Editors' Suggestion   Featured in Physics

Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking

Lai Zhou,[1] Jinping Lin,[1] Yuan-Mei Xie,[2] Yu-Shuo Lu,[2] Yumang Jing,[1]
Hua-Lei Yin,[2,1,*] and Zhiliang Yuan[1,†]

[1]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2]*National Laboratory of Solid State Microstructures and School of Physics,*
Collaborative Innovation Center of Advanced Microstructures, Nanjing University,
Nanjing 210093, China

(Received 28 November 2022; accepted 21 March 2023; published 20 June 2023)

Secure key rate (SKR) of point-point quantum key distribution (QKD) is fundamentally bounded by the rate-loss limit. Recent breakthrough of twin-field (TF) QKD can overcome this limit and enables long distance quantum communication, but its implementation necessitates complex global phase tracking and requires strong phase references that not only add to noise but also reduce the duty cycle for quantum transmission. Here, we resolve these shortcomings, and importantly achieve even higher SKRs than TF-QKD, via implementing an innovative but simpler measurement-device-independent QKD that realizes repeaterlike communication through asynchronous coincidence pairing. Over 413 and 508 km optical fibers, we achieve finite-size SKRs of 590.61 and 42.64 bit/s, which are respectively 1.80 and 4.08 times of their corresponding absolute rate limits. Significantly, the SKR at 306 km exceeds 5 kbit/s and meets the bitrate requirement for live one-time-pad encryption of voice communication. Our work will bring forward economical and efficient intercity quantum-secure networks.

DOI: 10.1103/PhysRevLett.130.250801

Introduction.—Quantum key distribution (QKD) [1,2] has been theoretically proven secure [3,4] to allow remote parties to share secret keys by the laws of physics. Its prospect for real-world use has motivated rapid experimental development over past forty years in terms of secure key rates (SKRs) [5], transmission distance [6,7], and network deployment [8–11]. However, realistic devices may have imperfections that could be exploited by an eavesdropper (Eve) [4], and among which detectors are conceivably the most vulnerable [12]. Fortunately, concerns about detectors have led to proposals [13,14] of using an intermediate measurement node to close all measurement-device-related security loopholes. Additionally, the measurement node can naturally be shared by many users to form a star-type network [15], thus reducing the resource requirement for expensive detectors.

On top of its security and topological advantages, measurement-device-independent (MDI) QKD [14] offers substantially improved signal-to-noise ratio and hence much longer communication distances as compared to conventional QKD. This is because placing the measurement node right in the middle of a communication line effectively halves the photon transmission loss, as illustrated in Fig. 1(a). However, the loss reduction cannot immediately translate to higher SKR as original MDI-QKD has to extract its raw key bits from two-photon coincidences. Using time-bin MDI-QKD as an example [Fig. 1(b)], strictly synchronous pairing leads to the probability of successful coincidence K to be proportional to the total channel transmittance η, $P(K) \propto \eta$. Consequently, the SKR of MDI-QKD remains governed by the fundamental

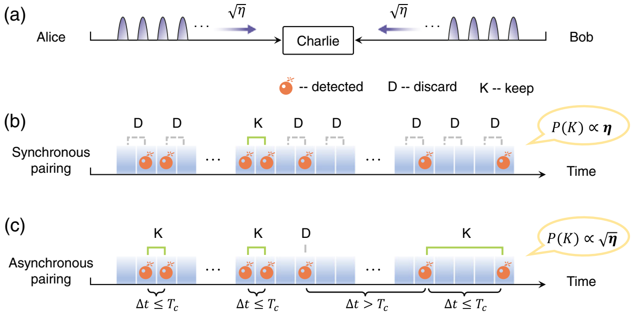

FIG. 1. Schematics for MDI-QKD protocols. (a) Generic MDI-QKD; Alice and Bob each sends a train of encoded weak coherent pulses to the intermediate node, Charlie. The transmittance of the entire quantum channel is denoted as η, so each user's segment has $\sqrt{\eta}$ transmittance. (b) Synchronous coincidence pairing; in original time-bin MDI-QKD, Alice and Bob apply pairwise global phase randomization. A valid coincidence occurs when both time bins registered a photon click. All single clicks are discarded. Its coincidence probability is proportional to η, i.e., $P(K) \propto \eta$. (c) Asynchronous coincidence pairing; in asynchronous MDI-QKD, Alice and Bob apply independent phase slice randomization individually for each pulse. This allows innovative, postmeasurement pairing of photon clicks with temporal separation within T_c. We have $P(K) \propto \sqrt{\eta}$ in the high count rate limit.

repeaterless limit [16–19]. A rigorous theorem [18] expresses this limit as $R = -\log_2(1-\eta)$ [18], which is known as the absolute repeaterless key capacity or SKC_0 for a point-to-point link.

We note that in MDI-QKD the users' lasers are independent from each other and bear no mutual phase relationship. Adding the ability to track the mutual phase can convert an MDI setup to a twin-field (TF) QKD implementation [20], in which single-photon events are used for distillation of quantum keys and thus its SKR becomes repeaterlike and proportional to the square root of the channel loss ($\sqrt{\eta}$). With the help of refined protocol variants [21–27], TF-QKD has been repeatedly demonstrated to overcome the SKC_0 over long fibers [28–33] and a remarkable record of 833 km for fiber transmission has been achieved [32]. However, the requirement for phase tracking has brought undesirable complexities to its implementations [28–33], all requiring service fibers to synchronize the users' lasers with one exception [33] that uses optical frequency combs instead. Moreover, it must transmit strong reference signals through the quantum channel, which reduces the effective clock frequency for quantum transmission and increases the background noise.

Recently, a new variant [34,35] of MDI-QKD has been proposed to overcome SKC_0 using postmeasurement coincidence pairing. As shown in Fig. 1(c), asynchronous MDI-QKD [34] (also called mode-pairing MDI-QKD [35]) allows any two-photon clicks to form a legitimate coincidence provided that their time separation (Δt) is shorter than a critical interval (T_c), within which the users' signals maintain mutually highly coherent. The relaxation in pairing rules drastically increases the coincidence probability to $P(K) \propto \sqrt{\eta}$ in the high count rate limit, when at least two clicks on average within T_c. Compared to TF-QKD, asynchronous MDI-QKD offers similar repeaterlike rate-loss scaling but has the advantage of not requiring global phase tracking.

In this Letter, we demonstrate the first asynchronous MDI-QKD that overcome SKC_0 without resorting to global phase tracking. We implement a 3-intensity protocol enhanced by a novel click filtering to provide security against coherent attacks in the finite-size regime. With fiber drift as the dominant decoherence source, our MDI-QKD system allows stable asynchronous two-photon interference over large time intervals of up to 200 μs. We obtain SKRs of 590.61 and 42.64 bit/s over fiber channels of 413.73 and 508.16 km, respectively.

Protocol.—Our asynchronous protocol has crucial operational differences from conventional time-bin MDI-QKD. Each quantum pulse requires separate phase-slice randomization, which enables asynchronous coincidence pairing after photon detection and thus the $\sqrt{\eta}$ rate scaling. Over the initial proposal [34], we have further improved the pairing strategy to intensity independence and thus gain immunity against coherent attacks, similarly to Ref. [35] but with an additional filtering operation for protocol efficiency.

We define a successful photon click as the event when one and only one detector clicked in a time bin. Specifically, we use $(k_a|k_b)$ to denote a successful click for which Alice and Bob sent their respective pulse intensities of k_a and k_b. Define $[k_a^{\text{tot}}, k_b^{\text{tot}}]$ as an asynchronous coincidence where the combined intensity in the two time bins Alice (Bob) sent is k_a^{tot} (k_b^{tot}). Let $\mu_{a(b)}$, $\nu_{a(b)}$, and $o_{a(b)}$, respectively, represent Alice's (Bob's) signal, decoy, and vacuum intensities, where $\mu_{a(b)} > \nu_{a(b)} > o_{a(b)} = 0$.

Assuming authenticated public message channels, execution of the asynchronous MDI-QKD protocol follows six steps, summarized below.

Step 1 (signal preparation and detection): For each time bin $i = 1, 2, \ldots, N$, Alice randomly prepares a weak coherent pulse $|e^{\mathrm{i}\theta_a}\sqrt{k_a}\rangle$ with intensity k_a and probability p_{k_a}. Thereinto, random phase $\theta_a = 2\pi M_a/M$ with $M_a \in \{0, 1, \ldots, M-1\}$ and random intensity $k_a \in \{\mu_a, \nu_a, o_a\}$. Likewise, Bob does the same. Alice and Bob send their optical pulses to Charlie via insecure quantum channels. Charlie performs the interference measurement and records successful clicks. For each, he broadcasts its time stamp and the corresponding detector (D_L or D_R) that clicked.

Step 2 (click filtering): For each event, Alice (Bob) announces whether she (he) applied the decoy intensity ν_a (ν_b) to the pulse sent. A simple filter is applied to discard clicks $(\mu_a|\nu_b)$ and $(\nu_a|\mu_b)$. All other clicks are kept.

Step 3 (coincidence pairing): For all kept clicks, Alice and Bob always pair a click with its immediate next neighbor within a time interval T_c to form a successful coincidence (see postmatching algorithm in the Supplemental Material [36]). A lone click is discarded if it failed to find a partner within T_c. For each coincidence, Alice (Bob) computes the total intensity k_a^{tot} (k_b^{tot}) she (he) used between the two time bins.

Step 4 (sifting): For each coincidence, Alice and Bob publish their computational result, k_a^{tot} or k_b^{tot}, and the phase differences they applied between the early (e) and late (l) time bins, $\varphi_{a(b)} = \theta^l_{a(b)} - \theta^e_{a(b)}$. They discard the data if $k_a^{\text{tot}} \geq \mu_a + \nu_a$ or $k_b^{\text{tot}} \geq \mu_b + \nu_b$. For $[\mu_a, \mu_b]$ coincidence, Alice (Bob) extracts a $\boldsymbol{Z}$-basis bit 0 if she (he) sends $\mu_{a(b)}$ in the early (late) time bin and $o_{a(b)}$ in the late (early) bin. Otherwise, an opposite bit is extracted. For $[2\nu_a, 2\nu_b]$ coincidence, Alice and Bob calculate the relative phase difference $\varphi_{ab} = (\varphi_a - \varphi_b) \bmod 2\pi$. If $\varphi_{ab} = 0$ or π, Alice and Bob extract an $\boldsymbol{X}$-basis bit 0. However, Bob will flip his bit value if $\varphi_{ab} = 0$ and both detectors clicked or $\varphi_{ab} = \pi$ and the same detector clicked twice. The coincidence with other phase differences is discarded. Additionally, they group their data to different sets $\mathcal{S}_{[k_a^{\text{tot}}, k_b^{\text{tot}}]}$ and count the corresponding number $n_{[k_a^{\text{tot}}, k_b^{\text{tot}}]}$.

Step 5 (parameter estimation and postprocessing): Alice and Bob use $n_{[\mu_a,\mu_b]}$ random bits from $\mathcal{S}_{[\mu_a,\mu_b]}$ to form the raw key $\mathcal{Z}$ and $\mathcal{Z}'$, respectively. The parameters s_{11}^z and ϕ_{11}^z are the number of bits and phase error rate in $\mathcal{Z}$ where both Alice and Bob sent a single-photon state. s_0^z is the number of bits in $\mathcal{Z}$ where Alice sent a vacuum state. By applying error correction and privacy amplification with security bound $\varepsilon_{\mathrm{sec}}$, the secret key rate R against coherent attacks in the finite-key regime can be written as

$$R = \frac{F}{N}\Bigg\{\underline{s}_0^z + \underline{s}_{11}^z[1 - H_2(\bar{\phi}_{11}^z)] - \lambda_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\Bigg\}, \qquad (1)$$

where F is the system clock frequency, $\underline{x}$ and $\bar{x}$ are the lower and upper bounds of the observed value x, respectively, λ_{EC} is the information revealed by Alice in the error correction step, and $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. $\varepsilon_{\mathrm{cor}}$, $\varepsilon_{\mathrm{PA}}$, ε', and $\hat{\varepsilon}$ are security coefficients regarding the secrecy and correctness.

We remark that filtering out clicks $(\mu_a|\nu_b)$ and $(\nu_a|\mu_b)$ is to increase the number of $[\mu_a,\mu_b]$ coincidence, which enables a higher SKR within 600 km fiber distance. We note that only $[\mu_a,\mu_b]$ coincidence is used for extracting secret key in the present filtering method since all decoy pulses are disclosed.

Setup.—Our experimental setup (Fig. 2) consists of three main modules: the senders Alice and Bob and the measurement node Charlie. Each sender contains a continuous-wave laser with a central wavelength of 1550.12 nm and featuring a short-term linewidth of 1 Hz. Their wavelengths are independently stabilized onto a transmission mode of their own high-fineness cavities using Pound-Drever-Hall technique. An electro-optical modulator (EOM) is present in the Pound-Drever-Hall locking path so as to shift the laser frequency with respect to the cavity mode. This allows control of the lasers' mutual frequency offset by finely adjusting the rf driving frequency to the electro-optical modulator.

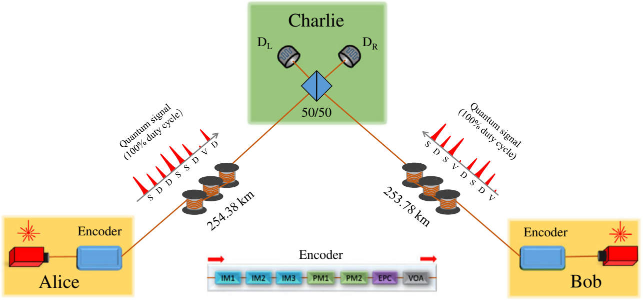

FIG. 2. Experiment setup. Alice and Bob generate encoded weak coherent pulses with their independent ultrastable lasers without mutual phase tracking. The encoder box contains three intensity and two phase modulators: IM, intensity modulator; PM, phase modulator; EPC, electrically driven polarization controller; VOA, variable optical attenuator; S, signal intensity; D, decoy intensity; V, vacuum intensity.

Passing through the encoder box, the laser signal is first carved into a train of 300 ps pulses at 1 ns intervals, followed by further intensity and phase encoding according to the requirements by the asynchronous MDI-QKD protocol. The encoded pulses are attenuated to the single-photon level before entering their respective quantum link. The quantum channel is formed by ultra-low-loss fiber spools (G654.C ULL) with a typical loss coefficient ranging from 0.158 to 0.162 dB km^{-1}.

After precompensating the polarization drift, the quantum signals from Alice and Bob travel through the corresponding link segment and arrive with identical polarization at Charlie's 50∶50 beam splitter for interference. The interference outcomes are detected by two superconducting nanowire single-photon detectors (D_L and D_R) having respective detection efficiencies of 78.1% and 77.0%, dark count rates of 10.1 and 12.7 Hz, and a time jitter of about 40 ps. Detection events are recorded by a time tagger with 300 ps gate width, and subsequently postprocessed to extract MDI-QKD protocol parameters. Between the senders and Charlie, we use electrical signals for clock synchronization, which can be upgraded to optical synchronization as routinely used in QKD field trials [9–11].

As compared with TF-QKD implementations [31–33,50], our MDI-QKD setup is substantially simpler as it does not require optical frequency dissemination, global phase tracking, and strong phase reference signals. With quantum transmission at 100% duty cycle, the asynchronous MDI-QKD can therefore surpass the SKR performance of TF-QKD systems [31,33] operating at the same clock frequency.

Experimental results.—It is crucial to have high visibility interference between the users' lasers, as the visibility is the key parameter for foiling Eve's attacks that break coherence among pulses. Theoretically, the first-order interference between two independent lasers can reach a temporal visibility (V_1) of 1 and the corresponding second-order coincidence interference has a maximum dip visibility (V_2) of 0.5. Here, we verify our experimental setup by transmitting the pulse-carved signals over short fibers and variable optical attenuators (VOAs) and obtain the respective visibilities of $V_1 = 0.989$ and $V_2 = 0.484$. Nevertheless, the measured V_2 is sufficient to give an $\boldsymbol{X}$-basis quantum bit error rate (QBER) (E_x) of 0.26, which has a theoretical minimum of 0.25.

We then verify the effect by the lasers' mutual frequency offset (Δf) and the fiber length fluctuation on the $\boldsymbol{X}$-basis QBER. We run several asynchronous MDI-QKD experiments over the quantum channel of 201.86 km fibers while setting different offsets of < 0.01, 1, 2, and 5 kHz. Here, signal modulation is performed exactly as the protocol

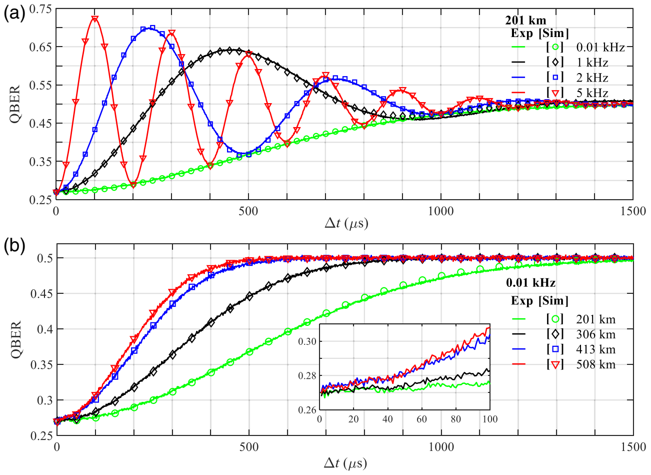

FIG. 3. Characterization of the asynchronous two-photon interference. (a) Evolution of the ***X***-basis QBER for different laser frequency offsets for a fixed fiber distance of 201.86 km. (b) ***X***-basis QBER as a function of time interval for different fiber distances, ranging from 201.86 to 508.16 km. Inset: magnified view for the region between 0 and 100 μs.

prescribes, including the 16-slices phase randomization. We collect 5 s data for each Δf. For convenience, we extract the ***X***-basis QBER from $[2\mu_a, 2\mu_b]$ coincidences, i.e., among click events when both Alice and Bob transmitted a signal state (μ_a or μ_b). A correct coincidence corresponds to either Alice and Bob used identical phase difference ($\varphi_{ab} = 0$) for the two time bins and the same detector clicked twice or $\varphi_{ab} = \pi$ and each detector clicked once. The experimental result is plotted in Fig. 3(a). With a negligible offset of 0.01 kHz, the fiber fluctuation dominates the dephasing between two coincident time bins, leading to a monotonous increase of ***X*** QBER to 0.5 when the time separation reaches 1.5 μs. In the presence of a larger frequency offset, ***X*** QBER exhibits oscillations at the corresponding offset frequency with a damping amplitude. The minima are bounded by the green curve ($\Delta f < 10$ Hz). The oscillation is due to the mutual phase evolution of the two lasers.

The effect by fiber fluctuation and frequency offset on the asynchronous two-photon interference can be theoretically derived as (see the Supplemental Material [36])

$$E_x = \frac{1 - V_2}{2} + \frac{V_2}{2}[1 - e^{-\sigma^2 \Delta t^2/2} \cos(2\pi \Delta f \Delta t)], \quad (2)$$

where σ is the standard deviation of the fiber drift rate. This equation can near perfectly reproduce the experimental results, as shown in Fig. 3(a). Here, we set $V_2 = 0.46$ taking into account further deterioration by phase randomization error and use an empirical value of 2100 rad s^{-1} for fiber phase drift [20]. No other fitting parameters are used.

Hundreds of kilometers of fiber can contribute a phase drift rate of several kHz, and this will limit the longest interval within which two clicks can be paired with an acceptable error ratio. At $\Delta f < 10$ Hz, it is possible to achieve ***X*** QBER of less than 0.30 over a coincidence interval of 200 μs, as shown in Fig. 3(a). To evaluate for longer distances, we keep the Δf below 10 Hz and then measure ***X***-basis QBER over different fiber lengths. As shown in Fig. 3(b), the ***X*** QBER deteriorates faster for longer fibers. At the maximum length of 508 km, the ***X*** QBER reaches 0.30 at the time interval of 85 μs; see Fig. 3(b), inset. However, the actual average interval is much smaller and we can therefore expect lower ***X*** QBER because our scheme pairs just adjacent photon clicks. As demonstrated later, we are able to use a large T_c of 200 μs for 508 km while still obtaining an acceptable ***X*** QBER of 0.293. We perform the theoretical simulation using Eq. (2) and find excellent agreement with experiments; see Fig. 3(b). In the simulation, we use empirical drift rates of 2100, 3400, 5300, and 5900 rad s^{-1} for 201, 306, 413, to 508 km of fibers, respectively. The used drift rates are in good agreement with previous experimental observations [20,33].

Finally, we run the asynchronous MDI-QKD protocol over for four fiber distances. We globally optimize the parameters μ, ν, p_μ, p_ν in the respective ranges [0.3, 0.5], [0, 0.1], [0.1, 0.4], and [0.1, 0.4] for a maximal secure key rate. To ensure high visibility interference, we compensate for polarization and temporal drift of the photon arrivals at Charlie's 50:50 beam splitter. To mitigate finite-size effects, we increase the number of sent pulses from 4.30×10^{12} to 7.24×10^{13} when the fiber length increases from 201.86 to 508.16 km. The average pairing intervals are 0.43 μs and 70.89 μs when setting the T_c as 5 μs and 200 μs for 201.86 and 508.16 km fibers. We measure ***X***-basis QBERs for coincidences $[2\nu_a, 2\nu_b]$ to be 0.269 and 0.293, respectively. The detailed encoding parameters and experimental results are summarized in the Supplemental Material [36].

Figure 4 presents our experimental results (red circle) in terms of SKR versus fiber distance, together with the theoretical simulation (solid red line). We include also the absolute SKC_0 to prove the repeaterlike behavior for our system. Taking into account of finite-size effects, we obtain SKRs of 57.63 k, 5.18 k, 590.61, and 42.64 bit/s for 201.86, 306.31, 413.73, and 508.16 km, respectively. Remarkably, the SKRs at 413.73 and 508.16 km beat their respective linear bounds with considerable margins, being 1.80 and 4.08 times higher than SKC_0. This is the first time for a QKD system to beat SKC_0 without resorting to complex global phase tracking.

To further appreciate the progress made by our system and protocol, we compare our results with the state-of-the-art QKD systems. Our asynchronous system has absolute advantage over existing MDI-QKD systems [51,52] implementing synchronous coincidence pairing. Its repeaterlike rate scaling allows it to beat the QKD system [7] operating

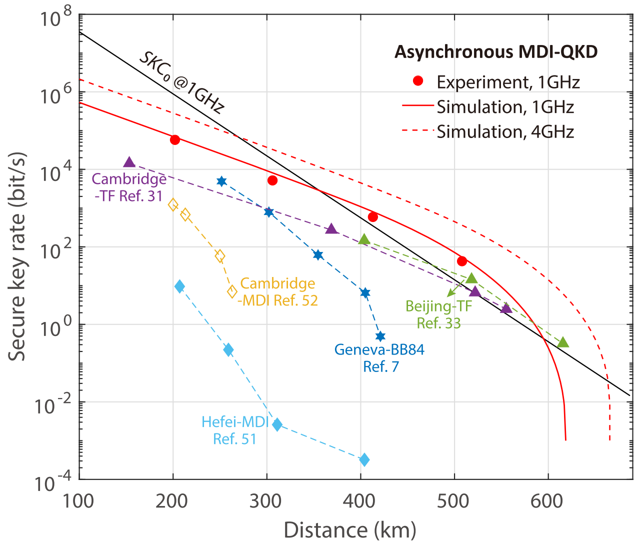

FIG. 4. Key rate simulations and results. Experimental data (solid red circles) and its simulation (solid red line) are plotted together with the absolute repeaterless bound, SKC_0. The red curve is the simulation result with the experimental parameters and a total of 7.24×10^{13} transmitted quantum pulses. Simulation for 4 GHz clock rate (red dashed line) is also shown. In the simulation, we set empirical drift rates of 5900 rad s^{-1}. Results of state-of-the-art QKD experiments [7,31,33,51,52] are included for comparison.

at a higher clock rate of 2.5 GHz. Strikingly, our system achieves higher performance even than TF-QKD systems [31,33] operating at the identical clock of 1 GHz over the distances between 200 and 500 km, despite that our system is substantially simpler and does not need global phase reconciliation. Over longer distances, our system performance is restricted by the loss of coincidence pairing efficiency due to both shortened T_c and less frequent photon clicks. This problem can be relieved partially by increasing the clock rate as simulated (dashed line, Fig. 4). Alternatively, we may use sideband stabilization technique [33] that can reduce the fiber drift rate by a factor of 1000 and thus substantially enlarges T_c to the order of 100 ms.

Discussion.—We have realized the first MDI-QKD experiment that breaks the SKC_0 bound, extending the maximal distance from 404 km to 508 km and improving the SKR over 400 km by more than 6 orders of magnitude. This success is attributed to the asynchronous pairing method and the optimization strategy through click filtering. The removal of phase tracking ensures an economical and efficient intercity quantum-secure network. In the future, we expect to improve the clock rate and also use less-demanding lasers for additional practicality enhancement. Increasing the system clock rate can proportionally shorten the pairing intervals, thereby further reducing the error rate and improving noise tolerance. We believe that the asynchronous MDI-QKD experiment design can be useful for applications such as quantum repeaters, entanglement swapping, and quantum internet.

This work was supported by the National Natural Science Foundation of China (62105034, 12274223, 62250710162), the Natural Science Foundation of Jiangsu Province (BK20211145), the Fundamental Research Funds for the Central Universities (020414380182), and the Key Research and Development Program of Nanjing Jiangbei New Area (ZDYD20210101).

L. Z., J. L., Y.-M. X., and Y.-S. L. contributed equally.

Note added.—We note that related experimental work has been reported in Ref. [53]. Both our work and Ref. [53] implement MDI-QKD with postmeasurement coincidence pairing. However, we realize the first MDI-QKD experiment that breaks the repeaterless bound and extends the maximal MDI-QKD distance from 404 to 508 km, while Ref. [53] achieved a maximal distance of 407 km but did not break the repeaterless bound.

[*]Corresponding author.
hlyin@nju.edu.cn
[†]Corresponding author.
yuanzl@baqis.ac.cn

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[2] A. K. Ekert, Quantum Cryptography based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[5] Z. Yuan *et al.*, 10-Mb/s quantum key distribution, J. Lightwave Technol. **36**, 3427 (2018).

[6] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).

[7] A. Boaron *et al.*, Secure Quantum Key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[8] M. Peev *et al.*, The SECOQC quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[9] M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[10] J. F. Dynes *et al.*, Cambridge quantum network, npj Quantum Inf. **5**, 101 (2019).

[11] Y.-A. Chen *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature (London) **589**, 214 (2021).

[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[13] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[14] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[15] Y.-L. Tang, H. L. Yin, Q. Zhao, H. Liu, X. X. Sun *et al.*, Measurement-Device-Independent Quantum Key Distribution Over Untrustful Metropolitan Network, Phys. Rev. X **6**, 011024 (2016).

[16] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and Reverse Secret-Key Capacities of a Quantum Channel, Phys. Rev. Lett. **102**, 050503 (2009).

[17] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[19] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal Limitations on Quantum Key Distribution Over a Network, Phys. Rev. X **11**, 041016 (2021).

[20] 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 (London) **557**, 400 (2018).

[21] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[22] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[23] H.-L. Yin and Y. Fu, Measurement-device-independent twin-field quantum key distribution, Sci. Rep. **9**, 3045 (2019).

[24] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).

[25] C. Cui, Z. Q. Yin, R. Wang, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Twin-Field Quantum Key Distribution Without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[26] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[27] K. Maeda, T. Sasaki, and M. Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, Nat. Commun. **10**, 3140 (2019).

[28] X.-T. Fang *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[29] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang *et al.*, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).

[30] C. Clivati *et al.*, Coherent phase transfer for real-world twin-field quantum key distribution, Nat. Commun. **13**, 157 (2022).

[31] 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).

[32] S. Wang *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[33] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).

[34] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).

[35] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).

[36] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.130.250801 for detailed security proof, finite-size analysis, experimental technologies, and experimental results, which includes Refs. [37–49].

[37] S. Bose and D. Home, Duality in Entanglement Enabling a Test of Quantum Indistinguishability Unaffected by Interactions, Phys. Rev. Lett. **110**, 140404 (2013).

[38] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[39] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[40] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[41] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[42] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[43] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, New J. Phys. **17**, 053014 (2015).

[44] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[45] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain Rules for Smooth Min- and Max-Entropies, IEEE Trans. Inf. Theory **59**, 2603 (2013).

[46] M. Curty, F. Xu, W. Cui, C. Ci Wen Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[47] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Tight security bounds for decoy-state quantum key distribution, Sci. Rep. **10**, 14312 (2020).

[48] Charles Ci Wen Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[49] W. Wang, F. Xu, and H.-K. Lo, Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks, Phys. Rev. X **9**, 041012 (2019).

[50] J.-P. Chen *et al.*, Quantum Key Distribution Over 658 km Fiber with Distributed Vibration Sensing, Phys. Rev. Lett. **128**, 180502 (2022).

[51] H.-L. Yin, T. Y. Chen, Z. W. Yu, H. Liu, L. X. You *et al.*, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[52] 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).

[53] H.-T. Zhu *et al.*, Experimental Mode-Pairing Measurement-Device-Independent Quantum Key Distribution Without Global Phase Locking, Phys. Rev. Lett. **130**, 030801 (2023).