optica

Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder

Costantino Agnesi,[1,2,†] Marco Avesani,[1,†] Luca Calderaro,[1,2,†] Andrea Stanco,[1,2] Giulio Foletto,[1] Mujtaba Zahidy,[1] Alessia Scriminich,[1] Francesco Vedovato,[1,2] Giuseppe Vallone,[1,2,3] and Paolo Villoresi[1,2,*]

[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy
[2]Istituto Nazionale di Fisica Nucleare (INFN) – sezione di Padova, Italy
[3]Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy
*Corresponding author: paolo.villoresi@dei.unipd.it

Received 18 October 2019; revised 27 January 2020; accepted 18 February 2020 (Doc. ID 381013); published 2 April 2020

Quantum key distribution (QKD) relies on quantum communication to allow distant parties to share a secure cryptographic key. Widespread adoption of QKD in current telecommunication networks will require the development of simple, low-cost, and stable systems. However, current QKD implementations usually include additional hardware that perform auxiliary tasks such as temporal synchronization and polarization basis tracking. Here we present a polarization-based QKD system operating at 1550 nm that performs synchronization and polarization compensation by exploiting only the hardware already needed for the quantum communication task. Polarization encoding is performed by a self-compensating Sagnac loop modulator that exhibits high temporal stability and the lowest intrinsic quantum bit error rate reported so far. The QKD system was tested over a fiber-optic link, demonstrating tolerance up to about 40 dB of channel losses. Due to its reduced hardware requirements and the quality of the source, this work represents an important step towards technologically mature QKD systems.

https://doi.org/10.1364/OPTICA.381013

1. INTRODUCTION

A major challenge for today's communication networks is to ensure safe exchange of sensitive data between distant parties. However, the rapid development of quantum information protocols towards the quantum computer [1–3] poses a substantial threat for current cyber-security systems. In fact, quantum routines such as Shor's factorization algorithm [4–6] could potentially render today's cryptographic schemes obsolete and completely insecure. Fortunately, quantum key distribution (QKD) [7–9] represents a solution to this catastrophic scenario. By leveraging on the principles of quantum mechanics and the characteristics of photons, QKD allows two distant parties, conventionally called Alice and Bob, to distill a perfectly secret key and bound the shared information with any adversarial eavesdropper [10]. Furthermore, QKD is an interesting solution for applications requiring long-term privacy, since algorithmic and technological advances for both classical and quantum computation do not threaten the security of keys generated with QKD.

Since its first proposal by Bennet and Brassard in 1984 [7], QKD has received much attention, and several experiments have shown its feasibility by exploiting different photonic degrees of freedom and platforms in free space [11–14], optical fibers [15–20], or even satellite links [21–25]. Recent developments have focused mainly on rendering QKD implementations simpler and more robust, aiming for compatibility with standard communication networks and widespread usage. This has led, for example, to the introduction of self-compensated modulators for different photonic degrees of freedom such as time-bin [26], mean photon number [27], and polarization [28,29], all based on Sagnac interferometric configurations. Also, simpler QKD protocols have been introduced such as a three-state [30,31] and one-decoy state version of the BB84 protocol, which simplifies the requirements of the quantum state encoder [32] and can provide higher rates in the finite-key scenario [33].

A critical aspect of QKD systems is the distribution of a temporal reference between the transmitter (Alice) and the receiver (Bob). This is crucial for at least two reasons. First, it allows to discriminate between the quantum signal and the noise introduced by either the quantum channel or detector defects. Second, it allows to correlate the qubit sequence transmitted by Alice with the detection events recorded by Bob. This correlation enables the distillation of the quantum-secure cryptographic key. The transmission of the temporal reference is usually achieved by sending a decimated

version of Alice's clock using an additional laser communication system that, in turn, requires the use of a secondary fiber channel [16,34], or time or wavelength multiplexing schemes to separate the quantum information from the classical light pulses [23,35]. Also, global navigation satellite systems (GNSSs) can be used to synchronize Alice and Bob, since these systems can give precise temporal references [14,36,37]. All these approaches, however, require additional hardware with respect to what is already needed for the quantum communication task.

Polarization-encoded QKD in fiber-optic links has been studied to a great extent [32,34,35,38,39]. Unfortunately, this type of link has an important drawback given by the natural birefringence of optical fibers, which causes the polarization state of transmitted photons to change continuously and in an unpredictable fashion [40]. Several approaches have been conceived to counteract these random polarization drifts, most of them requiring auxiliary laser pulses and time or wavelength multiplexing schemes [35,38,39,41], which, similar to the synchronization task discussed above, require additional hardware. A different approach was introduced by Ding *et al.* that used the revealed portion of the sifted key [42], produced during the error correction and privacy amplification procedures, to detect and compensate for the polarization drifts of the fiber link. Unfortunately, this method requires post-processing of an entire block of raw key, imposing a limit to the polarization tracking speed.

Here we present a simple QKD system, in which quantum communication, temporal synchronization, and polarization compensation are all realized in the same optical setup. The temporal synchronization is performed using a novel method, whose technical details are presented elsewhere [43]. This method does not require any auxiliary time reference and works by sending a public qubit sequence at pre-established times. Hence, it is named *Qubit4Sync*, because it uses only qubits for synchronization. Predetermined qubit sequences are also exploited to monitor and compensate for the polarization drift introduced by the quantum channel, constituted by a 26 km long fiber spool. With respect to Ref. [42], our solution does not require post-processing of an entire block of raw key, allowing for an increased compensation speed. Furthermore, the QKD source here presented exhibits several hours of stability and an intrinsic quantum bit error rate (QBER) on the order of 0.05%, which is, to the best of our knowledge, the lowest reported so far. This source exploits the scheme for polarization encoding based on a Sagnac loop (hence the name *POGNAC*) we introduced in Ref. [28]. The relaxed hardware requirements, the high stability, and the record-low QBER of the presented implementation represent an important technological step towards mature and efficient QKD systems.

2. SETUP

Our experimental setup, which implements the simplified three-state and one-decoy protocol proposed in [32], is sketched in Fig. 1. A gain-switched distributed feedback (DFB) laser source outputs a 50 MHz stream of phase-randomized pulses with 270 ps of full-width-at-half-maximum temporal duration at 1550 nm wavelength. The light pulses first pass through a lithium niobate intensity modulator (IM) used to set the intensity levels required by the decoy-state method. The pulses then enter the *POGNAC* polarization modulator realized using only standard commercial off-the-shelf (COTS) fiber components, namely, a circulator (CIRC), a polarization controller (PC), a polarizing beam splitter (PBS), and a phase modulator (ϕ-mod). Compared to other polarization modulators, the *POGNAC* requires a lower V_π voltage, can be developed using ϕ-mods that carry only a single polarization mode, exhibits no polarization mode dispersion, and has a self-compensating design that guarantees robustness against temperature and electrical drifts (see Ref. [28] for a full description and additional details).

The photons emerge from the *POGNAC* with a polarization state given by

$$|\psi_{\text{out}}^{\phi_e,\phi_\ell}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i(\phi_e-\phi_\ell)}|V\rangle\right), \tag{1}$$

where the phases ϕ_e and ϕ_ℓ can be set by carefully timing the applied voltage on a lithium niobate ϕ-mod. This was achieved with the Zynq-7000 ARM/FPGA System-on-a-Chip (SoC, manufactured by Xilinx), which in our implementation controls the operation of the QKD source.

If no voltages are applied by the SoC, the polarization state remains unchanged, i.e., $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. Instead, if ϕ_e is set to $\frac{\pi}{2}$ while ϕ_ℓ remains zero, the output state becomes $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$. Alternatively, if ϕ_e remains zero while ϕ_ℓ is set to $\frac{\pi}{2}$, the output state becomes $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$. In this way, we generate the three states required by the simplified three-polarization-state version of BB84 [32], with the key-generation basis $\mathcal{Z} = \{|0\rangle, |1\rangle\}$, where $|0\rangle := |L\rangle$, $|1\rangle := |R\rangle$, and the control state $|+\rangle$ of the $\mathcal{X} = \{|+\rangle, |-\rangle = (|H\rangle - |V\rangle)/\sqrt{2}\}$ basis.

The optical pulses then encounter an optical attenuator (ATT) that weakens the light to the single-photon level. A 99:1 beam splitter (BS) is used to estimate the intensity level of the pulses: the 1% output port is directed to a gated InGaAs/InP single-photon avalanche diode (SPAD, manufactured by Micro Photon Devices Srl [44]), while the other output port is directed to the quantum channel (QC). In our implementation, the QC is formed by a 26 km spool of G.655 dispersion-shifted fiber with 0.35 dB/km of loss followed by a variable optical attenuator (VOA). This VOA

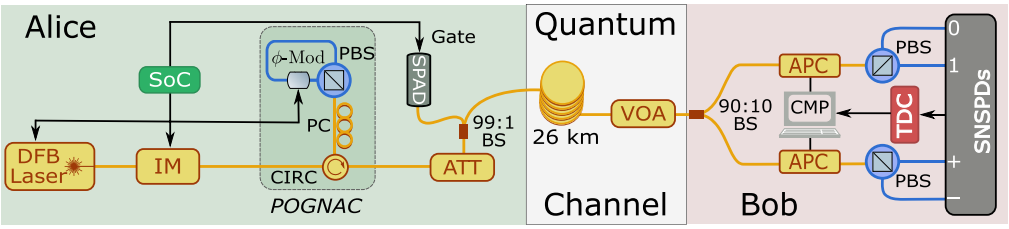

Fig. 1. Experimental setup. For a detailed description, see Section 2. Single-mode fibers are indicated in yellow, while polarization-maintaining fibers are in blue.

allows us to introduce further channel loss in order to test our system's resilience.

Alice sends key-generation states with probability $p_A^{\mathcal{Z}} = 0.9$ ($p_A^{\mathcal{X}} = 0.1$), while the two intensity levels are $\mu_1 \approx 0.80$ and $\mu_2 \approx 0.28$, which are sent with probabilities $p_{\mu_1} = 0.7$ and $p_{\mu_2} = 0.3$, respectively. This intensity modulation is driven by the SoC, and presents no drifts during the QKD runs, as attested by the data presented in Supplement 1. The used parameters are close to optimal according to our simulations and Ref. [33]. The random bits used in the QKD runs are obtained from the source-device-independent quantum random generator based on optical heterodyne measurements described in Ref. [45].

The fiber receiving setup consists of a 90:10 fiber BS setting the detection probabilities of the two measurement bases to $p_B^{\mathcal{Z}} = 0.9$ and $p_B^{\mathcal{X}} = 0.1$. Each output arm of the BS is connected to an automatic polarization controller (APC) and a PBS. The four outputs are then sent to four superconductive nanowire single-photon detectors (SNSPDs, manufactured by ID Quantique SA) cooled to 0.8 K. The detection efficiencies are around 85% for the detectors in the $\mathcal{Z}$ basis, whereas it is 90% and 30% for the $|+\rangle$ and $|-\rangle$ detectors, respectively. As discussed in Refs. [14,46], some events are randomly discarded in post-processing to balance the different efficiencies. All the detectors are affected by about 200 Hz of free-running intrinsic dark count rate. The SNSPD detections are recorded by the quTAG time-to-digital converter (TDC, manufactured by qutools GmbH) with 1 ps of temporal resolution and jitter of 10 ps. A computer (CMP) then reads the TDC data and uses it for temporal synchronization, polarization compensation, and QKD. The low dark count rate and negligible afterpulsing represent the main reasons that made us choose SNSPDs over, for example, InGaAs SPADs. Indeed, a low dark count rate allows the QBER to stay low even for strong levels of channel attenuation (i.e., long fiber links).

A. Synchronization

In this work, we use the *Qubit4Sync* algorithm to synchronize Alice's and Bob's clocks using the same qubits exchanged during the QKD protocol. This means that the setup does not need any synchronization subsystem, which is usually implemented with a pulsed laser or GNSS clock to share an external time reference. The synchronization method is described in detail in Ref. [43].

Here we report the main features of the algorithm. The synchronization is done in post-processing, adjusting the times in which Bob expects to receive the qubits from Alice. For this, Bob needs to determine at which frequency (in his time reference) the qubits are arriving at the detectors and the absolute time in which the first qubit should arrive. Our approach is to compute the frequency from the time-of-arrival measurements. To recover the absolute time, we send an initial public string encoded in the first L states. By correlating this string with the one received by Bob, it is possible to distinguish which state received by Bob is the first one sent by Alice, hence the absolute time of the first qubit. This is the typical technique used, for instance, by the Global Positioning System (GPS) receiver to synchronize with the satellite signal [47].

The novelty of *Qubit4Sync* is the implementation of a fast correlation algorithm requiring lower computational cost than the algorithms based on a sparse fast Fourier transform, as we show in Ref. [43]. This allows us to calculate, in real time, the position of the maximum correlation peak of long synchronization strings, which is required to cope with the high losses of a quantum channel. To the best of our knowledge, no similar algorithms have been previously proposed or used for QKD.

B. Polarization Compensation Scheme

Mechanical and temperature fluctuations lead to variations in the natural birefringence of fiber optics, transforming the polarization state of the photons that travel through the fiber. This transformation is troublesome for QKD since it causes Alice and Bob to effectively have different polarization reference frames. As a consequence of this mismatch, the QBER increases, lowering the secure key rate (SKR) up to the point where no quantum secure key can be established. To prevent this, a polarization compensation system must be utilized.

Here we propose a polarization compensation scheme that exploits a shared public string, not necessarily related to the synchronization string. Every second, the shared string of 10^6 states is transmitted by Alice encoded using weak coherent pulses in the $\mathcal{Z}$ basis with μ_1 intensity. Bob detects the sequence, and after performing the temporal synchronization routine, he estimates the QBER of his recorded sequence. Bob still has to estimate the $\mathcal{X}$ basis QBER. For this purpose, at the end of each interval, Alice reveals the basis used to encode the QKD qubits that follow the public string. This process is actually the standard basis reconciliation procedure of QKD. Since in this protocol only one state is transmitted in the $\mathcal{X}$ basis, Bob can immediately estimate the QBER [32].

The estimated QBER values are then fed into an optimization algorithm, based on coordinate descent [48] and running in Bob's CMP, which controls the APCs of Bob's setup. The APCs have four different piezoelectric 1D actuators, alternately at 0° and 45° to the horizontal plane, that stress and strain the optical fibers, changing the polarization of the light that traverses them [49]. Our optimization algorithm loops through the four actuators sequentially. At each round, the position of an actuator is changed with a step size proportional to the measured QBER. If such a change causes a reduction in the measured QBER, our algorithm keeps changing the position of the same actuator in the same direction, always with a step size proportional to the measured QBER. Instead, if an increased QBER is measured, the algorithm reverses the direction of motion for the actuator. Only one reversal is permitted per round, after which the next actuator is selected and a new round begins.

Compared to Ref. [42], our approach has the advantage that only the basis reconciliation step is required to obtain sufficient information to run the polarization compensation algorithm. This renders our approach less communication intensive, and we were able to achieve a 1 s feedback cycle, which is 12 times faster than the one reported in Ref. [42]. Also, the length of the shared string and its transmission frequency can be changed to best match the requirements of the fiber optical link. Furthermore, the public string can be transmitted in an interleaved fashion together with the QKD qubits at predetermined times.

3. RESULTS

A. POGNAC Low Intrinsic QBER and High Stability

The $\mathrm{QBER}_{\mathrm{opt}}$, i.e., intrinsic (or "optical") QBER of the source, gives a quantitative and qualitative measure of its suitability for

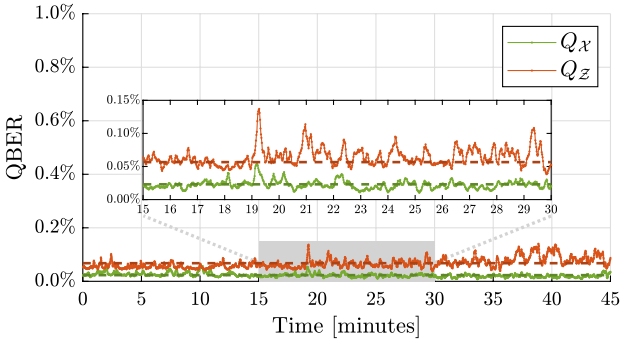

Fig. 2. Intrinsic QBER and temporal stability of the *POGNAC* polarization encoder. The average QBER measured for the key-generation basis was $Q_{\mathcal{Z}} = 0.07 \pm 0.02\%$ (dashed red line), while an average $Q_{\mathcal{X}} = 0.02 \pm 0.01\%$ (dashed green line) was measured for the control basis. A close-up between minutes 15–30 can be seen in the inset plot.

use in QKD [8]. Its characterization is relevant to predict the SKR under different conditions, such as different channels or detector technologies. It is also meaningful to measure its stability to find how long the source can function without realignment.

For these reasons, we report in Fig. 2 the stability of the intrinsic QBER of our QKD polarization source. This measurement was performed by sending a pseudo-random qubit sequence of $\{|0\rangle, |1\rangle, |+\rangle\}$ states (used only for this test) and measuring the QBER of the sifted string recovered by Bob. To remove all fluctuations not attributable to the source, the fiber spool of the QC was bypassed while the VOA was set to ≈ 11 dB of attenuation. Furthermore, the 90:10 BS was replaced with a 50:50 BS in order to have comparable statistics for both measurement bases. Every second, the QBER was estimated for both the $\mathcal{Z}$ key-generation basis and the $\mathcal{X}$ control basis. In 45 min, an average QBER of $Q_{\mathcal{Z}} = 0.07 \pm 0.02\%$ was measured for the $\mathcal{Z}$ basis, while the average QBER for the $\mathcal{X}$ was $Q_{\mathcal{X}} = 0.02 \pm 0.01\%$, giving a mean $\mathrm{QBER}_{\mathrm{opt}}$ in the two relevant bases for QKD of 0.05%. This corresponds to an extinction ratio of 33 dB for the used states. We note that the reported data include the contribution from dark counts, and therefore slightly overestimate the value of the $\mathrm{QBER}_{\mathrm{opt}}$. To verify that the $\mathcal{X}$ and $\mathcal{Z}$ bases are mutually unbiased, we also measured the QBER of the $\mathcal{Z}$ states when observed in the $\mathcal{X}$ basis and vice versa, obtaining $48.8 \pm 0.4\%$ in both cases.

These measurements corroborate the results of Ref. [28] and demonstrate the low intrinsic QBER, and high stability of the *POGNAC* polarization modulator. It is worth noticing that an extinction ratio above 30 dB is typically not achievable by using COTS polarization modulators, which also suffer from temporal drifts due to temperature and electronics fluctuations. These drifts can be suppressed by exploiting self-compensating schemes, as the *POGNAC* or the one in Ref. [50]. However, Ref. [50] reported a limited extinction ratio of less than 20 dB due to implementation imperfections.

Table 1 reports a comparison of the intrinsic QBER with the existing literature, in particular Refs. [14,20,29,51–55]. The $\mathrm{QBER}_{\mathrm{opt}}$ we registered here is the lowest ever reported, even considering encodings other than polarization (as used in Refs. [14,20,29,52]), such as time-bin (in Refs. [53–55]) and differential phase shift (in Ref. [51]), as well as different platforms to realize the source, as fibers-based schemes (in Refs. [29,51,52,54,55]) or integrated photonics chips (in Refs. [14,20]).

Table 1. Comparison among Intrinsic QBERs Reported in Literature[a]

Reference	$\mathrm{QBER}_{\mathrm{opt}}$	Encoding	Notes
[51]	0.46%	DPS	Estimated via ER
[52]	0.4%	Pol	Measured
[20]	0.3%	Pol	Estimated via ER
[29]	0.27%	Pol	Measured
[53]	0.25%	TB	Estimated via $\mathcal{V}$
[54]	0.15%	TB	Estimated via $\mathcal{V}$
[55]	0.1%	TB	Estimated via $\mathcal{V}$
[14]	0.1%	Pol	Estimated via ER
This work	0.05%	Pol	Measured

[a]If the intrinsic extinction ratio (ER) of the source is provided, $\mathrm{QBER}_{\mathrm{opt}}$ is estimated via $\mathrm{QBER}_{\mathrm{opt}} = \mathrm{ER}/(1+\mathrm{ER})$ [51]. If the intrinsic fringe visibility $\mathcal{V}$ is measured, then $\mathrm{QBER}_{\mathrm{opt}} = (1-\mathcal{V})/2$ [8]. We include QKD sources with different encodings: differential phase shift (DPS), polarization (Pol), and time-bin (TB).

B. Polarization Drift Compensation with 26 km of Optical Fiber

To test our polarization drift compensation algorithm, we performed a 6 h long run with the QC including both the 26 km optical fiber spool and the VOA for ≈ 19 dB of total losses.

On average, the detected bits of the shared polarization compensation string in the $\mathcal{Z}$ basis were $\approx 8 \times 10^3$, while the sifted bits from the control basis were $\approx 3 \times 10^3$. This allowed to correct the polarization drift with an average QBER measured for the key-generation basis of $Q_{\mathcal{Z}} = 0.3 \pm 0.1\%$ while an average $Q_{\mathcal{X}} = 0.2 \pm 0.1\%$ for the control basis, for 6 h of continuous operation (see Fig. 3). These values are about an order of magnitude lower than those observed in Ref. [42].

After the experimental run, we noted a lower detection efficiency of 45% for the detectors of the $\mathcal{Z}$ basis. This was due to a non-optimal polarization rotation of the photons entering the SNSPD detectors, which are polarization sensitive. This reduced detection efficiency did not hamper the polarization drift compensation algorithm, demonstrating its robustness even in non-optimal conditions.

C. QKD Secure Key Rate for Different Channel Losses

To test the performances of our system with qubit-based synchronization and a self-compensating polarization encoder, as well as

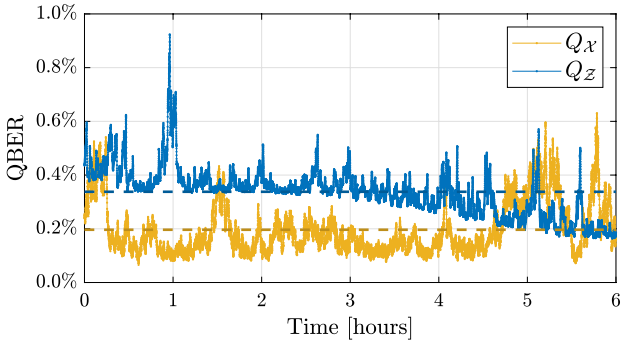

Fig. 3. QBER measurement for a 6 h long acquisition along a 26 km optical fiber channel. The average QBER measured for the key-generation basis was $Q_{\mathcal{Z}} = 0.3 \pm 0.1\%$ (dashed blue line), while an average $Q_{\mathcal{X}} = 0.2 \pm 0.1\%$ (dashed yellow line) was measured for the control basis.

its resistance to channel losses, several QKD runs were executed, each with increased losses, as reported in Fig. 4. The losses were added increasing the attenuation of the VOA after the 26 km of fiber. A random qubit sequence of $\{|0\rangle, |1\rangle, |+\rangle\}$ states was transmitted at a repetition rate of 50 MHz, where the first L qubits of the sequence formed the publicly known synchronization string.

For each run, the SKR was calculated in the asymptotic limit according to

$$\mathrm{SKR}_{\infty} = \left[s_{\mathcal{Z},0} + s_{\mathcal{Z},1}(1 - h(\phi_{\mathcal{Z}})) - f \cdot n_{\mathcal{Z}} \cdot h(Q_{\mathcal{Z}})\right]/t, \quad (2)$$

where t is the duration of each acquisition, $h(\cdot)$ is the binary entropy, $f = 1.06$ is the Shannon inefficiency of typical error correction algorithms, $n_{\mathcal{Z}}$ is the length of the sifted key in the $\mathcal{Z}$ basis, $s_{\mathcal{Z},0}$ and $s_{\mathcal{Z},1}$ are the lower bounds on the number of vacuum and single-photon detections in the $\mathcal{Z}$ basis, and $\phi_{\mathcal{Z}}$ is the upper bound on the phase error in the $\mathcal{Z}$ basis calculated from $Q_{\mathcal{X}}$ as in Ref. [33], but without finite-key corrections.

For the four runs with lower losses, we also performed the finite-key analysis using the bits produced in $t = 90$s of acquisition by using [33]

$$\mathrm{SKR}_{fk} = \mathrm{SKR}_{\infty} - \left[6\log_2(19/\epsilon_{\mathrm{sec}}) + \log_2(2/\epsilon_{\mathrm{conf}})\right]/t, \quad (3)$$

where $s_{\mathcal{Z},0}$, $s_{\mathcal{Z},1}$, and $\phi_{\mathcal{Z}}$ in SKR_{∞} now include finite-key corrections, and with secrecy and confirmation of correctness parameters $\epsilon_{\mathrm{sec}} = 10^{-10}$ and $\epsilon_{\mathrm{conf}} = 10^{-15}$, respectively. In Supplement 1, we also include simulations of the finite-key performance of the system with different key sizes and duration. As shown there, the system is able to produce a positive SKR_{fk} for up to ≈ 38dB of channel losses with an acquisition time $t = 6$ h, compatible with the measured stability of Fig. 3.

As discussed in Ref. [43], if the background and dark counts are not considered, the synchronization can be established with $L = 10^6$ for up to 40 dB of total losses, i.e., considering channel and receiver losses as well as detector inefficiency. A longer string, with $L = 10^7$, could be used to synchronize up to 50 dB of losses. In our experiment, the presence of dark counts lowers the bounds by about 6 dB. Indeed, using a synchronization string of length $L = 10^6$, we performed several QKD runs with losses up to 34 dB. With $L = 10^7$, we successfully ran QKD up to the channel loss at which the key rate drops to zero. In the QKD run with highest losses, we achieved a SKR of 80 bits per second at 40 dB channel losses, corresponding to about 200 km of SMF28 fiber (0.2 dB/km) or 235 of ultralow-loss fiber (0.17 dB/km). It is important to note that our QKD implementation withstands up to 41 dB of channel loss, as reported in the SKR_{∞} simulation in Fig. 4. Our results prove that the *Qubit4Sync* method properly works even at the highest losses tolerated by our QKD implementation.

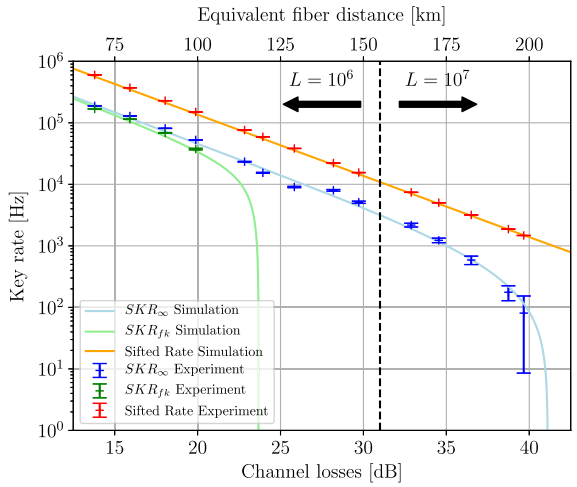

Fig. 4. Sifted and secure key rate as a function of channel losses. For the four runs with lower losses, we also include finite-key analysis (SKR_{fk}), for 90 s of acquisition each. The equivalent fiber distance (upper x-axis) is based on SMF28 losses (0.2 dB/km). The crosses represent the experimental runs, while the lines show the results of our simulation based on the physical parameters of our experiment. Error bars are standard deviations, obtained by simulating 1000 repetitions of the experiment.

4. CONCLUSION

Here we have presented a simple polarization encoded QKD implementation with qubit-based synchronization and a self-compensating polarization modulator. Its simple and hardware-efficient design reduces the complexity for both the QKD transmitter and receiver. In fact, the same optical setup is used for three different tasks, i.e., synchronization, polarization compensation, and quantum communication, without requiring any changes to the working parameters of the setup or any additional hardware. The QKD transmitter shows high stability and an intrinsic QBER below 0.1%. This, in addition to the effective polarization compensation technique and the use of high-performance SNSPD detectors, allows us to obtain high SKRs and resilience up to about 40 dB of channel losses, even with a repetition-rate of 50 MHz. Indeed, although the repetition rate of our source is an order of magnitude smaller than those of recent polarization-encoded fiber-based QKD experiments [18,20], we achieved a SKR that is comparable with that of Ref. [20] and an order of magnitude higher than that reported in Ref. [18] for distances greater than 50 km. If the SNSPDs were replaced with InGaAs SPADs, with a free-running dark count rate of 500 Hz, 15% quantum efficiency, and 20 μs hold-off time [44], we expect that the system would be able to produce a positive SKR_{∞} for up to 35 dB (31 dB) of channel losses using a temporal gating window of 0.3 ns (1 ns).

Currently, the *POGNAC* requires to be manually aligned once every day. However, to make our system more autonomous, its PC could be replaced with an APC controlled by a power monitor inside the fiber Sagnac loop. This would render our implementation compatible with different operative scenarios, ranging from urban QKD fiber links [20] to free-space satellite QKD links via CubeSats [56], or even to implement other quantum communication schemes such as quantum digital signatures [57] or remote blind qubit preparation [58]. Last, our implementation is particularly promising for free-space QKD [13,14,23] since polarization is not significantly affected by atmospheric propagation [59] and long-term stability is required, especially for links with satellites in medium Earth orbit [60] or part of a GNSS constellation [61].

Funding. Ministero dell'Istruzione, dell'Università e della Ricerca (Fondo dipartimenti universitari di eccellenza); Agenzia Spaziale Italiana (Q-SecGroundSpace (E16J16001490001)); Istituto Nazionale di Fisica Nucleare (MoonLIGHT-2); Horizon 2020 Framework Programme (Marie Skłodowska-Curie grant agreement No 675662).

Acknowledgment. The authors thank L. Palmieri and M. Calabrese for technical support on the 26 km fiber spool.

See Supplement 1 for supporting content.

†These authors contributed equally to this work.

REFERENCES

1. T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," Nature **464**, 45–53 (2010).
2. F. Flamini, N. Spagnolo, and F. Sciarrino, "Photonic quantum information processing: a review," Rep. Prog. Phys. **82**, 016001 (2018).
3. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, and B. Burkett, "Quantum supremacy using a programmable superconducting processor," Nature **574**, 505–510 (2019).
4. P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1997).
5. L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature **414**, 883–887 (2001).
6. A. Politi, J. C. F. Matthews, and J. L. O'Brien, "Shor's quantum factoring algorithm on a photonic chip," Science **325**, 1221 (2009).
7. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci. **560**, 7–11 (2014).
8. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
9. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," arXiv:1906.01645 (2019).
10. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du šek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
11. C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," Opt. Express **16**, 16840–16853 (2008).
12. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," Phys. Rev. Lett. **113**, 060503 (2014).
13. S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," Nat. Photonics **11**, 509–513 (2017).
14. M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," arXiv:1907.10039 (2019).
15. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," Opt. Express **16**, 18790–18797 (2008).
16. B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nat. Photonics **9**, 163–168 (2015).
17. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Sci. Adv. **3**, e1701491 (2017).
18. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).
19. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).
20. D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. Derose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
21. G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," Phys. Rev. Lett. **115**, 040502 (2015).
22. G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi, "Interference at the single photon level along satellite-ground channels," Phys. Rev. Lett. **116**, 253601 (2016).
23. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
24. R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj Quantum Inf. **3**, 30 (2017).
25. C. Agnesi, F. Vedovato, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, "Exploring the boundaries of quantum mechanics: advances in satellite quantum communications," Philos. Trans. Royal Soc. A **376**, 20170461 (2018).
26. S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, S.-F. Liu, Z. Zhou, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Practical gigahertz quantum key distribution robust against channel disturbance," Opt. Lett. **43**, 2030–2033 (2018).
27. G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution," Opt. Lett. **43**, 5110–5113 (2018).
28. C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, "All-fiber self-compensating polarization encoder for quantum key distribution," Opt. Lett. **44**, 2398–2401 (2019).
29. Y. Li, Y.-H. Li, H.-B. Xie, Z.-P. Li, X. Jiang, W.-Q. Cai, J.-G. Ren, J. Yin, S.-K. Liao, and C.-Z. Peng, "High-speed robust polarization modulation for quantum key distribution," Opt. Lett. **44**, 5262–5265 (2019).
30. C.-H. F. Fung and H.-K. Lo, "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry," Phys. Rev. A **74**, 042342 (2006).
31. K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," Phys. Rev. A **90**, 052314 (2014).
32. F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," Appl. Phys. Lett. **112**, 051108 (2018).
33. D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).
34. Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, "Decoy-state quantum key distribution with polarized photons over 200 km," Opt. Express **18**, 8587–8594 (2010).
35. A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, "A fully automated entanglement-based quantum cryptography system for telecom fiber networks," New J. Phys. **11**, 045013 (2009).
36. G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," Phys. Rev. A **91**, 042320 (2015).
37. J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," Phys. Rev. A **92**, 052339 (2015).

38. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. **98**, 010505 (2007).
39. D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen, G. Yu, and J.-H. Liu, "Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback," Opt. Express **26**, 22793–22800 (2018).
40. Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Polarization variations in installed fibers and their influence on quantum key distribution systems," Opt. Express **25**, 27923–27936 (2017).
41. G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**, 1867–1873 (2008).
42. Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. Li, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," Opt. Lett. **42**, 1023–1026 (2017).
43. L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, and G. Vallone, "Fast and simple qubit-based synchronization for quantum key distribution," arXiv:1909.12050 (2019).
44. A. Tosi, A. D. Frera, A. B. Shehata, and C. Scarcella, "Fully programmable single-photon detection module for InGaAs/InP single-photon avalanche diodes with clean and sub-nanosecond gating transitions," Rev. Sci. Instrum. **83**, 013104 (2012).
45. M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," Nat. Commun. **9**, 5365 (2018).
46. M. K. Bochkov and A. S. Trushechkin, "Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: tight bounds," Phys. Rev. A **99**, 032308 (2019).
47. H. Hassanieh, F. Adib, D. Katabi, and P. Indyk, "Faster GPS via the sparse Fourier transform," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, Mobicom (ACM, 2012), pp. 353–364.
48. S. J. Wright, "Coordinate descent algorithms," Math. Program. **151**, 3–34 (2015).
49. N. G. Walker and G. R. Walker, "Endless polarisation control using four fibre squeezers," Electron. Lett. **23**, 290–292 (1987).
50. I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, "Proof-of-concept of real-world quantum key distribution with quantum frames," New J. Phys. **11**, 095001 (2009).
51. T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer," Opt. Lett. **29**, 2797–2799 (2004).
52. K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, "A short wavelength gigahertz clocked fiber-optic quantum key distribution system," IEEE J. Quantum Electron. **40**, 900–908 (2004).
53. A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Appl. Phys. Lett. **112**, 171108 (2018).
54. H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Practical aspects of quantum cryptographic key distribution," J. Cryptol. **13**, 207–220 (2000).
55. G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, "Modulator-free coherent-one-way quantum key distribution," Laser Photon. Rev. **11**, 1700067 (2017).
56. D. K. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon, and R. Ursin, "CubeSat quantum communications mission," EPJ Quantum Technol. **4**, 6 (2017).
57. X.-B. An, H. Zhang, C.-M. Zhang, W. Chen, S. Wang, Z.-Q. Yin, Q. Wang, D.-Y. He, P.-L. Hao, S.-F. Liu, X.-Y. Zhou, G.-C. Guo, and Z.-F. Han, "Practical quantum digital signature with a gigahertz BB84 quantum key distribution system," Opt. Lett. **44**, 139–142 (2019).
58. Y.-F. Jiang, K. Wei, L. Huang, K. Xu, Q.-C. Sun, Y.-Z. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, F. Xu, Q. Zhang, and J.-W. Pan, "Remote blind state preparation with weak coherent pulses in the field," Phys. Rev. Lett. **123**, 100503 (2019).
59. C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger, "Influence of satellite motion on polarization qubits in a space-earth quantum communication link," Opt. Express **14**, 10050–10059 (2006).
60. D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental single-photon exchange along a space link of 7000 km," Phys. Rev. A **93**, 010301 (2016).
61. L. Calderaro, C. Agnesi, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, "Towards quantum communication from global navigation satellite system," Quantum Sci. Technol. **4**, 015012 (2018).