The Future of Communication

Nuno A. Silva[1]

[1]*Instituto de Telecomunicações, University of Aveiro, Portugal*

nasilva@ua.pt

Instituições Associadas

PTQCI Summer School
Quantum Communication & Space

Instituto Superior Técnico - Pólo de Oeiras

Society is protected by cryptography

- ❑ **Cryptography is an important pillar of the information age, and for our civilization as a whole.**

- ❑ **It secures nearly all modern communication – ranging from highly critical fields such as the exchange of classified government documents, to seemingly benign aspects as the confidentiality of a personal financial transaction.**

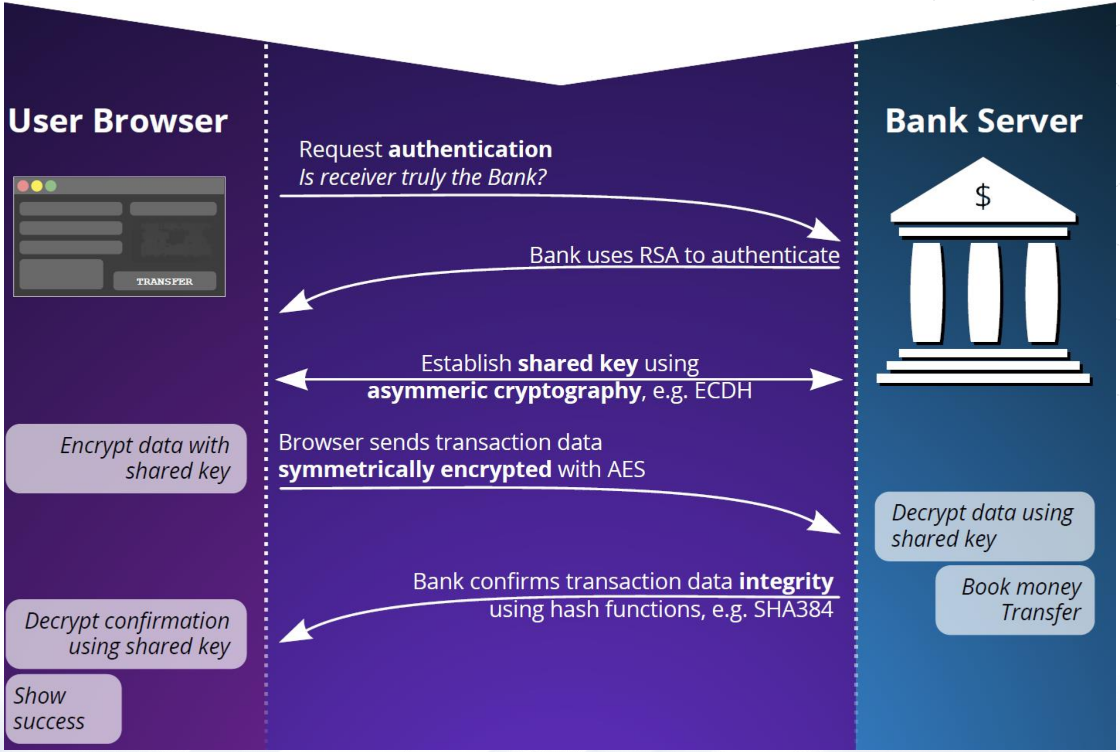
- ❑ **All critical infrastructure, the underpinning of our society, is protected by cryptography. This includes…**

Public-key cryptography: Overview

A day without safe cryptography

https://cloudsecurityalliance.org/group/quantum-safe-security/

How cryptography works today



instituto de telecomunicações | universidade de aveiro

Public-key cryptography: Overview

The RSA system:

➢ **Bob starts by selecting two large prime numbers *p* and *q*, which he multiplies so as to create a number *n*.**

➢ **Bob also chooses a number 3 ≤ e < n such that *e* and *n* have no common factor. He calculates *d* such that**

$$e*d = 1 \ (\text{mod}(p - 1)(q - 1)).$$

➢ **Once this is done, he may discard the prime numbers p and q. He publishes the pair *(e, n)* as his public key and secretly keeps the pair *(d, n)* as his private key.**

Public-key cryptography: Overview

The RSA system:

- **Encryption goes as follows: Alice calculates its *e*-th power and reduces the result modulo *n***

$$c = m^e \bmod (n)$$

- **Upon reception: Bob can decrypt the message using his private key by computing $c^d \bmod n$.**
- **The properties of modular exponentiation imply that:**

$$c^d \bmod n = m^{ed} \bmod n = m$$

instituto de telecomunicações | universidade de aveiro

Public-key cryptography: Overview

The RSA system:

- For example, with ***e* = *17*** and ***n* = *3763***, Alice can send a ciphertext as follows:

plaintext:	ju	st	th	ef	ac	to	rs	ma	am
numbers:	10, 21	19, 20	20, 8	5, 6	1, 3	20, 15	18, 19	13, 1	1, 13
together:	1021	1920	2008	506	103	2015	1819	1301	113
to the 17th power:	3397	2949	2462	3290	1386	2545	2922	2866	2634

- Bob knows the decryption exponent ***d*** and the public modulus ***n***, so he can decipher the message by raising the ciphertext to the d-th power modulo ***n***.

ciphertext:	3397	2949	2462	3290	1386	2545	2922	2866	2634
to the 1713th power:	1021	1920	2008	506	103	2015	1819	1301	113
split apart:	10, 21	19, 20	20, 8	5, 6	1, 3	20, 15	18, 19	13, 1	1, 13
plaintext:	ju	st	th	ef	ac	to	rs	ma	am

Public-key cryptography: Overview

Twenty Years of Attacks on the RSA Cryptosystem

Dan Boneh

Dan Boneh is an assistant professor of computer science at Stanford University. His e-mail address is dabo@cs.stanford.edu.

sufficient) padding algorithm may pad a plaintext M *by appending a few random bits to one of the ends prior to encryption. Adding randomness to the encryption process is necessary for proper security.*

FEBRUARY 1999 NOTICES OF THE AMS

Public-key cryptography: Overview

Possible Attacks on RSA

- Guessing *d*. ...
- Cycle Attack. ...
- Common Modulus. ...
- Faulty Encryption. ...
- Low Exponent. ...
- Factoring the Public Key.

✓The prizes for RSA-576 and RSA-640 have been awarded. The remaining prizes have been retracted since the challenge became inactive in 2007.

RSA number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US$1,000[4]	April 1, 1991[5]	Arjen K. Lenstra
RSA-110	110	364	US$4,429[4]	April 14, 1992[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	$5,898[4]	July 9, 1993[6]	T. Denny *et al.*
RSA-129 [**]	129	426	$100 USD	April 26, 1994[5]	Arjen K. Lenstra *et al.*
RSA-130	130	430	US$14,527[4]	April 10, 1996	Arjen K. Lenstra *et al.*
RSA-140	140	463	US$17,226	February 2, 1999	Herman te Riele *et al.*
RSA-150	150	496		April 16, 2004	Kazumaro Aoki *et al.*
RSA-155	155	512	$9,383[4]	August 22, 1999	Herman te Riele *et al.*
RSA-160	160	530		April 1, 2003	Jens Franke *et al.*, University of Bonn
RSA-170 [*]	170	563		December 29, 2009	D. Bonenberger and M. Krone [***]
RSA-576	174	576	$10,000 USD	December 3, 2003	Jens Franke *et al.*, University of Bonn
RSA-180 [*]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University[7]
RSA-190 [*]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	$20,000 USD	November 2, 2005	Jens Franke *et al.*, University of Bonn
RSA-200 [*] ?	200	663		May 9, 2005	Jens Franke *et al.*, University of Bonn
RSA-210 [*]	210	696		September 26, 2013[8]	Ryan Propper
RSA-704 [*]	212	704	$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA-220 [*]	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA-230	230	762			
RSA-232	232	768			
RSA-768 [*]	232	768	$50,000 USD	December 12, 2009	Thorsten Kleinjung *et al.*
RSA-240	240	795			

Worldwide Effort

CISA Announces Post-Quantum Cryptography Initiative

THE WHITE HOUSE

Released: July 06, 2022

An official website of the United States government

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Government and critical infrastructure organizations must take coordinated preparatory actions now to ensure a fluid migration to the new post-quantum cryptographic standard that the National Institute of Standards and Technology (NIST) will publish in 2024.

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

SWEDISH ARMED FORCES

French Cybersecurity Agency (ANSSI)
Netherlands National Communications Security Agency (NLNCSA)
Federal Office for Information Security (BSI)
Swedish National Communications Security Authority, Swedish Armed Forces

Jan 26, 2024

Position Paper on Quantum Key Distribution

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

PRESS RELEASE | Publication 11 April 2024

Commission publishes Recommendation on Post-Quantum Cryptography

European Commission

Shaping Europe's digital future

This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution.

Public-key cryptography: Overview

- Not only the RSA it is in risk

Cryptographic function	Protocol	QC Attack	Impact
Key exchange & Digital signatures	RSA, DH, ECC	Shor	**Broken**
Data encription	DES, AES	Groover	**Weakened**
Authentication	MAC, AEAD	Simon	**Broken**

Public-key cryptography: Overview

Shor's algorithm is a polynomial-time quantum computer algorithm for integer factorization

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechan ics conferred extra power to computation, he did show tha a Turing machine could be simulated by the reversible uni tary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] wa the first to give an explicit model of quantum computation He defined both quantum Turing machines and quantun circuits and investigated some of their properties.

The next part of this paper discusses how quantum com putation relates to classical complexity classes. We wil thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e. memory). The field of analysis of algorithms consider the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretica computer scientists generally classify algorithms as effi

Quantum computing: Shor algorithm

- Shor's algorithm is based on number theory for factoring. Suppose we want to find the prime factors (*Q*, *R*) of an integer *P*; i.e., $P = Q \times R$.
- Algorithm for finding the prime factors of an integer:

1. Choose a random number, say ***a***
2. Calculate $a^x \bmod P$ where $x = 0, 1, 2, 3, \ldots$ For $P=15$, $Q=3$, $R=5$

$$7^0 \bmod 15, 7^1 \bmod 15, 7^2 \bmod 15, 7^3 \bmod 15,$$
$$7^4 \bmod 15, 7^5 \bmod 15, 7^6 \bmod 15, 7^7 \bmod 15, \ldots$$
$$= 1, 7, 4, 13, 1, 7, 4, 13, \ldots,$$

Quantum computing: Shor algorithm

3. Find the periodicity of the above number sequence. In this example, r = 4 because the four numbers 1, 7, 4 and 13 repeats; i.e., $a^x \bmod P$ is a periodic function

4. If *r* is an odd number, start over. Otherwise, if *r* is an even number, then Q and R are given by

$Q = gcd(a^{r/2} - 1, P)$ and $R = gcd(a^{r/2} + 1, P)$ where *gcd* is the greatest common divisor.

Quantum computing: Shor algorithm

- For our example

$$Q = \gcd\left(a^{r/2} - 1, P\right) = \gcd\left(7^2 - 1, 15\right) = \gcd(48, 15)$$
$$= 3, \text{ since } 48/3 = 16 \text{ and } 15/3 = 5$$
$$R = \gcd\left(a^{r/2} + 1, P\right) = \gcd\left(7^2 + 1, 15\right) = \gcd(50, 15)$$
$$= 5, \text{ since } 50/5 = 10 \text{ and } 15/5 = 3$$

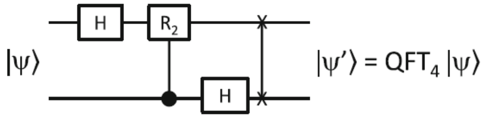
- There are efficient classical algorithms (Euclid's algorithm) for efficiently finding the ***gcd***. Therefore, the factoring problem reduces to efficiently finding the period (r) of the function $a^x \bmod P$.

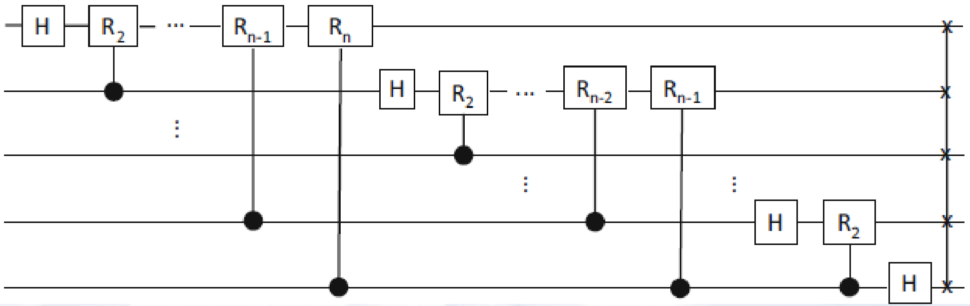
Quantum computing: Shor algorithm

Period Finding

- The Quantum Fourier Transform (QFT) is useful when there is an underlying periodicity to the wavefunction.

- In the QFT, we do a Discrete Fourier Transform on the amplitudes of a quantum state.

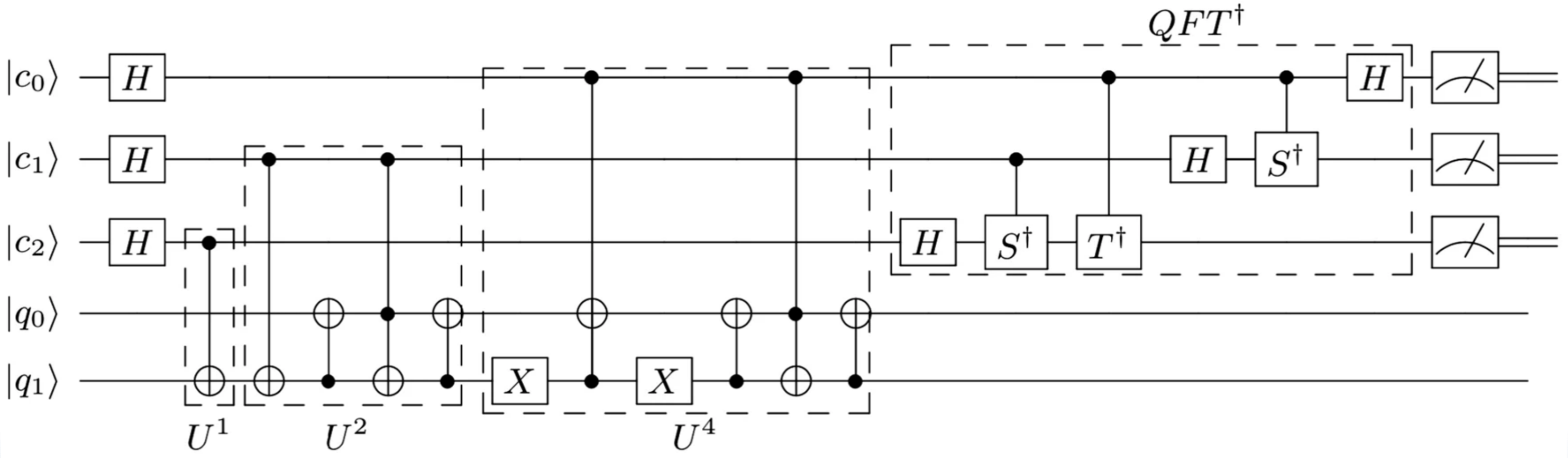




$$R_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^k} \end{pmatrix}$$

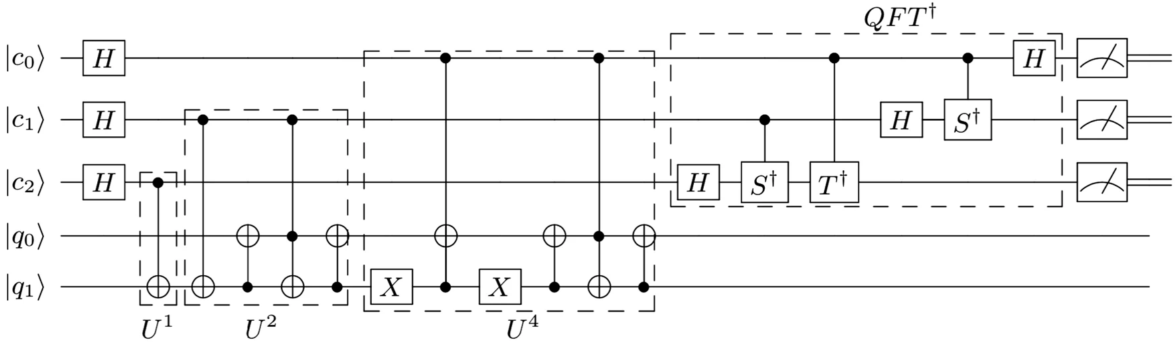
Quantum computing: Shor algorithm

An example for factoring 21 using 5 quibts on IBM quantum processors



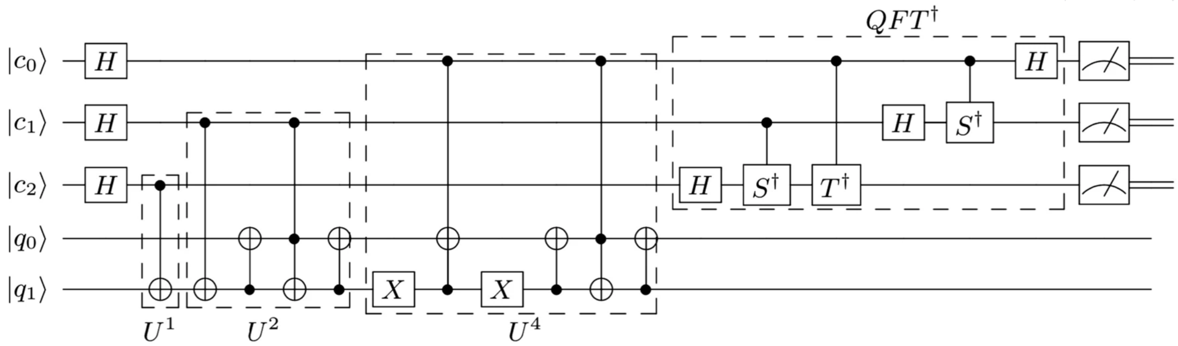
Quantum computing: Shor algorithm

An example for factoring 21 using 5 quibts on IBM quantum processors



1. Problem: Find the factors of a prime number n
2. Order nding: nd the least positive integer r ∈ {0, 1, . . .N} such that a^rmod(n)=1.
3. where a is an integer smaller than n picked at random.
4. This is done on the quantum computer!
5. All the other operations can be done on a classical computer

Quantum computing: Shor algorithm



Classical counterpart

- Compute gcd(a^r/2 + 1, n) and gcd(a^r/2 − 1, n) , i.e., the greatest common divisor;
- For n = 21, a = 4, and r = 3 we have gcd(9, 21) = 3 and gcd (7 , 21) = 7
- This is the factorization of the prime number!

Quantum computing: Shor algorithm

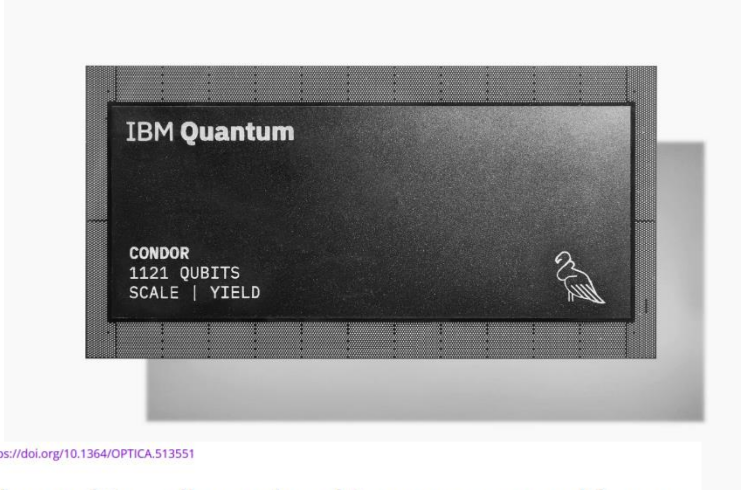
Where we are today in terms of number of qubits?

Technology

Record-breaking quantum computer has more than 1000 qubits

Atom Computing has created the first quantum computer to surpass 1000 qubits, which could improve the accuracy of the machines

By Alex Wilkins



Technology

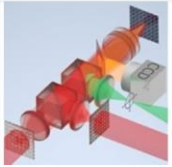
Record-breaking number of qubits entangled in a quantum computer

A group of 51 superconducting qubits have been entangled inside a quantum computer, not just in pairs but in a complex system that entangles each qubit to every other one

By Karmela Padavic-Callaghan

12 July 2023

Optica Vol. 11, Issue 2, pp. 222-226 (2024) • https://doi.org/10.1364/OPTICA.513551



Supercharged two-dimensional tweezer array with more than 1000 atomic qubits

Lars Pause, Lukas Sturm, Marcel Mittenbühler, Stephan Amann, Tilman Preuschoff, Dominik Schäffner, Malte Schlosser, and Gerhard Birkl

instituto de telecomunicações | universidade de aveiro

Quantum computing: Shor algorithm

- The question is: In practice what really the numbers that we already factored?

- We can factor the number 21 with the IBM quantum computer!

- Neverthless, when we try to factorize number 35 using Shor's algorithm using a quantum computer... the algorithm failed because of accumulating errors

PHYSICAL REVIEW A **100**, 012305 (2019)

Experimental study of Shor's factoring algorithm using the IBM Q Experience

Mirko Amico,[1] Zain H. Saleem,[2] and Muir Kumph[3]
[1]*The Graduate School and University Center, The City University of New York, New York, New York 10016, USA*
[2]*Theoretical Research Institute of Pakistan Academy of Sciences, Islamabad 44000, Pakistan*
[3]*IBM T. J. Watson Research Center, Yorktown Heights, New York 10598, USA*

(Received 2 March 2019; published 8 July 2019)

We study the results of a compiled version of Shor's factoring algorithm on the *ibmqx5* superconducting chip, for the particular case of $N = 15$, 21, and 35. The semiclassical quantum Fourier transform is used to implement the algorithm with only a small number of physical qubits, and the circuits are designed to reduce the number of gates to the minimum. We use the square of the statistical overlap to give a quantitative measure of the similarity between the experimentally obtained distribution of phases and the predicted theoretical distribution of phases for different values of the period. This allows us to assign a period to the experimental data without the use of the continued fraction algorithm. A quantitative estimate of the error in our assignment of the period is then given by the overlap coefficient.

DOI: 10.1103/PhysRevA.100.012305

instituto de telecomunicações

universidade de aveiro

Quantum computing: Shor algorithm

- The question: largest integer factored?

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

- We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm

Quantum computing: Shor algorithm

▶ Nevertheless…

A comment on "Factoring integers with sublinear resources on a superconducting quantum processor"

Tanuj Khattar[1,*] and Noureldin Yosri[2,†]

▶ we present an open-source implementation of the algorithm proposed by Yan et. al. and show that, even if we had a perfect quantum optimizer (instead of a heuristic like QAOA), the proposed claims don't hold true. Specifically, our implementation shows that the claimed sublinear lattice dimension for the Hybrid quantum+classical version of Schnorr's algorithm successfully factors integers only up to 70 bits!

instituto de telecomunicações | universidade de aveiro

Quantum computing: Shor algorithm

In practice, for a 2048 bits long RSA key, a malicious party would have to factorize something like:

1001644446681287751665134759209287760699932586715613490212647487057640131037150919793784 9497
3206182887984793481686168486286432644921428015547375730384153767035148690585574578895329 4686653
0566785268785568529811591040431130318040428710035458810831300648246773571504774325603612 8648480
8002719476248596585614014586422840074399930315657038208908677586573105529672414352122132 7468628
2195017126636063707376319376682705745720614662725215888360626639392643144722734269562862 3860494
8307618854998029560699082773196868742950778879278028644088217277000136795791170000068594 9637652
3883191447050929338233266941886830143678124885388500037066377835258125323927025715687166 0127150
0172576593385137863568965115176352714409927444772385737279747445266365072542238725601184 6500895
5604986268313564020629886261267911972070996858603421516099726030422015567343415113566832 0749865
8480793209312453902915691263483616045672800775320189807289782781559045999929529890822355 7195231
5897776372444163902817853904622495224753073188723909276916118985080359484732611986446218 1341673
6071601236994697502076824266159232358545997228507023610161642367243965317272447999925676 798119
7156009391944768555108382904714203968530197715359092484432633205677215978669352193544729 9870583
1 [2]

Quantum computing: Shor algorithm

Shor's algorithm could be used to break public-key cryptography schemes, such as the widely used RSA scheme

- This if we have sufficient number of qubits!!

doi:10.1103/PhysRevLett.127.140503

Factoring 2 048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory

Élie Gouzien* and Nicolas Sangouard†
Université Paris–Saclay, CEA, CNRS, Institut de Physique Théorique, 91 191 Gif-sur-Yvette, Fran
(Dated: September 29, 2021)

We analyze the performance of a quantum computer architecture combining a small processor and a storage unit. By focusing on integer factorization, we show a reduction by several orders of magnitude of the number of processing qubits compared with a standard architecture using a planar grid of qubits with nearest-neighbor connectivity. This is achieved by taking advantage of a temporally and spatially multiplexed memory to store the qubit states between processing steps. Concretely, for a characteristic physical gate error rate of 10^{-3}, a processor cycle time of

Quantum computing: Shor algorithm

Shor's algorithm could be used to break public-key cryptography schemes, such as the widely used RSA scheme

- This if we have sufficient number of qubits!!

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

The New York Times

The Race to Save Our Secrets From the Computers of the Future

Quantum technology could compromise our encryption systems. Can America replace them before it's too late?

By Zach Montague
Reporting from Washington

Oct. 22, 2023

They call it Q-Day: the day when a quantum computer, one more powerful than any yet built, could shatter the world of privacy and security as we know it.

It would happen through a bravura act of mathematics: the separation of some very large numbers, hundreds of digits long, into their prime factors.

That might sound like a meaningless division problem, but it would fundamentally undermine the encryption protocols that governments and corporations have relied on for decades. Sensitive information such as military intelligence, weapons designs, industry secrets and banking information is often transmitted or stored under digital locks that the act of factoring large numbers could crack open.

"This is potentially a completely different kind of problem than one we've ever faced," said Glenn S. Gerstell, a former general counsel of the National Security Agency and one of the authors of an expert consensus report on cryptology. "It may be that there's only a 1 percent chance of that happening, but a 1 percent chance of something catastrophic is something you need to worry about."

Q-Day

When to Switch to Quantum Secure?

- Q = # years to first large quantum computer … between 20 and 30
- X = # years it takes to switch … between 10 and 20
- Y = # years data needs to be confidential … ?

Need to start the switching in the year S = 2024 + Q – X - Y

If Y is equal to 10 it is about time, if it is small than 10 you are still ok, if it is more than 10 you are already late !!!

Mosca, Michele, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, September/October 2018, doi: 10.1109/MSP.2018.3761723.

Quantum cryptography

The most successful and commercially available application in quantum cryptography are the Quantum Key Distribution systems.

Other applications in the field of quantum cryptography are:

- **Quantum Random Number Generators**
- **Quantum Bit Commitment;**
- **Quantum Oblivious Transfer;**

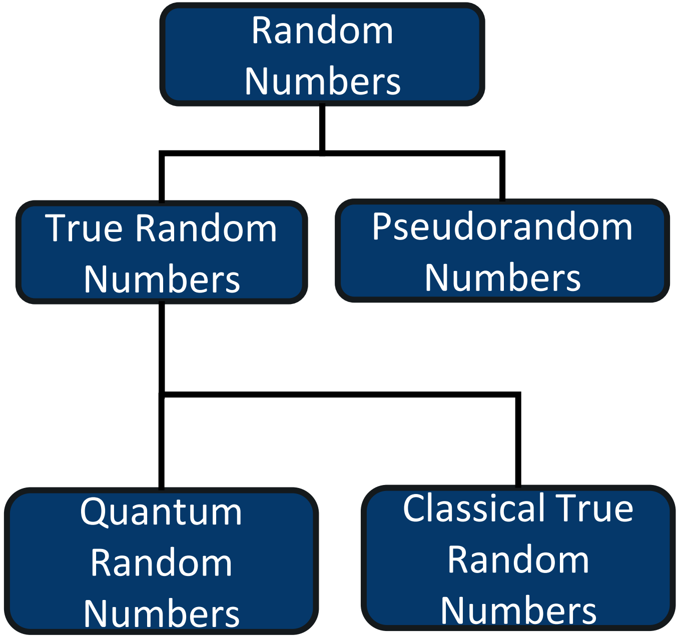
Quantum cryptography

Starting from the simplest quantum cryptographic system:

Quantum random number generators

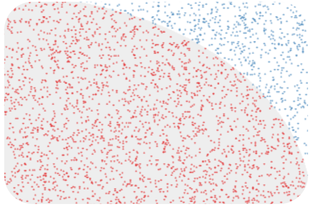
- **Only physical processes can generate true random numbers;**
- **They are in the field of data encryption, for example to create random cryptographic keys to encrypt data;**
- **They are a more secure alternative to pseudorandom number generators (PRNGs), software programs commonly used in computers to generate pseudo-random numbers.**

Quantum random number generators



- Why do we need random numbers?

Statistical Analysis



Simulation

(ex: Monte Carlo)

6 5 3 1 8 7 2 4

Randomized Algorithms

Decision Making

Gaming & Lotteries

Cryptography (ex: TLS, Quantum Key Distribution)

Quantum random number generators

In classical cryptography:

- one-time keys
- challenge-response data
- Public key cryptography - Diffie-Hellman

Quantum cryptography. All QKD protocols assume a local TRNG

- Discrete-Variable QKD
- Continuous Variable QKD
- Entangled-based QKD protocols

Quantum random number generators

For cryptographic purpose:

- ❖ An attacker that knows the whole sequence cannot guess the next bit with a probability better than one-half.
- ❖ The knowledge of a part of the sequence shall not permit an attacker to compute the previous values of the generator with better accuracy than guessing.

PHYSICAL REVIEW A 86, 062308 (2012)

Weak randomness seriously limits the security of quantum key distribution

Jan Bouda,[1,*] Matej Pivoluska,[1] Martin Plesch,[1,2] and Colin Wilmott[1]

M. Herrero-Collantes et al, "Quantum random number generators", REVIEWS OF MODERN PHYSICS, 2017

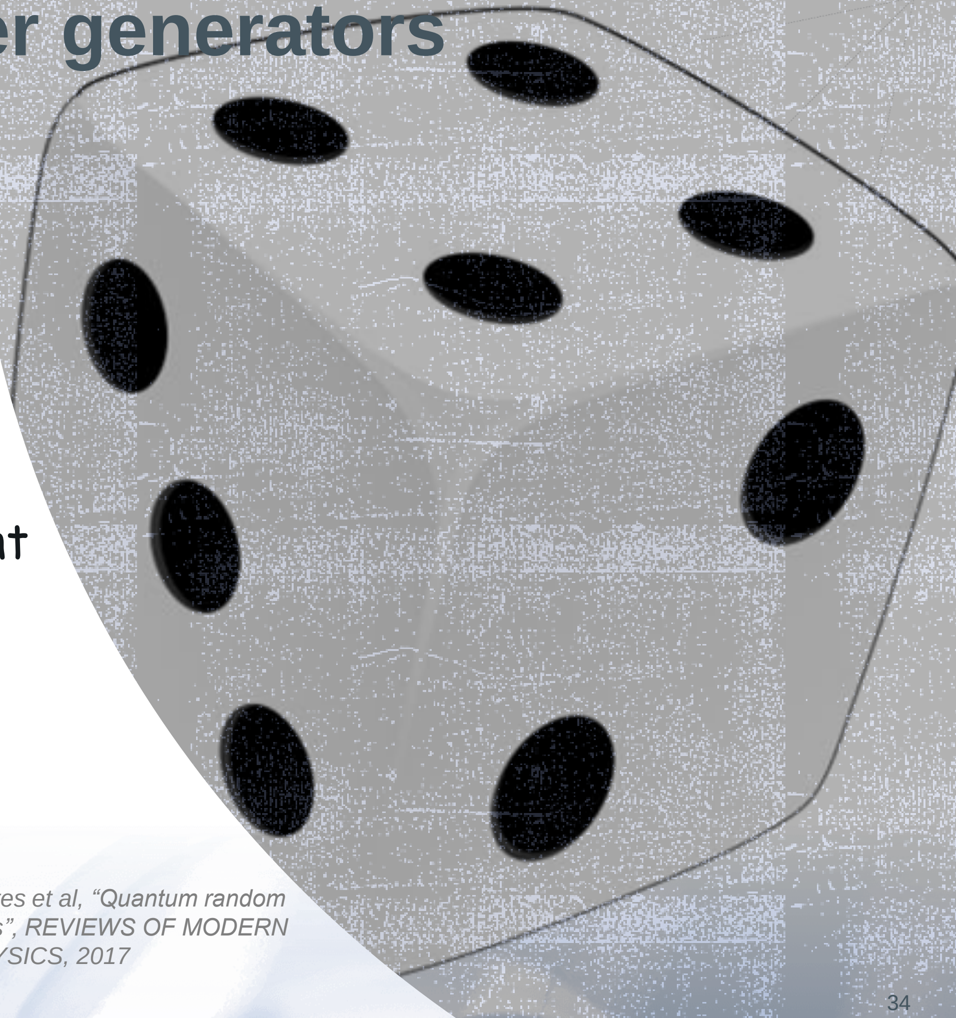
Quantum random number generators

Quantum random number generator relies on a physical process whose **randomness** is guaranteed by laws of **Quantum Mechanics.**

Examples of such processes are:

- Path superposition and measurement
- Photon number statistics
- Time of arrival statistics
- Laser phase noise
- Shot-noise measurement
- …

M. Herrero-Collantes et al, "Quantum random number generators", REVIEWS OF MODERN PHYSICS, 2017



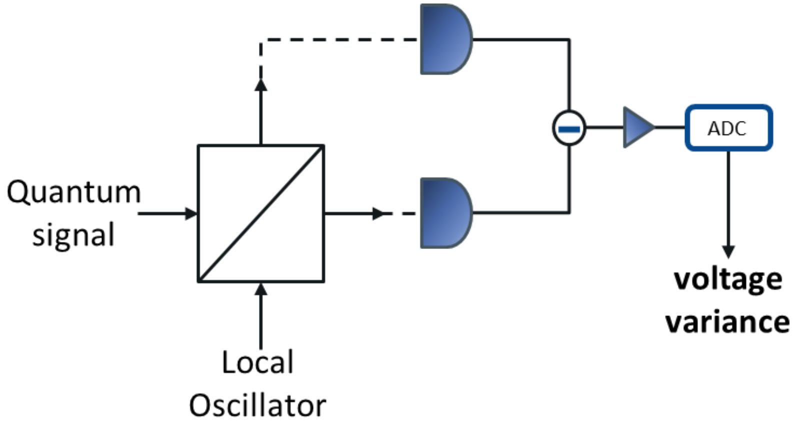
instituto de telecomunicações

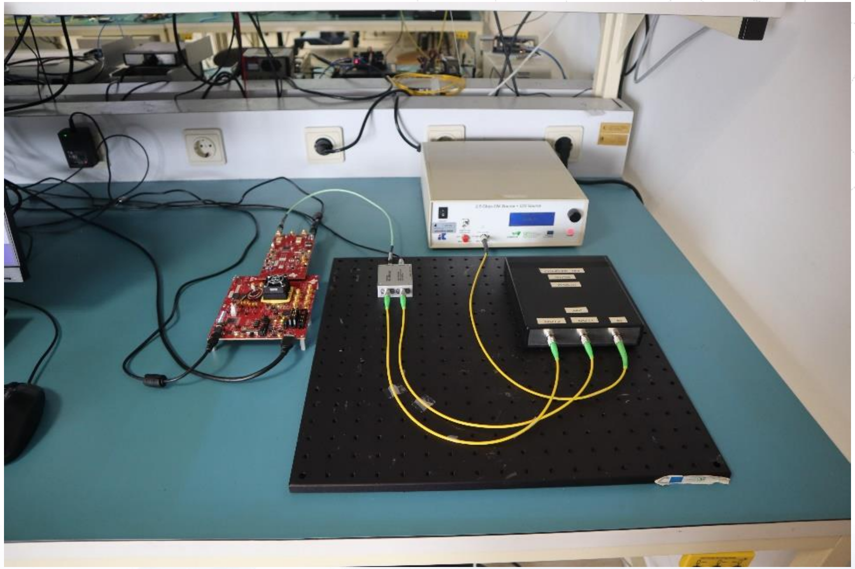
universidade de aveiro

34

Quantum random number generators

The homodyne detection system





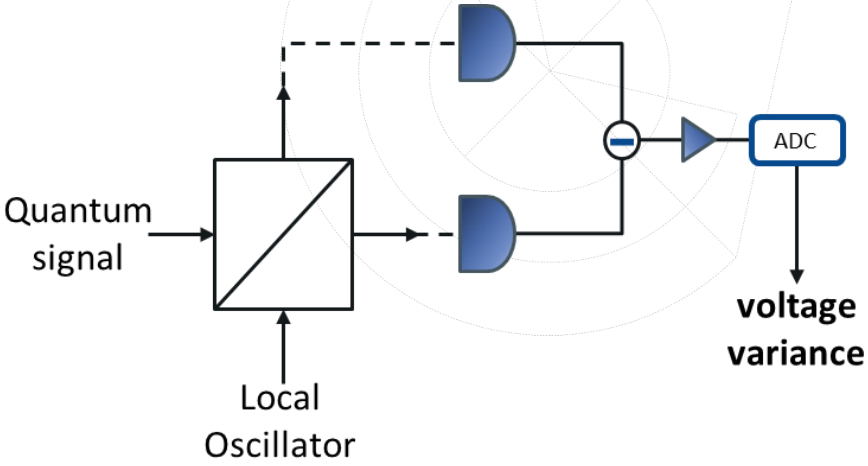
M. Ferreira et al, "Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations", Applied Science, 2021

Quantum random number generators

The homodyne detection system allows for the measurement of quadrutues:

$$\langle \hat{v} \rangle_x \propto \frac{1}{2} \int d\tau \langle \hat{a}_S^\dagger(\tau)\hat{a}_{LO}(\tau) + \hat{a}_{LO}^\dagger(\tau)\hat{a}_s\ (\tau)\rangle h(t-\tau)$$

$$\langle \hat{v} \rangle_p \propto \frac{\iota}{2} \int d\tau \langle \hat{a}_S^\dagger(\tau)\hat{a}_{LO}(\tau) + \hat{a}_{LO}^\dagger(\tau)\hat{a}_s\ (\tau)\rangle h(t-\tau)$$



The variance of the measured voltage is proportional to:

$$\sigma^2 \propto \langle \hat{n}_{LO} \rangle + \langle \hat{n}_S \rangle$$

If $\hat{a}_s$ is in a vacuum state:

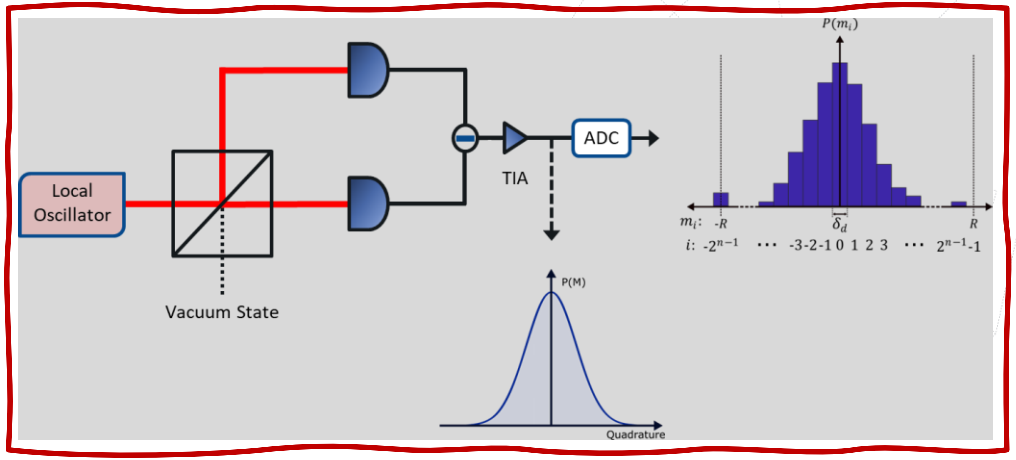
$$\sigma^2 \propto \langle \hat{n}_{LO} \rangle \rightarrow Shot\ noise$$

M. Ferreira et al, "Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations", Applied Science, 2021

Quantum random number generators

- Output proportional to the amplitude quadrature of the vacuum state, which follows a Gaussian distribution.

- Measurements contain simultaneously quantum and classical contributions.



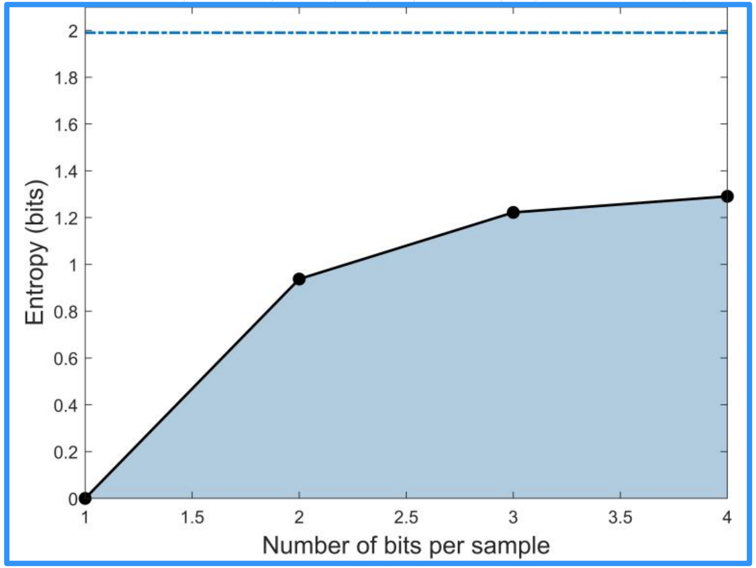
› Randomness extraction stage necessary to attain true random numbers

Quantum random number generators

Shannon entropy

$$\mathrm{H_q}(x) = n - \sum_{i=1}^{2^n} p_i^e \log_2 p_i^e$$

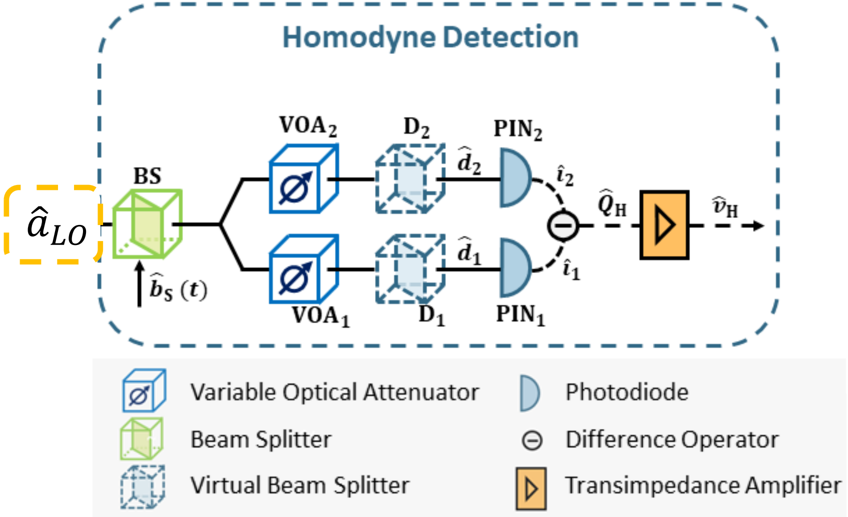
- The homodyne measurement distribution is divided into a set of 2^n equiprobable bins.
- The binning consistently converges to a **4-bit** sequence.
- A theoretical maximum of **1.99 bits** per sample can be extracted.
- Extraction ratio of **0.323** true random bits per raw bit



M. Ferreira et al, "Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations", Applied Science, 2021

Quantum random number generators

✓ Real Devices: Unbalanced homodyne detection



$$\hat{d}_1(t) = \sqrt{\left(\tfrac{1}{2} - \Delta\right)\eta_{\mathrm{PIN1}}\eta_{\mathrm{VOA1}}}\,\hat{a}_{\mathrm{LO}}(t) + \sqrt{\left(\tfrac{1}{2} + \Delta\right)\eta_{\mathrm{PIN1}}\eta_{\mathrm{VOA1}}}\,\hat{b}_{\mathrm{S}}(t) + \sqrt{\eta_{\mathrm{PIN1}}(1-\eta_{\mathrm{VOA1}})}\,\hat{b}_{\mathrm{VOA1}}(t) + \sqrt{1-\eta_{\mathrm{PIN1}}}\,\hat{b}_{\mathrm{PIN1}}(t)$$

$$\hat{d}_2(t) = \sqrt{\left(\tfrac{1}{2} - \Delta\right)\eta_{\mathrm{PIN2}}\eta_{\mathrm{VOA2}}}\,\hat{b}_{\mathrm{S}}(t) - \sqrt{\left(\tfrac{1}{2} + \Delta\right)\eta_{\mathrm{PIN2}}\eta_{\mathrm{VOA2}}}\,\hat{a}_{\mathrm{LO}}(t) + \sqrt{\eta_{\mathrm{PIN2}}(1-\eta_{\mathrm{VOA2}})}\,\hat{b}_{\mathrm{VOA2}}(t) + \sqrt{1-\eta_{\mathrm{PIN2}}}\,\hat{b}_{\mathrm{PIN2}}(t),$$

$$C_v(t, t+\tau) = 2g_{\mathrm{TIA}}^2 \frac{k_B T}{R} \int_{-\infty}^{+\infty} d\tau' h(t-\tau')h(t+\tau-\tau') + q_e^2 g_{\mathrm{TIA}}^2 \beta |\alpha_{lo}|^2 \int_{-\infty}^{+\infty} d\tau' |\xi(\tau')|^2 h(t-\tau')h(t+\tau-\tau') + q_e^2 g_{\mathrm{TIA}}^2 \gamma^2 \mathrm{RIN}|_{B_e} |\alpha_{lo}|^4 \int_{-\infty}^{+\infty} d\tau' |\xi(\tau')|^4 h(t-\tau')h(t+\tau-\tau').$$

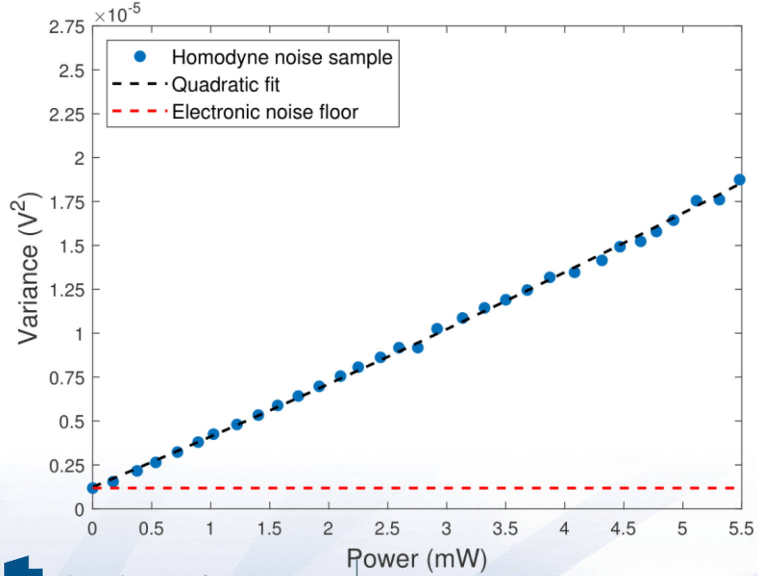
› The variance is now dependente of RIN of the LO

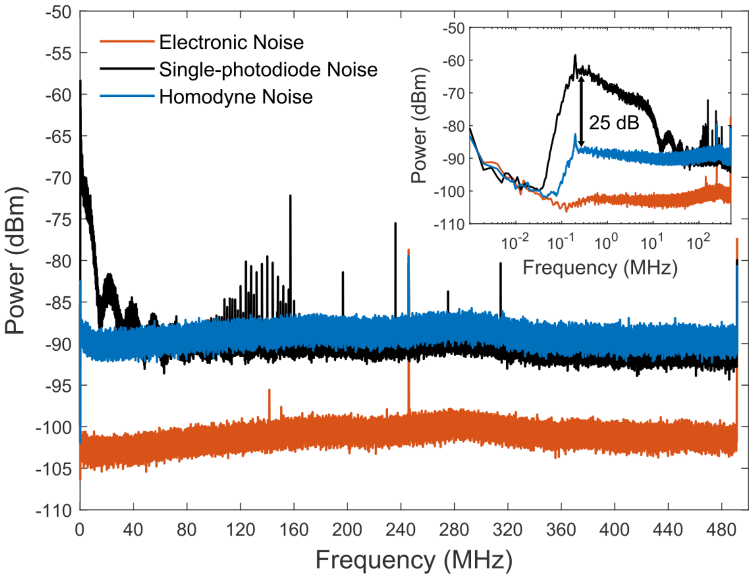
M. Almeida et al, *"Impact of imperfect homodyne detection on measurements of vacuum states shot noise", Optical and Quantum Electronics, 2020*

Quantum random number generators

✓ **Real Devices: Unbalanced homodyne detection**

$$\sigma^2 = 6.15 \times 10^{-8}\, P_{LO}^2 + 2.81 \times 10^{-6}\, P_{LO} + 1.24 \times 10^{-6}\ [V^2]$$





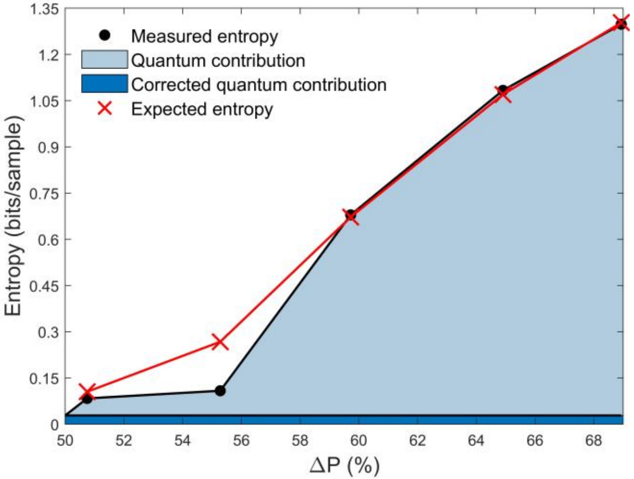
› Clear preponderance of quantum the quantum fluctuations was observed.

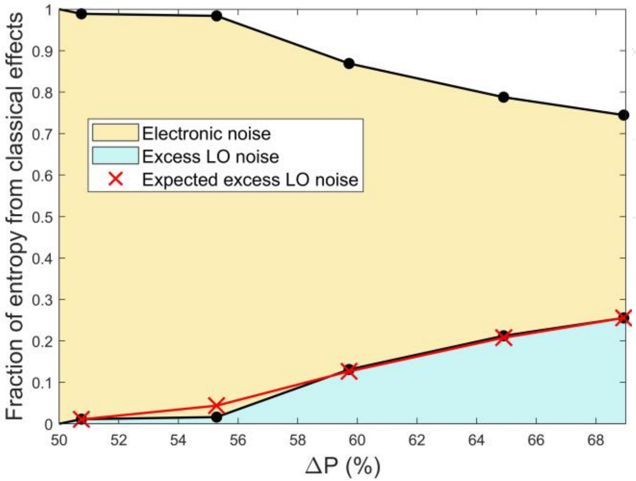
instituto de telecomunicações
universidade de aveiro

Quantum random number generators

➢ Excess LO Noise

$$\sigma^2 = \frac{2\pi}{3} G_{\mathrm{TIA}}^2 \Delta f \left[2\frac{k_b T}{R} + q\beta + \boldsymbol{q\mathrm{RIN}\gamma^2} \right] + \frac{\boldsymbol{\delta_d}^{\boldsymbol{2}}}{\boldsymbol{12}}$$





› An unbalanced detection results on an apparent entropy increase.

› Additional entropy contribution of **0.0554 bits** found due to imperfect detection balancing.

Quantum cryptography: The beautiful idea

- **The first protocol for quantum cryptography was proposed in 1984 by Charles H. Bennett, of IBM and Gilles Brassard.**

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomemon, the Einstein-Podolsky-Rosen paradox.

I. Introduction

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where otherwise noted the protocols are provably secure even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws.

Quantum cryptography: The beautiful idea

➢ **Following Wootters and Zurek (1982) one can easily prove that perfect copying is impossible in the quantum world:**

A single quantum cannot be cloned

W. K. Wootters*

Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, USA

W. H. Zurek

Theoretical Astrophysics 130–33, California Institute of Technology, Pasadena, California 91125, USA

If a photon of definite polarization encounters an excited atom, there is typically some nonvanishing probability that the atom will emit a second photon by stimulated emission. Such a photon is guaranteed to have the same polarization as the original photon. But is it possible by this or any other process to amplify a quantum state, that is, to produce several copies of a quantum system (the polarized photon in the present case) each having the same state as the original? If it were, the amplifying process could be used to ascertain the exact state of a quantum system: in the case of a photon, one could determine its polarization by first producing a beam of identically polarized copies and then measuring the Stokes parameters[1]. We show here that the linearity of quantum mechanics forbids such replication and that this conclusion holds for all quantum systems.

Quantum cryptography: The beautiful idea

- **In the BB84 protocol two sets of polarization states called the ⊕ and ⊗ bases are used:**

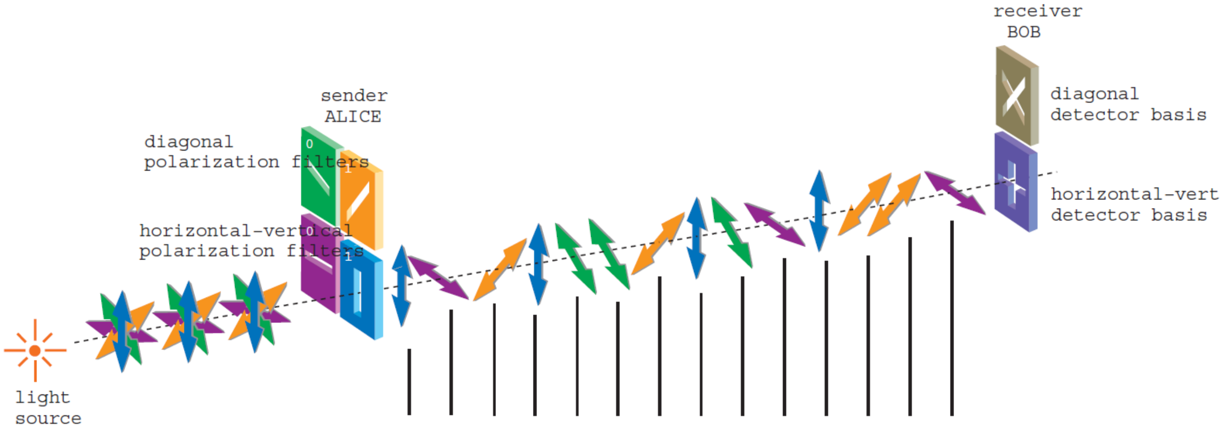
1. **The ⊕ basis: Binary 1 and 0 corresponds to photons with polarization angles of 0◦ and 90◦, respectively.**
2. **The ⊗ basis: Binary 1 and 0 corresponds to photons with polarization angles of 45◦ and 135◦, respectively.**

- **The two polarization states for the ⊕ basis can be represented in Dirac notation by |↕> and |↔>;**
- **The two states for the ⊗ basis are represented by $|\nearrow\rangle$ and $|\nwarrow\rangle$**

Basis	Binary 1	Binary 0
⊕	$\|\updownarrow\rangle$ $\theta = 0^\circ$	$\|\leftrightarrow\rangle$ $\theta = 90^\circ$
⊗	$\|\swarrow\!\nearrow\rangle$ $\theta = 45^\circ$	$\|\nwarrow\!\searrow\rangle$ $\theta = 135^\circ$

Quantum cryptography: The beautiful idea

- **A scheme for quantum cryptography according to the BB84 protocol is shown in the Figure:**



ALICE's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
BOB's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
BOB's measurements	1	0	0	1	0	0	1	1	0	0	0	1	0	0
retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Quantum cryptography: The beautiful idea

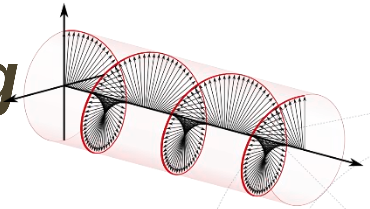
- **In the BB84 protocol the following steps are taken:**

A's data	1	0	0	1	1	1	0	0	1	0	0	1
A's basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
θ (°)	0	135	90	45	45	0	90	135	0	135	135	0
B's basis	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$
B's result	1	0	0	0	1	1	0	1	1	0	1	1
Same basis ?	n	y	y	n	y	y	n	n	y	y	n	n
Sifted bits		0	0		1	1			1	0		
Data check ?		y	n		y	n			y	n		
Private key			0			1				0		

Representative sequence of data choices according to the BB84 protocol. θ is the polarization angle according to the encoding scheme

Basis	Binary 1	Binary 0
$\oplus$	$\lvert\updownarrow\rangle$ $\theta = 0^\circ$	$\lvert\leftrightarrow\rangle$ $\theta = 90^\circ$
$\otimes$	$\lvert\nearrow\rangle$ $\theta = 45^\circ$	$\lvert\nwarrow\rangle$ $\theta = 135^\circ$

DV-QKD *Polarization Encoding*

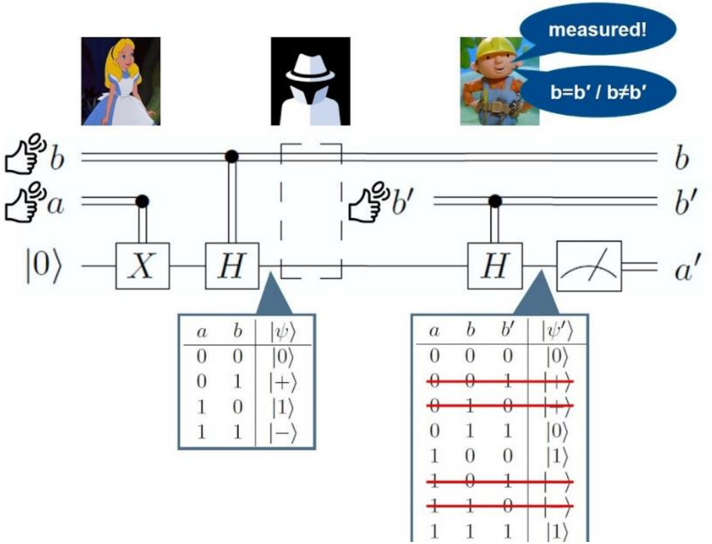


Why?

- ✓ Explored in the original BB84
- ✓ Polarization encoding with long-term temporal stability and low intrinsic QBER
- ✓ Simpler security proofs
- ✓ Degree-of-freedom most suitable for satellite-based QKD

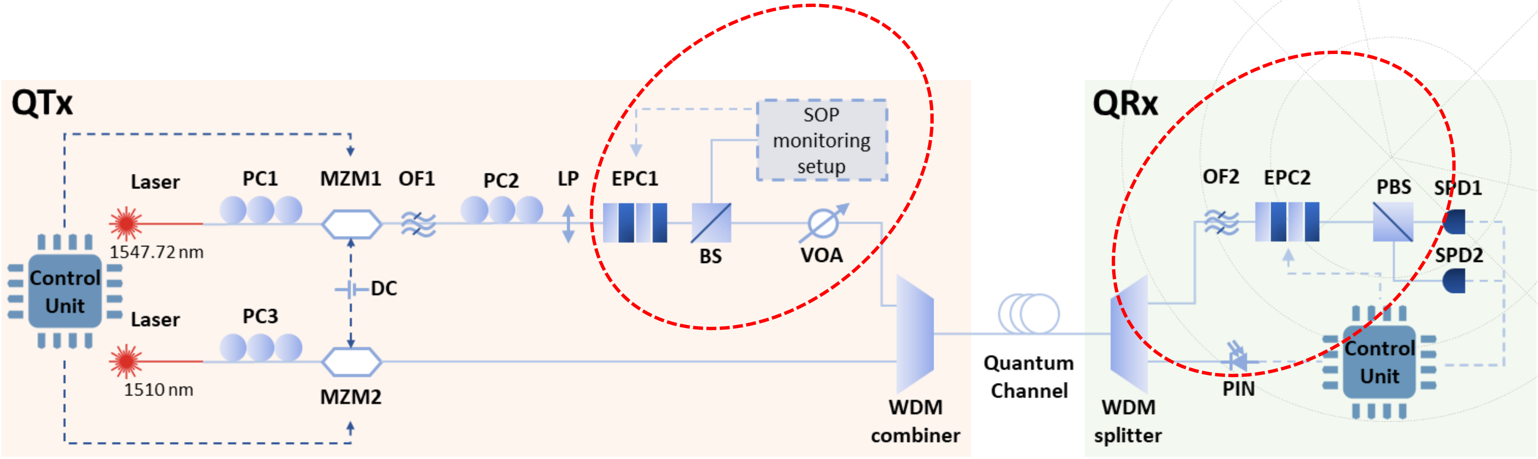
Current Challenges

- ✓ Optimization of coding/decoding for simpler implementations
- ✓ Co-existence between classical and quantum signals
- ✓ Integration of quantum networks with satellite-based links



The BB84 protocol

DV-QKD Experimental Setup



- **At the transmitter**, two signals are generated: a reference and a quantum signal, co-propagated in the quantum channel in a WDM approach.
- **At the receiver**, the reference signal is used for synchronization, and the quantum signal is measured by two single photon detectors.

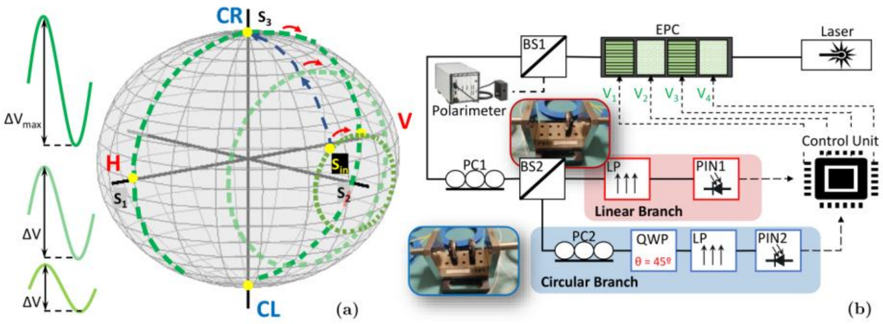
We have proposed, implemented and experimentally validated novel polarization encoding and polarization drift compensation schemes

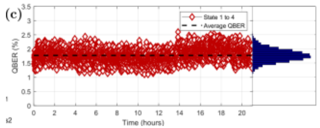
instituto de telecomunicações

universidade de aveiro

Implementation of Polarization Generation/Control Methods

Polarization States Generation

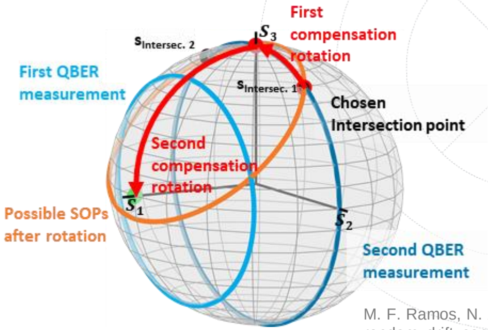




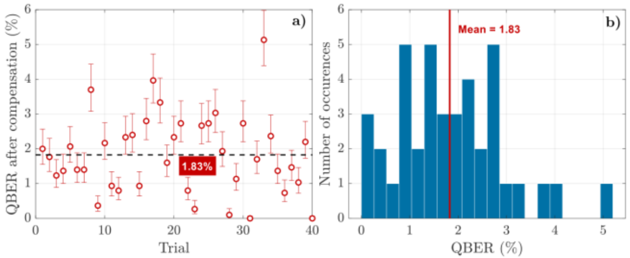
The average QBER after 21 hours was 1.8%, with only one calibration at the beginning of the measurements.

S. T. Mantey, M. F. Ramos, N. A. Silva, A. N. Pinto and N. J. Muga, "Demonstration of an Algorithm for Quantum State Generation in Polarization-Encoding QKD Systems," OFC, *San Diego, USA, March, 2022.*

Reversal Operator Basis Alignment



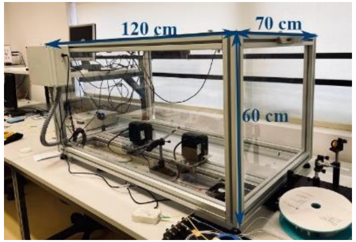
M. F. Ramos, N. A. Silva, N. J. Muga, A. N. Pinto, Full polarization random drift compensation method for quantum communication, Optics Express, 30(5):6907-6920, 2022.

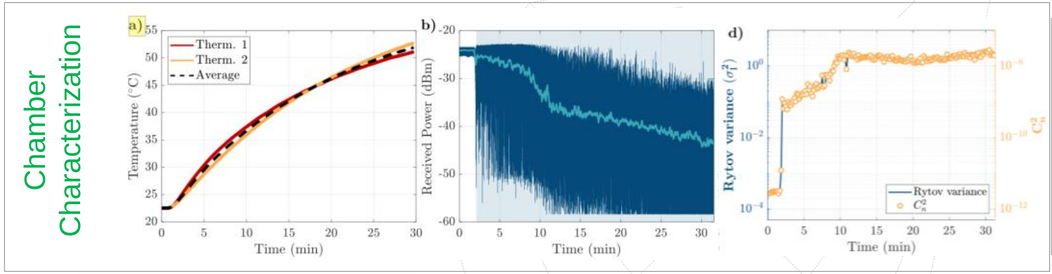


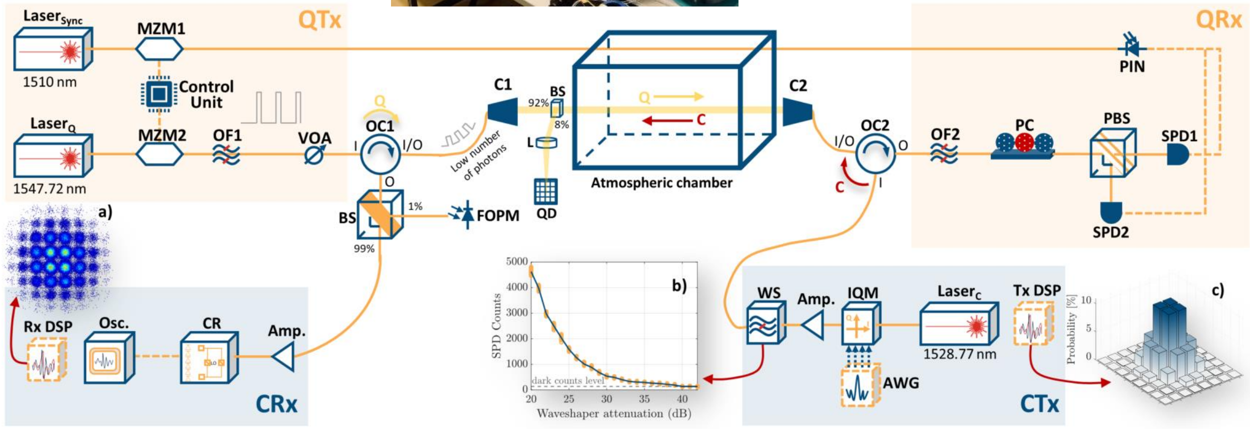
The experimental implementation has shown that the system is able to operate with an average QBER of 1.8%.

S. T. Mantey, M. F. Ramos, N. A. Silva, A. N. Pinto and N. J. Muga, Polarization Control Through Reversal Operator for QKD Systems, tb submitted to Optics Express, 2024.

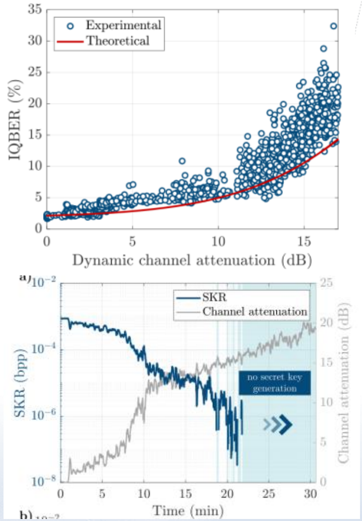
Coexistence of Quantum and Classical Signal Transmission Over Turbulent FSO Channels







Quantum signal performance



Fiber-wireless optical system that transmitted a 64-QAM 400 Gbps classical signal for high-rate data exchange and a 1 MHz quantum signal for QKD.

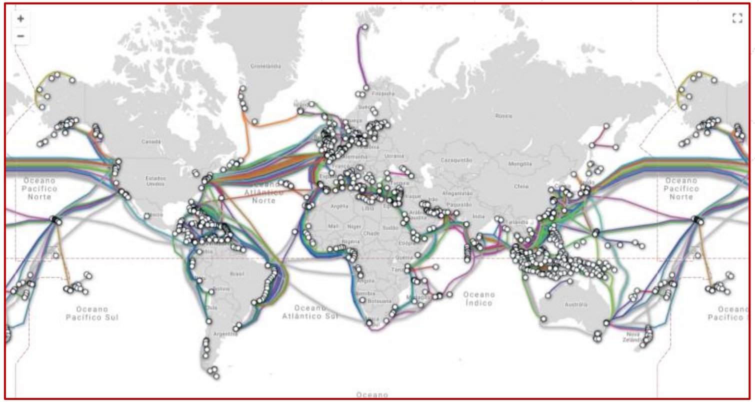
instituto de telecomunicações

universidade de aveiro

S. T. Mantey, M. A. Fernandes, G. M. Fernandes, N. A. Silva, F. P. Guiomar, P. Monteiro, A. N. Pinto, and N. J. Muga, On the Coexistence of Quantum and Classical Signal Transmission Over Turbulent FSO Channels, tb submitted to JLT, 2024.

Quantum cryptography: The beautiful idea

- **The world is connected by fiber systems:**



Why use continuous-variables for QKD?

The information is encoded on the quadratures of coherent states.

Discrete Variables QKD

Can achieve higher transmission distances.

Continuous Variables QKD

Higher secret key rates for metropolitan distances.

Off-the-shelf equipment

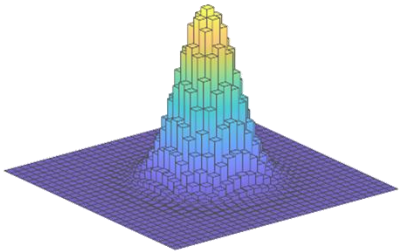
- Current optical fiber communication networks
- Commercial lasers
- Coherent detection

Coherent states modulation

Gaussian modulation → **Low-order discrete modulation** → **Higher-order discrete modulation**

Optimum performance

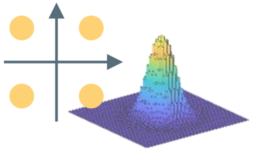
Difficult to achieve in practice

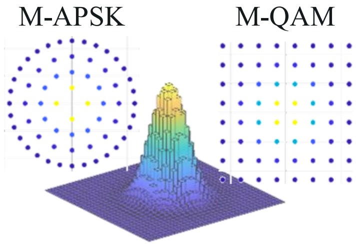


Simpler Implementation

Very-low amplitudes must be used to resemble Gaussian modulation

Far from the optimum performance of Gaussian modulation





Low amplitudes must be used to resemble Gaussian modulation.

Can approximate the performance of Gaussian modulation

M-QAM can achieve better performances than M-APSK

M. Almeida, D. Pereira, M. Facão, A. N. Pinto, and **N. A. Silva**, “Reconciliation Efficiency Impact on Discrete Modulated CV-QKD Systems Key Rates,” Journal of Lightwave Technology, vol. -, no. -, p. 1-9, 2023.

M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, and **N. A. Silva**, “CV-QKD Security Limits Using Higher-Order Probabilistic Shaped Regular M-APSK Constellations,” BRC Workshop de Comunicação e Computação Quântica WQuantum, Fortaleza, Brazil, May 2022 [Best paper award].

M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, and **N. A. Silva**, “Secret key rate of multi-ring M-APSK continuous variable quantum key distribution,” Optics Express, vol. 29, no. 23, p. 38669, Nov. 2021.

D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and **N. A. Silva**, “Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres,” Optics Letters, vol. 47, no. 15, p. 3948, July 2022.

A CV-QKD protocol: GG02

The most widespread protocol for CV-QKD is known as GG02 and was proposed in 2002 by Frédéric Grosshans and Philippe Grangier

- **Alice draws N 2-dimensional samples from a random distribution and uses them to modulate a coherent source obtaining the N coherent states, that are sent through an insecure quantum channel of transmittance T and excess noise ε.**
- **Bob performs the measurement of the received states, after which Alice and Bob share N pairs of correlated variables**
- **Alice and Bob reveal the part of the transmitted randomly chosen. With these parameters they will perform the parameter estimation. The security bounds can be calculated for estimated parameters to obtain the length of the final key.**

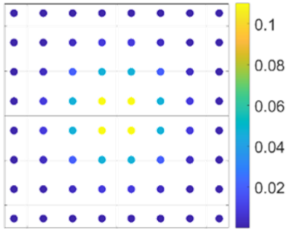
A CV-QKD protocol: GG02

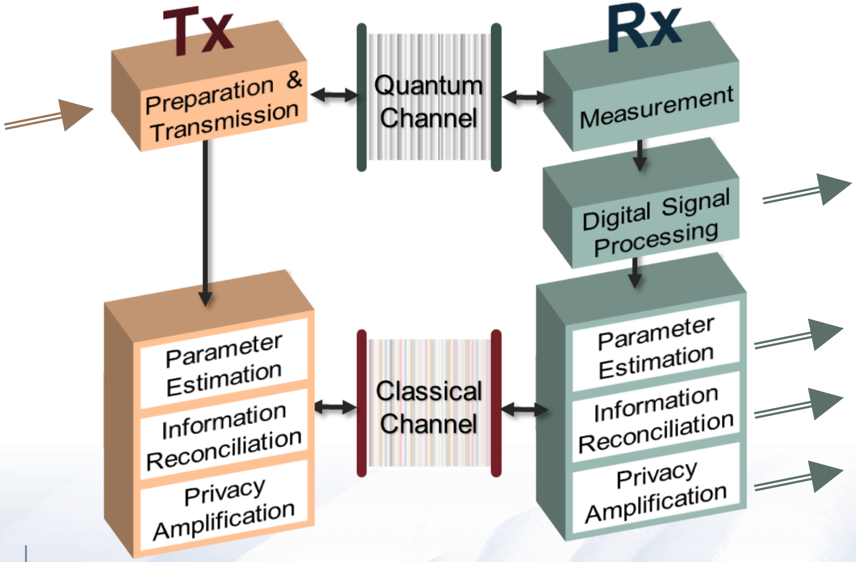
The most widespread protocol for CV-QKD is known as GG02 and was proposed in 2002 by Frédéric Grosshans and Philippe Grangier

- **Alice and Bob need to correct the errors on the $n = N - m$ remaining values they share. In practice they use the shared values to establish a common bit string U with the help of classical error correcting codes**
- **After reconciliation Alice and Bob share two identical strings U that are not completely secret. With U and the length of the key it is possible to implement a process of privacy amplification using 2-universal hashing. This process is common to all QKD protocols and when applied in both entities, Alice and Bob obtain two identical copies of the secret key.**

CV-QKD System Description

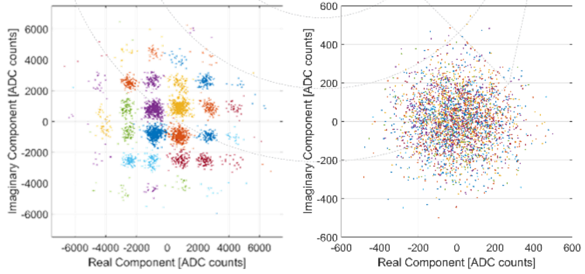
CV-QKD systems can be divided into a **physical layer** (preparation, transmission, measurement and digital signal processing) **and a post-processing layer** (parameter estimation, information reconciliation and privacy amplification).





Unsecure low attenuation

High attenuation with modulation variance of 1.0059 SNU.

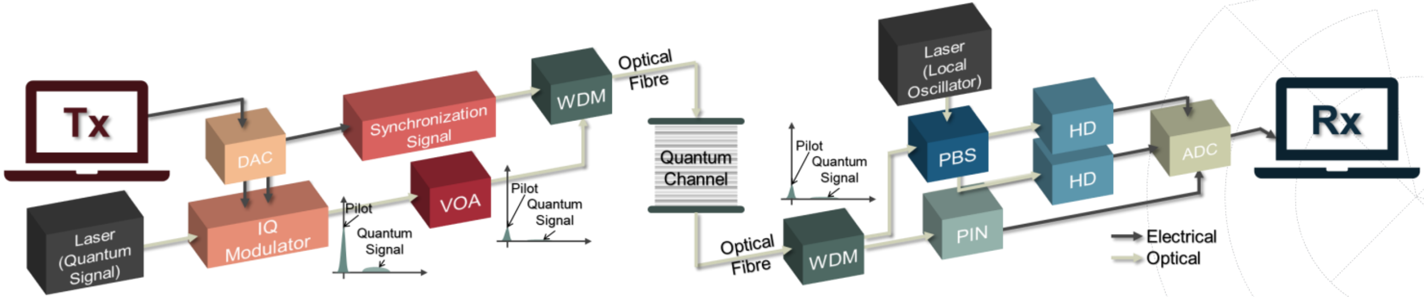


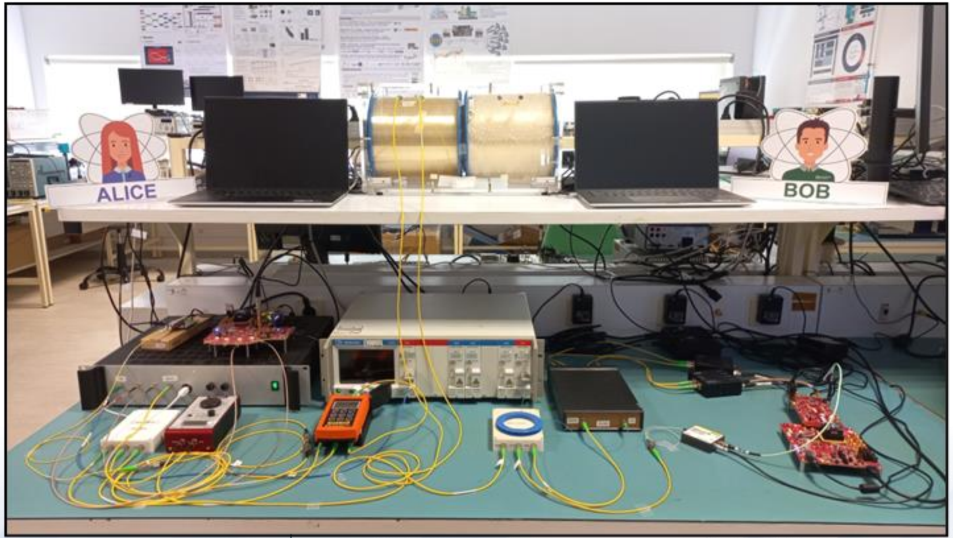
Secret key rate computation

Symmetric key extraction

Reduce eavesdropper knowledge

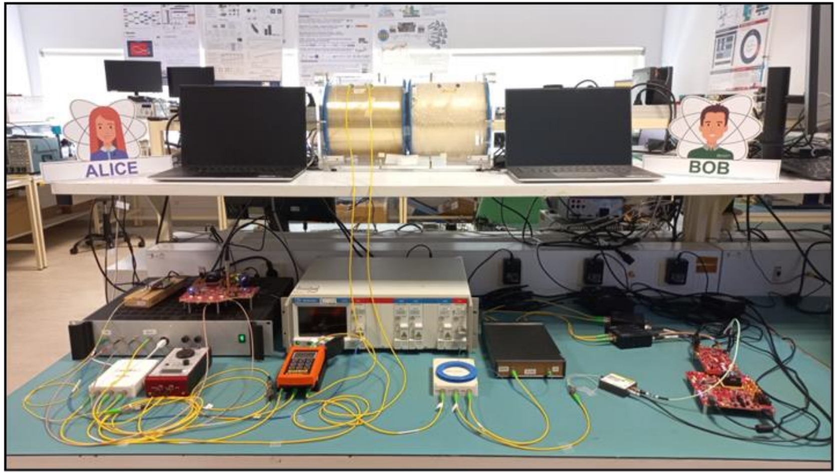
CV-QKD System Implementation





- Pilot signal at 0 Hz for frequency recovery and phase compensation
- Locally generated local oscillator
- Polarization diversity detection system
- True heterodyne detection

CV-QKD System Implementation

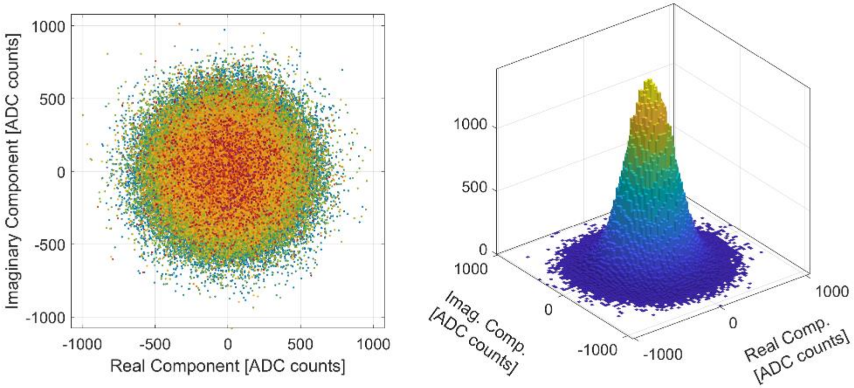


Input: 64-QAM probabilistic shaped

$$|\alpha_{k,l}| = (k + il)\sqrt{(V_A)/\left(2\sum_{k,l}P_{k,l}\sqrt{k^2 + l^2}\right)}$$

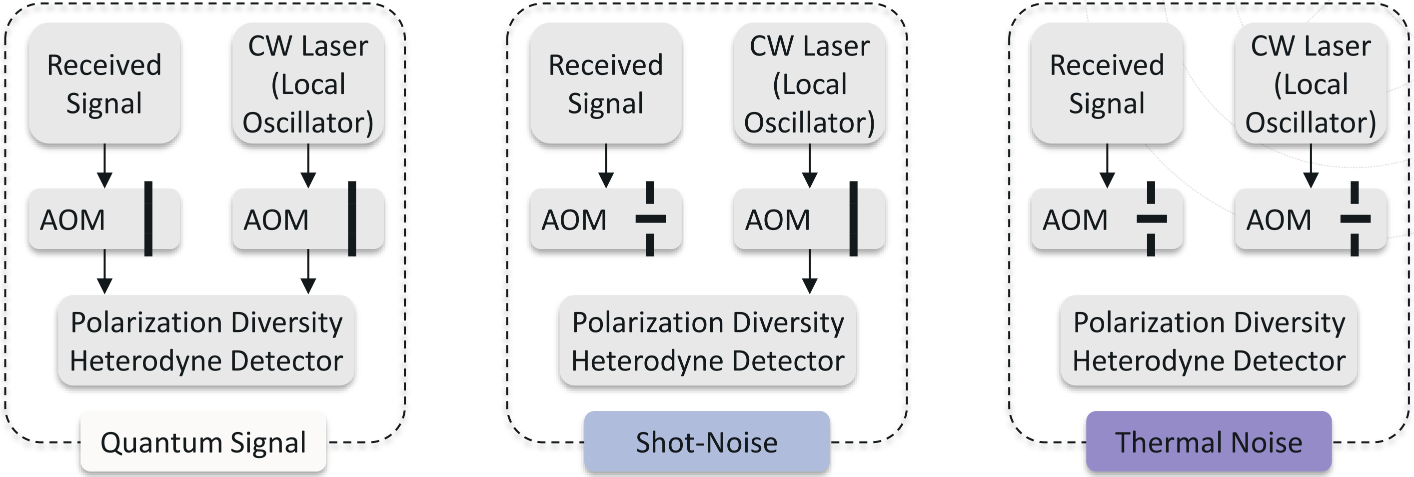
$$P_{k,l} = \exp\left(-\nu\left(k^2 + l^2\right)\right)/\sum_{k,l}P_{k,l}$$

- Quantum Signal at ADC+DSP output



CV-QKD System Implementation

The characterization of the receiver's noise is essential to assess the security of the CV-QKD system.

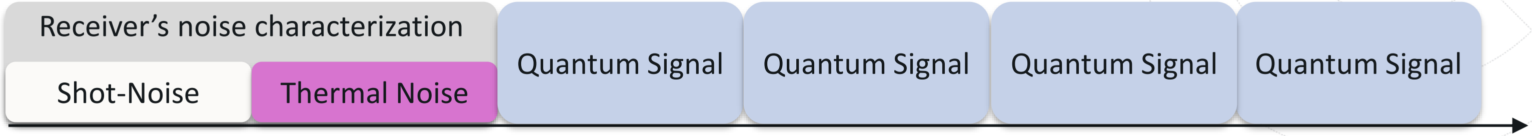


instituto de telecomunicações

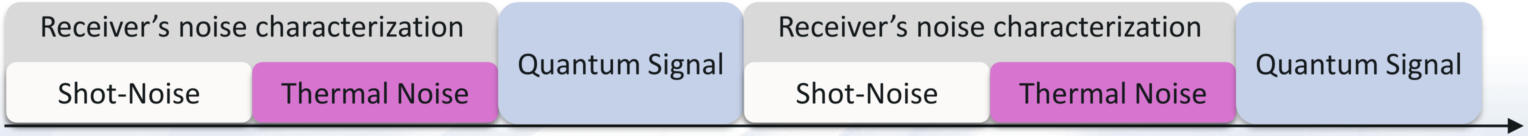
universidade de aveiro

CV-QKD System Implementation

Typically, the receiver's noise characterization is provided at the beginning of an experiment where several datasets of quantum signal are obtained considering the same receiver's noise characterization.

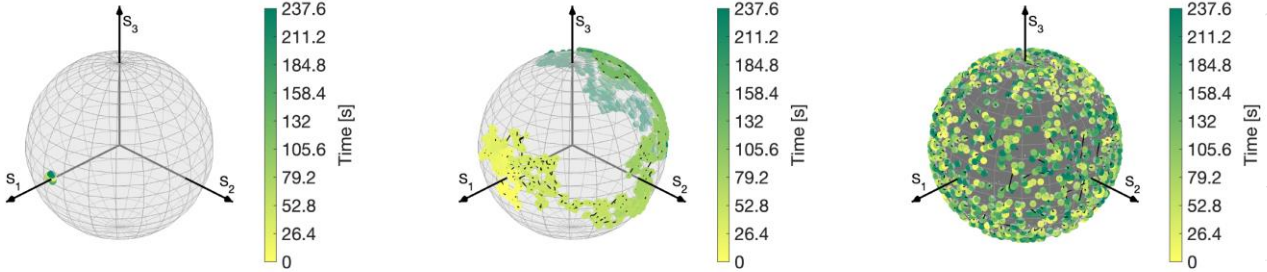


In a continuous operating system, the receiver's noise characterization should be provided from time to time. Ideally, the receiver's noise is characterized for each measured quantum signal dataset.



CV-QKD System Implementation

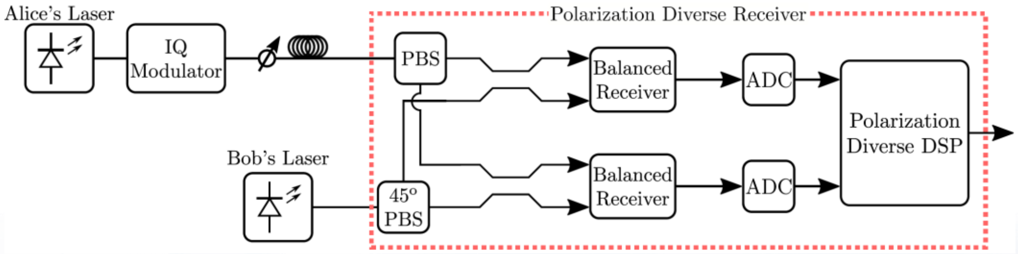
Polarization drift over optical fibers



Solution:

Polarization diversity heterodyne detection

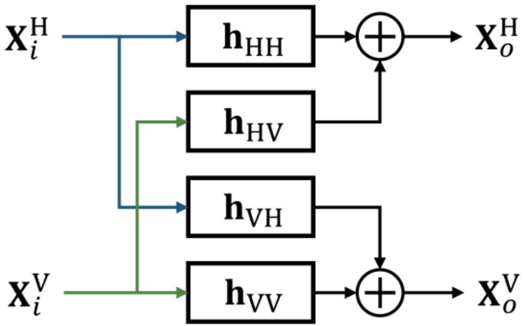
⇒ Passive equipment



Solution:

Constant modulus algorithm (CMA) equalization

$\Rightarrow$ Digital implementation



$$\mathbf{X}_i^{\mathrm{H}}(n) = \left[\hat{X}_{\mathrm{P,B_H}}(n), \hat{X}_{\mathrm{P,B_H}}(n-1), \cdots, \hat{X}_{\mathrm{P,B_H}}(n-N)\right],$$

$$\mathbf{X}_i^{\mathrm{V}}(n) = \left[\hat{X}_{\mathrm{P,B_V}}(n), \hat{X}_{\mathrm{P,B_V}}(n-1), \cdots, \hat{X}_{\mathrm{P,B_V}}(n-N)\right].$$

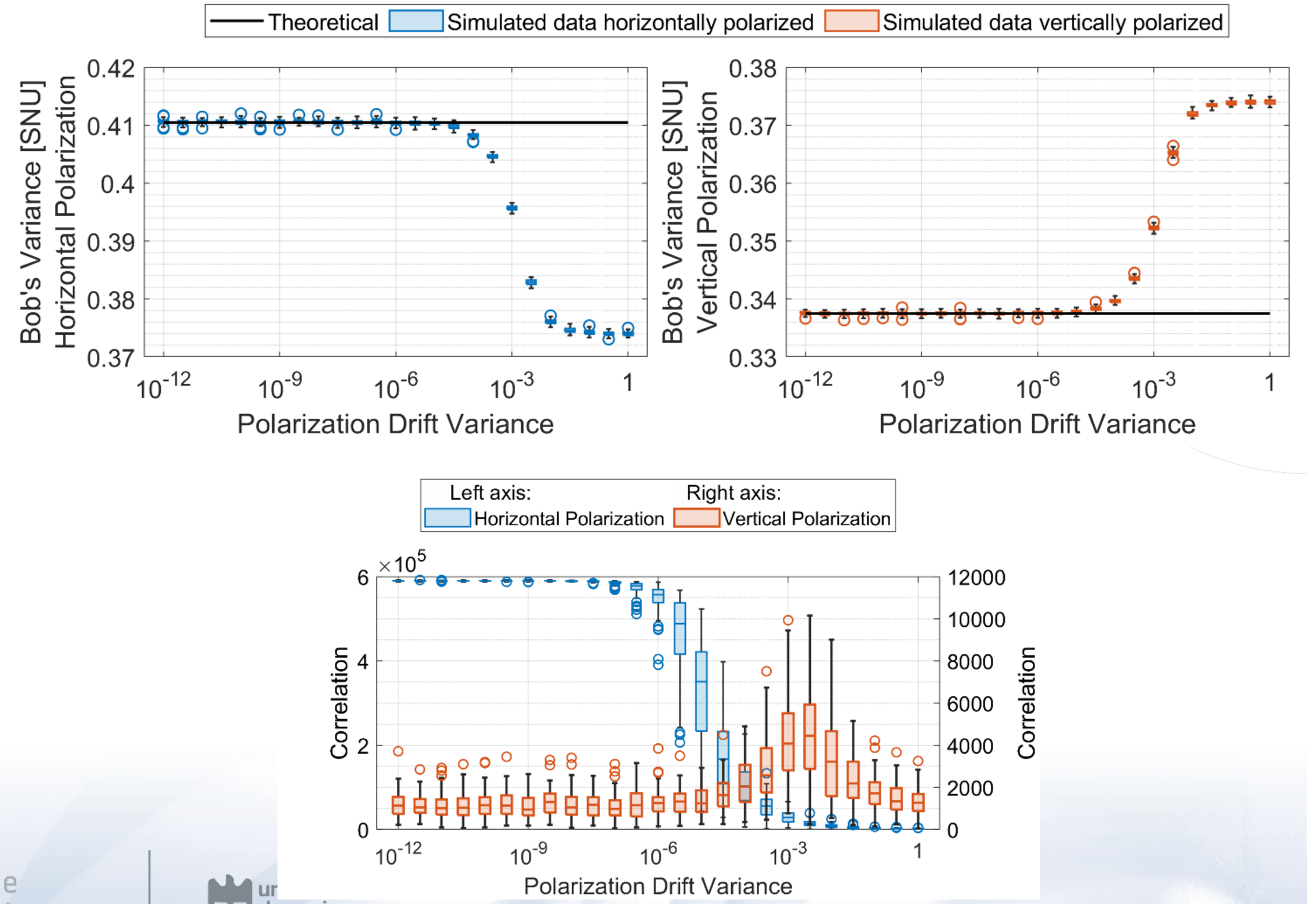
$$\mathbf{X}_o^{\mathrm{H}}(n) = \left(\mathbf{h}_{\mathrm{H}}(n)\right)^H \mathbf{u}_i(n),$$

$$\mathbf{X}_o^{\mathrm{V}}(n) = \left(\mathbf{h}_{\mathrm{V}}(n)\right)^H \mathbf{u}_i(n),$$

where

- $\mathbf{u}_i(n) = \left[\mathbf{X}_i^{\mathrm{H}}(n); \mathbf{X}_i^{\mathrm{V}}(n)\right]$,
- $\mathbf{h}_{\mathrm{H}}(n) = [\mathbf{h}_{\mathrm{HH}}(n); \mathbf{h}_{\mathrm{HV}}(n)]$,
- $\mathbf{h}_{\mathrm{V}}(n) = [\mathbf{h}_{\mathrm{VH}}(n); \mathbf{h}_{\mathrm{VV}}(n)]$.

CV-QKD System Implementation



instituto de telecomunicações

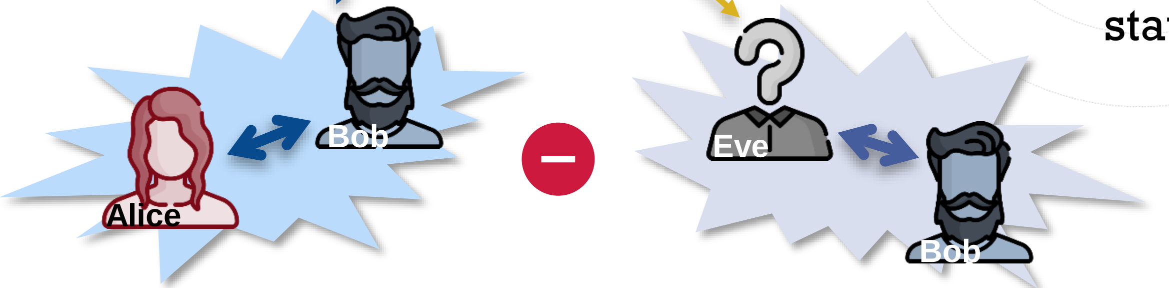
de aveiro

Extraction Key Rate

$$K \propto (1 - \mathrm{FER})\left(\beta I_{\mathrm{BA}} - \chi_{\mathrm{BE}} - \Delta(N^{\mathrm{IR}})\right)$$

Related with the exchange of a finite number of states.

Secret Key Rate =



Information amount **Alice** and **Bob** have in common

Information amount **Eve** and **Bob** have in common

Extraction Key Rate

$$K = \frac{n}{N}(1 - \mathrm{FER})\left[\beta I_{BA} - \chi_{BE} - \Delta(n)\right]$$

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{PA})$$

$$I_{\mathrm{BA}} = \log_2(1 + \mathrm{SNR}) = \log_2\left(1 + \frac{2T\eta\langle n\rangle}{T\eta\xi + 2 + 2\xi_{\mathrm{thermal}}}\right)$$

$$\chi_{\mathrm{BE}} = \sum_{i=1}^{2} G\left(\frac{\mu_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\mu_i - 1}{2}\right)$$

Covariance Matrix Alice-Bob

$$\gamma_{\mathrm{AB}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}Z\sigma_Z \\ \sqrt{T}Z\sigma_Z & (TV + 1 - T + T\epsilon)\mathbb{I}_2 \end{bmatrix}$$

$$Z = 2\sqrt{T_{\mathrm{ch}}}\mathrm{Tr}\left(\tau^{1/2}\hat{a}\tau^{1/2}\hat{a}^\dagger\right) - \sqrt{2T_{\mathrm{ch}}\xi W},$$

With:

$$W = \sum_{k,l} P_{k,l}\left(\langle\alpha_{k,l}|\hat{a}_\tau^\dagger\hat{a}_\tau|\alpha_{k,l}\rangle - |\langle\alpha_{k,l}|\hat{a}_\tau|\alpha_{k,l}\rangle|^2\right)$$

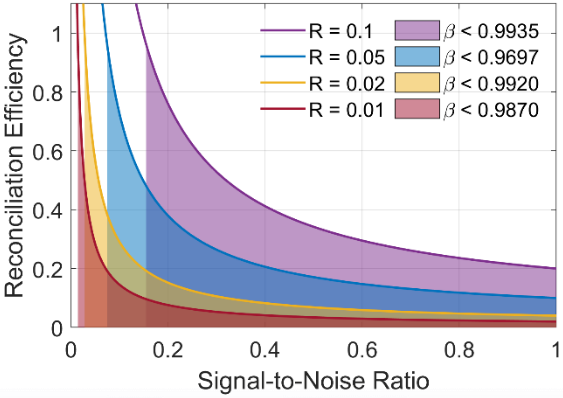
And, the density matrix describing the average state sent by Alice

$$\tau = \sum_{k,l} P_{k,l}|\alpha_{k,l}\rangle\langle\alpha_{k,l}|$$

Reconciliation Efficiency

Assures that the number of bits extracted is not higher than the value allowed by information reconciliation.

$$\beta = \frac{R}{C}$$



LDPC matrix code rate

$$R = \frac{\#\text{VNs} - \#\text{CNs}}{\#\text{VNs}}$$

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

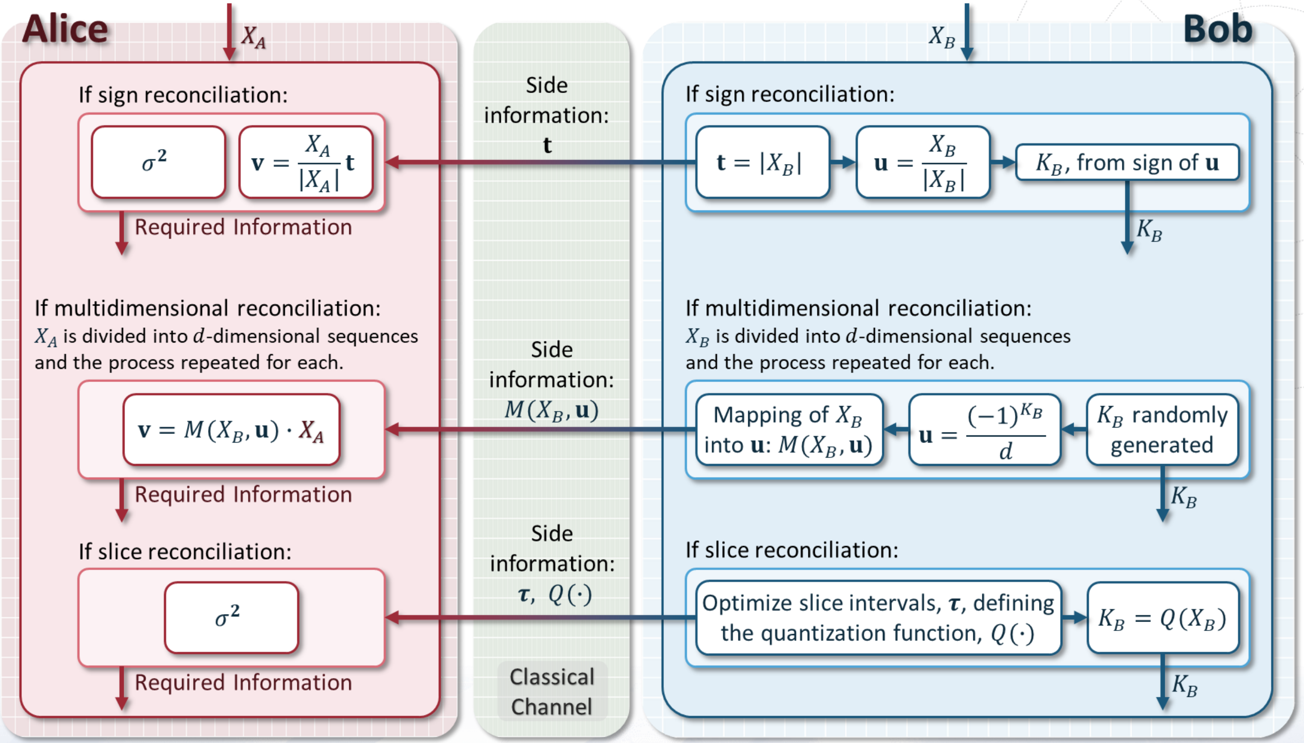
Check Nodes (CNs)

Variable Nodes (VNs)

Channel's capacity

$$C \approx 2\, I_{\mathrm{BA}} \approx 2 \log_2 (1 + \mathrm{SNR})$$

Information Reconciliation



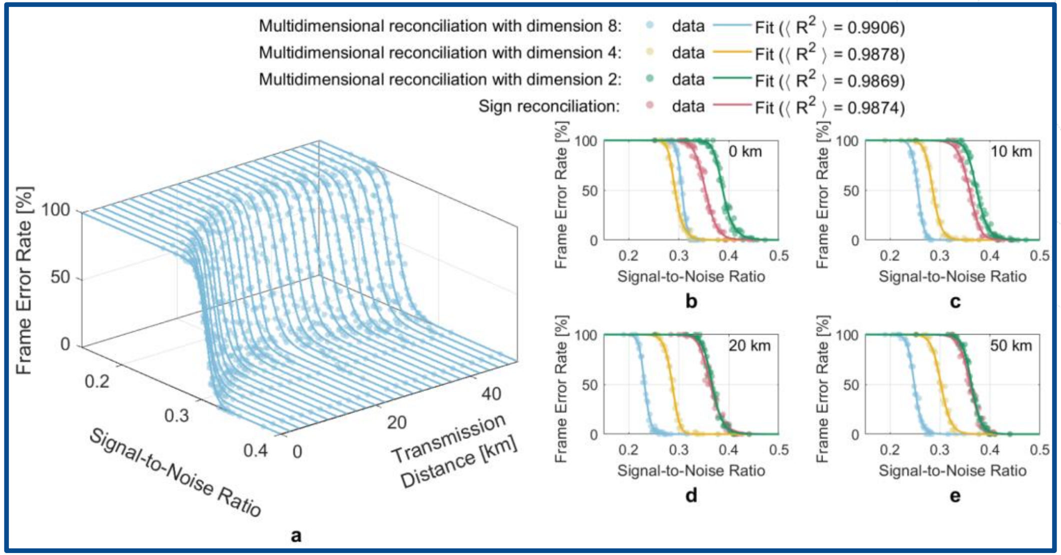
instituto de telecomunicações

universidade de aveiro

Frame Error Rate

$$K \propto (1 - \mathrm{FER})\,(\beta I_{\mathrm{BA}} - \chi_{\mathrm{BE}} - \Delta(N^{\mathrm{IR}}))$$

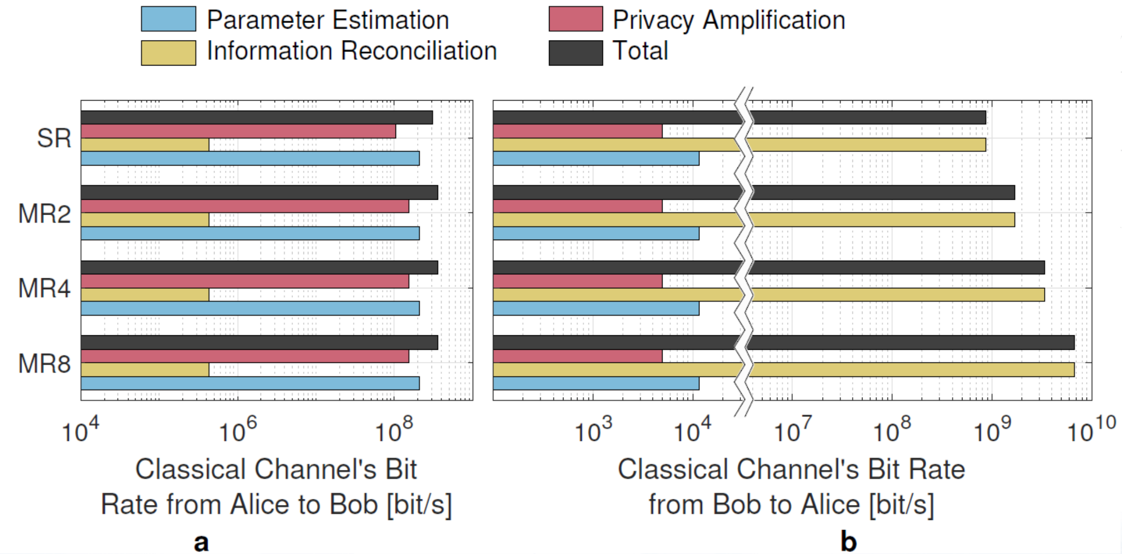
➢ Considering multidimensional and sign reconciliation:



- Multidimensional reconciliation of dimension 8 can extract keys for low SNR values.
- For short transmission distances, multidimensional reconciliation with dimension 4 shows higher performance.

Information Exchanged Alice - Bob

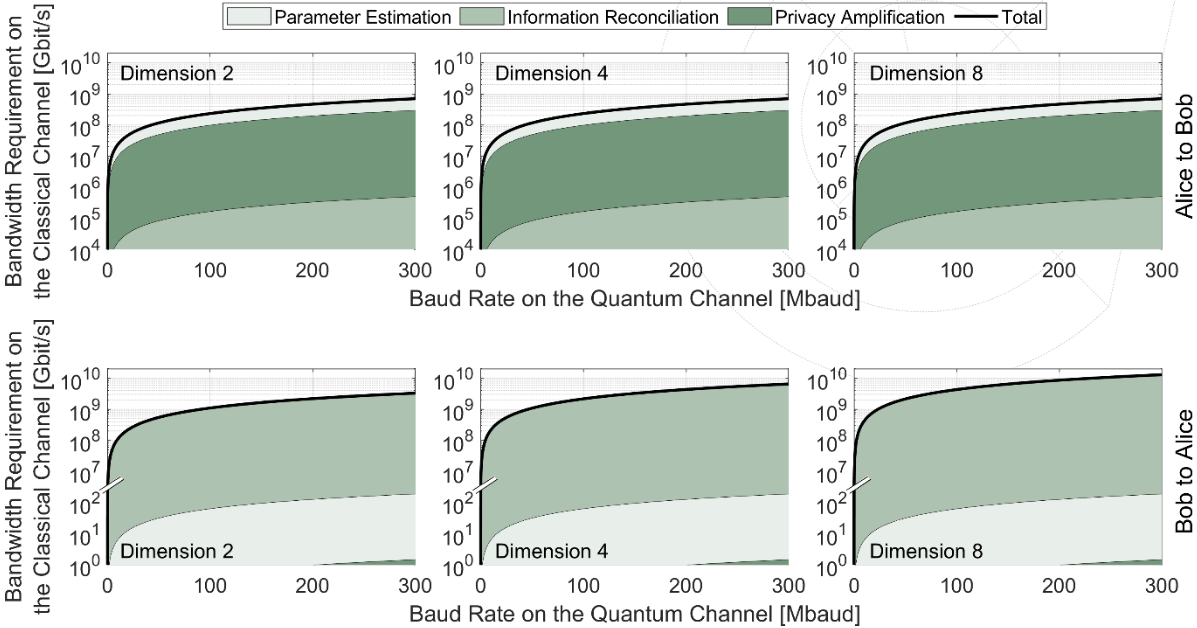
Amount of information exchanged from Alice to Bob and from Bob to Alice for each post processing step



The amount of information transmitted in the classical channel from Alice to Bob has a higher contribution of the parameter estimation step.

Bandwidth Requirements on the Classical Channel

- In the link direction from Alice to Bob, no difference is found in the classical channel's bandwidth regarding the dimension of multidimensional reconciliation
- In the link direction from Bob to Alice, the step demanding the highest amount of information to be exchanged in the classical channel is the information reconciliation step, with the parameter estimation and the privacy amplification step requiring several orders of magnitude less information



➢ The information reconciliation step is mostly due to the exchange of the side information, of namely the rotation matrices for multidimensional reconciliation, corresponding to 97.26%, 98.61%, and 99.30% of the bandwidth demand for multidimensional reconciliation of dimension 2, 4, and 8, respectively.

QSCRIPT

PAVING THE WAY WITH PORTUGUESE TECHNOLOGY

deimos · it · TÉCNICO LISBOA · altice labs · GNS Gabinete Nacional de Segurança · EMGFA

Two sites of MoD, 4.5km apart, were connected using a CV-QKD link

Hardware security modules were used to encrypt the communication

Fully Portuguese-developed technology

Instituições Associadas

TÉCNICO LISBOA

universidade de aveiro

UNIVERSIDADE D COIMBRA

altice labs

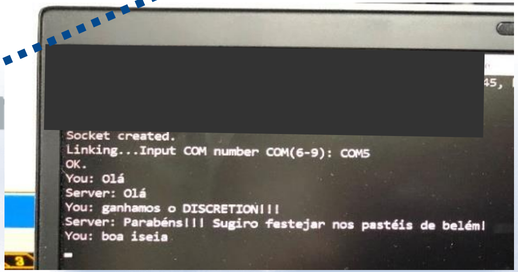
NOKIA

UNIVERSIDADE BEIRA INTERIOR

U.PORTO

ISCTE IUL Instituto Universitário de Lisboa

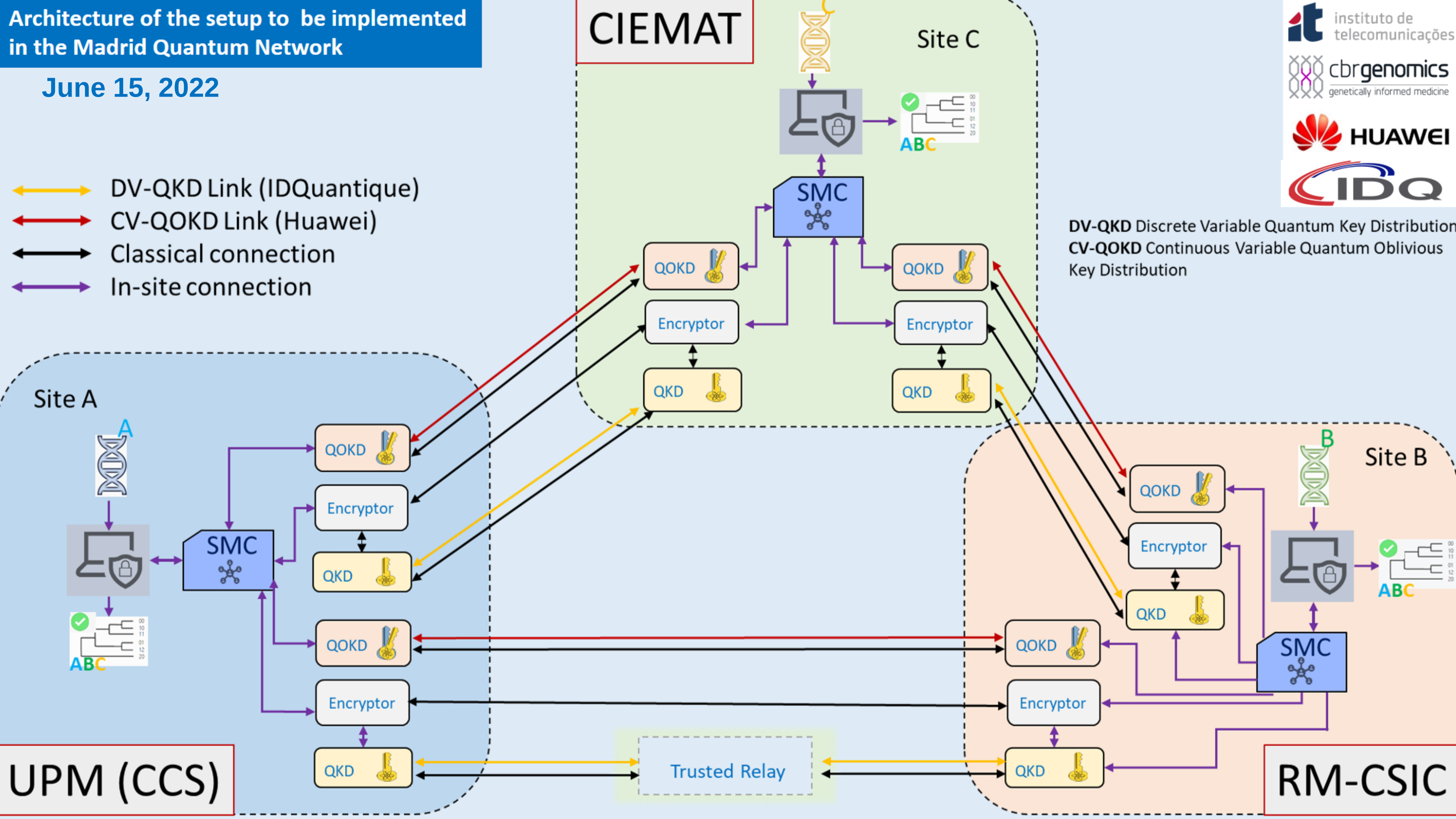
IPL Instituto politécnico de leiria



June 30, 2021

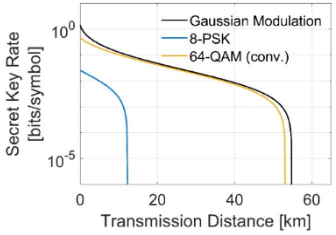
Architecture of the setup to be implemented in the Madrid Quantum Network

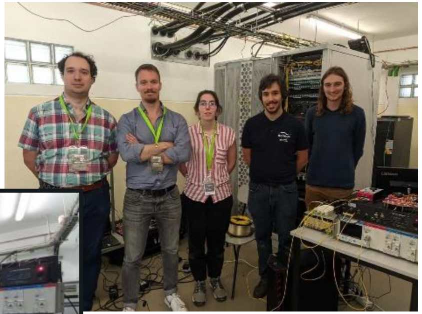
June 15, 2022

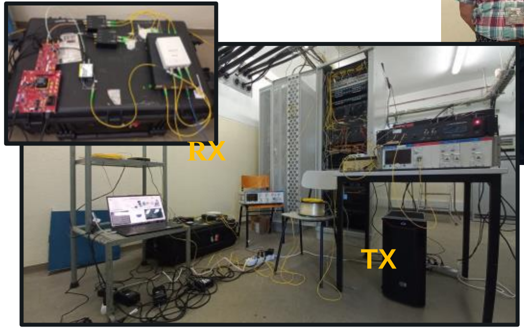


DV-QKD Discrete Variable Quantum Key Distribution
CV-QOKD Continuous Variable Quantum Oblivious Key Distribution

QSCRIPT2 - Field Experimentation of the CV-QKD system with 64-QAM as part of the Portuguese Army Exercise ARTEX (ARmy Technological EXperimentation), in the Campo Militar de Santa Margarida



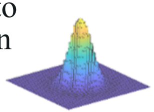




Instituições Associadas

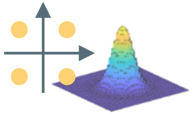
Gaussian modulation

Difficult to achieve in practice



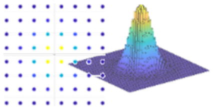
Discrete modulation

Simpler implementation



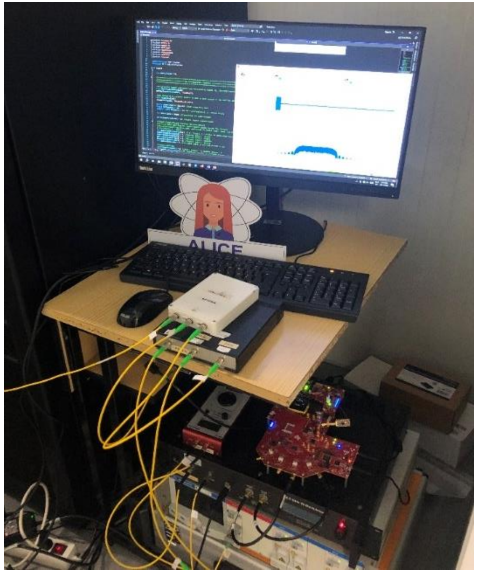
High-order cardinality

Best performance



June 1, 2023

Field Demonstration of a cutting-edge quantum-link CV-QKD system at REPMUS & NATO Dynamic Messenger 2023 (DYMS23) Exercises in the Portuguese Navy



Exchange of confidential information between a command center and a docked navy frigate.

Operational Experimentation Center in Troia, Portugal

September 21, 2023

Quantum Communications Group

Instituições Associadas

TÉCNICO LISBOA

universidade de aveiro

UNIVERSIDADE D COIMBRA

altice labs

NOKIA

UNIVERSIDADE BEIRA INTERIOR

U.PORTO

ISCTE IUL Instituto Universitário de Lisboa

IPL Instituto politécnico de leiria

Group Coordinator:

Armando Nolasco Pinto

anp@ua.pt

Group Websites:

Web: https://www.it.pt/Groups/Index/72
LinkedIn:https://www.linkedin.com/company/quantum-communications-group-it-av/
Intagram:https://www.instagram.com/quantumcommunicationsgroup/

instituto de telecomunicações

Thank you for Your Attention

Questions?

nasilva@ua.pt

Acknowledgements

PTQCI (GA 101091730)

Fundação para a Ciência e a Tecnologia (FCT):

- ✓ Project QuantumPrime: PTDC/EEI-TEL/8017/2020
- ✓ Project UIDB/50008/2020-UIDP/50008/2020

Cofinanciado por:

COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

FCT Fundação para a Ciência e a Tecnologia MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

instituto de telecomunicações

universidade de aveiro