


Decoy-State Quantum Key Distribution Over a Long-Distance High-Loss Air-Water Channel

Cheng-Qiu Hu^{1,2}, Zeng-Quan Yan^{1,2}, Jun Gao^{1,2}, Zhan-Ming Li^{1,2}, Heng Zhou^{1,2}, Jian-Peng Dou^{1,2}, and Xian-Min Jin^{1,2,*}

¹*Center for Integrated Quantum Information Technologies (IQIT), School of Physics and Astronomy and State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, China*

²*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

 (Received 6 August 2020; revised 15 January 2021; accepted 5 February 2021; published 24 February 2021)

Atmospheric free space and fiber have been widely exploited as the channels for quantum communication, and have enabled intercontinent and intercity applications. An air-sea free-space channel, being capable of linking the satellite-based quantum resource and underwater vehicle, has now become the last piece of the puzzle in building a global quantum communication network. Here, we present an experimental demonstration of air-water decoy-state quantum key distribution against high loss, meanwhile keeping a low quantum bit error rate less than 2.5% for different distances. We are able to reach a long-distance quantum key distribution in water channel that can enable real-life air-sea quantum-communication tasks. The demonstrated distance, even in coastal water of Jerlov type III, is up to 30 m, about one-order improvement over the proof-in-principle demonstrations in the previous experiments, and the channel loss is equivalent to 345-m-long clean seawater of Jerlov type I, representing a key step forward to practical air-sea secure communication.

DOI: [10.1103/PhysRevApplied.15.024060](https://doi.org/10.1103/PhysRevApplied.15.024060)

I. INTRODUCTION

Quantum key distribution (QKD), as an ingenious combination of traditional cryptography and quantum mechanics, allows remote individuals to share secrets with unconditional security. The first QKD protocol (known as BB84) was proposed in the mid 1980s and implemented over a 32-cm-long free-space air channel [1], after which worldwide researches ensued [2–6]. So far, satellite-based quantum resource [7–9] and fiber-linked quantum network [10–14] are applicable for intercontinental and intercity QKD, leaving only the links between the airborne quantum resource and the underwater vehicles unbuilt.

Compared with the 3-dB attenuation by aerosphere [15], only tens of meters of underwater free space will cause orders of magnitude higher photon loss. One of the core problems of air-sea QKD is to overcome the huge channel loss while still possessing security. Another problem is to directly share the time frame between the underwater terminal and the air-borne part. Fortunately, the proposal of the decoy-state method [16–18] makes it possible for practical QKD to overcome high channel loss up to 40–50 dB and at the same time remain unconditionally

secure [19–21]. In addition, we also develop a time-synchronization method using blue-green optical signals through underwater channel, which allows the air-borne terminal and its underwater counterpart to directly share the precise time reference.

It has been proved that photonic polarization and entanglement can be well maintained through a water channel [22,23]. Progresses have also been made in theoretical analysis [24–26] and underwater experiments using polarization encoding [22,23,27,28] and twisted photons [29–31], however, they are still limited as a proof-of-principle demonstration, in which the longest water channel is merely several meters.

In this work, we successfully implement quantum key distribution through a long and high-loss air-water channel with an average quantum bit error rate (QBER) less than 2.5%. The advantages of our self-developed high-speed blue-green QKD system and three-intensity decoy-state protocol allow our system to tolerate total high loss up to 35 dB and the underwater channel to reach 30 m long. Moreover, the channel loss of the underwater part is 27 dB, as high as in 345-m-long clean seawater of Jerlov type I, which is comparable with the ordinary submergence depth of underwater vehicles, thus making our results a useful step towards practical air-sea quantum links.

*xianmin.jin@sjtu.edu.cn

II. EXPERIMENTAL SETUP

In order to reach a long-distance underwater channel similar to a natural field situation, we choose a large-scale marine test platform to implement our experiment. As shown in Fig. 1(c), the whole platform is in a semiopen environment with a water pool measuring 300 m long, 16 m wide, and 10 m deep, which is close to a real field condition. Considering the impact of the air-sea interface on QKD, our experiment is designed to be the air-water way that involves 2-m-long free-space channels in both ends and the underwater channel [denoted by the dashed red line in Fig. 1(c)] between the air channels. The photon incident angle at the air-water interface is set to near 90° .

For the transmitter's end (referred to as Alice), we design a compact transmitter system for generating the quantum signals. The Alice end mainly contains two parts: a self-made BB84-encoding module of size $30 \times 30 \text{ cm}^2$ [see Fig. 1(a)] and a self-assembled laser system. We use four blue laser diodes to prepare decoy states and a green laser diode for time synchronization. An eight-channel arbitrary-wave generator (AWG) producing the key patterns is linked to the laser modulating port.

For the receiver's end (referred to as Bob), we use a two-lens system to collimate the laser beam and detect the photons using five silicon single-photon detectors ($D1-D5$) after the polarization measurement. As shown in Fig. 1(b), the BB84-decoding module mainly consists of a 50:50 beam splitter (BS), a half-wave plate (HWP), and two polarization beam splitters (PBSs).

III. FAST MODULATION AND POLARIZATION ENCODING IN THE BLUE-GREEN WINDOW

Like the wavelength around 1550 nm is usually used in fiber [12,13], the blue-green optical window (generally refers to 400–500 nm) is preferred involving underwater channel, wherein photons experience less loss and therefore can be utilized for cross-medium communication. Here, we choose the center wavelength at 450 and 520 nm for signal and timing pulses, respectively. According to the results of the previous researches [15,22,23], polarization encoding is suitable for QKD in underwater free space as well as in atmosphere because of its high fidelity through these channels. A big challenge is that unlike the telecom wavelengths, where polarization modulating (PM) technology (e.g., high-speed electro-optic modulator) is mature

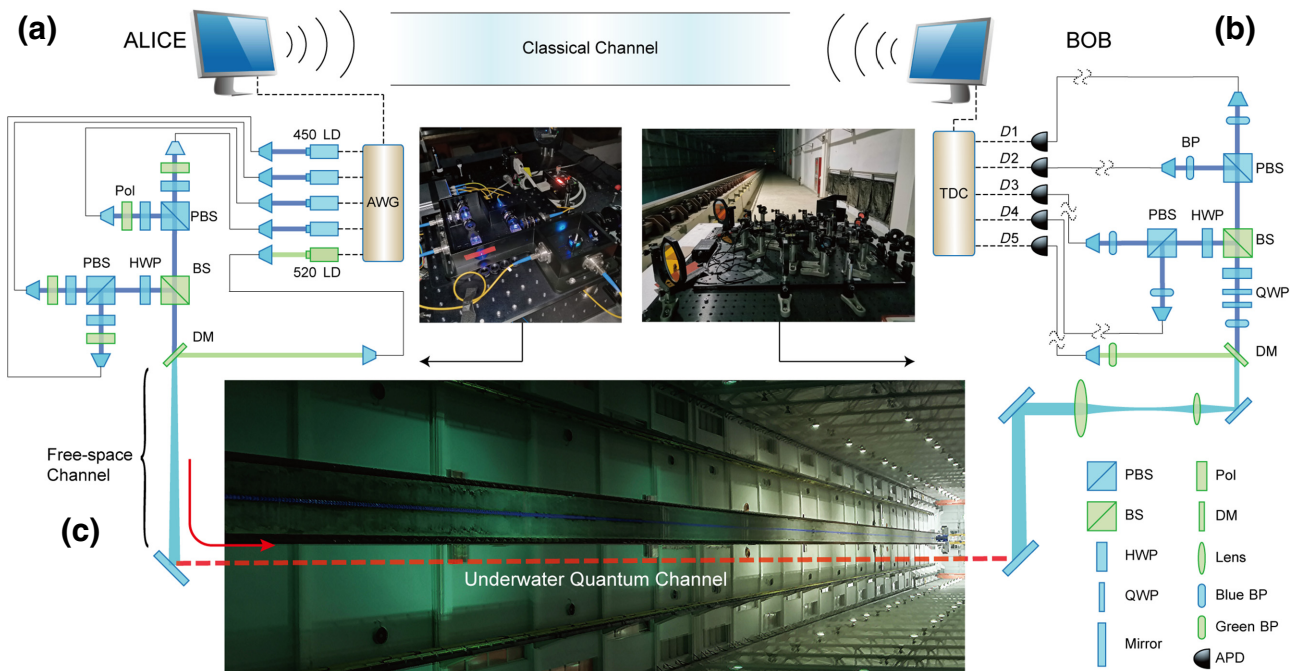


FIG. 1. Experimental setup. (a),(b) Illustration and photograph of the Alice and Bob end. At the Alice end, four blue laser diodes (450 LDs) are driven by the arbitrary wave generator (AWG) to emit short pulses (3 ns, 50 MHz). Their light beams are overlapped at the (polarization) beam splitters (PBS, BS). A green laser diode (520 LD) is used for synchronization. A dichroic mirror (DM) is used to combine the 450-nm and the 520-nm beams. The combined laser beam goes through a 2-m-long free-space channel and is guided to the underwater channel by two mirrors. At the Bob end, the laser beam is collimated and led to the BB84 decoding module by mirrors and lens. Blue and green bandpass filters (BP) are used for spectrum filtering. Photons are detected by the five single-photon detectors ($D1-D5$) and the time is recorded by the time-to-digital converter (TDC). Alice and Bob use the local area network for classical communication. (c) Photograph of our experimental site. The underwater channel is denoted by the dashed red line. HWP, half-wave plate; QWP, quarter-wave plate; Pol, polarizer; APD, avalanche photodiode.

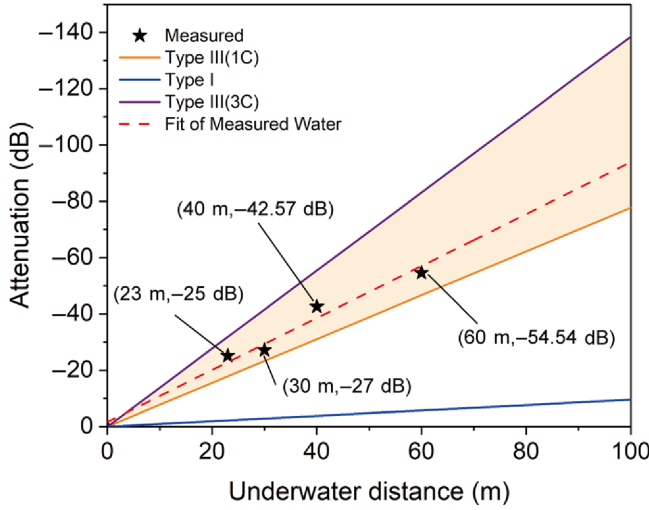


FIG. 2. (a) Power stability tested over 150 min. The average power is 1.242 mW and the variation is less than 0.017 mW (1.5%). (b) Temporal shape of the signal pulse. We use the single-photon detectors and time-to-digital converter to record the photon counts and reconstruct the temporal shape of the signal pulse. The pulse width is approximately 3 ns and the time window we pick in the experiment is 5 ns. (c),(d) Optical attenuation in different types of water. The corresponding optical wavelength: (c) 450 nm, (d) 520 nm. The attenuation of the water (denoted by the asterisks) in the experiment is between Jerlov type III(1C) and Jerlov type III(3C).

[32,33], there is no such effective PM modulator for the blue-green region in prior art.

To produce the high-speed and narrow pulses required by our experiment, we use voltage signals to directly modulate four independent laser diodes at a repetition rate up to 50 MHz. Each laser then goes through a HWP and a polarizer to precisely normalize its intensity and define its polarization. The laser diodes are integrated with a closed-loop temperature control so that their output powers and spectrum are stabilized. The stability performance of our self-assembled laser system and the optical signal pulse are presented in Figs. 2(a) and 2(b). The power variation of our laser system is less than 1.5% over the test time of two and a half hours. The temporal shape of the signal pulse we obtain is near Gaussian and its width is narrow enough to be covered by the 5-ns time window for the signal coincidence and noise filtering.

IV. EXPERIMENTAL PROCEDURE

We first characterize the underwater channel loss in several different distances, i.e., 23, 30, 40, and 60 m with 450- and 520-nm lasers and the obtained water attenuation listed in Table I. Referring to Jerlov's definition of water types [34,35], we plot the results in Figs. 2(c) and 2(d), from which we can see that our water is between Jerlov type III(1C) and Jerlov type III(3C) [36]. Here, the Jerlov water

TABLE I. Measured attenuation of the water in the experiment.

Distance/m	23	30	40	60
450 nm	25.13 dB	27.15 dB	42.57 dB	54.54 dB
520 nm	20.60 dB	23.17 dB	33.98 dB	49.72 dB

type (I, II, or III) is a parameter usually used for describing the clarity of water. For the 450-nm wavelength, the attenuation coefficient of Jerlov type I is 0.023 m^{-1} , i.e., 0.1 dB/m if converted to dB/m. The coefficient of Jerlov type II and type III are 0.062 m^{-1} (0.27 dB/m) and 0.124 m^{-1} (0.54 dB/m), respectively. Generally, the water in deep ocean belongs to the Jerlov type I and the shallow water far away from the coast is between Jerlov type I and type II. The coastal water is usually turbid and belongs to the Jerlov type III.

Taking the channel loss into consideration, the decoy-state BB84 protocol, which possesses the immunity to photon-number-splitting (PNS) attack and thus enables secure QKD using a weak coherent laser source over a high-loss channel, is a reasonable option for our experiment. By randomly mixing several decoy states of different intensities with certain proportions at the source of the transmitter, secret sharers make sure any PNS eavesdropping can be detected. Here, we utilize attenuators and adjust independent HWPs to get accurate three-intensity decoy states, of which the average photon numbers per pulse are high $u_s = 0.9$, moderate $u_1 = 0.3$, and vacuum $u_2 = 0$. The mixing ratio are 50, 25, and 25% for u_s , u_1 , and u_2 , respectively.

We use the four polarization states: horizontal (H), vertical (V), $+45$ (D), and -45 (A) equiprobably to encode the secret keys. For clarity, we illustrate the encoding protocol in Fig. 3(a). For each round, a 4-bit random number is consumed to drive the four lasers and determine which polarization and intensity level the pulse will be. We use four 450-nm laser diodes with a repetition rate of 50 MHz to prepare quantum signals according to decoy-state protocol. A 520-nm pulsed laser with a repetition rate of 500 KHz serves as the beacon light and the timing signal.

At the Bob end, we use a dichroic mirror (DM) to coarsely separate the photons of two different wavelengths, after which most of the 520-nm photons are reflected and detected by the $D5$. Then the 450-nm photons are further purified by the blue bandpass filter (center wavelength at 445 nm, band width 20 nm). Apart from the BB84 decoding module, there are two QWPs and a HWP functioning as polarization compensation, which we accurately adjust to calibrate the whole system before the QKD process. The four polarization states: H , V , D , and A are prepared at the Alice end and sent to Bob for testing. Figure 3(b) shows the fidelities of these states after the calibration. The average fidelity is as high as 0.982, which indicates that the system is ready for proceeding QKD.

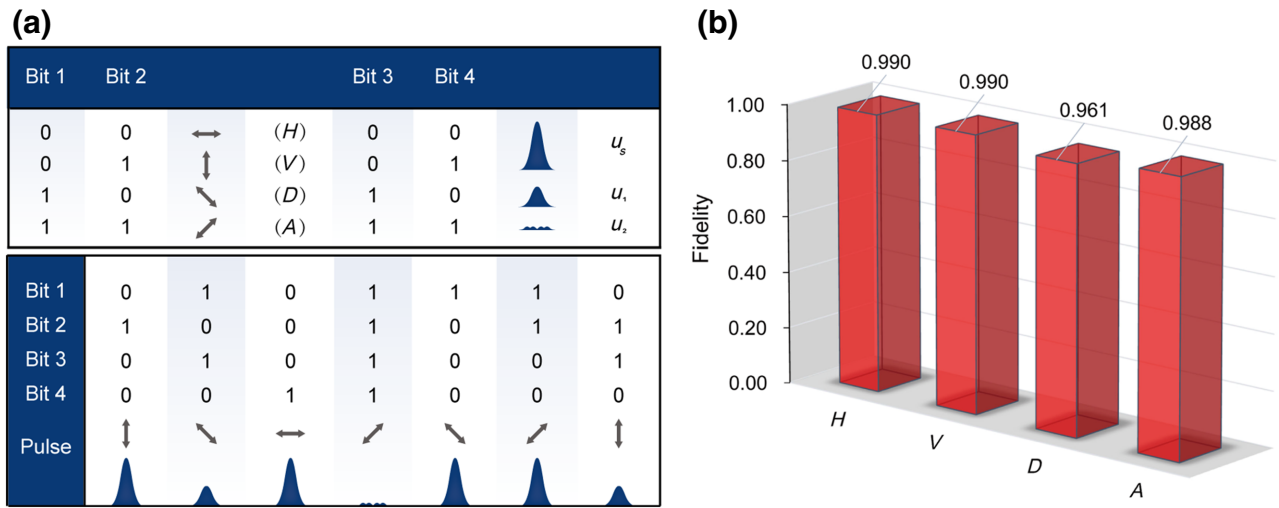


FIG. 3. (a) Illustration of the encoding protocol. Bit1 and bit2 decide the polarization states. At the same time, bit3 and bit4 decide the pulse intensity. For example, the combination of the 4-bit random number {0111} leads to a high-intensity pulse u_s of the state V . Some other combinations are listed in the bottom half of the table. (b) The fidelities of the four polarization states. High fidelities (>0.96) are obtained for all the four encoding states after the system calibration, of which the average value is up to 0.982.

V. RESULTS

The spot diameter of the light beam arriving at the Bob end after the collimation is approximately 2 mm. Through a fine optical alignment (see Appendix A), we finally obtain a photon collecting efficiency up to 70%. The single-photon detectors used in experiment possess an average quantum efficiency of 20% (25%) for 450-nm (520-nm) photons, an average dark count less than 50 Hz and time jitter less than 250 ps. The total loss of our system is about 35 dB. By spatial and spectrum filtering, the environment background noise is suppressed to approximately 100 Hz. The photoelectric signals of $D1-D5$ are collected by the time-to-digital converter and then sent to Bob's computer. We design a software for real-time post-processing, which includes base sifting, error estimation, error correction, and privacy-amplification process.

In two different distances of underwater channel (23 m and 30 m), we continuously run the system for 140 rounds, successfully sharing secret keys 72.8 Kbit in 23 m and 30.5 Kbit in 30 m. The experimental parameters of both distances over the first 30 rounds are shown in Table II, from which we can see the average QBER is less than 1.7% (2.5%) in 23 m (30 m). In the 23-m experiment, we obtain a maximum key rate of 715 bit/s in one single round and an average key rate $R_t = 595$ bit/s over the first 30 rounds.

TABLE II. Key parameters of the QKD experiment. E_u is the quantum bit error rate. Q_u and Q_v are the gains of the signal states u_s and the decoy states u_i . R_L is the key generation rate. R_t is the bit rate of the final keys.

	E_u	Q_u	Q_v	R_L (pulse $^{-1}$)	R_t (s $^{-1}$)	Total click
23 m	0.0169	7.07×10^{-5}	1.66×10^{-5}	2.38×10^{-5}	595.0	19 900
30 m	0.0248	3.04×10^{-5}	7.76×10^{-6}	8.82×10^{-6}	220.5	8725

We also present the detailed results of the 30-m experiment in Figs. 4(a) and 4(b) to show the system performance during a consecutive period of time. The average sifted key rate and the final key rate over the 30 rounds are 427.3 and 220.5 bit/s, respectively. With this key rate, sharing a 20byte personal banking password need only approximately 0.7 s. The average base sifting ratio is 0.489, which is very close to the ideal case 0.5. In addition, the individual error rate of each polarization state is analyzed and plotted in Figs. 4(c) and 4(d). An average error rate of 1.76% is obtained for the four encoding states.

The main contribution (about 70%) of the QBER comes from the device imperfections and imperfect polarization compensation. Other error leading factors include the dark count of the single-photon detectors, the environment background noise and the laser source background.

VI. CONCLUSION AND DISCUSSION

We successfully demonstrate QKD through a 30-m-long underwater channel with high loss. Our self-developed blue-green QKD system can tolerate up to 27-dB water attenuation and total system loss of 35 dB. As illustrated in Fig. 5, the same channel loss allows quantum communication over 345-m-long (120-m-long) water channel of Jerlov type I (II) according to the GLLP [4] analysis

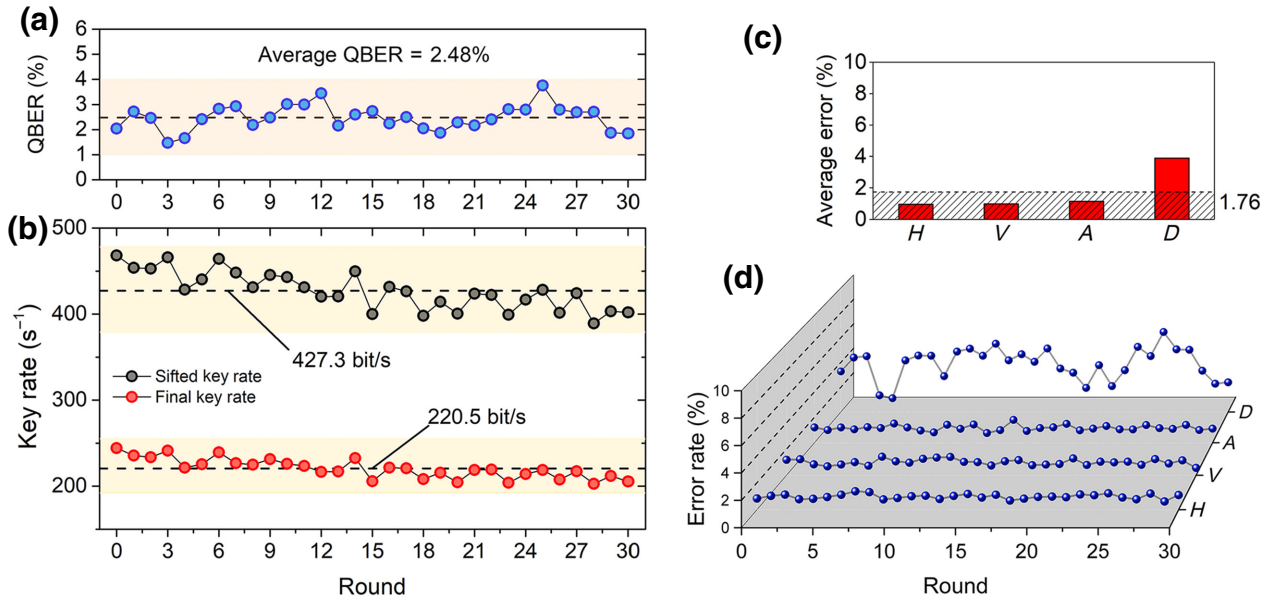


FIG. 4. Results of 30-m underwater QKD experiment. (a) The QBER of the first 30 rounds of QKD. The average QBER is 2.48%. (b) The sifted key rate and the final key rate. We obtain an average sifted (final) key rate of 427.3 bit/s (220.5 bit/s). (c),(d) Error rates of the four different encoding states. The error of each state over time is plotted in (d) and their average values are represented by the histograms in (c).

combined with the decoy method [18]:

$$R \geq q\{-Q_u f(E_u)H_2(E_u) + Q_1[1 - H_2(e_1)]\}, \quad (1)$$

where q depends on the sifting rate (in our experiment is 0.489). Q_1 and e_1 are the gain and the error rate of single-photon states, of which the lower bound and upper bound can be estimated by the decoy method. The long distance up to hundreds of meters reaches the submergence depth of ordinary underwater vehicles, and thus is promising for many practical applications, such as quantum communication between submersibles and satellites. Moreover, as seawater is a natural filter for most of the sunlight, optical noise will be significantly suppressed and therefore is negligible even in daytime at this depth under the sea. Combined with the fiber-connecting network and satellite-based resource, if only we could build the air-sea quantum links, the paradigm of the global quantum network would change.

Due to the skin effect, traditional rf signal can penetrate only a few meters of seawater. On the one hand, it makes the rf signal impractical for cross-medium communication. Meanwhile, in classical underwater wireless optical communication, the laser (or light-emitting diode) power is usually at mW–W level and the reached underwater distance is limited to 100–200 meters using traditional technology, wherein the channel loss is about 40–80 dB [37,38]. Noted in our QKD system, the emitting power of the light source is about 10^{-11} W as we strongly attenuate the laser to single-photon level, which is 110 dB lower

compared with the approximately W laser source, yet we can still obtain the bits after 27-dB channel loss. Extending the quantum techniques to the traditional underwater

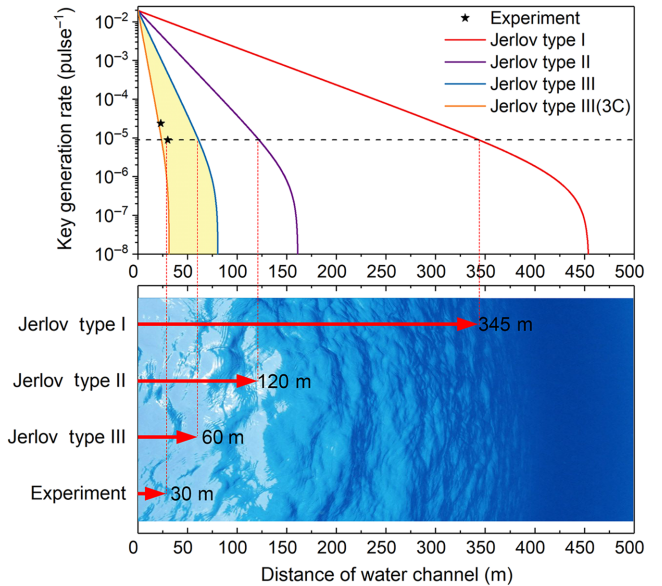


FIG. 5. Key generation rates in different distances of underwater channel. The relation curves are given by the GLLP analysis combined with the decoy method and the asterisks denote our experimental results. The bottom half of the figure shows that different distances can be achieved in different types of water, wherein photons will experience the same channel loss as in our 30-m experiment.

wireless optical communication, up to approximately 140 dB of channel loss can be tolerable, about 6 order of magnitude higher than the existing record and may hopefully push the underwater distance to even more than 1 km. Although limited by the repetition rate of single-photon detectors working on the Geiger mode, the communication bit rate might be relatively low. In the future, the use of the array of such detector chips instead of one single detector may solve this problem. For example, a 100-pixel array of single-photon detector chips can support the data rate up to 100 Mbit/s.

On the other hand, the direct realization of high-precision time synchronization for remote clocks, which often uses microwave or infrared signals in free-space air [39,40], is so far unachievable between the air-borne terminal and its underwater counterpart due to the high signal attenuation of seawater. In our experiment, we successfully synchronize Bob's clock with Alice's with a time error less than 0.5 ns per second through the high-loss long-distance underwater channel, which also provides possibilities for time transfer between satellites and underwater vehicles.

ACKNOWLEDGMENTS

The authors thank Jian-Wei Pan, Hang Li, Xiao-Ling Pang for helpful discussions. This research is supported by the National Key R&D Program of China (Grants No. 2019YFA0706302, No. 2019YFA0308700, and No. 2017YFA0303700), the National Natural Science Foundation of China (Grants No. 11904229, No. 11690033, No. 61734005, and No. 11761141014), the Science and Technology Commission of Shanghai Municipality (STCSM) (Grants No. 20JC1416300, No. 2019SHZDZX01, and No. 17JC1400403), and the Shanghai Municipal Education Commission (SMEC) (Grants No. 2017-01-07-00-02-E00049). X.-M.J. acknowledges additional support from a

Shanghai Talent Program and support from Zhiyuan Innovative Research Center of Shanghai Jiao Tong University.

APPENDIX A: OPTICAL ALIGNMENT

A good optical alignment through the underwater channel is very challenging. As shown in Fig. 6, to keep the polarization components (H , V , D , A) balanced at the receiver's end, perfectly overlapped spatial modes of the four signal paths must be guaranteed. Thus, we collect the signal beams into a single-mode fiber after the BS in the transmitter. The coupling efficiency of each component can be adjusted independently to reach the same value (50%). Firstly, we use the DM to combine the signal and the beacon light. We tune the collimator of the beacon light to change the pointing angle and focal length so that the spatial mode overlaps the signal light over a long distance of free space (200 m). Then we switch the 520LD to high-power mode and guide the combined light into water. After attenuation of the underwater channel, only the green beacon light is visible. We coarsely adjust the large-size mirrors at the Alice end to control the pointing direction and finely tune the large-size mirrors at the Bob end so that the light is well collected by the lens system, after that the optical alignment is finished.

APPENDIX B: THE POST PROCESSING

The postprocessing of our QKD demonstration mainly includes the time synchronization, base sifting, error estimation, error correction, and privacy amplification, of which the key procedure is the time synchronization.

First, Alice and Bob need to share a common time frame, which means the bit sequence detected by Bob corresponding to the optical pulses generated by Alice need to be matched with correct time tags. Here, we use the 500-KHz green laser pulses to define a relative time reference. At the

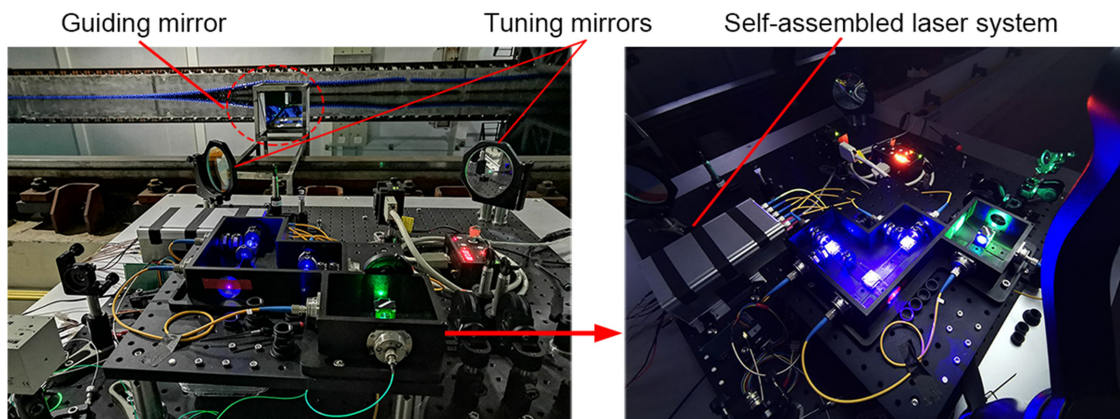


FIG. 6. QKD transmitter. For the transmitter's end (referred to as Alice), we design a compact transmitter system for generating the quantum signals. The Alice end mainly contains two parts: a self-made BB84-encoding module of size $30 \times 30 \text{ cm}^2$ and a self-assembled laser system. We use four blue laser diodes to prepare decoy states and a green laser diode for time synchronization. An eight-channel arbitrary-wave generator producing the key patterns is linked to the laser modulating port.

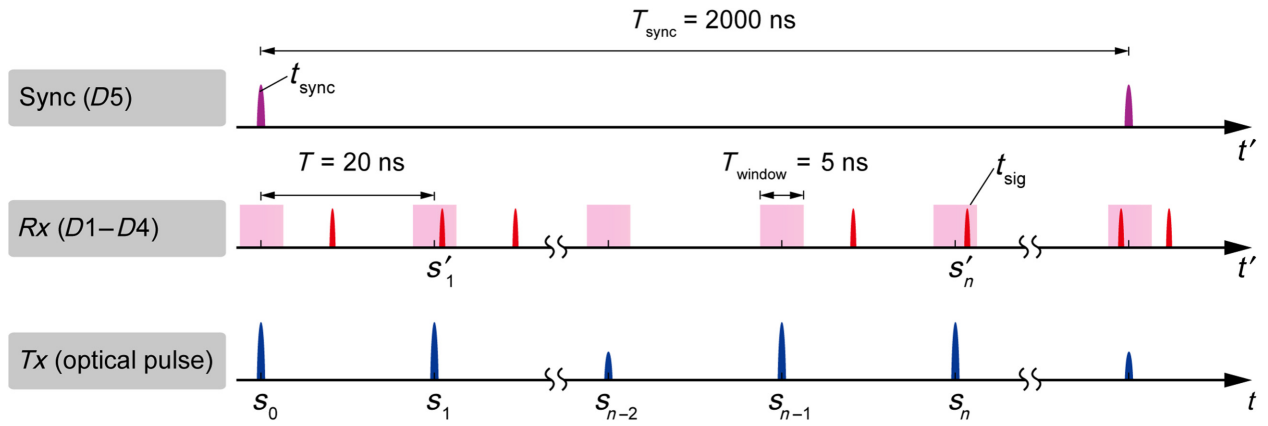


FIG. 7. Bit sequence.

Bob end, most of the green pulses will be detected by our APD ($D5$), and the time is also recorded by the TDC and denoted as t_{sync} . Between any two adjacent synchronization pulses, there are 100 signal pulses transmitted by Alice (tagged as s_0, s_1, s_2, s_{99}). Due to the time jitter of the APD (250 ps) and the limited time resolution of the TDC (64 ps), the detected events by Bob may deviate slightly from the base time and mix with some noise as well. Thus, we set a time window of $T_{\text{window}} = 5$ ns, and ascertain the time tag of any recorded event t_{sig} by the following algorithm:

$$n = \lfloor \frac{t_{\text{sig}} - t_{\text{sync}} + \Delta t}{\bar{T}} \rfloor$$

$$\text{if } \text{mod} \left(\frac{t_{\text{sig}} - t_{\text{sync}} + \Delta t}{\bar{T}} \right) \leq T_{\text{window}}, \quad (\text{B1})$$

wherein t_{sync} represents the adjacent synchronization event before t_{sig} and \bar{T} is the average signal period. The preoffset of the signal time is set to be $\Delta t = 2.5$ ns. If the event is within the time window, it will be regarded as a valid signal bit with sequence number n , otherwise it will be discarded

as noise. In this way we obtain the relative time tag s_n (see Fig. 7).

Owing to the high loss of the underwater channel, the sync pulses become single-photon level when they arrive at the Bob end. Thus, we use the on-off type single-photon detector for its high sensitivity, which also means some of the pulses can be missed. To solve this problem, we design a self-adapting algorithm, utilizing the accurate periodicity of the sync pulses to automatically recover the missed pulses as well as filtering out the error detections caused by random noise (see Fig. 8). In our experiment, only about 200 K of the sync signals can be detected, by which we perfectly recover the origin 500-KHz sync signals. Combining with the relative time reference mentioned before, the time synchronization for the whole system is completed.

Afterwards, Bob can share the accurate pulse positions he received with Alice. Alice then chooses the encoding messages (the first bit of the 4-bit random number for polarization encoding) of corresponding pulses and sends them to Bob for base sifting, after which about 49% of all the clicks are sifted as the raw keys. At the same time,

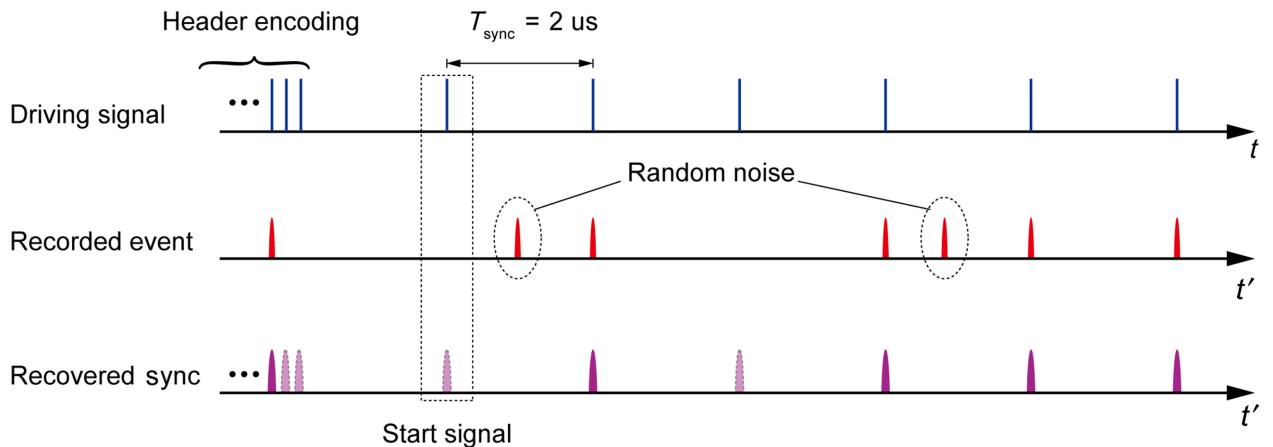


FIG. 8. Sync sequence.

Alice also calculates the checksums by dividing the raw keys into identical groups and shares them with Bob to finish the error estimation procedure. Subsequently, Bob sends back the estimated QBER and the low-density parity check (LDPC) matrix to Alice. Alice then uses this information to obtain the checking codes for error correction and the privacy-amplification parameter.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE New York, 1984), p. 175.
- [2] Hoi-Kwong Lo and Hoi Fung Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
- [3] Peter W. Shor and John Preskill, Simple Proof of Security of the bb84 Quantum key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [4] Daniel Gottesman, H-K. Lo, Norbert Lutkenhaus, and John Preskill, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.* (IEEE, Chicago, 2004), p. 136.
- [5] Marco Lucamarini, Zhiliang L. Yuan, James F. Dynes, and Andrew J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [6] Min Soo Lee, Min Ki Woo, Yong-Su Kim, Young-Wook Cho, Sang-Wook Han, and Sung Moon, Quantum hacking on a free-space quantum key distribution system without measuring quantum signals, *JOSA B* **36**, B77 (2019).
- [7] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, and Li Li *et al.*, Ground-to-satellite quantum teleportation, *Nature* **549**, 70 (2017).
- [8] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, and Zheng-Ping Li *et al.*, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [9] Hideki Takenaka, Alberto Carrasco-Casado, Mikio Fujiwara, Mitsuo Kitamura, Masahide Sasaki, and Morio Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, *Nat. Photonics* **11**, 502 (2017).
- [10] H. Jeff Kimble, The quantum internet, *Nature* **453**, 1023 (2008).
- [11] Masahide Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, and A. Tanaka *et al.*, Field test of quantum key distribution in the tokyo qkd network, *Opt. Express* **19**, 10387 (2011).
- [12] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nat. Photonics* **13**, 334 (2019).
- [13] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, Experimental measurement-device-independent quantum digital signatures, *Nat. Commun.* **8**, 1 (2017).
- [14] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, and Li-Xing You *et al.*, Measurement-Device-Independent Quantum key Distribution Over Untrustful Metropolitan Network, *Phys. Rev. X* **6**, 011024 (2016).
- [15] Xian-Min Jin, Ji-Gang Ren, Bin Yang, Zhen-Huan Yi, Fei Zhou, Xiao-Fan Xu, Shao-Kai Wang, Dong Yang, Yuan-Feng Hu, and Shuo Jiang *et al.*, Experimental free-space quantum teleportation, *Nat. Photonics* **4**, 376 (2010).
- [16] Won-Young Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [17] Xiang-Bin Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [18] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [19] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, and Yan-Lin Tang *et al.*, Direct and full-scale experimental verifications towards ground–satellite quantum key distribution, *Nat. Photonics* **7**, 387 (2013).
- [20] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter, Air-to-ground quantum communication, *Nat. Photonics* **7**, 382 (2013).
- [21] Alessandro Fedrizzi, Rupert Ursin, Thomas Herbst, Matteo Nespoli, Robert Prevedel, Thomas Scheidl, Felix Tiefenbacher, Thomas Jennewein, and Anton Zeilinger, High-fidelity transmission of entanglement over a high-loss free-space channel, *Nat. Physics* **5**, 389 (2009).
- [22] Ling Ji, Jun Gao, Ai-Lin Yang, Zhen Feng, Xiao-Feng Lin, Zhong-Gen Li, and Xian-Min Jin, Towards quantum communications in free-space seawater, *Opt. Express* **25**, 19795 (2017).
- [23] Cheng-Qiu Hu, Zeng-Quan Yan, Jun Gao, Zhi-Qiang Jiao, Zhan-Ming Li, Wei-Guan Shen, Yuan Chen, Ruo-Jing Ren, Lu-Feng Qiao, and Ai-Lin Yang *et al.*, Transmission of photonic polarization states through 55-m water: Towards air-to-sea quantum communication, *Photonics Res.* **7**, A40 (2019).
- [24] John Gariano and Ivan B. Djordjevic, Theoretical study of a submarine to submarine quantum key distribution systems, *Opt. Express* **27**, 3055 (2019).
- [25] Amir Hossein Fahim Raouf, Majid Safari, and Murat Uysal, Performance analysis of quantum key distribution in underwater turbulence channels, *JOSA B* **37**, 564 (2020).
- [26] Shi-Cheng Zhao, Xin-Hong Han, Ya Xiao, Yuan Shen, and Yong-Jian Gu, Wen-Dong Li, Performance of underwater quantum key distribution with polarization encoding, *JOSA A* **36**, 883 (2019).
- [27] Shicheng Zhao, Wendong Li, Yuan Shen, YongHe Yu, Xin-Hong Han, Hao Zeng, Maoqi Cai, Tian Qian, Shuo Wang, and Zhaoming Wang *et al.*, Experimental investigation of quantum key distribution over a water channel, *Appl. Opt.* **58**, 3902 (2019).
- [28] Dong-Dong Li, Qi Shen, Wei Chen, Yang Li, Xuan Han, Kui-Xing Yang, Yu Xu, Jin Lin, Chao-Ze Wang, and Hai-Lin Yong *et al.*, Proof-of-principle demonstration of

- quantum key distribution with seawater channel: Towards space-to-underwater quantum communication, *Opt. Commun.* **452**, 220 (2019).
- [29] Yuan Chen, Wei-Guan Shen, Zhan-Ming Li, Cheng-Qiu Hu, Zeng-Quan Yan, Zhi-Qiang Jiao, Jun Gao, Ming-Ming Cao, Ke Sun, and Xian-Min Jin, Underwater transmission of high-dimensional twisted photons over 55 meters, *Photonix* **1**, 1 (2020).
- [30] Frédéric Bouchard, Alicia Sit, Felix Hufnagel, Aazad Abbas, Yingwen Zhang, Khabat Heshami, Robert Fickler, Christoph Marquardt, Gerd Leuchs, and Ebrahim Karimi *et al.*, Quantum cryptography with twisted photons through an outdoor underwater channel, *Opt. Express* **26**, 22563 (2018).
- [31] Felix Hufnagel, Alicia Sit, Florence Grenapin, Frédéric Bouchard, Khabat Heshami, Duncan England, Yingwen Zhang, Benjamin J. Sussman, Robert W. Boyd, and Gerd Leuchs *et al.*, Characterization of an underwater channel for quantum communications in the ottawa river, *Opt. Express* **27**, 26346 (2019).
- [32] A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, and Y. Kurochkin, Low loss qkd optical scheme for fast polarization encoding, *Opt. Express* **25**, 28886 (2017).
- [33] Costantino Agnesi, Marco Avesani, Andrea Stanco, Paolo Villorosi, and Giuseppe Vallone, All-fiber self-compensating polarization encoder for quantum key distribution, *Opt. Lett.* **44**, 2398 (2019).
- [34] N. G. Jerlov, in *Optical Oceanography* (Elsevier, 1968), p. 115.
- [35] R. A. Arnone, A. M. Wood, and R. W. Gould Jr., The evolution of optical water mass classification, *Oceanography* **17**, 14 (2004).
- [36] Michael G. Solonenko and Curtis D. Mobley, Inherent optical properties of jerlov water types, *Appl. Opt.* **54**, 5392 (2015).
- [37] Frank Hanson and Stojan Radic, High bandwidth underwater optical communication, *Appl. Opt.* **47**, 277 (2008).
- [38] Hemani Kaushal and Georges Kaddoum, Underwater optical wireless communication, *IEEE Access* **4**, 1518 (2016).
- [39] Isaac Khader, Hugo Bergeron, Laura C. Sinclair, William C. Swann, Nathan R. Newbury, and Jean-Daniel Deschênes, Time synchronization over a free-space optical communication channel, *Optica* **5**, 1542 (2018).
- [40] Hui Dai, Qi Shen, Chao-Ze Wang, Shuang-Lin Li, Wei-Yue Liu, Wen-Qi Cai, Sheng-Kai Liao, Ji-Gang Ren, Juan Yin, and Yu-Ao Chen *et al.*, Towards satellite-based quantum-secure time transfer, *Nat. Phys.* **16**, 848 (2020).