nature COMMUNICATIONS

ARTICLE

https://doi.org/10.1038/s41467-022-31534-7 OPEN

Mode-pairing quantum key distribution

Pei Zeng [1], Hongyi Zhou[1], Weijie Wu[1] & Xiongfeng Ma [1]✉

Quantum key distribution — the establishment of information-theoretically secure keys based on quantum physics — is mainly limited by its practical performance, which is characterised by the dependence of the key rate on the channel transmittance $R(\eta)$. Recently, schemes based on single-photon interference have been proposed to improve the key rate to $R = O(\sqrt{\eta})$ by overcoming the point-to-point secret key capacity bound with interferometers. Unfortunately, all of these schemes require challenging global phase locking to realise a stable long-arm single-photon interferometer with a precision of approximately 100 nm over fibres that are hundreds of kilometres long. Aiming to address this problem, we propose a mode-pairing measurement-device-independent quantum key distribution scheme in which the encoded key bits and bases are determined during data post-processing. Using conventional second-order interference, this scheme can achieve a key rate of $R = O(\sqrt{\eta})$ without global phase locking when the local phase fluctuation is mild. We expect this high-performance scheme to be ready-to-implement with off-the-shelf optical devices.

[1] Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China. ✉email: xma@tsinghua.edu.cn

Quantum key distribution (QKD)[1,2] is currently the most successful application of quantum information science and serves as the first stepping stone towards a future quantum communication network[3]. A core advantage of QKD compared to other quantum communication tasks is that it is ready to implement with current commercially available off-the-shelf optical devices. However, two major characteristics of QKD —its practical security and key-rate performance—limit its real-life implementation. The key generation speed suffers heavily from transmission loss in the optical channel. Fundamentally, the asymptotic key rate for point-to-point QKD schemes is upper bounded by the repeaterless rate-transmittance bounds[4,5], which are approximately linear functions of the transmittance, $R \leq O(\eta)$. For example, when η is small, the PLOB repeaterless rate-transmittance bound[5] is about 1.44η. Quantum repeaters[6–8] have been proposed as a radical solution to this problem. Unfortunately, none of the quantum repeater proposals is easy to implement in the near term.

In real-life use, the deviation of the realistic behaviour of physical devices from their ideal ones gives rise to critical issues in practical security. There are many quantum attacks that can take advantage of the loopholes introduced by device imperfections[9]. A typical QKD system can be divided into three parts: source, channel, and measurement. The security of the channel has been well addressed in the security proofs for QKD[10–12]. The source is relatively simple and can be well characterised[13]. In contrast, the measurement device is complicated and difficult to calibrate. Moreover, an adversary could manipulate the measurement device by sending unexpected signals[14,15]. To solve this implementation security problem, measurement-device-independent quantum key distribution (MDI-QKD) schemes have been proposed to close the detection loopholes once and for all[16]. Various experimental systems have been successfully demonstrated[17–20], with extension to a communication network[21].

A generic MDI-QKD setup is shown in Fig. 1a. Each of the two communicating parties, Alice and Bob, holds a quantum light source, encodes random bits into quantum pulses, and sends these pulses to a measurement site through lossy channels. Measurement devices are possessed by an untrusted party, Charlie, who is supposed to correlate Alice's and Bob's signals via interference detection. Based on the detection results announced by Charlie, Alice and Bob sift the local random bits encoded in the pulses to generate secure key bits. Note that the security of MDI-QKD schemes does not rely upon the physical implementation of the detection devices. Alice and Bob need to trust only their own locally encoded quantum sources. Since neither Alice nor Bob receives quantum signals from the channel during key distribution, any hacker's attempt to manipulate the users' devices becomes extremely difficult compared to regular QKD schemes[14,15].

Strictly speaking, MDI-QKD is not a point-to-point scheme, as there is an interference site between Alice and Bob. Consequently, it is not necessarily limited by the repeaterless rate-transmittance bound. Nevertheless, the original MDI-QKD scheme[16], in which Alice and Bob both encode a 'dual-rail' qubit into a single-photon subspace on two polarization modes, unfortunately, cannot overcome this bound. Later, alternative schemes were proposed[22,23] in which the qubit is encoded into two optical time bins. We refer to schemes of this type as two-mode MDI-QKD, in the sense that the single-side key information is encoded in the relative phase of the coherent states in the two orthogonal optical modes, i.e., second-quantized electromagnetic fields. To correlate Alice's and Bob's encoded information in a two-mode scheme, a successful two-photon interference measurement is required. If either Alice or Bob's emitted photon is lost in transmission, there will be no conclusive detection result. For example, in the time-bin encoding scheme[23] shown in Fig. 1b, Alice and Bob each emit a qubit encoded in two time-bin modes, with Alice emitting A_1 and A_2 and Bob emitting B_1 and B_2. Only when both the interference between modes A_1 and B_1 and that between A_2 and B_2 yield successful detection can Alice restore Bob's raw key information. Thus, successful interference requires a coincidence detection. Due to this coincidence-detection requirement, rounds with only a single detection are discarded, resulting in a relatively low key generation rate—one that is a linear function of the transmittance, $O(\eta)$. From the perspective of practical implementation, however, coincidence detection also has certain merits. This approach can ensure stable optical interference, while Alice and Bob need only to stabilise the relative phases between the two modes.

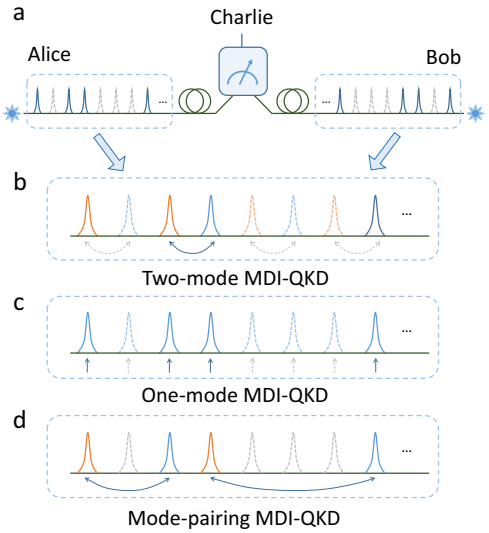

Fig. 1 Comparison of two-mode, one-mode and mode-pairing MDI-QKD schemes. a Schematic diagram of a generic MDI-QKD scheme. The solid and dashed pulses yield successful and unsuccessful detection, respectively, at the measurement site. For **b**, **c** and **d**, each wave packet in the diagram represents two independent pulses emitted simultaneously by Alice and Bob. **b** In two-mode MDI-QKD schemes, the pairing of the blue pulses (as phase references) and orange pulses (as signals) is predetermined, necessitating coincidence detection. **c** In one-mode MDI-QKD schemes (e.g., twin-field quantum key distribution and its variants), there is no phase reference pulse, necessitating global phase locking. **d** In the mode-pairing MDI-QKD scheme, in accordance with the detection results, Alice and Bob pair the clicked pulses and assign them to be either reference or signal pulses, such that neither coincidence detection nor global phase locking is required.

Coincidence detection is the essential factor that prevents MDI-QKD from overcoming the linear key-rate bound. To eliminate this requirement, a new type of MDI-QKD scheme called twin-field quantum key distribution (TF-QKD) based on encoding information into a single-optical mode have been proposed[24], illustrated in Fig. 1c. Later on, variants of TF-QKD have been proposed, among which the key information in encoded in either the phase[25,26] (known as phase-matching QKD) or the intensity[27] (known as sending-or-not-sending TF-QKD) of coherent states. In this work, we refer to these twin-field-type schemes as one-mode MDI-QKD schemes for a conceptual comparison to the traditional two-mode MDI-QKD schemes, since the single-side information in these schemes is encoded into a single-optical mode in each round. We remark that the single-optical-mode encoding MDI-QKD scheme was first proposed in ref. [28] as "MDI-B92" scheme. Similar to the

Box 1 | Mode-pairing scheme

1. **State preparation**: In the i-th round ($i = 1, 2, \ldots, N$), Alice prepares a coherent state $|\sqrt{\mu_i^a}e^{i\phi_i^a}\rangle$ in optical mode A_i with an intensity μ_i^a randomly chosen from $\{0, \mu\}$ and a phase ϕ_i^a uniformly chosen from $[0, 2\pi)$. Similarly, Bob randomly chooses μ_i^b and ϕ_i^b and prepares $|\sqrt{\mu_i^b}e^{i\phi_i^b}\rangle$ in mode B_i.
2. **Measurement**: Alice and Bob send modes A_i and B_i to Charlie, who performs single-photon interference measurements. Charlie announces the click patterns for both detectors L and R.
   Alice and Bob repeat the above two steps for N rounds. Then, they postprocess the data as follows.
3. **Mode pairing**: For all rounds with successful detection, in which one and only one of the two detectors clicks, Alice and Bob apply a strategy of grouping two clicked rounds as a pair. The encoded phases and intensities in these two rounds form a data pair. A simple pairing strategy is introduced in Box 2.
4. **Basis sifting**: Based on the intensities of the two grouped rounds indexed by i and j, Alice labels the 'basis' of the data pair as Z if the intensities are $(0, \mu)$ or $(\mu, 0)$, as X if the intensities are (μ, μ), or as '0' if the intensities are $(0, 0)$. Bob sets the basis using the same method. Alice and Bob announce the basis of each data pair; if they both announce the basis X or Z, they maintain the data pairs, whereas otherwise, the data pairs are discarded.
5. **Key mapping**: For each Z-basis pair (Z-pair for simplicity) at locations i and j, Alice sets her key as $\kappa^a = 0$ if $(\mu_i^a, \mu_j^a) = (0, \mu)$ and $\kappa^a = 1$ if $(\mu_i^a, \mu_j^a) = (\mu, 0)$. For each X-basis pair (X-pair for simplicity) at locations i and j, the key is extracted from the relative phase $(\phi_j^a - \phi_i^a) = \theta^a + \pi\kappa^a$, where the raw key bit is $\kappa^a = \left\lfloor ((\phi_j^a - \phi_i^a)/\pi \bmod 2) \right\rfloor$ and the alignment angle is $\theta^a := (\phi_j^a - \phi_i^a) \bmod \pi$. In a similar way, Bob assigns his raw key bit κ^b and determines θ^b. The difference in the key mapping for Z-pairs is that, Bob sets the raw key bit κ^b as 0 if $(\mu_i^b, \mu_j^b) = (\mu, 0)$ and $\kappa^b = 1$ if $(\mu_i^b, \mu_j^b) = (0, \mu)$. As an extra step on the X-pairs, if Charlie's detection announcement is (L, L) or (R, R), Bob keeps the bit κ^b; otherwise, if Charlie's announcement is (L, R) or (R, L), Bob flips κ^b. For the X-pairs, Alice and Bob announce the alignment angles θ^a and θ^b. If $\theta^a = \theta^b$, then the data pairs are kept; otherwise, the data pairs are discarded.
6. **Parameter estimation**: Alice and Bob estimate the fraction of clicked signals $q_{(1,1)}$ and the corresponding phase error rate $e_{(1,1)}^X$ of Z-pairs where Alice and Bob both emit a single photon at locations i and j, using the data of the Z-pairs and X-pairs. They also estimate the quantum bit error rate $E^{(\mu,\mu),Z}$ of the Z-pairs.
7. **Key distillation**: Alice and Bob use the Z-pairs to generate a key. They perform error correction and privacy amplification on the basis of $q_{(1,1)}$, $E^{(\mu,\mu),Z}$ and e_{11}^X.

Duan-Lukin-Cirac-Zoller-type repeater design[29], such one-mode schemes use single-photon interference instead of coincidence detection, hence yielding a quadratic improvement in key rate compared to two-mode schemes[24–26]. As a result, they can overcome the point-to-point linear key-rate bound[4,5]. Unfortunately, one-mode schemes are more challenging to implement due to the unstable optical interference resulting from the lack of global phase references. For example, in the phase-matching QKD (PM-QKD) scheme[25], the key information is encoded into the global phase of Alice's and Bob's coherent states. The phases of the coherent states generated by two remote and independent lasers need to be matched at the measurement site. A small phase drift or fluctuation caused by the lasers and/or channels is hazardous for key generation.

At first glance, it seems that we cannot simultaneously enjoy the advantages of one-mode schemes (i.e., quadratic improvement in successful detection) and two-mode schemes (i.e., stable optical interference), due to an intrinsic trade-off between the information-encoding efficiency and robustness. On the one hand, the relative information among different optical modes is more difficult to retrieve when the channel loss is large. On the other hand, the global phase of a coherent state is not as stable as the relative phase between two coherent states travelling through the same quantum channel. In a typical 200-km fibre with a telecommunication frequency of 1550 nm, the phase of a coherent state is susceptible to small fluctuations in the optical transmission time (~10^{-15} s), optical length (~200 nm) and light frequency (~100 kHz). Recently, experimentalists have made great efforts to demonstrate high-performance in one-mode schemes, utilising high-end technologies to perform a precise control operation to stabilise the global phase by locking the frequency and phase of the coherent states[30–37]. However, this increases the experimental difficulty and undermines the applicability of one-mode schemes in real life.

In this work, we propose a mode-pairing MDI-QKD scheme that aims to offer both—simple implementation and high performance. Hereafter, we refer to this scheme as the mode-pairing scheme for simplicity. By observing that the majority of detection events are single-clicks and are discard in the two-mode MDI-QKD schemes, we try to recycle the discarded single-click in the mode-pairing scheme. To do that, the coherent states in the transmitted modes are initially prepared independently with randomly encoded information. Based on the fact that the two detection events used to read out the encoded information do not need to occur at two predetermined locations, the key is extracted from two paired detection events rather than coincidence detection, as shown in Fig. 1d. This offers a quadratic improvement akin to that of one-mode schemes when the local phases can be stabilized using currently available phase stabilization techniques. Moreover, key information about the mode-pairing scheme is encoded in the relative phases or intensities, whose stability relies only upon the conditions of the local phase references and optical paths. Therefore, the technical complexity is similar to that of two-mode schemes, which have been widely implemented both in the laboratory[17–19,38] and in the field[21,39]. Notably, to adapt to different hardware conditions, the mode-pairing scheme can be freely tuned between the one-mode and two-mode schemes by adjusting a pulse-interval parameter (as discussed later in Results' subsection "Pairing strategy") during data postprocessing to optimise the system performance.

Results

Mode-pairing scheme. In the mode-pairing scheme, Alice and Bob first prepare coherent states with independently and randomly chosen intensities and phases in each emitted optical mode. These coherent states are sent to the untrusted measurement site, Charlie. Based on Charlie's announced measurement results, Alice and Bob pair the optical modes with successful detection and determine the key bits and bases for each mode pair locally. They then sift the bases and generate secure key bits via postprocessing. The scheme is introduced in Box 1 and illustrated in Fig. 2a. For simplicity of the introduction of the main protocol design, we omit the details of the decoy-state method[40] and

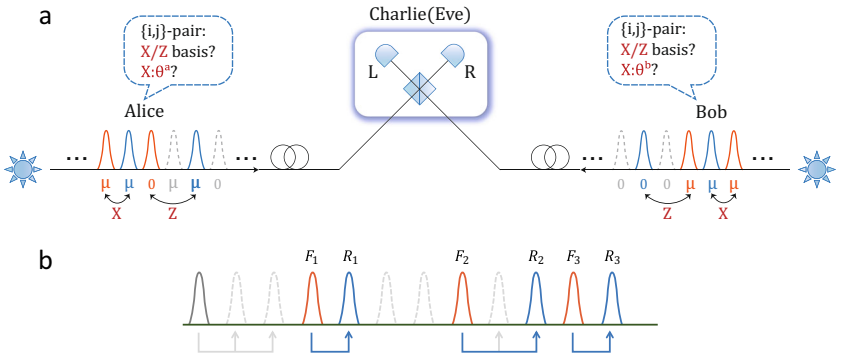

Fig. 2 Schematic diagram of the mode-pairing MDI-QKD scheme and the simple pairing strategy with maximal-pairing interval *l*. The solid and dashed pulses are those with and without successful detection, respectively. Orange and blue pulses are, respectively, the front and rear pulses that succeed in pairing within *l* pulses, while grey pulses are the ones fail in pairing. **a** In the mode-pairing MDI-QKD scheme, Alice and Bob, first prepare coherent pulses with random intensities chosen from $\{0, \mu\}$ and random phases $\phi_i^{a(b)} \in [0, 2\pi)$ and send them to Charlie. After interference measurement, Charlie announces the detection results, based on which Alice and Bob pair the pulses and determine their encoding bases. For *X*-pairs, they announce the alignment angles θ^a and θ^b and keep data for which $\theta^a = \theta^b$. They use *Z*-pairs to generate keys and other data for parameter estimation. **b** We set $l = 2$ in the simple pairing strategy for example. The labels F_k and R_k represent the front and rear pulses, respectively, in the *k*-th successful pair.

discrete phase randomisation here. A complete description of the mode-pairing scheme is given in the Methods' subsection "Mode-pairing scheme with decoy states".

In the mode-pairing scheme, we mainly consider the keys generated from the *Z*-pair data, since they have a much lower quantum bit error rate $E_{\mu\mu}^Z$ than the *X*-pair data. The encoding of the mode-pairing scheme in Box 1 originates from the time-bin encoding MDI-QKD scheme[23]. If Alice's two paired optical modes $\{A_i, A_j\}$ are assigned to the *Z*-basis, then the state of the two optical modes is either $|0\rangle_{A_i}|\sqrt{\mu}e^{i\phi_j^a}\rangle_{A_j}$ or $|\sqrt{\mu}e^{i\phi_i^a}\rangle_{A_i}|0\rangle_{A_j}$, where ϕ_i^a and ϕ_j^a are two independent random phases. We can write the encoded states in a unified form:

$$|\psi_Z^a\rangle_{A_i,A_j} = |\sqrt{\kappa^a\mu}e^{i\phi_i^a}\rangle_{A_i}|\sqrt{\bar{\kappa}^a\mu}e^{i\phi_j^a}\rangle_{A_j}, \quad (1)$$

where κ^a is the encoded key information and $\bar{\kappa} := \kappa \oplus 1$ is the inverse of κ. In the other case, in which the two optical modes $\{A_i, A_j\}$ are assigned to the *X*-basis, we can rewrite their two independent random phases ϕ_i^a and ϕ_j^a as

$$\begin{aligned} \phi^a &:= \phi_i^a \in [0, 2\pi), \\ \phi_\delta^a &:= \phi_j^a - \phi_i^a \in [0, 2\pi). \end{aligned} \quad (2)$$

In this way, the phase ϕ^a becomes a global random phase on the pulse pair, while ϕ_δ^a is the relative phase for quantum information 'encoding'. Due to the independence of ϕ_i^a and ϕ_j^a, the phases ϕ^a and ϕ_δ^a are also independent of each other and uniformly range from $[0, 2\pi)$. By definition, we have $\phi_\delta^a = \theta^a + \pi\kappa^a$. Then, the *X*-pair state can be written as,

$$|\psi_X^a\rangle_{A_i,A_j} = |\sqrt{\mu^a}e^{i\phi^a}\rangle_{A_i}|\sqrt{\mu^a}e^{i(\phi^a+\theta^a+\kappa^a\pi)}\rangle_{A_j}, \quad (3)$$

where $\mu^a \in \{0, \mu\}$. When $\theta = 0$ or $\pi/2$, Alice emits *X*-basis or *Y*-basis states, respectively, as used in the time-bin encoding MDI-QKD scheme[23].

We remark that in either the *Z*-pair state in Eq. (1) or the *X*-pair state in Eq. (3), there is a global random phase ϕ^a, which will not be revealed publicly. With this (global coherent state) phase randomisation, the emitted *Z*- and *X*-pair states can be regarded as a mixture of photon number states[40]. Then, Alice and Bob can estimate the detections caused by the pairs where they both emit single photons and use them to generate secure keys, in a manner similar to traditional two-mode schemes. Therefore, the security of the mode-pairing scheme is similar to that of two-mode schemes. Nevertheless, the mode-pairing scheme in Box 1 has the following unique features.

1. The emitted states in different optical modes $\{A_i\}$ are independent and identically distributed (i.i.d.). Therefore, the information encoded in different optical modes is completely decoupled.
2. Based on the postselection of clicked signals, different optical modes are paired afterwards. The relative information between the two modes is then converted into raw key data.

In the mode-pairing scheme, the key information is determined not in the state preparation step, but by the detection location, sharing some similarities with the differential-phase-shifting QKD scheme[41,42]. It is the untrusted measurement site that determines the location of successful detection and thereby affects the pairing setting. The 'dual-rail' qubits encoded on the single photons are 'postselected' on the basis of this detection. By virtual of the independence of the optical modes, the information encoded in the 'postselected' qubits cannot be revealed from other optical pulses.

For another comparison, the sending-or-not-sending (SNS) TF-QKD scheme[27] also uses a *Z*-basis time-bin encoding, whereby either Alice or Bob emits an optical mode to generate key bits. The state preparation of the mode-pairing scheme shares similarities with the SNS-TFQKD scheme. However, the information of the mode-pairing scheme is encoded into the relative information between the two optical modes. As a result, the basis-sifting and key mapping of the mode-pairing scheme follow different logic originated from the time-bin encoding MDI-QKD scheme[23]. Note that in the SNS scheme, bits 0 and 1 are highly biased in the *Z* basis, whereas in the mode-pairing scheme, they are evenly distributed.

A critical issue in the security analysis of the mode-pairing scheme is to maintain the flexibility to determine in which two optical modes to perform the overall photon number measurement until Charlie announces the detection results. Note that, in the original two-mode QKD schemes, the encoders can always be assumed to perform an overall photon number measurement and post-select the single-photon components as good 'dual-rail' qubits before they emit their signals to Charlie. In the mode-pairing scheme, however, this is not viable because the optical pulse pair, for which the single-photon component is defined, is postselected based on Charlie's detection announcement. To solve

Box 2 | Simple pairing strategy

Input: Charlie's announced detection results C_i for $i = 1$ to N; maximal pairing interval l.
Output: K pairs; front- and rear-pulse locations (F_k, R_k) for the k-th pair, where $k = 1$ to K.

Initialise the pairing index $k := 1$; initialise the flag $f := 0$.
for $i = 1$ **to** N **do** ▷ Enumerating all locations
  if $f = 0$ **then** ▷ Searching for the front-pulse location
    if $C_i = 1$ **then** ▷ Successful detection
      Set the temporary front-pulse location to $F_k := i$; set the flag to $f := 1$.
    end if
  else ▷ Searching the rear-pulse location
    if $C_i = 1$ **then** ▷ Successful detection
      Set the rear-pulse location to $R_k := i$; update the pairing index to $k := k + 1$; reset the flag to $f := 0$.
    else if $F_k - i \geq l$ **then** ▷ Pairing interval exceeding l
      Reset the flag to $f := 0$.
    end if
  end if
end for
Set the total number of pairs to $K := k - 1$.

this problem, we introduce source replacement for the random phases in the coherent states to purify them as ancillary qudits and define an indirect overall photon number measurement on them. The source-replacement procedure can be found in the Methods' subsection "Source replacement of the encoding state". Conditioned on the indirect overall photon number measurement result to be single-photon states, the X-basis error rate fairly estimates the Z-basis phase error rate for the signals for which Alice and Bob both emit single photons.

In Supplementary Note 2, we provide a detailed security proof based on entanglement distillation. The main idea is to introduce a 'fixed-pairing' scheme, in which the pairing setting, i.e., which locations are paired together, is predetermined and hence independent of Charlie's announcement. We first prove that, with any given pairing setting, the fixed-pairing scheme is secure, as it can be reduced to a two-mode MDI-QKD scheme. Afterwards, we examine the private state generated by the mode-pairing scheme and prove that it is the same as that of a fixed-pairing scheme under all possible measurements that Charlie could perform and announcement methods. In this way, we prove the equivalence of the mode-pairing scheme to a group of fixed-pairing schemes with different pairing settings.

Pairing strategy. The pairing strategy mentioned in Step 3 lies at the core of the mode-pairing scheme in Box 1, which correlates two independent signals and determines their bases and key bits. Note that the relative phase between two paired quantum signals determines the key information on the X basis. When the time interval between these two pulses becomes too large, the key information suffers from phase fluctuation, which is characterised by the laser coherence time. Therefore, Alice and Bob should establish a maximal pairing interval l, such that the number of pulses between the two paired signals should not exceed l. In practice, l can be estimated by multiplying the laser coherence time by the system repetition rate.

Here, we consider a simple pairing strategy in which Alice pairs adjacent detection pulses together if the time interval between them is not too large ($\leq l$). The details are shown in the simple pairing strategy in Box 2 and illustrated in Fig. 2b. Charlie's announcement in the i-th round is denoted by a Boolean variable C_i that indicates whether the detection is successful. That is, $C_i = 1$ implies that either the detector L or R clicks. Otherwise, there is no click or double clicks.

To check the efficiency of this pairing strategy, let us calculate the pairing rate r_p (i.e. the average number of pairs generated per pulse). We assume that Alice and Bob choose intensities 0 and μ with equal probability, maximising the number of successful pairs in the Z basis. With a typical QKD channel model, the pairing rate r_p is calculated as shown in the Methods' subsection "Mode-pairing-efficiency calculation",

$$r_p(p, l) = \left[\frac{1}{p[1-(1-p)^l]} + \frac{1}{p}\right]^{-1}, \tag{4}$$

where p is the probability that the emitted pulses result in a click event, given approximately by $\eta_s\mu$. Here, η_s and η denote the channel transmittance from Alice to Charlie and the total transmittance from Alice to Bob, respectively. When the channel is symmetric for Alice and Bob, we have $\eta = \eta_s^2$. An explicit simulation formula for p in a pure-loss channel is given in Supplementary Note 4. Note that both the pairing ratio r_p and the detection probability p can be directly obtained by experimentation.

The raw key rate mainly depends on the pairing rate r_p. Now, let us check the scaling of r_p with the channel transmittance in the symmetric-channel case. If the local phase reference is sufficiently stable, then the maximal interval can be set to $l \to +\infty$. In this case,

$$r_p = \frac{p}{2} \approx \frac{\eta_s\mu}{2} = O(\sqrt{\eta}), \tag{5}$$

where the optimal intensity is $\mu = O(1)$, as evaluated in Supplementary Note 5. On the other hand, if the local phase reference is not at all stable, one must set $l = 1$; then,

$$r_p = \frac{p^2}{1+p} \approx \frac{\eta_s^2\mu^2}{1+\eta_s\mu} = O(\eta). \tag{6}$$

In this case, the experimental requirements for the mode-pairing scheme are close to those of the existing time-bin MDI-QKD scheme[23]. Now, if we consider a finite value of l, the dependence of $r_p(p, l)$ on η will be decided by how the denominator of the first term in Eq. (4), $p[1-(1-p)^l]$, depends on $p \approx \eta_s\mu$. When $pl \gg 1$, $r_p(p, l)$ scales with p linearly, hence

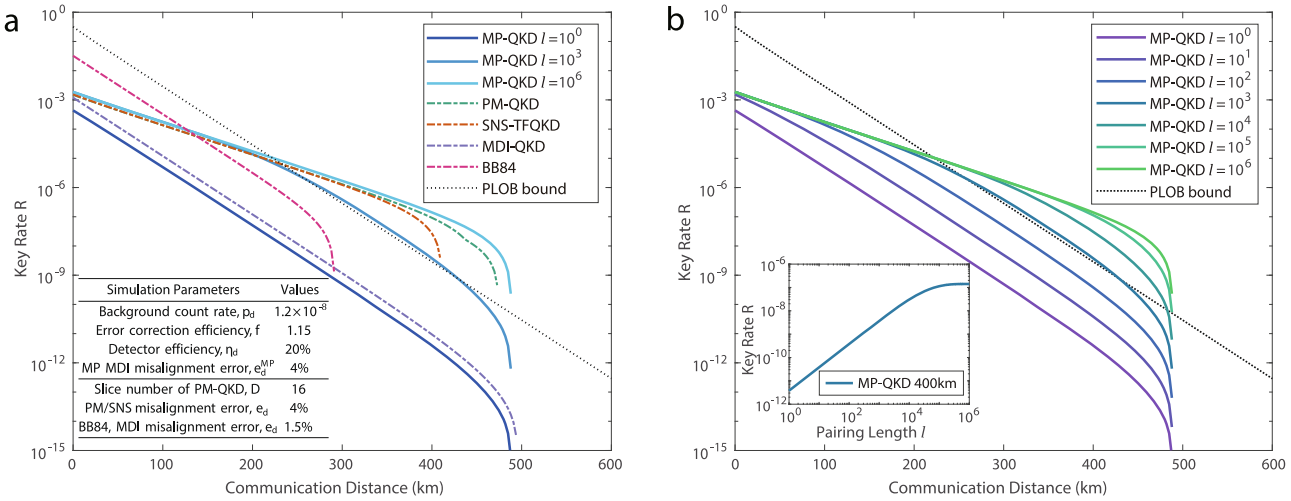

Fig. 3 Asymptotic key-rate performance of the mode-pairing scheme. The horizontal axis representing the total communication distance with a fibre loss of 0.2 dB/km and the vertical axis representing the key generation rate. **a** Main Panel: Performance comparison of the mode-pairing scheme (denoted by MP-QKD in the plot) with the decoy-state Bennett-Brassard 1984 (BB84)[1,13,40], MDI-QKD[16], PM-QKD[25,46], SNS-TFQKD[27,47] schemes and the repeaterless rate-transmittance bound (PLOB bound)[5]. Inset: The simulation parameters used in the key-rate plot, which are mainly from ref. [32]. **b** Main Panel: The rate-distance dependence of the mode-pairing scheme with different maximal-pairing intervals *l*. Inset: The key rate with respect to the pairing interval *l* for a communication distance of 400 km.

$r_p = O(\sqrt{\eta})$; when $pl \ll 1$, it scales with p^2, resulting in $r_p = O(\eta)$. Around $pl = 1$, there will be a performance transition from $r_p = O(\sqrt{\eta})$ to $r_p = O(\eta)$.

In practice, l can be adjusted in accordance with the laser quality and quantum-channel fluctuations. Note that l can also be adjusted during data postprocessing, offering flexibility for various environmental changes in real time. Generally, the whole pairing strategy can be adjusted through different realisations.

Practical issues and simulation. The key rate of the mode-pairing scheme, as rigorously analysed in the Supplementary Note 2, has a decoy-state MDI-QKD form:

$$R = r_p r_s \left\{ q_{(1,1)} \left[1 - H(e^X_{(1,1)}) \right] - f H(E^{(\mu,\mu),Z}) \right\}, \qquad (7)$$

where r_p is the pairing rate contributed by each block, r_s is the proportion of Z-pairs among all the generated location pairs (~1/8), $q_{(1,1)}$ is the fraction of Z-pairs caused by single-photon-pair states $\rho^{(1,1)}$ in which both Alice and Bob send single-photon states in the two paired modes, $e^X_{(1,1)}$ is the phase error rate of the detection caused by $\rho^{(1,1)}$, f is the error-correction efficiency, and $E^{(\mu,\mu),Z}$ is the bit error rate of the sifted raw data. The fraction $q_{(1,1)}$ and the phase error $e^X_{(1,1)}$ can be estimated using the decoy-state method[40,43,44]. A detailed estimation procedure for $q_{(1,1)}$ and $e^X_{(1,1)}$ with the vacuum + weak decoy-state method is introduced in Supplementary Note 3.

During the key mapping step in Box 1, the X-pair sifting condition $\theta^a = \theta^b$ is impossible to fulfil exactly. This results in insufficient data for X-basis error rate estimation. To solve this problem, one can apply discrete phase randomisation[45] such that θ^a and θ^b are chosen from a discrete set. We expect the discretisation effect to be negligible when the number of discrete phases is reasonably large, such as $D = 16$, similar to the situation in previous works on one-mode MDI-QKD[46].

Based on the above analysis, we simulate the asymptotic performance of the mode-pairing scheme under a typical symmetric quantum-channel model, using practical experimental parameter settings. We assign the maximal pairing interval l of the mode-pairing scheme as a value between 1 and 1×10^6, aiming to illustrate the dependence of the key rate on l. We also compare the key rate of the mode-pairing scheme with those of a typical two-mode scheme, time-bin encoding MDI-QKD[23], and two one-mode schemes — PM-QKD[46] and SNS-TFQKD[47]. The simulation results are shown in Fig. 3. We set the misalignment error rate of the mode-pairing scheme to be the same as the one-mode schemes for a fair comparison. In Supplementary Note 5, we show that the key-rate performance of the mode-pairing scheme is robust against misalignment errors. Even with a misalignment error rate of 15%, the mode-pairing scheme is able to surpass the repeaterless rate-transmittance bound with $l = 2000$. Here, we compare the asymptotic key-rate performance of all the schemes under the scenario of one-way local-operation and classical communication. The simulation formulas for these schemes are listed in Supplementary Note 4. Recently, researches[48,49] show that the key-rate performance of SNS-TFQKD can be further improved by introducing the two-way classical communication[50,51]. We will leave the advanced key distillation for future studies.

As shown in Fig. 3a, the mode-pairing scheme with only neighbour pairing, $l = 1$, show a performance comparable to that of the original two-mode scheme. These two schemes have the same scaling property, i.e., $R = O(\eta)$. The deviation is caused by an extra sifting factor in the mode-pairing scheme as a result of independent encoding. When the maximal pairing interval l is increased to 1×10^3, the key rate is significantly enhanced by 3 orders of magnitude compared to the $l = 1$ case, making it able to surpass the linear key-rate bound. If we further increase l above 1×10^5, then the mode-pairing scheme has a similar key rate to PM-QKD and SNS-TFQKD and a scaling property given by $R = O(\sqrt{\eta})$. In Fig. 3b, we further compare the key-rate performance of the mode-pairing scheme under different settings for l. When l falls within the range of 1 to 1×10^6, the key rate of the mode-pairing scheme lies between the two extreme cases of $O(\eta)$ and $O(\sqrt{\eta})$. The key-rate behaviour is dominated by the pairing rate given in Eq. (4).

In typical optical experiments, the typical line width of a common commercial laser is 3 kHz (see for example, ref. [32]). Hence, the coherence time of the laser is around 333 μs. In practice, the

Table 1 Comparison of the phase encoding and postprocessing procedures of the mode-pairing scheme presented in the main text and the modified scheme considered in the security proof.

	Modulated phase	*X*-basis postprocessing	Sifting condition
Original scheme	$A_1:\phi_1^a, A_2:\phi_2^a$	$\theta^a=(\phi_2^a-\phi_1^a)\mathrm{mod}\pi, \kappa^a=\lfloor\frac{1}{\pi}(\phi_2^a-\phi_1^a)\mathrm{mod}2\rfloor$	$\theta^a=\theta^b$
Modified scheme	$A_1:\phi_1^a+z_1''\pi, A_2:\phi_2^a+z_2''\pi$	$\theta^a=\phi_2^a-\phi_1^a, \kappa^a=z_1''\oplus z_2''$	$\theta^a-\theta^b=0$ or π

In the modified scheme, Alice introduces an extra π-phase modulation for the storage of a bit z_1''. This helps to decouple the phase randomisation and phase encoding analysis.

frequency fluctuation of the lasers will affect the stabilization of the phase. To test the feasibility of the mode-pairing scheme, we perform an interference experiment using a commercial optical communication system with a repetition rate of 625 MHz. The experiment detail is shown in Supplementary Note 6. Based on the experimental data, we find that the phase coherence can be maintained well in a time interval of 5 μs, corresponding to $l=3000\sim4000$. If we apply the state-of-the-art optical communication system with the repetition rate of 4 GHz[37], we can realize a pairing interval over $l=20000$. As an extra remark, our current discussion on the implementation of the mode-pairing scheme is based on the multiplexing of optical time-bin modes. Nonetheless, the proposed mode-pairing design is generic for the multiplexing of other optical degrees of freedom. For example, we can introduce frequency multiplexing. The optical modes with different frequencies are first prepared and interfered independently, i.e., only the pulses with the same frequency will be interfered. After the announcement of detection results, Alice and Bob then pair the locations with different frequencies during the post-processing. This can be used to increase the effective maximal pairing interval to an even larger value without the global phase locking. From Fig. 3b we can see that the key rate of the mode-pairing scheme with $l=1\times10^4$ remains $R\sim O(\sqrt{\eta})$ when η is smaller than 30 dB, corresponding to a communication distance of 300 km. The asymptotic key rate of the mode-pairing scheme is 3 to 5 orders of magnitude higher than that of the two-mode scheme. We remark that the decoherence effect caused by the optical-fibre channel is negligible compared to the laser coherence time. When the fibre length is around 500 km, the velocity of phase drift in the fibre is <10 rad/ms[32], which can be calibrated using strong laser pulses without the need for real-time feedback control. As a result, the value of l depends only upon the local phase reference and not the communication distance.

One advantage of the mode-pairing scheme is that it can be adapted to specific hardware conditions. In practice, optical systems may be unstable, causing the local phase reference to fluctuate rapidly. In this case, we can reduce the maximal pairing interval l and search for the optimal pairing strategy during the postprocessing procedure. As shown in the inset plot of Fig. 3b, the key rate of the mode-pairing scheme first increases linearly with increasing l before saturating when l is larger than $p^{-1}=(\mu\sqrt{\eta})^{-1}$. In this case, Alice and Bob find successful detection within l locations with a high probability. Even when the optical system is unstable, the key rate can be nearly l times higher than that of the original time-bin MDI-QKD scheme when the value of l does not exceed $p^{-1}=(\mu\sqrt{\eta})^{-1}$. We remark that, with the original experimental apparatus used in time-bin MDI-QKD, one can directly enhance the key rate by a factor of ~100 using the mode-pairing scheme. On the other hand, we note that for a given communication distance, l does not need to be very large to reach the maximal key-rate performance. For example, when the distance reaches 200 km, a maximal pairing interval of $l=1000$ is sufficient to achieve the optimal key-rate performance. We leave a detailed evaluation for future research.

Discussion

Based on a re-examination of the conventional two-mode MDI-QKD schemes and the recently proposed one-mode MDI-QKD schemes, we have developed a mode-pairing MDI-QKD scheme that retains the advantages of both, namely, achieving a high key rate with easy implementation. Since MDI-QKD schemes have the highest practical security level among the currently feasible QKD schemes, we expect the mode-pairing scheme paves the way for an optimal design for QKD, simultaneously enjoying high practicality, implementation security, and performance.

There remain several interesting directions for future work. Natural follow-up questions lie in the statistical analysis of the mode-pairing scheme in the finite-data-size regime and efficient parameter estimation. Due to the photon-number-based property of the mode-pairing scheme, previous studies of the statistical analysis of two-mode MDI-QKD schemes[52–54] can be readily extended to analyse the mode-pairing scheme. To improve the efficiency of data usage, Alice and Bob may perform parameter estimation before basis sifting in order to use all signals that were originally discarded. On the other hand, one could design a mode-pairing scheme using the *X*-basis for key generation and the *Z*-basis for parameter estimation.

In this work, we employ a simple mode-pairing strategy based on pairing adjacent detection pulses. A more sophisticated pairing method might make bit and basis sifting more efficient. To improve the pairing strategy, Alice and Bob could reveal parts of the encoded intensity and phase information. For example, in the simple pairing strategy introduced in Box 2, Alice and Bob reveal the bases of the generated data pairs immediately after locations i and j are paired. If their basis choices differ, Alice and Bob 'unpair' locations i and j, and seek the next good pairing location for location i until the basis choices match.

To further enhance the performance, we could extend the mode-pairing design to other optical degrees of freedom, such as angular momentum and spectrum mode. Meanwhile, we could multiplex the usage of different degrees of freedom to enhance the repetition rate and extend the pairing interval l. Such multiplexing techniques would have additional benefits for the mode-pairing scheme. Suppose that we multiplex m quantum channels for a QKD task. In a normal setting, the key generation speed would be improved by a factor of m. For the mode-pairing scheme, in addition to this m-fold improvement, multiplexing would also introduce a larger pairing interval ml, since Alice and Bob would be able to pair quantum signals from different channels. A larger pairing interval ml would result in more paired signals and, hence, more key bits. Especially in the high-channel-loss regime where the distance between two clicked signals is large, the number of successful pairs becomes proportional to the maximum pairing interval ml. Thus, the key generation rate is proportional to m^2 in the high-channel-loss regime.

Meanwhile, entanglement-based MDI-QKD schemes are essentially based on entanglement-swapping, which is the core design feature of quantum repeaters. The mode-pairing technique may help design a robust quantum repeater against a lossy channel. Note that our work shares similarities with the memory-assisted MDI-QKD protocol[55] with quantum memories in the middle and with

the all-photonic intercity MDI-QKD protocol[56] with adaptive Bell-state measurement on the postselected photons. It is interesting to discuss the possibility of combining the mode-pairing design with an adaptive Bell-state measurement to tolerate more losses.

Moreover, the mode-pairing scheme has a unique feature in that the key bits are determined not in the encoding or measurement steps but upon postprocessing, which is an approach that can be further explored in other quantum communication tasks, including continuous-variable schemes.

Methods

Source replacement of the encoding state. The main idea of the security proof for the mode-pairing scheme is to introduce an entanglement-based scheme and reduce the security of the scheme to that of a traditional two-mode MDI-QKD scheme. To realise this, we perform a systematic source-replacement procedure[57,58]. Without loss of generality, in this subsection, we always assume the paired locations (i, j) to be $(1, 2)$ to simplify the notations.

For convenience in the security proof, we slightly modify the scheme described in Box 1. First, we assume that the random phase of each mode is discretely chosen from a set of D phases, evenly distributed in $[0, 2\pi)$. We expect the corresponding correction term in the security analysis due to the discretisation effect to be negligible[45,46]. Second, in the security proof, we modify the phase encoding and postprocessing procedures, as shown in Table 1. In the original scheme, Alice modulates A_1 and A_2 based on two random phases ϕ_1^a and ϕ_2^a, respectively. During the X-basis processing, she calculates the relative phase difference $\phi_\delta^a := \phi_2^a - \phi_1^a$ and splits it into an alignment angle θ^a in the range of $[0, \pi)$ and a raw key bit κ^a. We modify these procedures as follows: in addition to the two random phases ϕ_1^a and ϕ_2^a, Alice also generates two bits z_1'' and z_2'' and applies extra phase modulations of $z_1''\pi$ and $z_2''\pi$ to A_1 and A_2, respectively. During the X-basis processing, she calculates the relative phase difference $\phi_\delta^a := \phi_2^a - \phi_1^a$ and directly announces it for alignment-angle sifting. In the Supplementary Information, we prove the equivalence of these two encoding methods.

With the modification above, Alice further generates a random bit z_1' and a random dit $(d = D)$ j_1 in the first round. Based on the values of z_1', z_1'' and j_1^a, she prepares the state

$$\left|\psi^{Com}\right\rangle = \left|\sqrt{z_1'\mu}e^{i(\pi z_1'' + \phi_1^a)}\right\rangle, \tag{8}$$

with $\phi_1 = j_1 \frac{2\pi}{D}$. As shown in Fig. 4, we substitute the encoding of random encoded information into the introduction of extra ancillary qubit and qudit systems labelled as $\tilde{A}_1$, A_1'' and A_1'. The purified encoding state is

$$\left|\tilde{\Psi}^{Com}\right\rangle_{\tilde{A}_1,A_1',A_1'',A_1} = \frac{1}{2\sqrt{D}}\sum_{j_1=0}^{D-1}\left|j_1\right\rangle_{\tilde{A}_1}\left(|00\rangle|0\rangle + |01\rangle|0\rangle + |10\rangle\left|\sqrt{\mu}e^{i\phi_1^a}\right\rangle + |11\rangle\left|\sqrt{\mu}e^{i(\phi_1^a+\pi)}\right\rangle\right)_{A_1',A_1'':A_1}. \tag{9}$$

In Fig. 4, we provide a specific state preparation procedure. The initial state is

$$\begin{aligned}\left|+_D\right\rangle &:= \frac{1}{\sqrt{D}}\sum_{j=0}^{D-1}\left|j\right\rangle,\\ \left|+\right\rangle &:= \left|+_2\right\rangle.\end{aligned} \tag{10}$$

Here Alice applies a controlled-phase gate $C_D - \hat{U}(\phi_\Delta)$ with $\phi_\Delta := \frac{2\pi}{D}$ from the qudit $\tilde{A}_1$ to optical mode A_1. The controlled-phase gate is defined as

$$C_D - \hat{U}(\phi)_{\tilde{A}A} := \sum_{j=0}^{D-1}\left|j\right\rangle_{\tilde{A}}\left\langle j\right| \otimes e^{i\phi j a^\dagger a}, \tag{11}$$

where $a^\dagger$ and a are the creation and annihilation operators, respectively, of mode A_1. Alice also applies a controlled-phase gate $C - \hat{U}(\pi)$ from A_1'' to A_1.

In the entanglement-based mode-pairing scheme, Alice and Bob generate the composite encoding state $\left|\tilde{\Psi}^{Com}\right\rangle$ defined in Eq. (9) in each round. They emit the optical modes to Charlie for interference. Based on Charlie's announcement, they pair the locations and perform global operations on the corresponding ancillaries to generate raw key bits and useful parameters. In Fig. 5, we list the global operations performed on Alice's paired locations. Among them, the relative encoded intensity $\tau^a := z_1' \oplus z_2'$ is used to determine the basis choice. The encoded intensity $\lambda^a := z_1'$ and the relative encoded phase $\sigma^a = z_1'' \oplus z_2''$ are the raw key bits in the Z-basis and X-basis postprocessing, respectively.

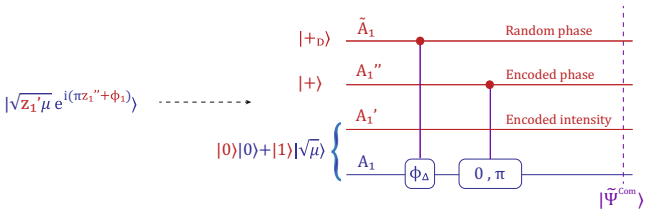

Fig. 4 Source-replacement procedure for the mode-pairing scheme. We substitute the encoding of all random encoded information into the introduction of purified ancillary systems.

A key point in our security proof is that we replace the random phases and register them into purified systems $\tilde{A}_1$ and $\tilde{A}_2$. This enables us to define a global measurement $M(k, \theta)$ on $\tilde{A}_1$ and $\tilde{A}_2$ to simultaneously obtain the overall photon number and the relative phase information encoded in optical modes A_1 and A_2. The construction of $M(k, \theta)$ is described in Supplementary Note 1. With the introduction of the purified systems $\tilde{A}_1$ and $\tilde{A}_2$ and the existence of the global measurement $M(k, \theta)$, Alice (same for Bob) is able to determine at which two locations to perform the global photon number measurement after Charlie's announcement. With this measurement, Alice and Bob can further reduce the encoding state to a two-mode scheme. The detailed security proof is provided in Supplementary Note 2.

Mode-pairing scheme with decoy states. Here, we present the mode-pairing scheme with an extra decoy intensity ν to estimate the parameters q_{11} and e_{11}^X. Of course, more decoy intensities can be applied in a similar manner.

1. **State preparation**: In the i-th round $(i = 1, 2, \ldots, N)$, Alice prepares a coherent state $\left|\sqrt{\mu_i^a}\exp(i\phi_i^a)\right\rangle$ in optical mode A_i with an intensity μ_i^a randomly chosen from $\{0, \nu, \mu\}$ $(0 < \nu < \mu < 1)$ and a phase ϕ_i^a uniformly chosen from the set $\{\frac{2\pi}{D}k\}_{k=0}^{D-1}$. She records μ_i^a and ϕ_i^a for later use. Likewise, Bob chooses μ_i^b and ϕ_i^b randomly and prepares $\left|\sqrt{\mu_i^b}\exp(i\phi_i^b)\right\rangle$ in mode B_i.
2. **Measurement**: (Same as Step 2 in Box 1.) Alice and Bob send modes A_i and B_i to Charlie, who performs the single-photon interference measurement. Charlie announces the clicks of the detectors L and/or R. Alice and Bob repeat the above two steps N times; then, they perform the following data postprocessing procedures:
3. **Mode pairing**: (Same as Step 3 in Box 1.) For all rounds with successful detection (L or R clicks), Alice and Bob establish a strategy for grouping two clicked rounds as a pair. A specific pairing strategy is introduced in Box 2.
4. **Basis sifting**: Based on the intensities of two grouped rounds, Alice labels the 'basis' of the data pair as:
   (a) Z if one of the intensities is 0 and the other is nonzero;
   (b) X if both of the intensities are the same and nonzero; or
   (c) '0' if the intensities are (0, 0), which will be reserved for decoy estimation of both the Z and X bases; or
   (d) 'discard' when both intensities are nonzero and not equal.

   See also Table 2 for the basis assignment. Alice and Bob announce the basis (X, Z, '0', or 'discard') and the sum of the intensities $(\mu_{i,j}^a, \mu_{i,j}^b)$ for each location pair i, j. If the announced bases are the same and no 'discard' state occurs, they record the pair basis and maintain the data pairs; if one of the announced bases is '0' and the other one is $X(Z)$, they record the pair basis as $X(Z)$ and keep the data pairs; if both of the announced bases are '0', they record the pair basis as '0' and maintain the data pairs; and otherwise, they discard the data. See also Table 3 for the basis-sifting strategy.
5. **Key mapping**: (Same as Step 5 in Box 1) For each Z-pair at locations i and j, Alice sets her key to $\kappa^a = 0$ if the intensity of the i-th pulse is $\mu_i^a = 0$ and to $\kappa^a = 1$ if $\mu_i^a = 0$. For each X-pair at locations i and j, the key is extracted from the relative phase $(\phi_j^a - \phi_i^a) = \theta^a + \pi\kappa^a$, where the raw key bit is $\kappa^a = \left\lfloor((\phi_j^a - \phi_i^a)/\pi \bmod 2)\right\rfloor$ and the alignment angle is $\theta^a := (\phi_j^a - \phi_i^a) \bmod \pi$. Similarly, Bob also assigns his raw key bit κ^b and determines θ^b. For the X-pairs, Alice and Bob announce the alignment angles θ^a and θ^b. If $\theta^a = \theta^b$, they keep the data pairs; otherwise, they discard them.
6. **Parameter estimation**: Alice and Bob estimate the quantum bit error rate $E_{\mu\mu}^Z$ of the raw key data in Z-pairs with overall intensities of $(\mu_{i,j}^a, \mu_{i,j}^b) = (\mu, \mu)$. They use Z-pairs with different intensity settings to estimate the clicked single-photon fraction q_{11} using the decoy-state method, and the X-pairs are used to estimate the single-photon phase error rate e_{11}^X. Specially, q_{11} and e_{11}^X are estimated via the decoy-state method introduced in Supplementary Note 3.
7. **Key distillation**: (Same as Step 7 in Box 1.) Alice and Bob use the Z-pairs to generate a key. They perform error correction and privacy amplification in accordance with q_{11}, $E_{\mu\mu}^Z$ and e_{11}^X.

Mode-pairing-efficiency calculation. We calculate the expected pairing number $r_p(p, l)$ that corresponds to the simple mode-pairing strategy in Box 2, which is related to the average click probability p during each round, and the maximal pairing interval l.

For calculation convenience, we assume that in addition to the front and rear locations (F_k, R_k) of the k-th pair, Alice and Bob also record the starting location S_k,

System	Size	Measurement	Outcomes	Usage	
$\tilde{A}_1$	Qudit $(d = D)$	Overall photon number and relative phase measurement $M(k,\theta)$	Overall photon number k^a	Post-select the rounds with $k^a = 1$: basis-independent source	
$\tilde{A}_2$	Qudit $(d = D)$		Relative phase θ^a	Z-basis: no use	
				X-basis: alignment angle for sifting	
A_1''	Qubit	CNOT gate from A_2'' to A_1'' followed by $Z \otimes Z$ measurement	Relative encoded phase $\sigma^a = z_1'' \oplus z_2''$	Z-basis: no use	
				X-basis: raw key	
A_2''	Qubit		Encoded phase on A_2: $\zeta^a = z_2''$	Z-basis: no use	
				X-basis: no use	
A_1'	Qubit	CNOT gate from A_1' to A_2' followed by $Z \otimes Z$ measurement	Encoded intensity on A_1: $\lambda^a = z_1'$	Z-basis: raw key	
				X-basis: parameter estimation	
A_2'	Qubit		Relative encoded intensity $\tau^a = z_1' \oplus z_2'$	Basis assignment:	$\tau^a = 1$: Z-basis $\tau^a = 0$: X-basis
A_1	Optical mode	Emitted to Charlie for interference			
A_2	Optical mode				

Fig. 5 The quantum operations and usage of Alice's encoding states on two paired locations (1, 2). There are 8 systems based on Alice's two paired locations. Among them, the two qudits $\tilde{A}_1$ and $\tilde{A}_2$ are measured to obtain the overall photon number k^a and the relative phase θ^a of two optical modes A_1 and A_2. The two qubits A_1'' and A_2'' are measured to obtain the relative phase, which is the raw key bit in the X-basis. Another two qubits A_1' and A_2' are measured to obtain the encoded intensity in A_1 and the relative encoded intensity, which are used for the key mapping on the Z-basis and the basis assignment, respectively.

Table 2 Alice's (or Bob's) basis assignment on the paired locations *i* and *j*.

μ_j \ μ_i	0	ν	μ
0	'0'	Z	Z
ν	Z	X	'discard'
μ	Z	'discard'	X

Based on the intensities μ_i and μ_j on the i-th and j-th location, Alice (or Bob) assign the basis to be either X, Z, '0', or 'discard'.

Table 3 Alice and Bob's basis sifting procedure on the paired locations *i* and *j*.

Bob \ Alice	'0'	X	Z
'0'	'0'	X	Z
X	X	X	'discard'
Z	Z	'discard'	Z (key generation)

Based on the assigned basis, Alice and Bob decide whether to keep the data for Z-basis key generation, $Z(X)$-basis parameter estimation, or discard the data.

which indicates the location at which the first successful detection signal occurs during the pairing procedure for the k-th pair. If the second successful detection signal R_k is found within the next l locations, then $F_k = S_k$; otherwise, F_k will be larger than S_k. Let $G_k := S_{k+1} - S_k$ denote a random variable that reflects the location gap between the k-th and $(k+1)$-th starting pulses. Then the expected pairing number per pulse is given by

$$r_p = \frac{1}{\mathbb{E}(G_k)}. \tag{12}$$

Hence, we need to calculate only the expectation value of G_k. First, we split it into two parts,

$$G_k = (R_k - S_k) + (S_{k+1} - R_k) = H_k + G_k^{(b)}, \tag{13}$$

where $H_k := R_k - S_k$ and $G_k^{(b)} := S_{k+1} - R_k$. Hence,

$$\mathbb{E}(G_k) = \mathbb{E}(H_k) + \mathbb{E}(G_k^{(b)}). \tag{14}$$

It is easy to show that $G_k^{(b)}$ obeys a geometric distribution,

$$\Pr(G_k^{(b)} = d) = (1-p)^{d-1}p, \quad d = 1, 2, \ldots \tag{15}$$

Then, the expectation value is $\mathbb{E}(G_k^{(b)}) = 1/p$.

The calculation of the pulse interval H_k is more complex. Suppose that we already know the expectation value $\mathbb{E}(H_k)$; now we calculate the expectation value $\mathbb{E}(H_k|d)$ conditioned on the distance between the starting point and the following click. We have

$$\mathbb{E}(H_k|d) = \begin{cases} d, & d \le l, \\ \mathbb{E}(H_k) + d, & d > l. \end{cases} \tag{16}$$

Therefore,

$$\begin{aligned} \mathbb{E}(H_k) &= \sum_{d=1}^{+\infty} \Pr(d)\mathbb{E}(H_k|d) \\ &= \sum_{d=1}^{l} (1-p)^{d-1}pd + \sum_{d>l} (1-p)^{d-1}p[\mathbb{E}(H_k) + d] \\ &= \sum_{d=1}^{+\infty} (1-p)^{d-1}pd + \mathbb{E}(H_k)\sum_{d>l} (1-p)^{d-1}p \\ &= \frac{1}{p} + \mathbb{E}(H_k)(1-p)^l \end{aligned} \tag{17}$$

We have

$$\mathbb{E}(H_k) = \frac{1}{p[1-(1-p)^l]}; \tag{18}$$

therefore,

$$\begin{aligned} \mathbb{E}(G_k) &= \frac{1}{p[1-(1-p)^l]} + \frac{1}{p}, \\ \Rightarrow r_p &= \left[\frac{1}{p[1-(1-p)^l]} + \frac{1}{p}\right]^{-1}. \end{aligned} \tag{19}$$

Note added to proof. After we submitted our work for reviewing, we became aware of a relevant work by Xie et al.[59], who consider a similar MDI-QKD protocol that match the clicked data to generate key information. Under the assumption that

the single-photon distributions in all the Charlie's successful detection events are independent and identically distributed, the authors simulate the performance of the protocol and show its ability to break the repeaterless rate-transmittance bound.

Data availability

The methods to generate the data in the plots are provided in Supplementary Information. The data that support the plots within this paper and other findings of this study are available from the corresponding authors upon reasonable request.

Code availability

The detailed simulation methods for the plots are provided in Supplementary Information. The specific code that support the plots within this paper and other findings of this study are available from the corresponding authors upon reasonable request.

Received: 18 November 2021; Accepted: 9 June 2022;
Published online: 07 July 2022

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*. pp. 175–179 (IEEE Press, New York, 1984).
2. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
3. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214 (2021).
4. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
5. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
6. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. "Event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287 (1993).
7. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932 (1998).
8. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6**, 6787 (2015).
9. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
10. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999).
11. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
12. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *N. J. Phys.* **11**, 045018 (2009).
13. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Info. Comput.* **4**, 325 (2004).
14. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74**, 022313 (2006).
15. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7**, 73 (2007).
16. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
17. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
18. Liu, Y. et al. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
19. Ferreira da Silva, T. et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
20. Woodward, R. I. et al. Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers. *npj Quantum Inf.* **7**, 1 (2021).
21. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).
22. Tamaki, K., Lo, H.-K., Fung, C.-H. F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).
23. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
24. Lucamarini, M., Yuan, Z., Dynes, J. & Shields, A. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
25. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
26. Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018).
27. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
28. Ferenczi, A. Security proof methods for quantum key distribution protocols, Ph.D. thesis http://hdl.handle.net/10012/7468 (2013).
29. Duan, L.-M., Lukin, M., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413 (2001).
30. Minder, M. et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **13**, 334 (2019).
31. Wang, S. et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
32. Fang, X.-T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **14**, 422–425 (2020).
33. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
34. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
35. Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photonics* **15**, 530–535 (2021).
36. Clivati, C. et al. Coherent phase transfer for real-world twin-field quantum key distribution. *Nat. Commun.* **13**, 1 (2022).
37. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
38. Tang, Z. et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
39. Tang, Y.-L. et al. Field test of measurement-device-independent quantum key distribution. *IEEE J. Sel. Top. Quantum Electron.* **21**, 116 (2014).
40. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
41. Inoue, K., Waks, E. & Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **68**, 022317 (2003).
42. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475 (2014).
43. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
44. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
45. Cao, Z., Zhang, Z., Lo, H.-K. & Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *N. J. Phys.* **17**, 053014 (2015).
46. Zeng, P., Wu, W. & Ma, X. Symmetry-protected privacy: Beating the rate-distance linear bound over a noisy channel. *Phys. Rev. Appl.* **13**, 064013 (2020).
47. Jiang, C., Yu, Z.-W., Hu, X.-L. & Wang, X.-B. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Phys. Rev. Appl.* **12**, 024061 (2019).
48. Xu, H., Yu, Z.-W., Jiang, C., Hu, X.-L. & Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. *Phys. Rev. A* **101**, 042330 (2020).
49. Jiang, C., Hu, X.-L., Yu, Z.-W. & Wang, X.-B. Composable security for practical quantum key distribution with two way classical communication. *N. J. Phys.* **23**, 063038 (2021).
50. Gottesman, D. & Lo, H.-K. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457 (2003).
51. Chau, H. F. Practical scheme to share a secret key through a quantum channel with a 27.6 bit error rate. *Phys. Rev. A* **66**, 060302 (2002).
52. Ma, X., Fung, C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).
53. Curty, M. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).
54. 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).
55. Panayi, C., Razavi, M., Ma, X. & Lütkenhaus, N. Memory-assisted measurement-device-independent quantum key distribution. *N. J. Phys.* **16**, 043005 (2014).

56. Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. *Nat. Commun.* **6**, 1 (2015).
57. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
58. Ferenczi, A. & Lütkenhaus, N. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A* **85**, 052310 (2012).
59. Xie, Y.-M. et al. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **3**, 020315 (2022).

Acknowledgements

We especially thank Norbert Lütkenhaus for the helpful discussions on the security analysis, thorough proofreading, and beneficial suggestions on the manuscript presentation. We thank Yizhi Huang, Guoding Liu, Zhenhuan Liu, Tian Ye, Junjie Chen, Minbo Gao, and Xingjian Zhang for the helpful discussion on the pairing rate calculation and general comments on the presentation. We especially thank Hao-Tao Zhu and Teng-Yun Chen for providing us with some preliminary results showing the phase stabilization after removing phase-locking in the mode-pairing scheme. This work was supported by the National Natural Science Foundation of China Grants No. 11875173 and No. 12174216 and the National Key Research and Development Program of China Grants No. 2019QY0702 and No. 2017YFA0303903.

Author contributions

X.M. conceived the research. P.Z., H.Z. and X.M. designed the protocol. X.M., P.Z., W.W. and H.Z. finished the security analysis. P.Z. and W.W. performed the protocol analysis and numerical simulation. All authors contributed extensively to the preparation of this manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-022-31534-7.

Correspondence and requests for materials should be addressed to Xiongfeng Ma.

Peer review information *Nature Communications* thanks the anonymous reviewer(s) for their contribution to the peer review of this work.

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.