate delays. The basic unit in Fig. 1b is composed of a $2 \times 2$ OS and a PZT cylinder wrapped by an optical fiber with delay x. If the $2 \times 2$ OS is in the bar state, then the basic unit has delay 0; if the $2 \times 2$ OS is in the cross state, then the basic unit has delay x. There are three basic units in the short arm, with delays of $2^0 = 1$, $2^1 = 2$, and $2^2 = 4$. In the long arm, there are three basic units, with delays of $2^3 = 8$, $2^4 = 16$, and $2^5 = 32$, and one PZT cylinder with a delay of $2^3 = 8$. By controlling the states of the basic unit, we can obtain delays of \{0,1,2,3,4,5,6,7\} in the short arm and delays of \{8,16,24,32,40,48,56,64\} in the long arm. Using this scheme, we need to prepare only $\log_2 64 = 6$ types of separate delays.
However, the IL of the basic unit in the cross state is approximately twice the IL in the bar state. Therefore, the losses of the long and short arms become unbalanced; e.g., for the variable-delay interferometer with a delay of 64, all three basic units of the long arm are in the cross state, with $0.8 \times 2 \times 3 = 4.8$ dB, whereas all three units of the short arm are in the bar state, with $0.8 \times 3 = 2.4$ dB, where 0.8 dB is the typical insertion loss of a $2 \times 2$ OS. This imbalance between the long and short arms makes the visibility of the variable-delay interferometer poor for some delays. Fig. 1c is a balanced scheme to implement the variable-delay interferometer. In the short arm, \( \{0,1,2,3,4,5,6,7\} \) delays lie between two $1 \times 8$ OSs, and in the long arm, \( \{8,16,24,32,40,48,56,64\} \) delays are also located between two $1 \times 8$ OSs. To obtain a more stable interference effect, these two active schemes can also be implemented based on the FMI. However, the IL of the variable interferometers will increase, and the simple scheme in Fig. 1b will become more unbalanced. Based on the FMI, the final experimental scheme we chose is balanced and stable, but the IL is nearly the same as that of the balanced active scheme shown in Fig. 1c.
II Timing analysis of the active RRDPS QKD experiment

In the experiment, Alice prepares encoded packets that are composed of a train of 65 pulses separated by intervals of 1 ns, and Bob uses a 1-GHz, 1-64-bit variable-delay interferometer to make the $k$th pulse interfere with the $(k + r)$th pulse in the same packet, where $1 \leq r \leq 64$, and $1 \leq k \leq 65 - r$. Once the delay $r = x - y$ is set by controlling two $1 \times 8$ OSs, the interferometer has a long arm with delay $x \in \{8, 16, 24, 32, 40, 48, 56, 64\}$ and a short arm with delay $y \in \{0, 1, 2, 3, 4, 5, 6, 7\}$.

For one packet with 65 pulses, its duration time is only 65 ns at Alice’s site. At Bob’s site, there are 64 possible delays, which come from the combination of the 8 possible delays in the long arm and the 8 possible delays in the long arm; thus, the possible duration time of
one packet increases to 129 ns (65+65-1). The sequence diagram is shown in Fig. 2. The possible duration time of 129 ns can be divided into three parts (from left to right): an 8-ns noninterference area, a 64-ns interference area (marked in Fig. 2), and a 57-ns noninterference area. To obtain a low error rate, the interference area of one packet cannot overlap with the noninterference area of the adjacent packets. Therefore, the interval between each two packets in the active RRDPS QKD system is essential. In our experiment, the interval should be longer than 57 ns. Considering the switching speed of the $1 \times 2$ OS and its driver (the switching speed of the switch itself is faster than 50 ns, but the switching speed of our designed switch driver is approximately 100 ns), we set 191 ns as the interval between each two packets in the experiment. Therefore, the interval between each two packets would confine the performance of the active system. In our experiment, approximately 25% of the time was effectively utilized. However, this interval would be shortened by improving the switch driver.

**FIG. 2.** Sequence diagram of the active RRDPS QKD experiment with $L=65$. Each encoded packet is composed of a train of 65 pulses. For the variable-delay interferometer that is used to decode the encoded data, there are eight possible delays \{0,1,2,3,4,5,6,7\} in the short arm and eight other possible delays \{8,16,24,32,40,48,56,64\} in the long arm. The possible interference area of the variable-delay interferometer is marked.

Based on the results of the timing analysis, the interval between each two packets is essential for the active implementation of the RRDPS QKD protocol. In contrast, the passive implementation using a $1 \times N$ beam splitter does not need the interval.
III Measures for stability robustness

The difficulty in RRDPS QKD lies in the realization of a low-loss variable-delay interferometer with high stability. Compared with the passive implementation with (L-1) fixed-delay interferometers, the active implementation requires only two single photon detectors. However, different optical delays are rapidly switched in or out from the interferometer in the active implementation. The switches, optical delays and environment make the variable-delay interferometer highly unstable.

**FIG. 3.** Encapsulation of the variable-delay interferometer. 

- **a.** Inner layer of the encapsulation. The variable-delay interferometer was first put in a copper box with dimensions of 30 cm×22 cm×1.7 cm. The content of the box could be divided into two parts: The common part included the BS, switches and PZT cylinders, and the second part included the fiber delays and Faraday mirrors, which were enveloped by thermal insulating material. 
- **b.** Two layers of the encapsulation. The copper box was then concentrically housed in a 40 cm×32 cm×11.7 cm ABS plastic case. The space between the two layers was filled with thermal insulating material.

In our experiment, the variable-delay interferometer showed good stability robustness because of the following reasons and measures: **(I) The structure of the variable-delay interferometer.** First, the basic structure of the variable-delay interferometer is the Faraday-Michelson interferometer (FMI), which is insensitive to polarization variation. Once a delay is chosen, the interferometer becomes a fixed-delay FMI, whose stability has been demonstrated in several previous QKD experiments. Second, the interferometer has good symmetry, which makes the interferometer have high visibility and weakens the effect of the environment. The final chosen delay \( r \) is the difference of one delay in the long arm and the other delay in the short arm. Therefore, the common part of the long arm and the short arm should be identical to weaken the effect of the environment. As shown in Fig. 3a, 8 delays in the long arm and 8 other delays in the short arm have nearly the same structure; only the fiber delays between the Faraday mirrors and PZT cylinders are different. **(II) The
**choice of the switch.** The bidirectional 1×2 switch is one of the key components, and it must not introduce an extra phase, which would otherwise add errors to the detection. The 1×2 switch that we chose is achieved using non-mechanical configurations with solid-state all-crystal designs (see the product description and its patent for Agiltron Inc.), so this choice eliminates the instability from the switch. **(III) The measures to isolate the environment.** The variable-delay interferometer was placed in a sealed copper box with dimensions of 30 cm×22 cm×1.7 cm, and this box was then concentrically housed in a 40 cm×32 cm×11.7 cm ABS plastic case (see Fig. 3b). The space between the inner box and the case was filled with thermal insulating material. As shown in Fig. 3a, the inner box could be divided into two parts. The common part included the BS, switches and PZT cylinders, and the second part included the fiber delays and Faraday mirrors, which were enveloped by thermal insulating material to keep the fiber delays stable. **(IV) Active compensation of phase shifts.** Sixteen PZT cylinders in the interferometer were used to actively compensate for the slowly varying phase drifts.

Good stability of the RRDPS QKD experiment was obtained through the rational design of the structure, the careful choice of the optical devices and the effective encapsulation of the variable-delay interferometer. The stability robustness has fully demonstrated the practicability of our RRDPS QKD system.