npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Intensity modulator for secure, stable, and high-performance decoy-state quantum key distribution

Feng-Yu Lu[1,2,3,4], Xing Lin[1,2,3,4], Shuang Wang[1,2,3]✉, Guan-Jie Fan-Yuan[1,2,3], Peng Ye[1,2,3], Rong Wang[1,2,3], Zhen-Qiang Yin[1,2,3], De-Yong He[1,2,3], Wei Chen[1,2,3], Guang-Can Guo[1,2,3] and Zheng-Fu Han[1,2,3]

The decoy-state method substantially improves the performance of quantum key distribution (QKD) and perfectly solves crucial issues caused by multiphoton pulses. In recent years, the decoy-state method has occupied a key position in practicality, and almost all the QKD systems have employed the decoy-state method. However, the imperfections of traditional intensity modulators limit the performance of the decoy-state method and bring side channels. In this work, a special intensity modulator and its accompanying modulation method are designed and experimentally verified for the secure, stable, and high-performance decoy-state QKDs. The experimental result indicates that its stable and adjustable intensities, convenient two-level modulation, inherently high speed, and compact structure is extremely fit for future trends and will help the decoy-state method to be perfectly applied to QKD systems.

npj Quantum Information (2021)7:75 ; https://doi.org/10.1038/s41534-021-00418-x

INTRODUCTION

Quantum key distribution (QKD)[1] provides a way for two legitimate remote users, namely, Alice and Bob, to share secret keys with information-theoretic security[2–6]. However, this security relies on the single-photon state while the ideal single-photon sources are not yet practically useful. As an alternative, a revolutionary method named the decoy-state method[7–9] is employed in almost all practical QKD systems. This method allows a practical system based on weak coherent pulse sources to achieve the security performance of a single-photon QKD, which is a perfect combination of theory and practice.

The decoy-state method significantly improves the secret key rate and achievable distance of practical systems, but the legitimate users have to modulate several different intensities[10–24] precisely and independently. Usually, a decoy-state QKD requires weak coherent pulses with three or more different intensities. Some systems also require a special decoy state named vacuum state. Compared with classic optical communications, the intensity modulation in QKD systems is more difficult since the conflict between completely random modulation and finite modulation bandwidth.

A good intensity modulation for decoy-state QKD should be secure, stable, and flexible. The 'secure' is a basic requirement that the modulation should not violate the security assumptions of the QKD. The 'stable' means the output intensities should be insensitive to disturbances in an electric signal. The 'flexible' is that the manipulation should be as simple as possible. Meanwhile, it is important for a good intensity modulation that it should not be a short slab of the system performance. However, existing modulators cannot meet all the above requirements at the same time. The most widely used commercial $LiNbO_3$-based Mach–Zehnder interferometer (MZI) is extremely sensitive to the electric signal disturbance, which violates the condition of 'stable', brings intensity fluctuation, and reduces the secret key rate[22,25–28]. To make the matter worse, a special intensity fluctuation named patterning effect[29] introduces correlation of adjacent signals, which provides additional information and allows Eve to perform sophisticated attacks since current security analysis usually assumes independent and identically distributed (*i. i. d*) pulses. The imperfection of the MZI modulator has shaken the basis of the QKD.

To fill the loophole in the intensity modulation, two countermeasures are proposed. The first one is a post-processing method[29]. It works by discarding some pulses depending on the state of predecessor and successor. Another countermeasure is an intensity modulator based on Sagnac interferometer[30]. It is used as a secure two-level intensity modulator for QKD, not only can mitigate the patterning effect but also is immune to the DC drift. The two countermeasures are secure and convenient but not so friendly to high-performance QKDs. The post-processing method ineluctably reduces the secret key rate since it discards too many key bits while the higher key rate is what people pursue in the QKD field. The Sagnac modulator is also not so suitable for the decoy-state method since its two-level intensity modulation and fixed stable intensities cannot meet the requirement of more than two adjustable intensities. Besides, the worst of it is that its common-path mechanism brings an inherent speed limit. Considering that the high-speed system is a trend of the QKD field, the Sagnac modulator may become a short slab in QKD systems in the future.

An interesting question is whether we can design an intensity modulator that can generate three, four, or even more stable intensities, and these stable intensities should be tunable to optimize intensities for improving the secret key rate[21,31–33]. Beyond that, it is lacing on the cake if its driving-voltages only switch between two different voltages, which would significantly reduce the modulation difficulty. Fortunately, the answer is yes. In this work, an intensity modulator named multipath Mach-Zehnder interferometer (MMZI) and its accompanying modulation method that meets all the above requirements are proposed. By working

[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui, PR China. [2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, PR China. [3]State Key Laboratory of Cryptology, Beijing, PR China. [4]These authors contributed equally: Feng-Yu Lu, Xing Lin. ✉email: wshuang@ustc.edu.cn

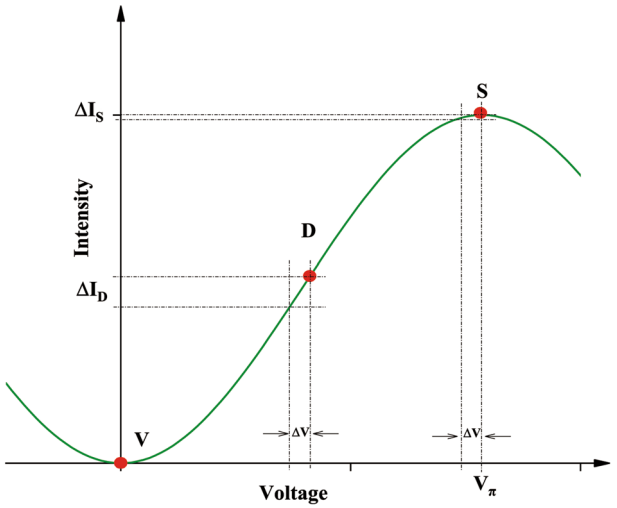

Fig. 1 The voltage response curve of a commercial $LiNbO_3$-based MZI with 50:50 splitting ratio. With the same voltage disturbance ΔV, the intensity difference ΔI on the slope point D is significantly larger than it on the stable point S. The V_π denotes the half-wave voltage.

only at the 'half-wave points', the MMZI can generate a variety of different stable intensities to mitigate the intensity fluctuation and the patterning effect for secure and robust QKD systems. The MMZI is also inherently high-speed and facility for integration due to the traveling-wave modulation and its compact structure.

RESULTS

Most QKD systems generate the decoy states by commercial $LiNbO_3$-based MZIs, in which an input pulse is first split into two parts by a 1×2 splitter and then recombined by a 2×1 coupler. The splitting ratios of the splitter and the coupler of commercial MZIs are both $\frac{1}{2}$. Thus, the output intensity $I(a)$ is

$$I(a)=\frac{\mu_{\text{in}}}{2}(1+\cos a), \tag{1}$$

where the a is the phase difference of the two paths and the μ_{in} is the input intensity. In many decoy-state QKD systems, commercial MZIs are applied to produce a signal state μ_s, a decoy state μ_d and a vacuum state $\mu_v=0$[20,23,34]. As illustrated in Fig. 1, the signal state corresponds to the flat peak point S and the decoy state corresponds to the slope point D. We define the points with 0 derivative as stable points. Here the point S is a stable point. It is obvious that comparing with the stable points, the slope points are more sensitive to disturbances such as timing jitter and electric waveform distortion, which would cause unforeseeable fluctuation on μ_a. Especially, in high-speed systems[35–37], a finite modulation bandwidth leads to a correlation between adjacent signals, namely, the intensity of a pulse would be correlated with its previous one, which violates the important *i.i.d.* assumption.

To make QKD systems more secure and robust, we present a MMZI and an accompanying modulation method, which can be perfectly applied to decoy-state QKD systems. By working at the half-wave voltage, the interferometer can generate several stable intensities to mitigate the intensity fluctuation and the patterning effect for the security. As illustrated in Fig. 2, the interferometer consists of an $1\times N$ splitter, a $N\times1$ coupler and N parallel paths. One of the path (path-0) includes a variable optical attenuator (VOA) to tune its attenuation ratio η and others paths (path-1 to $N-1$) each has a built-in phase modulator to shift the relative phases a_k for $k\in\{1, 2....N-1\}$. An input coherent pulse with intensity μ_{in} is first split by the $1\times N$ splitter whose splitting ratio to the path-k is denoted by t_k' and then modulated in each path.

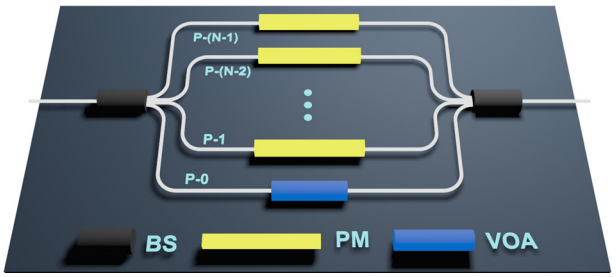

Fig. 2 The structure of our multipath Mach-Zehnder interferometer. In this modulator, input pulses are split by an $1\times N$ splitter and enter into N different paths. The path-0 has a VOA to attenuate the pulse and the path-1 to $N-1$ each has a phase modulator to modulate the relative phases. Finally, the split pulses interfere in a $N\times1$ coupler. P path; BS beam splitter; PM phase modulator; VOA variable optical attenuator.

After that, the pulses in each path couple and interfere in the $N\times1$ coupler whose splitting ratio to the path-k is denoted by t_k''. To make the following formulas clearer, we define $t_k=\sqrt{t_k't_k''}$.

Note that since QKD systems have an attenuator to attenuate the intensity to single-photon level[34–36,38–47], we ignore the insertion loss in the follows. The output pulse of the path-0 and path-k for $k\in\{1, 2, ..., N-1\}$ are, respectively, $\left|\sqrt{\eta}t_0\sqrt{\mu_{\text{in}}}\right\rangle$ and $\left|t_ke^{ia_k}\sqrt{\mu_{\text{in}}}\right\rangle$. After the interference, the MMZI outputs:

$$\left|\sqrt{\mu_{\text{out}}}\right\rangle=\left|\left(\sqrt{\eta}t_0+\sum_{k=1}^{N-1}t_ke^{ia_k}\right)\sqrt{\mu_{\text{in}}}\right\rangle. \tag{2}$$

The output intensity can be regarded as a function of relative phases:

$$\begin{aligned}I(a_1,a_2,....,a_{N-1})&=\langle\sqrt{\mu_{\text{out}}}|\sqrt{\mu_{\text{out}}}\rangle\\&=\mu_{\text{in}}\left[\eta{t_0}^2+2\sqrt{\eta}t_0\sum_{k=1}^{N-1}t_k\cos a_k\right.\\&\quad\left.+\sum_{k=1}^{N-1}{t_k}^2+\sum_{k=1}^{N-1}\sum_{l=k+1}^{N-1}2t_kt_l\cos(a_k-a_l)\right].\end{aligned} \tag{3}$$

Since the condition of a stationary point is that all its partial derivatives should be 0, namely, the

$$\begin{aligned}\frac{\partial I(a_1,a_2,....,a_{N-1})}{\partial a_k}&=-\left[2\sqrt{\eta}t_0t_k\sin a_k+\sum_{l}^{l\neq k}2t_kt_l\sin(a_k-a_l)\right]\\&=0,\ \text{for}\ k\in\{1,2,....,N-1\},\end{aligned} \tag{4}$$

the $\forall a_k\in\{0,\pi\}$ are general solutions of Eq. (4). For simplicity, we define these general solutions as the 'half-wave points' in the follows. In another word, when the voltages on each path is V_0 or V_π, the output intensity would be stable. Since each a_k can be tuned to be 0 or π, there are 2^{N-1} stable intensities, which can be denoted by $I_1, I_2, ..., I_{2^{N-1}}$.

For a specific decoy-state QKD system that requires optimized intensities $\mu_1, \mu_2, ..., \mu_n$, without loss of generality, we assume that the $\{I_1, I_2, ..., I_n\}$ and $\{\mu_1, \mu_2, ..., \mu_n\}$ are sorted in descending order. A user should firstly find a set of t_k and a η according to Eqs. (2) and (3) to make

$$\frac{I_i}{I_1}=\frac{\mu_i}{\mu_1},\ \text{for}\ i\in\{2....n\}. \tag{5}$$

After that, the user adjusts the attenuator in the QKD system to make the maximum intensity I_1, which always corresponds to the point $\forall a_k=0$, equals to the μ_1. Naturally the other stable intensities equal to the other optimized decoy states. We take the optimized intensity sets $[\mu_s=0.015, \mu_{d_1}=0.006, \mu_{d_2}=0.002, \mu_v=0]$ and $[\mu_s=0.43, \mu_{d_1}=0.19, \mu_{d_2}=$

0.05, $\mu_v = 0$] in the recent twin-field QKD experiments[45,46] as examples. We employ a three-path MMZI and denote its four stable intensities as $I(0, 0)$, $I(0, \pi)$, $I(\pi, 0)$ and $I(\pi, \pi)$, respectively. To generate the first optimized intensity set, an user should firstly set the splitting ratios and fine-tune the VOA to [$\sqrt{\eta}t_0 = 0.5$, $t_1 = 0.3170$, $t_2 = 0.1830$] to make the $I(0, \pi)/I(0, 0) = 0.4019$, $I(\pi, 0)/I(0, 0) = 0.1122$ and $I(\pi, \pi) = 0$. After that, he (she) adjust the attenuator in the QKD system to make $I(0, 0) = \mu_s = 0.015$, then naturally, the $I(0, \pi) = \mu_{d_1} = 0.006$, $I(\pi, 0) = \mu_{d_2} = 0.002$, and $I(\pi, \pi) = \mu_v = 0$. Similarly, to generate the second optimized intensity set, an user can set the t_k and η to [$\sqrt{\eta}t_0 = 0.5$, $t_1 = 0.3305$, $t_2 = 0.1695$] and adjust the attenuator in the QKD system to make $I(0, \pi) = \mu_{d_1} = 0.43$. Then the $I(0, \pi) = \mu_{d_1} = 0.19$, $I(\pi, 0) = \mu_{d_2} = 0.05$and $I(\pi, \pi) = \mu_v = 0$.

It is worth noting that, the stable intensities are adjusted by setting the splitting ratios and tuning the VOA. The MMZI would only has a limited tuning range when the splitting ratios are fixed. A more flexible structure with a larger tuning range can be achieved by adding VOA in each path. The details are introduced in the Discussion.

DISCUSSION

The stable intensities of the MMZI can be fine-tuned by the built-in VOA so that users can optimize the secret key rate. However, the tuning range is limited. In this section, another structure for improving the tuning range is proposed., As illustrated in Fig. 3, each path owns a VOA. The attenuation ratio of the path-k is denoted by η_k for $k \in \{0, 1, 2, ..., N-1\}$. By adjusting these η_k, the ratio of the stable intensities can be modified flexibly to meet the need for intensity optimization.

In order to simplify the problem, we assume that the splitter has a balanced splitting ratio, namely, $t_k = 1/N$ for $k \in \{0, 1, 2, ..., N-1\}$. The output state of the path-0 and the path-k ($k \in \{1, 2, ..., N-1\}$) are denoted by $\left|\frac{1}{N}\sqrt{\eta_0\mu_{\text{in}}}\right\rangle$ and $\left|\frac{e^{i\alpha_k}}{N}\sqrt{\eta_k\mu_{\text{in}}}\right\rangle$ respectively. the output state of the interferometer is:

$$\left|\sqrt{\mu_{\text{out}}}\right\rangle = \left|\frac{1}{N}\left(\sqrt{\eta_0} + \sum_{k=1}^{N-1}\eta_k e^{i\alpha_k}\right)\sqrt{\mu_{\text{in}}}\right\rangle. \tag{6}$$

The output intensity is:

$$\begin{aligned} I(\alpha_1, \alpha_2, ..., \alpha_{N-1}) &= \langle\sqrt{\mu_{\text{out}}}|\sqrt{\mu_{\text{out}}}\rangle \\ &= \frac{\mu_{\text{in}}}{N^2}\left(\eta_0 + 2\sqrt{\eta_0}\sum_{k=1}^{N-1}\sqrt{\eta_k}\cos\alpha_k \right. \\ &\quad \left. + \sum_{k=1}^{N-1}\eta_k + \sum_{k=1}^{N-1}\sum_{l=k+1}^{N-1} 2\sqrt{\eta_k\eta_l}\cos(\alpha_k - \alpha_l)\right). \end{aligned} \tag{7}$$

The outputs of the stable points mainly depend on η_k for $k \in \{0, 1, 2, ..., N-1\}$, namely, they can be modified flexibly by adjusting the built-in VOAs.

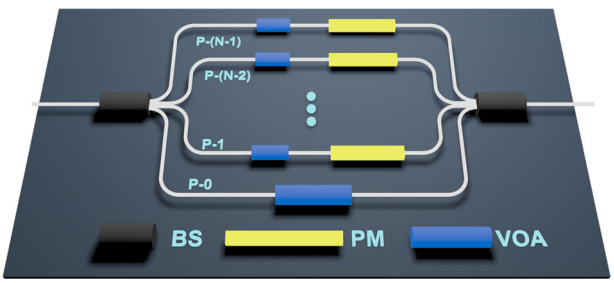

Fig. 3 A MMZI structure for improving the tuning range. In this scheme, each path owns a VOA. Adjusting attenuation ratios of these VOAs is equivalent to adjusting splitting ratios of the splitter and the coupler.

The partial derivative equations of Eq. (7) is expressed as:

$$\begin{aligned} \frac{\partial I(\alpha_1, \alpha_2, ..., \alpha_{N-1})}{\partial \alpha_k} &= -\frac{\mu_{\text{in}}}{N^2}\left[2\sqrt{\eta_0\eta_k}\sin\alpha_k + \sum_{l}^{l\neq k} 2\sqrt{\eta_k\eta_l}\sin(\alpha_k - \alpha_l)\right] \\ &= 0; \text{for } k \in \{1, 2, ..., N-1\}. \end{aligned} \tag{8}$$

Significantly, the general solution is also $\forall\alpha_k \in \{0, \pi\}$ for $k \in \{1, 2, ..., N-1\}$.

With the development of high-speed QKD systems, the widely used commercial $LiNbO_3$ MZIs are increasingly difficult to meet the need for security, robustness, and flexibility. To improve the performance of the decoy-state QKD and make it more practical, a MMZI and its accompanying modulation method are proposed in this work. Our method can generate 2^{N-1} different stable intensities to mitigate the intensity fluctuation and the patterning effect from imperfect modulation signals. The flexibility of its 'half-wave modulation' and tunable outputs makes it suitable for different protocols and systems. Its compact structure makes it easy to integrate. Besides, it is inherently high-speed due to the traveling-wave modulation. A user may generate stable decoy states by cascading several MZIs. However, in this scheme, the splitting ratio of each MZI must be specially designed. Considering that almost all commercial MZIs have a symmetric splitting ratio, each MZI in the series must be customized, which would increase difficulty and cost. Even if the customized MZIs are employed, the stable intensities of the cascade MZI design are fixed when connecting N MZIs in series, the user can generate at most 2^N stable intensities. By contrast, the user can build $2N$-path MMZI by connecting N MZIs in parallel, in another word, he (she) can generate at most 2^{2N-1} stable intensities, which is much more than connecting in series. Compared with cascading several customized MZIs, a 3-path MMZI (DPMZI or connecting two commercial MZI in parallel) can generate 4 stable intensities and the intensities are tunable, which is much more flexible and convenient in practical applications.

We have also experimentally demonstrated the modulation method by an commercial dual-parallel MZI (DPMZI) which could be regarded as a special case of the MMZI. We measured a random sequence consisting of signal, decoy, and vacuum state. The result suggests that our method can effectively mitigate the influence of the patterning effect. We have also demonstrated adjusting the ratio $\mathcal{R}$ to verify its convenience for intensity optimization. The details could be found in METHODS. The result indicates that our interferometer and modulation method are feasible in practice and will be secure, robust, and flexible for decoy-state QKD systems. Since its compact structure is easy to integrate, we believe that an integrated MMZI can be perfectly applied in high-speed decoy-state QKD systems and help the practical QKDs to achieve the optimized performance.

METHODS

Experimental demonstration

In this section, we demonstrate the MMZI and its accompanying modulation method by a commonly used three-intensity decoy-state method[17,22,48,49] which consists of a signal state, a decoy state, and a vacuum state. An integrated commercial modulator named DPMZI[50–52], which can be regarded as a special case of our MMZI is employed in the demonstration. As illustrated in Fig. 4, a DPMZI consists of two parallel sub-MZIs, one of which can be regarded as a VOA and the other one can be regarded as two independent paths. For simplicity, we use VOA to refer to the first sub-MZI. In other words, the DPMZI can be regarded as an equivalent of our modulator with three paths. Since all beam splitters in DPMZI have a 50:50 ratio, the splitting ratio t_0, t_1, and t_2 are fixed to, respectively, 0.5, 0.25 and 0.25. The output of DPMZI is written as:

$$\left|\sqrt{\mu_{\text{out}}}\right\rangle = \left|\left(\frac{1}{2}\sqrt{\eta} + \frac{1}{4}e^{i\alpha_1} + \frac{1}{4}e^{i\alpha_2}\right)\sqrt{\mu_{\text{in}}}\right\rangle. \tag{9}$$

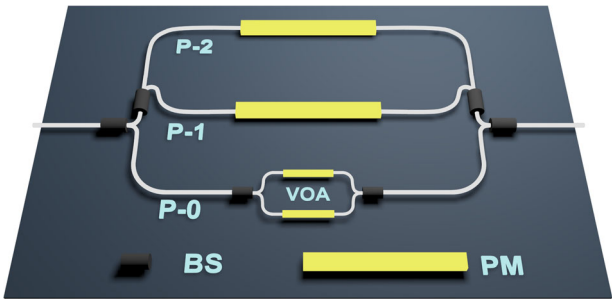

Fig. 4 The figure depicts the structure of the DPMZI, which contains two parallel sub-MZI. In our modulation method, one of the MZIs is regarded as a VOA.

The output intensity is a function of α_1 and α_2, which is written as:

$$I(\alpha_1,\alpha_2)=\frac{\mu_{in}}{4}\left[\eta+\sqrt{\eta}(\cos\alpha_1+\cos\alpha_2)+\frac{1}{2}+\frac{1}{2}\cos(\alpha_1-\alpha_2)\right]. \quad (10)$$

As discussed above, the half-wave points are stable. The $I(0, 0)$ is the maximum intensity, which is regarded as the signal state μ_s. The other half-wave points can be employed as decoy states, here we select the $I(0, \pi)$ as the decoy state μ_d. Since the splitting ratios of the integrated commercial DPMZI have been fixed (namely, we cannot adjust splitting ratios to make the vacuum state on a half-wave point), we employ a particular solution, which is the solution of the equation set

$$\frac{\partial I(\alpha_1,\alpha_2)}{\partial\alpha_1}=-\frac{1}{4}\left[\sqrt{\eta}\sin\alpha_1+\frac{1}{2}\sin(\alpha_1-\alpha_2)\right]=0;$$
$$\frac{\partial I(\alpha_1,\alpha_2)}{\partial\alpha_2}=-\frac{1}{4}\left[\sqrt{\eta}\sin\alpha_2+\frac{1}{2}\sin(\alpha_2-\alpha_1)\right]=0;$$
$$I(\alpha_1,\alpha_2)=\frac{\mu_{in}}{4}\left[\eta+\sqrt{\eta}(\cos\alpha_1+\cos\alpha_2)+\frac{1}{2}+\frac{1}{2}\cos(\alpha_1-\alpha_2)\right]=0,$$

as the vacuum state. Experimentally, we can obtain the vacuum point by scanning the driving-voltage of path-1 and 2 alternately and taking the voltage which minimizes the output intensity in each turn.

As illustrated in Fig. 5. The point S $(\alpha_1=0,\alpha_2=0)$ is a peak point which corresponds to the signal state μ_s; The point D $(\alpha_1=0,\alpha_2=\pi)$ is a saddle point that is selected to generate the decoy state μ_d. The point V is a trough point which corresponds to the vacuum state. Now that the t_k are fixed, the stable intensities are $I(0,0)=\frac{\mu_{in}}{4}(1+\sqrt{\eta})^2$ and $I(0,\pi)=\frac{\mu_{in}}{4}\eta$, which are functions of the η. Defining that $\mathcal{R}=\mu_d/\mu_s$, the user can adjust the VOA to $\eta=\left(\frac{\sqrt{\mathcal{R}}}{1-\sqrt{\mathcal{R}}}\right)^2$ to make $I(0,\pi)/I(0,0)=\mathcal{R}$.

In our experimental demonstration, a series of 50 ps light pulses generated from a 1 GHz high-speed picosecond laser were fed to a DPMZI (produced by FUJITSU OPTICAL COMPONENTS LIMITED and the model is FTM7960EX). A 5 GS/s-sampling-rate arbitrary waveform generator with two RF-amplifiers was applied to drive the interferometer. A pseudo-random number sequence was employed to the arbitrary waveform generator to generate random encoding signals. Complementary encoding signals similar to ref. [29] were employed to meet the need of the RF-amplifiers. On the detection side, the modulated pulses were detected by a 20-GHz-bandwidth high-speed photodiode and recorded by a 12.5-GHz-bandwidth oscilloscope. Since it is assumed that the average intensity reflects the mean photon number in the quantum pulses through heavy attenuation linearly[29], we measured the intensities before they are attenuated to single-photon magnitude and calculated the intensity by the area of the pulse traced by the oscilloscope.

To demonstrate the ability to mitigate the patterning effect, a random sequence consisting of signal, decoy, and vacuum state was measured and 20,000 pulses were collected for statistical analysis. A short subset of the tracing result was shown in Fig. 6. To show the flexibility of tuning the ratio of signal and decoy state, we measured the average intensities of different patterns with different η. We adjusted the η to make the $\mathcal{R}=\mu_d/\mu_s=0.24$, 0.21, 0.18, and 0.12 as the interval of 0.1–0.25 is widely used in decoy-state QKDs[18,43,53] and recorded the average intensities of different patterns in Table 1. After that, we did a control experiment in which all the devices were the same as the previous one except for the modulator was replaced by a commercial $LiNbO_3$ MZI. In the control experiment, we also prepared random sequences consisting of the three states, and we adjusted the voltage to tune the $\mathcal{R}$ to do a comparison with the DPMZI. The comparison is listed in Table 2. The results indicate that under the same condition, the patterning effect in our method is two or three orders of magnitude smaller than the traditional intensity modulator.

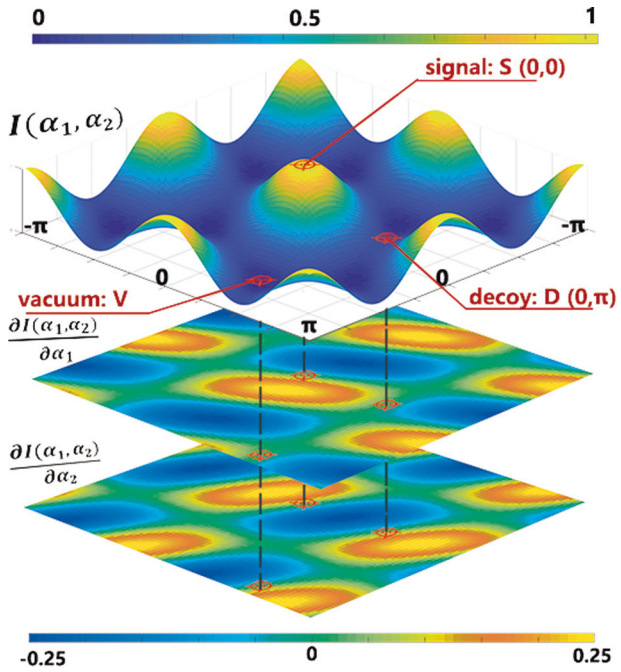

Fig. 5 The figure illustrates the output intensity and its partial derivatives. The upper surface plot illustrates and the two contour plots denote the two partial derivatives. The upper color bar belongs to the surface plot and the lower color bar belongs to the two contour plots. The 'S', 'D', and 'V' points are employed as the signal state, decoy state, and vacuum state respectively and the partial derivatives of the three points are all 0.

Employing our modulator is the inevitable demand for higher performance since in practical systems.

Simulation

Except for the patterning effect, the random intensity fluctuation due to thermal noise or timing jitter of modulation signal also brings side-channels to practical systems. As discussed in previous works[22,26,27,54], considering the worst case in the parameter estimation is a counter-measure for the loophole, but the system performance would be unavoidably reduced and the performance depends on the magnitude of the fluctuation. The MMZI can mitigate the random intensity fluctuation from the modulation signal so that the system performance could be improved. Here we demonstrate the MMZI by extending the intensity fluctuation to ref. [13], which is a three-intensity BB84 protocol with a finite-key analysis. (We emphasize that we only analyze the random intensity fluctuation in the simulation since the quantitative theoretical analysis against the correlated intensity fluctuation is still missing at present.).

The protocol definition is same with ref. [13], except that the worst case of the mean photon number in the range of $[\mu_a^L,\mu_a^U]$ $(a\in\{s,d,v\})$ is considered in the parameter estimation. The secret key is extracted from the events whereby Alice and Bob both choose the X basis. The intensities are denoted by μ_s, μ_d and μ_v, respectively, and they satisfy $\mu_s>\mu_d+\mu_v$ and $\mu_d>\mu_v\geq 0$. The intensities are selected with probabilties p_{μ_s}, p_{μ_d} and p_{μ_v}, respectively. In the scenario that the random intensity fluctuation and finite-key effect are considered, the parameters estimation of decoy state method should be modified. The lower-bound on the number of vacuum events $s_{b,0}$ in basis b $(b\in\{X,Z\})$ is estimated by:

$$\begin{aligned}s_{b,0}^L=\min:\ &\tau_0(\mu_s,\mu_d,\mu_v)\frac{\mu_d F^-(n_b^v,\mu_v)-\mu_v F^+(n_b^d,\mu_d)}{\mu_d-\mu_v},\\ s.t.\ &\mu_a^L\leq\mu_a\leq\mu_a^U,\\ &\text{for } a\in\{s,d,v\},\end{aligned} \quad (11)$$

where $n_{b,a}$ denotes the event number when Alice select basis b and intensity μ_a, the $\tau_0(\mu_s,\mu_d,\mu_v)=e^{-\mu_s}p_{\mu_s}+e^{-\mu_d}p_{\mu_d}+e^{-\mu_v}p_{\mu_v}$ is the

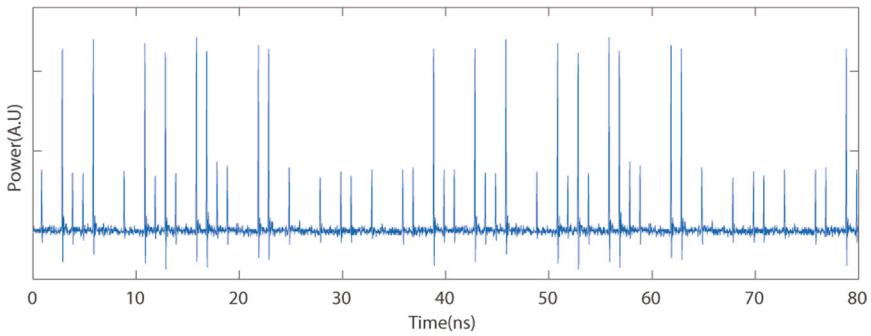

Fig. 6 Oscilloscope traces: a random sequence including μ_s, μ_d, μ_v. The figure shows part of the recorded data.

Table 1. Patterning effect test.

	Avg. int. 2nd pulse	Patt. eff. (%).
Patt. ($\mathcal{R} = 0.24$)		
$\mu_s \to \mu_s$	1.0001 ± 0.026	0.02
$\mu_d \to \mu_s$	0.9994 ± 0.025	−0.06
$\mu_v \to \mu_s$	1.0004 ± 0.024	0.04
$\mu_s \to \mu_d$	0.2373 ± 0.015	−0.18
$\mu_d \to \mu_d$	0.2381 ± 0.015	0.16
$\mu_v \to \mu_d$	0.2378 ± 0.014	0.02
Patt. ($\mathcal{R} = 0.21$)		
$\mu_s \to \mu_s$	1.0005 ± 0.043	0.05
$\mu_d \to \mu_s$	0.9947 ± 0.043	−0.54
$\mu_v \to \mu_s$	1.0048 ± 0.041	0.48
$\mu_s \to \mu_d$	0.2100 ± 0.016	0.20
$\mu_d \to \mu_d$	0.2088 ± 0.014	−0.39
$\mu_v \to \mu_d$	0.2100 ± 0.014	0.20
Patt. ($\mathcal{R} = 0.18$)		
$\mu_s \to \mu_s$	1.0008 ± 0.041	0.07
$\mu_d \to \mu_s$	0.9920 ± 0.041	−0.80
$\mu_v \to \mu_s$	1.0072 ± 0.039	0.72
$\mu_s \to \mu_d$	0.1815 ± 0.017	0.28
$\mu_d \to \mu_d$	0.1800 ± 0.016	−0.56
$\mu_v \to \mu_d$	0.1815 ± 0.016	0.28
Patt. ($\mathcal{R} = 0.12$)		
$\mu_s \to \mu_s$	0.9993 ± 0.030	-0.07
$\mu_d \to \mu_s$	0.9974 ± 0.028	−0.26
$\mu_v \to \mu_s$	1.0033 ± 0.027	0.33
$\mu_s \to \mu_d$	0.1176 ± 0.018	0.15
$\mu_d \to \mu_d$	0.1167 ± 0.019	−0.63
$\mu_v \to \mu_d$	0.1180 ± 0.018	0.48

The average intensity of each pattern extracted from 20,000 random patterns. The 'Avg. int.' is the intensity uniformed according to the average intensity of the 2nd S pulse. The value after '±' is the standard deviation which reflects the random fluctuation of our measurement. The random fluctuation consists of the fluctuation of laser source, the random noise from modulation signal, the noise from the oscilloscope and the error from intensity calculation. The 'Patt. eff.' reflects the patterning effect, which is defined as the deviation from the average intensity.

probability that Alice sends a 0-photon state and the

$$F^{\pm}(n_b^a, \mu_a) = \frac{e^{\mu_a}}{p_{\mu_a}}\left[n_b^a \pm \sqrt{n_b \ln \frac{21}{\epsilon_{\sec}}}\right]. \tag{12}$$

is an intermediate variable corresponding to the Hoeffding's inequality.

Table 2. Comparing the MZI and MMZI.

	Patt. eff. (MMZI)	Patt. eff. (MZI).
Patt. ($\mathcal{R} = 0.24$)		
$\mu_s \to \mu_d$	-0.18%	25.13%
$\mu_d \to \mu_d$	0.16%	1.18%
$\mu_v \to \mu_d$	0.02%	-23.95%
Patt. ($\mathcal{R} = 0.21$)		
$\mu_s \to \mu_d$	0.20%	20.78%
$\mu_d \to \mu_d$	-0.39%	1.15%
$\mu_v \to \mu_d$	0.20%	-21.92%
Patt. ($\mathcal{R} = 0.18$)		
$\mu_s \to \mu_d$	0.28%	13.88%
$\mu_d \to \mu_d$	-0.56%	2.24%
$\mu_v \to \mu_d$	0.28%	-16.11%
Patt. ($\mathcal{R} = 0.12$)		
$\mu_s \to \mu_d$	0.15%	25.46%
$\mu_d \to \mu_d$	-0.63%	-2.52%
$\mu_v \to \mu_d$	0.48%	-22.95%

The average intensity of each pattern extracted from 20,000 random patterns. The 'Patt. eff.' means the intensity deviation from the average μd, which reflects the patterning effect.

In addition, the lower-bound on the number of single-photon events $s_{b,1}$ in basis b ($b \in \{X, Z\}$) is estimated by:

$$\begin{aligned} s_{b,1}^L = \min : & \frac{\tau_1(\mu_s,\mu_d,\mu_v)\mu_s}{\mu_s(\mu_d-\mu_v)-\mu_d^2+\mu_v^2} \times [F^-(n_b^d,\mu_d) - F^+(n_b^v,\mu_v) \\ & - \frac{\mu_d^2-\mu_v^2}{\mu_s^2}(F^+(n_b^s,\mu_s) - \frac{s_{b,0}^L}{\tau_0(\mu_s,\mu_d,\mu_v)})], \\ & s.t.\ \mu_a^L \le \mu_a \le \mu_a^U, \\ & \text{for } a \in \{s,d,v\}, \end{aligned} \tag{13}$$

where the $\tau_1(\mu_s,\mu_d,\mu_v) = e^{-\mu_s}\mu_s p_{\mu_s} + e^{-\mu_d}\mu_d p_{\mu_d} + e^{-\mu_v}\mu_v p_{\mu_v}$ is the probability that Alice sends a single-photon state.

After that, the upper-bound of the number of bit errors associated with the single-photon events in Z-basis $v_{Z,1}$ is modified as:

$$\begin{aligned} v_{Z,1}^U = \max : & \tau_1(\mu_s,\mu_d,\mu_v)\frac{F^+(m_Z^d,\mu_d)-F^-(m_Z^v,\mu_v)}{\mu_d-\mu_v}, \\ & s.t.\ \mu_a^L \le \mu_a \le \mu_a^U, \\ & \text{for } a \in \{s,d,v\}, \end{aligned} \tag{14}$$

where the m_Z^a denotes the number of bit errors when Alice selects Z-basis and intensity μ_a.

With the modified formulas of the three-intensity decoy-state method, we can estimate a secret key rate when the random intensity fluctuation exists. Here simulate the BB84 protocol with random intensity fluctuation, and compare the system performance between employing commercial MZI and MMZI. The protocol definition and the formulas are same with ref. [13] except for the formulas of the decoy-state method are replaced by

Table 3. Intensity fluctuation.

	MZI	MMZI
$\delta_\alpha = \pi/20$		
μ_s	[0.4329, 0.4444]	[0.4297, 0.4444]
μ_d	[0.0615, 0.1183]	[0.0863, 0.0922]
μ_v	[0.0004, 0.0027]	[0.0004, 0.0022]
$\delta_\alpha = \pi/30$		
μ_s	[0.4344, 0.4444]	[0.4330, 0.4444]
μ_d	[0.0696, 0.1082]	[0.0868, 0.0904]
μ_v	[0.0004, 0.0012]	[0.0004, 0.0009]
$\delta_\alpha = \pi/40$	MZI	MMZI
μ_s	[0.4349, 0.4444]	[0.4341, 0.4444]
μ_d	[0.0739, 0.1032]	[0.0869, 0.0897]
μ_v	[0.0004, 0.0007]	[0.0004, 0.0005]

The table lists the intensity range $[\mu_a^L, \mu_a^U]$ in different electronic noise. The δ_α denotes the phase deviation due to the electronic noise, and we define $[\alpha^L, \alpha^U]$ is $[\alpha - \delta_\alpha, \alpha + \delta_\alpha]$. The ideal value of μ_s, μ_d, and μ_v are 0.4444, 0.088, and 0.0004, respectively.

Eqs. (11), (13), and (14), in which the intensity fluctuation $[\mu_a^L, \mu_a^U]$ is considered. The difference between employing commercial MZI and the DPMZI is that the fluctuation is different. Since the electronic noise, when Alice wants to a voltage corresponding to the relative phase α, she actually loads a random voltage in a range which corresponds to the relative phase in the range of $[\alpha^L, \alpha^U]$. When a commercial MZI is employed, the intensity fluctuation is

$$\begin{aligned} \mu'^L_a &= \min : \tfrac{\mu_{in}}{2}(1+\cos(\alpha_a)), \\ \mu'^U_a &= \max : \tfrac{\mu_{in}}{2}(1+\cos(\alpha_a)), \\ & s.t. \alpha_a \in [\alpha_a^L, \alpha_a^U], \end{aligned} \tag{15}$$

where $a \in \{s, d, v\}$ and the α_a denotes the corresponding relative phase for intensity μ'_a. Similarly, when the MMZI (we take the DPMZI as an example) is employed, the intensity fluctuation is

$$\begin{aligned} \mu'^L_a &= \min : \tfrac{\mu_{in}}{4}\left[\eta + \sqrt{\eta}(\cos\alpha_{1,a} + \cos\alpha_{2,a}) \right. \\ &\quad \left. + \tfrac{1}{2} + \tfrac{1}{2}\cos(\alpha_{1,a} - \alpha_{2,a})\right] \\ &= 0, \mu'^U_a = \max : \tfrac{\mu_{in}}{4}\left[\eta + \sqrt{\eta}(\cos\alpha_{1,a} + \cos\alpha_{2,a}) \right. \\ &\quad \left. + \tfrac{1}{2} + \tfrac{1}{2}\cos(\alpha_{1,a} - \alpha_{2,a})\right] \\ &= 0, \; s.t. \; \alpha_{1,a} \in \left[\alpha_{1,a}^L, \alpha_{1,a}^U\right], \; \alpha_{2,a} \in \left[\alpha_{2,a}^L, \alpha_{2,a}^U\right], \end{aligned} \tag{16}$$

where the $\alpha_{1,a}$ and $\alpha_{2,a}$ are corresponding relative phases for intensity μ_a and the η should be tuned to be 0.6545 to make $\mu_d = 0.2\mu_s$. We further assume that the source has a fluctuation of δ_I, the output μ_a is in the range of $[\mu_a^L, \mu_a^U]$, where

$$\begin{aligned} \mu_a^L &= \min(\mu'^L_a(1-\delta_I), 10^{-3}\mu_s), \\ \mu_a^U &= \mu'^U_a(1+\delta_I), \end{aligned} \tag{17}$$

where the 10^{-3} is the extinction ratio of the modulator.

Here, we compare the difference of intensity fluctuation and secret key rate between employing commercial MZI and MMZI. In our simulation, the detection efficiency is 10%, the dark count rate is 6×10^{-7}, the after-pulse probability is 4×10^{-2}, the misalignment error rate is 5×10^{-3}, and the fluctuation of the laser source $\delta_I = 1\%$. The security parameters for finite-key effect are all same with ref. [13] and the block size n_X is fixed to 10^7. The probabilities $p_{\mu_s} = 0.7$, $p_{\mu_d} = 0.2$, and $p_{\mu_v} = 0.1$. The probability of selecting X basis is 0.61. We fix the intensities to $\mu_s = 0.44$, $\mu_d = 0.2\mu_s = 0.088$, $\mu_v = 10^{-3}\mu_s$. The intensity fluctuations are listed in Table 3 and the secret key rates are showed in Fig. 7. The simulation results indicate that the MMZI mitigates the random intensity fluctuation and significantly improves the system performance. When the phase deviation is $\pi/20$, the system with DPMZI is nearly ideal while the system with MZI is nearly broken.

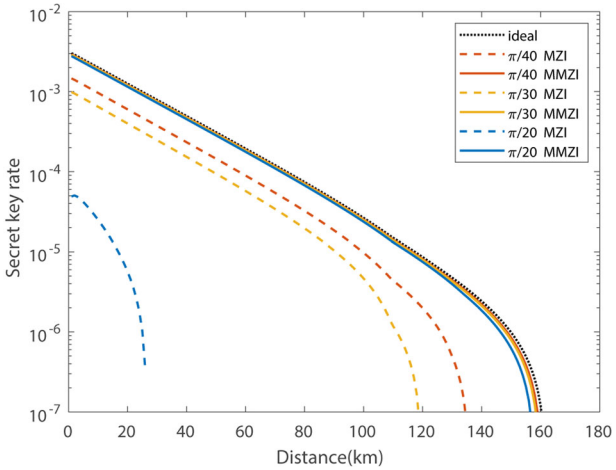

Fig. 7 The secret key rate as the function of communication distance in the scenario that the random intensity fluctuation is considered. The black-dot line denotes the ideal key rate without any intensity fluctuation. The red, yellow, and blue lines denote the maximum phase deviation δ_α is $\pi/40$, $\pi/30$, and $\pi/20$, respectively. The modulated phase is in the range of $[\alpha - \delta_\alpha, \alpha + \delta_\alpha]$. The solid line and dash line denote employing MMZI and MZI, respectively.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 19 November 2020; Accepted: 14 April 2021;
Published online: 20 May 2021

REFERENCES

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (IEEE, 1984).
2. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
3. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
4. Renner, R. Security of quantum key distribution. *Int. Symp. Inf. Theory* **6**, 1–127 (2008).
5. Scarani, V. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
6. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
7. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
8. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
9. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
10. Lo, H.-K. Quantum key distribution with vacua or dim pulses as decoy states. In *Proc International Symposium on information Theory, 2004. ISIT 2004,* 137 (IEEE, 2004).
11. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. In *Proc International Symposium on Information Theory, 2004. ISIT 2004*, 136 (IEEE, 2004).
12. Wang, X.-B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **72**, 012322 (2005).
13. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
14. Curty, M. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).
15. Cui, C. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **11**, 034053 (2019).
16. Lu, F.-Y. Improving the performance of twin-field quantum key distribution. *Phys. Rev. A* **100**, 022306 (2019).

17. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87**, 012320 (2013).
18. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A* **91**, 032318 (2015).
19. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93**, 042324 (2016).
20. Wang, C. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **115**, 160502 (2015).
21. Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052333 (2014).
22. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
23. Wang, C. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optica* **4**, 1016–1023 (2017).
24. Zhao, Y., Qi, B. & Lo, H.-K. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A* **77**, 052327 (2008).
25. Wang, X.-B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **75**, 052301 (2007).
26. Mizutani, A., Curty, M., Lim, C. C. W., Imoto, N. & Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* **17**, 093011 (2015).
27. Grasselli, F. & Curty, M. Practical decoy-state method for twin-field quantum key distribution. *New J. Phys.* **21**, 073001 (2019).
28. Lu, F.-Y. Practical issues of twin-field quantum key distribution. *New J. Phys.* **21**, 123030 (2019).
29. Yoshino, K.-I. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Inf.* **4**, 8 (2018).
30. Roberts, G. Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution. *Opt. Lett.* **43**, 5110–5113 (2018).
31. Zhang, C.-M., Zhu, J.-R. & Wang, Q. Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution. *Phys. Rev. A* **95**, 032309 (2017).
32. Boaron, A. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
33. Yin, H.-L. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
34. Tang, Z. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
35. Wang, S. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.* **37**, 1008–1010 (2012).
36. Takesue, H. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nat. Photonics* **1**, 343–348 (2007).
37. Thew, R. T. Low jitter up-conversion detectors for telecom wavelength ghz qkd. *New J. Phys.* **8**, 32 (2006).
38. Rubenok, A. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
39. Liu, Y. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502–130502 (2013).
40. Comandar, Lea Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photonics* **10**, 312 (2016).
41. Liu, H., Wang, J., Ma, H. & Sun, S. Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration. *Optica* **5**, 902–909 (2018).
42. Wang, S. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nat. Photonics* **9**, 832–836 (2015).
43. Wang, C. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding. *Opt. Lett.* **41**, 5596–5599 (2016).
44. Minder, M. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **13**, 334–338 (2019).
45. Wang, S. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
46. Liu, Y. Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **123**, 100505–100505 (2019).
47. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
48. Chen, J. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
49. Maeda, K., Sasaki, T. & Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat. Commun.* **10**, 3140 (2019).
50. Ji, Y. A phase stable short pulse generator using a dpmzm and phase modulators for application in 160 gbaud dqpsk systems. *Opt. Commun.* **285**, 1964–1969 (2012).
51. Li, Y. et al. 160gbaud/s to 40gbaud/s otdm-dqpsk de-multiplex based on a dual parallel mach-zehnder modulator. In *OFC/NFOEC*, 1–3 (IEEE, 2012).
52. Wang, H., Kong, D., Li, Y., Wu, J. & Lin, J. Simple asymmetric optical dqpsk modulation and demodulation scheme. *Opt. Commun.* **288**, 17–22 (2013).
53. Tang, Y.-L. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
54. Wang, X.-B., Yang, L., Peng, C.-Z. & Pan, J.-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **11**, 075006 (2009).

ACKNOWLEDGEMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grants Nos. 61622506, 61575183, 61627820, 61475148, and 61675189), and the Anhui Initiative in Quantum Information Technologies.

AUTHOR CONTRIBUTIONS

F.-Y.L. and X.L. start the project and design the experiment. F.-Y.L., X.L., S.W., and D.-Y.H. perform the experiment and complete the data analysis. G.-J.F.-Y., R.W., and P.Y. provide the theoretical calculations. Z.-Qi.Y., W.C., G.-C.G. and Z.-F.H. supervise the project.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to S.W.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.