Time-bin Quantum Key Distribution exploiting the iPOGNAC polarization moulator and Qubit4Sync temporal synchronization

Costantino Agnesi[1,*], Davide Scalcon[1,*], Marco Avesani[1], Luca Calderaro[1,†], Giulio Foletto[1], Andrea Stanco[1], Giuseppe Vallone[1,2], and Paolo Villoresi[1]

[1] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy*
[2] *Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, Padova, Italy*

[*] *These authors equally contributed to this work.*
[†] *Currently with ThinkQuantum S.r.l.*
Corresponding author: costantino.agnesi@unipd.it

Abstract: Here we present cross-encoded Quantum Key Distribution where state encoding is performed with a self-compensating and calibration-free polarization modulator, while transmission is performed in time-bin encoding resistant to perturbances from the fiber channel.

1. Introduction

Quantum Key Distribution (QKD) is a quantum technology that fosters disruptive potential for our telecommunication networks by allowing distant users to generate a shared secret key with unconditional security. Robust implementations of QKD systems are usually characterized by precise quantum state generation and measurement, as well as by a transmission scheme that is resistant to channel disturbances. This makes the encoding scheme choice non-trivial since it depends on several external factors such as the quantum channel and the performances of state generators. For example, stable and low-error encoders are available for polarization encoding, whereas time-bin encoding represent a good candidate for fiber-optic channels, as birefingence does not perturb this kind of states [1]. Here we present a cross-encoded scheme where the iPOGNAC, a self-compensating and calibration-free polarization modulator [2], is used to encode quantum states of high quality and a polarization to time-bin converter is used to transmit the quantum information without perturbances from the 50 km fiber spool used as the quantum channel. The implemented receiver is of a hybrid nature performing both time-of-arrival and polarization measurements to decode the quantum states. Furthermore, temporal synchronization between the two parties is performed with Qubits4Sync, a qubit-based method that does not require additional hardware to share a clock reference [3]. Our work enables the development of flexible QKD systems that can change the qubit encoding to best fit the characteristics of the quantum channel and represents an important step towards the development of hybrid QKD networks that employ both fiber-optical and free-space links.

2. Experimental Setup

Our cross-encoded QKD system is sketched in Fig. 1 with the transmitter, Alice, on the left and the receiver, Bob, on the right. It implements the three-state and one-decoy efficient BB84 protocol [4].

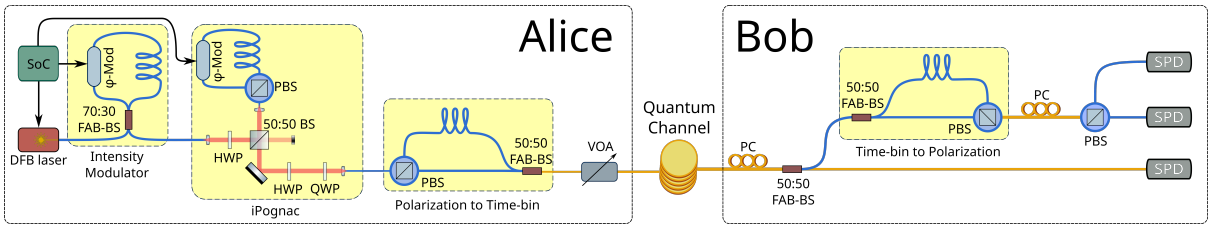


Fig. 1: Experimental setup. BS: beamsplitter, FAB-BS: fast-axis-blocking (polarizing) BS, PBS: polarization beamsplitter, ϕ-mod: phase modulator, H/QWP: half/quarter waveplate, VOA: variable optical attenuator, PC: polarization controller, SPD: single photon detector. Single mode fibers are in yellow, while polarization maintaining fibers are in blue.

2.1. Transmitter

A gain-switched laser generates optical pulses with 100 ps FWHM duration, 50 MHz repetition rate and 1550 nm wavelength. To implement the decoy-state scheme, the intensity of these pulses is modulated by a Sagnac-loop interferometer [5]. The polarization state of these light pulses is then modulated using the iPOGNAC encoder which 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. The modulated output states of polarization are circular left $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, circular right $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ or diagonal $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ [2]. By means of a Quarter Wave Plate (QWP) and a Half Wave Plate (HWP) $|L\rangle$ and $|R\rangle$ are transformed into horizontal $|H\rangle$ and vertical $|V\rangle$ polarization states, before being coupled again into a polarization-maintaining optical fiber. 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 Polarization Beam Splitter (PBS), which maps horizontal and vertical components of the light the early and late time slots of the two dimensional time-bin encoding

$$\alpha|H\rangle + \beta|V\rangle \longrightarrow \alpha|E\rangle + \beta|L\rangle. \tag{1}$$

The imbalance of the MZI is of ≈ 2.5 ns, obtained with 0.5 m of 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 $|+\rangle = (|E\rangle + |L\rangle)/\sqrt{2}$. These states are sufficient to implement the 3-state efficient BB84 protocol where the key generating basis $\{|E\rangle, |L\rangle\}$ 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 single-photon regime by a variable optical attenuator, then sent trough the quantum channel which in our experiment is composed of a 50km spool of single mode optical fiber with 0.2 dB/km attenuation and 10 dB of additional attenuation.

2.2. Receiver

A 50:50 beam splitter (BS) randomly the measurement basis at the receiver side. One of the ports is directly sent to a Superconducting Nanowires Single Photon Detector (SNSPD). The low time jitter of the detector (≈ 20 ps), combined with the 1 ps timing resolution of the time-to-digital converter enable a time-of-arrival measurements, which is a measurement in the key generation basis. Such a time-of-arrival measurement has the advantage of being independent of the polarization fluctuations introduced by the fiber channel and requires no active compensation. The other output port of the base-selection BS is sent to an UMZI that is identical to the one used at the transmitter but traversed in opposite direction. The imbalance of the UMZI temporally distributes the light in the three-peak configuration often observed in time-bin experiments where the two later peaks effectively correspond to time-of-arrival measurement, while the central peak contains relative phase information of the control basis encoded in the polarization state of the light

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

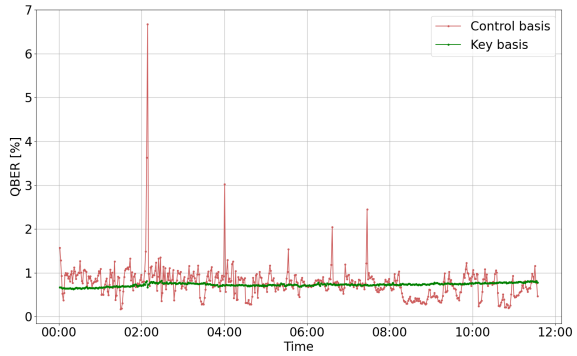
where θ is the phase difference between Alice's and Bob's UMZIs. The phase information is extracted by projecting the light into the $\{|\psi\rangle, |\psi^{\perp}\rangle = \left(|H\rangle - e^{i\theta}|V\rangle\right)/\sqrt{2}\}$ basis. This projection is performed using an all-fiber electronic Polarization Controller (PC) composed of 4 piezoelectric actuators, and a PBS while the light signals are detected by two SNSPDs.

Active drift compensation of the relative phase shift θ of the two interferometers is required to perform the measurement in the control basis. This is done by acting on the PC in front of the measurement PBS. The Quantum Bit Error Rate is minimized by acting upon the PC placed before the measurement PBS with an algorithm, developed for polarization tracking in polarization-encoded fiber links [6].

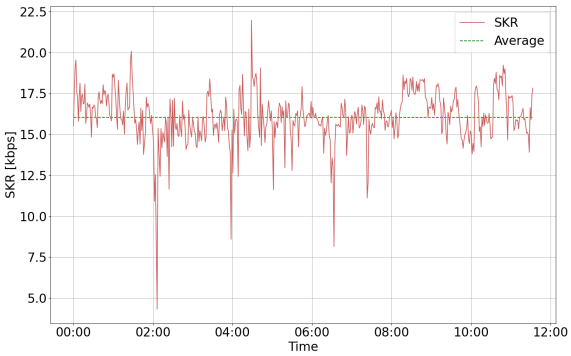
Temporal synchronization between the transmitter and the receiver is achieved by exploiting a slightly modified version of the Qubit4Sync algorithm [3]. In this way the two parties do not need a shared clock reference such as a pulsed laser or a GNSS clock. Alice's clock is recovered by Bob only using the time-of-arrival of qubits while the absolute time is recovered by sending an initial public string encoded in the first 10^6 states of the QKD transmission.

3. Results

We performed a 12-hours-long QKD run to test the performances of our system. The temporal evolution of the QBER on the key generation basis and on the control state is reported in Fig. 2a. The key generation basis QBER averages 0.765% and remains stable throughout the whole experimental run. This stability is inherited from the characteristics of the iPOGNAC polarization modulator used to encode the qubit states, as well as to the resilience to polarization fluctuations of time-bin encoding. This stability also demonstrates the robustness of the Qubit4Sync



(a) Temporal evolution for the QBER of the key generating basis averaging 0.765%, and of the control state averaging 0.792%.



(b) Temporal evolution for the SKR averaging 16 kbps.

Fig. 2: Experimental results during a 12-hour run with measurements every 80 seconds.

temporal synchronization method that enabled highly accurate time-of-arrival measurements without requiring any additional hardware to share a reference clock between the two parties. On the other hand, fluctuations are observed for the control state QBER. These are mainly caused by phase drifts of the UMZIs. However, our polarization tracking techniques effectively compensated these drifts and achieved an average QBER of 0.792% without ever interrupting the QKD. The temporal evolution of the obtained SKR is shown in Fig. 2b. It can observed that our cross-encoded QKD system successfully generated secure keys without interruptions throughout the 12 hours of the experimental run and achieved an average SKR of around 16 kbps.

4. Conclusions

In this work we described a novel cross-encoded QKD scheme, based on the conversion between polarization and time-bin degrees of freedom. This enabled us to exploit the iPOGNAC for stable and low-error state-generation [2] and transmission that is immune to the birefringence of the fiber optic channel by exploiting time-bin encoding. Additionally, by using the Qubit4Sync method [3], our work represents the first implementation of time-bin encoded QKD that does not require additional hardware to share a temporal reference between the transmitter and the receiver. The developed system was tested on a 12 hour run using a 50 km fiber spool, demonstrating a stable low QBER, and achieving an average SKR of of around 16 kbps without interruptions.

Since the qubit modulation capacities of our transmitter are based on the iPOGNAC, it can be promptly reconfigured to transmit polarization-encoded qubits for free-space transmission or, as demonstrated here, to convert them to time-bin for efficient propagation in an optical fiber. Therefore, the methods presented in this work represent an important enabling technology for the envisioned continental-scale hybrid quantum networks that employ both fiber-optical and free-space links [7].

References

1. S. Pirandola *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012-1236 (2020).
2. M. Avesani *et al.*, "Stable, low-error, and calibration-free polarization encoder for free-space quantum communication," Opt. Lett. **45**, 4706-4709 (2020).
3. L. Calderaro *et al.*, "Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution," Phys. Rev. Applied **13**, 054041 (2020).
4. F. Grünenfelder *et al.*, "Simple and high-speed polarization-based QKD," Appl. Phys. Lett. **112**, 051108 (2018).
5. G. L. Roberts *et al.*, "Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution," Opt. Lett. **43**, 5110-5113 (2018).
6. C. Agnesi *et al.*, "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder," Optica **7**, 284-290 (2020).
7. S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science **362**, eaam9288 (2018).