Twin-Field Quantum Key Distribution without Phase Locking

Wei Li,1,2,* Likang Zhang,1,2* Yichen Lu,1,2* Zheng-Ping Li,1,2,3* Cong Jiang,4 Yang Liu,4 Jia Huang,5 Hao Li,5 Zhen Wang,5 Xiang-Bin Wang,3,4,6 Qiang Zhang,1,2,3,4 Lixing You,5,5 Feihu Xu,1,2,3,3* and Jian-Wei Pan1,2,3,§

1Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China
2Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China
3Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
4Jinan Institute of Quantum Technology, Jinan, Shandong 250101, China
5National Key Laboratory of Materials for Integrated Circuits, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050 China
6State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China

(Received 6 December 2022; revised 30 March 2023; accepted 22 May 2023; published 20 June 2023)

Twin-field quantum key distribution (TF-QKD) has emerged as a promising solution for practical quantum communication over long-haul fiber. However, previous demonstrations on TF-QKD require the phase locking technique to coherently control the twin light fields, inevitably complicating the system with extra fiber channels and peripheral hardware. Here, we propose and demonstrate an approach to recover the single-photon interference pattern and realize TF-QKD without phase locking. Our approach separates the communication time into reference frames and quantum frames, where the reference frames serve as a flexible scheme for establishing the global phase reference. To do so, we develop a tailored algorithm based on fast Fourier transform to efficiently track the phase reference via data postprocessing. We demonstrate no-phase-locking TF-QKD from short to long distances over standard optical fibers. At 50-km standard fiber, we produce a high secret key rate (SKR) of 1.27 Mbit/s, while at 504-km standard fiber, we obtain the repeaterlike key rate scaling with a SKR of 34 times higher than the repeaterless secret key capacity. Our work provides a scalable and practical solution to TF-QKD, thus representing an important step towards its wide applications.

DOI: 10.1103/PhysRevLett.130.250802

Introduction.—Quantum key distribution (QKD) can provide information-theoretically secure keys among distant parties [1] and it has become an indispensable cryptographic primitive in the upcoming quantum era [2,3]. Because of the loss of photons in their transmission, the point-to-point secret key capacity (SKC) of a channel without the quantum repeater scales linearly $O(\eta)$ with the channel transmission [4–6]. The twin-field (TF) QKD protocol [7], an efficient version of measurement-device-independent QKD [8], can greatly enhance the transmission distance by achieving a repeaterlike rate-loss scaling of $O(\sqrt{\eta})$ with current available technology. Consequently, TF-QKD has been studied extensively in theory [9–12] and experiment [13–22]. These efforts make the long-haul fiber network within reach. Moreover, its measurement-device-independent advantage can remove trusted nodes from the networks, thus granting a security boost over deployed quantum communication network [23–25].

In practice, however, TF-QKD is phase sensitive [7], which normally requires sufficiently long coherence time for two independent laser sources. In previous TF-QKD realizations, such a stringent requirement has been fulfilled by phase locking laser sources using the optical phase-lock loop [13,15,18,22], the time-frequency dissemination [14,19–21], or the injection locking [16] techniques. These approaches require extra servo channels to disseminate the reference light and peripheral hardware to perform the locking, which could potentially hinder the wide deployment of TF-QKD in network settings. Furthermore, the future quantum network may involve users with free-space link [26,27] or with integrated photonic chip [28–30]. However, the servo channel is hard to establish in the free-space link, and the phase-locking components are challenging to be integrated on chip.

In this Letter, we propose and demonstrate an approach to realize TF-QKD without phase locking. We alternate the communication period into quantum frame ($Q$ frame) and reference frame ($R$ frame), and use the $R$ frame to provide a phase reference for the $Q$ frame by reconciling the signals via data postprocessing. We develop an algorithm based on the fast Fourier transform (FFT) to efficiently track the frequency and the phase fluctuation. By doing so, we are able to recover the interference pattern with 259 photon detections in a duration of 7 $\mu$s, yielding an interference...
error rate (ER) of 2.32%, or an ER of 3.74% with 159 photon detections in a duration of 11 μs. Moreover, we derive an analytical model to study the sources of phase fluctuation and provide a guideline to optimize the experimental parameters in the aspect of the ratio of the Q frame to the R frame. To test our approach, we build a TF-QKD setup without any phase locking (or phase compensation) at the transmitters (or receiver), and demonstrate TF-QKD from 50- to 504-km of standard fiber channels. A secret key rate (SKR) of 2.05 bit/s is generated over 504-km standard fiber (96.8 dB loss or equivalent to 605-km ultralow loss fiber) in the finite-size regime, which is 34 times higher than SKC0. At 50-km standard fiber, we are able to produce 1.27 Mbit/s secret keys.

**No-phase-locking scheme.**—The phase difference of two light fields $\Phi(t)$ evolves as

$$\Phi(t) = 2\pi\nu_0 t + \phi_0 + \Delta\phi(t),$$

where $\nu_0$, $\phi_0$, and $\Delta\phi(t)$ denote the beat-note frequency, the initial phase, and the phase fluctuation, respectively. Both $\nu_0$ and $\phi_0$ are constant and can be estimated via the data postprocessing, whereas $\Delta\phi(t)$ includes the intrinsic phase noise of the laser sources and the fluctuation introduced in the channel transmission.

To perform the parameter estimation, we propose to supplement the quantum pulses (Q frame) with strong R frame. The R frame is used to reconcile the phase in the Q frame through postprocessing the photon detection events. As shown in Fig. 1, the detection probabilities of two detectors are correlated with the interference pattern. In light of this, we develop an FFT-based algorithm to reconstruct the frequency spectrum (see Supplemental Material, Sec. II [31]). From the frequency spectrum, we choose the component with the largest amplitude within a certain frequency range. Then, $\nu_0$ is the frequency of the component and $\phi_0$ can be obtained from the angle of the complex amplitude of the component. Here, to reduce the estimation error, we propose to extend the detection series with padding zeros. This can greatly narrow the distribution of the frequency estimation and decrease the frequency deviation, thus enhancing the frequency estimation precision (see Supplemental Material, Fig. 1). Moreover, we duplex the detection events to use them more efficiently, i.e., each R frame is used twice by the two neighbor Q frames. This doubles the available photon events and reduces the error rate when the photon count rate is low.

According to the estimated $\nu_0$ and $\phi_0$, the ER can be further evaluated. When single photon events arrival time $t$ satisfy (a) $\cos[\Phi(t)] \geq (2\pi/M)$ or (b) $\cos[\Phi(t)] \leq \cos[2\pi\nu_0 t + \phi_0]$ with condition (a) $[\text{(b)}]$ is satisfied and $D_0 (D_1)$ clicks, it is counted as a correct event. Otherwise, if condition (a) [$(b)$] is satisfied and $D_1 (D_0)$ clicks, it is counted as an error event.

The ER originates from the difference $\Phi(t) - \hat{\Phi}(t) = 2\pi(\nu_0 - \nu) t + (\phi_0 - \hat{\phi}_0) + \Delta\phi(t)$. The third term (mainly contributed by the phase noise of laser source and the fiber length fluctuation) is a random noise, its contribution can be analyzed in theory and characterized in experiment. To do so, we derive an analytical model to study the phase fluctuation and provide a guideline to optimize the experimental parameters (see Supplemental Material, Sec. I [31]). The phase fluctuation can be analyzed in time domain [7,14,16] or frequency domain [20]. Here, we use the frequency-domain power spectral density (PSD) to characterize the random noise. By doing so, we are able to calculate the fluctuation in variable interval $\tau$ and relate it to the ER. Furthermore, the phase noise of the laser sources is also taken into consideration in our model. This was often ignored in the previous analysis for the phase-locked TF-QKD schemes [7,14,16]. Nonetheless, as the linewidth of the laser source increases, it will dominate the phase fluctuation. Even for the phase-locked laser sources, their phase noise replicates the one of the reference source at best, which cannot be ignored. By including the phase fluctuations...
noise, our model can properly analyze the linewidth requirement for the laser sources for both phase-locking and no-phase-locking TF-QKD.

Setup.—To implement the no-phase-locking TF-QKD scheme, we build an experimental setup as shown in Fig. 2. Alice and Bob transmit their quantum light to Charlie’s measurement site via symmetric quantum channels, constituted by standard telecom fiber spools (G.652). No servo link is used for the dissemination of a third phase reference laser. Each user holds a commercial external cavity laser diode (RIO PLANEX) with a Lorentzian linewidth of 5 kHz and the wavelength is set at 1550.12 nm, but with a slight frequency mismatch of about 100 MHz. The frequency drifts slowly to an extent of 30 MHz over one day (see Supplemental Material, Sec. VI), which can be tracked by the frequency estimation algorithm.

The continuous light is encoded into two frames by three cascaded intensity modulators. Because of the fact that two lasers are heterodyned, no modulation in intensity and phase is required for the \( R \) frame to resolve the phase ambiguity as in Refs. [14,16]. The \( Q \) frame is used to generate quantum signals following the three-intensity sending-or-not-sending (SNS) TF-QKD protocol [35] (see Supplemental Material, Sec. VII for full descriptions [31]) with a clock rate of 1.25 GHz. Two cascaded phase modulators are used for 16-level random phase modulation covering \( 2\pi \) range. One intensity modulator creates the two frames and modulates the weak decoy intensity (if the intensity contrast is over the capability of one modulator, the weak decoy is modulated by another modulator instead, see Supplemental Material, Table III [31]), and the other two shape the pulses in \( Q \) frame and extinct vacuum pulses jointly. Such configuration allow us to apply bias control on the first intensity modulator to stabilize the signal and decoy intensities.

Light from Alice and Bob interfere at Charlie’s 50:50 beam splitter with the same polarization as the output of the polarization beamsplitter is polarization-maintaining. This transforms the polarization variation into intensity variation. We use two electrical polarization controllers to rotate the polarization at 5 Hz so as to keep the photon rates at the other port of the polarization beamsplitter constant (5% of total photon rate). Moreover, the photons detected by \( D_2 \) (\( D_3 \)) are accumulated to track the delay drift of the fiber every 5 s. The transition edge from the \( Q \) frame to the \( R \) frame is used as the time mark. These are sufficient to compensate the polarization and delay drift caused by the indoor fiber spools.

The interference output is detected by two superconducting nanowire single photon detectors (SNSPD). We use two types of SNSPDs, SNSPD No. 1 and No. 2, to perform the measurements (see Supplemental Material, Sec. VIII for the characterization [31]). The detected photon events are registered by a time tagging unit and then processed by a computer. The frequency \( \hat{\nu}_0 \) and initial phase \( \hat{\phi}_0 \) of the beat note can both be estimated by the FFT-based algorithm. The valid arriving time \( t \) in \( X \) basis should satisfy

\[
| \cos [2\pi \hat{\nu}_0 t + \hat{\phi}_0 + (\phi_a - \phi_b)] | \geq \cos (\pi/16),
\]

where \( \phi_a (\phi_b) \) is phase modulated by the users and announced publicly in the postprocessing. We also use the actively odd-parity pairing method [36,37] in the error rejection through two-way classical communication, significantly reducing the bit-flip error rate.

Results.—We first analyze the system performance with the no-phase-locking scheme quantitatively. The phase noise PSD of the laser has a \(-20 \text{ dB/decade}\) slope, contributed by the white frequency noise. The phase noise PSD introduced by the fiber spool is also measured...
(see Supplemental Material, Secs. III and IV [31]), which is mainly distributed below the frequency 100 kHz and increases slightly with the fiber length. With these two results, the phase fluctuation in the $Q$ frame can be calculated accordingly. The fluctuation is converted to the ER and averaged over the duration of the $Q$ frame. To characterize the ER with different $T_Q$ and $T_R$, we use the same setup as in Fig. 2, except that no modulation is applied. We plot measured ER as a function of $T_R$ from 0.1 $\mu$s to 50 $\mu$s at a fixed $T_Q$ of 1 $\mu$s with different count rates in Fig. 3(a). A higher count rate enables accurate frequency estimation at smaller $T_R$, thus lowering the minimum ER. The simulation result excluding the estimation error is also plotted, assuming that $\hat{\nu}_0 = \nu_0$ and $\hat{\nu}_0 = \nu_0 + \Delta \nu(t)$ (see Supplemental Material, Sec. I) [31]. Based on these results and the constraint of the experimental system, we choose $T_R$ and $T_Q$ to be 4.9152 and 1.6384 $\mu$s, respectively. The ER contributes to the quantum bit error rate of phase ($X$) basis in SNS-TF-QKD protocol. As another important implication of our theoretical model, we can determine the linewidth requirement for different selected $T_Q$ and plot the simulated results in Fig. 3(b). As an example, to achieve a maximum channel loss of 66 dB in our system, the laser linewidth should be narrower than 35.5 kHz when $T_Q = 1$ $\mu$s, resulting in an ER of 11%. With the performance analysis and parameter optimization, we perform TF-QKD experiments from 50- to 504-km standard fiber spools with different detectors and finite sizes (Supplemental Material, Sec. VIII [31]). The channel is symmetrical and the total channel loss amounts to 9.6, 38.4, 56.8, 72.1, and 96.8 $\text{dB}$, respectively. The results are presented in Fig. 4. With SNSPD No. 1, we measure the dynamic range to be 44 $\text{dB}$ when the count rate of the $R$ frame is 24 M count/s and the duty cycle (i.e., the ratio of $Q$ frame) is 1/4. That is to say the dynamic dark count rate [38,39] is about 1000 count/s, which is the dominant noise. To increase the signal-to-noise ratio, we apply a gating window of 200 ps, resulting in a dark count probability of $2 \times 10^{-7}$. With less than one hour of continuous run, we achieve a finite-size SKR of $1.25 \times 10^{-7}$ bit/pulse, or 39 bit/s at 380-km standard fiber. At the short end, we increase the duty cycle of the $Q$ frame to 3/4 to enhance the per-second key rate. And it enables a secret key rate of 1.27 Mbit/s at 50-km standard fiber channel with a small number of sending pulses of $10^{10}$. [6].
To generate positive key rates at a longer distance, we replace the detectors with SNSPD No. 2, which has a dynamic range over 58 dB. Furthermore, we keep the detected count rate in the $R$ frame as low as possible (8 M counts/s per detector) and use a narrower gating window of 100 ps. With these upgrades, the scattering noise in fiber becomes dominant and results in a noise probability of $1.6 \times 10^{-5}$. This is an order of magnitude of improvement over SNSPD No. 1, allowing us to achieve a SKR of $6.56 \times 10^{-9}$ bit/pulse or 2.05 bit/s at 504-km standard optical fiber.

Discussion.—In summary, we have proposed and demonstrated the no-phase-locking scheme for TF-QKD. Our scheme does not only remove the service channels for the dissemination of the reference light, but also does not need active phase compensation setup at the measurement site. Such features greatly simplify the setup to match the one of measurement-device-independent QKD systems [40,41], with the ability to establish global phase reference nonetheless. We also show that commercial kilohertz linewidth semiconductor lasers are sufficient to perform TF-QKD with our scheme. Despite the simplification of setup with our scheme, the phase-sensitive ER is 2.69% for a channel distance of 504 km (Supplemental Material, Table I [31]) which is comparable to the state-of-art TF-QKD experiment with phase locking [18,21,22]. To achieve further transmission distance with our scheme, one could increase the clock rate and develop a more advanced algorithm to lower the required counts in the recovery of the carrier, which helps to reduce the influence of scattering noise. Overall, we believe our scheme provides a practical solution to the TF-QKD network and the phase recovery algorithm is applicable to other phase-sensitive applications [42,43].

While preparing the manuscript, we notice two related works which demonstrate different approaches [44,45] to solve the phase-locking issue. Comparing to Ref. [44], the setup has similarities, but the protocols are different. Our work uses the twin-field protocol, but Ref. [44] employs the so-called mode-pairing protocol. The mode-pairing protocol is a postpairing approach by postselecting time slots within the coherence time of the laser source. The postpairing distance for time slots has to increase with the transmission loss, which leads to a large interference error due to the limited coherence time of the laser. As a result, our system endures higher transmission loss (96.8 dB) comparing to Ref. [44] (66 dB). This can be compensated using ultrastable lasers [45] which have a much longer coherence time, but adding more complexity and cost. In contrast, we demonstrate an efficient method to reconcile the phase reference in TF-QKD protocol. Our approach has no stringent requirements for the laser source, but it requires the estimation of full phase information which may need further software processing and sufficient photon counts.

This work was supported by National Natural Science Foundation of China (Grants No. 62031024, No. 12204467), Innovation Program for Quantum Science and Technology (2021ZD0300300), Anhui Initiative in Quantum Information Technologies, Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), Shanghai Science and Technology Development Funds (22JC1402900) and Shanghai Academic/Technology Research Leader (21XD1403800). Y. L. acknowledges support from the Taishan Scholar Program of Shandong Province. F. Xu acknowledges the support from the Tencent Foundation.


