

# Cross-Encoded Quantum Key Distribution Exploiting Time-Bin and Polarization States with Qubit-Based Synchronization

Davide Scalcon, Costantino Agnesi, Marco Avesani, Luca Calderaro, Giulio Foletto, Andrea Stanco, Giuseppe Vallone, and Paolo Villorresi\*

Robust implementation of quantum key distribution requires precise state generation and measurements, as well as the choice of an optimal encoding to minimize channel disturbance. Time-bin encoding represent a good candidate for fiber links as birefringence does not perturb this kind of states whereas stable and low-error encoders and decoders are available for polarization encoding. Here a cross-encoded scheme where high accuracy quantum states are prepared through a self-compensating, calibration-free polarization modulator and transmitted using a polarization-to-time-bin converter is presented. The receiver performs time-of-arrival measurements in the key-generation basis and converts qubits back to polarization encoding for measurements in the control basis. Temporal synchronization between the transmitter and receiver is performed with a qubit-based method that does not require additional hardware to share a clock reference. The system is tested in a 12-h run and demonstrates good and stable performance in terms of key and quantum bit error rates. The flexibility of this approach represents an important step toward the development of hybrid networks with both fiber-optic and free-space links.

including computing, sensors, simulations, cryptography, and telecommunications. Quantum key distribution (QKD), one of the most mature quantum technologies, allows distant users to generate a shared secret key with unconditional security. QKD is characterized by a consolidated composable security framework<sup>[1,2]</sup> and by rapid and continuous technical advancements.<sup>[3]</sup> In fact, several QKD field trials are being performed to demonstrate the real-world applicability of this technology<sup>[4–10]</sup> and several start-ups and university spin-offs are being created to intercept the growing market demands.<sup>[11]</sup>

The most commonly used QKD protocol is the first one ever introduced, that is, the BB84 protocol.<sup>[12]</sup> It requires a transmitter, Alice, to send qubits encoded in two mutually unbiased bases (MUBs). Then, a receiver, Bob, randomly chooses a basis among the two MUBs for each received qubit and performs a projective measurement. After correlating their results

and performing classical post-processing, Alice and Bob end up with identical keys that can be securely used in cryptographic schemes such as the one-time pad.


The effectiveness of BB84 implementations depends on the choice of the photonic degree of freedom that encodes the qubits.

## 1. Introduction

Advancements in our ability to detect and manipulate single quantum objects has led to the development of quantum technologies with disruptive potential in many different areas,

D. Scalcon, C. Agnesi, M. Avesani, L. Calderaro, G. Foletto, A. Stanco, G. Vallone, P. Villorresi  
Dipartimento di Ingegneria dell'Informazione  
Università degli Studi di Padova  
via Gradenigo 6B, Padova IT-35131, Italy  
E-mail: paolo.villorresi@unipd.it

L. Calderaro  
ThinkQuantum S.r.l.  
Via della Tecnica, 85, Sarcedo (VI) IT-36030, Italy  
G. Vallone  
Dipartimento di Fisica e Astronomia  
Università degli Studi di Padova  
via Marzolo 8, Padova IT-35131, Italy  
G. Vallone, P. Villorresi  
Padua Quantum Technologies Research Center  
Università degli Studi di Padova  
via Gradenigo 6B, Padova IT-35131, Italy

 The ORCID identification number(s) for the author(s) of this article can be found under <https://doi.org/10.1002/qute.202200051>

© 2022 The Authors. Advanced Quantum Technologies published by Wiley-VCH GmbH. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

DOI: 10.1002/qute.202200051

Common choices are the polarization and time-bin degrees of freedom. Polarization is usually preferred for free-space QKD implementations,<sup>[13–15]</sup> even being exploited for satellite-based QKD links.<sup>[16]</sup> There are three main factors that encourage the use of polarization encoding for free-space links. The first factor is that atmospheric transmission does not change the polarization state of the transmitted qubits.<sup>[17]</sup> This allows Alice and Bob to share a well-defined polarization reference frame and eliminates the need of active components to compensate the unitary transformation introduced by the quantum channel. The second factor is that polarization encoders with long-term temporal stability and low intrinsic quantum bit error rate (QBER) can be designed and developed.<sup>[18–22]</sup> Among these, the POGNAC polarization encoder, with an average of 0.05%, has reported the lowest intrinsic QBER in scientific literature<sup>[21]</sup> while the iPOGNAC<sup>[23]</sup> reported a stable polarization output for over 24 h.<sup>[22]</sup> The third factor is that polarization receivers can be easily constructed with inexpensive optical components such as polarization beam splitters (PBS), half-wave plates (HWP), and quarter-wave plates (QWP) that guarantee high extinction ratios and stable performances over time.

Unfortunately, polarization encoding has some drawbacks when propagating through a fiber channel. This is mainly due to the random changes of the fiber birefringence introduced by ambient conditions and mechanical stress. This causes a random rotation of the polarization and, as a consequence, increases the QBER. In turn, it lowers the secret key rate (SKR) up to the point where no quantum secure key can be established.<sup>[24]</sup> To prevent this, a polarization compensation system becomes essential. Such systems have been developed<sup>[21,25,26]</sup> and successfully tested in deployed fibers.<sup>[5,8–10]</sup> However, for fiber channels that are strongly coupled to the external environment, such as deployed aerial fibers exposed to wind-induced movements, polarization compensation becomes a complex and demanding task requiring the implementation of dedicated auxiliary hardware including additional light sources, detectors, and fast control electronics.<sup>[24,27]</sup>

To make QKD performance independent of the polarization fluctuations of the optical fiber, time-bin encoding was introduced as it exploits time-of-arrival of photons and the relative phase between time bins.<sup>[28]</sup> This encoding has been employed in many QKD field trials in deployed fibers,<sup>[4,6,7]</sup> as well as in the record-setting 421 km fiber QKD link demonstration of the BB84 protocol.<sup>[29]</sup> However, time-bin has the disadvantage of requiring phase stabilization of the interferometers which encode and decode the superposition of time bins.<sup>[30]</sup> Furthermore, time-bin encoding is not suitable for applications involving moving terminals since a kinematic phase shift emerges,<sup>[31]</sup> complicating the decoding of the phase information even further.

In this work, we present a cross-encoded implementation of the BB84 QKD protocol where polarization is used for state encoding while time-bin is used to propagate the qubits along a quantum channel composed of 50 km long fiber spool. The iPOGNAC polarization encoder is used to generate the states required to perform QKD, which guarantees long-term temporal stability and low intrinsic QBER. The polarization encoding is then transformed to time-bin encoding to guarantee that the birefringence of the fiber-optic channel does not modify the quantum information. Quantum state decoding is achieved with a hybrid

QKD receiver that performs both time-of-arrival and polarization measurements. In addition, temporal synchronization between the transmitter and the receiver is established using the qubit-based Qubit4Sync method,<sup>[32]</sup> without requiring supplementary hardware with respect to what is already needed for the quantum communication. Our work enables the implementation of flexible QKD systems that can convert the qubit encoding to best fit the characteristics of the quantum channel and represents a step toward the development of hybrid QKD networks where both fiber and free-space links are employed.

## 2. Experimental Setup

Our cross-encoded polarization and time-bin implementation of the three-state and one-decoy efficient BB84 protocol<sup>[33]</sup> is sketched in **Figure 1** with the transmitter, Alice, on the left and the receiver, Bob, on the right.

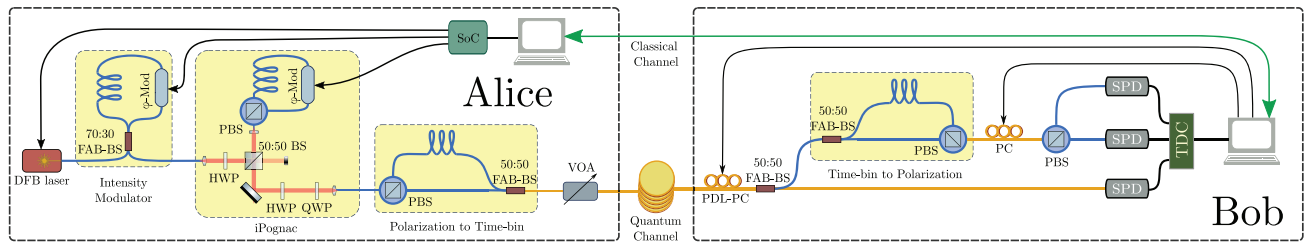
### 2.1. Transmitter

The laser source used at the transmitter is a gain-switched distributed feedback 1550 nm laser (Eblana EP1550-0-DM-H16-FM), emitting 100 ps FWHM pulses at  $R = 50$  MHz repetition rate. The state of these light pulses is then modulated by an encoder composed of three sections: an intensity modulator, a polarization encoder, and a polarization to time-bin conversion stage. The intensity modulator is based on a fiber-optic Sagnac loop and includes a 70:30 beamsplitter (BS), a lithium-niobate phase modulator (iXBlue MPZ-LN-10), and a 1m-long delay line.<sup>[34]</sup> This scheme implements the decoy state method with one decoy by setting two possible mean photon numbers (signal  $\mu = 0.60$  and decoy  $\nu = 0.18$ ) of the transmitted pulse. These parameters are chosen in such a way that their ratio is  $\mu/\nu \approx 3.33$  and the decoy intensity is sent with  $P_\nu = 30\%$  probability ( $P_\mu = 70\%$ ).

The second section, the iPOGNAC,<sup>[22]</sup> is used to modulate the polarization state of the light. The iPOGNAC offers fast polarization modulation with long-term stability, and a low intrinsic error rate, and, contrary to previous solutions, generates predetermined polarization states with a fixed reference frame in free-space. Moreover, it has also been tested in a field trial in an urban environment.<sup>[8]</sup> This polarization encoder relies on an unbalanced Sagnac interferometer containing a lithium-niobate phase modulator, and with the BS replaced by a fiber-based PBS with a polarization-maintaining (PM) optical fiber input and outputs. A free-space segment (Thorlabs FiberBench), composed of a BS and a HWP, ensures the light entering the loop has the diagonal state of polarization (SOP)  $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ . Hence, the light is equally split into the clockwise (CW) and counterclockwise (CCW) modes of the loop. Thanks to the asymmetry of the interferometer, by properly setting the voltage and the timing of the pulses driving the phase modulator, one can control the SOP exiting the device as follows

$$|\Phi_{\text{out}}^{\phi_{\text{CW}}, \phi_{\text{CCW}}}\rangle = \frac{1}{\sqrt{2}} (|H\rangle + e^{i(\phi_{\text{CW}} - \phi_{\text{CCW}})} |V\rangle) \quad (1)$$

where  $\phi_{\text{CW}}$  and  $\phi_{\text{CCW}}$  are the phases applied by the phase modulator to the CW and CCW propagating light pulses. In this experiment, the driving electric pulse amplitude was set to induce a  $\pi/2$



**Figure 1.** Experimental setup. BS, beam splitter; FAB-BS, fast-axis-blocking BS; PBS, polarization beam splitter;  $\phi$ -mod, phase modulator; H/QWP, half/quarter-wave plate; VOA, variable optical attenuator; PC, polarization controller; TDC, time-to-digital converter; SPD, single photon detector. Single mode fibers are in yellow, polarization maintaining fibers are in blue.

radians phase shift, allowing the iPOGnac to generate circular left  $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ , circular right  $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$  or diagonal  $|D\rangle$  polarized light. Before being coupled again into a PM optical fiber, a QWP and a HWP are used to transform circular left and right SOPs into horizontal  $|H\rangle$  and vertical  $|V\rangle$  SOPs, while  $|D\rangle$  remains unaltered. Such transformation is achievable due to the iPOGnac's long term stability and its ability to generate polarization states with a fixed reference frame.

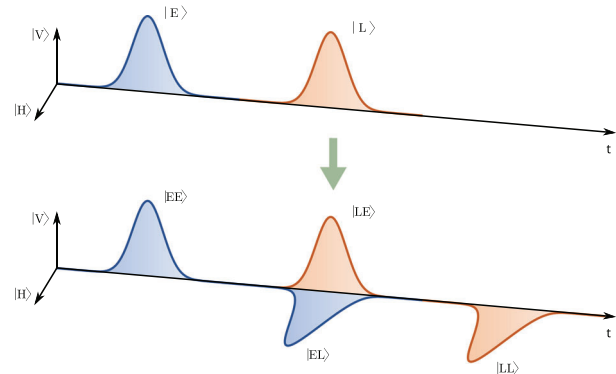
Finally, the transformation of polarization encoding to time-bin is performed. This is done by a PM fiber-based unbalanced Mach-Zehnder interferometer (UMZI) where the input element is a PBS, which maps horizontal and vertical components of the light into the early and late time slots of the 2D time-bin encoding

$$\alpha|H\rangle + \beta|V\rangle \rightarrow \alpha|E\rangle + e^{i\phi_A}\beta|L\rangle \quad (2)$$

where  $\phi_A$  is the intrinsic phase of Alice's UMZI, which also includes any relative phase induced by the polarization mode dispersion of the PM fiber before the UMZI. The imbalance of the MZI is  $\approx 2.5$  ns, obtained with a 0.5 long PM fiber. The scheme is thus able to generate the early  $|E\rangle$ , late  $|L\rangle$  time-bin states and the superposition of the two  $|+\rangle = (|E\rangle + e^{i\phi_A}|L\rangle)/\sqrt{2}$ . These states are sufficient to implement the 3-state efficient BB84 protocol<sup>[35]</sup> where the key generating basis  $\mathcal{Z} = \{|E\rangle, |L\rangle\}$  is sent with 90% probability and the control state  $|+\rangle$  is sent with 10% probability. The time-bin encoded signals are then attenuated down to the single-photon regime by a variable optical attenuator, then sent through the quantum channel.

It is important to note that after the conversion to time-bin, the polarization degree-of-freedom contains no information as all the light exiting the UMZI shares the same SOP. This is guaranteed by two factors. First, by design, the fiber-based PBS couples the orthogonal polarization modes into the slow-axis of the PM fiber outputs. Second, the BS used to recombine the two arms of the UMZI is a fast-axis blocking (FAB) device. FAB devices have the characteristic of discarding polarization states of the light that are aligned to the fast axis of the PM fiber, as if embedded with polarizers at both ends.

The whole system is managed by a computer, performing resource intensive tasks related to the protocol and handling classical communication. The electronic signals driving the laser and the modulators are controlled by a system-on-a-chip (SoC) which includes both a field programmable gate array (FPGA) and



**Figure 2.** Input and output state from the receiver's unbalanced Mach-Zehnder interferometer. Blue and red curves represent the two possible times of emission at the transmitter. The two lateral peaks correspond to a measurement in the key generating basis while the central peak is used to extract information on the control basis via a polarization measurement.

a CPU<sup>[36]</sup> and is integrated on a dedicated board (Zedboard by Avnet).

Compared to the polarization-based transmitter used in the urban environment QKD field trail reported in ref. [8], our setup only requires the addition of the UMZI for polarization to time-bin encoding conversion and a QWP and HWP to transform the output SOPs of the iPOGnac to those required by the UMZI. All of these components are fully passive and require no calibration after installation, rendering the conversion between the two degrees of freedom straightforward.

## 2.2. Receiver

At the receiver side, the measurement basis is randomly selected by a 50:50 FAB BS. One of its output ports is directly sent to a superconducting nanowire single photon detector (SNSPD) with  $\approx 80\%$  quantum efficiency (ID281 by ID Quantique). The overall time jitter of about 30 ps, considering both the detector and the time-to-digital converter (quTAG by Qtools), allows discrimination between the 2.5-ns-distant time-bins, effectively performing a measurement on the key generation basis as depicted in the upper half of **Figure 2**. This time-of-arrival measurement has the advantage of being independent of the polarization fluctuations introduced by the fiber-optic channel, and does not require active compensation.

The other output port of the basis-selection BS is sent to an UMZI that is identical to the one used at the transmitter. However, in this case the light is split equally between the two arms by the BS before being recombined by the PBS. Used in this way, the UMZI outputs horizontal or vertical SOPs depending on which arm light has traveled. Furthermore, as depicted in the lower half of Figure 2, the imbalance of the UMZI temporally distributes the light in the three-peak configuration often observed in time-bin experiments. Correspondingly, the output state from Bob's UMZI is

$$|\Psi_E\rangle = \frac{1}{\sqrt{2}}(|EE\rangle \otimes |V\rangle + e^{i\phi_B}|EL\rangle \otimes |H\rangle) \quad (3)$$

when Alice transmits  $|E\rangle$ ,

$$|\Psi_L\rangle = \frac{1}{\sqrt{2}}(|LE\rangle \otimes |V\rangle + e^{i\phi_B}|LL\rangle \otimes |H\rangle) \quad (4)$$

when Alice transmits  $|L\rangle$ , and

$$|\Psi_+\rangle = \frac{1}{2}(|EE\rangle \otimes |V\rangle + e^{i\phi_B}|EL\rangle \otimes |H\rangle + e^{i\phi_A}|LE\rangle \otimes |V\rangle + e^{i(\phi_A+\phi_B)}|LL\rangle \otimes |H\rangle) \quad (5)$$

when Alice transmits  $|+\rangle$ , where  $\phi_B$  is the intrinsic phase of Bob's UMZI. The lateral peaks  $|EE\rangle$  and  $|LL\rangle$  correspond to light traveling along the short or long arms of both transmitter and receiver's UMZI and since those times-of-arrival are a measurement in the  $\mathcal{Z}$  basis, they are used to generate the secret key.

Since 50% of the light falls in these lateral peaks, by taking into account both outputs of the FAB-BS, the overall probability of measuring in the key generation basis is 75%. Only the central peak contains the superposition between the indistinguishable early-late  $|EL\rangle$  and late-early  $|LE\rangle$  components, and the relative phase information between them is encoded in the polarization state of the light. In fact the output SOP of the central peak when  $|+\rangle$  is transmitted by Alice, is

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\theta}|V\rangle) \quad (6)$$

where  $\theta = \phi_A - \phi_B$  is the phase difference between Alice's and Bob's UMZIs. An all-fiber electronic polarization controller (PC) composed of four actuators (EPC-400 by OZ Optics) is then used to transform the polarization state  $|\psi\rangle$  into  $|D\rangle$  state and projected in the  $\{|D\rangle, |A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}\}$  basis. This projection is performed using a fiber PBS while the light signals are detected by two SNSPDs. Alternatively, a free-space setup with a liquid crystal, or a phase modulator with its fiber rotated by  $45^\circ$ <sup>[37]</sup> could be used instead of the PC. These solutions give the advantage of a simpler control scheme, due to the presence of a single degree of freedom, but would increase the losses at the receiver.

Contrary to the key generation basis, where no compensation is necessary, to perform the measurement in the control basis we need to actively compensate drifts of the relative phase shift  $\theta$  of the two interferometers. This is done by acting on the PC in front of the measurement PBS. A coordinate descent algorithm<sup>[38]</sup> is

used to minimize the measured QBER =  $N_A/(N_D + N_A)$  by controlling the state of the PC, where  $N_D$  ( $N_A$ ) is the number of counts in the detector associated with  $|D\rangle$  ( $|A\rangle$ ). This algorithm, described in ref. [21] was developed for polarization tracking in polarization-encoded fiber links, and was tested in an urban QKD field trial.<sup>[8]</sup> It starts operating without interrupting the QKD when the QBER exceeds 1%, and stops when it becomes smaller than 1%. In our implementation the QBER is calculated rapidly by exploiting a public string of states, known to both Bob and Alice that is interleaved with the exchange of secret qubits. The ratio between public and secret states is 4 to 36. However, it is important to consider that compensation in the control basis can be done without sharing any public string since the standard basis reconciliation procedure would reveal all the necessary information to estimate the QBER.<sup>[21,33]</sup> This approach would have the advantage of dedicating 100% of time to QKD, but could be prone to some latency due to the classical communication between Alice and Bob.

Polarization dependent losses (PDL) are present in the receiver. The first source of PDL is the use of SNSPDs since their quantum efficiency depends on the polarization of the impinging light.<sup>[39]</sup> A second source of PDL is the UMZI used for time-bin to polarization conversion since it discards fast-axis polarized light. Since the latter PDL mainly affects the control basis, the effective measurement probability for each basis would depend on the SOP of the photons that arrive from the quantum channel. This can be a security concern, since an eavesdropper could manipulate the SOP in the channel to prevent Bob from measuring the attacked states in the control basis, thus gaining information on the key without increasing the QBER. To avoid this, in our implementation the basis-selection BS is, as mentioned, FAB, meaning that only the slow-axis polarized light is measured in either basis, equalizing the PDL for both measurement bases.

To mitigate the PDL, which affects the detection rate but does not influence the measurement outcome, a PC (labeled as PDL-PC in Figure 1) is placed in front of the receiver. This element simply maximizes the total detection rate using a coordinate descent algorithm in real-time using Bob's raw local data without requiring qubit decoding and postprocessing nor any communication with the transmitter. Similar PDL and mitigation strategies have been used in other time-bin encoded QKD experiments.<sup>[4,40,41]</sup> It is important to note that PDL-PC is not involved in the measurement procedure but it is only a countermeasure to the possible degradation in the count rate due to polarization fluctuations. Another way to mitigate the detection rate fluctuations would be to apply a real time selection protocol<sup>[42,43]</sup> to select the intervals with higher transmissivity, enabling a secure QKD implementation without requiring active polarization compensation but sacrificing the performance of the QKD system. Here, however, we chose to actively compensate the polarization to guarantee the highest possible SKR throughout the experiment.

The temporal synchronization is achieved using the Qubit4Sync algorithm.<sup>[32]</sup> This implies that the two parties do not need a shared clock reference such as a pulsed laser.<sup>[6,7,29]</sup> Alice's clock period is recovered by Bob only using the time-of-arrival of qubits while the relative delay is recovered by sending an initial public string encoded in the first  $10^6$  states of the QKD transmission. The Qubit4Sync algorithm was originally

**Table 1.** Experimental results of the cross-encoded QKD system during the 12 h run.

Parameter	Mean value	Standard deviation
QBER $\mathcal{Z}$ [%]	0.76	0.08
QBER $ +\rangle$ [%]	0.79	0.65
SKR [kbps]	16.0	1.6
$R_{\text{det}}$ [kHz]	80.0	4.8

developed to work with polarization-based QKD systems, making this work the first implementation of the the technique for time-bin encoded systems.

We used this hybrid time-bin to polarization scheme in the receiver to decouple the needed interferometer with the phase compensation mechanism. This is different from most time-bin encoded receivers since the phase tracking is often performed by acting on the interferometer itself, using devices like fiber stretchers<sup>[29]</sup> or phase modulators<sup>[19]</sup> inserted in one of the optical paths. We find that our approach of having an interferometer that is completely passive comes with at least two advantages. First of all, it can be fully isolated from the environment, improving its overall phase stability. Second, the receiver can be developed using the components of polarization-based receivers. In fact, compared to the receivers such as the ones employed in refs. [8, 21], our hybrid QKD scheme only requires the addition of the UMZI for time-bin to polarization conversion, as well as a slight rearrangement of the optical components. It is also important to note that our scheme and the setups in refs. [8, 21] use the same number of PCs, and the control of these devices is performed using the same algorithm.

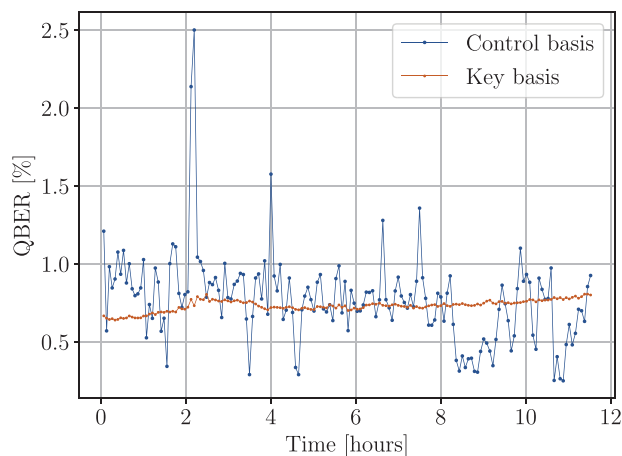
Similar hybrid decoding schemes have also been proposed or implemented in the context of time-bin and energy-time entanglement purification<sup>[44,45]</sup> and for non-local Bell-state analysis in entanglement-based one-step quantum secure direct communication (QSDC).<sup>[46,47]</sup>

### 3. Results

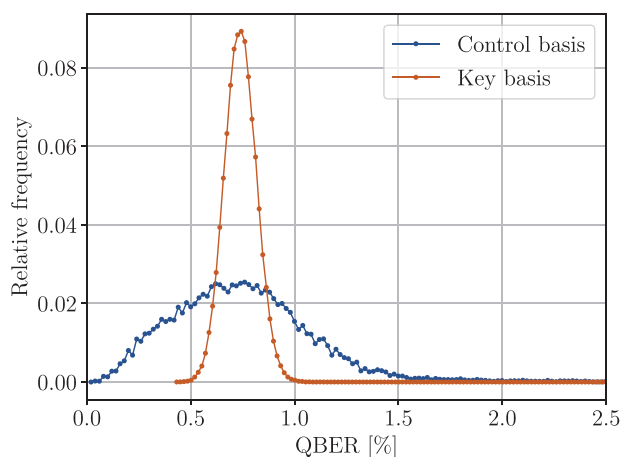
To test the performances of the developed cross-encoded QKD system, we performed a 12-h-long QKD run exploiting a quantum channel that consisted of a 50 km spool of single mode optical fiber (SM G.652.D) with  $0.2 \text{ dB km}^{-1}$  attenuation and 10 dB of additional attenuation. A summary of the main results obtained in this experiment can be found in **Table 1**.

The mean detection rate  $R_{\text{det}}$  was of  $8 \times 10^4$  events per seconds. Considering that on average the source emitted  $(\mu P_{\mu} + \nu P_{\nu}) \times R = 2.37 \times 10^7$  photons per second, the measured total losses were  $\approx 25$  dB. The channel contribution to these losses is about 20 dB, while the remaining 5 dB can be attributed to detectors efficiencies, insertion losses of optical components, and fiber mating sleeves.

The temporal evolution of the QBER on the key generation basis and on the control state is reported in **Figure 3**, while in **Figure 4** their distribution is reported. The  $\mathcal{Z}$  basis QBER averages 0.765% and remains stable throughout the whole experimental run, with a standard deviation of the 0.078%. The control basis QBER takes greater values, with an average of 0.792%, and dis-



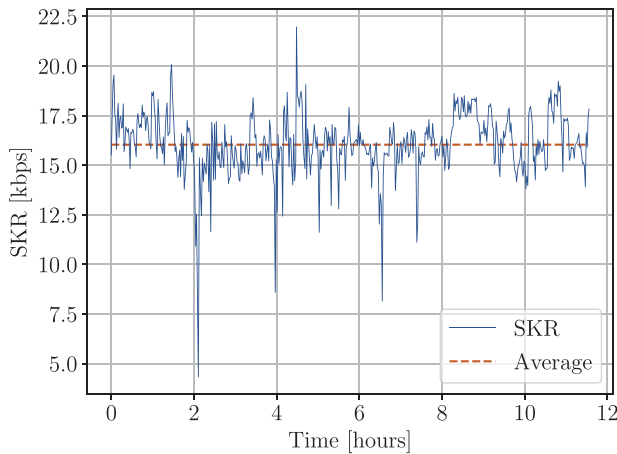
**Figure 3.** Temporal evolution for the quantum bit error rate (QBER) of the key generating basis and of the control state measured every 260 s. The averages are 0.765% and 0.792% for the key generating basis and control state, respectively.



**Figure 4.** Histogram of the distribution of the quantum bit error rate (QBER) of the key generating basis and of the control state.

tributes over a wider range, with a standard deviation of 0.651%. Furthermore, it can be observed that the  $\mathcal{Z}$  basis QBER is  $\leq 1\%$  for more than 99.8% of the time without any compensation, while the QBER of the actively compensated control state is  $\leq 1\%$  for 81% of the time, and  $\leq 2.5\%$  for 99.2% of the time. These results certify the stability of our system and its capacity of correcting the phase drifts of the UMZIs.

The  $\mathcal{Z}$  basis QBER stability is inherited from the characteristics of the iPOGNAC polarization modulator used to encode the qubit states, as well as to the resistance to fluctuations of time-bin encoding. This also demonstrates the robustness of the Qubit4Sync temporal synchronization method, which enabled highly accurate time-of-arrival measurements. On the other hand, fluctuations are observed for the control state QBER, mainly caused by phase drifts of the UMZIs. However, our polarization-tracking techniques effectively compensated these drifts, without ever interrupting the QKD. The spikes in measured QBER can be attributed to the compensation algorithm



**Figure 5.** Secret key rate (SKR) measured on sifted key blocks of  $4 \times 10^6$  bits (corresponding to approximately 80 s of acquisition). An average rate of around 16 kbps was observed.

that in some cases struggles to follow rapid phase fluctuations and performs erroneous corrections with the APC.

The post-processing uses a modified version of the AIT QKD R10 software suite<sup>[48]</sup> following the finite-size analysis of ref. [49]:

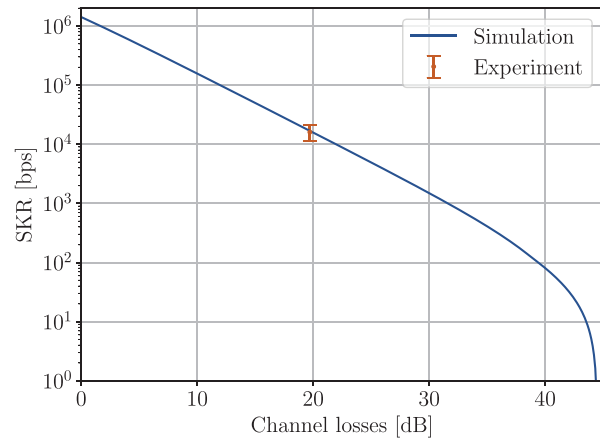
$$\text{SKR} = \frac{1}{t} [s_0 + s_1(1 - h(\phi_z)) - \lambda_{\text{EC}} - \lambda_c - \lambda_{\text{sec}}] \quad (7)$$

where terms  $s_0$  and  $s_1$  are the lower bounds on the number of vacuum and single-photon detection events in the key generating  $\mathcal{Z}$  basis,  $\phi_z$  is the upper bound on the phase error rate in the  $\mathcal{Z}$  basis corresponding to single photon pulses,  $h(\cdot)$  is the binary entropy,  $\lambda_{\text{EC}}$  and  $\lambda_c$  are the number of bits published during the error correction and confirmation of correctness steps,  $\lambda_{\text{sec}} = 6 \log_2(\frac{19}{\epsilon_{\text{sec}}})$  with  $\epsilon_{\text{sec}} = 10^{-10}$  is the security parameter associated to the secrecy analysis, and finally  $t$  is the duration of the quantum transmission phase. Equation (7) is applied to  $4 \times 10^6$ -bit-long key blocks, a value that was chosen to produce new secret keys at a rapid pace, approximately every 80 s. Increasing this value by a factor of ten would have improved the SKR by about 20%, at the cost of a much higher delay between the beginning of the experiment and the production of the first key. The SKR obtained during the experiment is shown in **Figure 5**.

It can be observed that our cross-encoded QKD system successfully generated secure keys without interruptions throughout the 12 h of the experimental run and achieved an average SKR of around 16 kbps. This result is consistent with our simulation of the performance of the system, which also predicts its behavior for different values of the channel losses, shown in **Figure 6**. The simulation makes the strong assumption that the compensation mechanisms maintain their good performance also in conditions of strong losses, but this is in agreement with previous experiments in which the same algorithms were used for polarization correction and synchronization.<sup>[21,32]</sup>

## 4. Conclusions

In this work we described a novel cross-encoded QKD scheme, based on the conversion between time-bin and polarization de-



**Figure 6.** Simulation of the SKR as function of the channel losses. All other physical parameters are fixed and depend on the features of the experimental setup. The error bar associated to the experimental data point represents three times the standard deviation.

grees of freedom, that implements the one-decoy, three-state BB84 protocol.<sup>[33]</sup> By exploiting the temporally stable iPOGNAC polarization encoder we obtained polarization qubits with low error,<sup>[22]</sup> that were converted to time-bin to allow transmission that is immune to the birefringence of the fiber-optic channel. We implemented a hybrid receiver that performed time-of-arrival measurements for key generation as well as polarization measurements for the control states. In such scheme, channel polarization fluctuations will not influence measurement outcomes, but only affect the detection rate. Temporal synchronization was successfully achieved with the Qubit4Sync method<sup>[32]</sup> making our work the first implementation of time-bin encoded QKD that does not require dedicated hardware to share a temporal reference between the transmitter and the receiver. The developed system was tested on a 12-h run using a 50 km fiber spool, showing a stable QBER of 0.765% in the key basis and 0.792% in the control state, and achieving an average SKR of of  $\approx 16$  kbps without interruptions.

This scheme can represent an important enabling technology for the envisioned continental-scale hybrid quantum networks that employ both fiber-optics and free-space links<sup>[9,50]</sup> to implement protocols such as QKD<sup>[2,3]</sup> and QSDC.<sup>[51,52]</sup> In fact, since the qubit modulation of our transmitter is based on the iPOGNAC, it can be promptly reconfigured to transmit polarization-encoded qubits for free-space scenarios or, as demonstrated in this work, to convert them to time-bin for efficient propagation in an optical fiber. Similarly, our hybrid receiver allows for time-bin state decoding exploiting the optical components and methods already exploited in polarization-based receivers. In this way our system is compatible with any quantum channel and the best possible encoding scheme can be chosen according to the characteristics of the link. Last, the polarization to time-bin conversion here presented can be used to relay quantum signals from optical ground stations to fiber-based networks. In this way, users would gain access to satellite-based quantum communication networks without requiring installation of costly telescopes and tracking systems while maintaining an optimal encoding for both the free-space and the fiber link.

## Acknowledgements

Part of this work was supported by: MIUR (Italian Minister for Education) under the initiative “Departments of Excellence” (Law 232/2016); Agenzia Spaziale Italiana (2018-14-HH.0, CUP: E16J16001490001, *Q-SecGroundSpace*; 2020-19-HH.0, CUP: F92F20000000005, *Italian Quantum CyberSecurity I-QKD*). The AIT Austrian Institute of Technology is thanked for providing the initial elements of the post-processing software used here.

Open Access Funding provided by Universita degli Studi di Padova within the CRUI-CARE Agreement.

## Conflict of Interest

The authors declare no conflict of interest.

## Author Contributions

D.S. and C.A. contributed equally to this work. C.A., M.A., G.V., and P.V. designed the transmitter. C.A., D.S., and M.A. designed the receiver. A.S., M.A., and D.S. developed the transmitter electronics and the FPGA-based control system. L.C., D.S., and C.A. developed the transmitter and receiver control software. G.F. developed the post-processing and simulation software. D.S. performed the experiment. All authors discussed the results. C.A. and D.S. wrote the manuscript with inputs from all the authors.

## Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## Keywords

encoding conversion, polarization, quantum communications, quantum key distribution, quantum optics, qubit-based synchronization, time-bin

Received: May 23, 2022

Revised: September 13, 2022

Published online: October 17, 2022

- [1] R. Renner, *Ph.D. Thesis*, Institut für Theoretische Informatik - Eidgenössische Technische Hochschule (ETH), Zürich **2005**.
- [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.
- [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, *Adv. Opt. Photonics* **2020**, *12*, 1012.
- [4] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, et al., *Opt. Express* **2011**, *19*, 10387.
- [5] 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, D. Englund, *Phys. Rev. X* **2018**, *8*, 021009.
- [6] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greiße, I. H. White, R. V. Pentyl, A. J. Shields, *npj Quantum Inf.* **2019**, *5*, 101.
- [7] D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, A. Zavatta, *EPJ Quantum Technol.* **2019**, *6*, 5.
- [8] M. Avesani, L. Calderaro, G. Foletto, C. Agnesi, F. Picciariello, F. B. L. Santagiustina, A. Scriminich, A. Stanco, F. Vedovato, M. Zahidy, G. Vallone, P. Villoresi, *Opt. Lett.* **2021**, *46*, 2848.
- [9] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, et al., *Nature* **2021**, *589*, 214.
- [10] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, H.-F. Zhang, K. Cui, H. Liang, X.-G. Li, Y. Mao, L.-J. Wang, S.-B. Feng, Q. Chen, Q. Zhang, L. Li, N.-L. Liu, C.-Z. Peng, X. Ma, Y. Zhao, J.-W. Pan, *npj Quantum Inf.* **2021**, *7*, 134.
- [11] Such as, for example, ThinkQuantum, KETS and qtlabs.
- [12] C. H. Bennett, G. Brassard, *Theor. Comput. Sci.* **2014**, *560*, 7.
- [13] Y.-H. Gong, K.-X. Yang, H.-L. Yong, J.-Y. Guan, G.-L. Shentu, C. Liu, F.-Z. Li, Y. Cao, J. Yin, S.-K. Liao, J.-G. Ren, Q. Zhang, C.-Z. Peng, J.-W. Pan, *Opt. Express* **2018**, *26*, 18897.
- [14] H. Ko, K.-J. Kim, J.-S. Choe, B.-S. Choi, J.-H. Kim, Y. Baek, C. J. Youn, *Sci. Rep.* **2018**, *8*, 15315.
- [15] 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. Soriano, F. Vedovato, G. Vallone, P. Villoresi, *npj Quantum Inf.* **2021**, *7*, 93.
- [16] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steinbrecher, G. Kirchner, C.-Y. Lu, R. Shu, et al., *Phys. Rev. Lett.* **2018**, *120*, 030501.
- [17] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, A. Zeilinger, *Opt. Express* **2006**, *14*, 10050.
- [18] X. Liu, C. Liao, J. Mi, J. Wang, S. Liu, *Phys. Lett. A* **2008**, *373*, 54.
- [19] 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, Z.-F. Han, *Opt. Lett.* **2018**, *43*, 2030.
- [20] Y. Li, Y.-H. Li, H.-B. Xie, Z.-P. Li, X. Jiang, W.-Q. Cai, J.-G. Ren, J. Yin, S.-K. Liao, C.-Z. Peng, *Opt. Lett.* **2019**, *44*, 5262.
- [21] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, P. Villoresi, *Optica* **2020**, *7*, 284.
- [22] M. Avesani, C. Agnesi, A. Stanco, G. Vallone, P. Villoresi, *Opt. Lett.* **2020**, *45*, 4706.
- [23] The iPOGNAC is object of the Italian Patent No. 102019000019373 filed on 21.10.2019 as well as of the International Patent Application no. PCT/EP2020/079471 filed on 20.10.2020.
- [24] Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, Z.-F. Han, *Opt. Express* **2017**, *25*, 27923.
- [25] G. B. Xavier, G. Vilela de Faria, G. P. Temporão, J. P. von der Weid, *Opt. Express* **2008**, *16*, 1867.
- [26] Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. Li, S. Wang, Z.-Q. Yin, G.-C. Guo, Z.-F. Han, *Opt. Lett.* **2017**, *42*, 1023.
- [27] 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, J.-H. Liu, *Opt. Express* **2018**, *26*, 22793.
- [28] C. H. Bennett, *Phys. Rev. Lett.* **1992**, *68*, 3121.
- [29] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussiè, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Phys. Rev. Lett.* **2018**, *121*, 190502.
- [30] V. Makarov, A. Brylevski, D. R. Hjelm, *Appl. Opt.* **2004**, *43*, 4385.

- [31] G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, P. Villoresi, *Phys. Rev. Lett.* **2016**, *116*, 253601.
- [32] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, G. Vallone, *Phys. Rev. Appl.* **2020**, *13*, 054041.
- [33] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2018**, *112*, 051108.
- [34] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, A. J. Shields, *Opt. Lett.* **2018**, *43*, 5110.
- [35] C. H. F. Fung, H.-K. Lo, *Phys. Rev. A* **2006**, *74*, 042342.
- [36] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, P. Villoresi, *IEEE Trans. Quantum Eng.* **2022**, *3*, 6000108.
- [37] A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, Y. Kurochkin, *Opt. Express* **2017**, *25*, 28886.
- [38] S. J. Wright, *Math. Program.* **2015**, *151*, 3.
- [39] V. Anant, A. J. Kerman, E. A. Dauler, J. K. W. Yang, K. M. Rosfjord, K. K. Berggren, *Opt. Express* **2008**, *16*, 10750.
- [40] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, A. J. Shields, *Opt. Express* **2012**, *20*, 16339.
- [41] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, A. J. Shields, *Opt. Express* **2015**, *23*, 7583.
- [42] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, P. Villoresi, *Phys. Rev. A* **2015**, *91*, 042320.
- [43] W. Wang, F. Xu, H.-K. Lo, *Phys. Rev. A* **2018**, *97*, 032337.
- [44] Y.-B. Sheng, L. Zhou, *Laser Phys. Lett.* **2014**, *11*, 085203.
- [45] S. Ecker, P. Sohr, L. Bulla, R. Ursin, M. Bohmann, *Phys. Rev. Appl.* **2022**, *17*, 034009.
- [46] Y.-B. Sheng, L. Zhou, G.-L. Long, *Sci. Bull.* **2022**, *67*, 367.
- [47] L. Zhou, Y.-B. Sheng, *Sci. China: Phys., Mech. Astron.* **2022**, *65*, 250311.
- [48] AIT QKD R10 Software, <https://sq.ait.ac.at/software/projects/qkd> (accessed: May 2022).
- [49] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2018**, *112*, 171104.
- [50] S. Wehner, D. Elkouss, R. Hanson, *Science* **2018**, *362*, eaam9288.
- [51] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, G.-C. Guo, *Phys. Rev. Lett.* **2017**, *118*, 220501.
- [52] H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, J. Lu, *Light Sci. Appl.* **2022**, *11*, 83.