


Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers

Yoann Pelet,^{*} Grégory Sauder[✉], Mathis Cohen, Laurent Labonté[✉], Olivier Alibart, Anthony Martin,[†] and Sébastien Tanzilli[‡]

Université Côte d'Azur, CNRS, Institut de Physique de Nice (INPHYNI), UMR 7010, Nice Cedex 2 06108, France

 (Received 17 October 2022; revised 13 March 2023; accepted 7 September 2023; published 3 October 2023)

We present a field-deployed quantum key distribution (QKD) link based on energy-time entanglement. Three nodes are connected, bridging the cities of Nice and Sophia Antipolis, by means of commercial grade optical fibers, spanning over a total distance of 50 km. We have built a packaged and resilient source of energy-time entangled photon pairs and implemented remote interferometer stabilization. Moreover, the clocks of the two end users are synchronized exploiting photon-counting techniques only, therefore requiring no dedicated channel. The system runs over the ITU 100-GHz standard telecom grid, through which a secure key rate of 7.0 kbit/s is extracted for one pair of channels. A homemade software performs all the necessary postprocessing procedures enabling to establish secret keys in real time. We present the first fully operational entanglement-based metropolitan QKD system being totally self-sufficient, i.e., requiring no additional overheads to be operated on a conventional metropolitan fiber network.

DOI: [10.1103/PhysRevApplied.20.044006](https://doi.org/10.1103/PhysRevApplied.20.044006)

I. INTRODUCTION

Quantum key distribution (QKD) offers the possibility of sharing unconditionally secure cryptographic keys between multiple distant users. Being one of the most mature quantum applications, protocols have improved and diversified to meet all the specific requirements of practical secret key distribution in terms of security, distance, and rate. QKD protocols, purely theoretical at first [1], were soon tested in the laboratory [2].

Over the last 10 years, QKD has been one of the most iconic quantum technologies finding its way out of laboratories. In this perspective, different but complementary research trends have emerged. A first direction aims at extending the covered distance as far as possible. To achieve such a goal with optical fibers, alternative protocols have been designed, such as twin field, allowing key sharing over hundreds of kilometers of optical fiber [3]. Another approach lies in the use of satellites to make space QKD [4]. A second direction focuses on demonstrating the highest rate possible. For such a scenario, the technological development of efficient sources [5] or high-rate single-photon detectors [6] is often required. A third direction explores advanced network topologies and associated required resources [7,8] to develop trusted user free quantum networks.

In this quest for ultrahigh performance, most of these demonstrations are still far from a fully operational solution. This would imply a global approach offering a self-sufficient solution for field-deployed QKD. Such an implementation would require fully automated stabilization of the link, time synchronization, as well as real-time treatment of the secret key. To go further, we have chosen to exploit only commercially available components and to build compact source and analyzers.

As described in Fig. 1, we present a fully operational QKD link over 50 km of deployed telecom fibers, with a total of 20.5 dB of transmission losses, exploiting energy-time entangled photon pairs distributed to two users (named Alice and Bob) across the Métropole Côte d'Azur. A fully automated stabilization protocol continuously maintains the mean value of the quantum bit error rate (QBER) at 4.7%. A complete post-treatment program produces a final key rate of 7 kbit/s for one pair of ITU channels among the 40 pairs that are available with our multiplexing strategy. There are three main features in our scheme. First, the users' clock synchronization, fundamental in QKD protocols, is carried out using the same qubits transmitted during the QKD protocol, without requiring any additional dedicated channel [9–11]. It allows, in real-time, the two distant clocks to be actively paced with a precision of 12 ps. Second, we exploit an asymmetric detection protocol, increasing by a factor 2 the raw key rate and requiring one less detector compared to similar implementations [12]. Third, we implement a homemade software performing on-the-fly post-treatment operations

^{*}yoann.pelet@univ-cotedazur.fr

[†]anthony.martin@univ-cotedazur.fr

[‡]sebastien.tanzilli@univ-cotedazur.fr

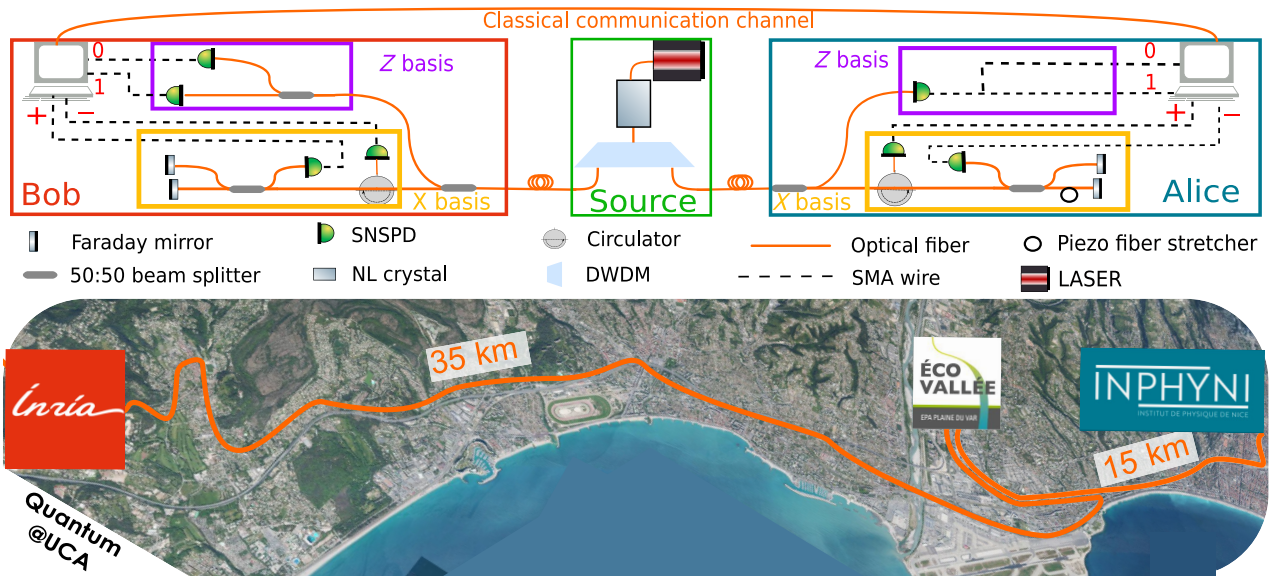


FIG. 1. Experimental setup. The source, located at the central station, creates energy time bipartite entanglement shared between Alice and Bob (end stations) using DWDM (ITU channels 20 and 22). Each analyzer (Alice and Bob) sends randomly the photons in either the Z or the X basis using a 50 : 50 beam splitter. The X basis is set up using two, stabilized Michelson interferometers with similar delays, one at Alice's station, the other at Bob's. The Z basis consists of a 50 : 50 beam splitter on Bob's side with a short and a long path to the detectors while Alice only has one detector with short and long paths created electronically afterward. Everything is fibered, with standard SMF-28 fibers for all components except for the connection between the pump laser and the PPLN waveguide ensured by a polarization-maintaining fiber.

required to transform the raw correlated bits into secured secret keys. With those features, our network generates continuously secret keys ready for practical exploitation of secured communication over 48 h.

II. CONCEPTUAL OPERATION

The *photon pairs* are generated via spontaneous parametric down-conversion (SPDC) by means of continuous laser light sent to a nonlinear crystal. Thanks to the conservation of energy and momentum between the three interacting fields, the emission time of each pair is unknown to the coherence length of the pump laser. The photon-pair distribution is poissonnian, guaranteeing true randomness of the emission time.

The *measurements* of the photons' states are performed randomly using two complementary basis, Z and X , with equal probabilities ($1/2$). Here, the random outcome sequence for basis X or Z is induced at the fundamental level by the beam splitter included in Alice's and Bob's station (see Fig. 1). The basis and time of arrival of the photons are recorded for each detection event. The Z basis is used to generate the key and corresponds to the measurement of the arrival time of the photons $\{|0\rangle, |1\rangle\}$. The X basis is used to estimate the eavesdropper's potential information by measuring two-photon interference between the two possible arrival times $\{|0\rangle, |1\rangle\}$, using the coherent superposition $|\pm\rangle = s|0\rangle \pm |1\rangle/\sqrt{2}$.

Time correlation and basis reconciliation occurs every 100 ms. Bob publicly announces his photons' detection times, measurement basis and, only for the X basis, output bits. In her data set, Alice searches the time and basis correlated events and sends back to Bob the event occurring in the Z basis. Alice and Bob can then filter their detection events to generate blocks of raw key containing n_Z events. Simultaneously, Alice records all coincidence events in the X basis to compute the phases error rates ϕ_x contributing to the QBER in the X basis: QBER_x .

The *error-correction* protocol is applied over blocks of n_Z^{EC} bits. We use a cascade algorithm to correct every error in the key, with a reconciliation efficiency of $f_{\text{EC}} = 1.06$ [13]. This correction requires that the two users communicate classically. Doing so, they disclose a certain number of bits to a potential eavesdropper (leakage). These leaked bits are no longer secure, which has to be taken into account during the next step of the protocol, that of privacy amplification. More specifically, the leakage (λ_{EC}) can be estimated with $\lambda_{\text{EC}} = f_{\text{EC}} \times n_Z^{\text{EC}} \times h(Q_z)$, where f_{EC} is the efficiency of reconciliation, $h(x)$ the binary entropy, and Q_z the error rate in the Z basis.

Privacy amplification (PA) stands as the last step toward generating a secure key. Based on the estimation of Eve's information, the PA generates an alternative, shorter, but more secure key from the output bits of the error correction. Eve's information is estimated using the leakage of the cascade algorithm and the calculation of the upper

bound of the phase error rate, taking into account the finite statistics of the keys. Here, k error-correction blocks are fused to create a PA block. On each PA block, Alice computes the lower bound over the length l of the secret key taking into account the finite-key effect, $l < n_z(1 - h(\phi_z^u)) - \lambda_{EC}$, with $n_z = kn_z^{EC}$ and ϕ_z^u the upper bound on the phase error rate estimated with the events in the Z basis. The extractor is based on a Toeplitz-hashing function extracting l bits from the n_z input bits [14]. The extractor is based on a Toeplitz-hashing function [14].

III. EXPERIMENTAL OPERATION

A. Source

The photon pairs are emitted via SPDC from a cw laser at 780.10 nm with 1-MHz linewidth (Toptica-DLpro) interacting with a $\chi^{(2)}$ nonlinear crystal. The latter is commercially available periodically poled lithium niobate ridge waveguide (PPLN) from NTT. The phase matching has been engineered so as to produce degenerate paired photons at 1560.20 nm over a spectral bandwidth of 80 nm as shown in Fig. 2. The crystal has a normalized brightness of 1.8×10^8 pairs/nm/mW with a coupling efficiency of 54.2% in a standard telecom single-mode fiber. For the two-user demonstration, we exploit one pair of commercial 100-GHz ITU channel dense wavelength demultiplexers (DWDMs) from AC-Photonics around the degeneracy, showing a side-channel isolation of approximately 30 dB. A quick calculation shows that less than 0.01% of optical noise from adjacent channels is to be expected within the coincidence window and can therefore be neglected. The channels at $\lambda = 1560.61$ and 1559.79 nm are sent to Alice and Bob, respectively.

More complex network topologies can be implemented by exploiting the broadband emission of the crystal. With the 100-GHz ITU channels, about 40 independent sources of energy-time entangled photon pairs can be operated in parallel. This allows the creation of either a 40-user fully connected network following the scaling demonstrated in Ref. [8], or an increase of the key rate proportionally [7].

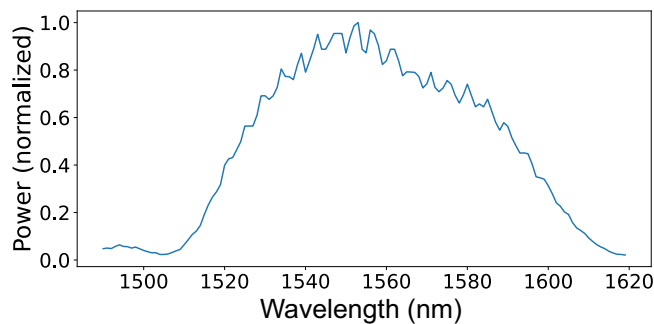


FIG. 2. Spectrum of the photon pairs generated from the nonlinear crystal inside of the photon-pair source.

These numbers can get even larger by using 50 GHz or 25-GHz DWDM, which can offer 80 or 160 pairs of channels instead of 40 by splitting the emission spectrum in a thinner way, while keeping a 30-dB side-channel isolation. As mentioned above, our implementation currently exploits 100-GHz DWDMs, for which no channel crosstalk is measurable, confirming the suitability of our approach for network applications.

B. Analyzers

Each analyzer allows for a passive basis choice between X and Z basis measurement (energy correlation or time-correlation measurements) thanks to a 50 : 50 fibered beam splitter, i.e., $P_Z = P_X = \frac{1}{2}$, as shown in Fig. 1.

The Z basis decodes the time correlations using a short and a long path separated by a time delay τ . As shown in Fig. 1, on Bob's side, this is done with a 50 : 50 beam splitter connected to detectors "0" and "1," each corresponding to a bit value of the raw key, with a delay τ added on the arm associated with "1." On Alice's side, we employ only one detector connected to two channels of the time-to-digital converter (TDC), with an electrical delay τ between the two. Similarly to Bob's side, the channel with a delay corresponds to the bit "1" while the other is referred to as "0." As such, every detection event on Alice's Z basis leads to the measurement of both $|0\rangle$ and $|1\rangle$. However, comparing both detection times with Bob's timestamps allows Alice to know whether Bob has measured $|0\rangle$ or $|1\rangle$ by post-selecting only the ones with a zero coincidence delay. To properly distinguish between $|0\rangle$ and $|1\rangle$, the delay τ must be larger than the timing jitter of the coincidence detection electronics. Usually, time-bin encoding is done using two different optical paths of different length [12] leading to the detection of $|0\rangle$ or $|1\rangle$. The choice between these two paths being passive, the probability that both photons take the same path and create an exploitable coincidence in the Z basis is of 50%. By making Alice able to measure both $|0\rangle$ and $|1\rangle$ for each photon, we bypass the passive choice between the two paths on Alice's side, improving to 100% the probability of recording a coincidence in the Z basis. This leads to an effective gain of 3 dB of losses, and allows using one detector instead of two for Alice's Z basis.

The X basis monitors energy correlation via the visibility of the two-photon interference in delocalized unbalanced fibered Michelson interferometers. Here, two-photon interference is made possible independently of the incoming polarization by using the polarization independent 50 : 50 beam splitter together with Faraday mirrors, thus avoiding the need for active polarization stabilization. For the X basis to be able to guarantee security of the link, the path-length difference between the two arms of each interferometer is set to τ , the same as the delay used in the Z basis. To maximize the two-photon interference visibility, the delay of the interferometers must satisfy the

following equations:

$$\begin{aligned} \tau_s^c &< \tau_{a,b} < \tau_p^c, \\ |\tau_a - \tau_b| &\ll \tau_s^c, \end{aligned} \quad (1)$$

where τ_a (τ_b) corresponds the delay between the arms of Alice's (Bob's) interferometer, and where τ_s^c and τ_p^c are the coherence times of the single photons and the photon pairs, respectively. In the continuous regime, the coherence of the pairs corresponds to the coherence of the pump laser (approximately equal to 1 μ s), while the coherence of the single photons (approximately equal to 10 ps) is given by the bandwidth of the ITU channel used, i.e., 100 GHz. To satisfy the first relation of Eq. (1), we chose an optical path-length difference of 46 cm for the interferometers, i.e., $\tau_{a,b} = 1.6$ ns. The second relation imposes to make the interferometers as identical as possible, i.e., within the coherence time of the single photons. To this end, we build two interferometers with similar delays, such as $|\tau_a - \tau_b| < 3$ fs, i.e., a fiber length difference shorter than 100 μ m. Experimentally, this delay is measured by sending low-coherence light in two cascaded interferometers, one being tunable, and the other being the interferometer under test. Scanning the delay of the tunable interferometer allows the maximum of the visibility of the interferences to be located, which enables the precise measurement of the delay of the QKD interferometer. Then, by repeating the measurement, a second identical interferometer can be built. Following this procedure, we build the interferometers, and measure a two-photon interference raw visibility of 99.7%. The two interferometers are set up at remote locations, separated by 50 km of optical fiber. Consequently, they need to be temperature stabilized to reduce relative phase fluctuations. An active temperature control paired with a insulated packaging allows the natural drift of the phase to be slowed down to 2π every 5 h for each interferometer. In addition, a piezo fiber stretcher is added on one arm of Alice's interferometer to follow Bob's natural drift and to lock the relative phase between Alice and Bob to an appropriate value. For such slow and short corrections in phase, the piezo stretching range is of 30 μ m only in order to minimize heating and other spurious effects.

All photons are detected with superconducting nanowire single-photon detectors (SNSPD) IDQuantique ID281 showing a dead time of approximately 50 ns and a detection efficiency of 80%. Timestamps are recorded with two time-to-digital converters (TDC—Swabian Instrument Timetagger Ultra) showing a 1-ps resolution. The combination of the detector and TDC jitters gives a coincidence peak with a FWHM of 80 ps.

The SNSPDs employed in our QKD system have a meander pattern, which introduces polarization-dependent efficiency [15]. In fibers, the polarization rotates over time, which creates instability of the secret key rate generated by the system. To overcome this issue, two electrical

adjustable polarization controllers are placed at the output of the source, and are constantly adjusted to maximize the number of detection events at Alice's and Bob's.

C. Quantum channel

The QKD protocol is operated over a dedicated optical fiber network deployed over the Métropole Côte d'Azur, provided by Orange. As shown in Fig. 1, the analyzers, Alice and Bob, are located, respectively, in Nice and in Sophia Antipolis, with the source placed in-between the two sites. More specifically, we exploit two commercial grade, telecom, single-mode dark fibers. The fibers induce 5.7 and 10.5 dB of losses from the source to Alice's or Bob's end station, respectively, estimated with an OTDR measurement. Chromatic dispersion along the fibers broadens the peaks in the coincidence histogram, leading to a decrease of the signal-to-noise ratio in the coincidence window [16]. This makes the use of a dispersion compensation module mandatory. Energy-correlated photon pair allows nonlocal dispersion cancelation, such that the effect of dispersion on one photon can be canceled out by the dispersion experienced by its correlated photon [17]. Therefore, a single 50-km fiber dispersion compensation module is only added before Alice's analyzer to compensate the dispersion accumulated by the photon pairs. We measure the losses of the dispersion compensation module to be of 4.3 dB and advantageously place it on the short fiber link so as to balance the losses between the source and the two users. Without such a loss balance, the signal would partially saturate Alice's detectors, lowering their efficiency and, consequently, lowering the keyrate.

As detailed in Table I, the analyzers add on average 11 dB of losses before each detector for both X bases, 6 dB for Bob's Z basis, and 3 dB for Alice's Z basis. The propagation losses between the source and the analyzers are expected figures when it comes to commercial optical dark fiber link (approximately 0.3 dB/km). At the analyzers, one should keep in mind that we use only off-the-shelf commercial components, which are not custom tuned for our purpose. Therefore, the losses are mostly due to the beam splitters for the Z basis. For the X basis, the interferometers stand as the primary source of losses, due to the splices and the required optical components: circulator, Faraday mirror, and beam splitter. It should be highlighted that any improvement of the losses would lead to easier stabilization of the QBERx leading to a higher keyrate.

TABLE I. Losses from the source to each detector, with A and B for Alice and Bob and X and Z for the measurement basis.

| Detector | AZ | $AX1$ | $AX2$ | $BZ1$ | $BZ2$ | $BX1$ | $BX2$ |
|-------------|------|-------|-------|-------|-------|-------|-------|
| Losses (dB) | 12.6 | 20.33 | 20.46 | 15.86 | 16.22 | 21.83 | 22.47 |

IV. DATA POST-TREATMENT

All data acquisition and post-treatment operations are automatically performed using a homemade LabView software, which performs, in real time, every calculation [18] and stabilization from the detection events to the generation of the secure key on Alice and Bob sides.

Our QKD protocol heavily relies on the precision of the recorded arrival times of the photons at Alice's and Bob's detectors. To measure those, two independent TDCs are used, one on each site. When a detection occurs, the TDC generates a 64-bit time tag corresponding to the elapsed time between the start of the device and the arrival time of the photon. The time-tagging precision relies on that of the clock used as a reference. When using two distant devices, two synchronization problems need to be addressed [19]: (i) defining a time zero, and (ii) maintaining the same clock rate on both systems.

Here, we address that issue without any classical resource overhead, and we explain in the following the operational procedure, only exploiting the time correlation of the emitted photon pairs. During the initialization of the QKD system, the laser beam is blocked by an electronically tunable optical attenuator. When unblocking the light, the SPDC source starts to generate pairs of photons that are subsequently separated and sent simultaneously to Alice and Bob. On each side, an algorithmic filtering function verifies, every millisecond, if the number of detections is largely greater than the dark-count rate of the detectors. When the detection rate becomes larger than a set threshold, the two TDCs send an acquisition block of data detection of 100 ms for all detectors. In such a block, the difference between the two first time tags recorded by Alice and Bob is used as the first estimation of the delay between correlated events. The time-tagger functions allow determination of this first delay with a precision of 10 ms. Alice performs a correlation calculation on one set of acquisition blocks around the delay given by the time tagger with the first time-tag event and looks for the coincidence peak within a 20-ms time window. The identification of this peak allows to define with a better accuracy the zero delay between the two TDCs with a precision of about 1 ns. Once done, the time window for the correlation can be reduced to 10 ns and, by using 4-ps long time bins, we improve the precision of the zero-delay measurement to 8 ps for the next blocks of raw keys.

While absolutely necessary, getting a precise initialization time does not guarantee an everlasting synchronization. Two independent clocks will drift apart over time. Our system requires at all times, a clock synchronization better than the coincidence window used to validate correlated detection events. The time taggers' internal clocks show a drift of 100 ns/s. When replaced by a rubidium atomic clocks (Spectratime LNRClock 1500), the drift lowers to 100 ps/s. Since the cumulative drift over one day

is largely greater than the coincidence window. 24/7 operation of the link requires active synchronization of Alice's and Bob's clocks. To do so, another coincidence calculation is performed every second. It allows measurement of the evolution of the zero delay by comparing the position of the measured peak to the previous one. Once the drift is measured, we pace the internal frequency of Alice's clock to remain synchronized to Bob's. This active correction ensures that the clocks' synchronization is always better than 12 ps.

Unlike standard methods [20], this kind of synchronization does not require any dedicated channel. The drift measurement is straightforwardly done by exploiting the natural time correlation of the entangled photons used to perform the QKD protocol and does not lower the keyrate. It also allows compliance with the optical length fluctuation of the quantum channel. All those perturbations normally affect the synchronization over long time scales but are here simply and constantly corrected. We choose a coincidence window in the post-treatment of 120 ps, which is the smallest size we can set before losing too much coincidence events due to detection timing jitter and residual clock drift.

For each acquisition block received from Bob, Alice performs the sifting to extract the time tags and basis of all the correlated events. Alice sends back to Bob the relevant events obtained in the Z basis to allow the generation of the key, while she keeps the events in the X basis to compute the QBER $_x$. The events in the Z basis are accumulated to generate a correction block of $n_Z^c = 16\,384$ bits, without disclosing the bit value. The block is then sent to the error-correction function based on a cascade algorithm [13]. After a run of the error-correcting code, we can extract the percentage of errors (mostly errors caused by multiple-pair statistical contributions) in our block, defining the the QBER $_z$.

On the other hand, the events in the X basis are fully disclosed. It allows computation of the fraction of correlated detection over the total number of coincidences in the X basis, defining the QBER $_x$. The error rate in the X basis is mostly due to multiple-pair contributions and is also impacted by the extra losses experienced by the photons and by imperfect stabilization of the interferometers. To minimize the impact of the stabilization errors, the QBER $_x$ is calculated for each correction block and the value is used as input of a feedback loop algorithm controlling the piezo stretcher. Setting the relative phase of the interferometers close to 0 minimizes the QBER $_x$.

Lastly, the corrected key is sent to a privacy amplification function based on a Toeplitz-hashing extractor to compute the final secret key on both sides. For this step, we have to take into account finite key effects, as described in Ref. [18]. By simulating the finite key effect on our raw keys, we find that accumulating 100 corrected blocks,

i.e., $n_z = 1.6384 \times 10^6$ detections, is the optimal trade-off between reducing the statistic uncertainty and keeping a block small enough to maintain the computing complexity of the privacy amplification as low as possible. All operations from data acquisition to privacy amplification are performed simultaneously between Alice's and Bob's computers, allowing the link to operate continuously without any downtime required for post-treatment.

V. RESULTS

The value of the secret key rate (SKR) results from a competition between the number of entangled photons detected and the error rate in the recorded detection events. Increasing the pump power results in a higher SKR. However, the higher the power, the higher the probability of generating more than one pair of photons within the same time window, which increases the QBER. To ensure unconditional security for the key-sharing process, all errors in the detection events have to be considered as a potential eavesdropper's actions. Therefore, to compensate for the Poissonian statistic of the pair-generation process induced errors, some bits of the raw key have to be sacrificed to create the secret key resulting in a decrease of the SKR. Therefore, the optimal SKR is found for the highest pump power before reaching a critical rate of multiple pairs. This optimal value depends on several parameters: the losses, the detectors' dark counts, the size of the coincidence window, and the imperfections in the source and in the analyzers. We have simulated the evolution of the SKR and QBERz as a function of the photon-pair generation probability per windows of interest (120 ps), as shown in Fig. 3. This simulation takes into account the statistic of the photons, the optical losses of the setup, the dark counts, the efficiency of the detectors, as well as all bits lost during the post-treatment with error correction and finite-key analysis, as described in Ref. [18]. By simulating our SKR for different pump powers, we find the optimal value for the QBER to be approximately 4.7% in the Z basis.

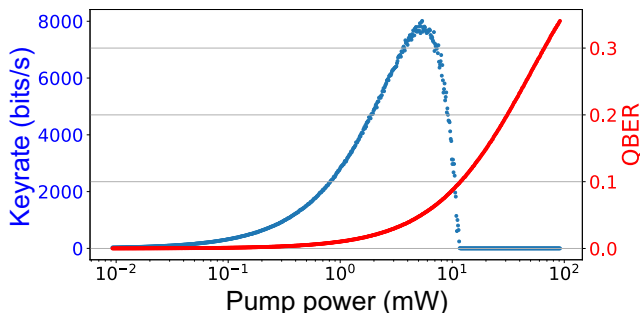


FIG. 3. Simulated SKR (blue) and QBERz (red) as a function of the pump power.

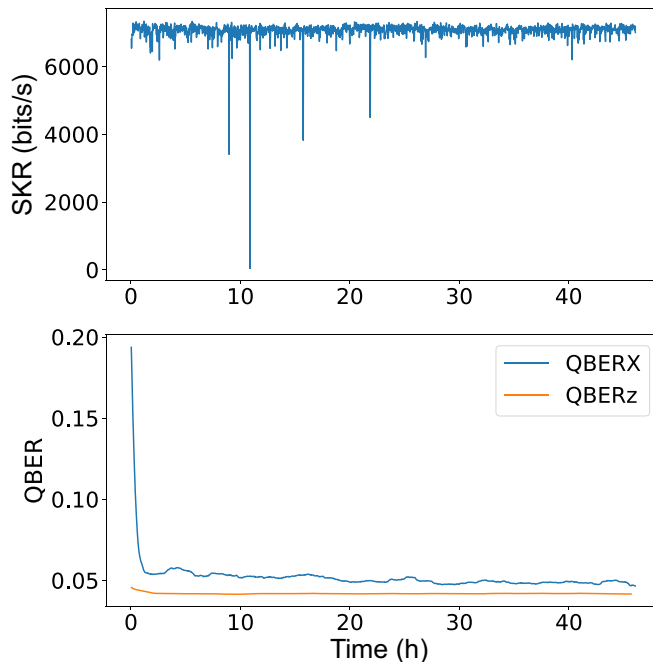


FIG. 4. Secret key rate (top) and QBER in both basis (bottom) as a function of time for a 48 h uninterrupted run.

We set our pump power to reach the optimal QBERz and start the QKD experiment. As shown in Fig. 4, the results obtained experimentally in the optimal configuration lead to an average SKR of 7 kbit/s, which close to our numerical simulation. We perform a continuous measurement lasting 48 h, before a helium condensation cycle is necessary for our SNSPD system. As we can see, all feedback loops of the system act on the different devices to maintain both the QBER and SKR during the entire operation time. The SKR depicted here corresponds to an experimental value of secret bits stored on a hard drive on each user's computer than can be directly used as cryptographic keys.

The use of commercial grade, off-the-shelf components is key to demonstrate a strong operationnability. However, the associated impact on the keyrate cannot be neglected. Reducing the overall losses within the source, analyzers, and fibers by using high-quality components and detectors would lead to a lower QBER and therefore, to a higher keyrate. What is more, a reduction of the detection timing jitter would improve the keyrate by allowing a reduction of the width of the coincidence peak. This change in the size of the coincidence window would result in a reduction of the noise measured, leading to a better QBER and a to higher keyrate.

VI. CONCLUSION

We have demonstrated a fully functional and automated quantum key distribution system, operated over 50 km of

deployed standard telecom fibers, allowing shared secret keys to be established between two distant users. All processing steps required to perform the key distillation protocol are implemented on a single computer on each site. To reach such a level of operability, we have also implemented a simple and efficient way to synchronize distant users without requiring an extra physical channel or specific dedicated data. The secure key rate reached over the link is 7 kbit/s on average for a single pair of DWDM channels and could theoretically reach approximately 8 kbit/s with more advanced stabilization processes. Lastly, more users can be added to the link by connecting them to the source using multiplexing strategies, leading to more complex and interesting topologies. This physical configuration would allow a fully connected network to be made with up to 40 users using only standard, off-the-shelf 100-GHz DWDM following the method described in Ref. [8].

Data are available from the authors on reasonable request.

ACKNOWLEDGMENTS

This work has been conducted within the framework of the French government financial support managed by the Agence Nationale de la Recherche (ANR), within its Investments for the Future programme, under the Université Côte d’Azur UCA-JEDI project (Quantum@UCA, ANR-15-IDEX-01), under the Stratégie Nationale Quantique through the project of the PEPR-quantum QComtestbeds (ANR 22-PETQ-0011), within the framework of the OPTIMAL project, funded by the European Union and the Conseil Régional SUD-PACA by means of the “Fonds Européens de développement régional” (FEDER), and with fundings from the EUROPE HORIZON-FPA project QSNP and the EUROPE DIGITAL project FranceQCI. The authors also acknowledge financial support from the Conseil Régional SUD-PACA through the INTRIQUE (APEX2019) and SIPS (Apex 2021) projects. Y. Pelet acknowledges PhD funding from Accenture. The authors are grateful to S. Canard, A. Ouorou, L. Chotard, L. Londeix from Orange & Orange Labs for their support, and to Orange for the installation and the connection of the dark fibers between the three different sites of our network, as well as for all the support they provided for their characterization. The authors also thank the Métropole Nice Côte d’Azur and the Inria Centre at Université Côte d’Azur for the access to their buildings and for their continuous help in making this network a reality. The authors also acknowledge IDQuantique and Swabian Instruments GmbH teams for all the technical support and the development of new features that were needed for the implementation of our operational QKD system and related experiment.

The authors declare no competing interests.

- [1] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell’s theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *J. Crypto* **5**, 3 (1992).
- [3] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, and H. Liu, *et al.*, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, *Nat. Photonics* **15**, 570 (2021).
- [4] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, and Z.-P. Li, *et al.*, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [5] S. P. Neumann, M. Selimovic, M. Bohmann, and R. Ursin, Experimental entanglement generation for quantum key distribution beyond 1 gbit/s, *Quantum* **6**, 822 (2022).
- [6] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, and S. El-Khoury, *et al.*, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, *Nat. Photonics* **17**, 422 (2023).
- [7] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonté, and S. Tanzilli, Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography, *Laser Photonics Rev.* **10**, 451 (2016).
- [8] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, and L. Kling, *et al.*, A trusted node-free eight-user metropolitan quantum communication network, *Sci. Adv.* **6**, eaba0959 (2020).
- [9] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, Clock synchronization by remote detection of correlated photon pairs, *NewJ. Phys.* **11**, 045011 (2009).
- [10] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, Free-space quantum key distribution with entangled photons, *Appl. Phys. Lett.* **89**, 101122 (2006).
- [11] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, and T. Jennewein, *et al.*, Feasibility of 300 km quantum key distribution with entangled states, *NewJ. Phys.* **11**, 085002 (2009).
- [12] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, *Nat. Commun.* **13**, 6134 (2022).
- [13] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Demystifying the information reconciliation protocol cascade, *Quantum Inf. Comput.* **15**, 453 (2015).
- [14] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, Generalized privacy amplification, *IEEE Trans. Inform. Theory* **41**, 1915 (1995).
- [15] F. Zheng, R. Xu, G. Zhu, B. Jin, L. Kang, W. Xu, J. Chen, and P. Wu, Design of a polarization-insensitive superconducting nanowire single photon detector with high detection efficiency, *Sci. Rep.* **6**, 1 (2016).
- [16] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: A comparison of two

- chromatic dispersion reduction methods, [Eur. Phys. J. D **30**, 143 \(2004\)](#).
- [17] A. Steinberg, P. Kwiat, and R. Chiao, Dispersion cancellation in a measurement of the single-photon propagation velocity in glass, [Phys. Rev. Lett. **68**, 2421 \(1992\)](#).
- [18] R. Y. Cai and V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, [New J. Phys. **11**, 045024 \(2009\)](#).
- [19] C. Spiess, S. Töpfer, S. Sharma, A. Kržič, M. Cabrejo-Ponce, U. Chandrashekhara, N. L. Döll, D. Rieländer, and F. Steinlechner, Clock synchronization with correlated photons, [Phys. Rev. Appl. **19**, 054082 \(2023\)](#).
- [20] Y.-A. Chen *et al.* An integrated space-to-ground quantum communication network over 4600 km, [Nature **589**, 214 \(2021\)](#).