# Simple and robust QKD system with Qubit4Sync temporal synchronization and the POGNAC polarization encoder

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

*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy*

[*] *These authors contributed equally to this work.,*
[†] *Corresponding author: costantino.agnesi@phd.unipd.it*

**Abstract:** Here we present a simple and robust polarization encoded QKD system that performs synchronization, polarization compensation and QKD with the same optical setup without requiring any changes or any additional hardware. 

**OCIS codes:** 270.5568, 270.5565.

## 1. Introduction

The security of our communication networks is of strategic importance for our modern societies. Commercial and financial transactions, military and diplomatic operations, and the everyday privacy of ordinary citizens depends on the strength of current cyber-security standards. However, technological advances, mainly the development of the quantum computer, can render our modern cyber-security systems obsolete. In fact, algorithms that exploit quantum resources can be developed to crack the mathematical problems that are at the basis of most cryptographical schemes [1]. Quantum Key Distribution (QKD), that allows two distant parties to distill perfectly secret key by exchanging qubits, is the only cryptographic technique that can guarantee unconditional security based exclusively on the laws of quantum mechanics [2]. Furthermore, QKD is future-proof since algorithmic and technological advances for both classical and quantum computation do not threaten the security of the protocol.

Growing interest from the private and public sectors has led to a fast-paced development of QKD, with the current state-of-the-art prototypes aiming for compatibility with telecommunication networks and the development of a global-scale quantum internet [3]. However, wide-spread deployment of QKD in our current telecommunication networks will require the development of simpler and more robust systems. In fact, many recent studies have focused on developing setups with high intrinsic stability and, by minimizing the number of components, preventing non-idealities and performance drifts. Nevertheless, essential auxiliary tasks, such as temporal synchronization and polarization basis tracking, are generally assigned to separate sub-systems. These sub-systems are often composed of additional lasers and require intricate time or wavelength multiplexing schemes, which add unwanted complexity to the QKD setups.

To address these issues, here we present a simple and robust polarization encoded QKD experiment exploiting a 26 km fiber-optic link where synchronization, polarization compensation and QKD are all performed with the same optical setup, without requiring any changes or any additional hardware and develop exclusively with commercial off-the-shelf (COTS) components [4]. The QKD source is comprised of the POGNAC polarization modulator, which exhibits high stability and a low intrinsic Quantum Bit Error Rate (QBER) [5]. The temporal synchronization is performed using the Qubit4Sync method, with no need for auxiliary time reference, by sending a public qubit sequence at pre-established times [6]. Predetermined qubit sequences are also exploited to monitor and compensate the polarization drift introduced by the 26 km of optical fiber. The reduced complexity of both the transmitter and the receiver, as well as the robustness and stability demonstrated by our implementation, represent an important technological step towards mature QKD systems fully compatible with the our current telecommunication networks.

## 2. Experimental setup

We implement the simplified three-state and one-decoy BB84 protocol [7] with the setup represented in Fig. 1. At Alice's side, a 1550 nm gain-switched laser generates a stream of pulses at 50 MHz repetition rate. An intensity modulator (IM) then sets the intensity levels required by the decoy-state method. The polarization modulation is performed with the POGNAC [5], which allows us to generate, with high fidelity, the $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$,

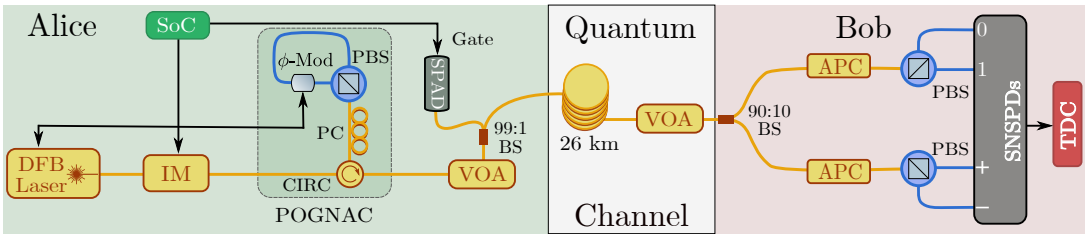



Fig. 1: Our simple and robust QKD implementation fully developed with COTS components.

$|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ states by carefully timing the applied voltage on a phase modulator ($\phi$-Mod). A variable optical attenuator (VOA) then 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 Single Photon Avalanche Diode (SPAD), while the other output port is directed to 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 VOA, which allows us to simulate further channel loss. Bob's setup instead consists of a 90:10 fiber BS which sets the detection probabilities of the two measurement bases accordingly. Each output arm of the BS is connected to an automatic polarization controller (APC) and a polarizing beam splitter (PBS) which perform the required projective measurements. The four outputs are finally sent to four superconductive nanowire single-photon detectors (SNSPDs) and recorded by a time-to-digital converter (TDC) with 1 ps temporal resolution.

## 3. Temporal Synchronization

A pulsed laser or a GNSS clock are usually employed to share an external time reference between the communicating parties. In our implementation, however, we exploit the Qubit4Sync algorithm to synchronize Alice and Bob's clocks using the same qubits exchanged during the QKD protocol [6]. For a successful temporal synchronization, Bob needs to determine the transmission frequency and the absolute time at which the first qubit should arrive. For the former, we compute the frequency from the time-of-arrival measurements. For the latter, we send an initial public string encoded in the first $L$ states and correlate it with what Bob received, allowing us to determine the first one that was sent by Alice. Such technique is typically used, for instance, by the GPS receiver to synchronize with the satellite signal [8]. The novelty of Qubit4Sync is the implementation of a fast correlation algorithm requiring lower computational cost than the algorithms which allows real-time operation and copes with the high losses of a quantum channel.

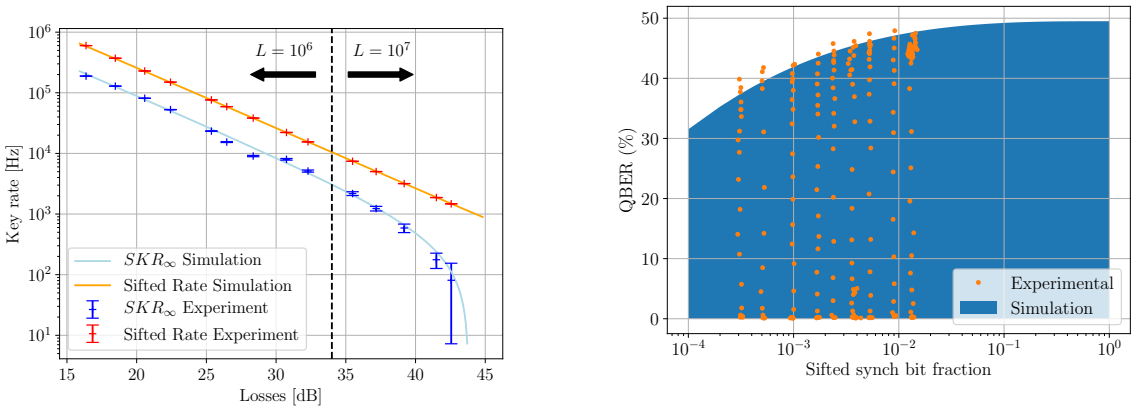
## 4. Polarization basis tracking

Mechanical and temperature fluctuations transform the polarization state of the photons that travel through the fiber. As a result, the QBER increases, up to the point where no quantum secure key can be established. Our QKD prototype here presented uses a compensation scheme that exploits a shared public string. Every second, the shared string of $10^6$ states is transmitted by Alice and detected by Bob. In addition to the bits revealed during the standard reconciliation procedure, Bob can use this shared string to calculate the QBER. The estimated QBER values are then fed into an optimization algorithm which controls Bob's APCs.

## 5. Results

To test the performances of our simple QKD system, several runs were executed each with increased losses. The losses were added increasing the attenuation of the VOA after the 26 km of fiber. For each run the Secure Key Rate ($SKR_\infty$) was calculated in the asymptotic limit. The results are presented in Fig. 2a, where the crosses represent the experimental runs, while the lines are generated by simulations. Using a synchronization string of length $L = 10^6$, we performed several QKD runs with losses up to 34 dB. Instead, with a longer string of $L = 10^7$, we successfully ran QKD protocols up to the channel loss at which the key rate drops to zero. In the QKD run with highest losses, we achieved a secure key rate of 80 bits per second at 43 dB total channel losses, corresponding to about 215 km of SMF28 fiber (0.2 dB/km) or 253 km of ultra low-loss fiber (0.17 dB/km).

We also tested the robustness of the Qubit4Sync synchronization algorithm by tuning the QBER and the number of received bits. In Fig. 2b, the results of the simulation are highlighted by the blue region, corresponding to the values of QBER and received bit fraction in which the algorithm is expected to work. On the other hand, the orange dots represent successful synchronization trials of our QKD system. The simulation shows a good outcome of the analysis up to $10^{-4}$ sifted synchronization bit fraction for $L = 10^6$. This is no longer true for high value of the QBER. With over 30% of QBER, the algorithm needs more bits to contrast the reduction of the maximum




(a) Sifted rate and $SKR_\infty$ as a function of total channel losses. (b) Qubit4Sync robustness for several QBERs and bit fractions.

Fig. 2: Experimental results obtained with our simple and robust QKD implementation.

correlation due to the bits flip. The background detection comes into play in the experimental runs, reducing the amount of losses the algorithm can tolerate. In our case, the analysis fails below a sifted synchronization bits ratio of $3 \times 10^{-4}$, with 200 Hz of free-running background detection rate. It is interesting to note the very high robustness to the QBER, well above the $\approx 11\%$ threshold to establish a secure channel. In fact, a very rough alignment between transmitter and receiver is sufficient for the synchronization to take place.

## 6. Conclusions

Here, we have presented a simple polarization encoded QKD implementation that exploits the Qubit4Sync temporal synchronization [6] and the POGNAC polarization encoder [5]. Its simple design, fully realized with COTS components, reduces the complexity for both the QKD transmitter and receiver. In fact, the same optical setup is used for the tasks of synchronization, polarization compensation and QKD, without requiring changes to the working parameters of the setup, or additional hardware. Our results prove that the Qubit4Sync method properly works even at the highest losses tolerated by our QKD system. The simplicity of our QKD implementation renders it compatible with many different scenarios, ranging from urban QKD fiber links [9] to free-space QKD [10], where simplicity and stability are of critical importance. Lastly, our prototype could be of interest for the development of the Italian Quantum Backbone [11], a fiber-based infrastructure connecting the National Institute of Metrological Research (INRIM) in Turin with the Space Center of the Italian Space Agency (ASI) in Matera.

## References


1. A. Ekert and R. Jozsa, "Quantum algorithms: entanglement–enhanced information processing," Philos. Trans. R. Soc. A **356**, 1769 (1998).
2. V. Scarani *et al.*, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301 (2008).
3. S. Pirandola *et al.*, "Advances in Quantum Cryptography," arXiv:1906.01645 (2019).
4. C. Agnesi, M. Avesani, L. Calderaro *et al.*, "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder," arXiv:1909.12703 (2019).
5. C. Agnesi, M. Avesani *et al.*, "All-fiber self-compensating polarization encoder for quantum key distribution," Opt. Lett. **44**, 2398 (2019).
6. L. Calderaro *et al.*, "Fast and simple qubit-based synchronization for quantum key distribution," arXiv:1909.12050 (2019).
7. F. Grünenfelder *et al.*, "Simple and high-speed polarization-based QKD," Appl. Phys. Lett. **112**, 051108 (2018).
8. H. Hassanieh *et al.*, "Faster GPS via the sparse Fourier transform," in Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, Mobicom '12 (ACM, 2012) pp. 353–364.
9. D. Bunandar *et al.*, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
10. M. Avesani *et al.*, "QCoSOne: a chip-based prototype for daylight free-space QKD at telecom wavelength," in Frontiers in Optics + Laser Science APS/DLS, OSA Technical Digest (Optical Society of America, 2019), paper FTu6A.2. [arXiv:1907.10039]
11. D. Calonico, "A fibre backbone in Italy for precise time and quantum key distribution," in 4th ETSI/IQC Workshop on Quantum-Safe Cryptography, Toronto, 19-21 September 2016. ⟨https://docbox.etsi.org/Workshop/2016/201609_QUANTUMSAFECRYPTO/TECHNICAL_TRACK/INRIM_Calonico.pdf⟩