Article:
Lo, Y. S., Woodward, R. I., Walk, N. et al. (8 more authors) (2023) Simplified intensity- and phase-modulated transmitter for modulator-free decoy-state quantum key distribution. APL Photonics. 036111. ISSN 2378-0967

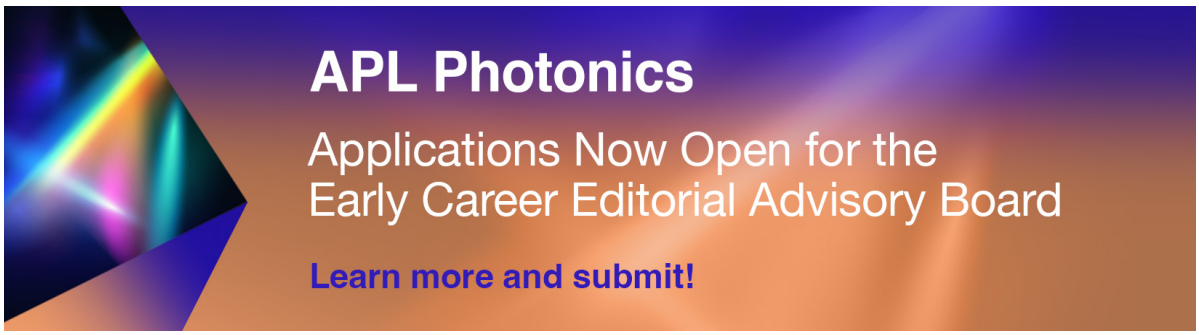
https://doi.org/10.1063/5.0128445

APL Photonics

Simplified intensity- and phase-modulated transmitter for modulator-free decoy-state quantum key distribution

Cite as: APL Photonics **8**, 036111 (2023); https://doi.org/10.1063/5.0128445
Submitted: 28 September 2022 • Accepted: 24 February 2023 • Published Online: 20 March 2023

Y. S. Lo, R. I. Woodward, N. Walk, et al.



AIP Publishing

Simplified intensity- and phase-modulated transmitter for modulator-free decoy-state quantum key distribution

Cite as: APL Photon. 8, 036111 (2023); doi: 10.1063/5.0128445
Submitted: 28 September 2022 • Accepted: 24 February 2023 •
Published Online: 20 March 2023

Y. S. Lo,[1,2,a)] R. I. Woodward,[1] N. Walk,[1] M. Lucamarini,[1,3] I. De Marco,[1] T. K. Paraïso,[1] M. Pittaluga,[1] T. Roger,[1] M. Sanzaro,[1] Z. L. Yuan,[1] and A. J. Shields[1]

AFFILIATIONS

[1] Toshiba Europe Ltd., Cambridge, United Kingdom
[2] Quantum Science and Technology Institute, University College London, London, United Kingdom
[3] Department of Physics and York Centre for Quantum Technologies, University of York, YO10 5DD York, United Kingdom

[a)] **Author to whom correspondence should be addressed:** yuen.lo@crl.toshiba.co.uk

ABSTRACT

Quantum key distribution (QKD) allows secret key exchange between two users with unconditional security. For QKD to be widely deployed, low cost and compactness are crucial requirements alongside high performance. Currently, the majority of QKD systems demonstrated rely on bulk intensity and phase modulators to generate optical pulses with precisely defined amplitude and relative phase difference—i.e., to encode information as signal states and decoy states. However, these modulators are expensive and bulky, thereby limiting the compactness of QKD systems. Here, we present and experimentally demonstrate a novel optical transmitter design to overcome this disadvantage by generating intensity- and phase-tunable pulses at GHz clock speeds. Our design removes the need for bulk modulators by employing directly modulated lasers in combination with optical injection locking and coherent interference. This scheme is, therefore, well suited to miniaturization and photonic integration, and we implement a proof-of-principle QKD demonstration to highlight potential applications.

INTRODUCTION

Quantum key distribution (QKD) allows two parties to exchange secret keys with security guaranteed by the fundamental laws of physics.[1,2] Driven by its potential, tremendous progress has been made in both theoretical and technological developments, such as satellite-based QKD,[3,4] QKD networks,[5–8] chip-based QKD,[9–11] as well as the invention of novel protocols allowing higher secret key capacity.[12–14]

In QKD protocols, time-bin encoding is commonly used,[15–18] where the temporal modes of a time-bin qubit (early and late time bins) and the phase between them are used to encode the key bits. As practical single photon sources are not yet widely available, QKD systems typically employ lasers to generate weak coherent states to approximate the time-bin qubits. Since the photon number statistics of laser emission follow a Poisson distribution, the emitted pulses have a non-negligible probability of containing more than one photon, making laser-based QKD systems susceptible to a photon-number-splitting (PNS) attack.[19] Although it is still possible to obtain unconditional security, the signal flux has to be heavily attenuated in order to suppress multi-photon emission, thus giving a poor scaling of the secure key rate with transmission distance.[20] Fortunately, this problem can be overcome by employing the decoy state method:[21,22] in addition to sending signal states, one also randomly sends a small number of states with reduced intensity, known as decoy states. A potential eavesdropper cannot distinguish between signal states and decoy states; thus, any attempt to perform photon-number-dependent attacks can be detected from the measured photon statistics. As a result, with the decoy state method, single-photon bounds can be reliably estimated, which, therefore, improves the scaling of the secure key rate with distance significantly.

Implementing a decoy-state QKD transmitter requires the ability to on-off modulate each time bin within a state, modulate the phase between time bins, as well as vary the intensity level to generate decoy states. To date, this has been achieved by placing intensity modulators after a light source to control the output intensity, and phase modulators are also required in order to encode the phase information. Conventional intensity and phase modulators are based on $LiNbO_3$ crystals. While these modulators are widely available and offer high performance, they are expensive, bulky (centimeter-scale), and require high driving voltage (typically > 4 V), which often necessitates the addition of amplifiers. It is, therefore, highly beneficial to develop an alternative approach that can replace such modulators, as it would significantly reduce the overall complexity, making QKD systems more compact and cost-effective.

Recently, Yuan *et al.* demonstrated an efficient scheme to perform direct phase modulation without the need for phase modulators.[23] Precise phase control is enabled by exploiting optical injection locking (OIL) and gain-switching techniques. Following this work, direct phase modulated laser transmitters for QKD have been studied more widely,[24] bringing the benefits of compact low-drive-voltage phase modulation for chip-based QKD[9] as well as other emerging protocols such as measurement-device-independent QKD.[25] More recently, the theoretical aspect of the direct phase modulation scheme has also been studied, verifying its favorable features in practical usage.[26] While this scheme allows phase information to be directly encoded, it cannot be used to control the intensity of pulses for decoy state generation. Since a direct intensity modulation scheme is still missing, the use of bulk intensity modulators has been unavoidable.

In this work, we present a novel approach that can directly generate intensity and phase modulated optical pulses. Our scheme only requires two laser diodes and a passive asymmetric Mach–Zehnder interferometer (AMZI). Such a pulse source can generate all the encoding states required for decoy-state QKD, thereby eliminating the need for external modulators and opening a new route for the development of compact, cost-effective, and high-performance QKD systems.

DIRECT GENERATION OF ENCODING STATES

Our scheme further extends direct phase modulation techniques[23] by generating and interfering with three intermediate pulses with carefully crafted relative phases in order to accurately control both the relative phase and intensity of the final output pulses. The experimental setup is shown in Fig. 1(a). The two laser diodes (referred to as "master" and "slave" following standard nomenclature) are connected in an OIL configuration. The master laser is gain-switched such that the laser produces long pulses (i.e., with a high duty cycle) when it is driven above the threshold and switched off between the pulses. As a result, each pulse is produced with a random phase as they are seeded by spontaneous emission photons.[27] Subsequently, these pulses are injected through a circulator into the slave laser, which is gain-switched to produce three short pulses within each long master pulse [see Figs. 1(b-i) and 1(b-ii)]. Because the stimulated emission of the slave laser is seeded by the injected photons, the three slave pulses inherit the phase of the corresponding injected master pulse. The relative phases between these pulses are well defined as they are seeded by the same master pulse; however, collectively, their global phase is random.

In order to prepare the slave pulses for interference to achieve the desired outputs, their relative phases need to be carefully controlled. This is achieved by manipulating the phase evolution of the master pulse , which can be realized by introducing an amplitude perturbation to the electrical driving signal of the master laser[23] [Fig. 1(b-i)]. This electrical modulation, with a temporal width of

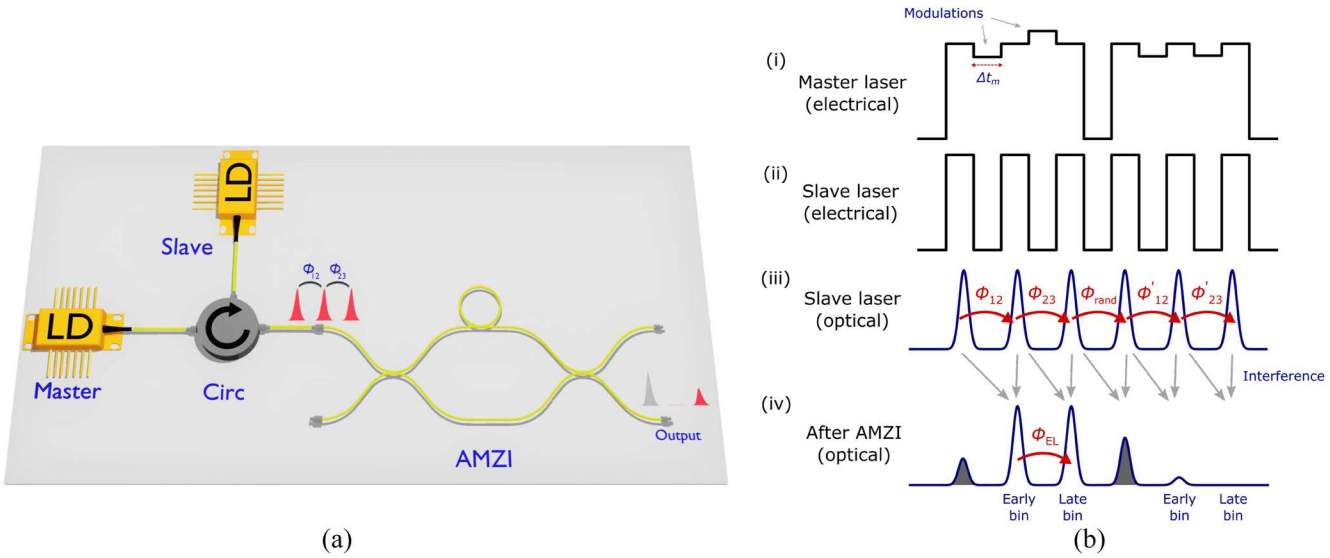


FIG. 1. Directly intensity and phase modulated transmitter scheme: (a) the design of the transmitter based on two directly modulated lasers in an optical injection locking setup and an AMZI. (b) Schematic illustration of the operating principle.

Δt_m, changes the carrier density in the laser cavity, which in turn alters the cavity refractive index and causes a temporary optical frequency shift of $\Delta\nu$, thus the photons produced after the modulation experience a phase shift of $\Delta\phi = 2\pi\Delta\nu\Delta t_m$.[23] By locating the modulation in the interval between the onsets of two slave pulses, this phase difference can be transferred to the slave pulses. As shown in Fig. 1(b), the relative phases between the three slave pulses, ϕ_{12} and ϕ_{23}, can be implemented independently by adding two small electrical perturbations to the master laser.

The prepared slave pulses then pass through an AMZI with one of its arms having a delay line that matches the temporal separation of the slave pulses, resulting in interferences between consecutive slave pulses. As shown in Fig. 1(b-iv), at the outputs of the AMZI, three pulses are formed within a single logical bit: two of them with their intensities and the relative phase completely determined by ϕ_{12} and ϕ_{23}, whereas the third pulse has a random intensity due to the interference of two slave pulses originating from different master pulses with random phase relation (indicated in gray shading). As a result, the first two pulses could be used to represent the early and late bins for time-bin encoding.

To express the relative phase between the early and late time bins and their intensities in terms of ϕ_{12} and ϕ_{23}, we consider the pulses generated by the slave laser as three coherent states $|\alpha_1\rangle$, $|\alpha_2\rangle$, and $|\alpha_3\rangle$, with amplitude A,

$$\begin{aligned} |\alpha_1\rangle &= \left|Ae^{i(\omega t+\phi_1)}\right\rangle, \\ |\alpha_2\rangle &= \left|Ae^{i(\omega t+\phi_1+\phi_{12})}\right\rangle, \\ |\alpha_3\rangle &= \left|Ae^{i(\omega t+\phi_1+\phi_{12}+\phi_{23})}\right\rangle, \end{aligned} \tag{1}$$

where the phase of the first coherent state, ϕ_1, is uniformly distributed over $[0, 2\pi)$.

In the AMZI, the interference between $|\alpha_1\rangle$ and $|\alpha_2\rangle$ ($|\alpha_2\rangle$ and $|\alpha_3\rangle$) gives rise to the early (late) time bin $|\alpha_E\rangle$ ($|\alpha_L\rangle$), which can be expressed as

$$\begin{aligned} |\alpha_E\rangle &= \frac{A}{2}e^{i(\omega t+\phi_1)}\left(1+e^{i\phi_{12}}\right), \\ |\alpha_L\rangle &= \frac{A}{2}e^{i(\omega t+\phi_1+\phi_{12})}\left(1+e^{i\phi_{23}}\right), \end{aligned} \tag{2}$$

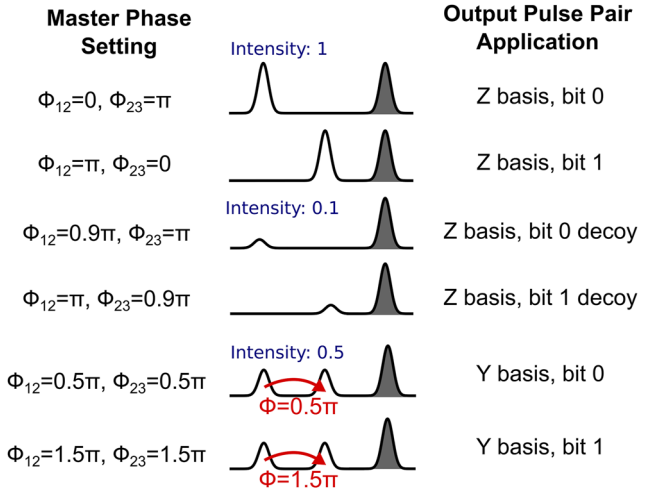


FIG. 3. Direct generation of possible QKD states with the corresponding phase settings on the master laser.

and their corresponding intensities and phases are given by

$$\begin{aligned} r_E &= A\cos\left(\frac{\phi_{12}}{2}\right), \quad \phi_E = \omega t + \phi_1 + \frac{\phi_{12}}{2}, \\ r_L &= A\cos\left(\frac{\phi_{23}}{2}\right), \quad \phi_L = \omega t + \phi_1 + \phi_{12} + \frac{\phi_{23}}{2}, \end{aligned} \tag{3}$$

respectively. The relative phase between the early and late time bins ϕ_{EL} and their intensities are simulated based on Eq. (3) and shown in Fig. 2. This scheme could, therefore, be applied to time-bin based BB84 decoy-state QKD with Z and Y basis encoding. For Z-basis encoding, a pulse is located in either the early time bin (representing bit 0) or the late time bin (representing bit 1). To encode bit 0, ϕ_{12} is set to 0 to produce a pulse with maximum intensity in the early time bin, and ϕ_{23} is set to π to suppress any light in the late time bin. Similarly, bit 1 can be encoded by choosing $\phi_{12} = \pi$ and $\phi_{23} = 0$.

A decoy state in the Z basis can be generated in a similar way as described earlier. Instead of using zero relative phase , which results in a pulse with maximum intensity, a decoy state with a lower intensity can be generated by choosing a relative phase close to π, according to Fig. 2(a). For example, a decoy bit-0 state with

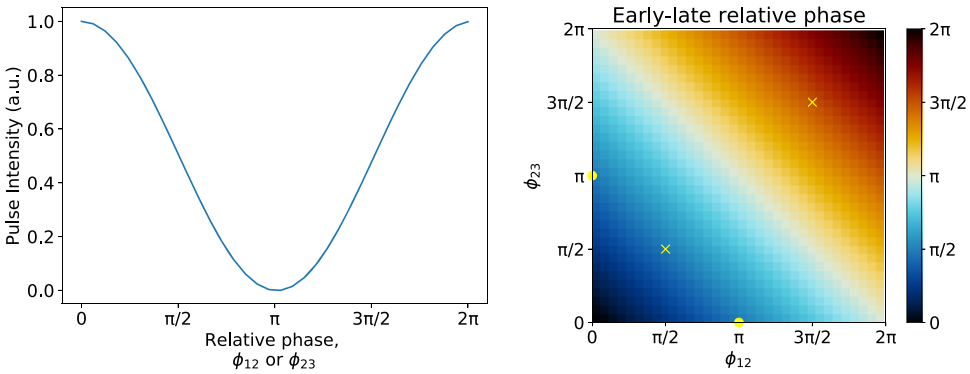


FIG. 2. (a) Simulated intensity of the final output pulse as a function of the relative phase between the two slave pulses. For the pulse in the early (late) time bin, the intensity is determined by ϕ_{12} (ϕ_{23}). (b) Simulated relative phase between the final output pulse pair, ϕ_{EL}, as a function of ϕ_{12} and ϕ_{23}. For Y-basis (Z-basis) encoding, the suitable values for ϕ_{12} and ϕ_{23} are marked by yellow crosses (dots).

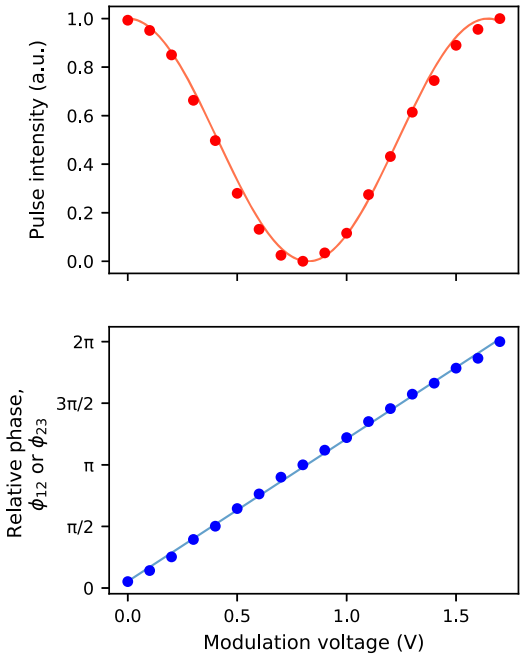


FIG. 4. Experimental characterization of the pulse generated at the outputs of the AMZI. Intensity of an individual pulse (top) and the relative phase between a pulse pair (bottom) as a function of modulation voltage applied to the master laser. A cosine (linear) fit is applied to the top (bottom) plot.

an intensity of 0.1 can be generated by choosing $\phi_{12} = 0.9\pi$ and $\phi_{23} = \pi$. Therefore, the flexibility to adjust the intensity level of the decoy state is enabled simply by implementing the appropriate relative phases, which itself is controlled by simple modulation of the electrical drive signal applied to the master laser.

In the Y-basis, a single bit comprises both the early and late time bins with a relative phase of $\pi/2$ (bit 0) or $3\pi/2$ (bit 1). Each time bin has half the intensity of the signal state in the Z basis. From Eq. (2), the relative phase between the early and late time bins is simply $\phi_{EL} = (\phi_{12} + \phi_{23})/2$. Since the intensities of the early and late time bins must be equal, it is necessary that $\phi_{12} = \phi_{23}$. As a result, to encode bit 0 with $\phi_{EL} = \pi/2$, $\phi_{12} = \phi_{23} = \pi/2$. Similarly, to encode bit 1 with $\phi_{EL} = 3\pi/2$, $\phi_{12} = \phi_{23} = 3\pi/2$. A summary of the phase settings for various potential encoding states, including an example of a decoy state, is illustrated in Fig. 3.

RESULTS

A key element to implement our proposed scheme is precise control of the relative phases between slave laser pulses, ϕ_{12} and ϕ_{23}, as they completely determine the final output states. This can be achieved by carefully adjusting the amplitude of the modulation applied to the master laser's electrical signal. The master laser is operated at 667 MHz and the slave laser at 2 GHz so that every master pulse is long enough to seed three slave pulses. A modulation with a fixed temporal width of 150 ps is applied to the electrical signal between the onsets of two slave pulses, and its voltage amplitude is varied. The amplitude of the pulse at the output of the AMZI is measured as a function of modulation voltage, as shown in Fig. 4(a), confirming the ability to continuously tune the transmitter output pulse intensity. Figure 4(b) shows that the half-wave voltage, V_π is around 0.8 V, which is significantly lower than that of common $LiNbO_3$ phase modulators. The minor deviation from the theoretical values can be attributed to the imperfections in experimental equipment (e.g., phase noise in lasers).

To demonstrate the potential of our scheme for QKD, we implement the BB84 protocol with two decoy states.[28] The experimental setup is shown in Fig. 5. The outputs of Alice (the transmitter) (Fig. 6) consist of a random mixture of the signal states with intensity μ prepared in the Z and Y bases and the decoy states

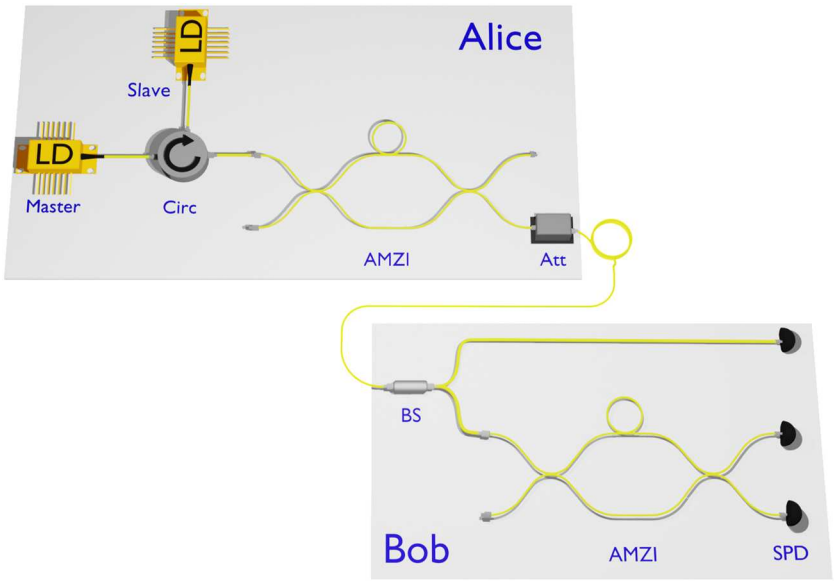


FIG. 5. Experimental setup for BB84 protocol. LD, laser diode; Circ, circulator; AMZI, asymmetric Mach–Zehnder interferometer; Att, attenuator; BS, beamsplitter; SPD, single-photon detector.

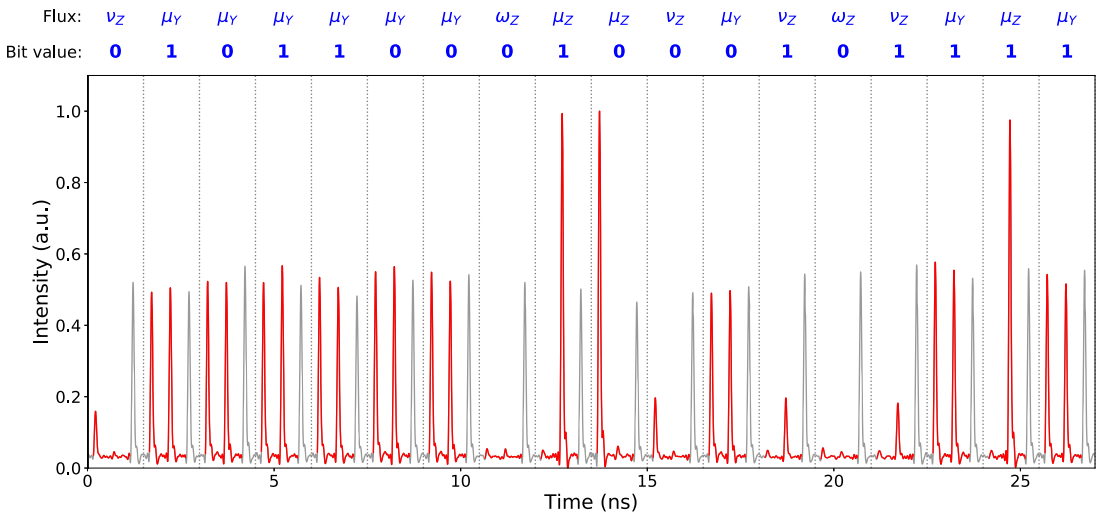


FIG. 6. Time-averaged pulse pattern generated with direct modulation scheme. The corresponding flux and bit value for each bit are indicated at the top of the figure. The red pulses are used for QKD operation, whereas the gray pulses are phase-randomized pulses. Signal states (μ) and decoy states (ν and ω) can be readily generated without any external modulator.

with intensities ν and ω prepared in the Z basis, where $\mu > \nu > \omega$. The intensity levels of the decoy states can be accurately adjusted to maximize the key rate performance. A variable optical attenuator is placed before the output of Alice in order to attenuate the signals to the desired mean photon number level. Bob (the receiver) adopts a passive basis of choice using a beamsplitter. In the Z basis, the photons are directly detected by a single-photon detector (SPD), where the bit value can be retrieved from their arrival time using a time-tagger. In the Y basis, the photons pass through an AMZI , which results in three interfering pulses within a bit. Only the first interfering pulse is measured, as it originated from the interference between the early and late time bins. The phase basis of the AMZI is adjusted such that bits 0 and 1 correspond to the detections in different detectors. The other two interfering pulses involve the interference of photons with no deterministic phase difference, and they are not processed to be used for key generation (similar to the traditional processing scheme for detecting phase-encoded time bins using an AMZI at Bob[23]). The very slight variation in pulse heights in Fig. 6 is related to the finite bandwidth of real-world high-speed components. This has been observed in other QKD transmitter designs too, but not related to our new approach introduced here. The study of such real-world encoding imperfections is a topic in itself, and various solutions have been proposed, including variations to the security proofs and post-processing.[29,30]

In our proof-of-principle QKD experiment, we implement a standard, asymptotic, decoy-state BB84 analysis,[28] which does not explicitly consider the presence of the extra pulses inherent to our modulation scheme. A full security proof is beyond the scope of this work, but we provide some arguments as to why this should not represent an issue in the discussion section. The quantum bit error rate (QBER) is measured and used to compute the secure key rate (SKR), as shown in Fig. 7. Positive key rates can extend up to a channel loss of 48 dB (equivalent to 240 km of standard fiber with an attenuation of 0.2 dB/km). A secure key rate of 2.21 Mbps is measured at 15 dB (75 km), demonstrating the suitability of our system for metro-scale QKD networks. The QBER can be maintained at a base level of 3.3% before the detector noise becomes comparable to the signal counts at high channel losses. This is comparable to the performance achieved by QKD systems using conventional phase and intensity modulators.[16,31]

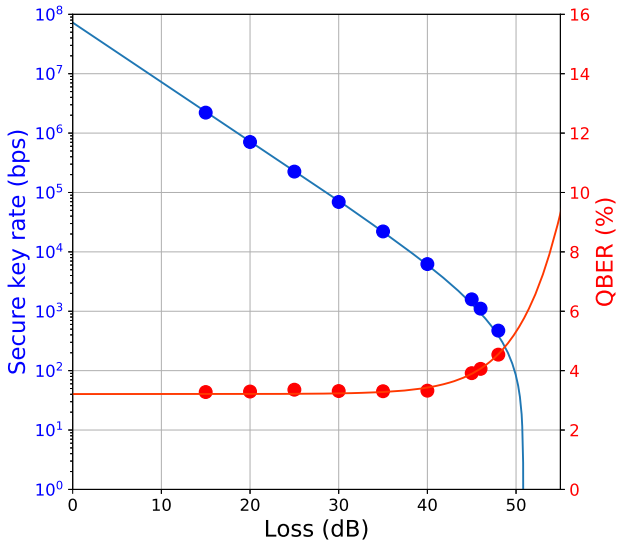


FIG. 7. Key rates and QBER performance of the BB84 protocol carried out by our directly modulated transmitter scheme. The experimental data (dots) are consistent with simulated rates (lines).

DISCUSSION

We have demonstrated a simple scheme to generate phase- and intensity-tunable pulses at GHz clock speeds, which can implement the BB84 protocol without the need for any phase or intensity modulators. As shown earlier, the performance of QKD based on our scheme approaches that of conventional $LiNbO_3$ modulators. We attribute this feature to the adoption of OIL , which significantly reduces the timing jitter and the frequency chirp in the output pulse[27,32] while maintaining a coherent phase transfer from the master to the slave laser.

The presence of additional pulses in this modulation method means it is not completely trivial to apply the security proof for a standard scheme.[28] The concern would be that Eve could somehow break security by attacking these extra pulses. However, this is unlikely to be true, as the state in these extra time bins is essentially obfuscated by the phase randomization procedure. Additionally, well known uncertainty relations between phase and photon number further constrain Eve's ability to extract relevant information. In the Appendix, we describe these arguments in more detail and provide a sketch for how a fully general security proof could be carried out.

Compared to the common approach, where dedicated phase and intensity modulators are required in the transmitter to generate the encoding states and the decoy states, our scheme allows all such states to be generated directly from two lasers and an AMZI by exploiting direct phase modulation technique[23] and coherent interference. In this way, we not only remove the modulators but also the high-speed RF signals and power supplies necessary to drive the modulators, thereby reducing the complexity and cost of a QKD system significantly.

As our transmitter only has two active components (i.e., the lasers), the power consumption is expected to be low. Together with the low V_π, the design is well-suited for on-chip integration,[9] offering a route to compact, low cost and power efficient quantum transmitters. Beyond QKD, this simple approach to generating intensity- and phase-variable pulses could find other applications in classical optical communications, where the ability to precisely manipulate intensity and phase enables novel high-density encoding schemes for pushing communication bit rates.

In conclusion, we have demonstrated a scheme to directly generate phase- and intensity-tunable pulses at high speed using two gain-switching lasers in an OIL configuration with an AMZI. By applying appropriate electrical driving signals to the lasers, the intensity and phase of the pulses can be simply varied. The design is shown to have strong potential as a QKD transmitter for decoy-state QKD, where all required encoding and decoy states for a BB84 protocol can be directly generated without any bulk modulators. Therefore, our scheme offers a new possibility to perform QKD using compact, low-cost, yet high-performance devices, advancing the development of quantum communications toward larger scale deployments.

ACKNOWLEDGMENTS

We thank D. E. Browne for his helpful discussions. We acknowledge funding from the European Union Horizon 2020 Research and Innovation Program (Grant No. 857156, "OPENQKD"). Y.S.L. acknowledges financial support from the EPSRC funded CDT in Delivering Quantum Technologies (Grant No. EP/L015242/1) and Toshiba Europe Ltd.

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

Y. S. Lo: Data curation (lead); Formal analysis (lead); Investigation (equal); Software (equal); Validation (equal); Visualization (equal); Writing – original draft (lead); Writing – review & editing (lead). **R. I. Woodward**: Conceptualization (lead); Formal analysis (equal); Investigation (equal); Methodology (equal); Project administration (equal); Resources (equal); Software (equal); Supervision (equal); Validation (equal); Visualization (equal). **N. Walk**: Conceptualization (equal); Formal analysis (equal); Investigation (equal); Validation (equal); Writing – original draft (equal). **M. Lucamarini**: Conceptualization (equal); Investigation (equal). **I. De Marco**: Conceptualization (equal); Methodology (equal). **T. K. Paraïso**: Investigation (equal); Supervision (equal). **M. Pittaluga**: Conceptualization (equal); Methodology (equal). **T. Roger**: Conceptualization (equal); Methodology (equal). **M. Sanzaro**: Conceptualization (equal); Investigation (equal). **Z. L. Yuan**: Conceptualization (equal); Investigation (equal); Project administration (equal); Supervision (equal). **A. J. Shields**: Funding acquisition (equal); Project administration (equal); Resources (equal); Supervision (equal).

DATA AVAILABILITY

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

APPENDIX: EXPERIMENTAL DETAILS AND SECURITY CONSIDERATIONS

1. Experimental setup

The transmitter consists of two independent distributed feedback (DFB) lasers with a 10 GHz modulation bandwidth and an integrated thermoelectric cooler, operating at 1550 nm. The two lasers are connected through a circulator, allowing light to be injected from the master laser to the slave laser. A variable optical attenuator is used to adjust the injection power. Each laser is driven by an arbitrary waveform generator with a sampling rate of 24 GS/s and 10-bit vertical resolution. The RF driving signal is amplified by an RF amplifier and then combined with a DC bias via a bias-tee. The two modulations on the master RF signals have a temporal width of 150 ps and a separation of 450 ps from each other. The modulation level depends on the desired outputs. The delay between the RF signals of the two lasers is temporally aligned with picosecond resolution to ensure that the slave pulses are coherently seeded by the correct master pulses. The master (slave) laser is driven at a clock rate of 667 MHz with an on-time of 1.4 ns (2 GHz with an on-time of 300 ps). The AMZIs placed in the transmitter and the receiver are chip-based interferometers. Each of them has a delay

line of 500 ps and an integrated heater that can be controlled electronically in one of its arms. The heater acts as a phase shifter , which is used to tune the phase delay between the two arms and align the phase basis between the transmitter and the receiver. An optical filter is also used in the transmitter to reduce the noise and enhance the phase coherence. The channel loss is emulated using a variable optical attenuator. A superconducting nanowire single photon detector with ~70% efficiency and 50 Hz dark counts is used in the receiver. The detection events are measured with a 100 ps resolution time tagger. A central window of 300 ps in the time bin is selected in order to suppress the errors due to timing jitter.

2. QKD protocol

We implement the two-decoy-state BB84 protocol in the asymptotic case[28] with imbalanced basis choice, where the Y (Z) basis is selected with a probability of 90% (10%), i.e., the Y (Z) basis is the majority (minority) basis. The average photon numbers of the signal (μ), decoy (ν), and vacuum (ω) states are 0.4, 0.16, and 0.015, respectively. Alice randomly prepares μ, ν, and ω in the Z basis but only prepare the μ in the Y basis. To match with Alice's basis-sending probability, Bob uses a beamsplitter with a splitting ratio of 90:10 to implement passive basis choice, where Z basis is chosen with a probability of 10% and Y basis is chosen with a probability of 90%. The key bits are extracted from the Y basis only, whereas the Z basis is used to estimate the information leakage. The gain and QBER for each state are measured to estimate the final secure key rate analytically.[28]

3. Security discussion

Here we provide some more details about the additional security considerations that may arise due to the additional pulse that arises in our modulation scheme and sketch how the standard decoy-state BB84 security proof could be modified to account for these. The two issues to keep in mind are (i) whether any information about the encoded bits is leaked directly or (ii) whether the global phase randomization (and hence the decoy-state analysis) is compromised, potentially overestimating the secret key rate.

a. Modulation scheme

We begin by describing the modulation scheme in Fig. 1 in more detail. Each encoding is created from an initial triplet of pulses ($|\alpha_1\rangle$, $|\alpha_2\rangle$, $|\alpha_3\rangle$) passed through an AMZI, leading to an output triplet ($|\alpha_1\rangle$, $|\alpha_2\rangle$, $|\alpha_3\rangle$) where the key is encoded in the phase difference between the pulses in the first two time bins, labeled early (E) and late (L), followed by an unused, randomized pulse in the so-called random (R) bin. To fully capture all the potentially relevant correlations, we also need to consider the pulses either side of a given encoding (i.e., the last pulse of the preceding triplet, $|\alpha_3^P\rangle$, and the first pulse of the following triplet, $|\alpha_1^F\rangle$). The action of the AMZI is to mix each pulse with a vacuum state at the input beamsplitter and then delay the upper (U) arm to be recombined with the subsequent pulse at the final beamsplitter. This means that, before the AMZI, the first pulse of a given encoding triplet occupies the time bin associated with the random pulse of the preceding triplet. In other words, the states in the various time bins before the AMZI are given by (see also Fig. 8)

$$\begin{aligned} L_P: &\quad |\alpha_3^P\rangle = \left|Ae^{i(\omega t+\phi_1+\phi_R^P)}\right\rangle,\\ R_P: &\quad |\alpha_1\rangle = \left|Ae^{i(\omega t+\phi_1)}\right\rangle,\\ E: &\quad |\alpha_2\rangle = \left|Ae^{i(\omega t+\phi_1+\phi_{12})}\right\rangle,\\ L: &\quad |\alpha_3\rangle = \left|Ae^{i(\omega t+\phi_1+\phi_{12}+\phi_{23})}\right\rangle,\\ R: &\quad |\alpha_1^F\rangle = \left|Ae^{i(\omega t+\phi_1+\phi_{12}+\phi_{23}+\phi_R^F)}\right\rangle, \end{aligned} \tag{A1}$$

where $A \in \mathbb{R}$ is the input intensity of each pulse and ϕ_{12} and ϕ_{23} are the relative phases that are chosen to encode one of the four BB84 states. Note that ϕ_1 must be uniformly distributed over $[0, 2\pi)$ in order to make the output ensemble phase randomized. The preceding and following triplets also have a randomized phase, which for brevity we here write relative to the first triplets phases via the variables ϕ_R^F, ϕ_R^P, which is, therefore, also uniformly distributed over $[0, 2\pi)$.

These states can be propagated through the initial beamsplitter, time delay, and final beamsplitter to derive the following output states:

$$\begin{aligned} |\alpha_{R_P}\rangle &= \frac{A}{2}\left(1+e^{i\phi_R^P}\right)e^{i(\omega t+\phi_1)},\\ |\alpha_E\rangle &= \frac{A}{2}e^{i(\omega t+\phi_1)}\left(1+e^{i\phi_{12}}\right),\\ |\alpha_L\rangle &= \frac{A}{2}e^{i(\omega t+\phi_1+\phi_{12})}\left(1+e^{i\phi_{23}}\right),\\ |\alpha_R\rangle &= \frac{A}{2}e^{i(\omega t+\phi_1+\phi_{12}+\phi_{23})}\left(1+e^{i\phi_R^F}\right). \end{aligned} \tag{A2}$$

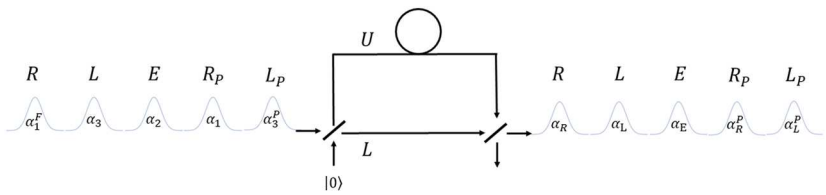


FIG. 8. Schematic of direct phase and intensity modulation technique. The incoming pulse train of five time bins shows a complete triplet $\alpha_{1,2,3}$ along with the first pulse of the following triplet α_1^F and the last pulse of the preceding triplet α_3^P. A delay in the top arm of the AMZI causes interference between successive pulses, which facilitates modulation of the relative phase and intensity of the output state in the early (E) and late (L) time bins.

The complex amplitude describing a coherent state can be expressed as a phase and an intensity, $|\alpha\rangle = |re^{i\phi}\rangle$, where

$$r = \sqrt{\mathrm{Re}(\alpha)^2 + \mathrm{Im}(\alpha)^2}, \qquad \phi = \tan^{-1}\left(\frac{\mathrm{Im}(\alpha)}{\mathrm{Re}(\alpha)}\right), \tag{A3}$$

which gives,

$$\begin{aligned} r_{R_P} &= A\cos\left(\frac{\phi_R^P}{2}\right), \quad \phi_{R_P} = \omega t + \frac{\phi_R^P}{2} + \phi_1, \\ r_E &= A\cos\left(\frac{\phi_{12}}{2}\right), \quad \phi_E = \omega t + \phi_1 + \frac{\phi_{12}}{2}, \\ r_L &= A\cos\left(\frac{\phi_{23}}{2}\right), \quad \phi_L = \omega t + \phi_1 + \phi_{12} + \frac{\phi_{23}}{2}, \\ r_R &= A\cos\left(\frac{\phi_R^F}{2}\right), \quad \phi_R = \omega t + \frac{\phi_R^F}{2} + \phi_1 + \phi_{12} + \phi_{23}. \end{aligned} \tag{A4}$$

From this, we can immediately verify the claims in the main text that the intensity of the E and L bins is controlled by ϕ_{12} and ϕ_{23} and that the phase difference between the E and L bins is given by $\phi_{EL} = (\phi_{12} + \phi_{23})/2$, which allows the following encoding pattern for all four BB84 states:

$$\begin{aligned} |0\rangle &: \phi_{12} = 0, \phi_{23} = \pi, \quad |1\rangle : \phi_{12} = \pi, \phi_{23} = 0, \\ |+\rangle &: \phi_{12} = \frac{\pi}{2}, \phi_{23} = \frac{\pi}{2}, \quad |-\rangle : \phi_{12} = \frac{3\pi}{2}, \phi_{23} = \frac{3\pi}{2}. \end{aligned} \tag{A5}$$

b. Security considerations

Turning to the security implications of the "random" pulses, a straightforward substitution of Eq. (A5) into Eq. (A2) shows that the coherent amplitude of both the R and R_P bins is identical for all encoding choices. This is because for all settings in Eq. (A5), it holds that $\phi_{12} + \phi_{23} = \pi \bmod 2\pi$. This might initially seem sufficient to argue that there is no additional information leakage due to the extra pulses. However, one should also consider the possibility that Eve could choose to combine different pulses in her attack. For instance, the relative phases between the early and late bins and their adjoining randomized pulses are

$$\phi_{LR} = \frac{\phi_R^F + \phi_{23}}{2}, \qquad \phi_{ER_P} = \frac{\phi_R^P - \phi_{12}}{2}. \tag{A6}$$

By themselves, the values of ϕ_{LR} and ϕ_{ER_P} leak no information because the phases that determine the secret key, ϕ_{12} and ϕ_{23}, are effectively one-time padded by the uniformly distributed variables, ϕ_R^P and ϕ_R^F. However, by considering Eq. (A4), we can see information about ϕ_R^P and ϕ_R^F could in turn be obtained by measuring the intensity of the random pulses (r_{R_P} and r_R). Nevertheless, security can still be maintained provided it is impossible for Eve to simultaneously learn the relative phases of any two pulses and the corresponding intensities, which is the case due to the conjugate nature of the number and phase operators. A measurement that perfectly revealed that photon number in either the R or R_P bins would totally randomize the phase. Moreover, even if Eve chooses to maximize her information about relative phases in Eq. (A4), this will tell her nothing about the absolute phase of each encoding triplet (ϕ_1, ϕ_1^P, etc.) since learning the difference between two uniformly random variables leaks no information about either variable. Therefore, the phase randomization condition required for a decoy state analysis is not compromised.

Although a full security proof is beyond the scope of this work, we provide a sketch of how one could proceed. Firstly, one would adapt the standard decoy argument to show that, from Eve's perspective at the ensemble level, the experimental scheme is indistinguishable from a scheme in which Alice and Bob prepare true single photon qubits in the E and L bins along with extra coherent states in the random bins. Then, construct a complete entanglement based version of this modulation scheme, including a fictitious measurement on a suitably prepared entangled state that determines the randomized phase of each encoding triplet and projectively prepares the appropriate coherent state in each random bin. The total system would then be described by a pure state $|X_A B E R_A R\rangle$, where R describes the extra coherent pulses and R_A is Alice's register of the randomized phase values (these are never used in the protocol, so there is no actual need for Alice to possess this register, it is only necessary that Eve does not possess it). Then, in the worst case one, would simply assume that Eve is given the entire R system, and one would then bound Eve's conditional entropy about the Alice's key generation measurements, $S(Z_A|ER)$. Note that this approach means no extra monitoring of the random bins is required. The previous arguments regarding the impossibility of learning the key from the R register could be made quantitative by utilizing tools such as entropic uncertainty relations for phase and photon number (e.g., Refs. 33 and 34). Some of these results require an upper bound on the energy, but this is simply given by the maximum encoding amplitude, A. These would be combined with the standard security arguments for the information leaked through Eve's purification of the channel describing the measured time bins[28] would be sufficient to determine the secret key rate.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145 (2002); arXiv:0601207 [quant-ph].

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, 1984), Vol. 175.

[3] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43 (2017); arXiv:1707.00542.

[4] Y.-A. Chen, Q. Zhang, T.-Y. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature **589**, 214–219 (2021).

[5] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field

test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**, 10387 (2011); arXiv:1008.1508.

[6]D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New J. Phys. **13**, 123001 (2011).

[7]J. F. Dynes, A. Wonfor, W. W. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J. P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," Npj Quantum Inf. **5**(1), 101 (2019).

[8]T. Y. Chen, X. Jiang, S. B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L. K. Chen, W. Y. Liu, H. F. Zhang, K. Cui, H. Liang, X. G. Li, Y. Mao, L. J. Wang, S. B. Feng, Q. Chen, Q. Zhang, L. Li, N. L. Liu, C. Z. Peng, X. Ma, Y. Zhao, and J. W. Pan, "Implementation of a 46-node quantum metropolitan area network," Npj Quantum Inf. **7**(1), 134 (2021).

[9]T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," Npj Quantum Inf. **5**, 42 (2019).

[10]D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. Derose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018); arXiv:1708.00434.

[11]P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017); arXiv:1509.00768.

[12]M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400 (2018).

[13]J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," Nat. Photonics **15**, 570 (2021).

[14]M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M. J. Li, Z. Yuan, and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," Nat. Photonics **15**, 530 (2021); arXiv:2012.15099.

[15]A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018); arXiv:1807.03222.

[16]Z. Yuan, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, A. J. Shields, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, and J. F. Dynes, "10-Mb/s quantum key distribution," J. Lightwave Technol. **36**, 3427 (2018).

[17]B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69 (2013); arXiv:1309.6431.

[18]Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Phys. Rev. X **6**, 011024 (2016).

[19]G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330 (2000).

[20]D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325 (2004); arXiv:0212066 [quant-ph].

[21]W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003); arXiv:0211153 [quant-ph].

[22]H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005); arXiv:0411004 [quant-ph].

[23]Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, "Directly phase-modulated light source," Phys. Rev. X **6**, 031044 (2016); arXiv:1605.04594.

[24]T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. Yuan, and A. J. Shields, "Advanced laser technology for quantum communications (tutorial review)," Adv. Quantum Technol. **4**, 2100062 (2021); arXiv:2108.13642.

[25]R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. L. Yuan, and A. J. Shields, "Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers," Npj Quantum Inf. **7**, 58 (2021).

[26]R. Shakhovoy, M. Puplauskis, V. Sharoglazova, A. Duplinskiy, V. Zavodilenko, A. Losev, and Y. Kurochkin, "Direct phase modulation via optical injection: Theoretical study," Opt. Express **29**, 9574 (2021); arXiv:2011.09263.

[27]Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, "Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications," Phys. Rev. Appl. **2**, 064006 (2014); arXiv:1501.01900.

[28]X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005); arXiv:0503005 [quant-ph].

[29]X. Sixto, V. Zapatero, and M. Curty, "Security of decoy-state quantum key distribution with correlated intensity fluctuations," Phys. Rev. Appl. **18**, 044069 (2022).

[30]K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses," Npj Quantum Inf. **4**, 8 (2018).

[31]M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express **21**, 024550 (2013); arXiv:1302.4139.

[32]E. K. Lau, L. J. Wong, and M. C. Wu, "Enhanced modulation characteristics of optical injection-locked lasers: A tutorial," IEEE J. Sel. Top. Quantum Electron. **15**, 618 (2009).

[33]M. J. W. Hall, "Phase resolution and coherent phase states," J. Mod. Opt. **40**, 809 (1993).

[34]P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, "Entropic uncertainty relations and their applications," Rev. Mod. Phys. **89**, 015002 (2017).