Simple and robust **QKD** with ***Qubits4Sync*** temporal synchronization and the ***POGNAC polarization encoder***

Costantino AGNESI
QuantumFuture Research Group

Department of Information Engineering
University of Padua

C. Agnesi *et al.*,
Optica **7**(4), 284 (2020)

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

UNIVERSITÀ DEGLI STUDI DI PADOVA

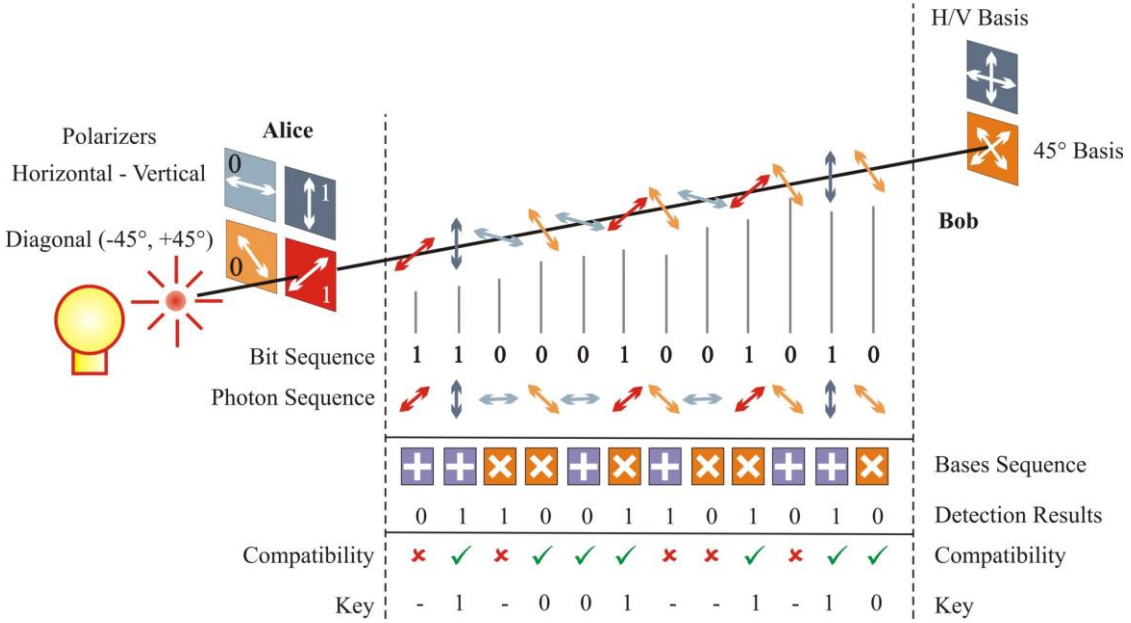
Quantum Communications

- New paradigm with the potential to resolve many of the problems of communications such as privacy, secrecy and integrity of messages by exploiting quantum resources.

Quantum Communications

- New paradigm with the potential to resolve many of the problems of communications such as privacy, secrecy and integrity of messages by exploiting quantum resources.

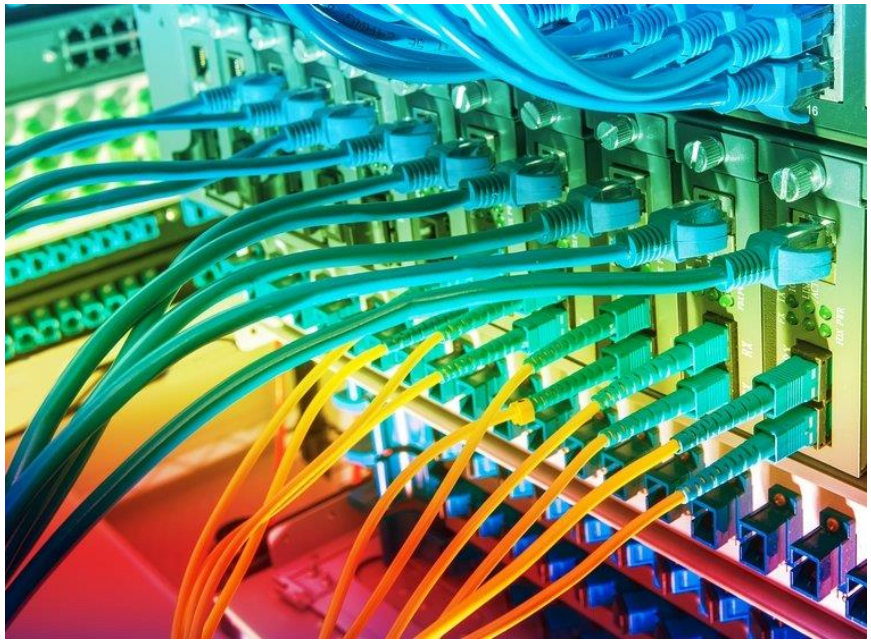
- Most advanced application is Quantum Key Distribution (QKD) [1]



[1] V. Scarani *et al.,* Rev. Mod. Phys. **81**, 1301 (2009)

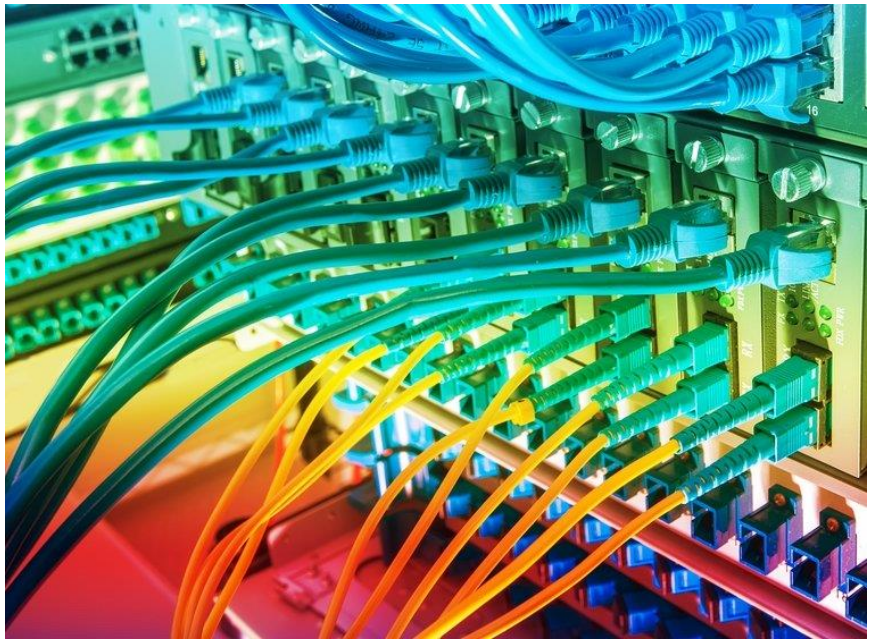
Motivations

- QKD is currently aiming towards **widespread adoption** in our telecom networks



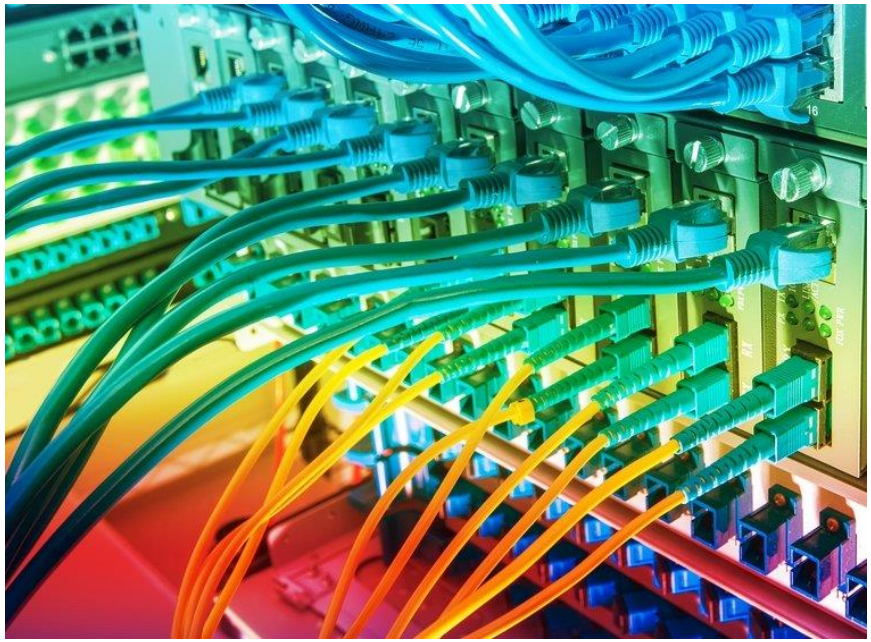
Motivations

- QKD is currently aiming towards **widespread adoption** in our telecom networks
- Many studies are developing **simpler** protocols and setups with **high stability**



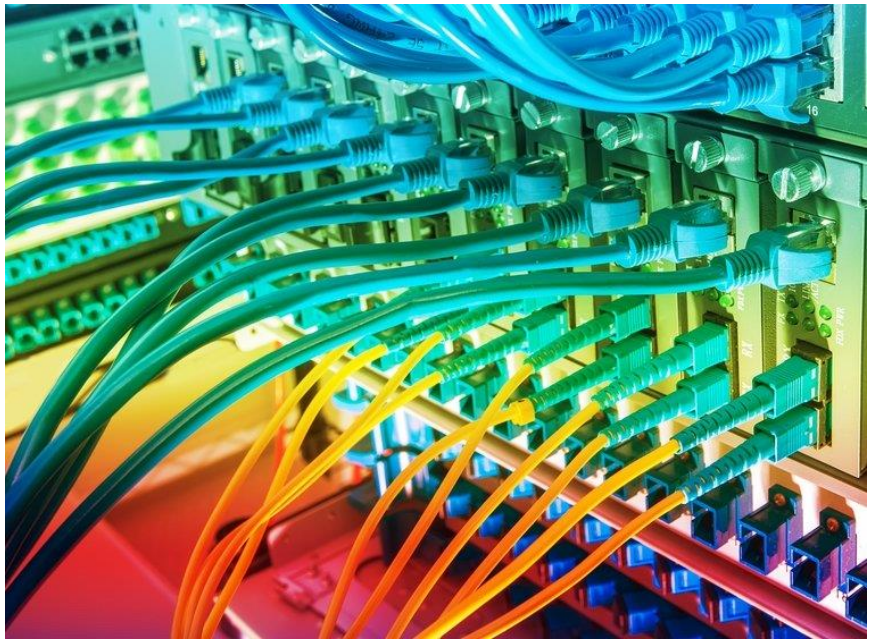
Motivations

- QKD is currently aiming towards **widespread adoption** in our telecom networks
- Many studies are developing **simpler** protocols and setups with **high stability**
- Essential auxiliary tasks are performed by separate sub-systems.



Motivations

- QKD is currently aiming towards **widespread adoption** in our telecom networks
- Many studies are developing **simpler** protocols and setups with **high stability**
- Essential auxiliary tasks are performed by separate sub-systems.

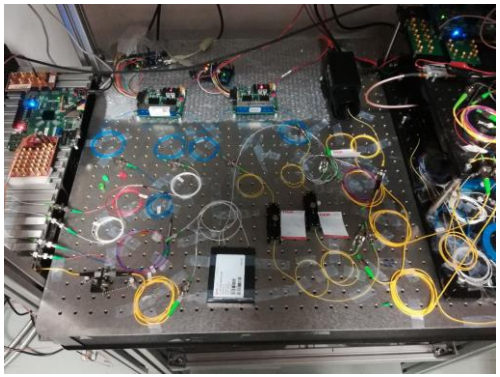


Wide-spread deployment of QKD in our current telecommunication networks will require the development of:

Simpler and more **robust** systems

Key features

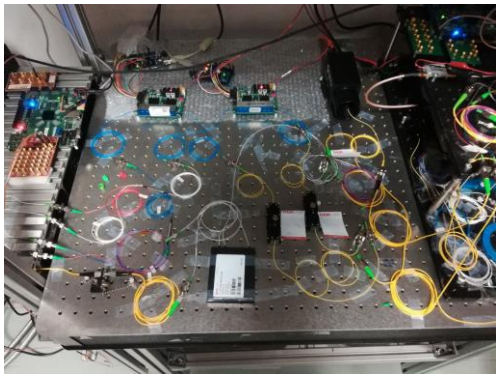
The QKD system we developed performs synchronization and polarization compensation by exploiting **only the hardware already needed** for the quantum communication task.



Key features

The QKD system we developed performs synchronization and polarization compensation by exploiting **only the hardware already needed** for the quantum communication task.

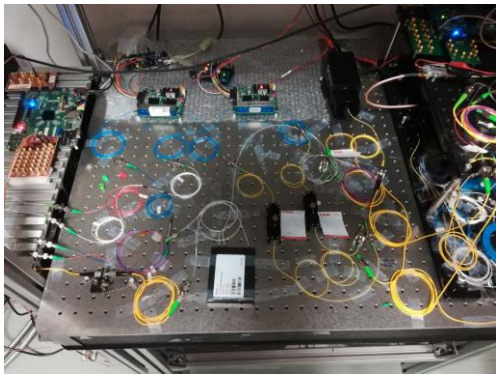
1. **Synchronization is performed with *Qubits4Sync* which works by sending a public qubit sequence at pre-established times.** [L. Calderaro *et al.*, *Phys. Rev. Applied* ***13***,*054041* (*2020*)]



Key features

The QKD system we developed performs synchronization and polarization compensation by exploiting **only the hardware already needed** for the quantum communication task.

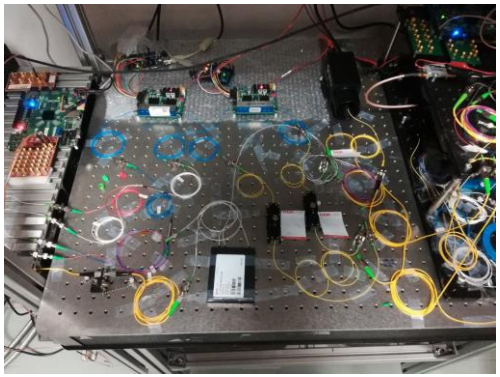
1. **Synchronization is performed with *Qubits4Sync* which works by sending a public qubit sequence at pre-established times.** [L. Calderaro *et al.*, *Phys. Rev. Applied* ***13***,*054041* (*2020*)]
2. **Predetermined qubit sequences are also exploited to monitor and compensate polarization drifts of the quantum channel.**



Key features

The QKD system we developed performs synchronization and polarization compensation by exploiting **only the hardware already needed** for the quantum communication task.

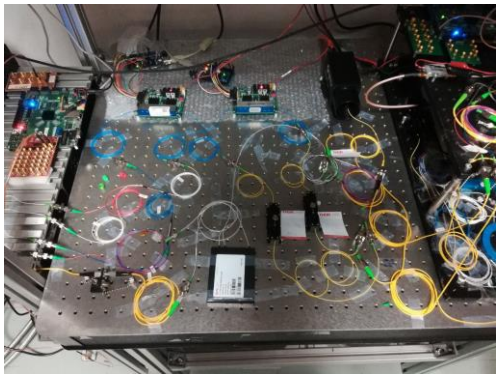
1. **Synchronization is performed with *Qubits4Sync* which works by sending a public qubit sequence at pre-established times.** [L. Calderaro *et al.*, *Phys. Rev. Applied* ***13***,*054041 (2020)*]
2. **Predetermined qubit sequences are also exploited to monitor and compensate polarization drifts of the quantum channel.**
3. **Polarization encoding is performed with the self-compensating *POGNAC* scheme based on a Sagnac loop.** [C. Agnesi *et al.*, *Opt. Lett.* ***44***, *2398 (2019)*]



Key features

The QKD system we developed performs synchronization and polarization compensation by exploiting **only the hardware already needed** for the quantum communication task.

1. **Synchronization is performed with *Qubits4Sync* which works by sending a public qubit sequence at pre-established times.** [L. Calderaro *et al.*, *Phys. Rev. Applied* ***13***,*054041 (2020)*]
2. **Predetermined qubit sequences are also exploited to monitor and compensate polarization drifts of the quantum channel.**
3. **Polarization encoding is performed with the self-compensating *POGNAC* scheme based on a Sagnac loop.** [C. Agnesi *et al.*, *Opt. Lett.* ***44***, *2398 (2019)*]
4. **We implement the 3 state 1 decoy efficient BB84 protocol introduced in** [F. Grünenfelder *et al., Appl. Phys. Lett.* ***112***, *051108 (2018)*]



C. Agnesi *et al.*,
Optica **7**(4), 284 (2020)

Temporal Synchronization: *Qubits4Sync*

Temporal Synchronization is of **fundamental importance** for QKD:

1. **Discriminating the noise from the quantum signal**
2. **Correlating Alice's transmitted sequence with Bob's detected events**

Temporal Synchronization: *Qubits4Sync*

Temporal Synchronization is of **fundamental importance** for QKD:

1. **Discriminating the noise from the quantum signal**
2. **Correlating Alice's transmitted sequence with Bob's detected events**

Successful synchronization requires:

1. **Period Recovery**
2. **Time-offset Recovery**

Temporal Synchronization: *Qubits4Sync*

Temporal Synchronization is of **fundamental importance** for QKD:

1. **Discriminating the noise from the quantum signal**
2. **Correlating Alice's transmitted sequence with Bob's detected events**

Successful synchronization requires:

1. **Period Recovery**
2. **Time-offset Recovery**

Temporal Synchronization is usually performed with additional laser system, exploiting time and/or wavelength multiplexing or using GPS receivers.

Temporal Synchronization: *Qubits4Sync*

Temporal Synchronization is of **fundamental importance** for QKD:

1. **Discriminating the noise from the quantum signal**
2. **Correlating Alice's transmitted sequence with Bob's detected events**

Successful synchronization requires:

1. **Period Recovery**
2. **Time-offset Recovery**

Temporal Synchronization is usually performed with additional laser system, exploiting time and/or wavelength multiplexing or using GPS receivers.

We propose ***Qubits4Sync*** which only uses qubits to synchronize the transmitter with the receiver.

L. Calderaro et al., Phys. Rev. Applied 13,054041 (2020)]

Period Reconstruction

Needed to correctly reconstruct the separations τ between consecutive states.

- We first estimate the period of the transmitter (Alice) τ_0^A via a Fast Fourier Transform of $N = 10^6$ samples and $4/\tau$ sampling rate
- If T_{acq} is larger than the sample time we perform a linear regression of the time of arrival modulus τ_0^A

Period Reconstruction

Needed to correctly reconstruct the separations τ between consecutive states.

- We first estimate the period of the transmitter (Alice) τ_0^A via a Fast Fourier Transform of $N = 10^6$ samples and $4/\tau$ sampling rate
- If T_{acq} is larger than the sample time we perform a linear regression of the time of arrival modulus τ_0^A

Time-offset Reconstruction

Needed to associate each detection to the corresponding bits in Alice's raw string.

- Alice sends a predetermined sequence in a single basis with length $L \sim \frac{1}{\eta}$.
- Bob performs a cross-correlation calculation between the detection sequence and the sent sequence. The maximum indicates the time-offset.
- A particular sequence is sent which allows to speed up the cross-correlation maximization process.

L. Calderaro et al., Phys. Rev. Applied 13,054041 (2020)]

Polarization Compensation

- Mechanical and temperature fluctuations **transform** the polarization state of the photons that travel through the fiber.
- This transformation causes the transmitter and receiver to effectively have different polarization reference frames, **increasing** the QBER.
- Real-time estimation of the QBER can be fed to a minimization algorithm that acts on motorized polarization controllers at the receiver to compensate for the polarization state transformation

Polarization Compensation

- Mechanical and temperature fluctuations **transform** the polarization state of the photons that travel through the fiber.
- This transformation causes the transmitter and receiver to effectively have different polarization reference frames, **increasing** the QBER.
- Real-time estimation of the QBER can be fed to a minimization algorithm that acts on motorized polarization controllers at the receiver to compensate for the polarization state transformation

We Propose a polarization compensation scheme that exploits a shared public string

- Alice sends $N = 10^6$ states in the *Z* basis, Bob estimates the *Z* basis QBER
- Each second Alice reveals her basis choices, Bob estimates the *X* basis QBER

Polarization Compensation

- Mechanical and temperature fluctuations **transform** the polarization state of the photons that travel through the fiber.
- This transformation causes the transmitter and receiver to effectively have different polarization reference frames, **increasing** the QBER.
- Real-time estimation of the QBER can be fed to a minimization algorithm that acts on motorized polarization controllers at the receiver to compensate for the polarization state transformation

We Propose a polarization compensation scheme that exploits a shared public string

- Alice sends $N = 10^6$ states in the Z basis, Bob estimates the Z basis QBER
- Each second Alice reveals her basis choices, Bob estimates the X basis QBER

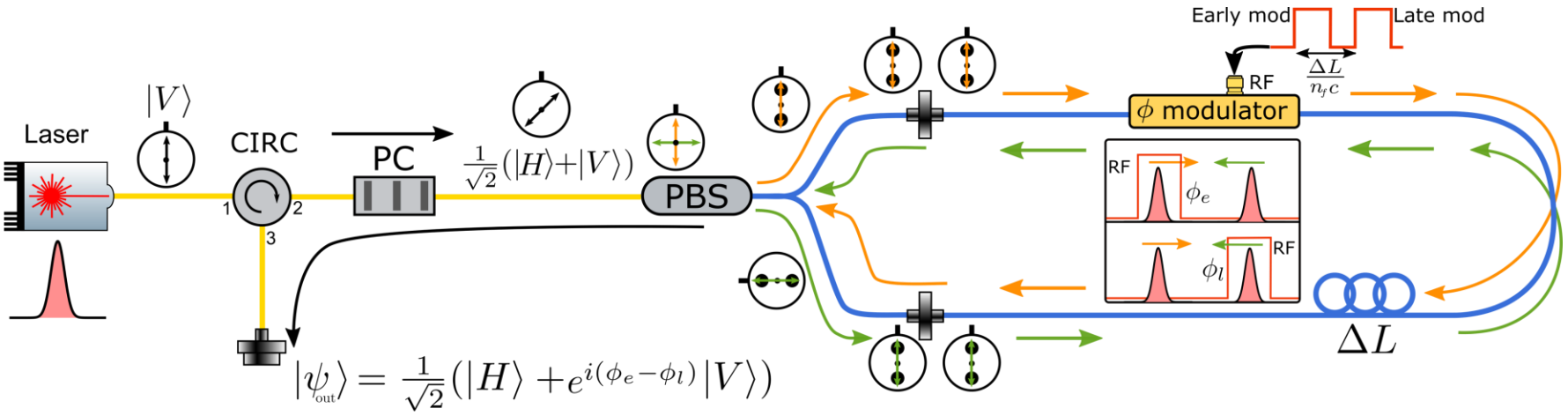
Similar schemes have been proposed but require **entire postprocessing** of the transmitted string in [F. Grünenfelder *et al., Appl. Phys. Lett.* ***112****, 051108 (2018)*] and [Y.-Y. Ding *et al., Opt. Lett.* ***42****, 1023 (2017)*]. As a result, our approach has a feedback cycle about 10 times faster than those approaches.

POGNAC polarization encoder

Past polarization encoders are **expensive**, **unstable**, showed **limited** polarization extinction ratios, or exhibit side channels that **undermine** security.

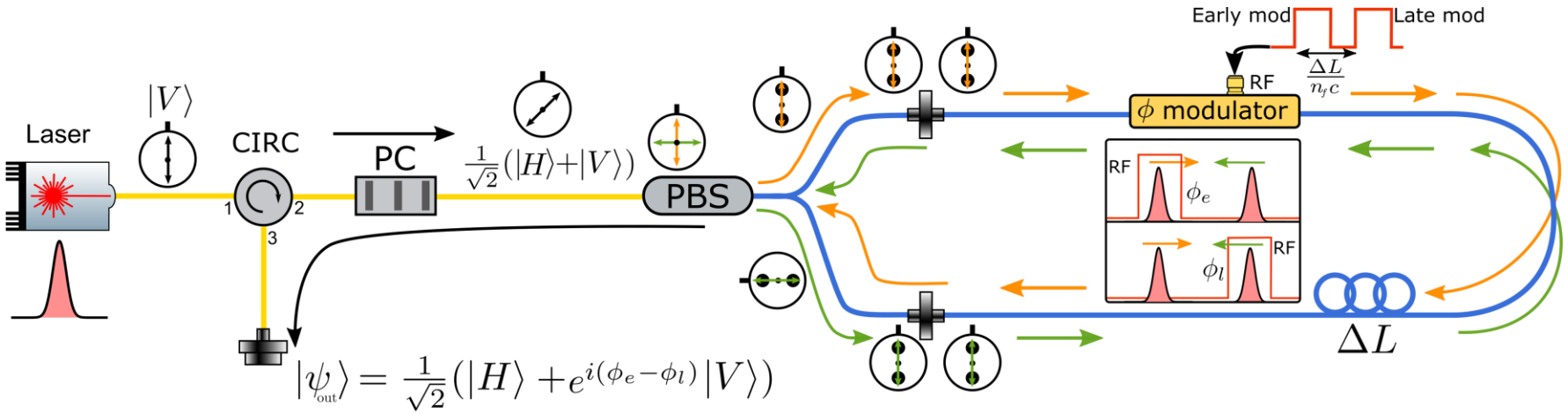
POGNAC polarization encoder

Past polarization encoders are **expensive**, **unstable**, showed **limited** polarization extinction ratios, or exhibit side channels that **undermine** security.



POGNAC polarization encoder

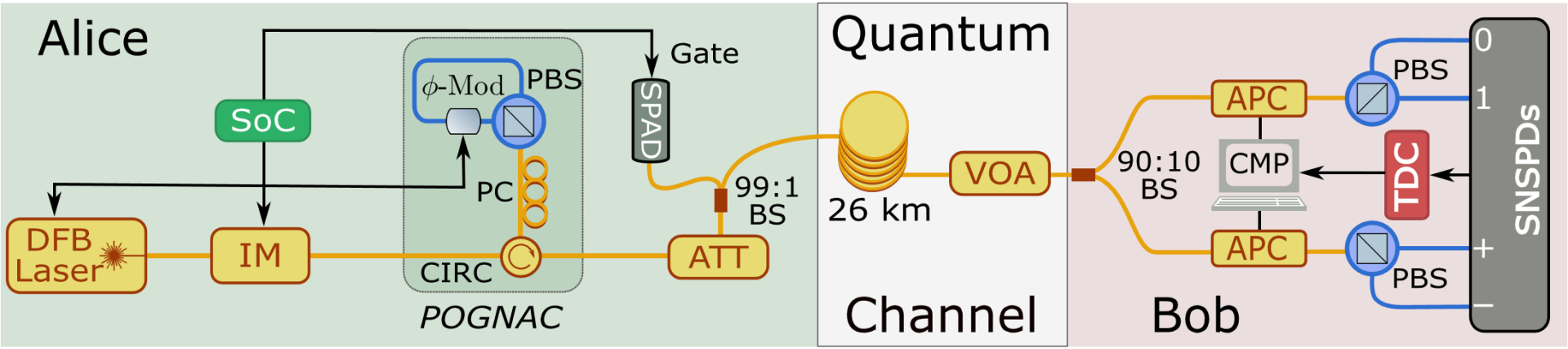
Past polarization encoders are **expensive**, **unstable**, showed **limited** polarization extinction ratios, or exhibit side channels that **undermine** security.



ϕ_e	ϕ_l	$\lvert\psi_{out}\rangle$
0	0	$\lvert D\rangle$
0	$\frac{\pi}{2}$	$\lvert L\rangle$
$\frac{\pi}{2}$	0	$\lvert R\rangle$
0	π	$\lvert A\rangle$

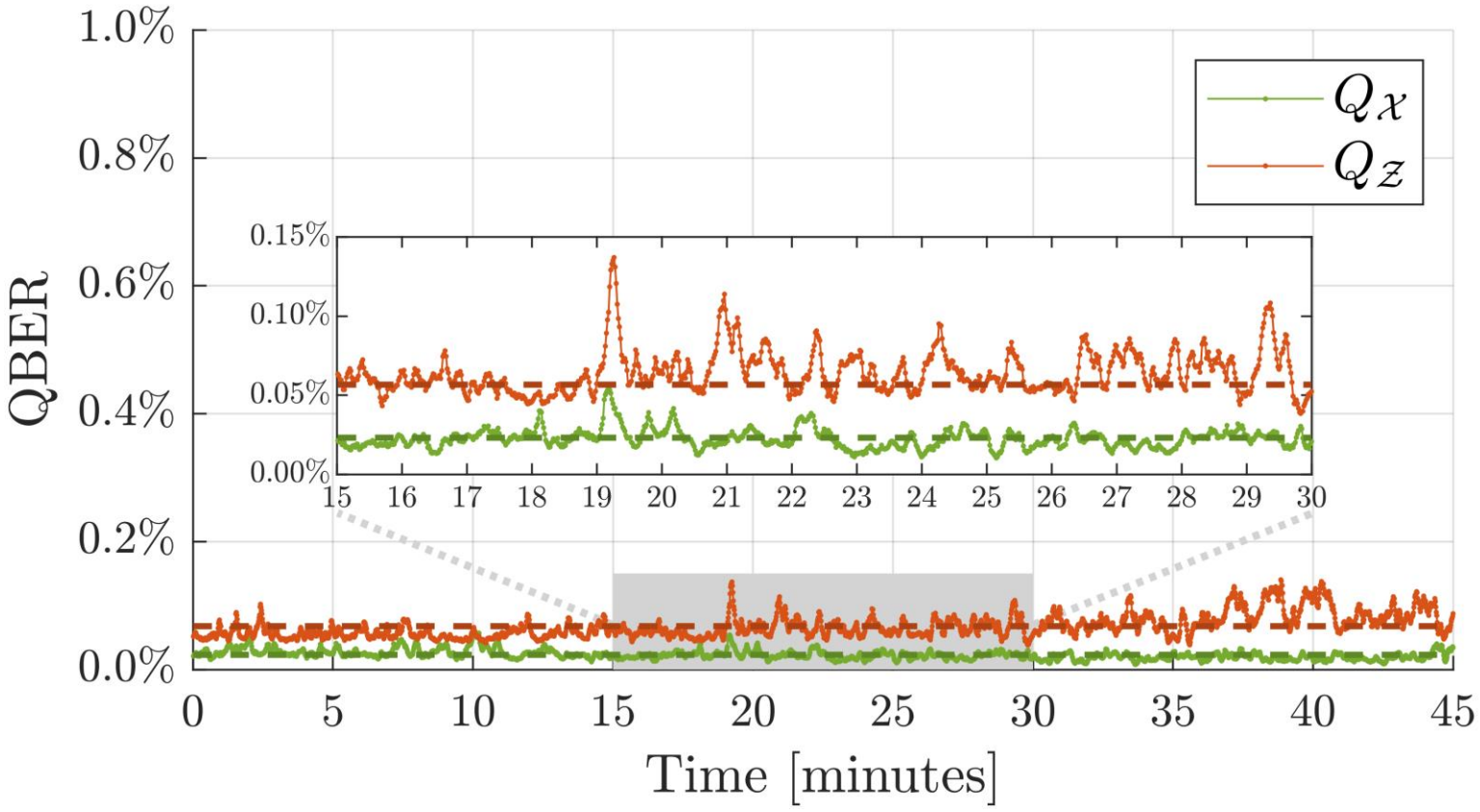
C. Agnesi *et al.*, *Opt. Lett.* **44**, 2398 (2019)

QKD Setup



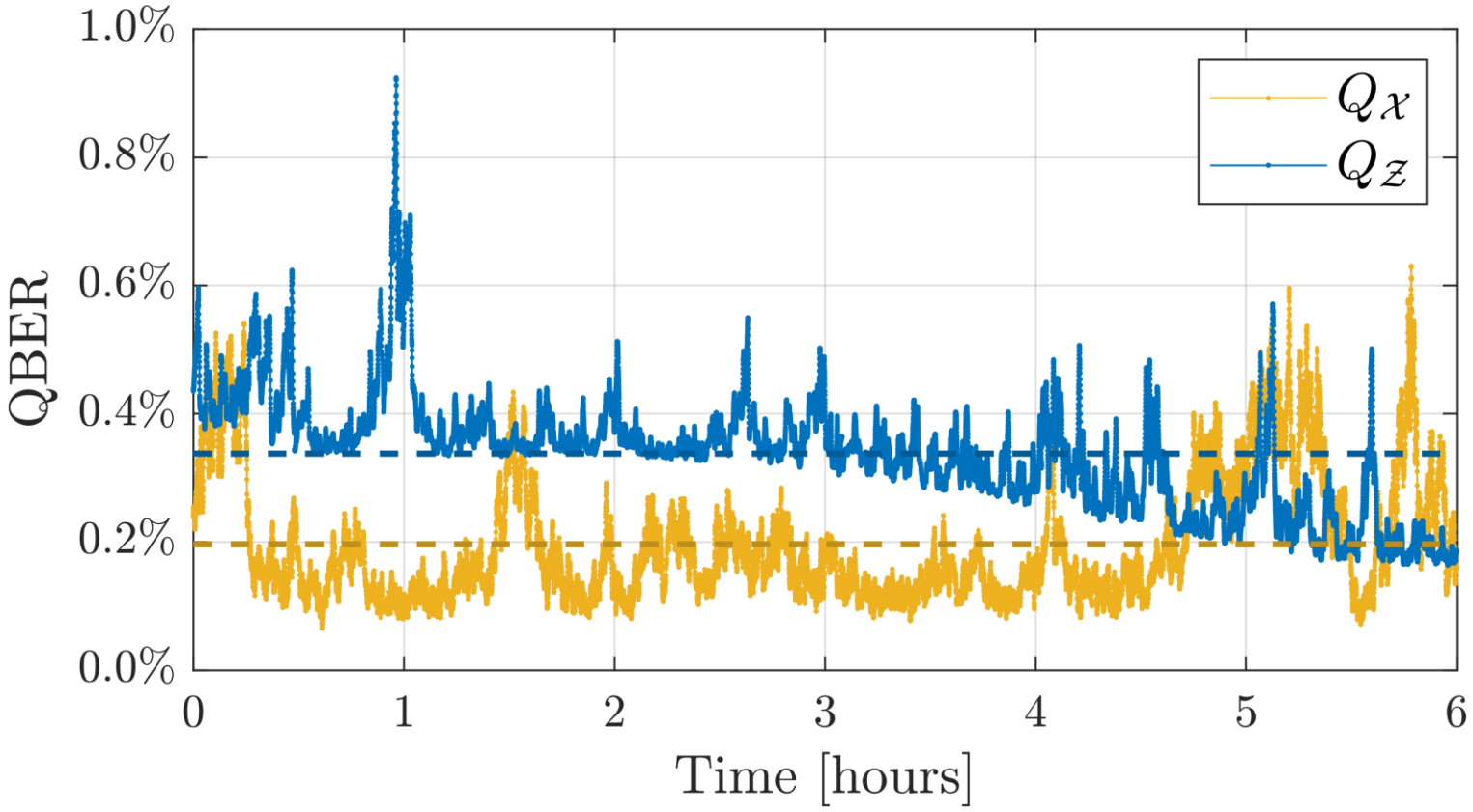
- **Laser pulses at 1550nm, 200ps HWFM, 50 MHz**
- **The state analyzer is composed of COTS elements** (fiber BS, PBS, polarization controllers) **, four SNSPDs and TDC with 1 ps accuracy.**

Result: Intrinsic Stability



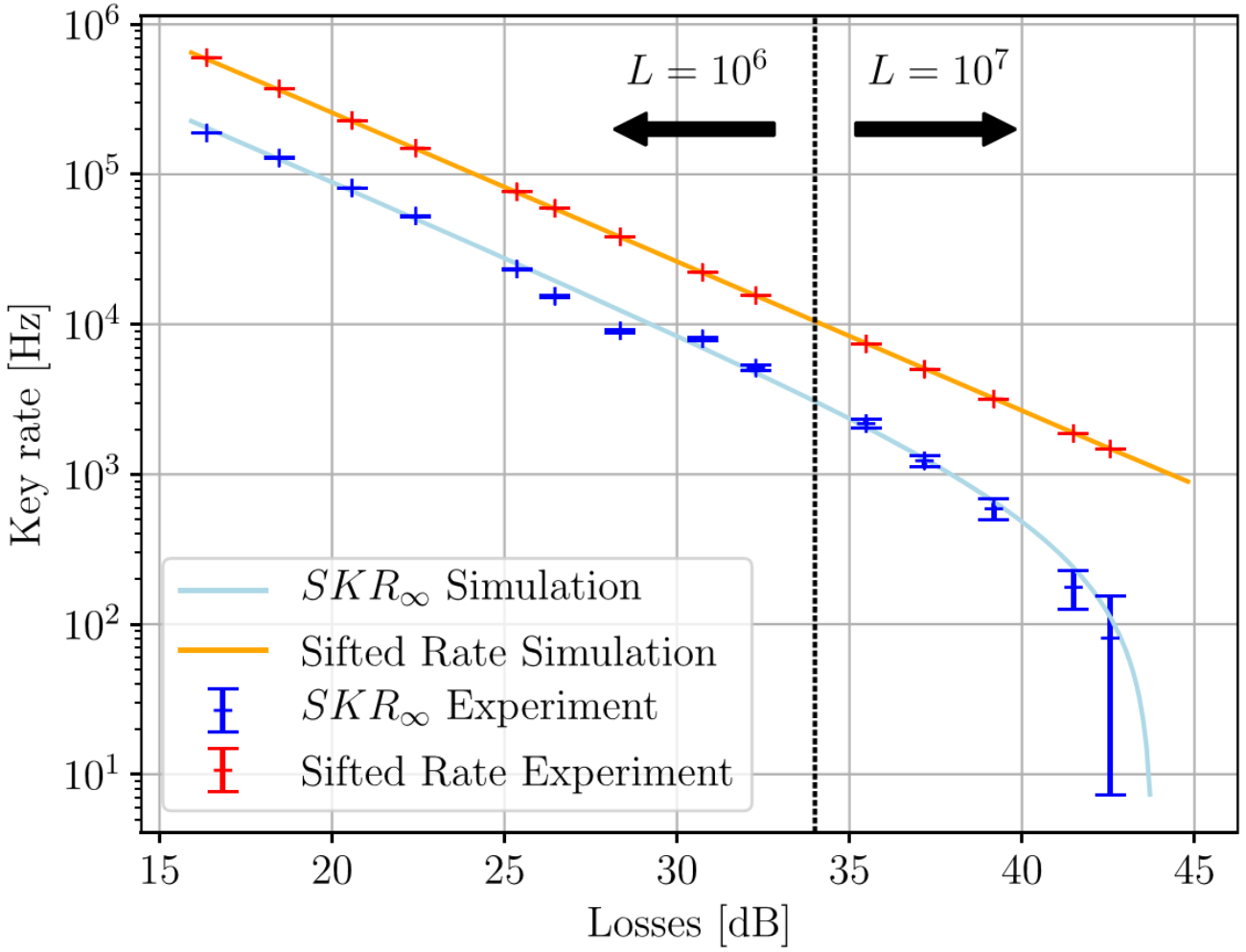
With over 33dB of Polarization Extinction Ratio, the *POGNAC exhibits the* ***lowest intrinsic QBER ever reported***

Result: Polarization Compensation



An **average QBER** 0.3± 0.1% was measured for the key-generation basis while an average 0.2± 0.1% for the control basis with the QC including both the **26 km optical fiber spool** and the VOA for about 19 dB of total losses.

Result: Secure Key Rate vs channel losses



Conclusions

- We demonstrated a **simple** QKD system with **reduced hardware requirements**. 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.

Conclusions

- We demonstrated a **simple** QKD system with **reduced hardware requirements**. 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 *POGNAC* polarization encoder exhibits **record low intrinsic QBER**

Conclusions

- We demonstrated a **simple** QKD system with **reduced hardware requirements**. 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 *POGNAC* polarization encoder exhibits **record low intrinsic QBER**

- We obtain **high Secure Key Rates** and **resilience up to about 40 dB of channel losses**, even with only 50 MHz repetition rate. In fact, our results are comparable with those of polarization-based systems with GHz base clocks.

Conclusions

- We demonstrated a **simple** QKD system with **reduced hardware requirements**. 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 *POGNAC* polarization encoder exhibits **record low intrinsic QBER**

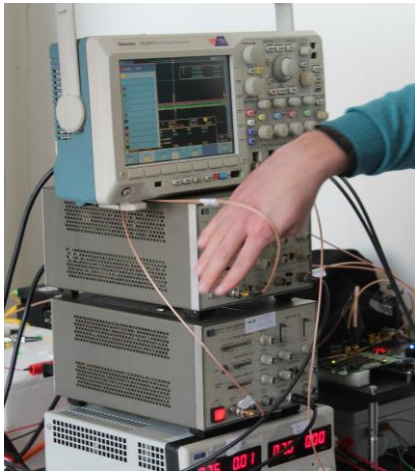
- We obtain **high Secure Key Rates** and **resilience up to about 40 dB of channel losses**, even with only 50 MHz repetition rate. In fact, our results are comparable with those of polarization-based systems with GHz base clocks.

- Due to its reduced hardware requirements and the quality of the source, this work represents an important step towards technologically mature QKD systems.

The authors

Costantino Agnesi,[1,2,†] Marco Avesani,[1,†] Luca Calderaro,[1,2,†] Andrea Stanco,[1] 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*



C. Agnesi *et al.*,
Optica **7**(4), 284 (2020)