Fast and simple qubit-based synchronization for quantum key distribution

merged with

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

Quantum Future
The shift in the communication paradigm

Università degli Studi di Padova


DEPA
INFO
ENG
UNIVER
ESTINTORE

Index

- Introduction
- Qubits4Sync Temporal Synchronization for QKD
- POGNAC Polarization Encoder
- QKD Experiment
- Conclusions

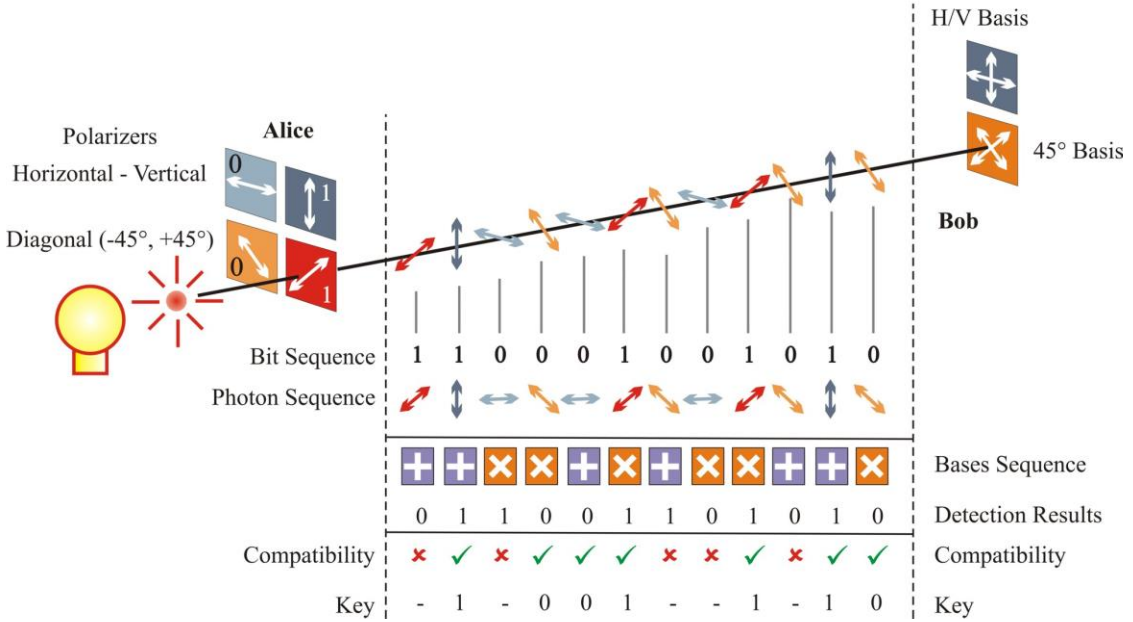
Index

- ❑ **Introduction**
- ❑ Qubits4Sync Temporal Synchronization for QKD
- ❑ POGNAC Polarization Encoder
- ❑ QKD Experiment
- ❑ Conclusions

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.

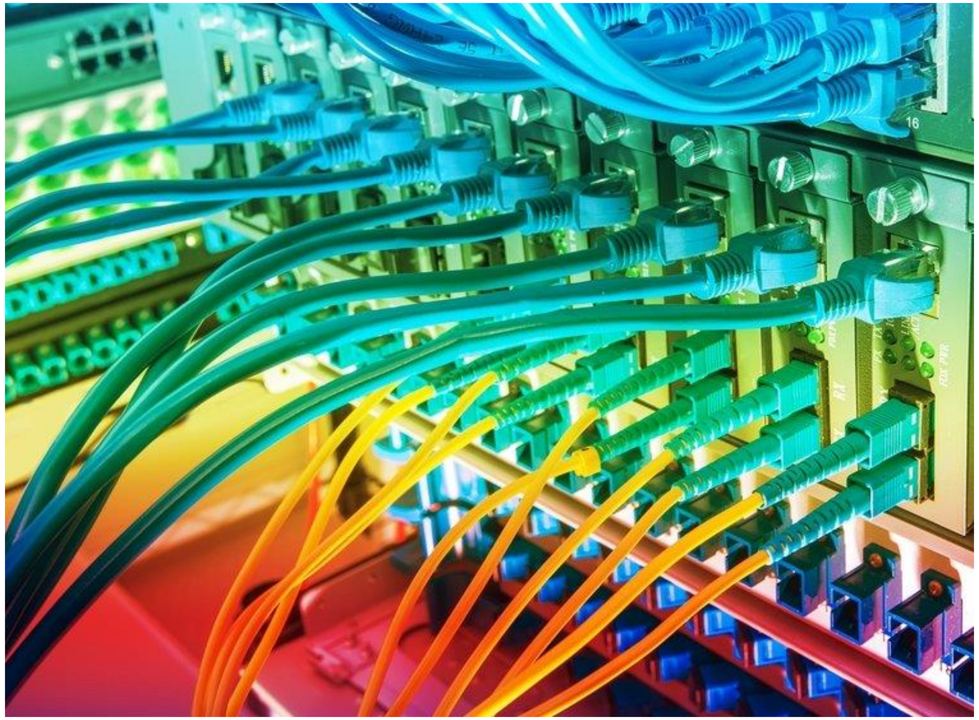
- Most advanced application is Quantum Key Distribution (QKD) [1]



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

Motivations

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



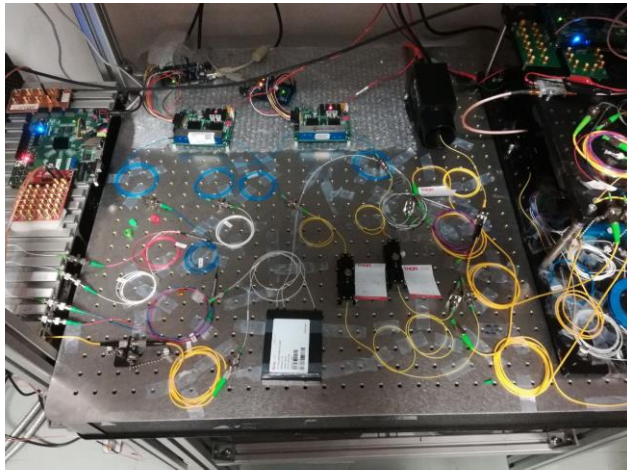
Wide-spread deployment of QKD in our current telecommunication networks will require the development of:

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.

1. **Synchronization is performed with the *Qubits4Sync* method which works by sending a public qubit sequence at pre-established times.** [L. Calderaro *et al.*, Phys. Rev. Appl. **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)]



Index

Temporal Synchronization

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

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

Most adopted synchronization solutions are:

1. **Clock distribution** from transmitter to receiver via pulsed laser
2. Transmitter and receiver locked to an **external time reference**

The performances of the synchronization solution are crucial to filter out the noise

Temporal Synchronization

Temporal Synchronization in **classical communication systems** do not require an external synchronization service. **The clock information is carried by the signal itself**.

This approach has several advantages:

1. **Data throughput is maximized** as any physical channel is exploited for data stream.
2. **Less hardware** is required: simplicity and robustness of the system.

In the same spirit, we propose a synchronization method, ***Qubit4Sync***, which uses the qubits exchanged during the QKD protocol, to synchronize the transmitter with the receiver.

Temporal Synchronization

A synchronization method has to solves the following problems:

1. Reconstruct the transmitter **period** at the receiver.
2. Find the **time-offset:** the time at which the first qubit arrives at the receiver.

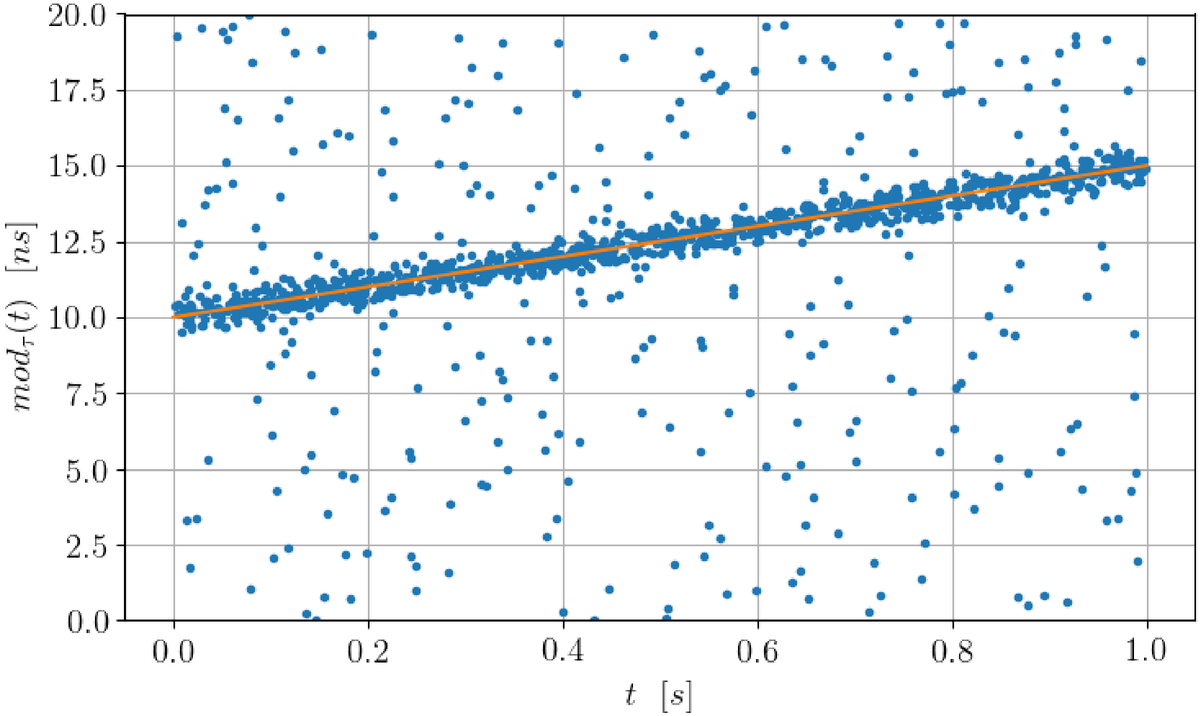
Qubit4Sync main idea**:**

1. Uses the time of arrival of the qubits to perform a frequency analysis and find the transmitter frequency.
2. The time-offset is calculated via cross-correlation of a public qubit sequence (synchronization string) pre-pended to the Alice's random sequence. We introduce a novel cross-correlation algorithm with computational complexity of $Llog(\log(L)$.

Period Reconstruction

Given an acquisition interval T , the algorithm has to correctly reconstruct the time separations τ of consecutive states sent by Alice:

- We first estimate the period of the transmitter (Alice) τ_0^A via a Fast Fourier Transform of $N = 10^6$ samples. The sampling rate is four times the nominal frequency of the transmitter.
- If T is larger than the sample time $\tau_0^A N$, the estimate τ_0^A is not sufficiently precise. Then, we perform a linear regression of the time of arrival modulus τ_0^A. The slope of the linear fit is used to correct the estimation of the period.



Temporal Synchronization

Time-offset Reconstruction

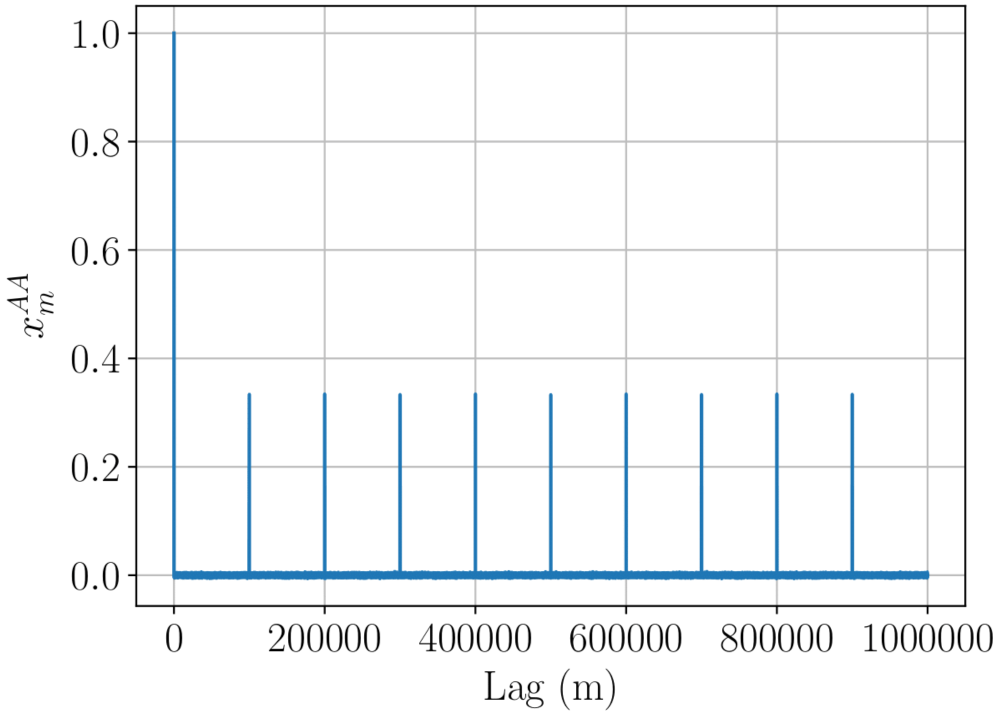
The higher the losses, the longer the synchronization string needs to be in order to have a significant correlation: $L = \frac{1}{\eta}$. An efficient cross-correlation algorithm is needed for lossy channels.

The idea

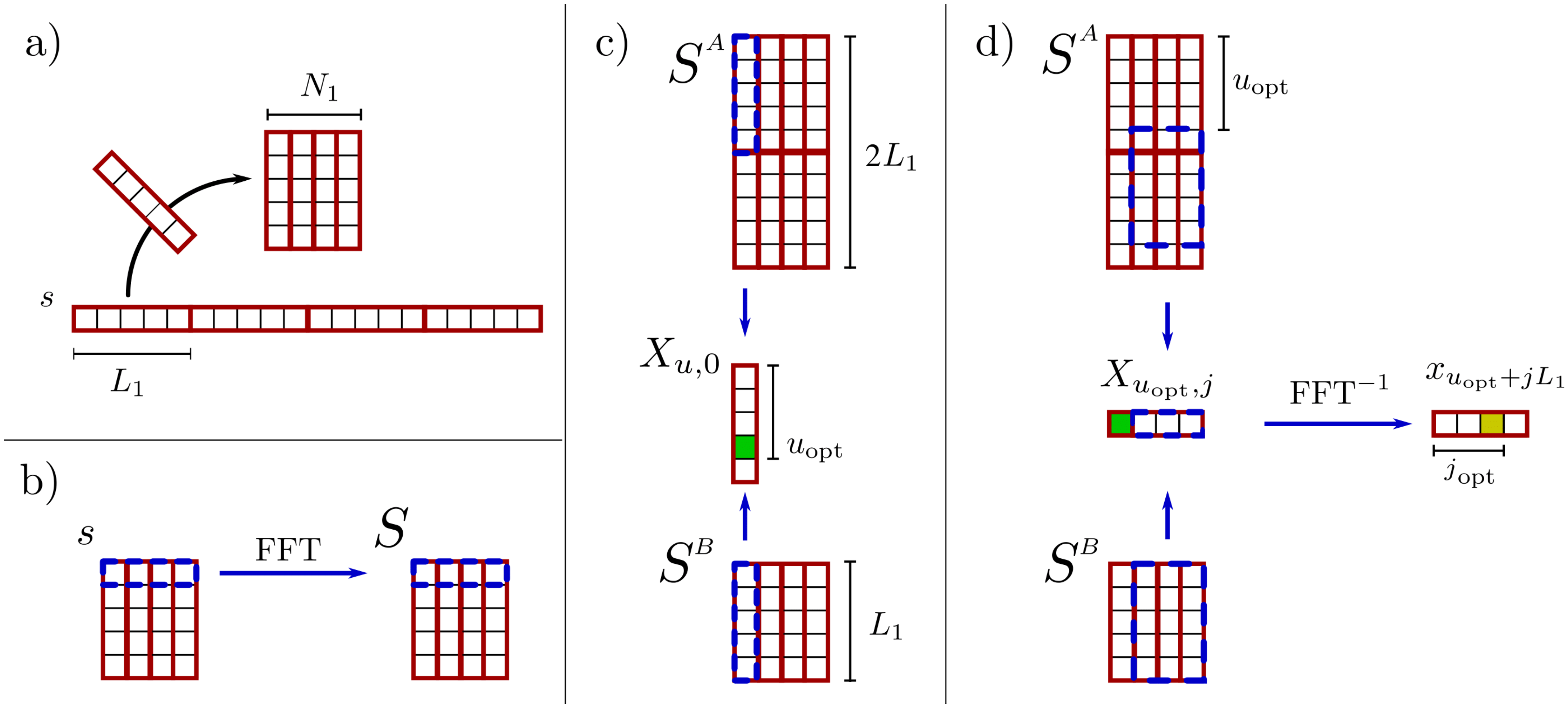
Assume to have a synchronization string, whose auto-correlation has N_1 periodic peaks:

1. Find the lag of any of those peaks

2. Take the lag corresponding to the global maximum among the lags of the local maxima.

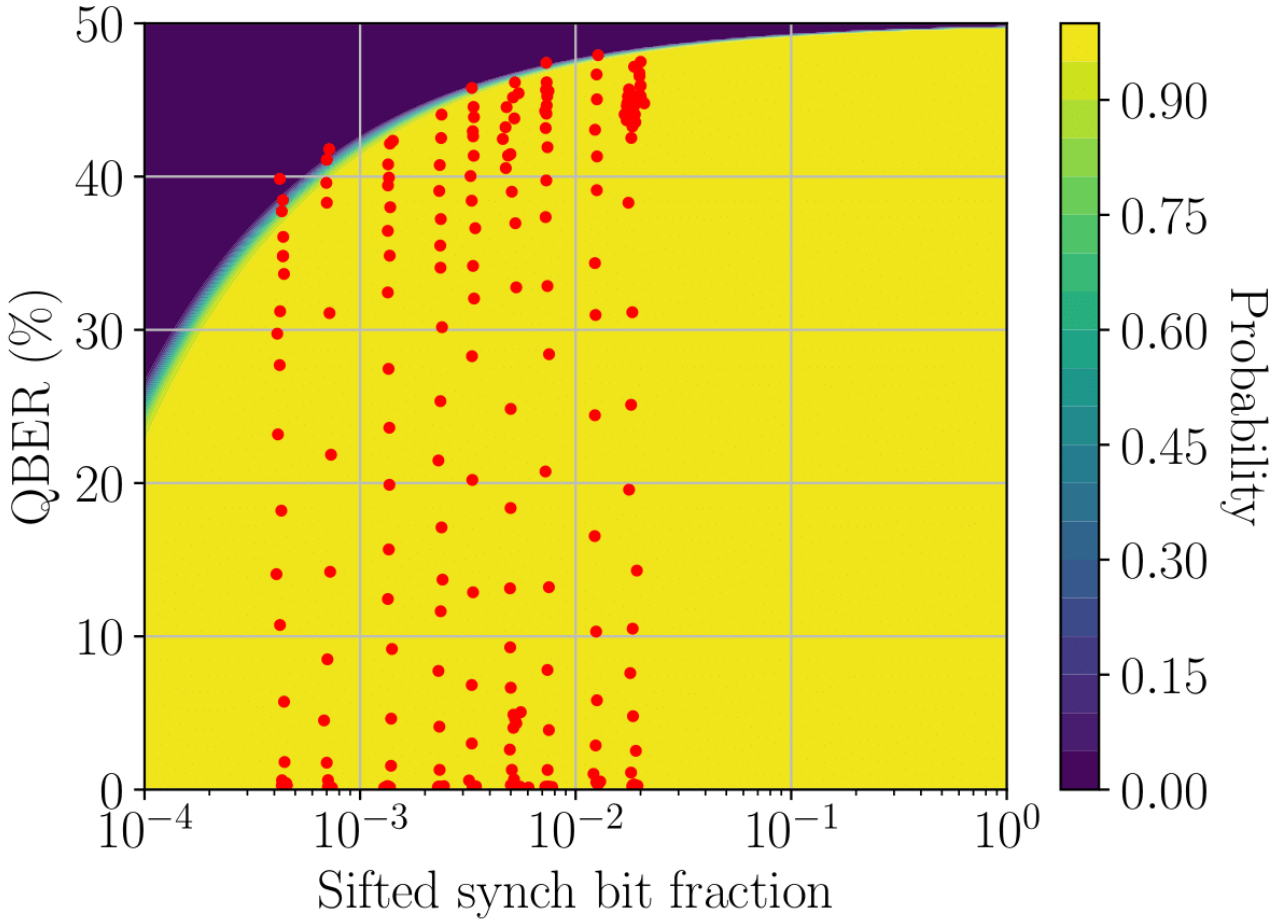


Temporal Synchronization



Temporal Synchronization

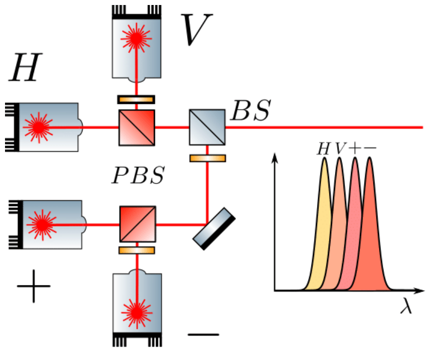
Simulated probability of success (heat map) and experimentally realized synchronization (red dots), for several channel losses and QBER ($L = 10^6$).

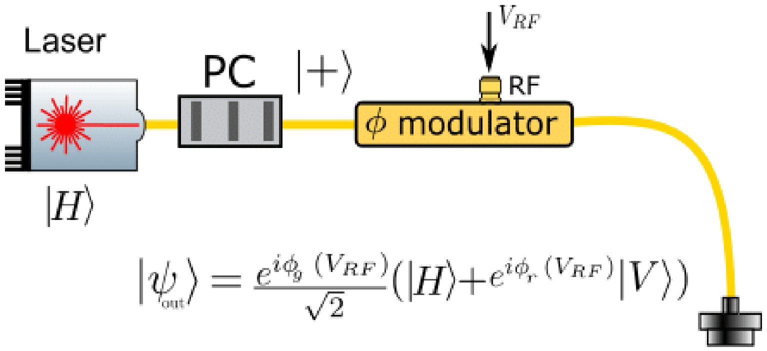


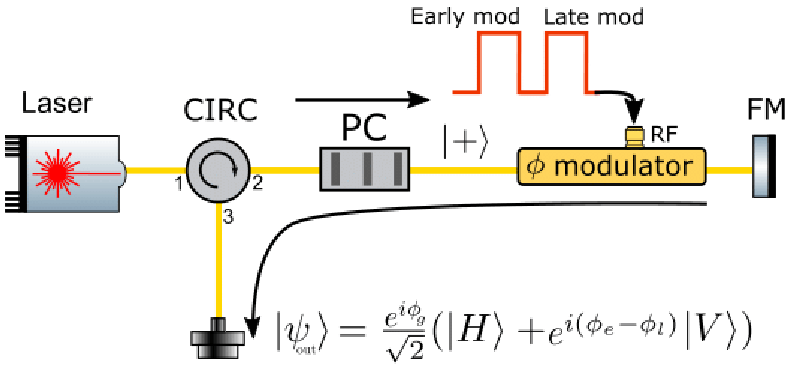
Index

POGNAC polarization encoder

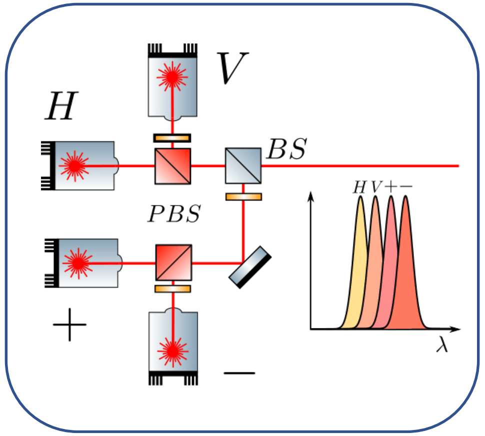
Past polarization encoders are **expensive**, **unstable**, showed **limited** polarization extinction ratios, or exhibit side channels that **undermine** security.

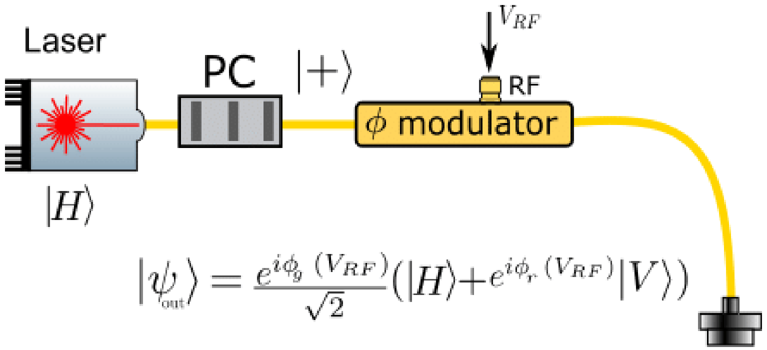


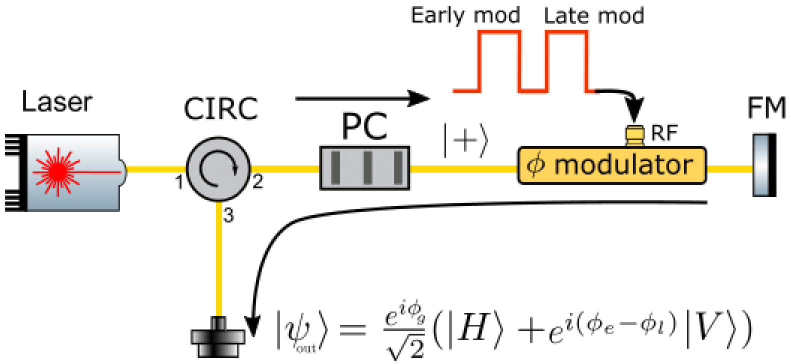




POGNAC polarization encoder





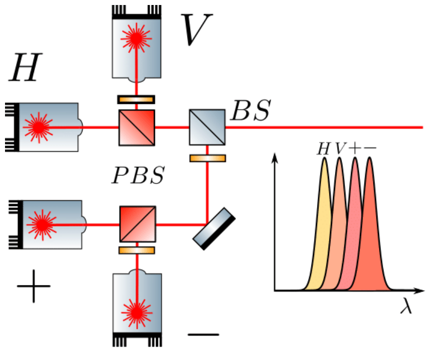


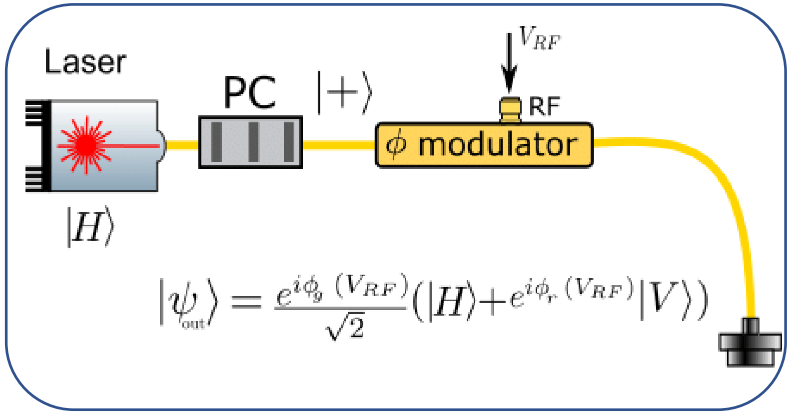
Solution 1: **Four different lasers,** one for each polarization state. Used for example in Micius QKD experiments. [S.-K. Liao *et al.*, Nature **549**, 43 (2017)]

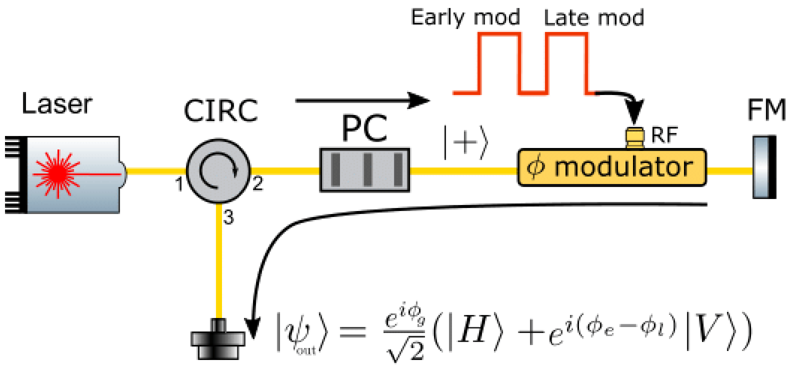
Drawbacks:

- **Bulky** and **complex.** High power consumption.
- Side-channels due to **temporal** and **spectral mismatch.**
- Vulnerable to some **Quantum Hacking** attacks. [M. S. Lee *et al.*, J. Opt. Soc. Am. B **36**, B77 (2019)]

POGNAC polarization encoder





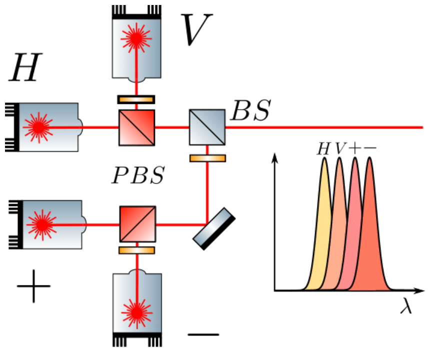


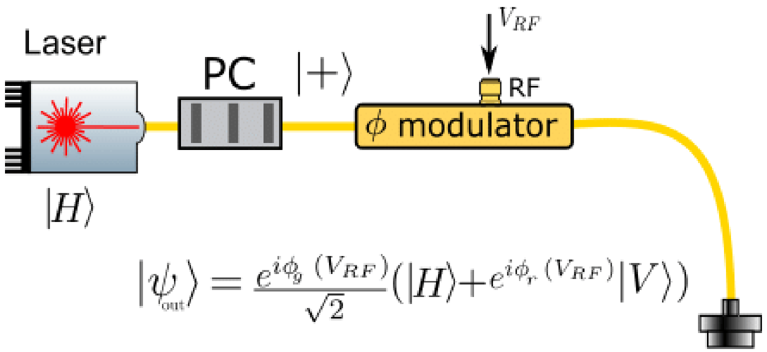
Solution 2: **Inline Polarization Modulator**. As used in [M. Joffre *et al.*, J. Light. Technol. **28**, 2572 (2010)] and [F. Grünenfelder *et al.*, Appl. Phys. Lett. **112**, 051108 (2018)].

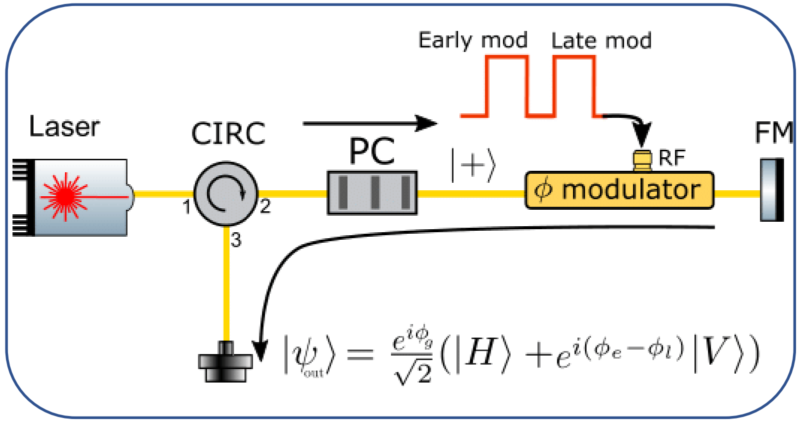
Drawbacks:

- **Unstable.** RF and Temperature Drifts.
- **High** V_π voltage.
- Extinction ratio **limited** by the birefringence of the crystal.
- Phase modulator needs to support **both** polarization modes.

POGNAC polarization encoder







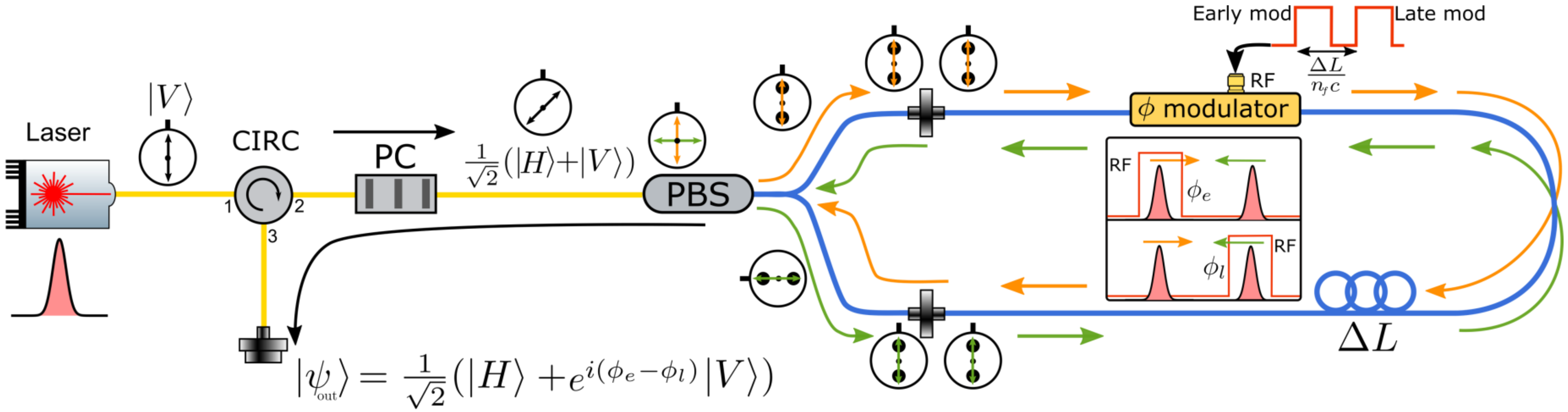
Solution 3: **Double-Pass Polarization Modulator with a Faraday Mirror.** Introduced by [I. Lucio-Martinez *et al.*, New J. Phys. 11, 095001 (2009)].

Drawbacks:

- **High** V_π voltage.
- Extinction ratio **limited** by the birefringence of the crystal.
- Phase modulator needs to support **both** polarization modes.

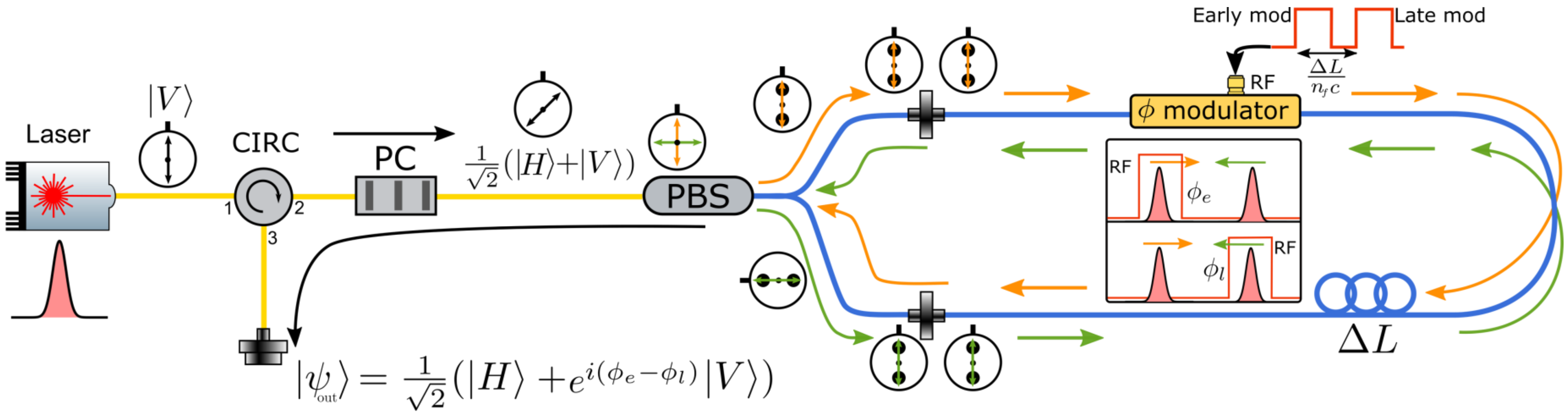
POGNAC polarization encoder

All the previous problems can be solved placing a phase modulator with polarization maintaining fibers inside an asymmetric Sagnac interferometer. [C. Agnesi *et al.*, Opt. Lett. **44**, 2398 (2010)]



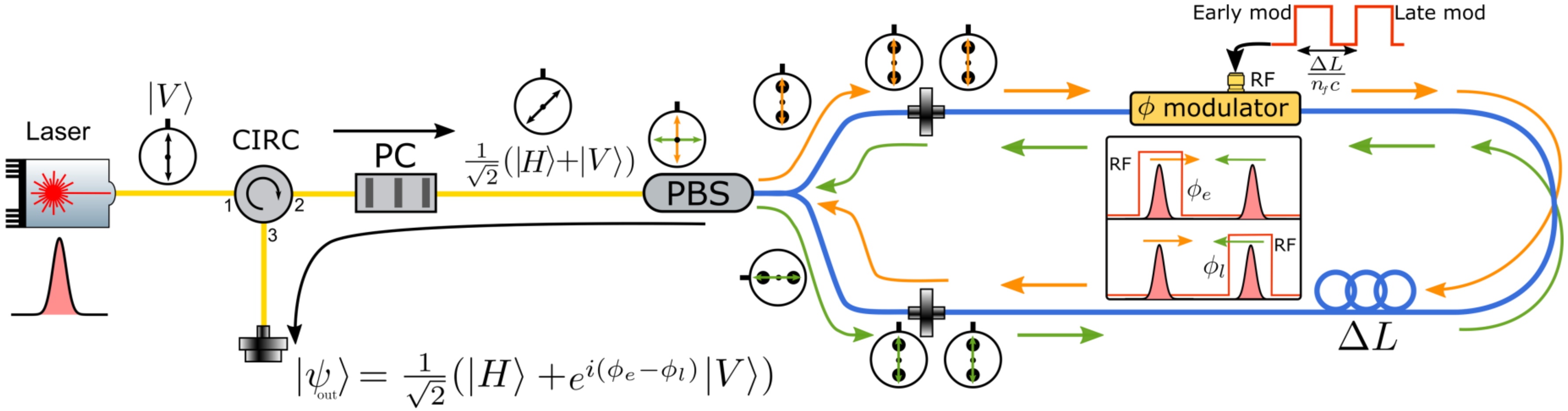
POGNAC polarization encoder

All the previous problems can be solved placing a phase modulator with polarization maintaining fibers inside an asymmetric Sagnac interferometer. [C. Agnesi *et al.*, Opt. Lett. **44**, 2398 (2010)]



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

POGNAC polarization encoder

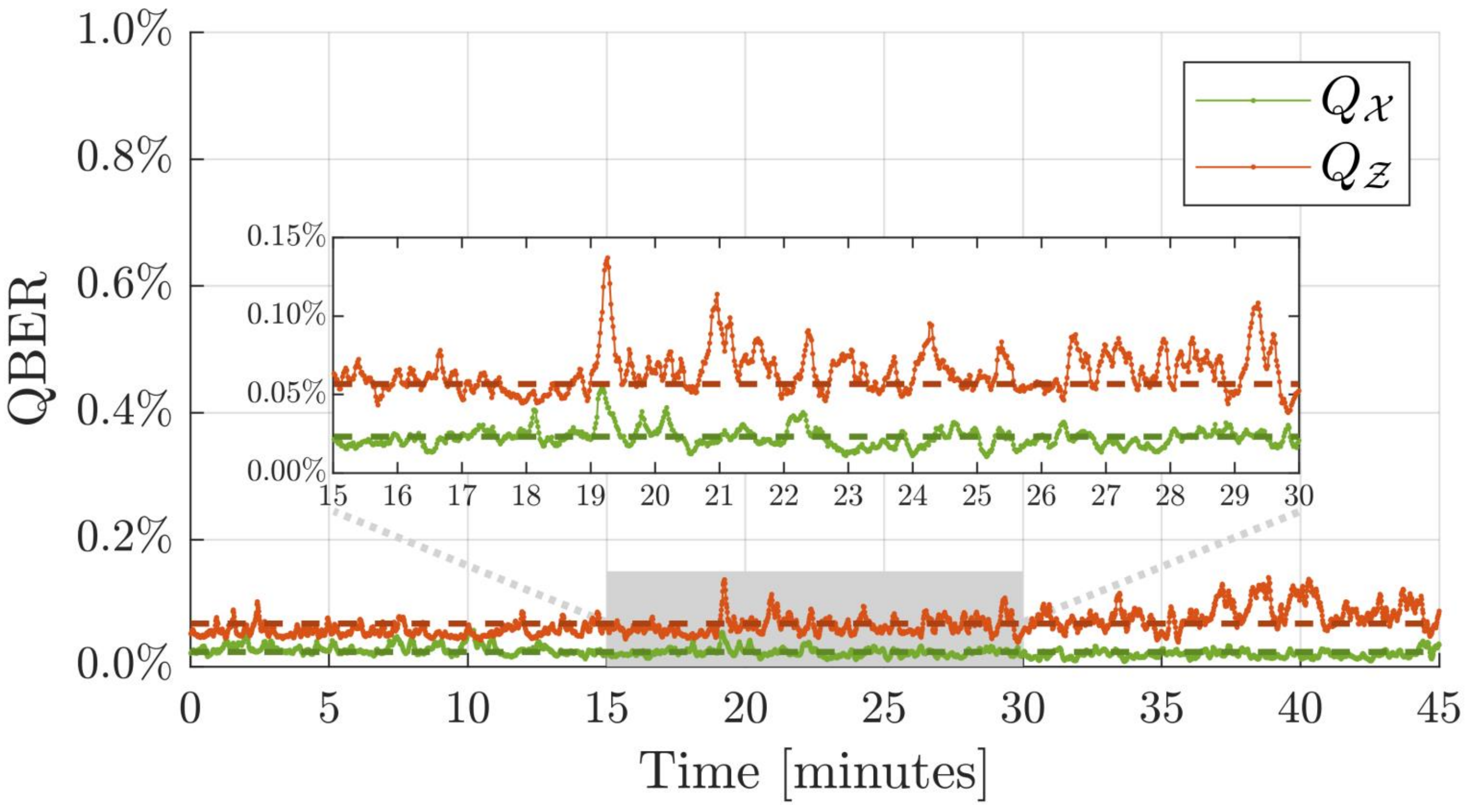


Advantages:

- ❑ **Long term stability:** Thermal and mechanical phase drifts are automatically compensated
- ❑ Phase modulator needs to support only one polarization mode: **COTS modulators at 800nm.**
- ❑ **Low** V_π voltage.
- ❑ No Polarization Mode Dispersion: **Extremely low QBER**

Low Intrinsic QBER and High Stability

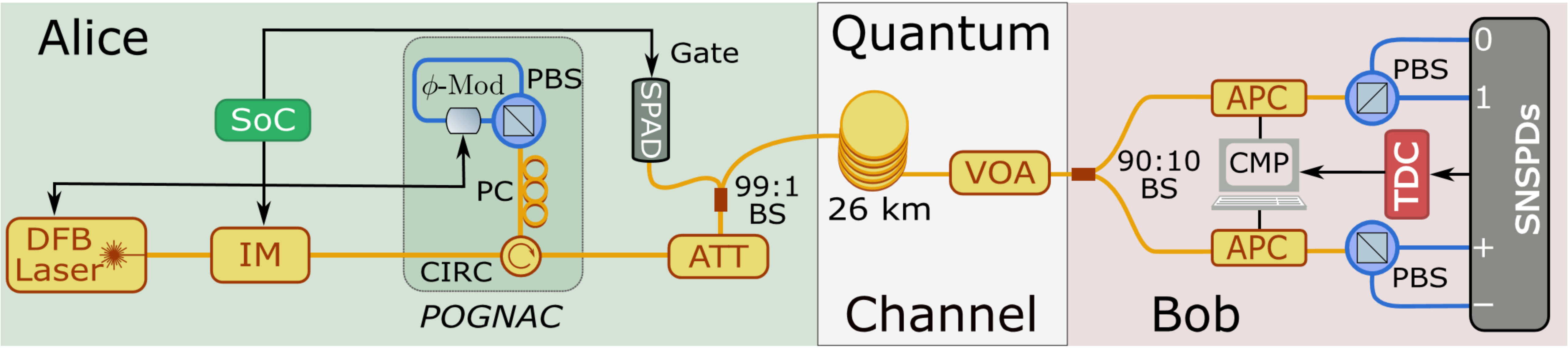
The intrinsic QBER gives a **quantitative and qualitative** measure of its **suitability** for QKD. It is also meaningful to measure its **stability** to find how long the source can function **without realignment**. [N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002)]



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

Index

QKD Setup



- **Laser pulses at 1550nm, 200ps HWFM, 50 MHz**
- **We implement the 3 state 1 decoy efficient BB84 protocol introduced in** [F. Grünenfelder *et al.*, Appl. Phys. Lett. **112**, 051108 (2018)].
- **The Quantum Channel is composed of 26 km spool of G.655 dispersion-shifted fiber with 0.35 dB/km of loss followed by a variable optical attenuator**
- **The state analyzer is composed of COTS elements** (fiber BS, PBS, polarization controllers) **, four SNSPDs and TDC with 1 ps accuracy.**

QKD Setup: Polarization Compensation

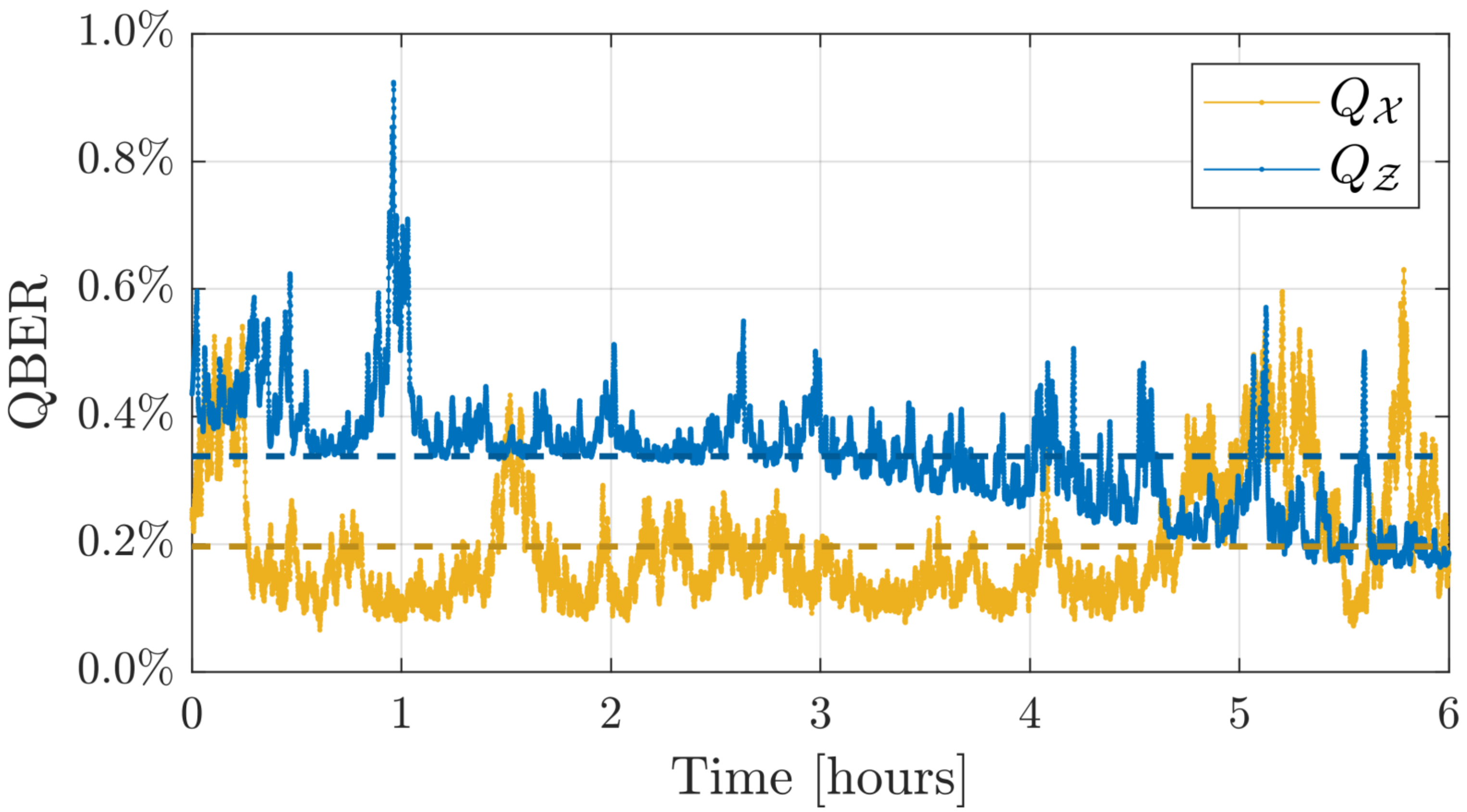
- Mechanical and temperature fluctuations **transform** the polarization state of the photons that travel through the fiber.
- This transformation causes the transmitter and receiver to effectively have different polarization reference frames, **increasing** the QBER.
- Real-time estimation of the QBER 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

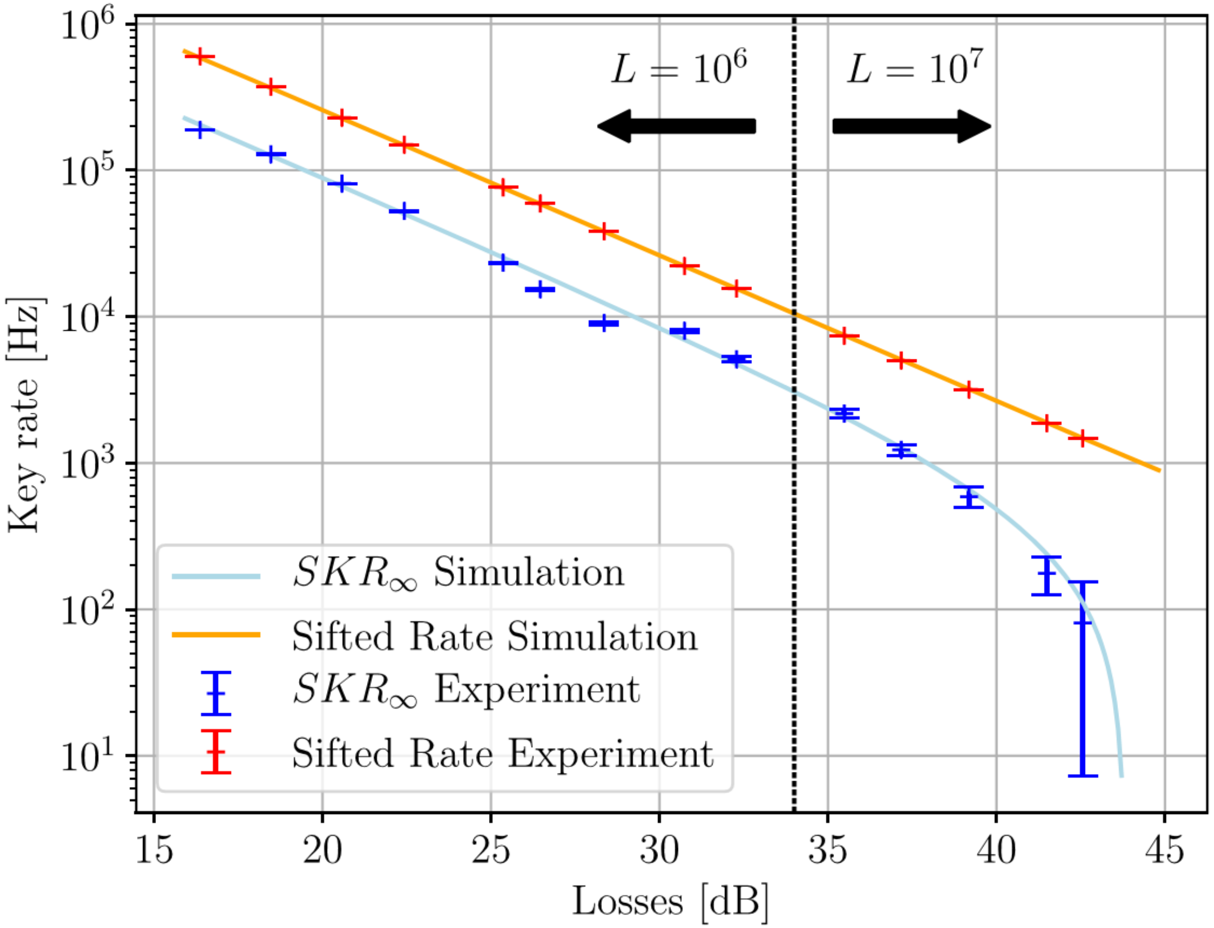
Similar schemes have been proposed but require **entire postprocessing** of the transmitted string in [F. Grünenfelder *et al.*, Appl. Phys. Lett. **112**, 051108 (2018)] and [Y.-Y. Ding *et al.*, Opt. Lett. **42**, 1023 (2017)]. As a result, our approach has a feedback cycle about 10 times faster than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

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



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 with Qubits4Sync synchronization up to the total loss at which the key rate drops to zero.**

Index

- ❑ Introduction
- ❑ Qubits4Sync Temporal Synchronization for QKD
- ❑ POGNAC Polarization Encoder
- ❑ QKD Experiment
- ❑ **Conclusions**

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.

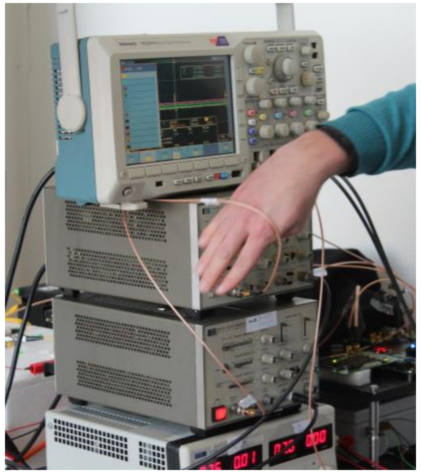
PHYSICAL REVIEW APPLIED **13**, 054041 (2020)

Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution

Luca Calderaro,[1,2,*] Andrea Stanco,[1,2] Costantino Agnesi,[1,2] Marco Avesani,[1]
Daniele Dequal,[3] Paolo Villoresi,[1,2] and Giuseppe Vallone[1,2,4]

[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, Via Marzolo 8, 35131, Padova, Italy*
[3] *Matera Laser Ranging Observatory, Agenzia Spaziale Italiana, Matera, Italy*
[4] *Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy*

(Received 22 October 2019; revised manuscript received 12 December 2019; accepted 9 April 2020; published 18 May 2020)



284 Vol. 7, No. 4 / April 2020 / *Optica* **Research Article**

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