

Quantum key distribution transmitter chip based on hybrid-integration of silica and lithium niobates

Xiao Li(李骁), Liang-Liang Wang(王亮亮), Jia-shun Zhang(张家顺), Wei Chen(陈巍), Yue Wang(王玥), Dan Wu (吴丹), and Jun-Ming An (安俊明)

Citation: Chin. Phys. B, 2022, 31 (**6**): 064212. DOI: 10.1088/1674-1056/ac40fe
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Proof-of-principle experimental demonstration of quantum secure imaging based on quantum key distribution

Yi-Bo Zhao(赵义博), Wan-Li Zhang(张万里), Dong Wang(王东), Xiao-Tian Song(宋萧天), Liang-Jiang Zhou(周良将), Chi-Biao Ding(丁赤飚)
Chin. Phys. B, 2019, 28 (**10**): 104203. DOI: 10.1088/1674-1056/ab3e66

Multi-functional optical fiber sensor system based ona dense wavelength division multiplexer

Yue-Xin Yin(尹悦鑫), Zhifa Wu(吴志发), Siwen Sun(孙思文), Liang Tian(田亮), Xibin Wang(王希斌), Yuanda Wu(吴远大), Daming Zhang(张大明)
Chin. Phys. B, 2019, 28 (**7**): 074202. DOI: 10.1088/1674-1056/28/7/074202

16-channel dual-tuning wavelength division multiplexer/demultiplexer

Pei Yuan(袁配), Yue Wang(王玥), Yuan-Da Wu(吴远大), Jun-Ming An(安俊明), Xiong-Wei Hu(胡雄伟)
Chin. Phys. B, 2018, 27 (**12**): 124208. DOI: 10.1088/1674-1056/27/12/124208

Low power consumption 4-channel variable optical attenuator array based on planar lightwave circuit technique

Mei-Zhen Ren(任梅珍), Jia-Shun Zhang(张家顺), Jun-Ming An(安俊明), Yue Wang(王玥), Liang-Liang Wang(王亮亮), Jian-Guang Li(李建光), Yuan-Da Wu(吴远大), XiaoJie Yin(尹小杰), Xiong-Wei Hu(胡雄伟)
Chin. Phys. B, 2017, 26 (**7**): 074221. DOI: 10.1088/1674-1056/26/7/074221

Effect of electromagnetic disturbance on thepractical QKD system in the smart grid

Li Fang-Yi, Wang Dong, Wang Shuang, Li Mo, Yin Zhen-Qiang, Li Hong-Wei, Chen Wei, Han Zheng-Fu
Chin. Phys. B, 2014, 23 (**12**): 124201. DOI: 10.1088/1674-1056/23/12/124201

Quantum key distribution transmitter chip based on hybrid-integration of silica and lithium niobates

Xiao Li(李骁)[1,2,3], Liang-Liang Wang(王亮亮)[1], Jia-shun Zhang(张家顺)[1,†], Wei Chen(陈巍)[4], Yue Wang(王玥)[1,3], Dan Wu (吴丹)[1,2,3], and Jun-Ming An (安俊明)[1,3,‡]

[1] *State Key Laboratory on Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences (CAS), Beijing* 100083, *China*
[2] *College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing* 100049, *China*
[3] *Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing* 100049, *China*
[4] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei* 230026, *China*

(Received 14 September 2021; revised manuscript received 5 December 2021; accepted manuscript online 8 December 2021)

A quantum key distribution transmitter chip based on hybrid-integration of silica planar light-wave circuit (PLC) and lithium niobates (LN) modulator PLC is presented. The silica part consists of a tunable directional coupler and 400-ps delay line, and the LN part is made up of a Y-branch, with electro-optic modulators on both arms. The two parts are facet-coupled to form an asymmetric Mach–Zehnder interferometer. We successfully encode and decode four BB84 states at 156.25-MHz repetition rate. Fast phase-encoding of 0 or π is achieved, with interference fringe visibilities 78.53% and 82.68% for states $|+\rangle$ and $|-\rangle$, respectively. With the aid of an extra off-chip LN intensity modulator, two time-bin states are prepared and the extinction ratios are 18.65 dB and 15.46 dB for states $|0\rangle$ and $|1\rangle$, respectively.

Keywords: quantum key distribution, hybrid-integration, BB84

PACS: 42.82.Bq, 42.82.Fv, 42.50.Ex **DOI:** 10.1088/1674-1056/ac40fe

1. Introduction

Cyber communication provides much convenience in daily life and becomes more and more indispensable to us. However the boost and innovation of computing capacity drastically increase the risk of failure for classic data encryption method. Therefore the need for higher-level information security becomes urgent. Quantum key distribution (QKD) can ensure best security based on quantum mechanics. Bennett and Brassard,[1] and Bennett *et al.*,[2] first proposed the effective and famous BB84 protocol. Bulk optics connected by fibers were used for the realization of BB84 protocol, in which weak coherent pulse pairs (WCPs) with a temporal delay were generated for encoding and decoding quantum states.[3,4] In these systems too much room, however, is required for apparatuses to lay on a heavy and large optical platform, which is not conducive to manufacture and practical applications.

One way to miniaturize the system is to turn into integrated photonics technology. Silica planar light-wave circuits (PLCs) have been used first for the WCP generation at Alice and state decoding at Bob.[5–14] Recently, various photonic integrated circuits (PICs) technologies have been integrated into QKD systems, such as indium phosphide (InP)[15,16] and Si photonic (SiP)[17–23] based integrated photonic platforms, which have shown a good application prospect. The BB84 system based on the combination of a silica asymmetric Mach–Zehnder interferometer (AMZI) and off-chip lithium niobates (LN) modulators was reported,[9,13] where high speed of phase modulation and intensity modulation were implemented by extra LN modulators.

To further increase the degree of integration, a promising way is to integrate silica and LN into one single chip. The relevant technology has been reported in the field of coherence communication,[24] where low-loss silica PLCs and LN phase modulator array chip were spliced together to implement quadrature phase shift keying (QPSK). In the field of QKD, Nambu *et al.* demonstrated a prototype of BB84 QKD transmitter based on hybrid integration,[25] where an AMZI silica PLC was coupled with an MZI LN PLC. His demo could realize the high-speed intensity modulation but lacked the function to modulate relative phase between WCPs in a dynamic fashion and a fast fashion.

Here we present a transmitter with a different structure based on this hybrid-integration technique. There are two main parts in our chip. One is the silica part which consists of a tunable directional coupler (DC) and 400-ps delay line. The other is the LN part which consists of a Y-branch, with electro-optic (EO) modulators on both arms. The two parts are facet-coupled to form an AMZI. Our design has three features. First, we make it in one single AMZI to implement both functions of WCP generation and high-speed relative phase modulation. This is different from other researches[9–14] where these two functions are usually done by separate apparatuses. Second, a combination of slow silica thermo-optic phase modulator (TOPM) and fast LN EO phase modulator makes our chip more flexible to regulate any defined relative phase. Third,

†Corresponding author. E-mail: zhangjiashun@semi.ac.cn
‡Corresponding author. E-mail: junming@semi.ac.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

the LN phase modulator is designed in a push-and-pull model in order to reach a higher EO modulation efficiency. With the aid of an extra off-chip LN intensity modulator and a passive silica decoder chip,[26] we demonstrate the preparation of four BB84 states and the corresponding states decoding.

2. Design and fabrication of hybrid chip

We design and fabricate a hybrid chip for a telecom (1.55 μm) wavelength window. The structure is shown in Fig. 1(a). The silica chip on the left consists of two sub-parts. Part 1 is a 2×2 MZI with a TOPM1 in one arm, which functions as a tunable DC. Part 2 consist of two arms of waveguides, whose path difference produces 400-ps temporal delay. There is another TOPM2 in the short arm. It is worth noting that this silica part is different from that in Ref. [26], which is terminated with a DC at the output. We here remove the DC for the coupling with the LN chip. The relative refractive index difference Δ is 2.0% between the waveguide core and cladding. The full-vectorial beam propagation method (BPM) is used to find the geometric zero birefringence condition for the stripe waveguides, where the effective indices are found equal for both TE and TM modes. The fabrication process can be referred to Refs. [26,27].

The LN chip on the right has a Y-branch structure, with electro-optic (EO) modulators on both arms. The ground-signal-ground (GSG) coplanar waveguide electrodes are designed in a push-pull model, making electric fields opposite to each other for both arms. The LN modulation chip is prepared by diffusion method. First, the design waveguide structure pattern is transferred to the LN wafer by lithography. Next, the wafer is placed into the C_6H_5COOH solution at 120 °C–250 °C, where Li^- in the lithium niobate material is exchanged with H^+ to form the core $H_xLi_{1-x}NbO_3$ and diffused for 5 h–10 h at 300 °C–400 °C to form the exchange diffusion waveguide. The relative refractive index difference Δ is about 0.3% between the waveguide core and cladding. Then photolithography is again used to transfer the traveling wave electrode pattern, and the GSG electrode is formed by electroplating method.

The silica chip is facet-coupled with a single mode fiber array (FA) on the left side, with a coupling loss of 0.4 dB. The LN chip is facet-coupled with a polarization maintenance FA on the right side, whose slow-axis coincides with the x-cut direction of LN chip, with a coupling loss of 3 dB. Next the silica and LN chips, with the connecting end-faces polished at an 8° angle, are facet-coupled to form an AMZI chip in the way shown in Fig. 1(a). The chip size is 2.3 cm×0.6 cm for silica part and 3.8 cm×0.1 cm for LN part. The hybrid chip is fixed on a large silicon substrate together with the designed printed circuit board (PCB). Wire bonding is employed to connect the electrodes between the PCB and the chip. The chip's temperature is controlled by a commercial temperature controller (TEC) based on the Peltier effect.

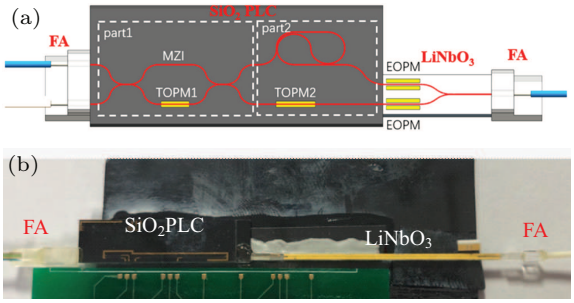


Fig. 1. (a) Schematic diagram of the hybrid-integration chip and (b) packaging.

3. Measurement of temporal delay and phase modulation speed

The temporal delay of the WCP generated by our hybrid chip is measured by both normal-intensity light and strongly-attenuated light (mean photon per cycle $\mu < 0.01$). A train of pulses, with pulse 50-ps duration, are input to our chip. The pulse pair graph in one cycle captured by the sampling oscilloscope (SOC) and the histogram of the two time-bins scanned by the gated-mode single photon detector (SPD) are shown in Figs. 2(a) and 2(b), respectively.

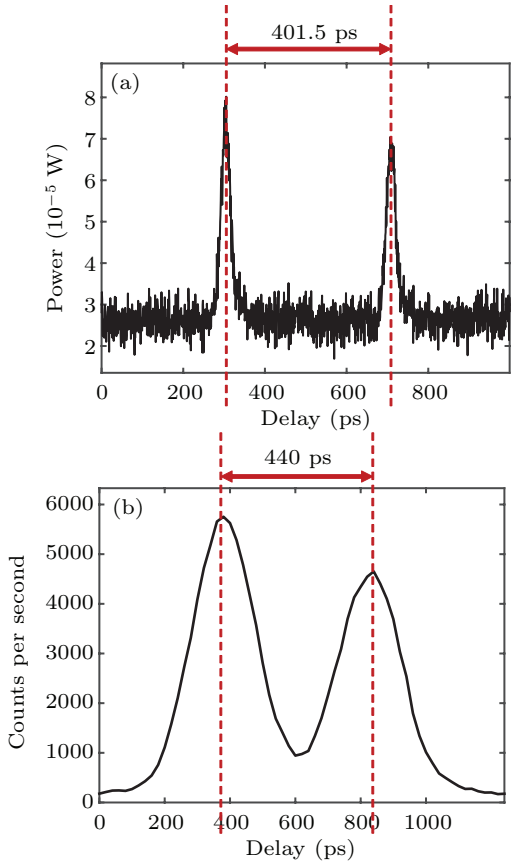


Fig. 2. Measurement of temporal delay of WCP for our chip: (a) measured by SOC with normal-intensity light, (b) measured by SPD with strongly-attenuated light ($\mu < 0.01$).

The measured temporal delay is 401.5 ps for SOC and 440 ps for SPD. The value for SPD is about 40 ps larger than

that for SOC. This is because SPD has small time-resolution than SOC and its gate width is wider than 400 ps. Therefore the value of 401.5 measured by SOC is closer to the true one. The difference between measurement and design is below 0.4%, which proves the accuracy of our design and fabrication.

In addition, the speed of phase modulation for the hybrid chip is tested. The hybrid chip is fixed on the TEC platform and the microwave probe is used to connect GSG electrode on chip. As shown in Fig. 3, the eye diagram under 10 Gbps is obtained. The rise/fall time is around 100 ps and the extinction ratio of the eye diagram is 6.12 dB. From the test results, we can see that the modulation rate of the integrated chip can meet the needs of fast phase-encoding.

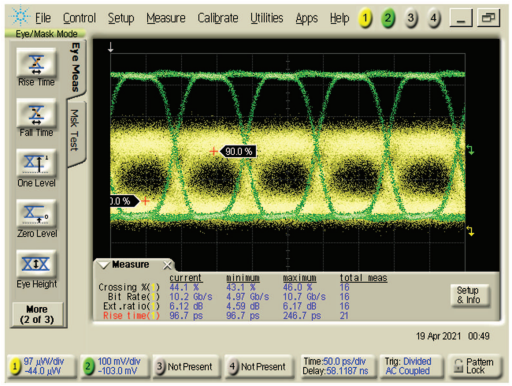


Fig. 3. Eye diagram of hybrid chip. Green is driving signal from PPG before amplified; yellow is optical signal.

4. Polarization characteristic analysis on interference

In order to optimize the interference visibility in QKD, it is necessary to analyze the dependence of interference visibility on the chip temperature for both Alice and Bob chips. With the aid of the pulse self-interference method,[27] we conduct the following experiments. Considering the limit of our TEC, We scan the hybrid chip temperature from 17 °C to 60 °C. The interference fringes against temperature are shown in Fig. 4(a). We can observe that the photon count for the TE mode is much larger than that of the TM mode. This is because the polarization characteristic of LN waveguide. Furthermore, the TE and TM modes are in phase despite the change of chip temperature. Since the visibility increases with the temperature and our TEC has lower control precision above 55°, we decide to use this value as the optimal temperature for the hybrid chip. Next, we use the same method to determine the Bob AMZI chip temperature as shown in Fig. 4(b), In the vicinity of 42°, the visibility reaches a minimum value, and TE mode and TM mode are in anti-phase. Though in the scope of TEC temperature domain there is no such temperature point, where both modes are perfectly in phase, we obtain the best visibility as we can in the vicinity of 17°. Therefore the Bob chip temperature is set to be this value.

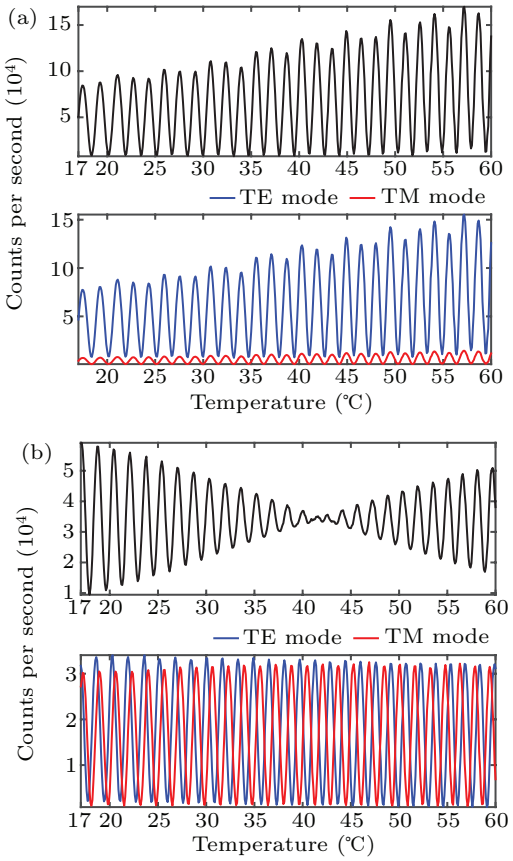


Fig. 4. Interference fringes of TE mode (blue) and TM mode (red) *versus* chip temperature in a range from 17 °C to 60 °C. Top black curve is the sum of TE and TM modes. (a) Hybrid chip for Alice and (b) silica AMZI chip for Bob.

5. Encoding and decoding of four BB84 states

The four BB84 states are encoded on relative phase and amplitudes of WCPs. The encoder/decoder scheme is demonstrated in Fig. 5.

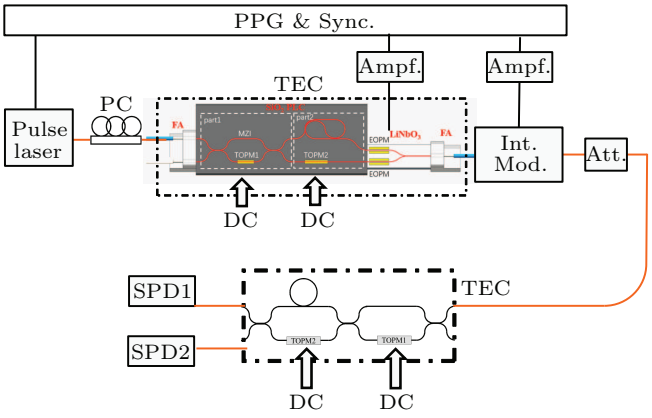


Fig. 5. Schematic diagram of QKD system based on hybrid chip at Alice and silica AMZI chip at Bob. PC: polarization controller; TEC: temperature controller; DC: direct current source; PPG&Sync: pulse pattern generator and synchronization clock; Ampf.: RF amplification; Int. Mod: LN intensity modulator; Att.: off-chip optical attenuator; SPD: gated mode single photon detector.

The Alice section includes a pulse laser, a polarization controller, the hybrid chip, an off-chip LN intensity modulator, and an off-chip attenuator, in sequence. The Bob section

includes SPDs and an silica AMZI chip,[26,27] with the identical temporal delay of Alice. Pulse pattern generator (PPG) provides the system clock to synchronize all the devices including pulse laser and SPDs. The driving signal from PPG is amplified by the radio-frequency (RF) amplifier, up to 3-dB bandwidth of 10 GHz with a 26-dB gain, to drive the EO modulator in the hybrid chip. Direct current source is used to drive the TOPMs in both Alice and Bob chips

5.1. Phase basis states $|+\rangle$ and $|-\rangle$

We input to the system the pulses of 50-ps duration at 156.25-MHz repetition rate. We set the attenuator so that $\mu = 0.1$. The Alice and Bob chips are separately temperature-controlled according to what we discussed in Section 2. We set the TOPM of tunable DC in both Alice and Bob chips to make intensity-balanced for WCPs. The system output generates three time slots in SPDs. Interference occurs in the middle time-slot, named S2, allowing the states $|+\rangle$ and $|-\rangle$ to be measured.

The interference fringes *versus* PPG driving voltage are shown in Fig. 6(a). It can be seen that the curve profile is sine-like within 0.66 Vpp, beyond which the curve becomes flat due to the saturation of the RF amplifier. The relative phases between WCPs are 0 and π corresponding to 0.1 Vpp and 0.62 Vpp, respectively. When the voltage is 0.1 Vpp, the output count at S2 is 0.28×10^5 for SPD1 and 2.02×10^5 for SPD2. When the voltage is 0.62 Vpp, the output count at S2 is 2.38×10^5 for SPD1 and 0.19×10^5 for SPD2. The interference visibility, $V = (\max - \min)/(\max + \min)$, is 78.53% for SPD1 and 82.68% for SPD2. The histograms of three time slots are scanned as shown in Figs. 6(b) and 6(c) corresponding to 0.1 Vpp and 0.62 Vpp, respectively. Next, we conduct the research on the phase stability. We keep the voltage at 0.62 Vpp, The ratio between outputs of both SPDs at S2 is recorded every 3 min over 8 h. Figure 7 shows the plot of the ratio variation *versus* time. It can be seen that most of values vary from 4 dB to 8 dB.

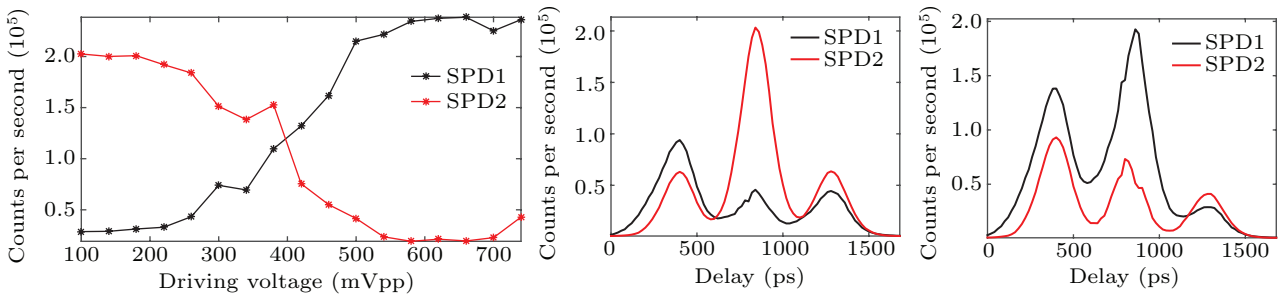


Fig. 6. Measurements of BB84 states $|+\rangle$ and $|-\rangle$, showing (a) interference fringe *versus* PPG driving voltage, and histogram of the three time slots corresponding to (b) 0.1 Vpp and (c) 0.62 Vpp, respectively.

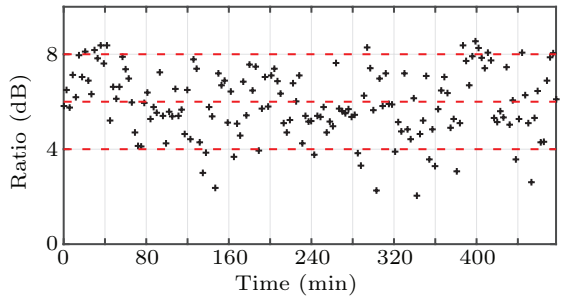


Fig. 7. Test of phase stability, indicating ratio between two outputs *versus* time, with voltage fixed at 0.62 Vpp.

Next we will discuss the visibility and phase stability shown by our system. The visibility is related to the ratio given in Ref. [27]

$$V = \frac{N_{\max} - N_{\min}}{N_{\max} + N_{\min}} = 2\frac{\sqrt{N_1 N_2}}{N_1 + N_2}\left|\cos\frac{\Delta\phi_{\text{Mode}}}{2}\right|, \tag{1}$$

where N_1 and N_2 are the photon counts of two interfering pulses and $\Delta\phi_{\text{Mode}}$ is the modal phase mismatch. The interference visibility is relatively low. For that there are two major reasons. One reason is that the increase of driving voltage breaks the intensity-balance of WCP. As can be seen from the SPD2 (red curve) in Figs. 6(b) and 6(c), the count ratio between the first and final times lot dramatically changes when the driving voltage changes from 0.1 Vpp ($N_1 = N_2$) to 0.62 Vpp ($N_1 \neq N_2$). The increase of voltage breaks the count balance between N_1 and N_2, thus reducing the visibility. The other reason is that the temperature of Bob chip is not optimal due to TEC limitation. At this temperature point, the TE mode and TM mode are not perfectly in phase, namely, $\Delta\phi_{\text{Mode}} \neq 0$, thus leading to none-perfect interference and low visibility. It is promising to improve the visibility in these two aspects by compensating for the imbalance of intensity and upgrading TEC to cover the optimal AMZI temperature. Besides, the relative phase between WCPs is unstable. The reason is that the LN EO phase modulator is quite polarization sensitive. Therefore the interference is very sensitive to the fluctuation of driving signal or the fiber stress change.

5.2. Time-bin basis states $|0\rangle$ and $|1\rangle$

With the aid of an extra off-chip LN intensity modulator as shown in Fig. 5, we prepare states $|0\rangle$ and $|1\rangle$ for the time-bin basis. Figure 8 illustrates a histogram of the states' generation before Bob (left column) and the corresponding fi-

nal measurement outcomes on both SPDs (right two columns). Measurement in the first time slot (S1) of either SPD output represents a $|0\rangle$ and a measurement in the third time slot (S3) is $|1\rangle$. The extinction ratio $\mathrm{ER}_{\mathrm{time}}$ for state $|0\rangle$ (or $|1\rangle$) can be represented by the ratio in dB of sum of both SPD outputs at S1 (or S3) to the counterpart at S3 (or S1). Therefore $\mathrm{ER}_{\mathrm{time}}$ is 18.65 dB for state $|0\rangle$ and 15.46 dB for state $|1\rangle$. It is worth noting that the two SPDs cannot achieve the balanced WCP simultaneously. In this case the SPD2 has nearly balanced counts at the two time slots while SPD2 has not. This is because the ending DC of AMZI at Bob is not perfectly 3 dB. This can be optimized by scanning and finding the optimal coupling length of DC in the fabrication process.

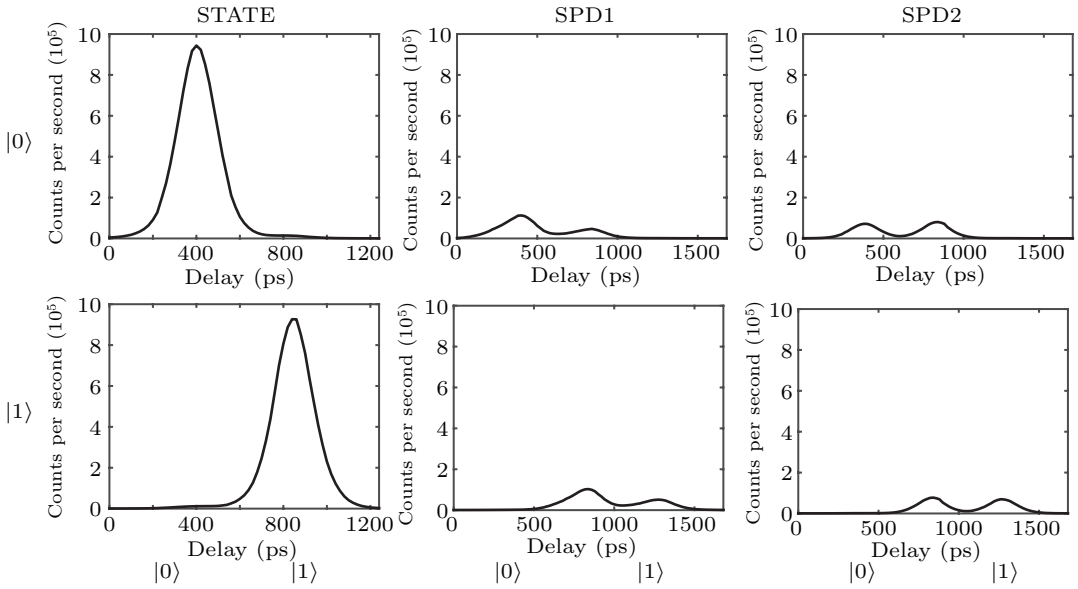


Fig. 8. Measurements of BB84 states $|0\rangle$ and $|1\rangle$. Measurement in slot S1 of either SPD output represents a $|0\rangle$ and a measurement in slot S3 is $|1\rangle$.

6. Asymptotic secure key analysis

We perform an asymptotic secure key estimation based on the visibility and extinction ratio $\mathrm{ER}_{\mathrm{time}}$ measured in our case. Since our circuit does not include another intensity modulator that is required for the use of decoy states. We therefore use a security proof,[28] to provide security against general attacks in the case of non-phase-random, non-decoy state BB84, with the key rate per pulse given by

$$K_{\mathrm{BB84}} = \frac{1}{2} R \left[1 - f(\varepsilon) H_2(\varepsilon) - H_2(\varepsilon_{\mathrm{ph}})\right], \tag{2}$$

where R is the fraction of pulses for which Bob detects the signal. Since we lack experimental conditions to measure the raw key rate, instead, we estimate the value of R[29] from the following formula:

$$R = \frac{\text{raw key rate}}{\text{repetition rate}} = \mu t_{\mathrm{link}} \eta, \tag{3}$$

where μ is the mean photon number of the signal emitted from Alice, and η is the detection efficiency of the SPD. In this work, we attenuate the source optical pulses to achieve $\mu = 0.1$ and set the SPD $\eta = 10\%$. Here t_{link} is the probability of a photon arriving at the detector given by

$$t_{\mathrm{link}} = 10^{(-\alpha L + IL_{\mathrm{Bob}})/10}, \tag{4}$$

where IL_{Bob}, the excess loss of Bob AMZI chip, is measured to be 2.48 dB, $\alpha = 0.2$ dB/km is the loss coefficient of single mode fiber and L is the fiber length. Here ε is the quantum bit error rate (QBER) observed in the verification test, and $f(\varepsilon) \geq 1$ is the error correction inefficiency used to perform key reconciliation (here $f(\varepsilon) = 1.22$ according to the literature estimate value). $H_2(\varepsilon)$ is the binary Shannon entropy given by

$$H_2(\varepsilon) = -\varepsilon \log_2(\varepsilon) - (1-\varepsilon)\log_2(1-\varepsilon). \tag{5}$$

Here $\varepsilon_{\mathrm{ph}}$ is a function of ε, given by

$$\begin{aligned} \varepsilon_{\mathrm{ph}} = {} & \varepsilon + 4\Delta'(1-\Delta')(1-2\varepsilon) \\ & + 4(1-2\Delta')\sqrt{\Delta'(1-\Delta')\varepsilon(1-\varepsilon)}, \end{aligned} \tag{6}$$

with

$$\Delta' = \frac{\Delta}{R_0} = \frac{1}{2R_0}\left(1 - \mathrm{e}^{-\mu/2}\left(\cos\left(\frac{\mu}{2}\right) + \sin\left(\frac{\mu}{2}\right)\right)\right) \tag{7}$$

and R_0 refers to the R at 0 km.

Since we also lack experimental conditions to measure error rate, instead, we use the following equation to estimate it:

$$\varepsilon = \mathrm{QBER}_{\mathrm{opt}} + \mathrm{QBER}_{\mathrm{det}}. \tag{8}$$

One can identify two major contributions to the QBER for this weak-coherent source BB84 scenario. The first one $\mathrm{QBER}_{\mathrm{opt}}$ arises from photons that end up in the wrong detector due to imperfection of our chips and is given by

$$\mathrm{QBER}_{\mathrm{opt}} = \frac{1}{2}\mathrm{QBER}_{\mathrm{phase}} + \frac{1}{2}\mathrm{QBER}_{\mathrm{time}}, \tag{9}$$

where the factor of 1/2 in each term on the right-hand side is related to the random basis selection of 50% possibility. The $\mathrm{QBER}_{\mathrm{phase}}$ is due to imperfect phase state and given by

$$\mathrm{QBER}_{\mathrm{phase}} = \frac{1-V}{2}, \tag{10}$$

where V is the measured interference fringe visibility. The $\mathrm{QBER}_{\mathrm{time}}$ due to the imperfect time-bin states is

$$\mathrm{QBER}_{\mathrm{time}} = \frac{1}{10^{ER/10}+1}, \tag{11}$$

where ER is the time-bin extinction ratio. According to the previous measurements, the average visibility is 80.6% , therefore the $\mathrm{QBER}_{\mathrm{phase}} = 0.097$; the average time-bin extinction ratio $ER = 17.06$ dB, therefore the $\mathrm{QBER}_{\mathrm{time}}$ is 0.019. The whole $\mathrm{QBER}_{\mathrm{opt}}$ is 0.058. The $\mathrm{QBER}_{\mathrm{opt}}$ is independent of the transmission distance. It can be considered as a measure of the optical quality of the chip.

The second contribution, $\mathrm{QBER}_{\mathrm{det}}$ is given by

$$\mathrm{QBER}_{\mathrm{det}} = \frac{p_{\mathrm{dark}} n}{2 t_{\mathrm{link}} \eta \mu}, \tag{12}$$

where p_{dark} is the probability of recording a dark count per time gate and per detector. In our case, p_{dark} is 3×10^{-6}/gate. The $n = 2$ is the number of detectors. It is clear that $\mathrm{QBER}_{\mathrm{det}}$ increases with distance, since the dark-count rate remains constant while the bit rate comes down like t_{link}.

It is worth noting that the fluctuation of the phase state can also increase the QBER. The analysis of this factor is also out of our experimental capability. Fortunately, our AMZI chips are capable of actively compensating for the phase variation. The TOPM in the AMZI can be used to actively compensate for the phase fluctuation. An online feedback procedure,[22] based on the TOPM has been demonstrated by some researchers to implement the compensation, showing good effect on reducing the QBER.

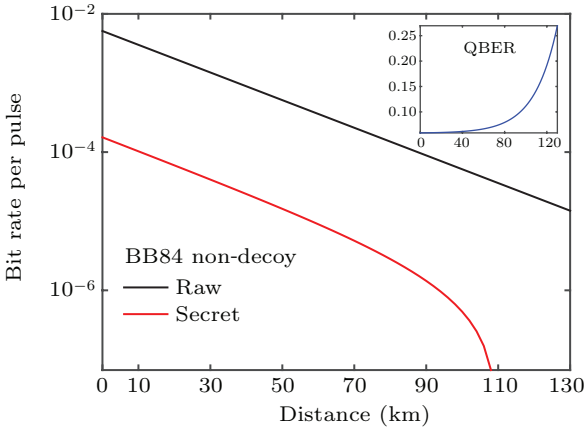


Fig. 9. Estimated asymptotic secret key rate and relevant QBER for non-decoy BB84 QKD.

The raw key R equation (3), secret key K_{BB84} equation (2), and QBER equation (8) are plotted against the distance as shown in Fig. 9. A secure key rate of 10.041 kbps (6.4265×10^{-5} bit per pulse) is expected at 156.25-MHz repetition rate over a 20-km distance with an estimated QBER of 0.059.

7. Conclusions and perspectives

In this work, we design and prepare a BB84 QKD transmitter based on hybrid-integration of silica and LN chips. Four BB84 states are encoded and decoded at a repetition rate of 156.25 MHz. The interference fringe visibility is 78.53% for phase state $|+\rangle$ and 82.68% for phase state $|-\rangle$. The extinction ratio is 18.65 dB for time-bin state $|0\rangle$ and 15.46 dB for time-bin state $|1\rangle$. An asymptotic estimated secure key rate of 10.041 kbps is expected over a 20-km distance with an estimated QBER of 0.059. We give several possible reasons for the low visibility and low-stability that our system shows, based on which future work is needed to improve the performance.

Acknowledgements

Project supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306403), the National Natural Science Foundation of China (Grant Nos. 61435013 and 61627820), the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDB43000000), and the K. C. Wong Education Foundation, Anhui Initiative in Quantum Information Technologies, China (Grant No. AHY030000).

References

[1] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[2] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *Journal of Cryptology* **5** 3
[3] Muller A, Zbinden H and Gisin N 1996 *Europhys. Lett.* **33** 335
[4] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[5] Bonfrate G, Harlow M, Ford C, Maxwell G and Townsend P D 2001 *Electron. Lett.* **37** 13
[6] Honjo T, Inoue K and Takahashi H 2004 *Opt. Lett.* **29** 2797
[7] Nambu Y, Hatanaka T and Nakamura K 2004 *Jpn. J. Appl. Phys.* **43** L1109
[8] Kimura T, Nambu Y, Hatanaka T, Tomita A, Kosaka H and Nakamura K 2004 *Jpn. J. Appl. Phys.* **43** L1217
[9] Nambu Y, Yoshino K i and Tomita A 2006 *Jpn. J. Appl. Phys.* **45** 5344
[10] Nambu Y, Yoshino K i and Tomita A 2008 *J. Mod. Opt.* **55** 1953
[11] Tanaka A, Fujiwara M, Nam S W, Nambu Y, Takahashi S, Maeda W, Yoshino K i, Miki S, Baek B, Zhen W, Tajima A, Tomita A and Sasaki M 2008 *Optical Fiber Communication Conference/National Fiber Optic Engineers Conference*, 2008/02/24, San Diego, California, USA, p. OWJ2
[12] Tanaka A, Fujiwara M, Nam S W, Nambu Y, Takahashi S, Maeda W, Yoshino K-i, Miki S, Baek B, Wang Z, Tajima A, Sasaki M and Tomita A 2008 *Opt. Express* **16** 11354
[13] Tomita A, Yoshino K-i, Nambu Y, Tajima A, Tanaka A, Takahashi S, Maeda W, Miki S, Wang Z, Fujiwara M and Sasaki M 2010 *Opt. Fiber Technol.* **16** 55
[14] Tanaka A, Fujiwara M, Yoshino K, Takahashi S, Nambu Y, Tomita A, Miki S, Yamashita T, Wang Z, Sasaki M and Tajima A 2012 *IEEE J. Quantum Electron.* **48** 542
[15] Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner M G, Natarajan C M, Hadfield R H, O'Brien J L and Thompson M G 2017 *Nat. Commun.* **8** 13984

[16] Vaquero A, Kirkwood, R A , Burenkov, V, Chunnilall, C J, Sinclair A G, Hart A, Semenenko H, Sibson P Erven C and Thompson M G 2018 *SPIE Photonics Europe, Quantum Technologies*, 106741A-1–106741A-8

[17] Ma C, Sacher W D, Tang Z, Mikkelsen J C, Yang Y, Xu F, Thiessen T, Lo H K and Poon J K S 2016 *Optica* **3** 1274

[18] Wang J, Bonneau D, Villa M, Silverstone J W, Santagati R, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner M G, Natarajan C M, Hadfield R H, O'Brien J L and Thompson M G 2016 *Optica* **3** 407

[19] Sibson P, Kennard J E, Stanisic S, Erven C, O'Brien J L and Thompson M G 2017 *Optica* **4** 172

[20] Cai H, Long C M, DeRose C T, Boynton N, Urayama J, Camacho R, Pomerene A, Starbuck A L, Trotter D C, Davids P S and Lentine A L 2017 *Opt. Express* **25** 12282

[21] Avesani M, Calderaro L, Schiavon M, Stanco A, Agnesi C, Santamato A, Zahidy M, Scriminich A, Foletto G, Contestabile G, Chiesa M, Rotta D, Artiglia M, Montanaro A, Romagnoli M, Sorianello V, Vedovato F, Vallone G and Villoresi P 2021 *npj Quantum Information* **7** 93

[22] Geng W, Zhang C, Zheng Y, He J, Zhou C and Kong Y 2019 *Opt. Express* **27** 29045

[23] Zhang G, Haw J Y, Cai H, Xu F, Assad S M, Fitzsimons J F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C and Liu A Q 2019 *Nat. Photon.* **13** 839

[24] Aratake A, Tsuzuki K, Ishii M, Saida T, Goh T, Doi Y, Yamazaki H, Fukumitsu T, Yamada T and Mino S 2020 *IEICE Trans. Electron.* **103** 353

[25] Nambu Y, Hatanaka T and Nakamura K 2004 *Jpn. J. Appl. Phys.* **43** L1109

[26] Ren M, Li X, Zhang J, Wang L, Wang Y, Wu Y and An J 2020 *Optics & Laser Technology* **122** 105837

[27] Li X, Ren M, Zhang J, Wang L, Chen W, Wang Y, Yin X, Wu Y and An J 2021 *Photon. Res.* **9** 222

[28] Lo H K and Preskill J 2007 *Quantum Information and Computation* **7** 431

[29] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145