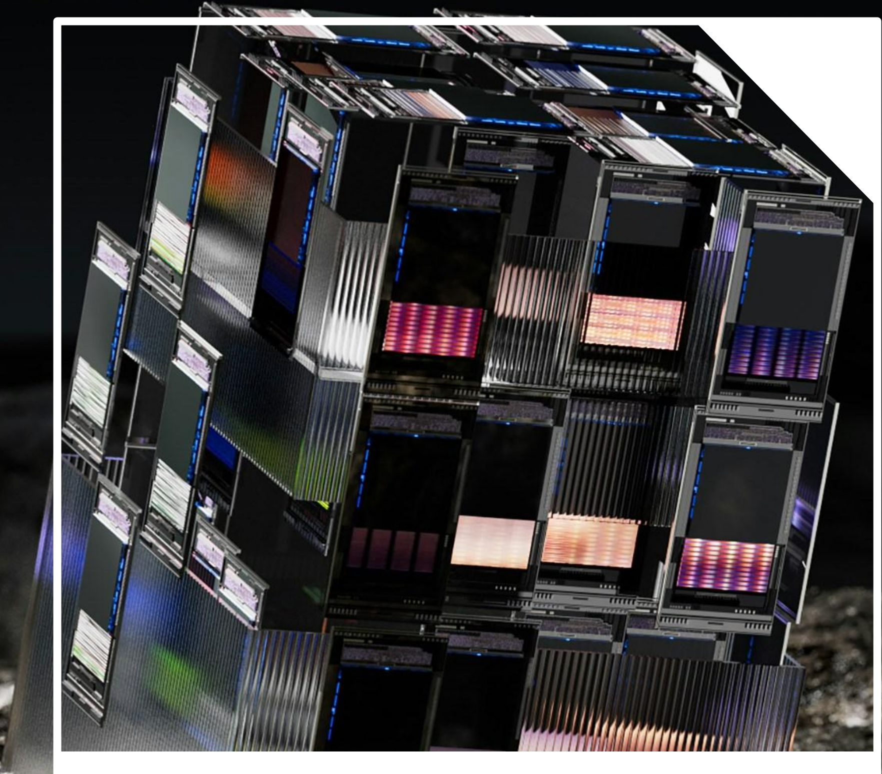
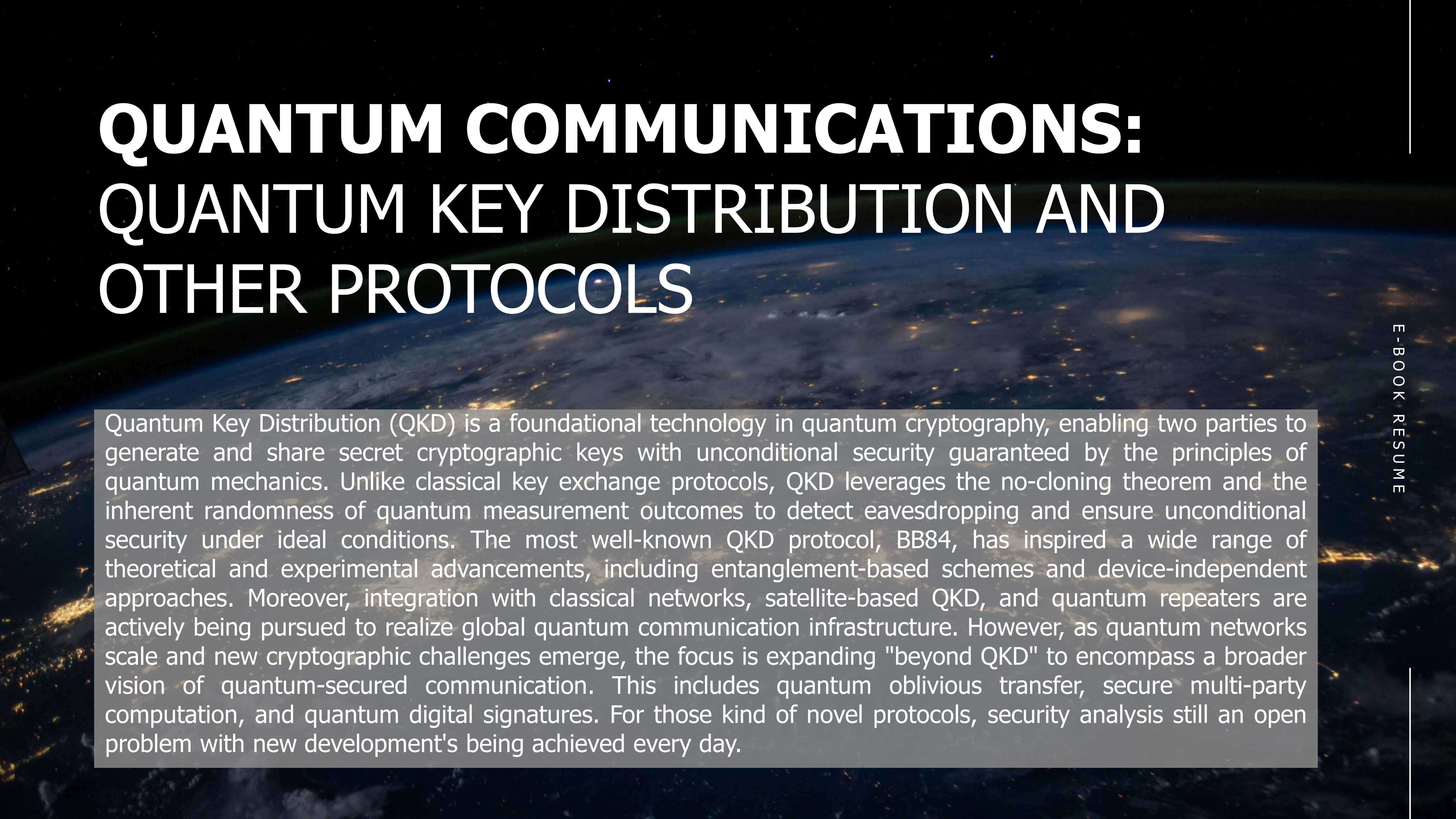


QUANTUM COMMUNICATIONS

PORTUGUESE QUANTUM
COMMUNICATION
INFRASTRUCTURE

ABSTRACT



QUANTUM COMMUNICATIONS: QUANTUM KEY DISTRIBUTION AND OTHER PROTOCOLS

E-BOOK RESUME

Quantum Key Distribution (QKD) is a foundational technology in quantum cryptography, enabling two parties to generate and share secret cryptographic keys with unconditional security guaranteed by the principles of quantum mechanics. Unlike classical key exchange protocols, QKD leverages the no-cloning theorem and the inherent randomness of quantum measurement outcomes to detect eavesdropping and ensure unconditional security under ideal conditions. The most well-known QKD protocol, BB84, has inspired a wide range of theoretical and experimental advancements, including entanglement-based schemes and device-independent approaches. Moreover, integration with classical networks, satellite-based QKD, and quantum repeaters are actively being pursued to realize global quantum communication infrastructure. However, as quantum networks scale and new cryptographic challenges emerge, the focus is expanding "beyond QKD" to encompass a broader vision of quantum-secured communication. This includes quantum oblivious transfer, secure multi-party computation, and quantum digital signatures. For those kind of novel protocols, security analysis still an open problem with new development's being achieved every day.

RICARDO **FALEIRO**

Postdoc researcher at Instituto de Telecomunicações (IT), broadly interested in quantum information and quantum foundations.

His research focuses on the non-classicality of quantum correlations (Bell nonlocality, contextuality) and their applications in quantum information, particularly in quantum cryptography.

2022 - PhD in Physics, Instituto Superior Técnico de Lisboa

2016 - Master in Physics, Universidade de Coimbra

ABSTRACT

ABSTRACT

A CRASH COURSE ON QUANTUM INFORMATION AND QUANTUM CRYPTOGRAPHY

In this talk, I introduce Quantum Information without assuming any background in either Quantum Mechanics or Information Theory.

I begin by providing a historical perspective on the birth of the field, starting with Wiesner’s seminal Conjugate Coding paper. From there, I highlight key stylistic and philosophical differences between Quantum Information and Quantum Mechanics to motivate an operational perspective for the former.

Rooted in this operational approach, where processes idealized as black boxes define the theory, I introduce three fundamental such processes: preparations, transformations, and measurements. I characterize the input-output behavior of each type of box and then describe how these can be connected or "wired" together.

To illustrate these concepts, I present paradigmatic scenarios arising from specific wirings of these black-box processes. Notable among these are the Prepare-Transform-Measure (PTM) scenario, which consists of a single preparation, transformation, and measurement connected sequentially, and bi-partite Bell-type scenarios, which involve a preparation followed by two measurements in parallel. I focus more concretely on the PTM scenario and demonstrate that, since transformations in PTM can always be absorbed into either preparations or measurements, we can, without loss of generality, reduce our consideration to the simpler Prepare-and-Measure (PM) scenario. This simplified scenario is particularly relevant for applications in Quantum Cryptography.

Finally, I revisit Wiesner’s original Conjugate Coding idea and reframe it within the PM scenario. I then analyze how Conjugate Coding fits into the broader landscape of Quantum Information Theory and its relationship with modern cryptographic primitives. In particular, I highlight its conceptual connection to 1-out-of-2 Oblivious Transfer (OT)—a fundamental cryptographic primitive in which a sender transmits two pieces of information to a receiver, who can choose to access only one while ensuring that the sender remains oblivious to their choice. I show that Wiesner’s Conjugate Coding can, in fact, be framed as a primitive of this nature under very strict assumptions. These include a globally fixed and separable measurement on the receiver’s side, which, although unrealistic by today’s standards, provides valuable historical and theoretical insight into the evolution of quantum cryptographic protocols.

A crash course on Quantum Information and Quantum Cryptography

Ricardo Faleiro, IT-Aveiro

13/11/24

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101091730.

Co-funded by the European Union

A crash course on Quantum Information and some examples for Quantum Cryptography

Ricardo Faleiro, IT-Aveiro

13/11/24

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101091730.

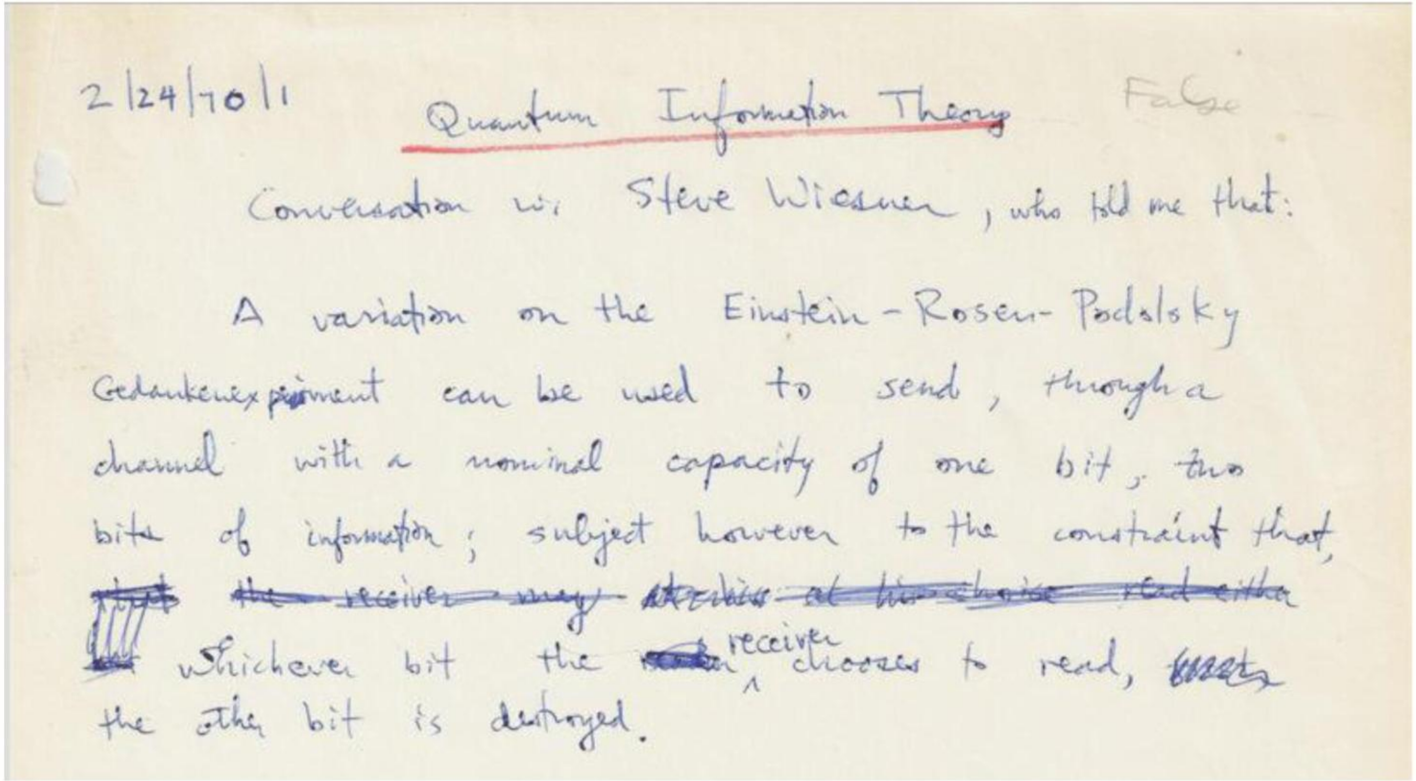
Co-funded by the European Union

A crash course on Quantum Information and some examples for Quantum Cryptography
... If there's time

Ricardo Faleiro, IT-Aveiro

13/11/24

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101091730.



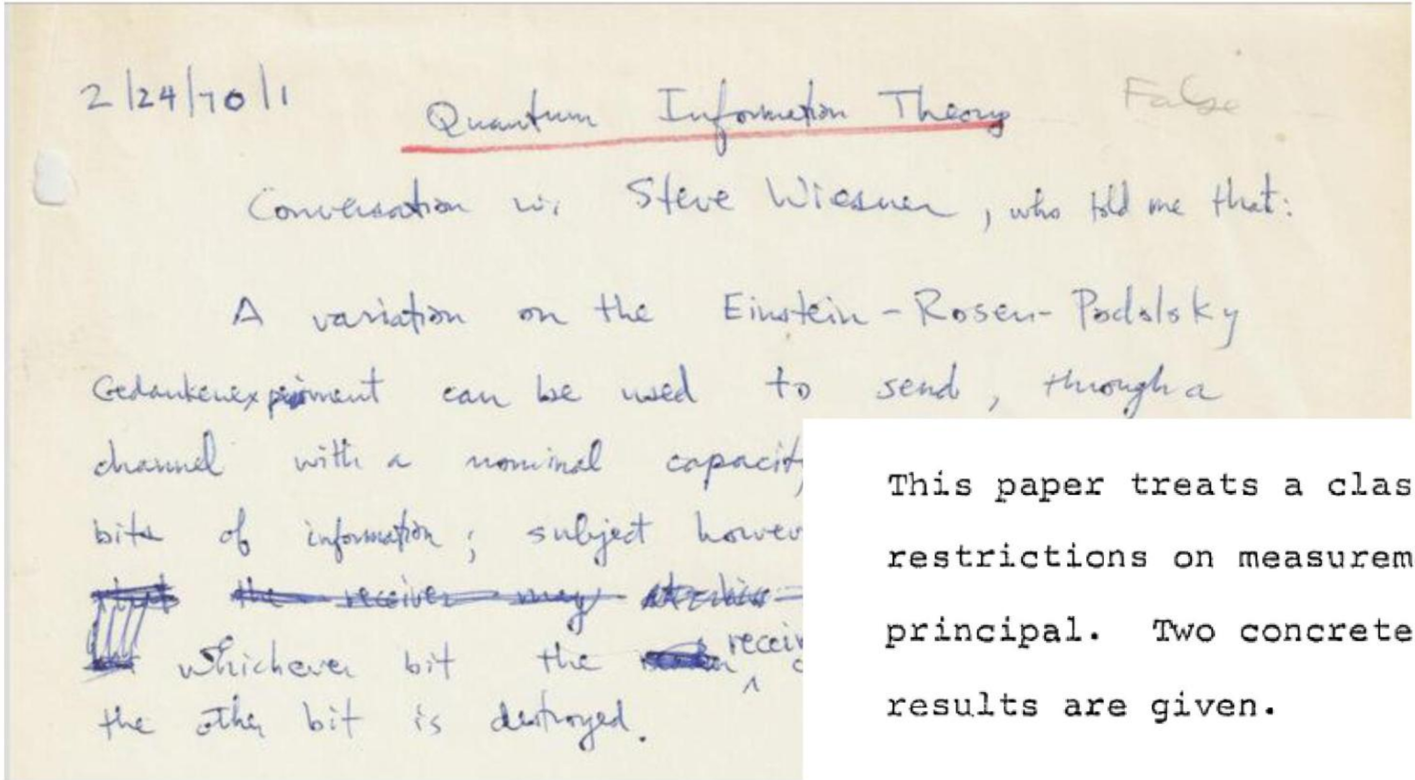
2/24/70 | 1

Quantum Information Theory

False

Conversation w/ Steve Wiesner, who told me that:

A variation on the Einstein-Rosen-Podolsky Gedankenexperiment can be used to send, through a channel with a nominal capacity of one bit, two bits of information; subject however to the constraint that, ~~that~~ ~~the receiver may~~ [illegible] ~~at his choice read either~~ [illegible] whichever bit the [illegible] receiver chooses to read, [illegible] the other bit is destroyed.



2/24/70/1 Quantum Information Theory False

Conversation w/ Steve Wiesner, who told me that:

A variation on the Einstein-Rosen-Podolsky Gedankenexperiment can be used to send, through a channel with a nominal capacit

bits of information; subject howev

~~the receiver may either~~

whichever bit the receiv

the other bit is destroyed.

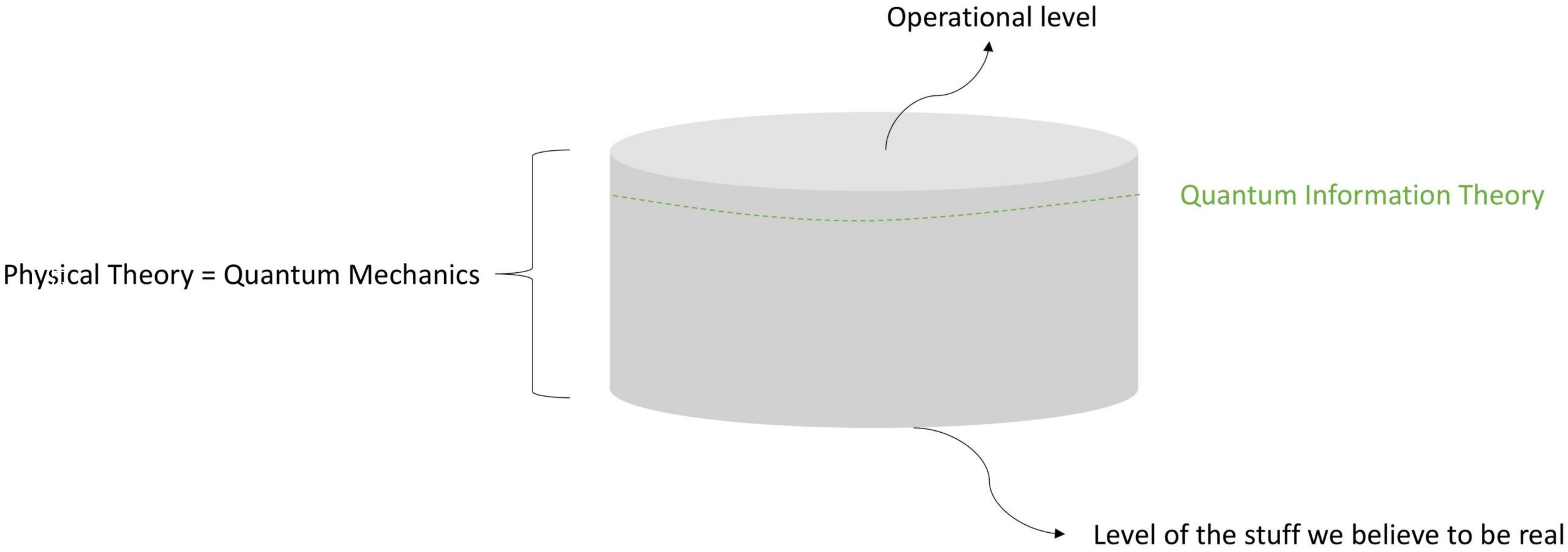
This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be “real”	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	State vectors or density matrices of finite dimensional registers of abstract systems, evolving discretely with unitary operators.
Philosophical stance	Physical theory; Abides implicitly to physicalism;	Informational theoretic framework; Instrumental;
Goals	Understanding and predicting physical phenomena (e.g., atomic structures, scattering processes, decays).	Manipulating and processing information, often for tasks like quantum computing, communication, and cryptography



Operational level

Quantum Information Theory

Physical Theory = Quantum Mechanics

Level of the stuff we believe to be real

"But if quantum mechanics isn't physics in the usual sense — if it's not about matter, or energy, or waves, or particles — then what is it about? From my perspective, it's about information and probabilities and observables, and how they relate to each other." – Scott Aaronson, Quantum Computing Since Democritus

So what is different? The theory is the same, but taken from a new perspective:

- **QM is a physical theory grounded in a notion of physicalism, that is, it focuses on "real" physical systems and their properties;**

- **QI is an epistemic framework concerned with studying the manipulation and processing of information emergent from the quantum mechanical phenomena**.

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

- We don’t really care about the inner workings of the processes/boxes in great detail;
- We have a good understanding of how the boxes behave, with respect their inputs/outputs, such that, we can model them within the formalism of quantum mechanics consistently with the observed behavior of the boxes;

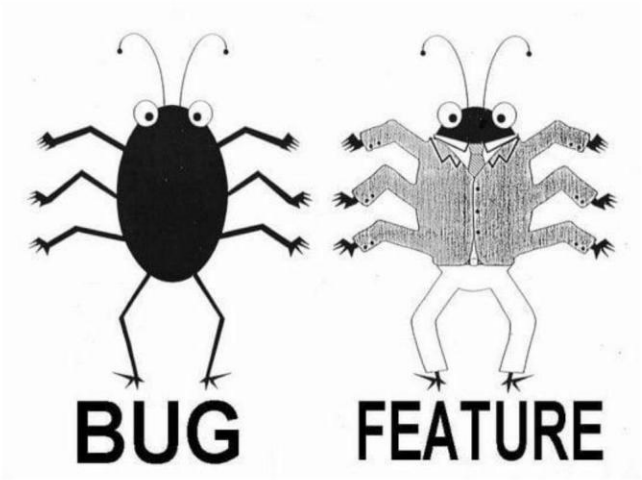
E.g. Typically, one tries to be as agnostic as possible about the contents of the boxes, but sometimes general assumptions can be established. For instance, we may consider preparations that only output states up to a certain dimension or energy.

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

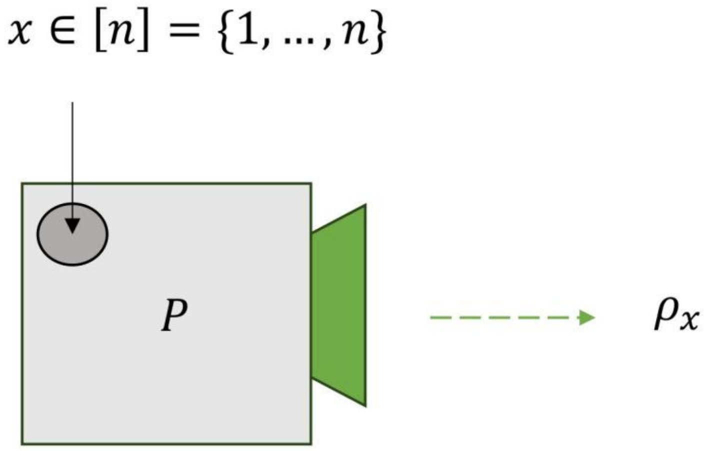
- We don’t really care about the inner workings of the processes/boxes in great detail;
- We have a good understanding of how the boxes behave, with respect their inputs/outputs, such that, we can model them within the formalism of quantum mechanics consistently with the observed behavior of the boxes;

Going from QM to QI some aspects of the phenomenology of quantum mechanics which were consider troubling can be promoted to resources for information processing:

- Coherence, superposition;
- Measurement incompatibility;
- Entanglement;
- Nonlocality



(Deterministic) Preparations



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\rho_x |\, x \in [n]\} \rangle$
    - $\boldsymbol{H}$ = Hilbert space

(For finite dimension, can be assumed to be a complex Euclidean space. A linear (vector) field with the Euclidean metric and usual inner product of vectors in $\mathbb{C}^n$, where the vectors, operators etc, can have over complex numbers as components.)

- $\{\rho_x |\, x \in [n]\} = \{\rho_1, \rho_2, \dots, \rho_n\}$

Each ρ_x is called a ***density operator***. They are, positive semi-definite, trace one, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

Hermiticity: $\rho_x = \rho_x^\dagger$

Positive Semi-Definiteness: For any vector $|\,\psi\rangle \in \boldsymbol{H}$, we have $\langle\psi \mid \rho \mid \psi\rangle \geq 0$. Equivalent to say that the spectrum, the set of eigenvalues, is non-negative.

Trace Condition: $Tr(\rho) = 1$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

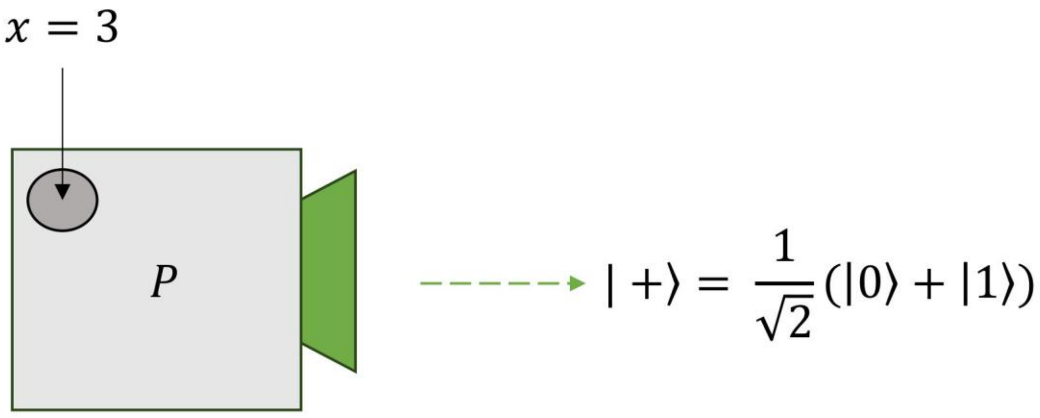
Second, define the density operators for the possible inputs:

- $\{\rho_1 = |0\rangle\langle 0|, \rho_2 = |1\rangle\langle 1|, \rho_3 = |+\rangle\langle +|, \rho_4 = |-\rangle\langle -|\}$

Where,
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

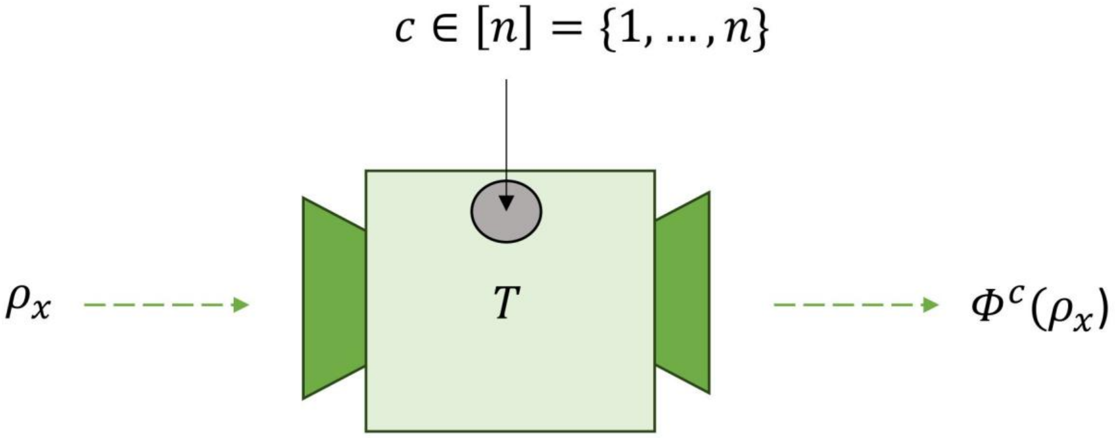
$$\{|0\rangle\langle 0| = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, |1\rangle\langle 1| = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix},$$
$$|+\rangle\langle +| = \begin{pmatrix}1/2 & 1/2\\1/2 & 1/2\end{pmatrix}, \ |-\rangle\langle -| = \begin{pmatrix}1/2 & -1/2\\-1/2 & 1/2\end{pmatrix}\},$$

Special case, where the density operators are outer products of a single vectors. These are called pure state.



$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

(Control-)Transformations



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\Phi^c\}_c \rangle$

A transformation is described by a Completely-Positive-Trace-Preserving (CPTP) Map

$$\forall_c\, \Phi^c : \boldsymbol{H} \rightarrow \boldsymbol{H}$$

In the Kraus representation $\forall_c\, \Phi^c \Leftrightarrow \{K_i\}^c$

- $\Phi^c(\rho_x) = \sum_i K_i^c \rho_x K_i^{c\,\dagger}$

Complete Positivity: A map Φ is completely positive if, for any state ρ, $\Phi(\rho)$ is positive semi-definite. This ensures that no negative probabilities arise.

Trace Preservation: $Tr\big(\Phi(\rho)\big) = Tr(\rho)$ for all ρ.

To guarantee this property, the Kraus operators must satisfy : $\sum_i K_i^\dagger K_i = I$, where I is the identity operator on the Hilbert space $\boldsymbol{H}$.

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{\Phi^c\}_{c\in\{1,2\}}: \mathbb{C}^2 \to \mathbb{C}^2 \Leftrightarrow$

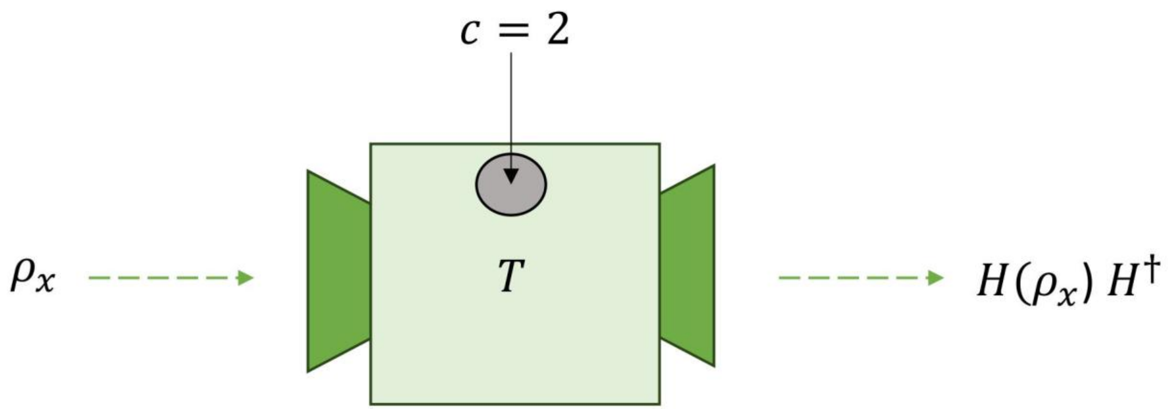
$$\Phi^1 = I = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \ \Phi^2 = H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

- $\Phi^1(\rho_x) = \rho_x$; $\Phi^2(\rho_x) = H\ \rho_x\ H^\dagger$

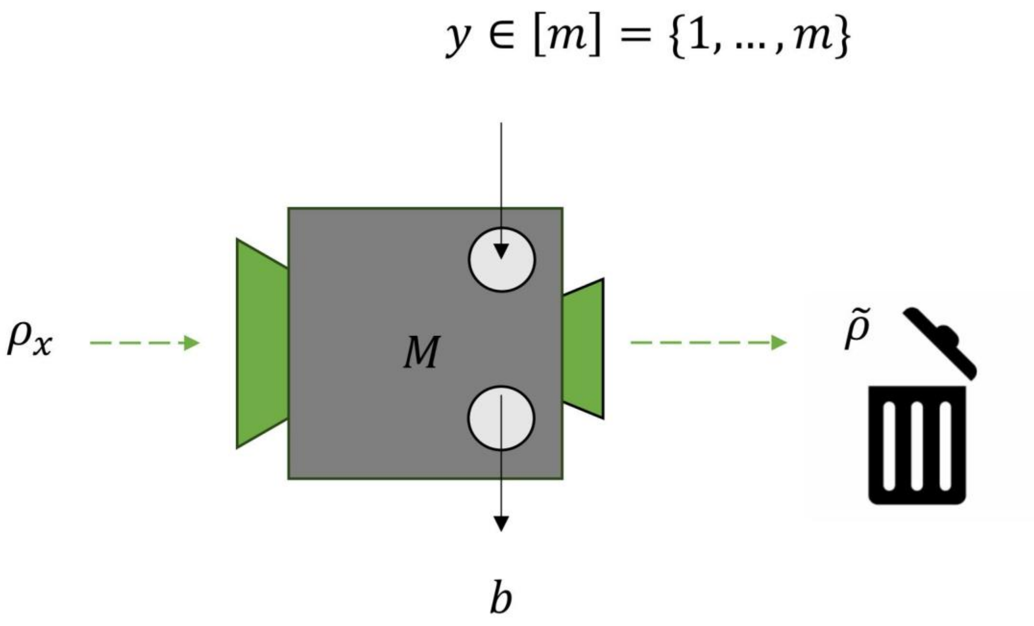
Special case, where transformations are given by unitaries U,i.e there is only one Kraus operator, the unitary itself, $U^\dagger\ U = I$

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$



Measurements (non-destructive)



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

Hermiticity: $E_{b|y} = {E_{b|y}}^{\dagger}$

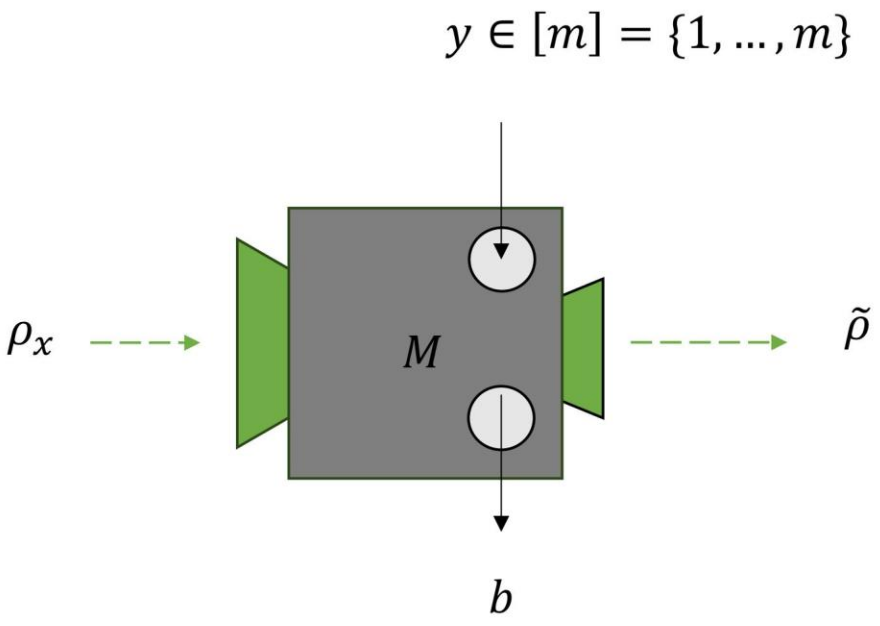
Positive Semi-Definiteness: For any vector $|\,\psi\rangle \in \boldsymbol{H}$, we have $\langle\psi \mid E_{b|y} \mid \psi\rangle \geq 0$. Equivalent to say that the spectrum, the set of eigenvalues, is non-negative.

Sum to identity: For all y, $\sum_b E_{b|y} = I_H$,

- Probability of outcome b for POVM defined by y, and state prepared by x is given by the Born rule as follows,

$$\boxed{p(b|y,x) = Tr(\rho_x\, E_{b|y})}$$

Measurements (non-destructive)



In the lab it might look more like this…

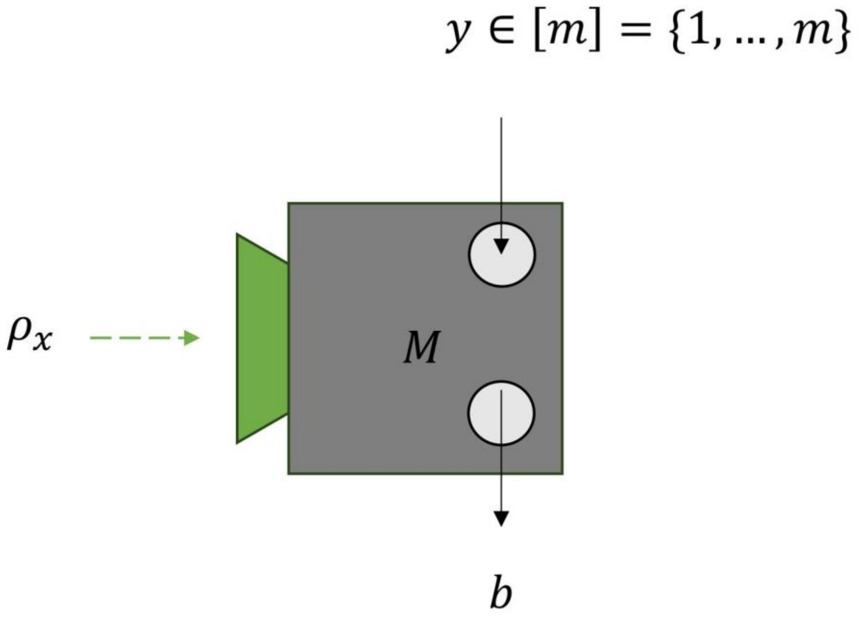
- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.
- Probability of outcome b for POVM defined by y, and state prepared by x is given by the Born rule as follows,

$$\boxed{p(b|y, x) = Tr(\rho_x \, E_{b|y})}$$

- For a non-destructive measurement the post-measurement state is

$$\boxed{\rho_{\{x,y,b\}} = \frac{K_{b|y}\rho_x K_{b|y}{}^{\dagger}}{Tr(K_{b|y}\rho_x K_{b|y}{}^{\dagger})}} \qquad E_{b|y}{}^{\dagger} = K_{b|y}K_{b|y}{}^{\dagger}$$

Measurements (destructive)



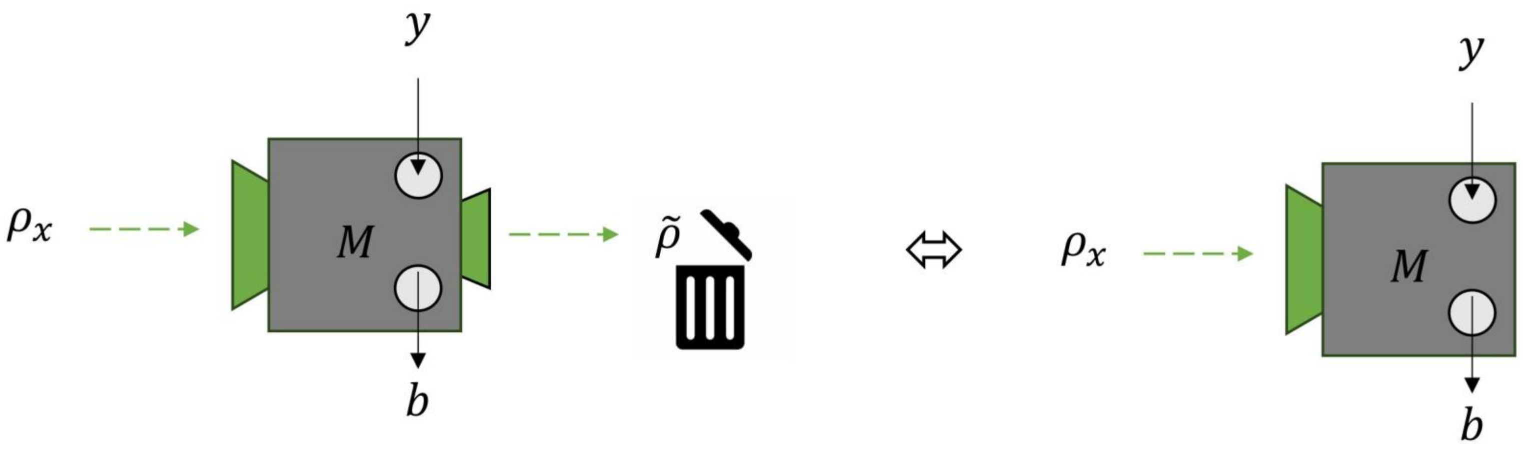
In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.
- Probability of outcome b for POVM defined by y, and state prepared by x is given by the Born rule as follows,

$$\boxed{p(b|y,x) = Tr(\rho_x \, E_{b|y})}$$

- For a destructive measurement there is no post-measurement state

Operationally, to trash the system is equivalent to assume that it did not exist.



First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

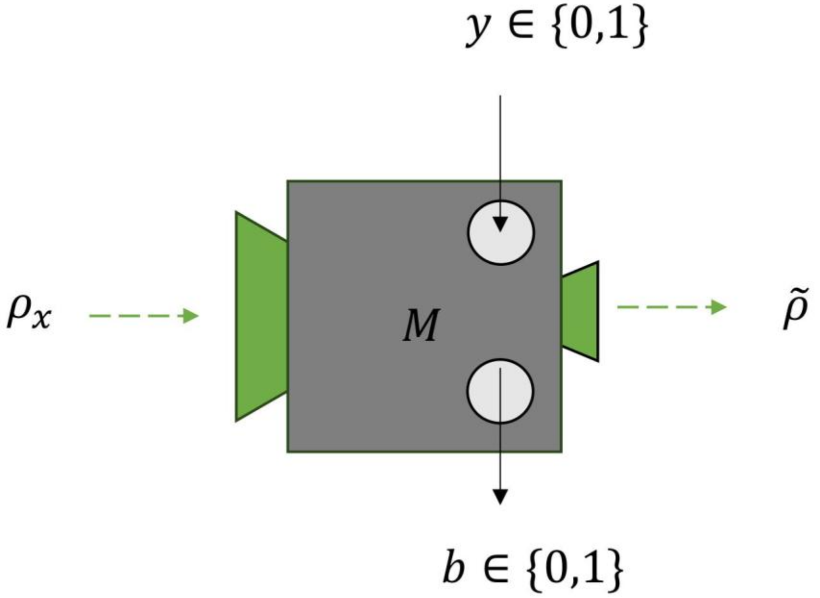
$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$$\{E_{b|y}\} \Leftrightarrow \quad \{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\},$$

$$\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\},$$

Special case, where the POVM elements are projections, $P^2 = P$.



$$p(0|0,x) = Tr(\rho_x|0\rangle\langle 0|) \Rightarrow \tilde{\rho} = |0\rangle\langle 0|$$

$$p(1|0,x) = Tr(\rho_x|1\rangle\langle 1|) \Rightarrow \tilde{\rho} = |1\rangle\langle 1|$$

$$p(0|1,x) = Tr(\rho_x|+\rangle\langle +|) \Rightarrow \tilde{\rho} = |+\rangle\langle +|$$

$$p(1|1,x) = Tr(\rho_x|-\rangle\langle -|) \Rightarrow \tilde{\rho} = |-\rangle\langle -|$$

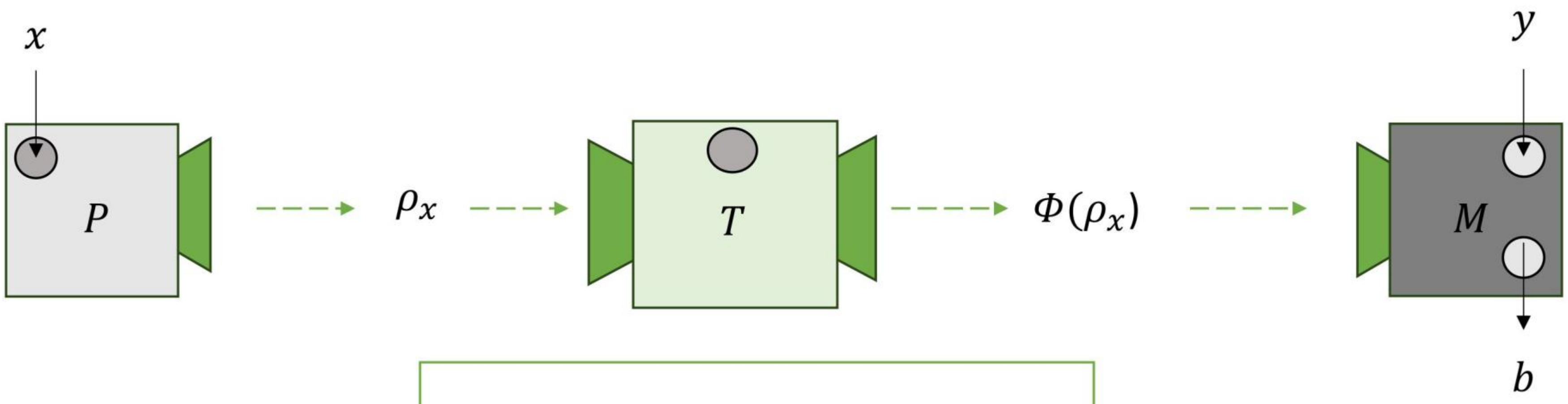
Calculating the post-measurement state for projective measurements is easier, it is just the state associated with the classical value registered y.

Now that we have the boxes defined…

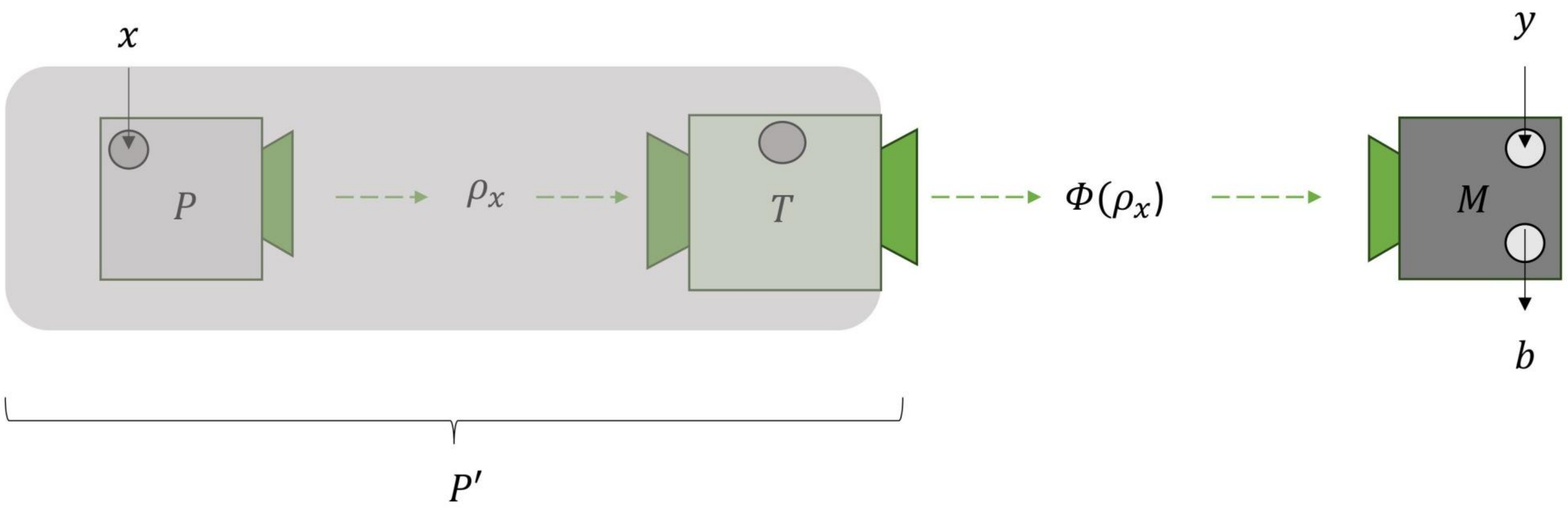
How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

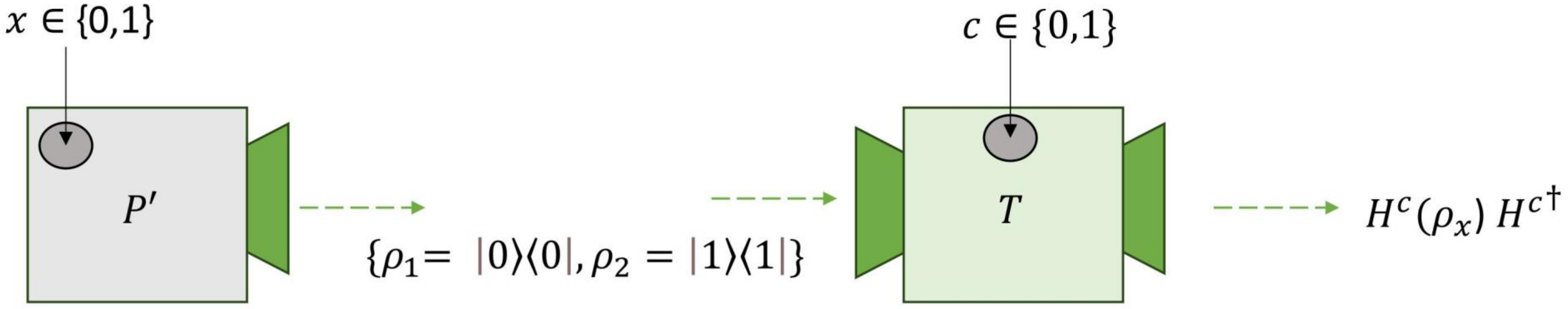
- $P < T$; $P < M$;
- $T < T$; $T < M$;
- $(M < M)$; $(M < T)$;

What is the simplest diagram using: 1 Preparation, 1 Transformation and 1 Measurement?

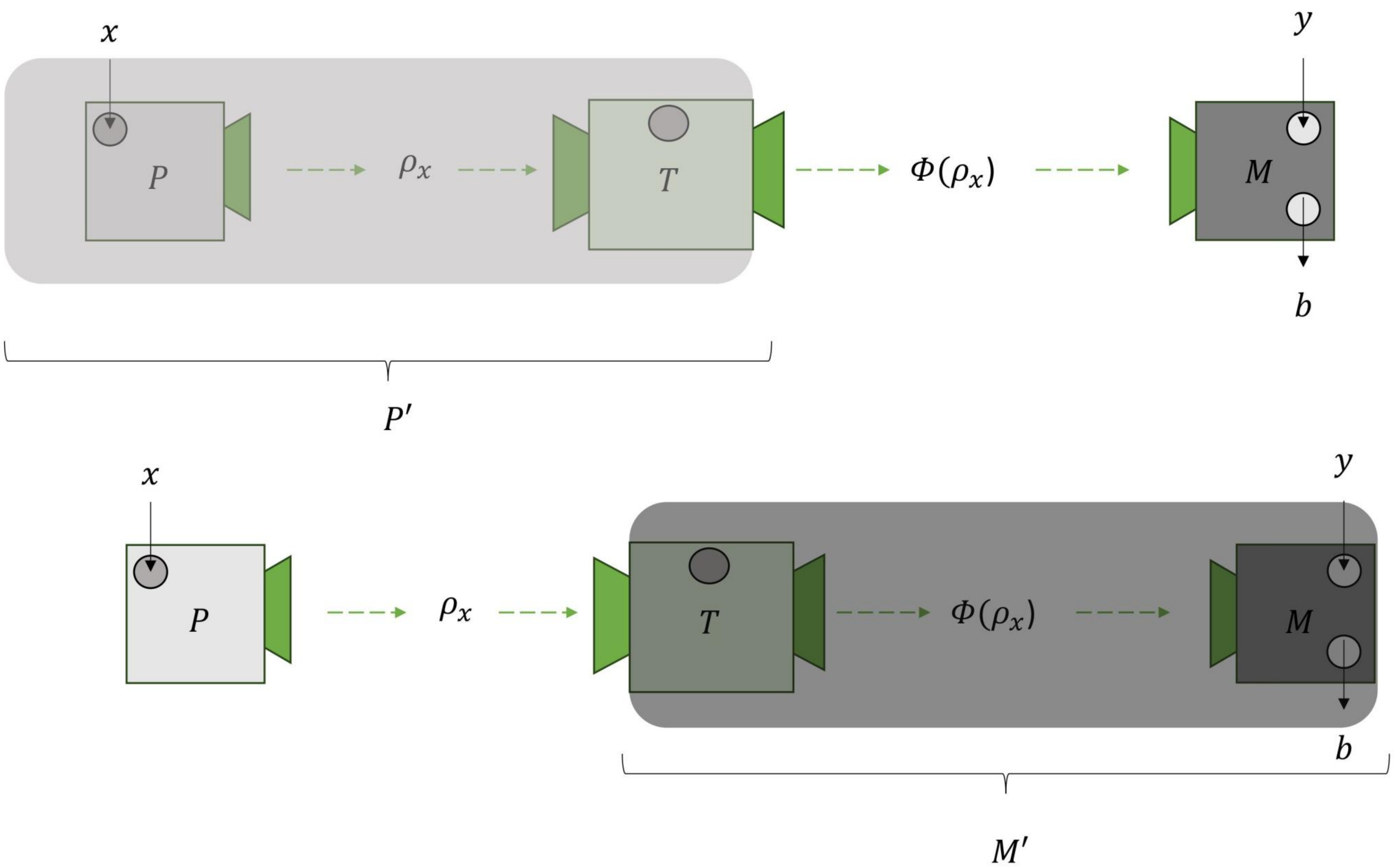


$$p(b|y,x) = Tr(\Phi(\rho_x)E_{b|y})$$




$x \in \{0,1\}$
P'
$\{\rho_1 = |0\rangle\langle 0|, \rho_2 = |1\rangle\langle 1|\}$
$c \in \{0,1\}$
T
$H^c(\rho_x)\, H^{c\dagger}$

This is equivalent to the original example of the preparation we saw.


x
y
P
ρ_x
T
$\Phi(\rho_x)$
M
b
P'
x
y
P
ρ_x
T
$\Phi(\rho_x)$
M
b
M'

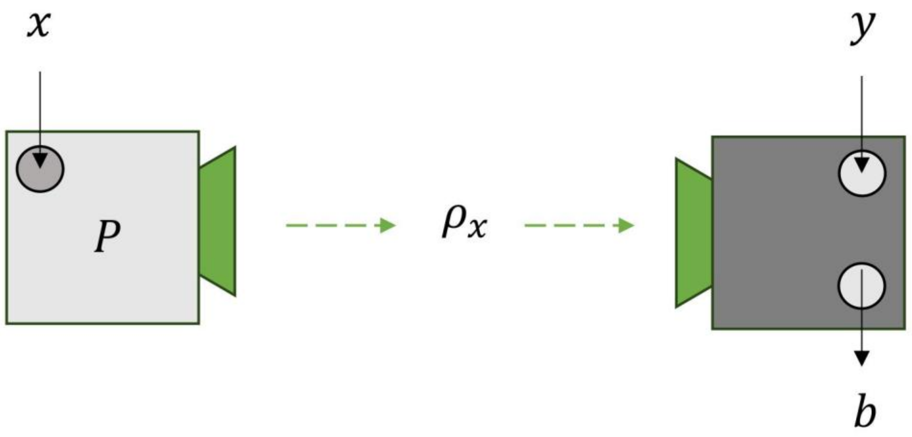
How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:

Quantum outputs can connect to quantum inputs (ignoring Transformations)

- $P < M; \ \ (M < M);$

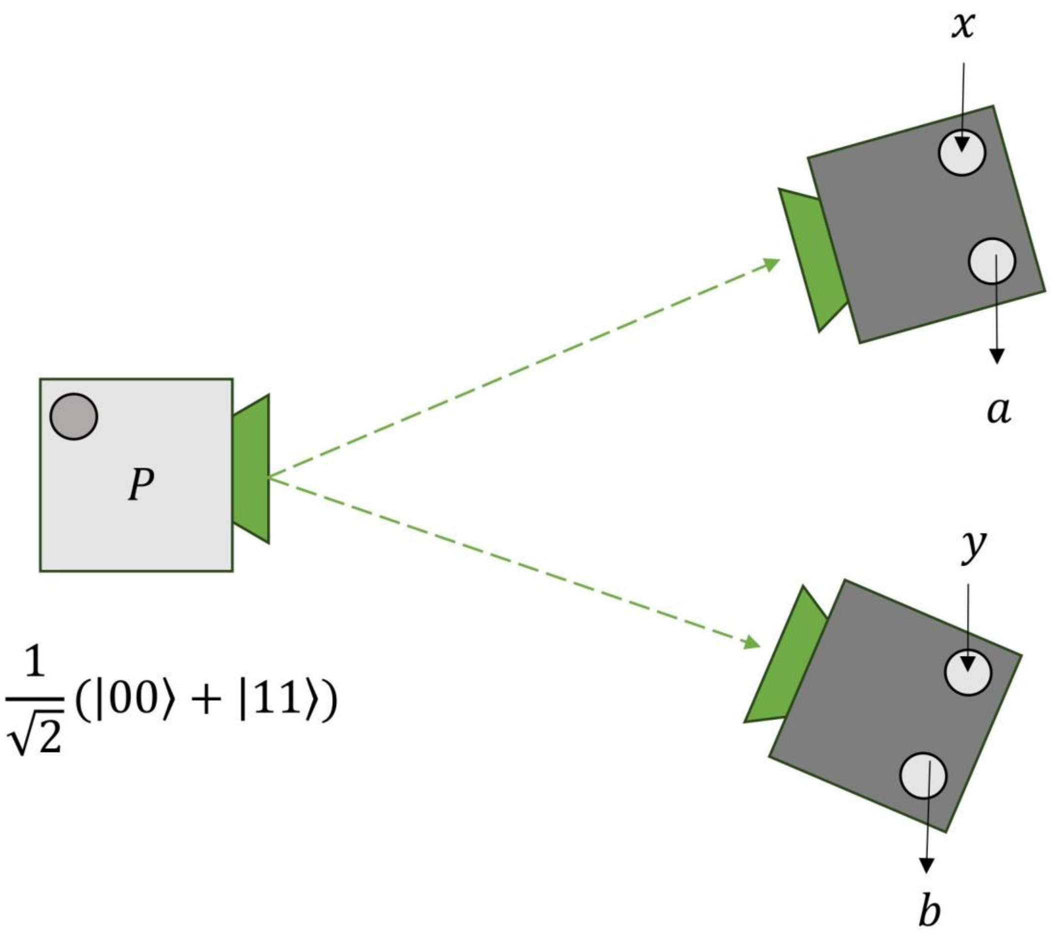
We are going to focus only on Preparation and Measurements.
What is the simplest diagram using: 1 Preparation and 1 Measurement? There is only one…

Prepare and Measure scenario



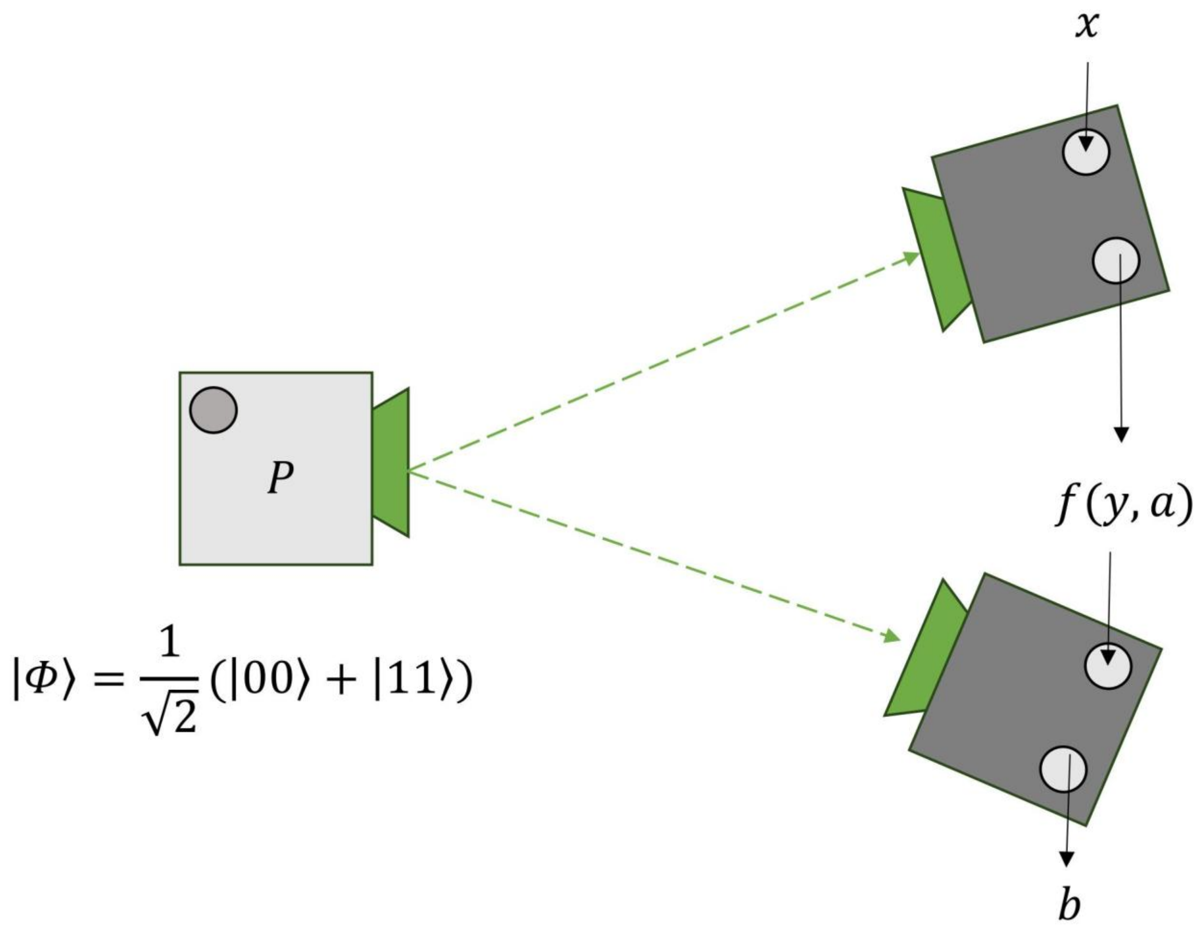
$$p(b|y,x) = Tr(\rho_x E_{b|y})$$

1 Preparation and 2 Measurements: Bi-partite Bell (Nonlocality)

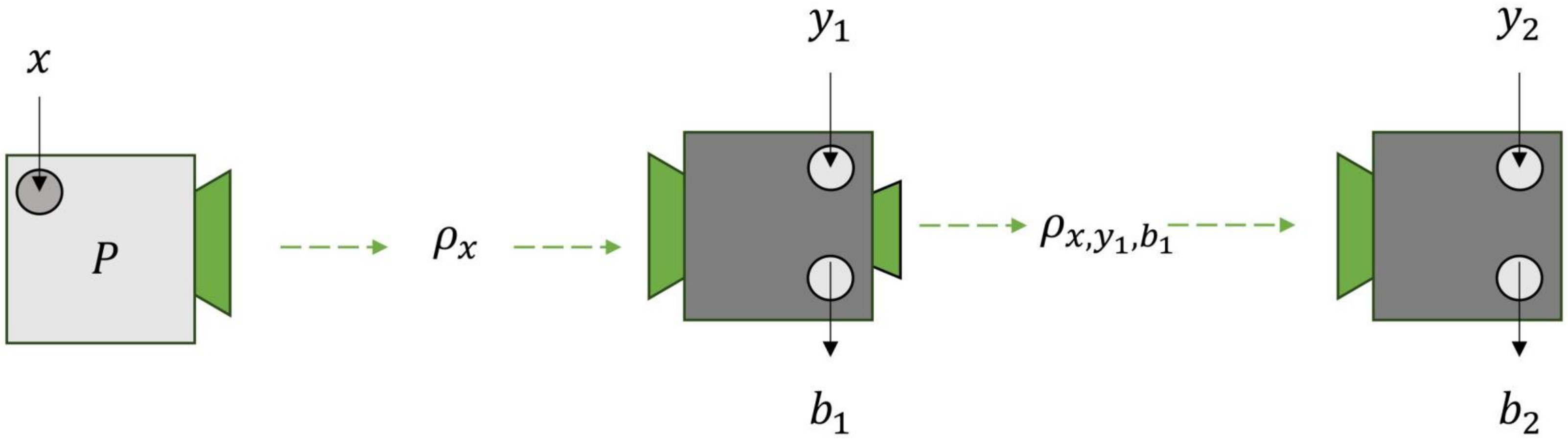


$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

1 Preparation and 2 Measurements: Bi-partite Bell w/ restricted classical communication


x
P
$f(y,a)$
b
$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

1 Preparation and 2 Measurements: Sequential Measurement Scenario with two measurements (Legget-Garg Inequalities, Temporal correlation, KS-Contextuality)



1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

2 Preparations and (up to) 4 Measurements:

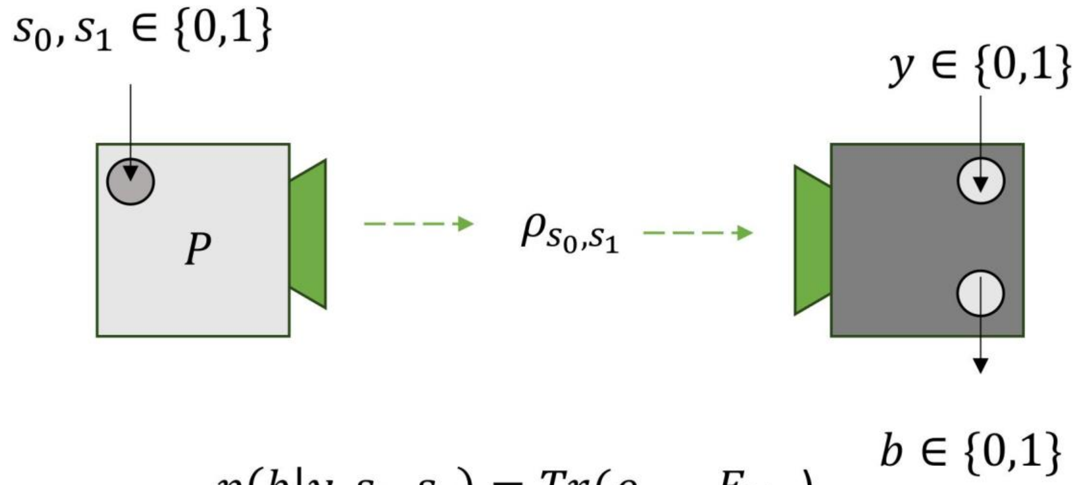
- Bi-local scenario
- Entanglement-assisted PM

… and many more!

Reduced to a caricature, the operational perspective could be read to say

- Quantum Information = Finding interesting ways to connect boxes;
- Quantum Cryptography = Finding interesting ways to <u>securely</u> connect boxes;

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.



$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

Define the density operators for the possible inputs:

- $\{\rho_{00} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \rho_{01} = |+\rangle\langle +|, \rho_{11} = |-\rangle\langle -|\}$

Define the measurements:

- $\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\}$
- $\{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\}$,

$p(b = s_0|y = 0, s_0, s_1 = 0) = 1$

$p(b \neq s_0|y = 0, s_0, s_1 = 0) = 0$

$p(b = s_0|y = 1, s_0, s_1 = 0)= 1/2$

$p(b \neq s_0|y = 1, s_0, s_1 = 0) = 1/2$

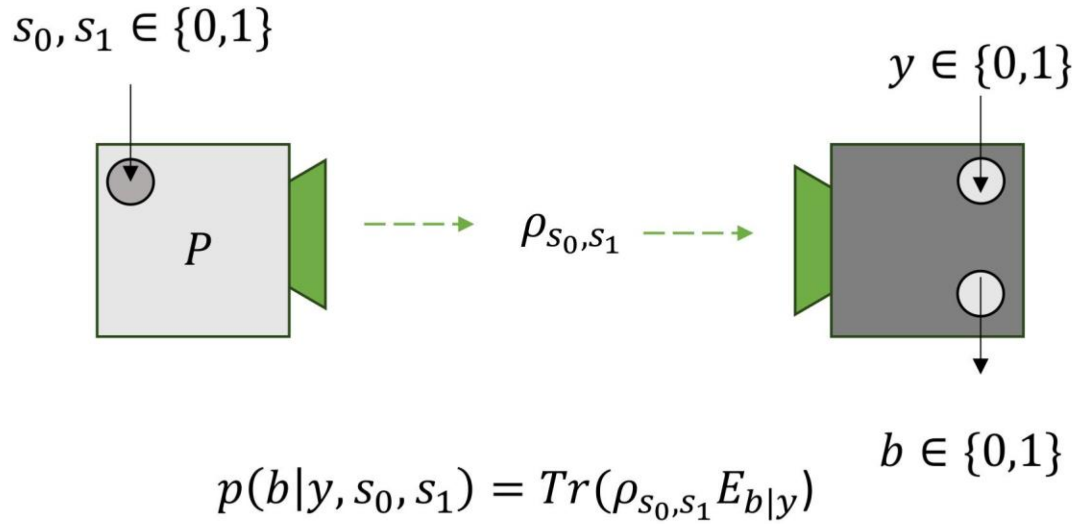
$p(b = s_0|y = 1, s_0, s_1 = 1) = 1$

$p(b \neq s_0|y = 1, s_0, s_1 = 1) = 0$

$p(b = s_0|y = 0, s_0, s_1 = 1)= 1/2$

$p(b \neq s_0|y = 0, s_0, s_1 = 1) = 1/2$

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.



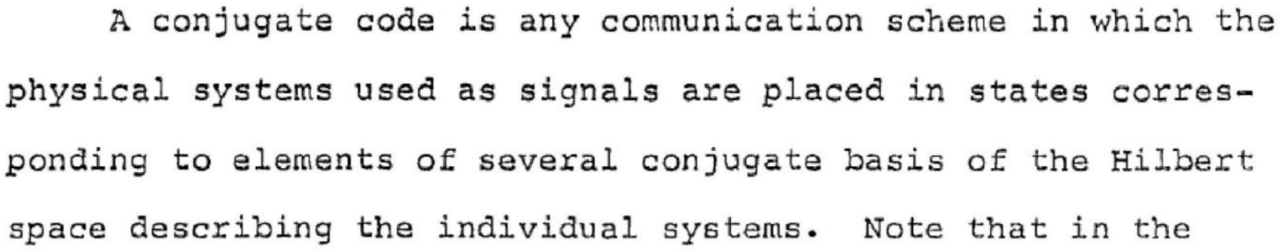
$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

Define the density operators for the possible inputs:

- $\{\rho_{00} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \rho_{01} = |+\rangle\langle +|, \rho_{11} = |-\rangle\langle -|\}$

These states form Mutually Unbiased Basis (or Conjugate Basis) i.e. Computational and Diagonal, these are states such that, when projected to the other basis no information is obtained about the state of the system.

This is the basic idea of Wiesner's Conjugate Coding paper:



A conjugate code is any communication scheme in which the physical systems used as signals are placed in states corresponding to elements of several conjugate basis of the Hilbert space describing the individual systems. Note that in the

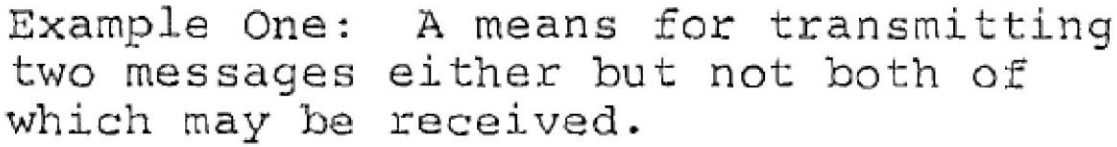
Thes scheme is the building block for:

- The first Quantum Oblivious Transfer (QOT) protocol proposed;
- The Bennet-Brassard QKD protocol (BB84)

… and even some recent work from IT-Aveiro (Q-OLE by M. Santos et al)

But even in the original conjugate coding, Wiesner already gave two applications of this idea. As we will see, under some very strong assumptions, the first example can already be rightfully claimed to be an OT.

First application of Conjugate Coding:

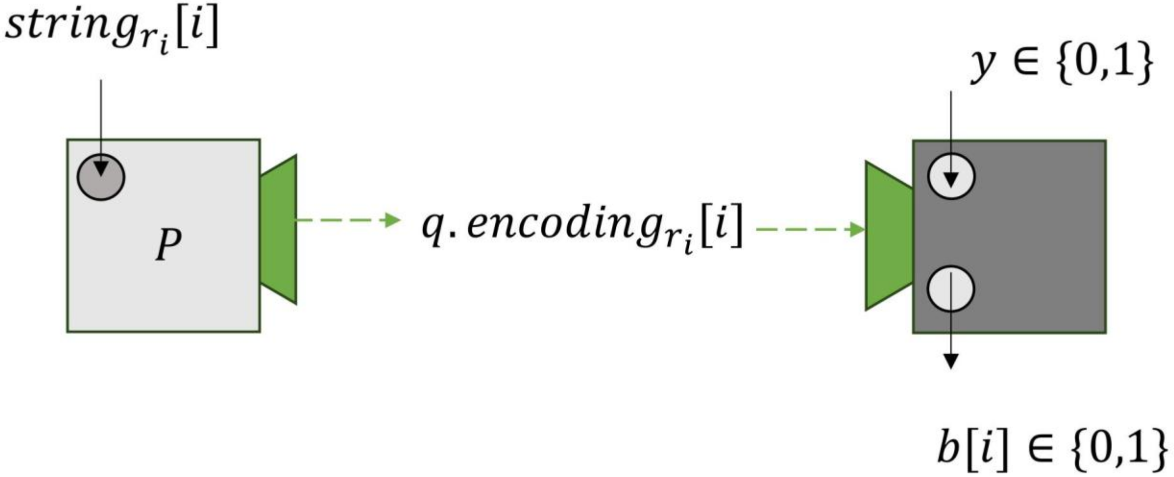


Example One: A means for transmitting two messages either but not both of which may be received.

$$string_1 = 0010100\ldots \qquad q.encoding_1 = |0\rangle\langle 0|, |0\rangle\langle 0|, |1\rangle\langle 1|, |0\rangle\langle 0| \ldots$$

$$string_2 = 1011100\ldots \qquad q.econding_2 = |-\rangle\langle -|, |+\rangle\langle +|, |-\rangle\langle -| \ldots$$

$For\ i\ rounds, r_i \underset{\$}{\leftarrow} \{1,2\}$:

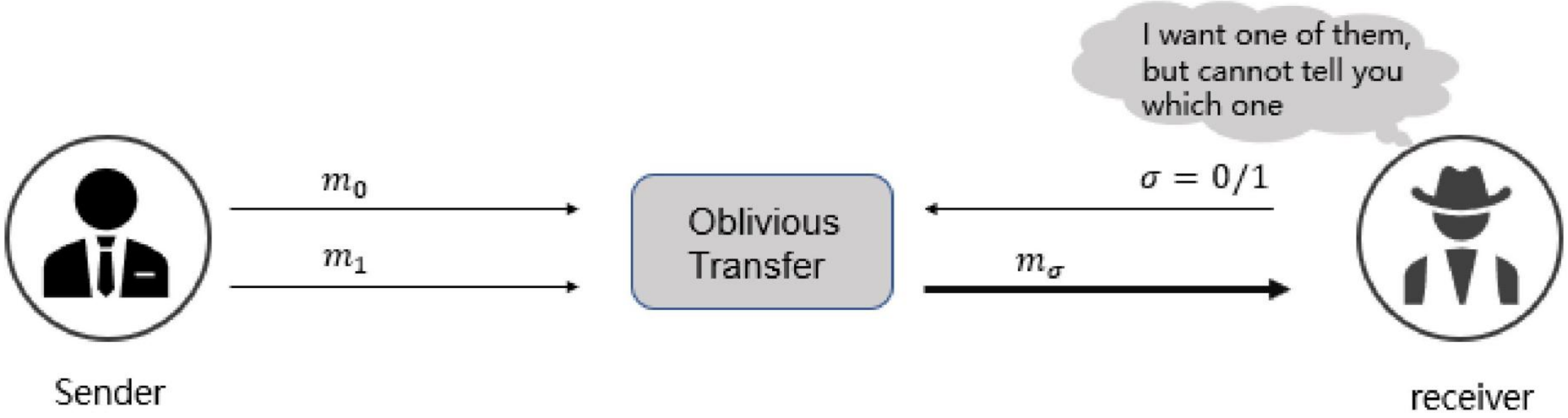


Bob's measurement is not so good, so it needs to fix à priori the y globally for all rounds.

So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

⇩

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.



So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.

- It is perfectly secure against a malicious Sender/Alice;
- It is secure against a semi-honest Receiver/Bob, for a trusted model of non-adaptative single qubit measurements

Collective measurements are a problem.
Solved with extra physical assumptions on the trusted model, or computational assumptions.

Thanks!

(You can ask me for references, I forgot to put them on the slides)

MARIANO
LEMUS

MARIANO **LEMUS**

PostDoc researcher at Instituto de Telecomunicações (IT). His main scientific interests include quantum physics, information theory, cryptography, and the connections between these fields. His research focuses on developing quantum cryptographic protocols and studying their security properties, as well as the study of multipartite quantum correlations and quantum algorithmic information theory.

2022 – PhD in Physics, Instituto Superior Técnico de Lisboa

2015 – Master in Theoretical Physics, Russian People's Friendship University

2010 – BSc in Physics, Universidade del Valle de Guatemala

ABSTRACT

THE ABC OF COMPOSABLE SECURITY IN CRYPTOGRAPHY

ABSTRACT

Cryptographic protocols often arise from informal description of communication tasks. These descriptions generally take the form of a communication scenario together with a list of desired features about the way information is exchanged within the involved parties. In order to mathematically analyse the security of a protocol, these features must be first formalised; however, there is more than one way of mathematically modelling protocols, information, and filling the details that are often left from such informal descriptions.

The Universal Composability (UC) framework is a powerful tool that provides us with:

- A straightforward way to model communication tasks as ideal functionalities
- A security definition with which we can evaluate if any given protocol securely realises its target task
- The guarantee that any protocol whose proven secure under the framework can replace its associated ideal functionality when used as a subroutine of other (arbitrary) protocols

The main objects of study in the UC framework are protocols, which are understood as algorithms or computer programs written for a distributed system. A protocol consists of several separated programs called machines. Each program runs independently from the others and is able to send and receive messages to/from others, and has its own individual inputs/outputs. Machines are defined by having a unique identifier Id, a communication set C, and its own associated program P. We may formalise a cryptographic task as a trusted machine, which parties can send inputs and it will run its internal program to produce outputs that satisfy the desired features of the task, these machines are referred as ideal functionalities.

In order to define what does it mean for a protocol to securely realise a given functionality we must first define the notions of execution and emulation. To model the execution of a protocol we consider an augmented protocol which consists of its own machines plus two special machines, called environment, and adversary. The adversary is used to account for the information leaked during the parties' communication, as well as behaviours outside what is scripted in the protocol's programs. In particular this can be used to model dishonest behaviours or device malfunctions; the adversarial model defines how much power the adversary is given. On the other hand, the environment is connected to the adversary and to the external input/output channels of the machines in the protocol. The role of the environment in security is to characterise the behaviour of the protocol "as seen from outside". We say that a protocol P1 UC-emulates a protocol P2 if, for any adversary on A1, there exists an analogous adversary on A2, such that no environment can distinguish between a run of P1 with A1 and P2 with A2. When P2 is considered to be an ideal functionality, the associated adversary A2 is usually called a simulator.

Using the notion of emulation, we can say that a protocol UC-securely realises a given functionality if it emulates it according to the above notion. The universal composition theorem states that if one protocol emulates another, it can substitute it in any network context and the results will be indistinguishable. This property makes UC secure protocols very desirable, as they can be straightforwardly used in complex schemes without the concern of them introducing unforeseen vulnerabilities.

The ABC of Composable Security in Cryptography

Mariano José Lemus Hernández

Instituto de Telecomunicações - Aveiro

January 8, 2025

Motivation: Defining Security in Cryptography

- Cryptographic protocols often arise from informal descriptions of communication tasks.

  “A wants to send a message to B without C knowing what the message is”

- Provable security generally requires quantifying its security features.

  “How do we measure how much of the message C knows?”

- More than one way of mathematically modeling protocols, information, and filling the details left from such descriptions.

  “What is acceptable if the protocol fails?”

  “What is acceptable if later C finds out half of the message?”

- The security of a protocol as a measure of how well it “does its job”.

A Classification of Security Definitions

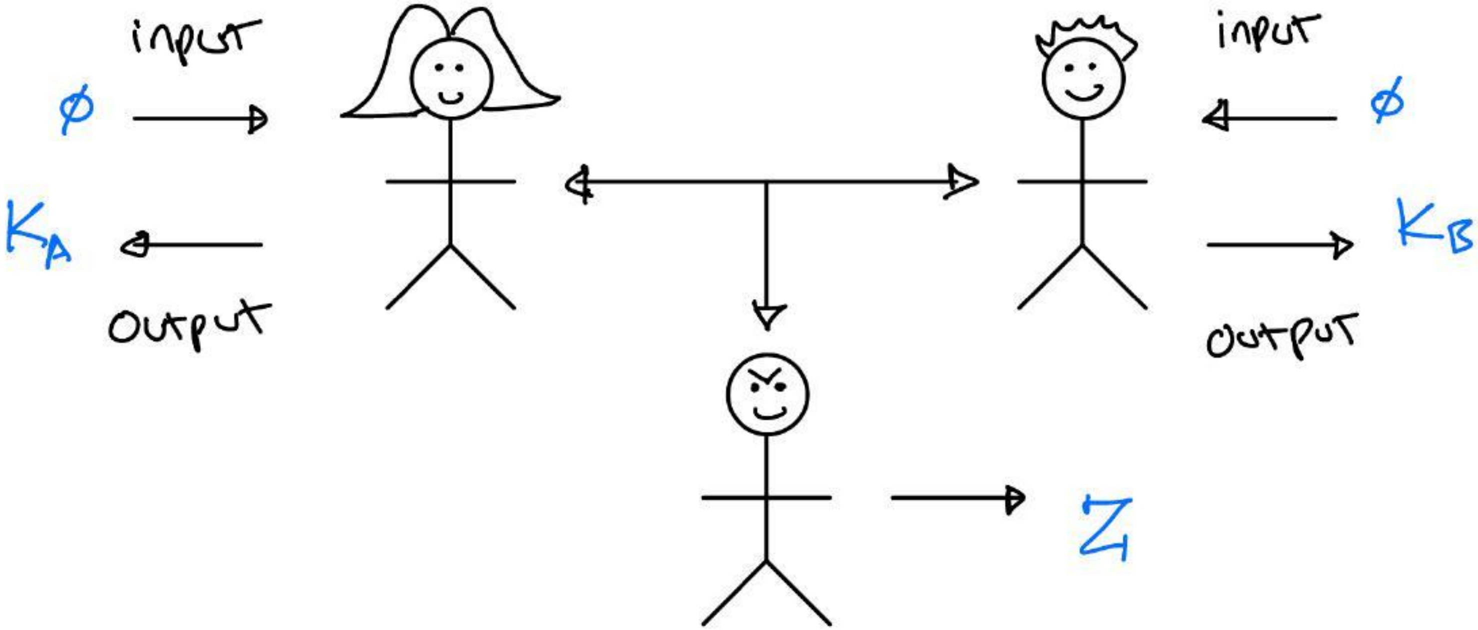
We can classify modern security definitions as follows:

- Stand-alone security – as list of properties expressed in terms of guessing probability, mutual information, entropy, etc.
- Indistinguishability-based security – as a list of indistinguishability relations between variables of the protocol and their respective “ideal” outcomes.
- Simulation-based security – as a list of (implied) indistinguishability relations between the executions of the protocol and its respective ideal functionality.

An Example: Key Distribution

Informal statement of the communication task:

"Alice wants to share a random n-bit key k with Bob without Eve knowing what the key is"



An Example: Key Distribution – Stand-Alone Security

1. $k_A = k_B$, except with negligible probability in n (The key is shared)
2. The distribution of K_A is uniform in the set of n-bit strings (The key is random)
3. The accessible information $I_{\text{acc}}(K_A : E)$ is negligible in n (Eve does not know the key)

$$I_{\text{acc}}(K_A : E) = \max_{\mathcal{M}} I(K_A : Z) \tag{1}$$

An Example: Key Distribution – Stand-Alone Security

Consider the following quantum state with:

$$\rho_{XYE} = \frac{1}{2 \cdot 3^m} \sum_{\substack{x \in \{0,1\} \\ y \in \{1,2,3\}^m}} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \rho_E^{x,y} \tag{2}$$

with

$$\rho_E^{x,y} = \frac{1}{2^m} \left(I + (-1)^x \sigma_y \right). \tag{3}$$

It can be shown that $I_{\text{acc}}(XY : E) \leq \frac{2}{3}^{\frac{m}{2}}$. However, for a fixed value of y the states $\rho_E^{0,y}$ and $\rho_E^{1,y}$ are orthogonal.

An Example: Key Distribution – Indistinguishability-based security

Using the second approach, all security features can be combined into one statement

$$\rho_{XYE} \approx \frac{1}{2^n} \sum_{k \in \{0,1\}^n} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B} \otimes \rho_E \tag{4}$$

In other words, the trace distance between both sides of Eq.(4) is negligible in n.

An Example: Key Distribution – Simulation-based security

Functionality $\mathcal{F}'_{\text{KD}}$

Parameters:

- Parties Alice and Bob, eavesdropper Eve.
- Size n of the output key.

1. Upon receiving the message (*send keys*) from Alice, sample uniformly $k \leftarrow \{0, 1\}^n$, output k to Alice and Bob, and the message (*key shared*) to Eve and halt.

An Example: Key Distribution – Simulation-based security

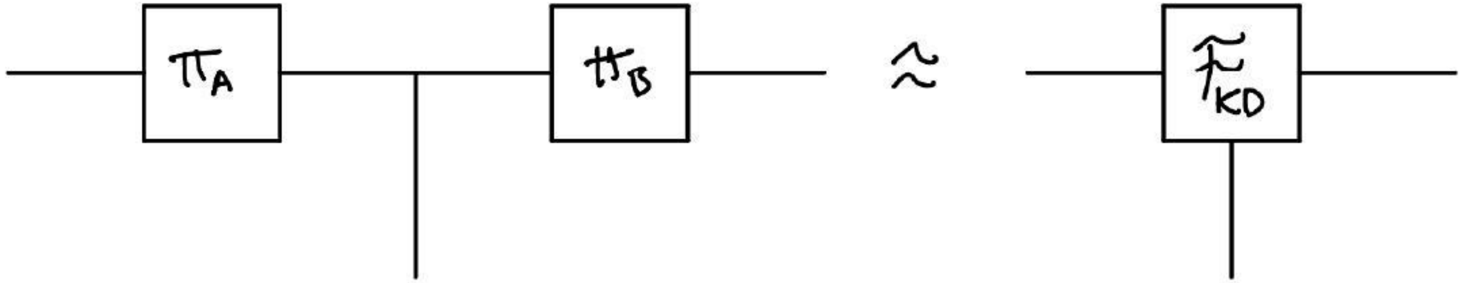


Figure: Emulation-based security statement: The ϕ_A, ϕ_B represent the local programs Alice and Bob run as part of executing the protocol and the wires represent communication channels.

More than one Flavor

Examples of simulation-based frameworks

- Universal Composability Framework (Canetti, 2001)
- Quantum Universal Composability Framework (Unruh, 2009)
- Abstract Cryptography Framework (Maurer, Renner, 2011)
- Simplified UC Framwork (Canetti, Cohen, Lindell, 2014)

Universal Composability Framework

- Main object of analysis are **Protocols**, which are understood as *algorithms* or *computer programs* written for a distributed system.
- A protocol consist of several separated programs called **Machines**:
  - Each program runs independently from the others and is able to send and receive messages to/from others
  - Each program has its own individual inputs/outputs

Machines and Protocols

- Formally, a machine is a triplet $\mu = (\mathsf{Id}, C, \tilde{\mu})$, where
  - Id is the identifier of the machine within the communication network
  - C is a communication set; a set of communication channels with other machines within the network
  - $\tilde{\mu}$ is the program of the machine
- A protocol is a set of machines $\pi = (\mu_1, \ldots, \mu_n)$, satisfying a set of compatibility requirements. (Note: machines in a protocol may have communication channels to machines not in the protocol)
- Protocols may be parametrized by a security parameter k

Execution and Emulation

The model of execution for protocol π consists of the machines in π plus two additional special machines, called the environment $\mathcal{E}$ and the adversary $\mathcal{A}$:

- The environment $\mathcal{E}$ communication set allows it to provide inputs and receive outputs from the *external communication* channels of the machines in π, and to $\mathcal{A}$. Additionally, it has a single external channel for input/output. Its outputs are always binary.
- The adversary $\mathcal{A}$ communication set allows it receive backdoor information from *all* machines in π, who are augmented with an extra communication channel with $\mathcal{A}$.

The resulting set of machines can be understood as an associated protocol which can only receive inputs through $\mathcal{E}$.

Execution and Emulation

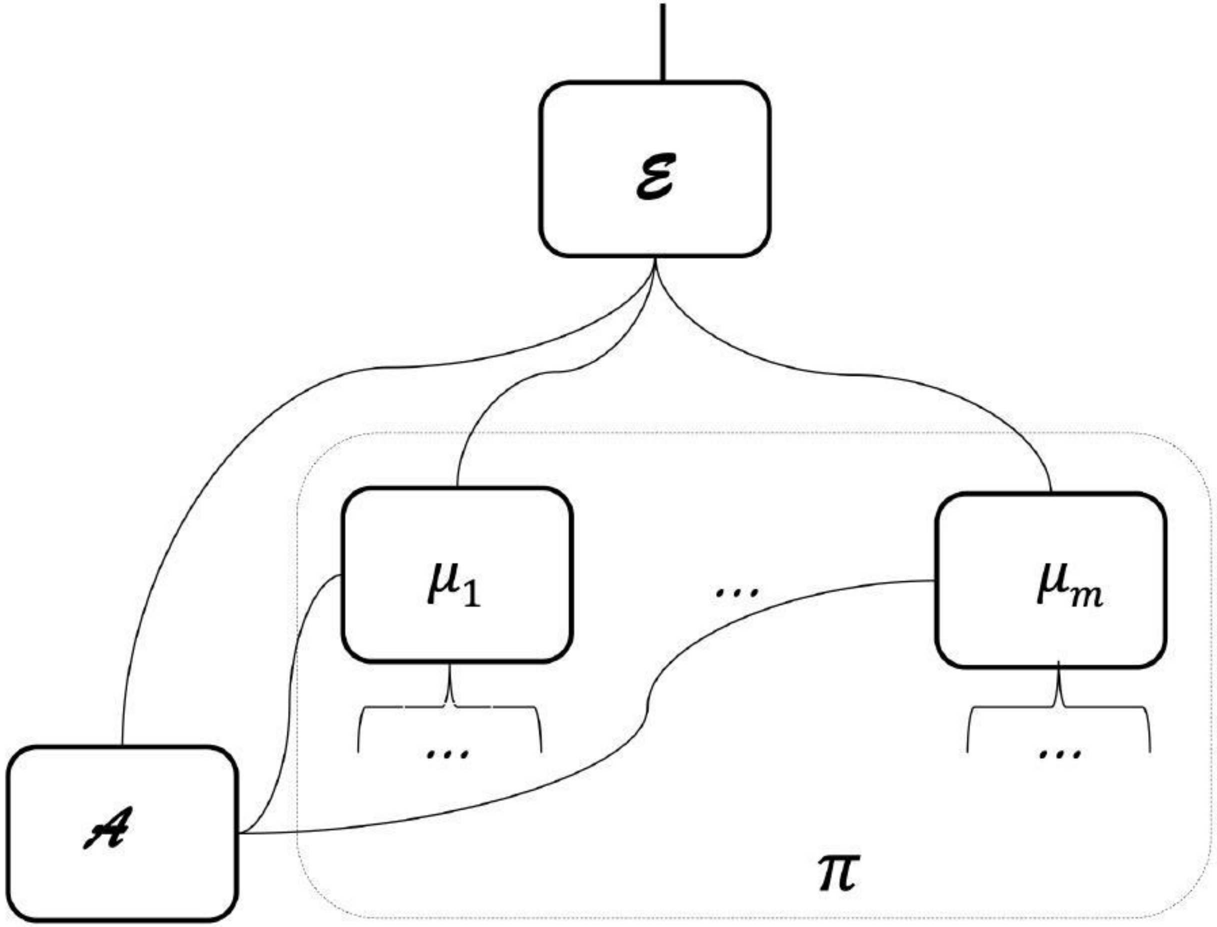


Figure: Diagram of a protocol execution. (Canetti, 2001)

Execution and Emulation

- Denote by $\text{EXEC}_{\pi,\mathcal{A},\mathcal{E}}(k,z)$ the random variable associated to the output of an execution of the joint programs of $\pi, \mathcal{A}, \mathcal{E}$ on input z and security parameter k.
- Denote by by $\text{EXEC}_{\pi,\mathcal{A},\mathcal{E}}(k)$ the ensemble $\{\text{EXEC}_{\pi,\mathcal{A},\mathcal{E}}(k,z)\}_{z\in\{0,1\}^*}$
- A protocol π **UC-emulates** a protocol ϕ if for any adversary $\mathcal{A}$, there exists an adversary $\mathcal{S}$, such that, for any environment $\mathcal{E}$, the ensembles $\text{EXEC}_{\pi,\mathcal{A},\mathcal{E}}(k)$ and $\text{EXEC}_{\phi,\mathcal{A},\mathcal{E}}(k)$ are indistinguishable in k.
- Statistical vs Computational security

Execution and Emulation

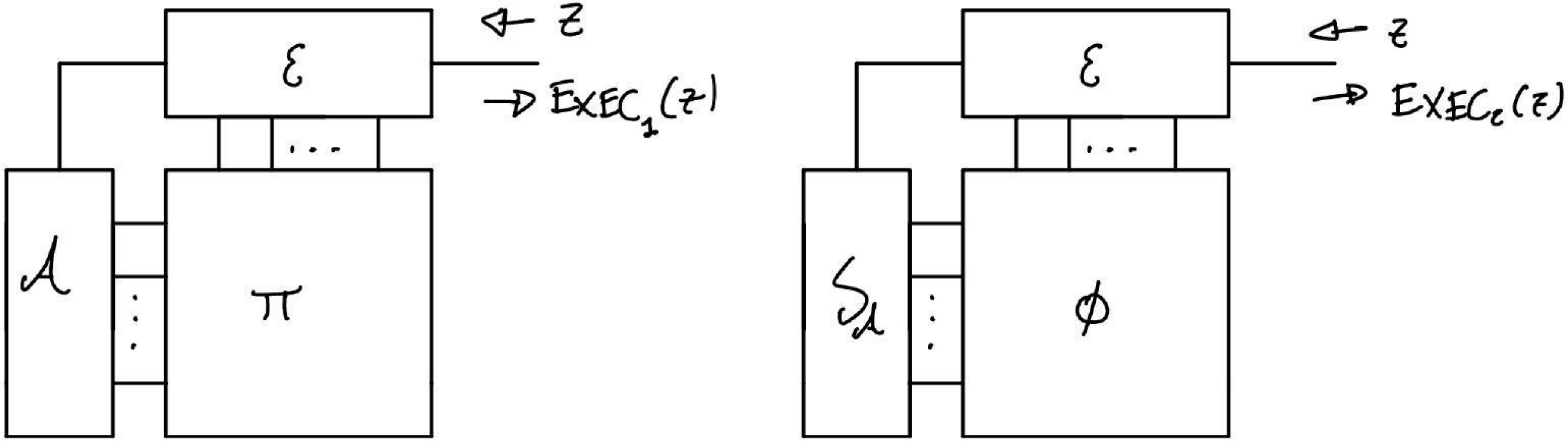


Figure: Execution of two protocols π and ϕ

Ideal Functionalities

- Ideal functionalities are understood as trusted machines that perform the desired task.
- The formalization of a cryptographic task is done by defining its respective ideal functionality.

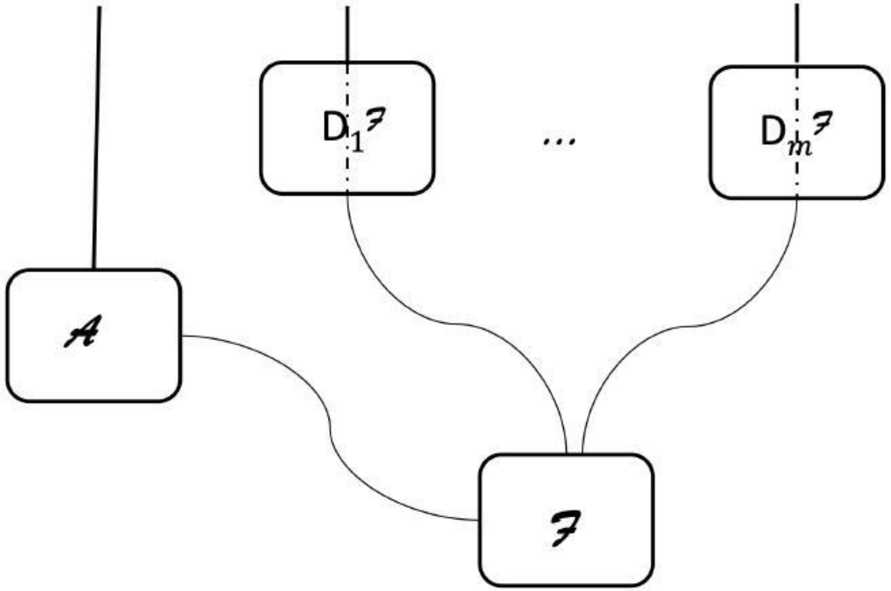


Figure: Protocol associated to an ideal functionality, $\text{IDEAL}_{\mathcal{F}}$. (Canetti, 2001)

Security in the UC framework

A protocol π UC-securely realizes an ideal functionality $\mathcal{F}$, if π UC-emulates IDEAL$_{\mathcal{F}}$.

Universal Composition Theorem

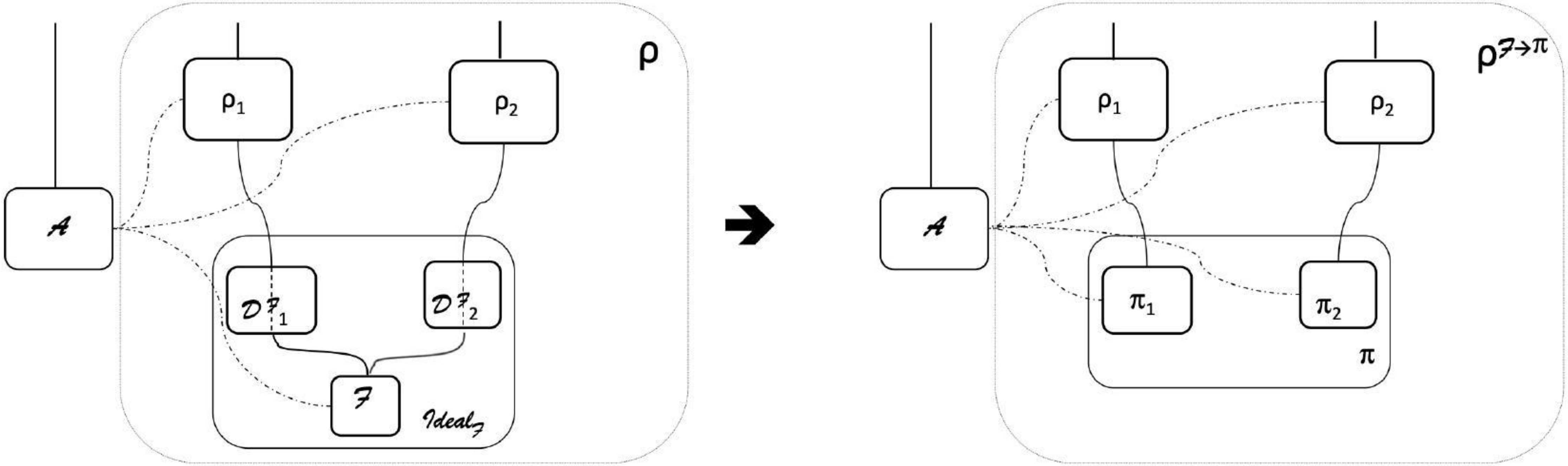

ρ
ρ_1
ρ_2
$\mathcal{A}$
$\mathcal{D}^{\mathcal{F}}_1$
$\mathcal{D}^{\mathcal{F}}_2$
$\mathcal{F}$
$\mathcal{I}deal_{\mathcal{F}}$
$\rho^{\mathcal{F}\to\pi}$
ρ_1
ρ_2
$\mathcal{A}$
π_1
π_2
π

Figure: Universal composition operation. (Canetti, 2001)

Some additional features

- Party corruption – Introduced in the definition of the programs of each machine to allow for interaction with the Adversary.
- Hybrid models – Protocols can be assumed to have access to trusted ideal functionalities. Useful for finding reductions.
    - E.g. Random Oracle model, Public-key infrastructure model...

From Classical to Quantum

- Unruh's Quantum UC-security framework is a direct generalization of Canetti's
- It separates itself in the machine model and in the addition of quantum communication channels

Quantum lifting theorem
Let π and ϕ be classical protocols such that π statistically (classically) UC-emulates ϕ, then π statistically quantum UC-emulates ϕ.

MPC reduction to BC
It has been proven that Oblivious Transfer (and thus, secure multiparty computation) can be quantum UC-securely realized through a quantum protocol in the $\mathcal{F}_{\text{BC}}$-hybrid model, which is believed to be impossible classically.

An Example: Key Distribution – Simulation-based security

Functionality $\mathcal{F}'_{\text{KD}}$

Parameters:

- Parties Alice and Bob, eavesdropper Eve.
- Size n of the output key.

1. Upon receiving the message (*send keys*) from Alice, send the message (*keys requested*) to Eve.
2. Upon receiving m from Eve:
   - If $m =$ (*allow*), sample uniformly $k \leftarrow \{0,1\}^n$, output k to Alice and Bob and the message (*key shared*) to Eve and halt.
   - Else, output the message (*unable to send keys*) to Alice, Bob, Eve and halt.

Closing Thoughts

- Simulation security frameworks are powerful tools for abstracting and analyzing the security of cryptographic protocols
- Great security comes with great requirements, not all useful protocols need be UC-secure
- Cryptography is a game of trade-offs

References

- Canetti, Ran. ”Universally composable security: A new paradigm for cryptographic protocols.” Proceedings 42nd IEEE Symposium on Foundations of Computer Science. IEEE, 2001.
- Unruh, Dominique. ”Universally composable quantum multi-party computation.” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.
- Maurer, Ueli and Renato Renner. “Abstract Cryptography.” International Conference on Supercomputing, 2011.
- Renner, Renato. Security of quantum key distribution. International Journal of Quantum Information, 6(01), 1-127, 2008.
- König, Robert, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. Physical Review Letters, 98(14), 140502, 2007.
- Canetti, Ran, Asaf Cohen, and Yehuda Lindell. ”A simpler variant of universally composable security for standard multiparty computation.” Advances in Cryptology–CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015.

Thank you for your attention!

ARMANDO N.
PINTO

ARMANDO N. **PINTO**

ABSTRACT

Full Professor at the Department of Electronics, Telecommunications and Informatics at the University of Aveiro and leads the Optical Quantum Communications group at the Instituto de Telecomunicações in Aveiro. He is an author and has presented his work in more than 200 international scientific journals and conferences. The work carried out by him and the team he coordinates has been awarded more than 23 scientific awards. He holds 4 international patents and has participated in 57 research projects, having been global coordinator of 24. He is currently coordinator of a European Union project and a NATO project, both in the area ofquantum communication technologies. He is a member of the Editorial Board of the journals “Scientific Reports”, published by Nature, and of the journals “Optical and Quantum Electronics” and “Quantum Communication”, published by Springer and the Institute of Engineering and Technology, respectively. He is the President of the Technical Committee for Standardization CTE JTC 22 – Quantum Technologies, operating within the scope of IEP - Instituto Eletrotécnico Português. He is a Senior Fellow of the Institute of Electrical and Electronics Engineers and a Senior Fellow of the Optica Society.

ABSTRACT

QUANTUM COMMUNICATIONS

Quantum communications are at the forefront of a global technological revolution, promising to redefine the very foundations of information security, computation, and network infrastructure. At the heart of this transformation is the exploitation of quantum mechanical principles—superposition, entanglement, and the no-cloning theorem—to enable new paradigms of communication that are inherently secure and fundamentally different from classical methods. This presentation provides a comprehensive overview of quantum communications, from core principles and key technologies to the broader vision of integrated quantum networks and beyond.

One of the most mature and commercially significant applications of quantum communication is Quantum Key Distribution (QKD). QKD allows two parties to generate a shared, random secret key, used to encrypt and decrypt messages, with the security of the process guaranteed by the laws of quantum mechanics. Unlike classical encryption methods, whose security is based on computational assumptions and thus vulnerable to future quantum computers, QKD provides information-theoretic security—even against adversaries with unlimited computational power.

The transition from point-to-point QKD links to quantum networks represents a significant leap in capability. Significant efforts are underway globally to develop testbeds and deploy regional and national-scale quantum networks, where European Union initiatives, including the Quantum Communication Infrastructure (EuroQCI), are working toward a pan-European quantum-secure network.

Portugal is actively participating in this ecosystem through collaborative projects involving academic institutions, industry leaders such as Altice Labs, and international partners. The Instituto de Telecomunicações (IT) and the Universidade de Aveiro have been at the forefront of quantum communication research in Portugal, contributing to the development and testing of new quantum communication protocols, photonic systems, and QKD hardware. This collaborative environment fosters innovation not only in fundamental research but also in practical, deployable systems that are interoperable with existing telecommunications infrastructure.

While QKD is the most prominent and commercially advanced application, the landscape of quantum communications is rapidly expanding beyond QKD. New directions include quantum oblivious transfer protocols to assist secure multiparty computation applications:

These advancements reflect a shift toward a broader quantum cryptographic ecosystem, where QKD is just one component of a more general infrastructure for secure communication and information processing. Importantly, this ecosystem must be designed to coexist and integrate with classical infrastructure, ensuring a hybrid model that leverages the strengths of both domains. This hybridization will be critical as we transition through the "quantum-safe" era—where post-quantum classical cryptography and quantum cryptographic methods are deployed in parallel to provide layered security.

The presentation will also touch upon the societal and ethical implications of quantum communication. The shift toward unbreakable encryption has consequences for law enforcement, data sovereignty, and digital rights. Policymakers and technologists must work together to balance the benefits of quantum security with transparency and responsible governance.

INSTITUIÇÕES ASSOCIADAS

Quantum Communications

Armando Nolasco Pinto
anp@ua.pt

TechDay – Comunicações Quânticas
Altice Labs
Aveiro, Portugal, 5 de dezembro de 2024

What are quantum technologies?

They are technologies that profit from the peculiarities of quantum theory to do new things or to improve the way we do things

no-cloning

superposition

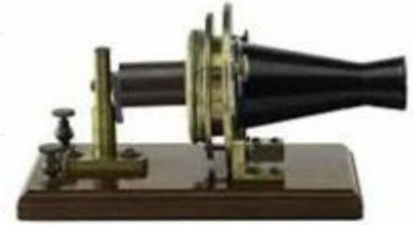
entanglement

Electromagnetic Theory of Information

Michael Faraday, 1831,
electromagnetic induction

James Clerk Maxwell, 1865,
electromagnetic radiation

Hendrik Lorentz, 1892,
propagation of light



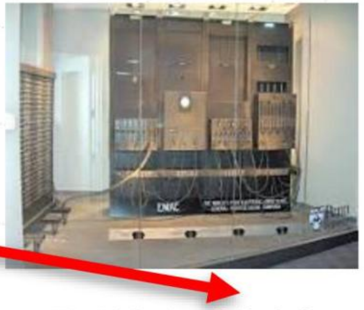
Alexander Bell, 1876,
the telephone

~50 years

~100 years

~150 years

~100 years



ENIAC, 1946,
the computer

Alan Turing, 1937,
general-purpose computer

John von Neumann, 1945,
digital computer

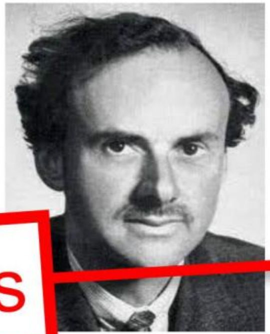
Claude Shannon, 1948,
information theory

WWW, 1990,
the internet

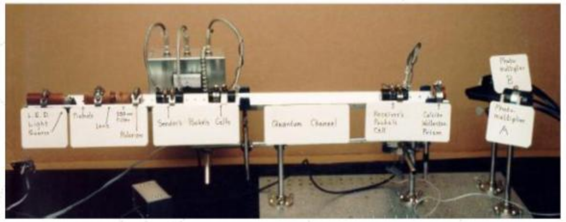
Quantum Theory of Information

Werner Heisenberg, 1925,
quantum matrix formulation

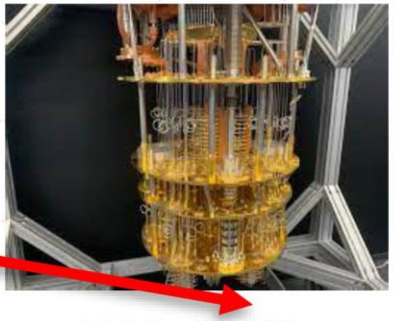
Wolfgang Pauli, 19
quantum theory of m



Paul Dirac, 1940s,
quantum electrodynamics



BB84, 1992,
quantum key distribution



IBM, 1998,
the quantum computer

Stephen Wiesner, 1970s,
quantum information

Charles Bennet,
Gilles Brassard, 1984,
quantum cryptography

Peter Shor, 1994,
quantum computing

~65 years

~70 years

~50 years

~100 years

2025 ?

2025 International Year of Quantum Science and Technology (IYQ)

- On June 7, 2024, the United Nations proclaimed 2025 as the International Year of Quantum Science and Technology (IYQ).

https://quantum2025.org

100 years of quantum is just the beginning...

What is a quantum computer?

- **Superposition:** from a bit to a qubit you gain 1 dimension (a qubit models a vector in a 2-dimension Hilbert space)

n bits vs n qubits : n vs 2n

- **N entangled qubits:** **2^n** (n entangled qubits models a vector in a 2^n -dimension Hilbert space)

n qubits vs n entangled qubits : 2n vs 2^n

- **Non-cloning/Interference:** probabilistic algorithm

Quantum Computer Threat

The security of our communication and information systems is based on computational complexity, so they are vulnerable to advances in computational power and algorithms

Quantum Computer Threat

Our systems can be vulnerable to anyone who has access to a quantum computer

The Grover and the Shor Algorithms

- Shor algorithms (quantum Fourier transform) and Grover (quantum search) are two of the most relevant quantum algorithms.

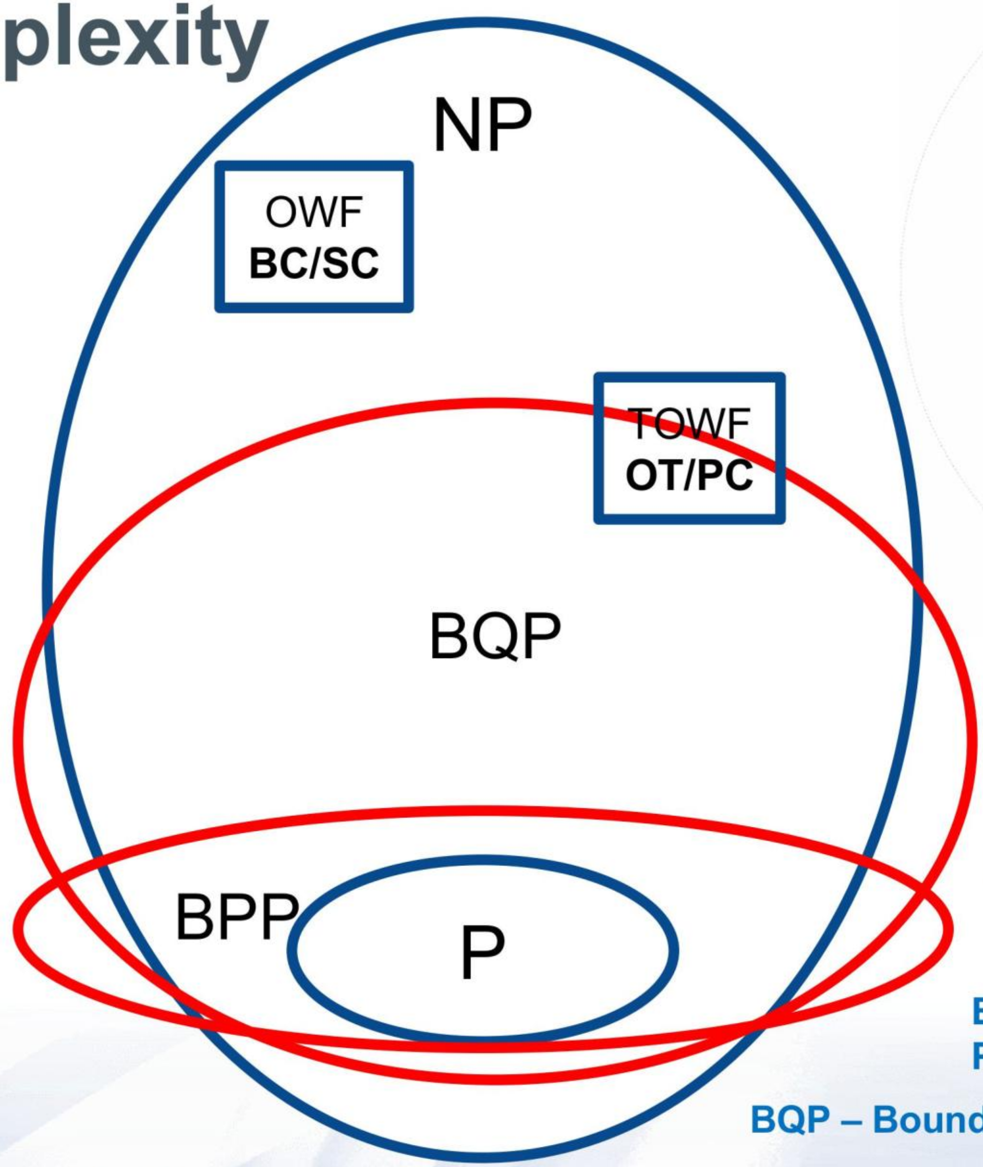
Peter Shor

Shor, P.W. "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press. pp. 124–134, 1994.

Grover, Lov K. "A fast quantum mechanical algorithm for database search". Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery. pp. 212–219, 1996.

Lov Grover

Foundations of cryptography
Computational complexity



P – Polynomial Time

NP – Verifiable in Polynomial Time

BPP – Bounded-error Probabilistic Polynomial Time

BQP – Bounded-error Quantum Polynomial Time

BC - Bit-Commitment **OWF – One-Way Function** **SC - Symmetric Cryptography**

OT – Oblivious Transfer **TOWF – Trapdoor One-Way Function** **PC – Public Cryptography**

Exhaustive Search (Classical)(AES-128)

- Assuming we can achieve 1 tera flops per second, using classical computing.

$$\frac{2^{128}}{2 \times 10^{12} \times 60 \times 60 \times 24 \times 365} \sim 5395141535403007426\ years$$

- Age of the universe ~ 13.7 billion years ($\sim$ *half a billion times* greater than *the age of the universe*).

(AES-128 can be considered secure)

EU announced the funding of the Jupiter supercomputer, capable of executing one exaflop (10^{18} calculations per second), Science Business, 23 Jan 2024.
It is reported that the US has already three exaflop supercomputers (El Capitan, Frontier, and Aurora).

Exhaustive Search (Quantum))(AES-128)

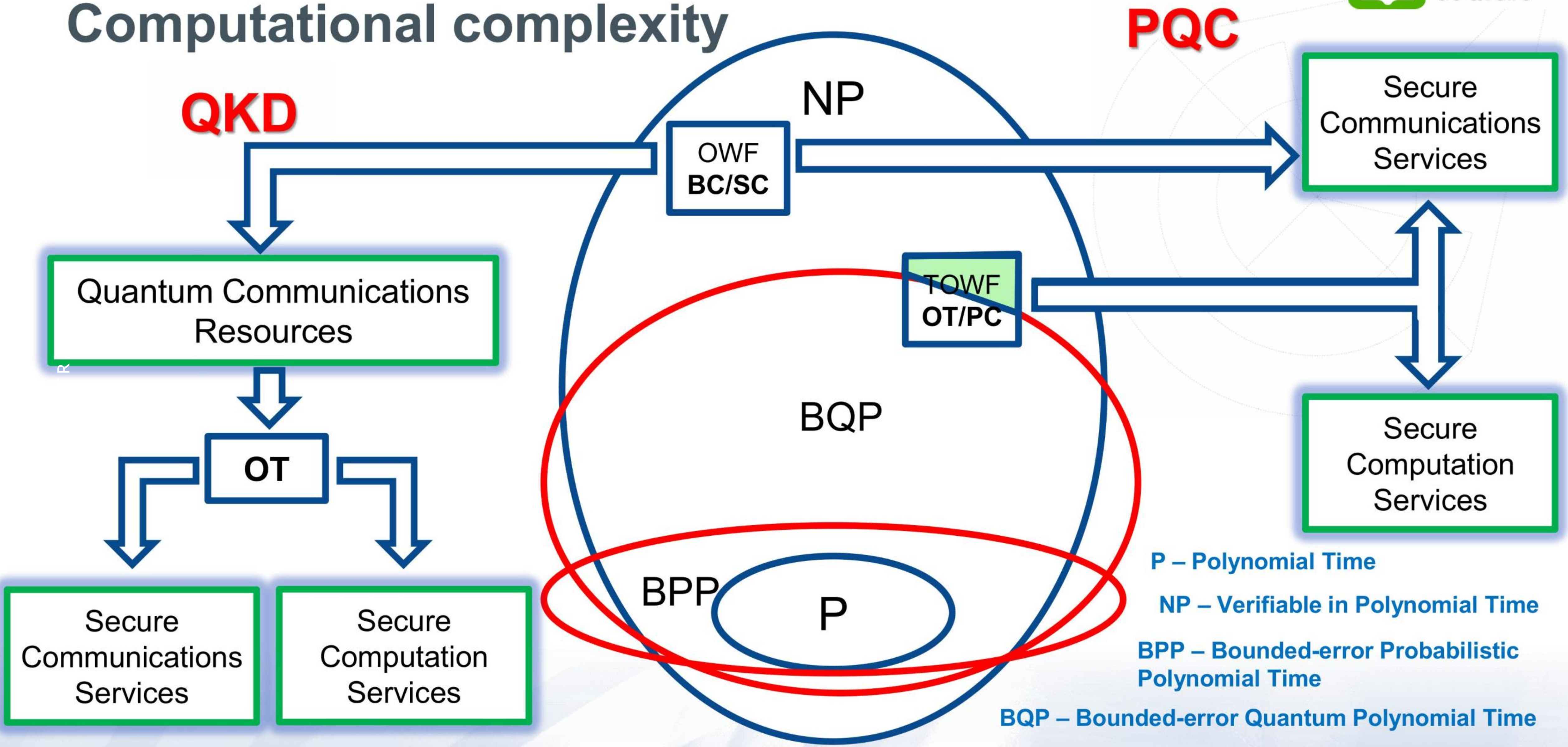
$$\frac{2^{64}}{2 \times 10^{12} \times 60 \times 60 \times 24 \times 365} \sim 3\ months$$

With a quantum computer running the Grover's algorithm AES-128 cannot be considered secure anymore

Doubling the key size makes AES secure against quantum exhaustive search

…for crypto, the bad news will come with the Shor Algorithm, and for RSA

Foundations of cryptography
Computational complexity



PQC

QKD

NP

OWF
BC/SC

Secure Communications Services

Quantum Communications Resources

TOWF
OT/PC

BQP

Secure Computation Services

OT

BPP

P

Secure Communications Services

Secure Computation Services

P – Polynomial Time

NP – Verifiable in Polynomial Time

BPP – Bounded-error Probabilistic Polynomial Time

BQP – Bounded-error Quantum Polynomial Time

BC - Bit-Commitment

OT – Oblivious Transfer

OWF – One-Way Function

TOWF – Trapdoor One-Way Function

SC - Symmetric Cryptography

PC – Public Cryptography

PQC…why?

1) It’s based on a more mature technology

2) It allows a smother transition

3) It is based on software (upgrade through new releases)

4) It is a certified technology

QKD…why?

1) Its security can be made independent of algorithms or computational power advances

2) It can provide very high entropy sources

3) It can avoid the use of public cryptography (perfect forward secrecy)

4) It allows the detection of an eavesdropper

5) It allows device-independent systems

My opinion…

PQC can offer a short/medium term solution, there will be scenarios where will be robust and fast enough, and others where QKD will be practical enough, and there will be even other scenarios where a mix of both approaches offers the best solution.

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 … ?

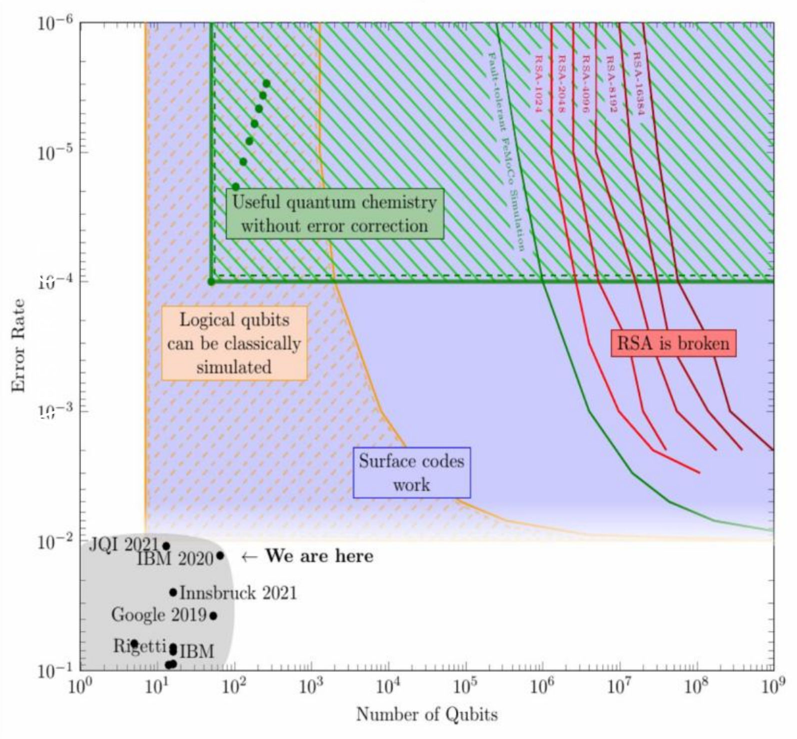
Need to start the switching in the year S = 2024 + Q – X - Y

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 !!!

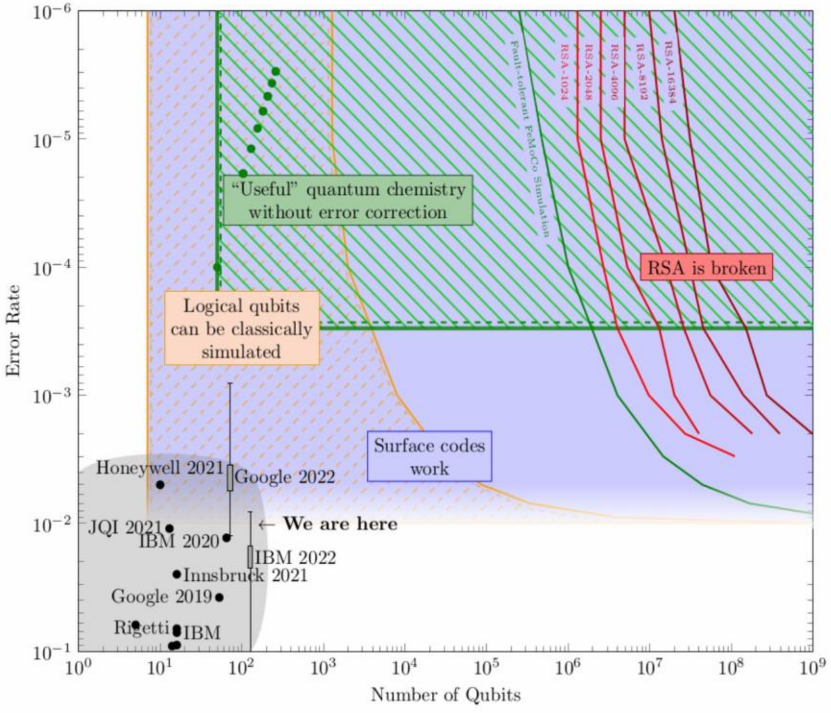
Mosca, Michele, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, September/October 2018, doi: 10.1109/MSP.2018.3761723.

Quantum Computers – Progresses

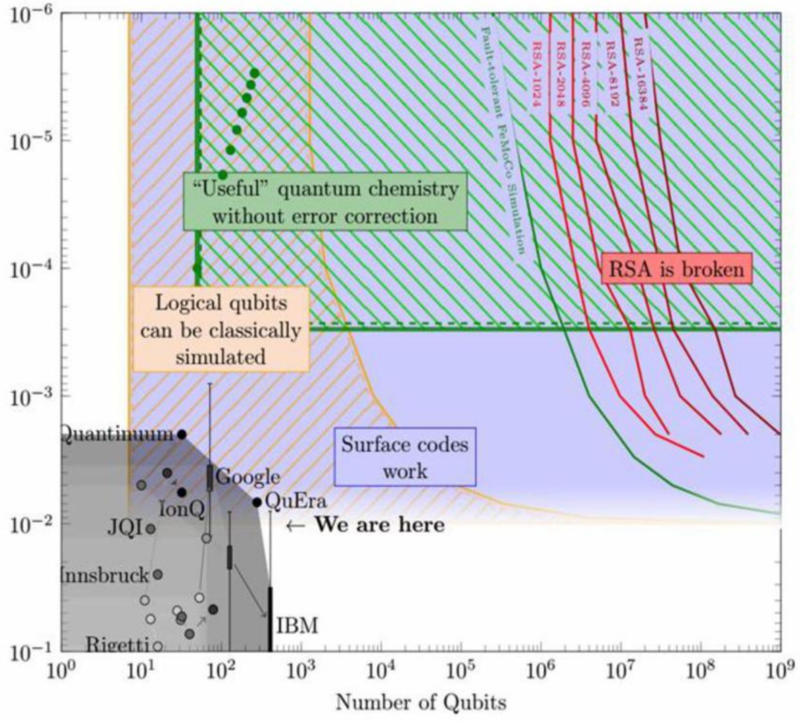
2021



2022



2023



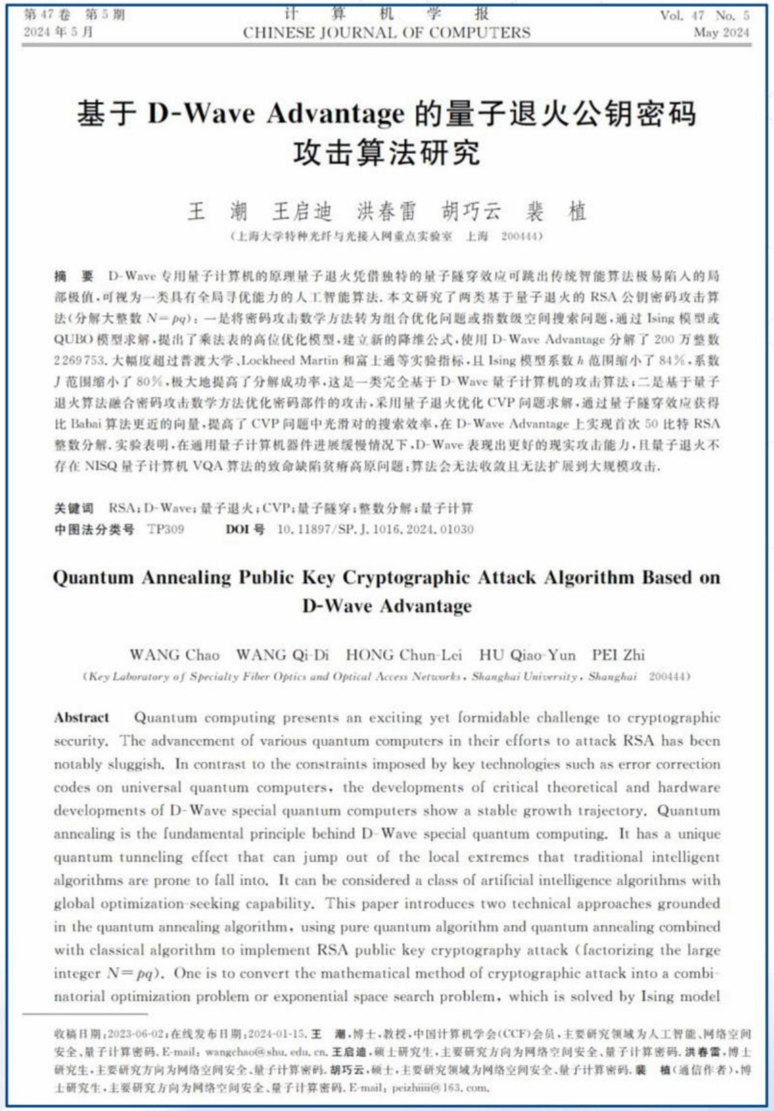
https://sam-jaques.appspot.com/quantum_landscape

Chinese Scientists Broken the RSA, but…

- Researchers at China's Shanghai University using D-Wave's Advantage successfully factor a 50-bit integer.

- They explore specialized quantum techniques rather than full-fledged universal quantum computers.

…standard RSA uses 2048 bits…



第 47 卷 第 5 期
2024 年 5 月

计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS

Vol. 47 No. 5
May 2024

基于 D-Wave Advantage 的量子退火公钥密码攻击算法研究

王 潮 王启迪 洪春雷 胡巧云 裴 植

（上海大学特种光纤与光接入网重点实验室 上海 200444）

摘 要 D-Wave 专用量子计算机的原理量子退火凭借独特的量子隧穿效应可跳出传统智能算法极易陷入的局部极值，可视为一类具有全局寻优能力的人工智能算法. 本文研究了两类基于量子退火的 RSA 公钥密码攻击算法（分解大整数 $N=pq$）：一是将密码攻击数学方法转为组合优化问题或指数级空间搜索问题，通过 Ising 模型或 QUBO 模型求解，提出了乘法表的高位优化模型，建立新的降维公式，使用 D-Wave Advantage 分解了 200 万整数 2269753. 大幅度超过普渡大学、Lockheed Martin 和富士通等实验指标，且 Ising 模型系数 h 范围缩小了 84%，系数 J 范围缩小了 80%，极大地提高了分解成功率，这是一类完全基于 D-Wave 量子计算机的攻击算法；二是基于量子退火算法融合密码攻击数学方法优化密码部件的攻击，采用量子退火优化 CVP 问题求解，通过量子隧穿效应获得比 Babai 算法更近的向量，提高了 CVP 问题中光滑对的搜索效率，在 D-Wave Advantage 上实现首次 50 比特 RSA 整数分解. 实验表明，在通用量子计算机器件进展缓慢情况下，D-Wave 表现出更好的现实攻击能力，且量子退火不存在 NISQ 量子计算机 VQA 算法的致命缺陷贫瘠高原问题：算法会无法收敛且无法扩展到大规模攻击.

关键词 RSA；D-Wave；量子退火；CVP；量子隧穿；整数分解；量子计算
中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.01030

Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage

WANG Chao WANG Qi-Di HONG Chun-Lei HU Qiao-Yun PEI Zhi

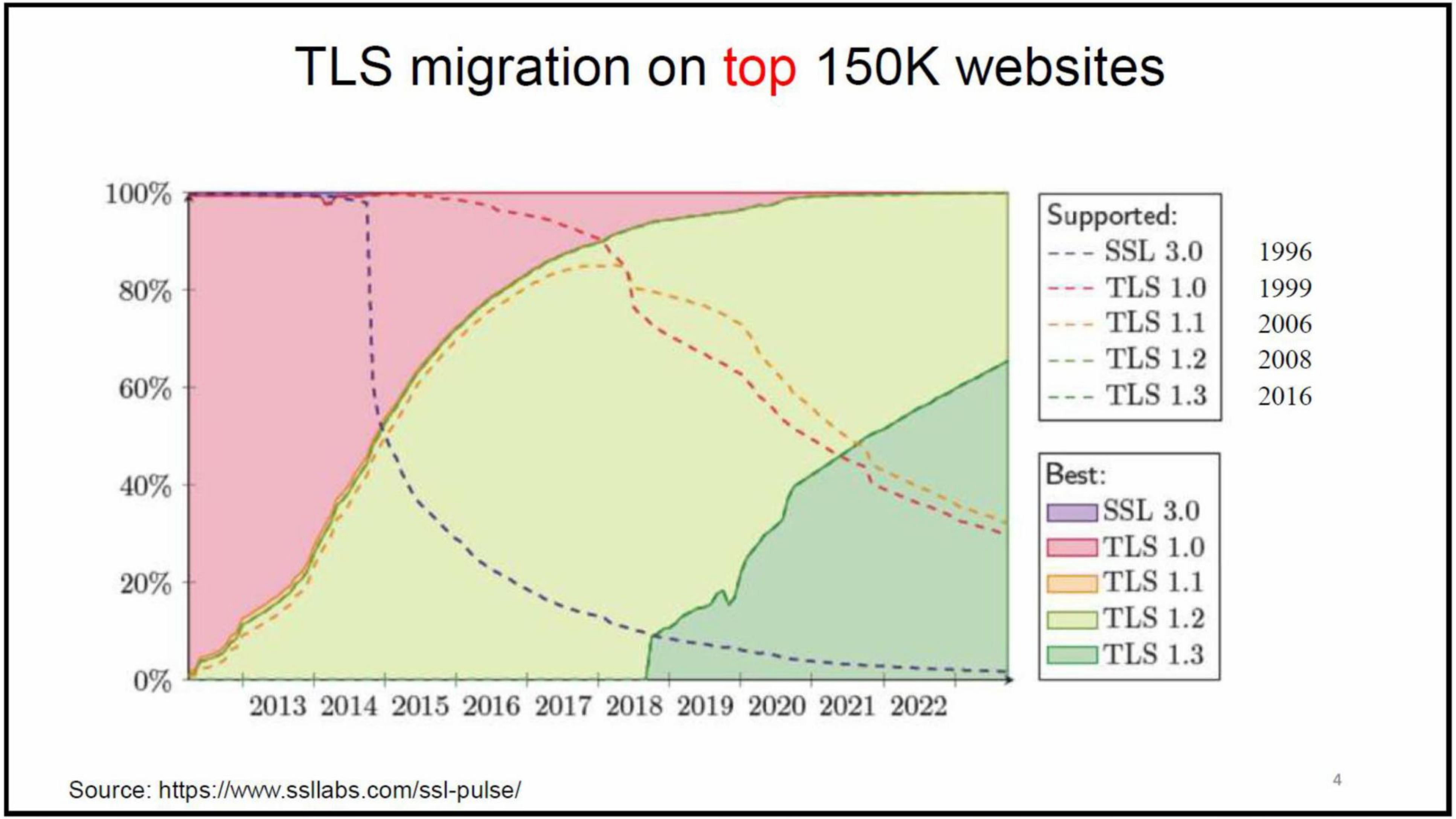
(Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444)

Abstract Quantum computing presents an exciting yet formidable challenge to cryptographic security. The advancement of various quantum computers in their efforts to attack RSA has been notably sluggish. In contrast to the constraints imposed by key technologies such as error correction codes on universal quantum computers, the developments of critical theoretical and hardware developments of D-Wave special quantum computers show a stable growth trajectory. Quantum annealing is the fundamental principle behind D-Wave special quantum computing. It has a unique quantum tunneling effect that can jump out of the local extremes that traditional intelligent algorithms are prone to fall into. It can be considered a class of artificial intelligence algorithms with global optimization-seeking capability. This paper introduces two technical approaches grounded in the quantum annealing algorithm, using pure quantum algorithm and quantum annealing combined with classical algorithm to implement RSA public key cryptography attack (factorizing the large integer $N=pq$). One is to convert the mathematical method of cryptographic attack into a combinatorial optimization problem or exponential space search problem, which is solved by Ising model

收稿日期：2023-06-02；在线发布日期：2024-01-15. **王 潮**，博士，教授，中国计算机学会（CCF）会员，主要研究领域为人工智能、网络空间安全、量子计算密码. E-mail：wangchao@shu.edu.cn. **王启迪**，硕士研究生，主要研究方向为网络空间安全、量子计算密码. **洪春雷**，博士研究生，主要研究方向为网络空间安全、量子计算密码. **胡巧云**，硕士，主要研究领域为网络空间安全、量子计算密码. **裴 植**（通信作者），博士研究生，主要研究方向为网络空间安全、量子计算密码. E-mail：peizhiiii@163.com.

May 2024

When to Switch to Quantum Secure?



TLS migration on top 150K websites

Source: https://www.ssllabs.com/ssl-pulse/

4

When to Switch to Quantum Secure?

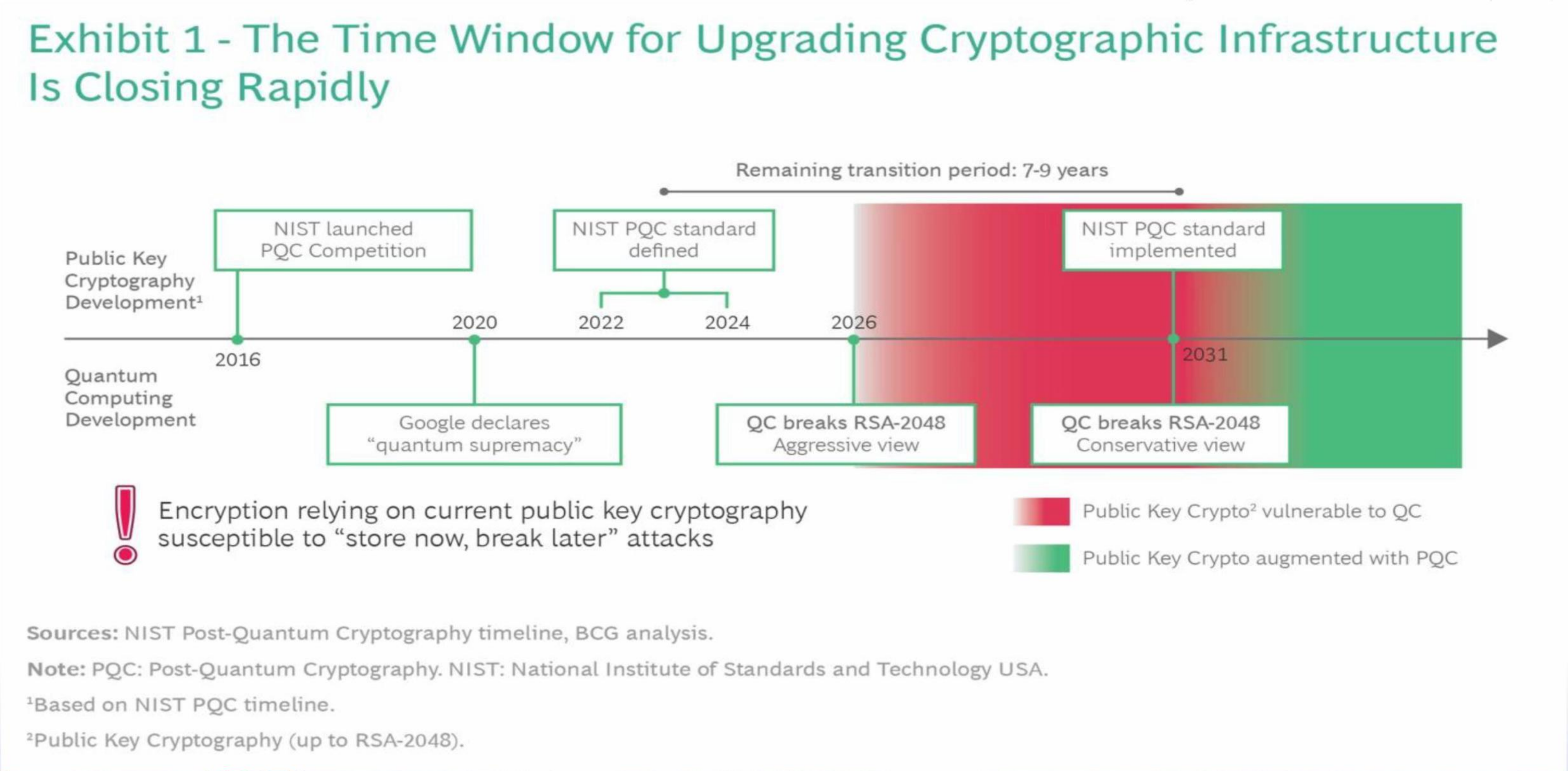


Exhibit 1 - The Time Window for Upgrading Cryptographic Infrastructure Is Closing Rapidly

Remaining transition period: 7-9 years
Public Key Cryptography Development[1]
NIST launched PQC Competition
NIST PQC standard defined
NIST PQC standard implemented
2016
2020
2022
2024
2026
2031
Quantum Computing Development
Google declares "quantum supremacy"
QC breaks RSA-2048 Aggressive view
QC breaks RSA-2048 Conservative view

! Encryption relying on current public key cryptography susceptible to "store now, break later" attacks

🟥 Public Key Crypto[2] vulnerable to QC

🟩 Public Key Crypto augmented with PQC

Sources: NIST Post-Quantum Cryptography timeline, BCG analysis.

Note: PQC: Post-Quantum Cryptography. NIST: National Institute of Standards and Technology USA.

[1] Based on NIST PQC timeline.

[2] Public Key Cryptography (up to RSA-2048).

L. Comandar, J. Bobier, M. Coden, S, Deutscher, Ensuring Online Security in a Quantum Future, Boston Consulting Group, 2021

My opinion…

Starting today is already late…

Paulo Antunes, Paulo S. B. Andr , Armando N. Pinto, Simplified Model for a Single-Photon Detector Module, SEON'06, IV Symposium on Enabling Optical Networks and Sensors, Porto, Portugal, pp. 87-88, June 16, 2006;

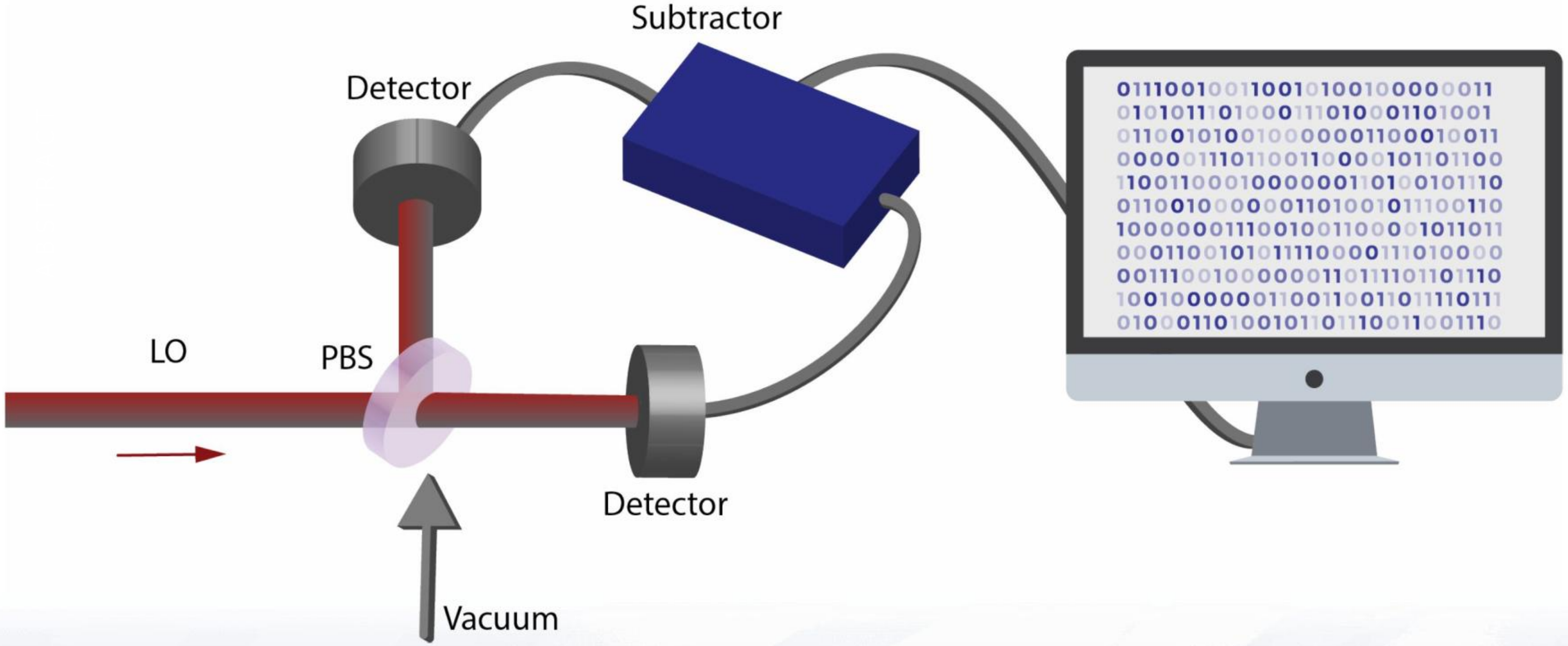
Armando N. Pinto, Govind P. Agrawal, Loss of Quantum Information Due to the Kerr Effect in Optical Fibers, ICQI 2007, The International Conference on Quantum Information, Paper IFG4, Rochester, New York, USA, June 13-15, 2007;

Armando N. Pinto, Nuno A. Silva, Quantum Optical Communication Systems, SEON'08, VI Symposium on Enabling Optical Networks and Sensors, Porto, Portugal, pp. 111-114, June 20, 2008;

What are the systems that we are developing?

QRNG Based on Vacuum Fluctuations

We generate random noise and from its measurement we generate random numbers



True Random Numbers
Random Prime Numbers

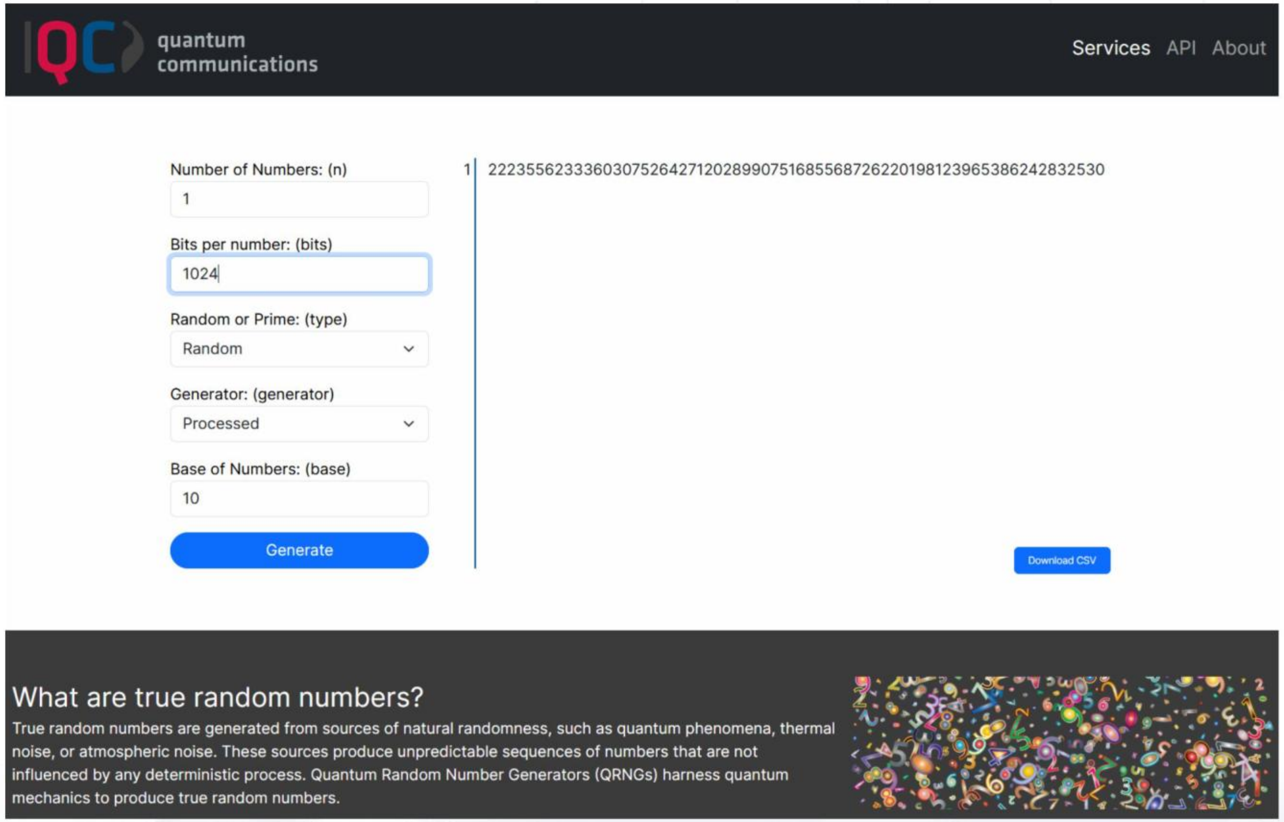
QRNG Based on Vacuum Fluctuations

All NIST SP 800-22 tests PASSED

https://qrng.av.it.pt

Random Number

Prime Number



Number of Numbers: (n)
1

Bits per number: (bits)
1024

Random or Prime: (type)
Random

Generator: (generator)
Processed

Base of Numbers: (base)
10

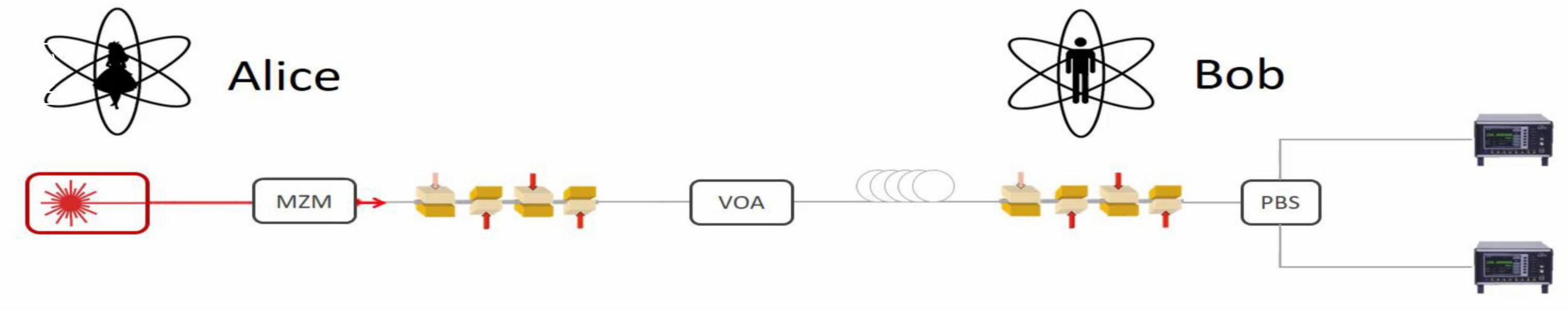
```
1 | 222355623336030752642712028990751685568726220198123965386242832530
```

What are true random numbers?

True random numbers are generated from sources of natural randomness, such as quantum phenomena, thermal noise, or atmospheric noise. These sources produce unpredictable sequences of numbers that are not influenced by any deterministic process. Quantum Random Number Generators (QRNGs) harness quantum mechanics to produce true random numbers.

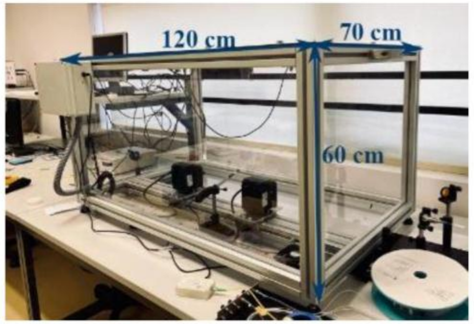
Quantum Keys Distribution

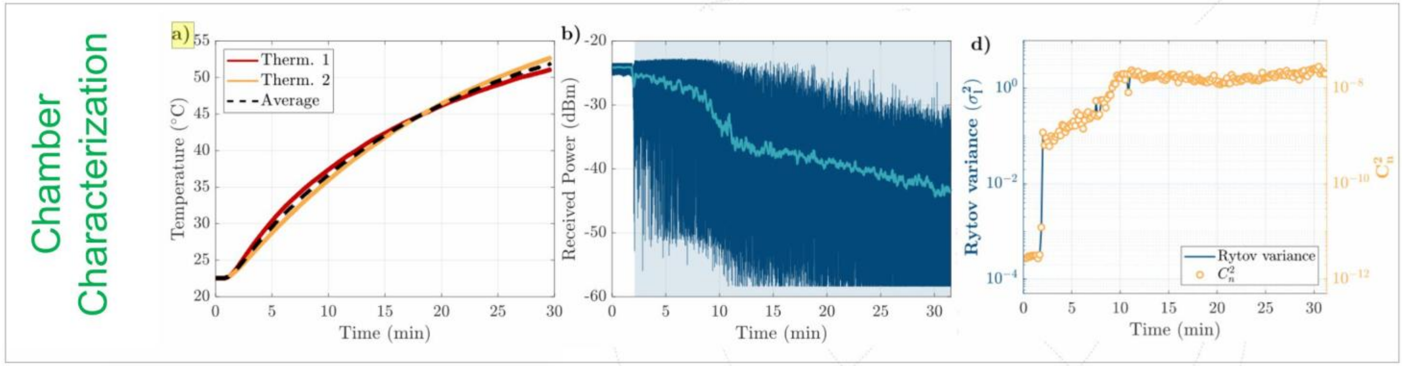
We encode information in the polarization of single photons pulses and we pos–process the measurements results

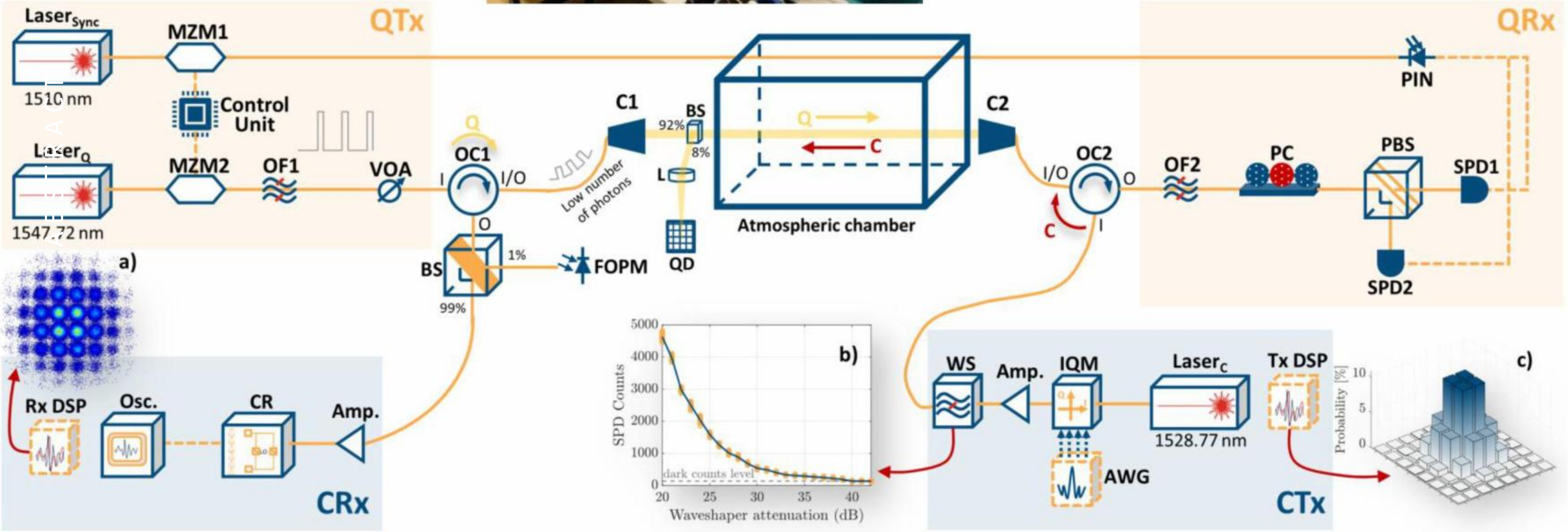


Discrete Variable Systems

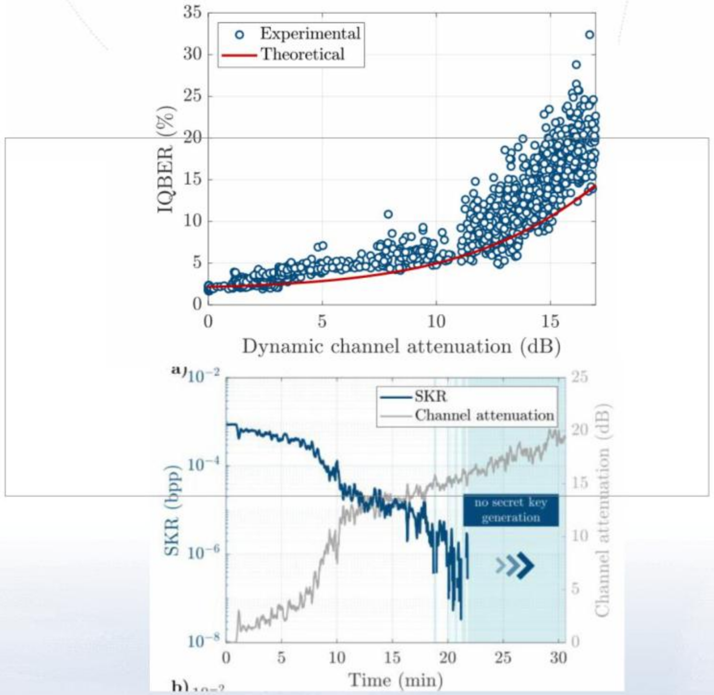
Coexistence of Quantum and Classical Signal Transmission Over Turbulent FSO Channels







Quantum signal performance

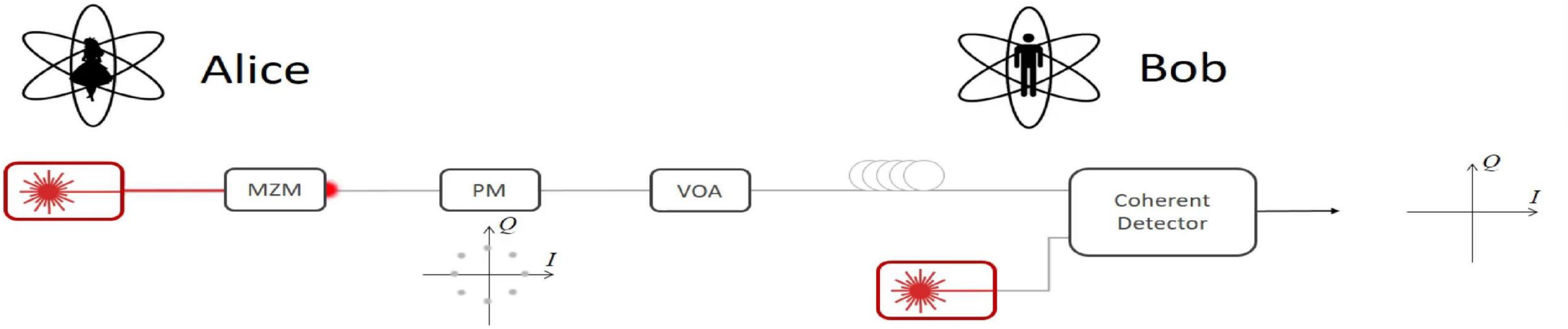


Fiber-wireless optical system that transmitted a 64-QAM 400 Gbps classical signal for high-rate data exchange and a 1 MHz quantum signal for QKD.

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 Keys Distribution

We encode information in the phase of quasi-single photon pulses, and we perform reverse reconciliation



Continuous Variable Systems

CV-QKD System

The key information (QRNG) is mapped in the phase and amplitude of a continuous wave laser source attenuated to the quantum level.

- **Physical Layer**

Implements **CV-QKD** protocol

Reduced number of photons/symbol

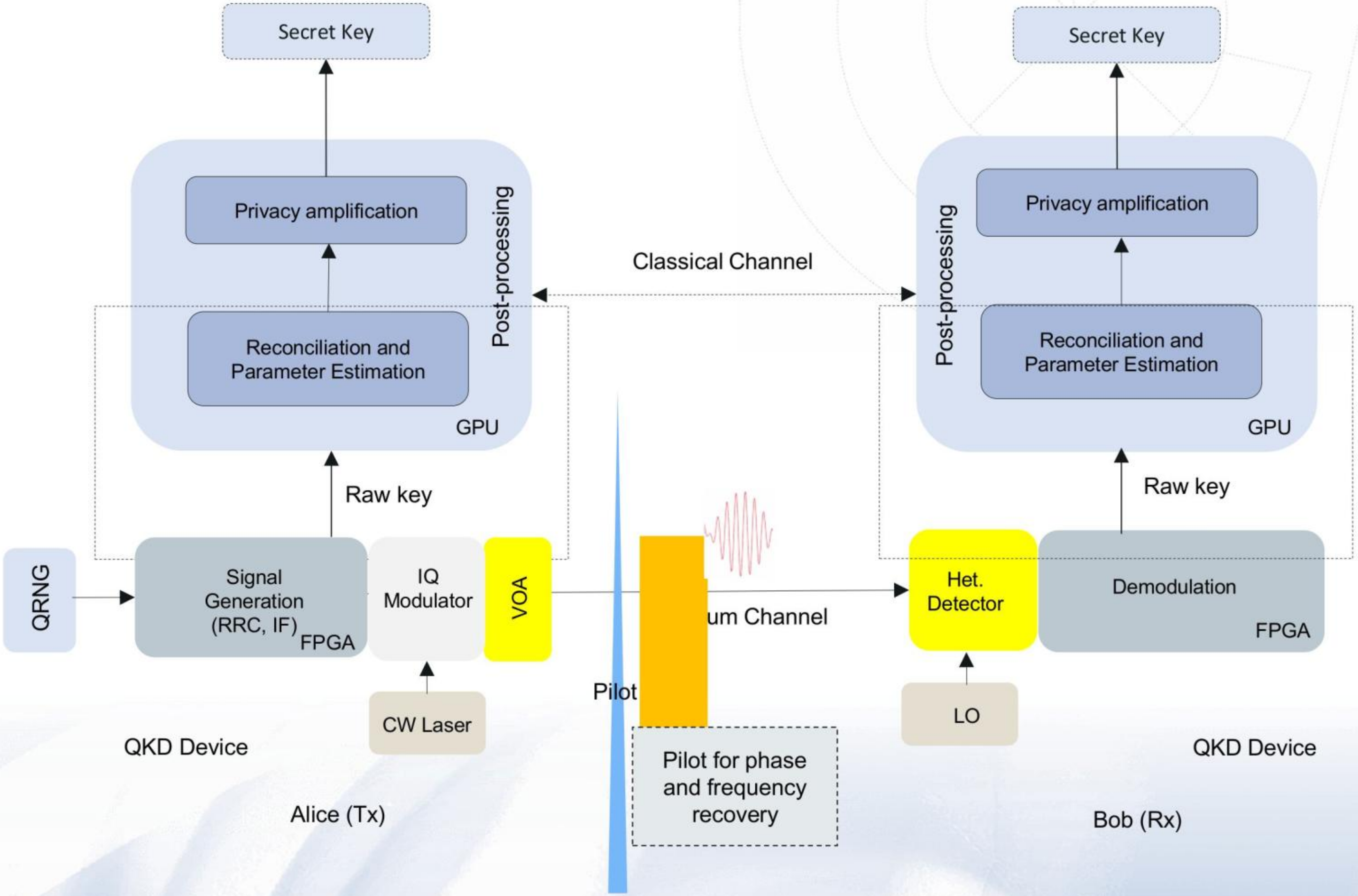
Raw key with **~40% of BER**

DSP runs in **FPGA** and **GPU**

- **Post-processing Layer**

GPU parallelization for fast computing

LDPC error correction enables correcting high BER values



What are the projects that we are working on?

universidade de aveiro

QuantumPrime

https://quantumprime.av.it.pt

DISCRETION

https://discretion-eu.com

PTQCI

https://ptqci.av.it.pt/

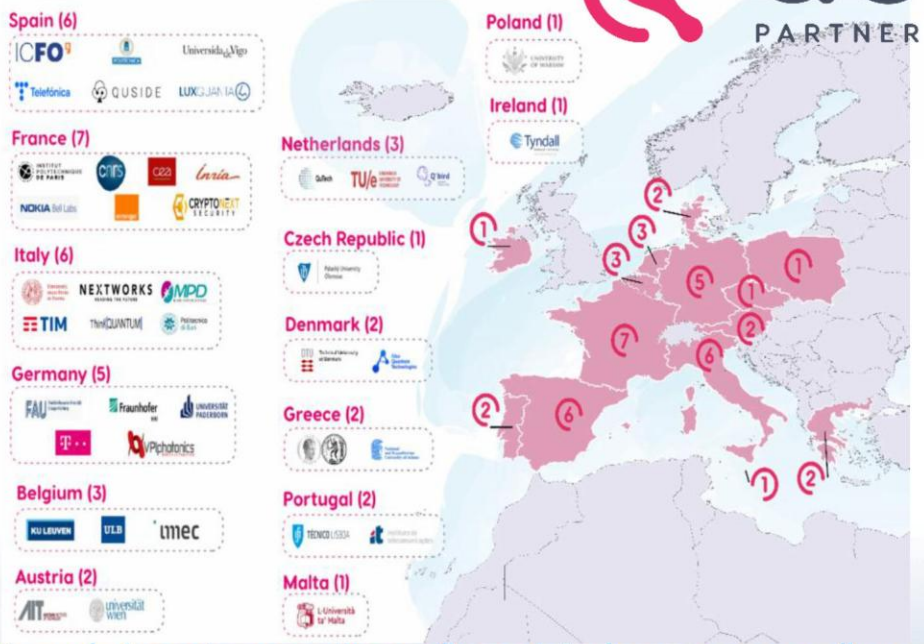
QSN PARTNERSHIP

QSCAN - Quantum Space Surveillance

QuantaGENOMICS Consortium

SU & INRIA
UPM & ICFO
IT & Ophiomics
instituto de telecomunicações
POLITÉCNICA
SORBONNE UNIVERSITÉ
ophiomics
ICFO
The Institute of Photonic Sciences
Inria

https://quantagenomics.av.it.pt



https://qt.eu/about-quantum-flagship/newsroom/launch-of-quantum-secure-networks-partnership-qsnp/

instituto de telecomunicações

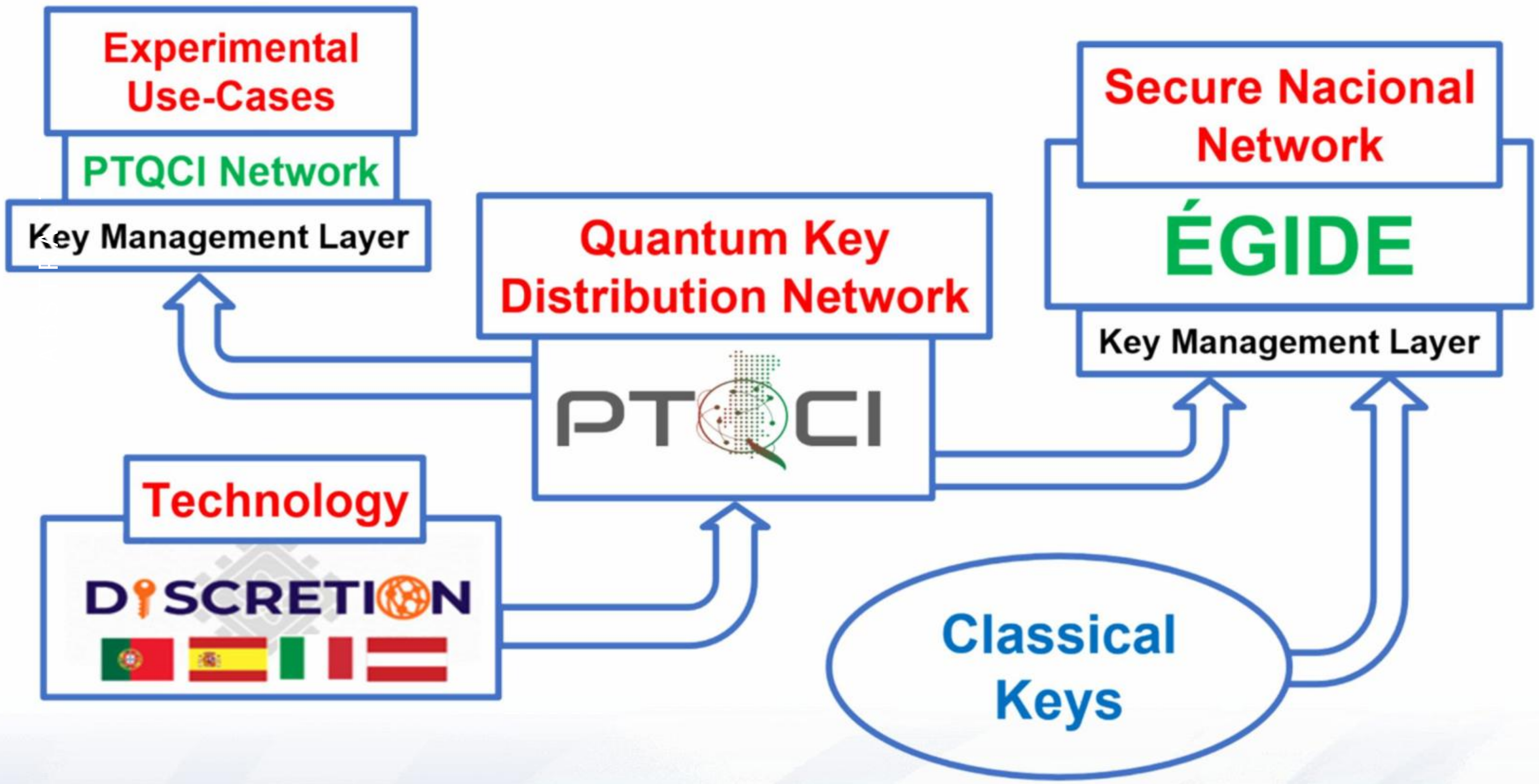
IQC quantum communications

PORTUGUESE QUANTUM COMMUNICATION INFRASTRUCTURE

SEED OF 1ST SEGMENT OF EUROQCI IN PORTUGAL

universidade de aveiro

deimos · it · altice labs · adyta · IP Telecom · GNS Gabinete Nacional de Segurança PORTUGAL · ISEL · warpcom · omnidea · FCT Fundação para a Ciência e a Tecnologia · IPQ · TÉCNICO LISBOA



Experimental Use-Cases

PTQCI Network

Key Management Layer

Quantum Key Distribution Network

PTQCI

Technology

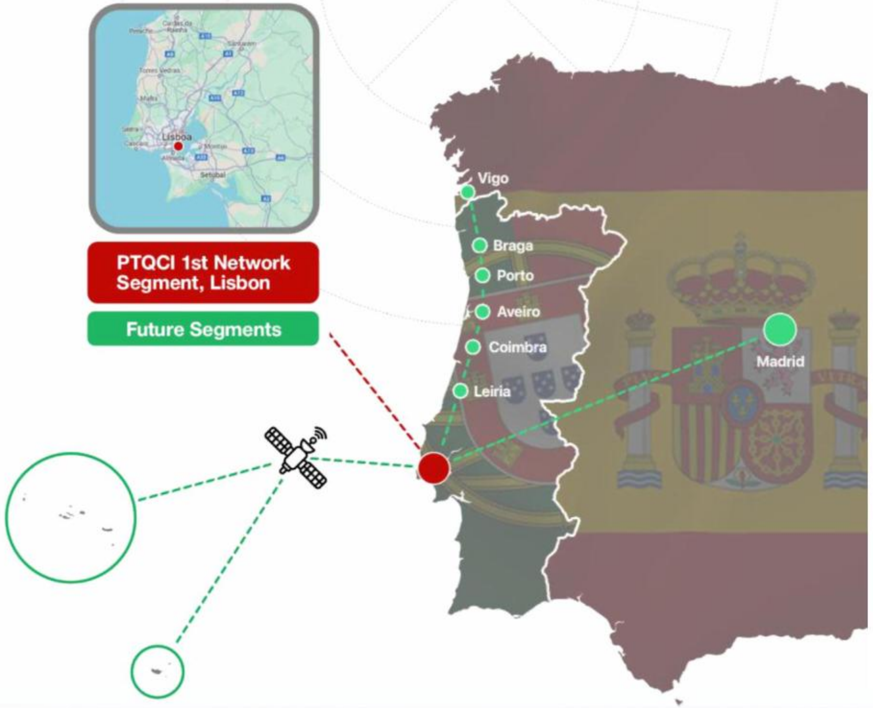
DISCRETION

Secure Nacional Network

ÉGIDE

Key Management Layer

Classical Keys



instituto de telecomunicações

IQC quantum communications

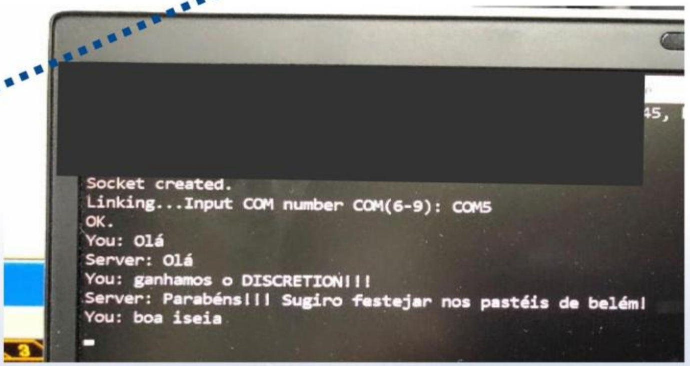
Co-funded by the European Union

QSCRIPT

PAVING THE WAY WITH PORTUGUESE TECHNOLOGY

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

GNS
Gabinete Nacional de Segurança
4003
Com a colaboração de:
TÉCNICO LISBOA
inescid lisboa
it Instituto de Telecomunicações



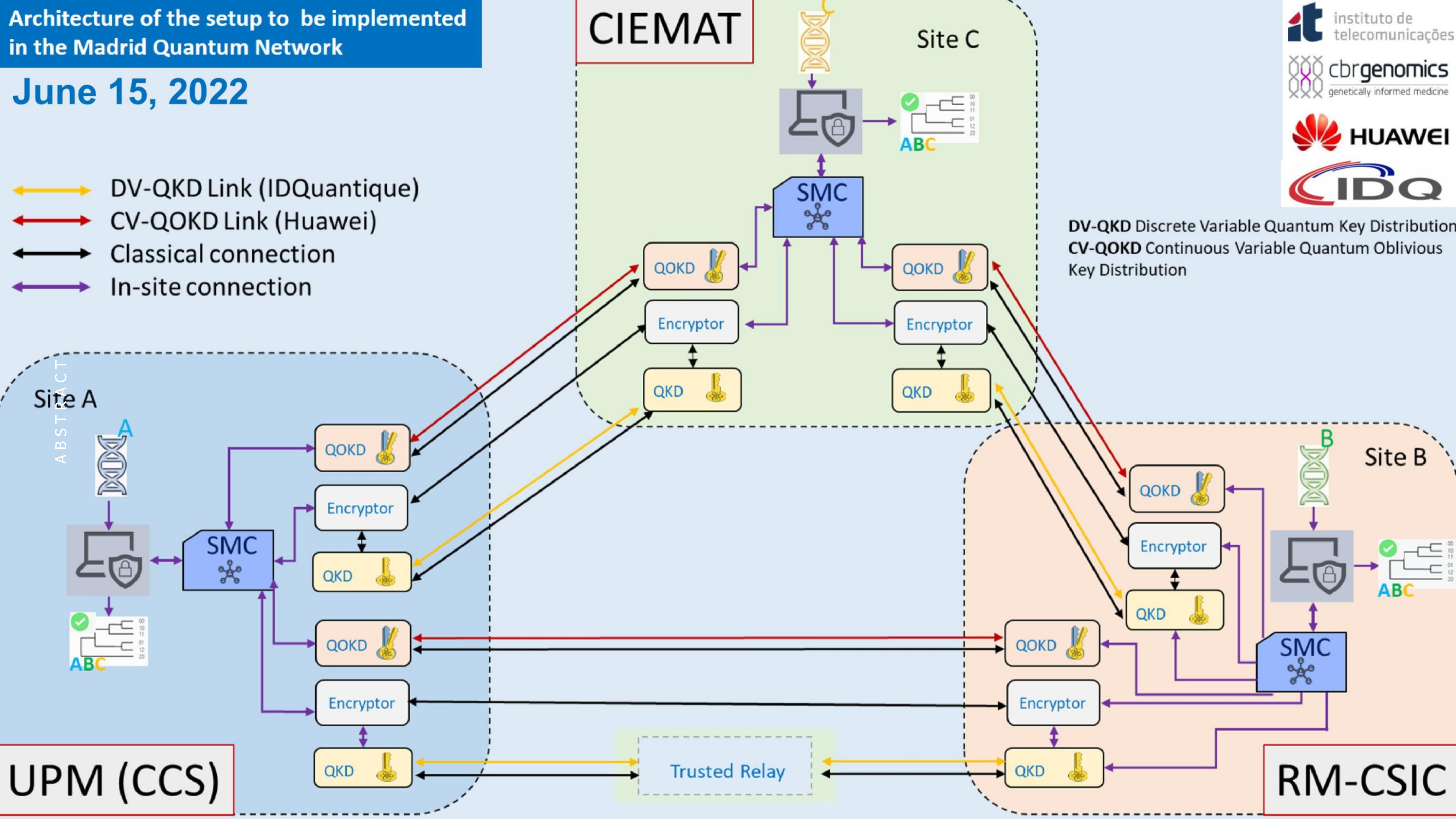
```
[redacted]
Socket created.
Linking...Input COM number COM(6-9): COM5
OK.
You: Olá
Server: Olá
You: ganhamos o DISCRETION!!!
Server: Parabéns!!! Sugiro festejar nos pastéis de belém!
You: boa iseia
```

June 30, 2021

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

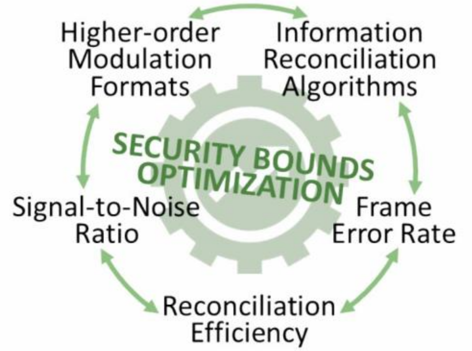
June 15, 2022

- ⟷ DV-QKD Link (IDQuantique)
- ⟷ CV-QOKD Link (Huawei)
- ⟷ Classical connection
- ⟷ In-site connection



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



Higher-order Modulation Formats

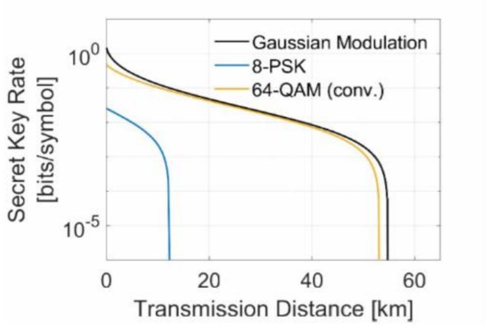
Information Reconciliation Algorithms

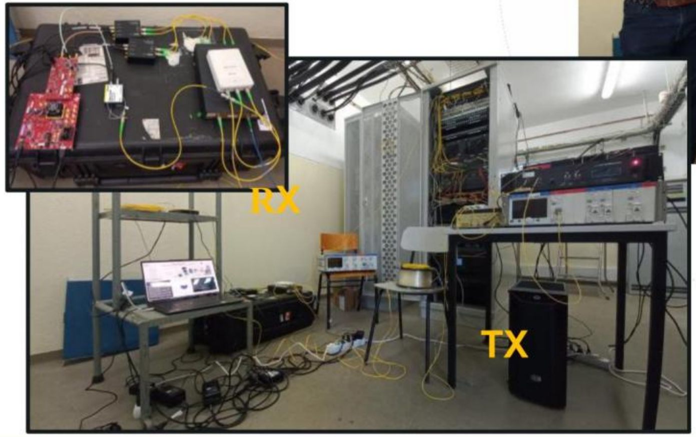
SECURITY BOUNDS OPTIMIZATION

Signal-to-Noise Ratio

Frame Error Rate

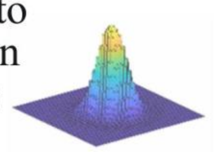
Reconciliation Efficiency





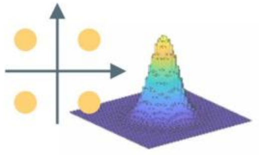
Gaussian modulation

Difficult to achieve in practice



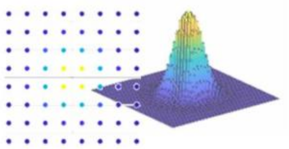
Discrete modulation

Simpler implementation



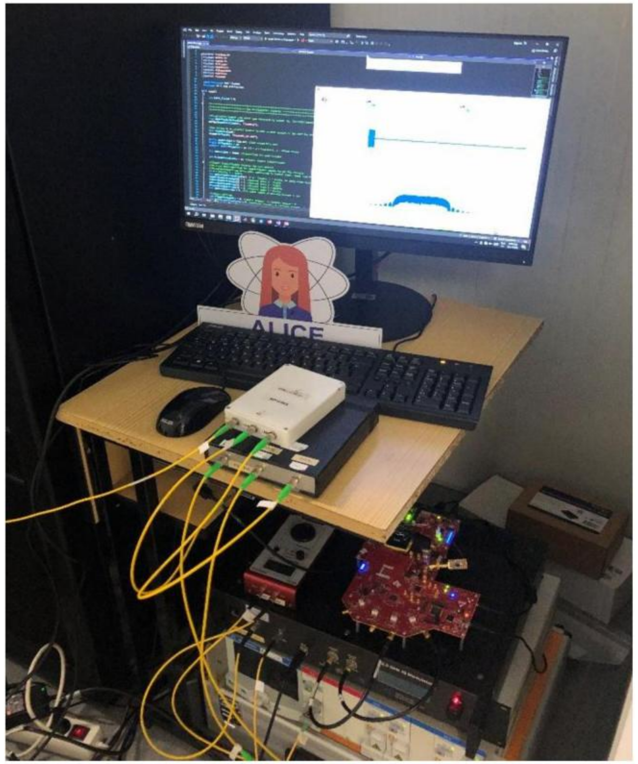
High-order cardinality

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

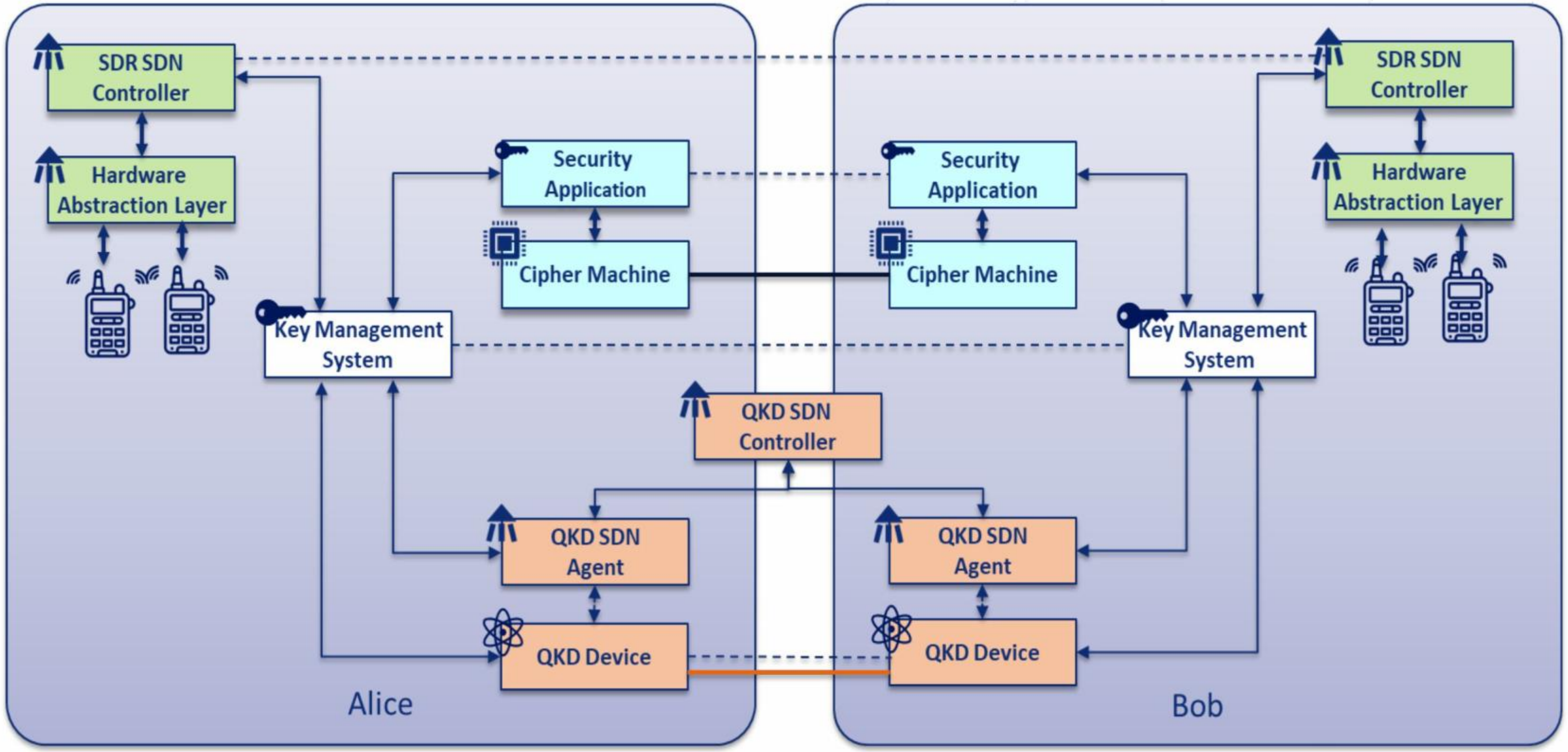


Exchange of confidential information between a command center and a docked navy frigate.

Operational Experimentation Center in Troia, Portugal

September 21, 2023

The DISCRETION system was demonstrated in an operational scenario for the first time at the REPMUS exercise in Troia and Sesimbra, Portugal



🟧 QKD SDN – Quantum Key Distribution Network □ Key Management System 🟦 Cipher Machine Use Case 🟩 SDR SDN Use Case

The system integrates a Continuous-Variable Quantum Key Distribution, a Software-Defined Network Control Plane, a Key Management System, a Cipher Machine Secure Link, and a Software-Defined Secure Radios.

September 17, 2024

Co-funded by the European Union

DISCRETION project has received funding from the European Defence Industrial Development Programme (EDIDP) under grant agreement No SI2.858093

Supported also by:

GUSTAVO
ANJOS

ABSTRACT

Gustavo Anjos received his Master's and PhD degrees in Electrical Engineering from the University of Aveiro in 2013 and 2022, respectively. He has been developing research work at the Institute of Telecommunications in Aveiro, participating in multiple projects such as FLEXICELL, SWING2 and DISCRETION.

He currently works as a researcher at the Institute of Telecommunications at the University of Aveiro, developing work in the quantum communications group.

In parallel, he collaborates with the Department of Electronics, Telecommunications and Informatics by teaching courses in electrical engineering.

His current research interests include physical layer security for wireless communications, and quantum key distribution systems. In the latter case, the focus of his work is on the implementation of these types of protocols on dedicated hardware platforms with a view to the efficient computation of the associated algorithms.

ABSTRACT

CONTINUOUS VARIABLE QKD SYSTEM

Quantum Key Distribution (QKD) is one of the most mature and promising applications of quantum information science, enabling information-theoretic secure communication through the laws of quantum physics. This presentation focuses on Continuous Variable Quantum Key Distribution (CV-QKD), a class of QKD protocols that leverage the phase and amplitude quadratures of coherent light to encode quantum information, offering practical advantages in integration with existing telecommunications infrastructure.

Unlike discrete-variable QKD systems that rely on single-photon sources and detectors, CV-QKD uses standard coherent detection techniques with homodyne or heterodyne detection, enabling higher key generation rates, easier integration into classical optical networks, and compatibility with standard telecom components such as IQ modulators and CW lasers. The protocol maps quantum random numbers (QRNG) onto modulated coherent states and transmits them over a quantum channel. At the receiver side, Bob measures these quadratures and estimates channel parameters to assess potential eavesdropping through excess noise. Security is ensured through post-processing procedures including parameter estimation, error reconciliation using LDPC codes, and privacy amplification, typically executed via parallelized algorithms on GPUs and FPGAs.

The system implemented and demonstrated in this work dedicates approximately one-third of its operation time to key generation, with the remaining two-thirds allocated to essential calibration phases—specifically, shot and thermal noise estimation. This calibration is critical to accurately quantify trusted noise and to detect possible eavesdropping. The post-processing chain is highly demanding computationally, due to the need to correct high bit-error rates (BER ~40%) and to ensure that secret key rates remain viable under noisy and lossy channel conditions.

An innovative feature discussed is the integration of CV-QKD devices into Software Defined Networking (SDN) environments, following the ETSI-defined SD-QKD node model. By embedding SDN agents in QKD nodes and coordinating them through a centralized SDN controller and Key Management Systems (KMS), the system enables flexible, scalable, and programmable quantum-secured networks. This architecture supports dynamic key routing, automated node configuration, and application-layer key distribution—all critical features for future quantum communication infrastructures.

INSTITUIÇÕES ASSOCIADAS

Continuous Variable QKD System

Gustavo Miranda Castilho dos Anjos
PhD Researcher

PTQCI
7 Mar 2025

OUTLINE

❑ FOUNDATIONS

❑ CV-QKD PROTOCOL

❑ SD-QKD NETWORK

❑ CHALLENGES

❑ OPPORTUNITIES

FOUNDATIONS

Quantum Physics

Every measure perturbs the system

No perturbation, no measure, no eavesdropper

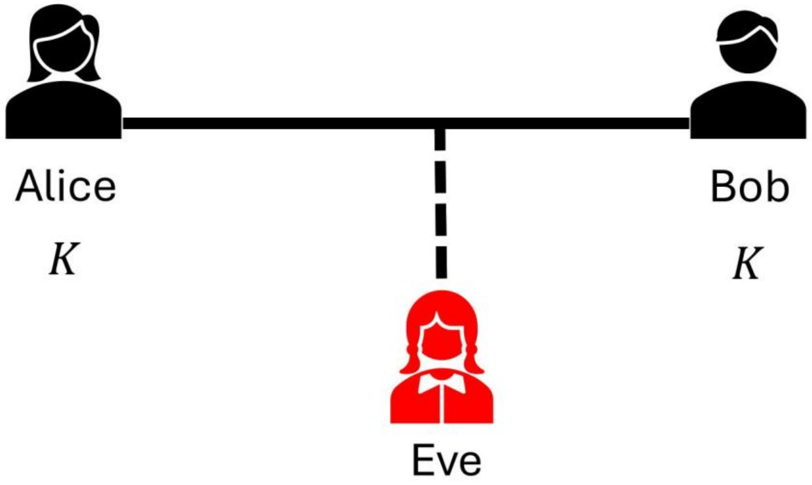
Secret key

Quantum systems can be used for **secret key distribution.**

QKD Protocol: Prepare and Measure

- ❑ Alice prepares and transmits the quantum key K;
- ❑ Bob measures the key and checks for Eve signatures;
- ❑ Key is dropped or reduced if Eve is present;

Eve cannot get the key without being detected



CV-QKD PROTOCOL

The key information (QRNG) is mapped in the phase and amplitude of a continuous wave laser source.

Post-processing Layer

GPU parallelization for fast computing

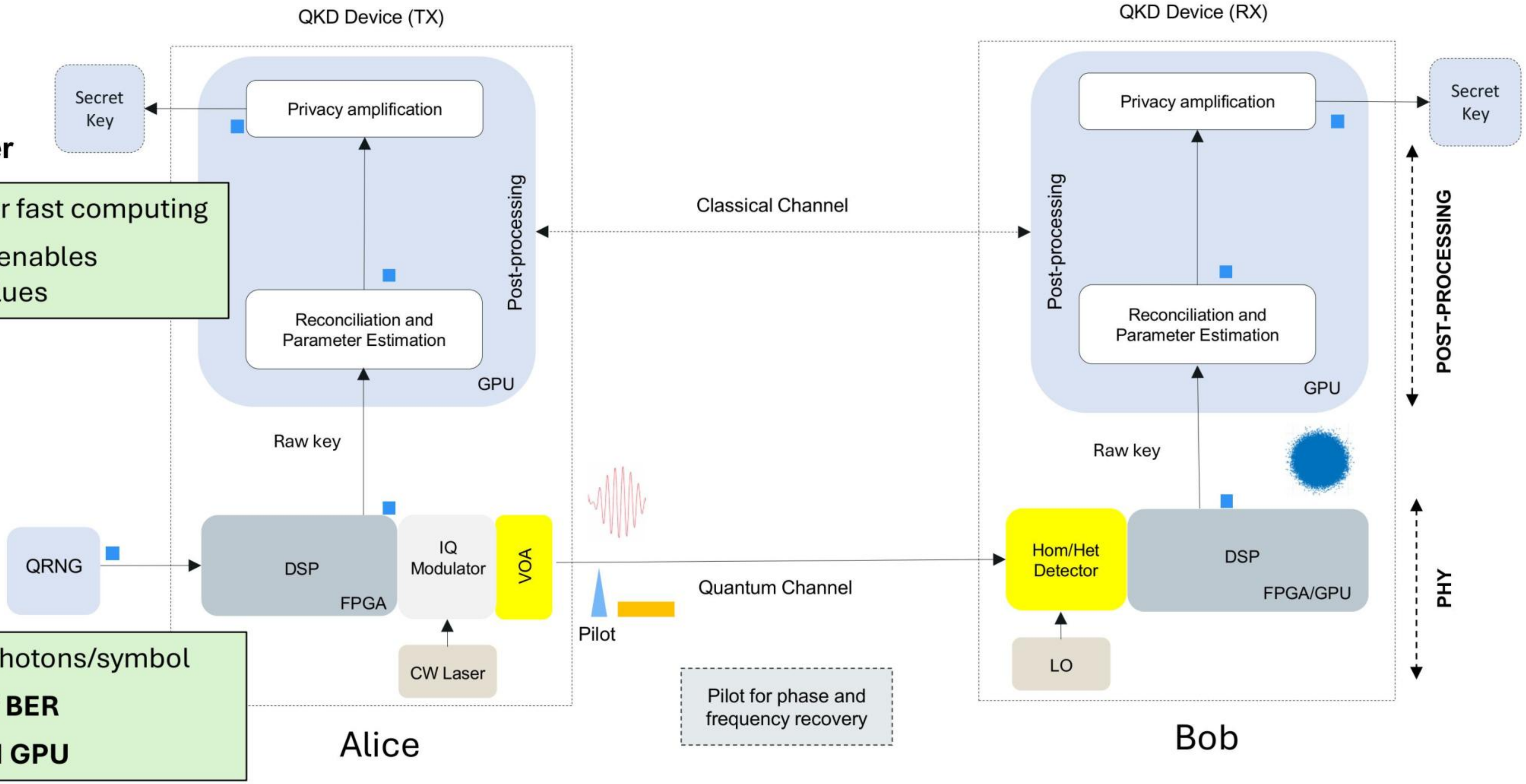
LDPC error correction enables correcting high BER values

Physical Layer

Reduced number of photons/symbol

Raw key with **~40% of BER**

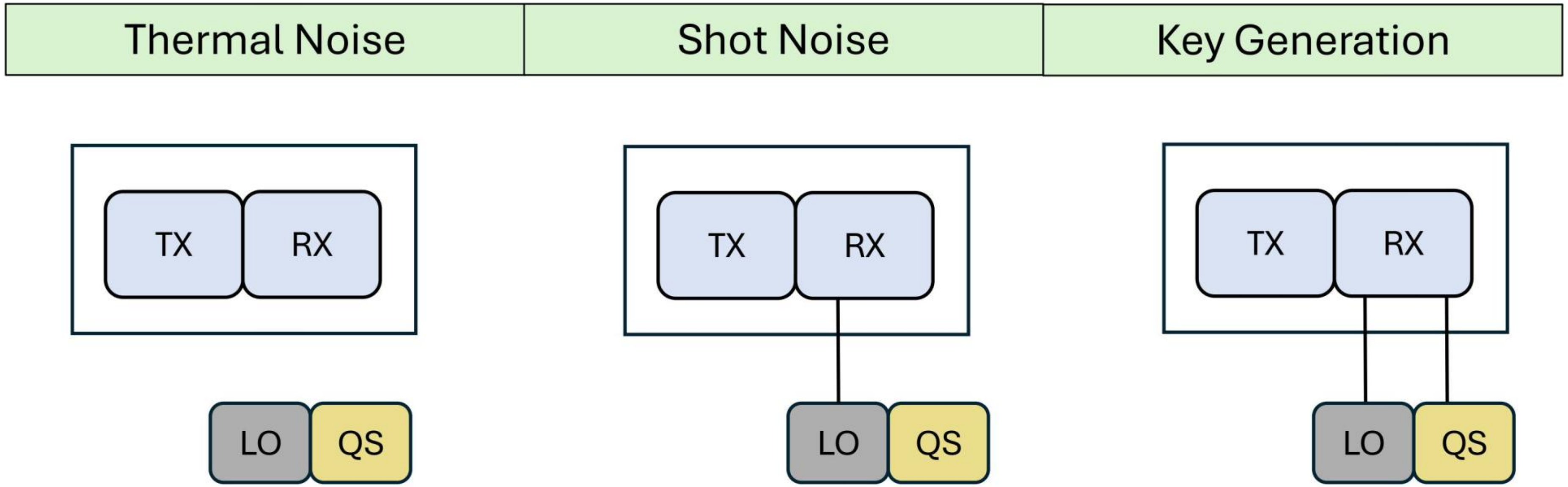
DSP runs in **FPGA** and **GPU**



CV-QKD PROTOCOL

Channel monitoring:

System generates keys 1/3 of the time, the other 2/3 for shot and thermal noise calibration.



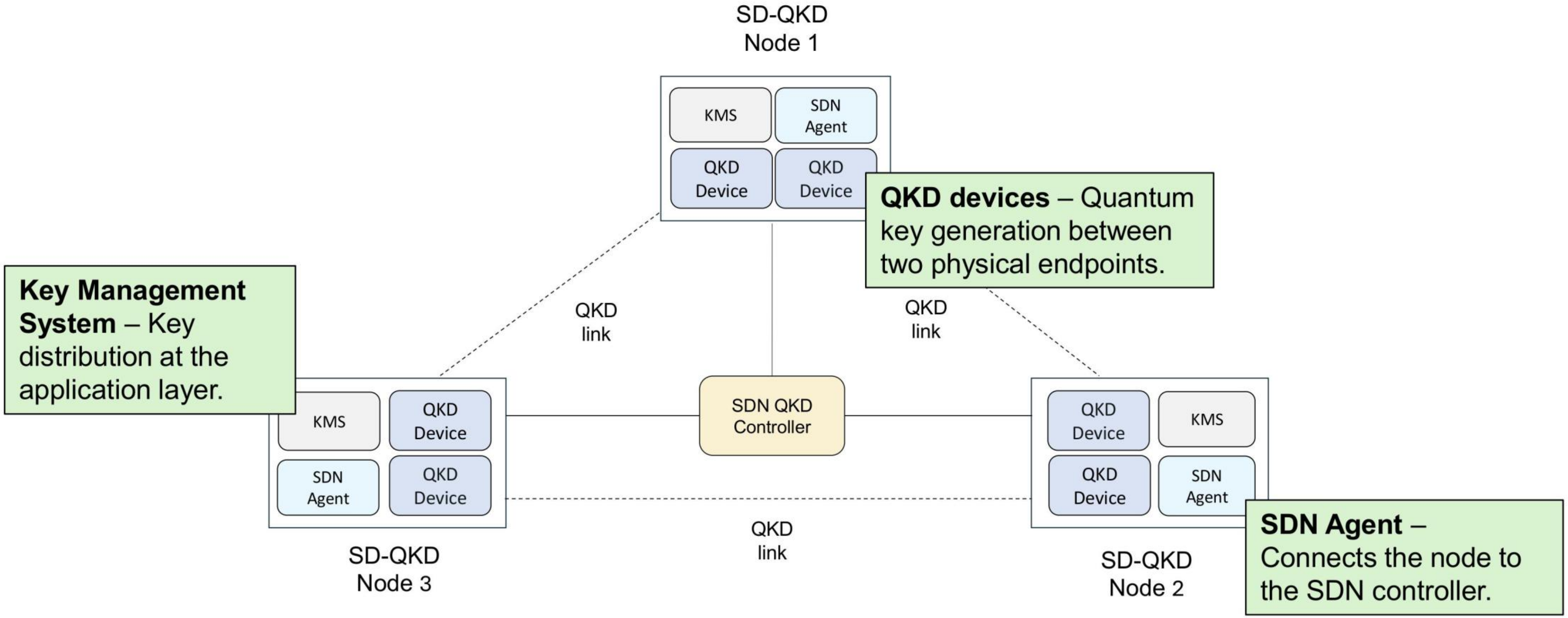
Calibration is essential to real-time quantification of trusted noise.

Eavesdropper signature in the form of excess noise.

SDN-QKD NETWORK

SDN enables centralized control, programming flexibility and scalability of QKD networks.

ETSI15 standard defines the concept of **Software Defined** (SD) – **QKD node**.



QKD devices – Quantum key generation between two physical endpoints.

Key Management System – Key distribution at the application layer.

SDN Agent – Connects the node to the SDN controller.

CHALLENGES

Performance limitations

- Secret key rate lower than classical systems (Kbps)
- Distance limitation, 40-50 km (trusted nodes, repeaters)

Implementation complexity

- Faulty hardware implementation susceptible to attacks
- Heavy DSP chains to prepare and measure
- Computationally intensive LDPC reconciliation (QBER~40%)
- Photonics Integration Circuits (PICs) required
- Multidisciplinary topic, complex knowledge integration

OPPORTUNITIES

- Promise of unbreakable cryptosystem
- Provably secure ITS solution (bits)
- Forward secrecy can be ensured
- Protocol CV built on top of classical coherent systems
- Part of the hardware and algorithms can be reused
- Easy integration with classical systems
- Emerging market, 50% annual growth

PAULO
SANTOS

PAULO
SANTOS

Coronel Paulo Jorge Soares dos Santos is an officer of the National Republican Guard (GNR). He was born on April 23, 1973, and entered the Military Academy in 1992, where he completed a degree in Military Sciences, GNR Branch.

He holds a postgraduate degree in criminology in the field of Cybercrime and another in Information Systems from the Instituto Superior Técnico (IST), as well as a master's degree in Law and Security that dealt with the topic of Cyberterrorism.

In 2000, he served as liaison officer in the Rapid Intervention Unit of a GNR force deployed in East Timor, as part of the UNTAET international mission; In 2001 he was placed in the General Command of the GNR where he came to hold several leadership positions in the field of Information and Knowledge Technologies; In 2014, he also served as coordinator of the GNR Cybersecurity Working Group, having subsequently been placed in the Intelligence Directorate, where in 2016 he headed the Counter-Intelligence Division; From 2017 to April 2020, he held the position of “Crime Portfolio Manager” at the European Police Training and Education Agency at CEPOL based in Hungary. In 2020, he served as 2nd Commander of the Viseu Territorial Command of the GNR.

Since 2021, he has served as Deputy for Technological Security at the National Security Office (GNS).He is also co-author of 2 books, namely: “Cyberwar – Phenomena, Technologies and Authors” and “Safe Internet for Children”.

ABSTRACT

ABSTRACT

SECURING THE FUTURE: THE ROLE AND PURPOSE OF GNS IN THE PTQCI PROJECT

In this talk I introduce the Portuguese National Security Agency (GNS) and its pivotal role in the Portuguese Quantum Communication Infrastructure (PTQCI) project, which is part of the broader European Quantum Communication Infrastructure (EuroQCI) initiative. So, GNS is responsible for safeguarding national and European classified information through advanced cybersecurity measures and quantum communication technologies.

I describe the PTQCI project aims to create a resilient and secure communication network in Portugal, leveraging Quantum Key Distribution (QKD) to protect sensitive data against interception and cyber threats, contributing to both national sovereignty and European security.

I highlight that PTQCI is designed to integrate with existing fiber optic infrastructures, connecting public entities and expanding across Portuguese territories, with potential interoperability with Spain to enhance EuroQCI's strategic goals. GNS leads the implementation, regulatory oversight, and risk management of this quantum infrastructure, ensuring it aligns with both national and EU security standards. By building a self-sufficient quantum network, Portugal strengthens its digital sovereignty, reduces dependency on foreign communication infrastructures, and positions itself as a leader in quantum-secure communications.

Finally, I emphasize the importance of public trust and stakeholder collaboration. Enhancing that GNS is committed to transparent communication, public education, and community engagement to foster awareness and support for quantum technologies, through cooperation with governmental, industrial, and academic partners. In this context, GNS aims to ensure that PTQCI not only protects critical national interests but also drives technological innovation in secure communications within Europe and beyond.

REPÚBLICA PORTUGUESA

GNS Gabinete Nacional de Segurança PORTUGAL

EuroQCI PTQCI

GNS Gabinete Nacional de Segurança PORTUGAL

Portuguese National Security Agency - Gabinete Nacional de Segurança

COLONEL Paulo Santos – JAN25

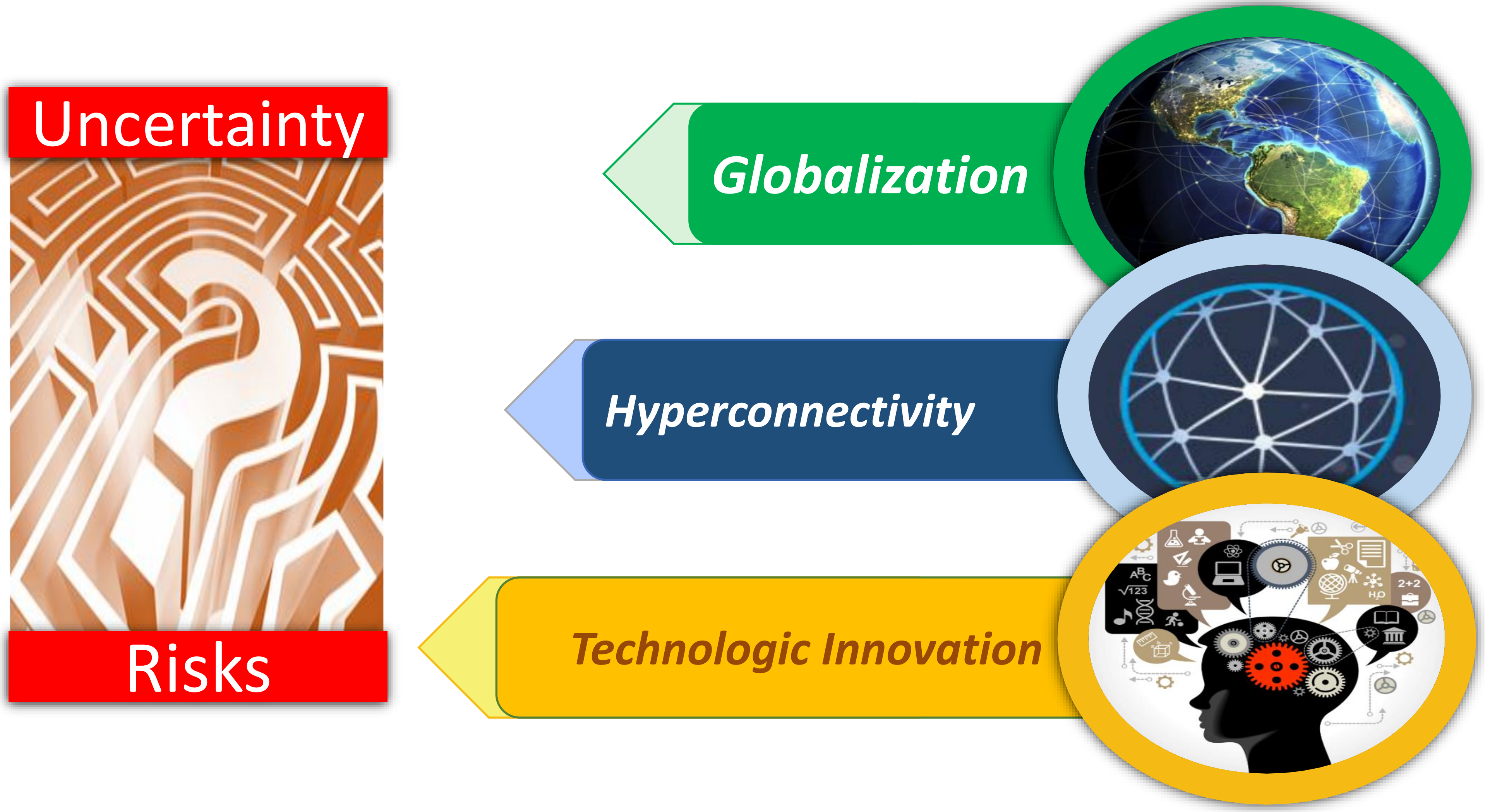
This project has received funding from the European Union's Digital European Programmed under the project "Portuguese Quantum Communication Infrastructure" (PTQCI, grant agreement No 101091730).

Securing the Future: The Role and Purpose of GNS in the PTQCI Project

This project has received funding from the European Union's Digital European Programmed under the project "Portuguese Quantum Communication Infrastructure" (PTQCI, grant agreement No 101091730).

The World in a permanent state of change

Change & Risks:



Uncertainty

Risks

Globalization

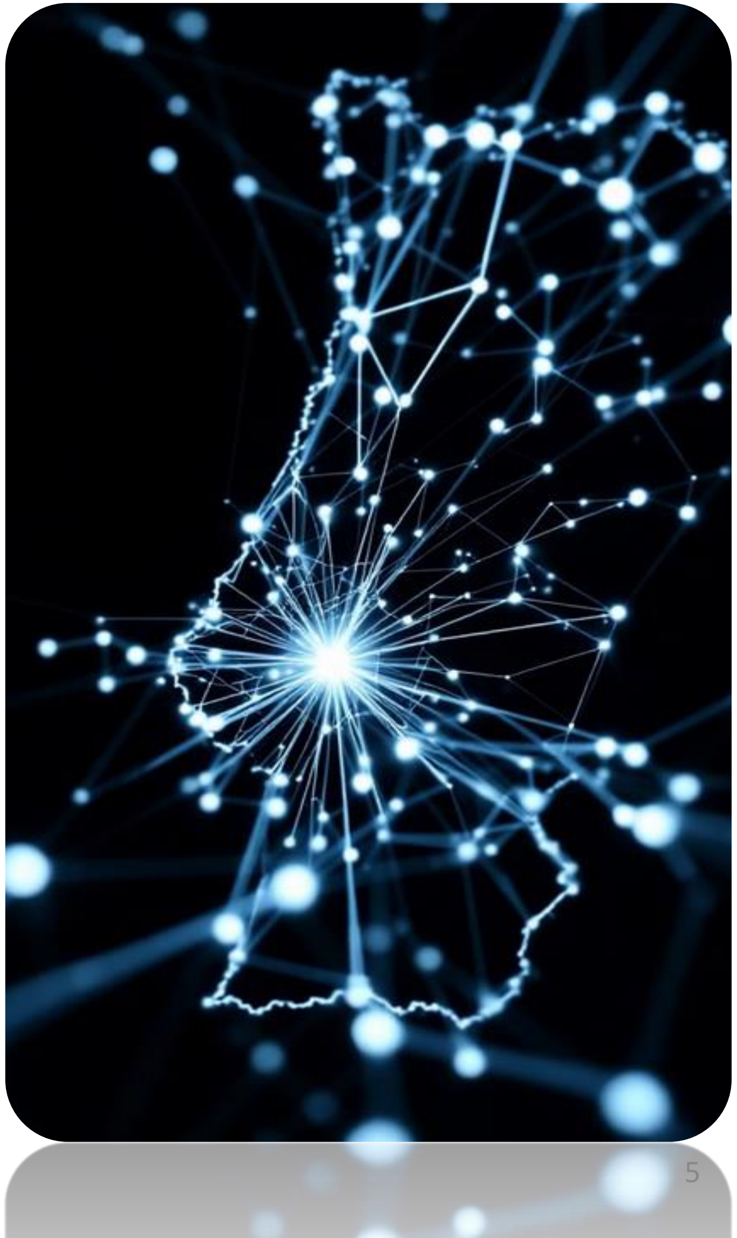
Hyperconnectivity

Technologic Innovation

EuroQCI

Portugal Role in EUROQCI

- Portugal participates as a key member state.
- Provide the EU with "EUwide" service for secure communications.
- Future Potential: Quantum Key Distribution (QKD) system could evolve into a complete quantum communication network, including state of the art developments in this technology.



PTQCI

Implementation of the PTQCI

- Integrated into Portugal's broader cybersecurity framework.
- National Instance of EuroQCI
- Pioneer in establishing the first national quantum communication infrastructure

Main Roles and Responsabilities of GNS

- Guarantee the security of Classified Information (CI) at the national level and for international organizations.

- Accredit individuals and entities for access to and handling of Classified Information.

- Serve as the accreditation and inspection authority for entities within the State Electronic Certification System — Public Key Infrastructure (SCEE).

GNS
Gabinete Nacional
de Segurança
PORTUGAL

GNS vs PTQCI

- Establishes and achieves strategic goals to enhance the security and efficiency of the Portuguese State.

- The PTQCI network will be created using homegrown European technologies to ensure security, reliability and strategic autonomy.

PTQCI

- Development of a highly resilient network utilizing existing fiber optic infrastructures.
- Plans for expansion beyond mainland Portugal, including the islands.

Collaboration for EUROQCI Interoperability

- PTQCI designed with significant collaboration with other EU member states, including EUROQCI's Spanish partners.

- Aims to achieve in the future full interoperability of quantum communication systems at the Iberian Peninsula level.

Enhancing Secure Communications in Europe and Portugal

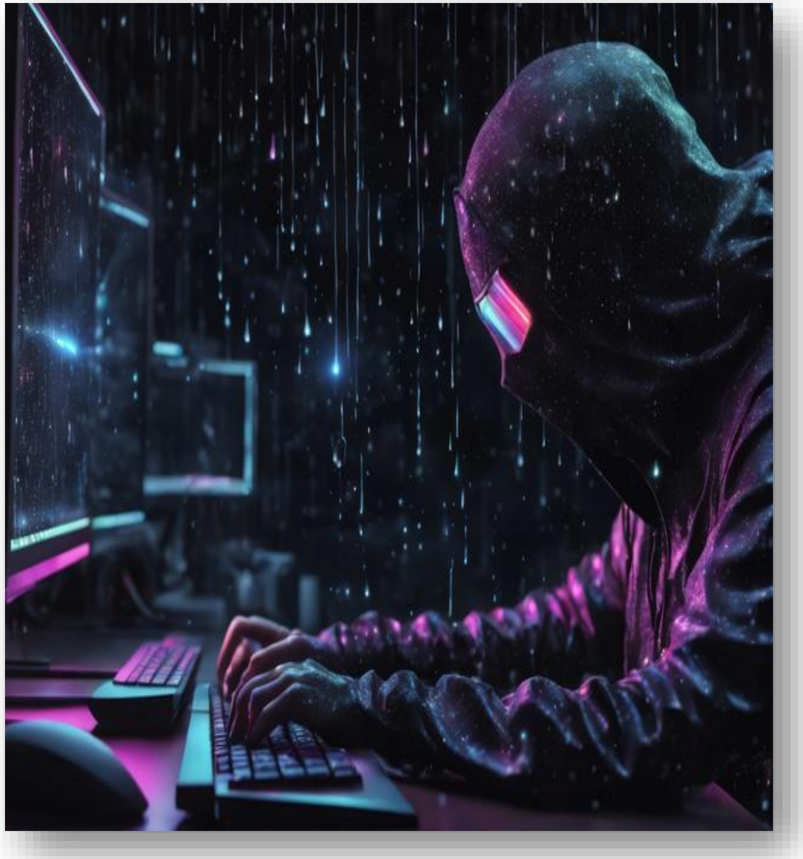
- Ensure privacy across Europe amid rising cyber threats and data breaches.

- Focus on securing critical infrastructure across various sectors including government and business.

- Integration of cutting-edge quantum solutions to secure data transfer and maintain public trust in digital systems.

Addressing Cyber Threats with Quantum Communication

- Unprecedented Cyber Challenges
- Evolving Digital Vulnerabilities
- Advancement of Quantum Communication Technologies



PTQCI Project: Transforming Secure Communications

- Aims to change substantially communication security
- Leverages principles of quantum physics for advanced secure communications.
- Safeguards critical national security data from unauthorized access.

Addressing Cyber Threats with PTQCI

- The sophistication of cyber threats demands a robust communication infrastructure.
- PTQCI demonstrates Portugal's proactive approach to safeguarding communication networks.
- Changes the landscape of data security, ensuring safer and more reliable communications.

PTQCI

Broader Implications of the PTQCI

Quantum communication technology has diversified potential applications

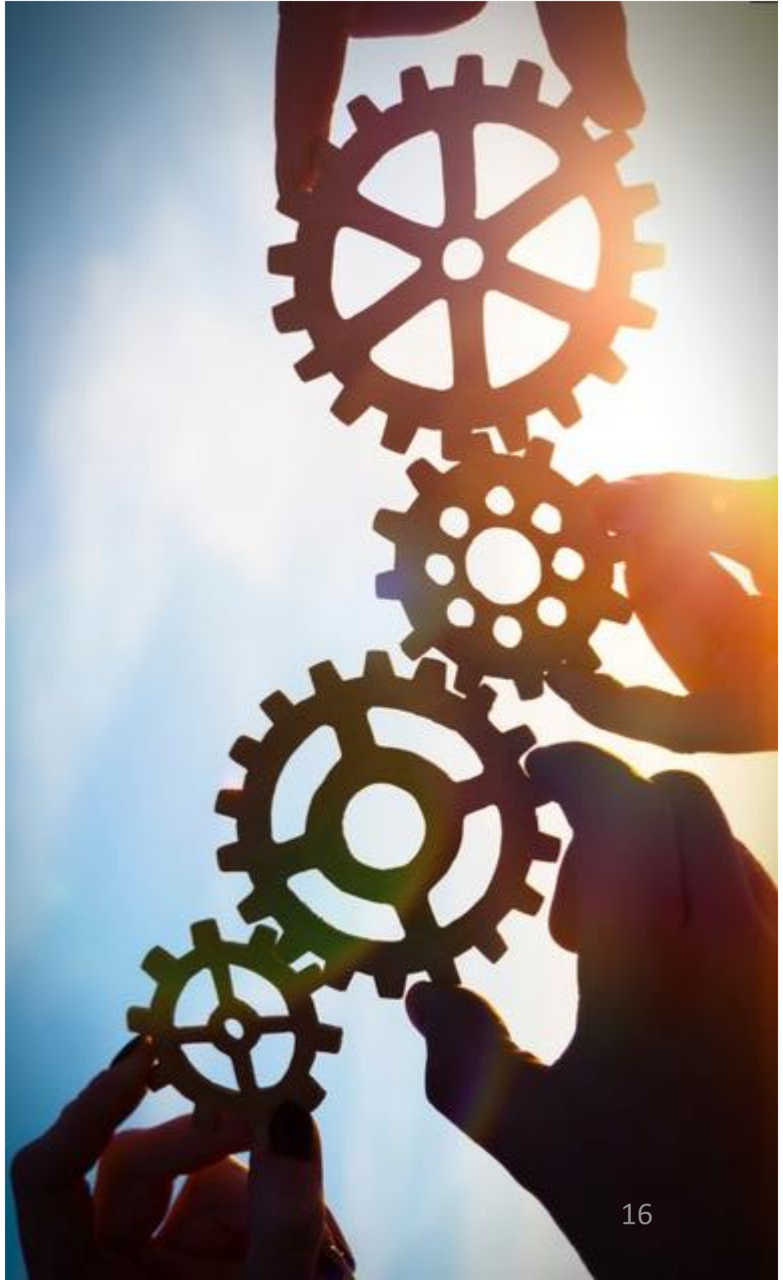
Secure information transmission enhances trust and operational efficiencies across critical sectors

The PTQCI project is about much more than technology; it redefines how security is perceived in our interconnected world

Positions Portugal to play a vital role in shaping discussions on the future of secure communications within Europe and beyond.

Role of the Portuguese NSA (GNS) in the PTQCI Project

- Emphasis on Collaboration
- Stakeholder Engagement
- Harnessing Collective Expertise
- Building a Secure Future
- Promoting R&D in this important field



Purpose of the Portuguese NSA(GNS) in the PTQCI Project

- Ensure successful implementation and oversight of the PTQCI project

- Alignment with National Security Objectives

- Proactively address and minimize risks associated with the introduction of new technologies

- Provide a clear governance framework

Risk Management Responsibilities of the GNS in the PTQCI Project

- Understanding Quantum Technology Risks
- Ensuring Infrastructure Resilience
- Development of Mitigation Strategies
- Achieving Security Objectives

GNS: Fostering Collaboration for the PTQCI Project

- Active Engagement with Stakeholders
- Creating a Comprehensive Approach
- Facilitating Knowledge Exchange
- Incorporating an International Perspective

Building Trust in Quantum Communications

- GNS's commitment to ensuring national security through advanced technologies
- Stakeholders & Citizens must feel confident that their data is protected
- GNS is dedicated to transparent operations and effective community engagement

Community Outreach Initiatives for Quantum Technologies

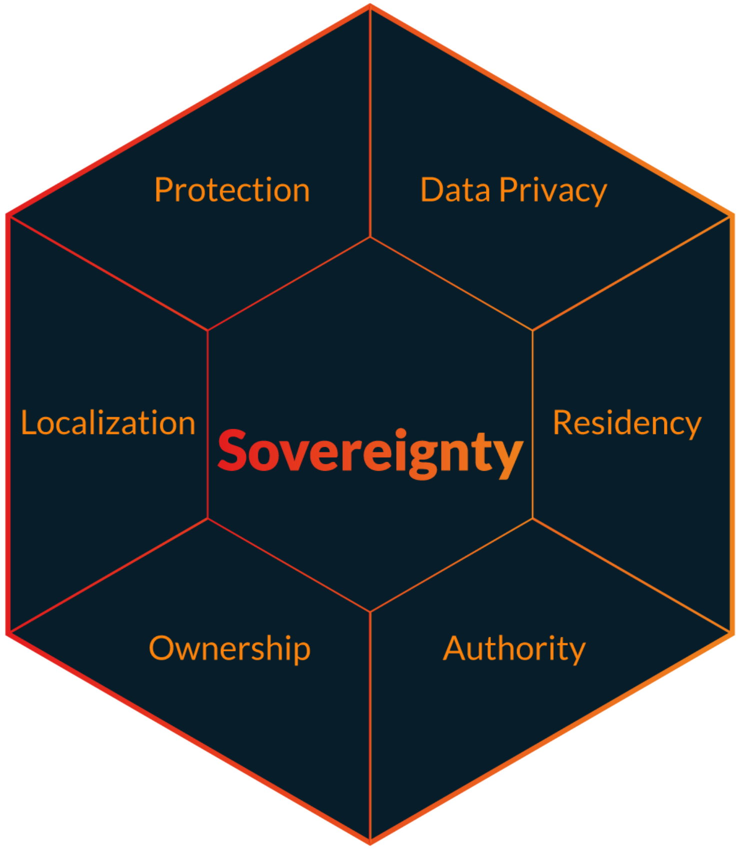
- Building awareness of quantum technologies
- Fostering an Informed Citizenry and Companies
- Enhancing Public Confidence
- Support for Quantum Technology Deployment

Enhancing Communication for National Security

- Gathering Feedback and Insights
- Addressing Public Concerns
- Creating Shared Responsibility
- Strengthening Commitment to Security

GNS's Role in Reinforcing National Sovereignty through PTQCI

- Safeguarding National Interests
- Response to Cybersecurity Threats
- Ensuring Independence and Safety
- Secure Management of Sensitive Communications



GNS Contribution to National Sovereignty via PTQCI

- Alignment with National Security Objectives
- Compliance with EU Standards
- Secure Management of Sensitive Communications
- Preventing External Influences

PTQCI

Conclusion

- GNS is essential to advancing Portugal's national security goals in the context of evolving communication threats.
- Engages in proactive risk assessments to ensure security and resilience of communications infrastructure.
- Committed to open communication with stakeholders about security initiatives and developments.
- Positions the GNS to effectively protect Portugal's security infrastructure against future challenges through quantum communication technology.

Securing the Future: The Role and Purpose of GNS in the PTQCI Project

Thank You

Gabinete Nacional de Segurança

Colonel Paulo Santos
paulo.jorge.santos@gns.gov.pt
Tel: +351210403695

This project has received funding from the European Union's Digital European Programmed under the project "Portuguese Quantum Communication Infrastructure" (PTQCI, grant agreement No 101091730).

RICARDO
CHAVES

RICARDO **CHAVES**

Ricardo Chaves is an associate professor at the Computer Science Department at the University of Lisbon/IST and a researcher at INESC-ID. He is also a senior member of IEEE. His research interests are focused on cryptography systems including Quantum and Post Quantum security, reconfigurable hardware architectures, and on embedded and user-oriented systems.

He has participated in several European research projects and collaborative actions, of which can be highlighted: Disruptive SDN secure communications for European Defence (DISCRETION); The Portuguese Quantum Communication Infrastructure (PTQCI); Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module (FutureTPM).

ABSTRACT

ABSTRACT

CRYPTOGRAPHY 101

This talk introduces the fundamentals of cryptography, covering its historical origins, the basics of secret key cryptography, and simple cryptanalysis concepts. We highlight the evolution of symmetric encryption, focusing on block and stream ciphers used in modern systems. Designed for beginners, the talk provides a clear overview of how cryptography ensures secure communication and sets the foundation for deeper exploration and how Quantum Key Distribution can take advantage of it.

Cryptography 101

Crypto + graphikos
Hidden + graphic/writing

PORTUGUESE
QUANTUM COMMUNICATION INFRASTRUCTURE

Index

- Cryptography - History and Usage
- Secret Key cryptography
- Basic cryptanalysis
- Evolution of cryptography
- Modern Symmetric Ciphers
  - Block Ciphers
  - Stream Ciphers

Cryptography - History and Usage

- 1900 BC is the 1st kwon usage of cryptography by the Egyptians – simple substitution scheme

Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

- 1 AD Julius Cesar used the simple letter shift cipher in the Gallic Wars

Msg: *OMNIA GALLIA EST DIVISA IN PARTES TRES*
Enc: RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

- 200 AD a new mathematical cryptographic scheme was used by Sun Tzu (a military strategist)

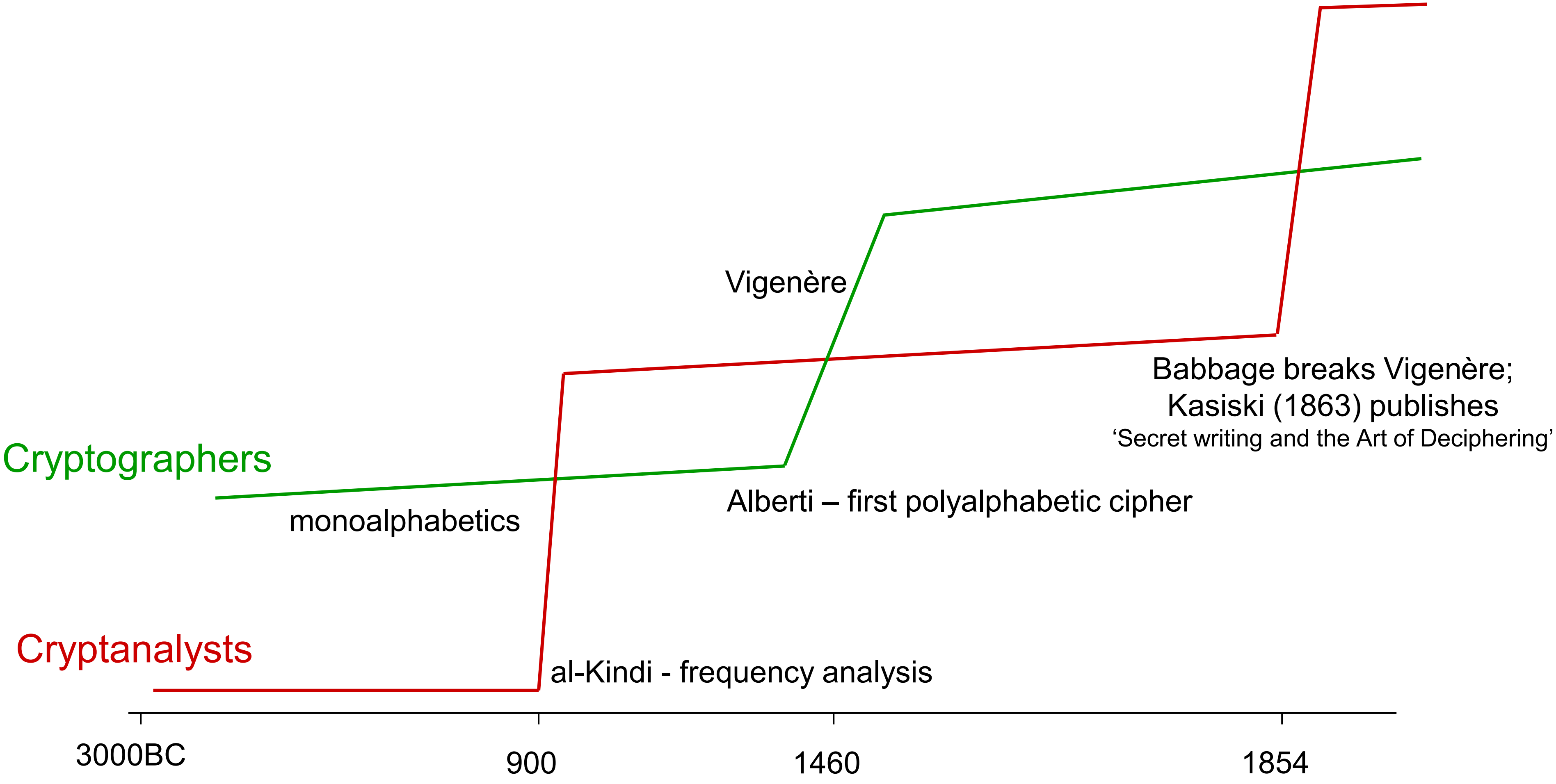
$$CRT\,(2,3,2)_{(357)} = ??\ (23)$$

- 4th century AD Kama-sutra: women should study 64 arts, including the art of secret writing (Vatsyayana cipher)

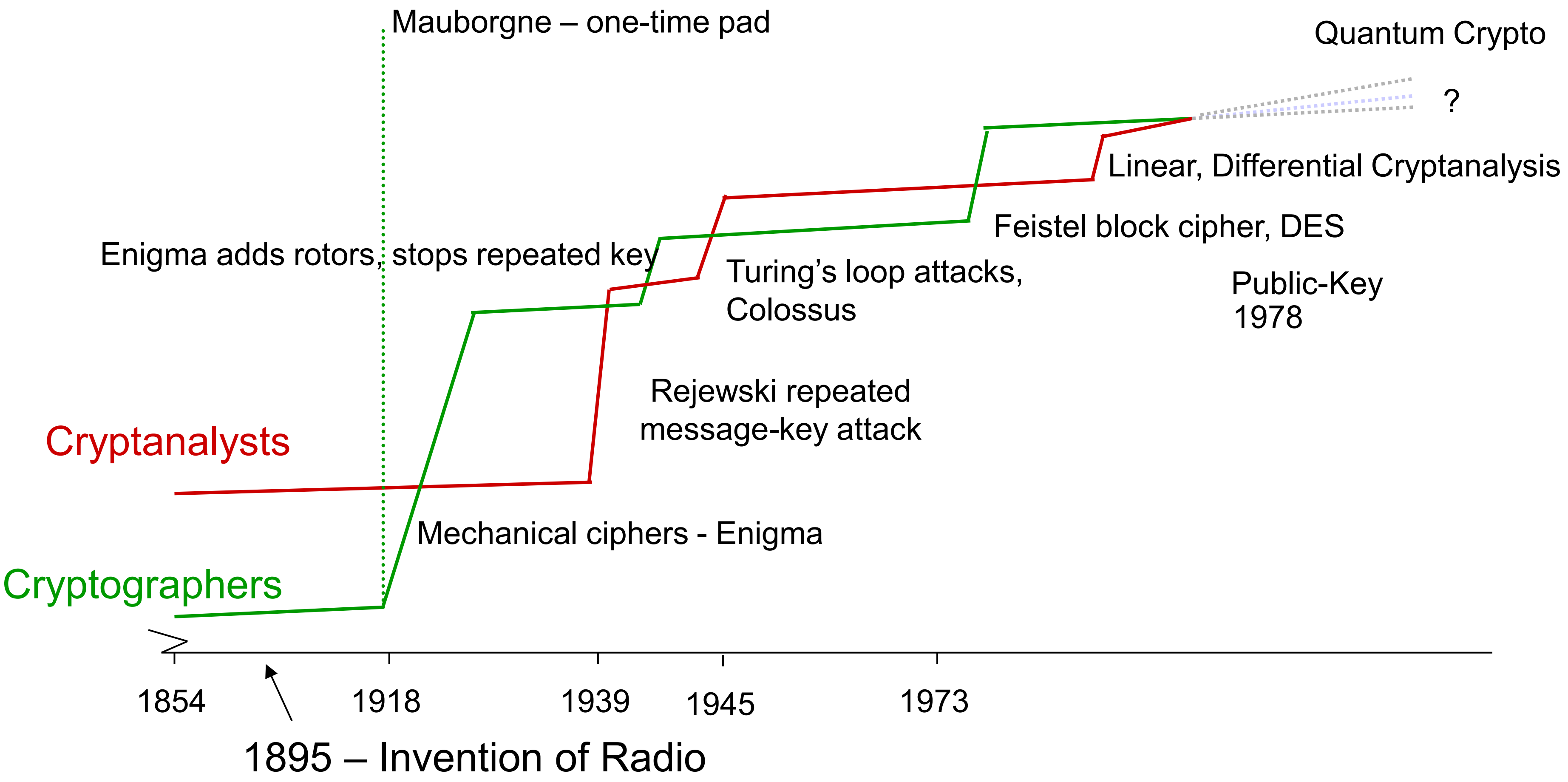
- 1412 AD an 14vol encyclopaedia on Cryptanalysis is compiled by the Arabs

- In the 2nd world war the enigma rotor machine is used (substitution scheme using a continuously changing alphabet)

Really Brief History - First 4000 years



Really Brief History - last 100 years



Cryptography - Theme

- Arms race between cryptographers and cryptanalysts
  - But, often disconnected between the two (e.g., Mary Queen of Scots used monoalphabetic cipher long after known breakable)
- Motivated by war (more recently: commerce)
- Driven by advances in technology, mathematics
- Multi-disciplinary field
  - Linguists, classicists, mathematicians, computer scientists, physicists
- Secrecy often means advances rediscovered and miscredited

Cryptography - Current usage

- nowadays a variety of cryptographic algorithms and systems are used as part of our everyday lives:
  - Accessing the internet & E-shopping
  - Cash payment systems & ATM machines
  - Electricity meters
  - Buildings and public transportation access
  - Pay TV
  - Anti-car theft systems
  - Nautical charts
  - Private communications
  - …

Security vs. Pragmatics

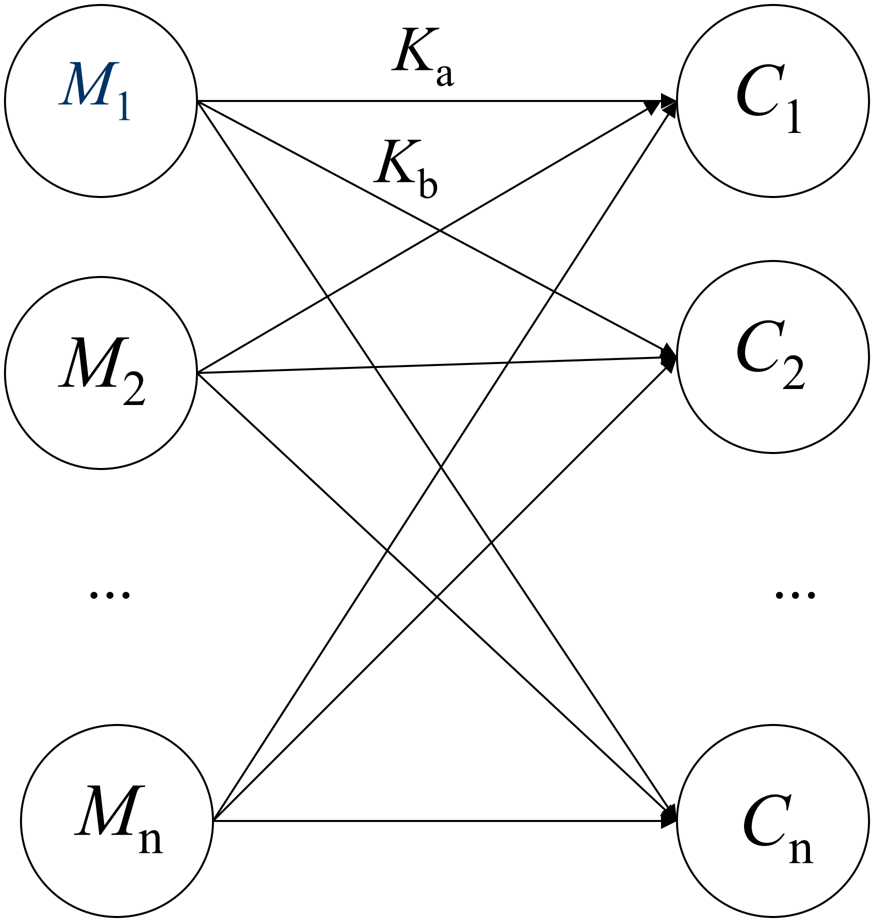
- Trade-off between security and effort
  - one-time pad: perfect security, but requires distribution and secrecy of long key
  - DES: short key, fast algorithm, but breakable
  - quantum cryptography: perfect security, guaranteed secrecy of key, slow, requires expensive hardware, limited distances

- Don’t spend €10M to protect €1M.

- Don’t protect €1B with encryption that can be broken for €1M.

Secret Key cryptography

Perfect Cipher: Definition



A perfect cipher: there is some key that maps any message to any ciphertext with equal probability.

For any i, j:

$$p\,(M_i|C_j) = p\,(M_i)$$

Perfect Cipher - Keyspace Theorem

Theorem: If a cipher is perfect, there must be at least as many keys (l) as there are possible messages (n).

Perfectly Secure Cipher: One-Time Pad

- Mauborgne/Vernam [1917]
- XOR (⊕):

  $0 \oplus 0 = 0 \quad 1 \oplus 0 = 1$

  $0 \oplus 1 = 1 \quad 1 \oplus 1 = 0$

  $a \oplus a = 0$

  $a \oplus 0 = a$

  $a \oplus b \oplus b = a$

- $E(P, K) = P \oplus K$

  $D(C, K) = C \oplus K = (P \oplus K) \oplus K = P$

Perfect Encryption Scheme?

- One-Time Pad (XOR message with key)
- Example:
  - Message: ONETIMEPAD
  - Key: TBFRGFARFM
  - Ciphertext: IPKLPSFHGQ

  - The key TBFRGFARFM decrypts the message to ONETIMEPAD
  - The key POYYAEAAZX decrypts the message to SALMONEGGS
  - The key BXFGBMTMXM decrypts the message to GREENFLUID

Problems!

- Cannot reuse K
  - What if receiver has

$$C_1 = P_1 \oplus K \text{ and } C_2 = P_2 \oplus K$$

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K$$

$$= P_1 \oplus P_2$$

- Need to generate truly random bit sequence as long as all messages
- Need to securely distribute key

Kerckhoff's Principle

- Cryptography **always** involves:
  - Transformation
  - Secret
- **Security should depend only on the key**
- Do not assume the enemy won't know the algorithm
  - Can capture machines, disassemble programs, etc.
  - Too expensive to invent a new algorithm if it might have been compromised
- Security through obscurity isn't good
  - Look at history for examples
  - Better to have scrutiny by open experts

"The enemy knows the system being used."
Claude Shannon

Big numbers

- Uses really big numbers
  - 1 in 2^{61} odds of winning the lotto and being hit by lightning on the same day
  - 2^{92} atoms in the average human body
  - 2^{128} possible keys in a 128-bit key
  - 2^{170} atoms in the planet
  - 2^{190} atoms in the sun
  - 2^{233} atoms in the galaxy
  - 2^{256} possible keys in a 256-bit key

Basic cryptanalysis

PORTUGUESE
QUANTUM COMMUNICATION INFRASTRUCTURE

Simple Substitution Cipher

- $C = E_K(p)$

  $C_i = K[p_i]$
- Key is alphabet mapping:

  a → J, b → L, ...
- Suppose the attacker knows the algorithm but not the key, how many keys to try?

26! $\approx 4 \times 10^{26}$

If every person on earth tried one per second, it would take 5000 million years.

However…!

Monoalphabetic Cipher

"XBW HGQW XS ACFPSUWG FWPGWXF CF AWWKZV CDQGJCDWA CD BHYJD DJXHGW; WUWD XBW ZWJFX PHGCSHF YCDA CF GSHFWA LV XBW KGSYCFW SI FBJGCDQ RDSOZWAQW OCXBBWZA IGSY SXBWGF."

Can we discover the message without the Key?

Frequency Analysis

“XBW HGQW XS ACFPSUWG FWPGWXF CF AWWKZV
CDQGJCDWA CD BHYJD DJXHGW; WUWD XBW
ZWJFX PHGCSHF YCDA CF GSHFWA LV XBW
KGSYCFW SI FBJGCDQ RDSOZWAQW OCXBBWZA
IGSY SXBWGF.”

W: 20
C: 11
F: 11
G: 11

“Normal” English:

e	12%
t	9%
a	8%

Pattern Analysis

"XBe HGQe XS ACFPSUeG FePGeXF CF AeeKZV CDQGJCDeA CD BHYJD DJXHGe; eUeD XBe ZeJFX PHGCSHF YCDA CF GSHFeA LV XBe KGSYCFe SI FBJGCDQ RDSOZeAQe OCXBBeZA IGSY SXBeGF."

XBe = "the"

Most common trigrams in English:

the = 6.4%

and = 3.4%

Guessing

“the HGQe tS ACFPSUeG FePGetF CF AeeKZV CDQGJCDeA CD hHYJD DJtHGe; eUeD the ZeJFt PHGCSHF YCDA CF GSHFeA LV the KGSYCFe SI FhJGCDQ RDSOZeAQe OCthheZA IGSY StheGF.”

S = “o”

Guessing

“the HrQe to ACscoUer sePrets is deeKZV iDQrJiDed iD hHYJD DJtHre; eveD the ZeJst cHrioHs YiDd is roHsed LV the KroYise oI shJriDQ RDoOZedQe OithheZd IroY otheGF.”

otheGF = “others”

Guessing

“the HrQe to ACscoUer sePrets is deeKZV iDQrJiDed iD hHYJD DJtHre; eveD the ZeJst cHrioHs YiDd is roHsed LV the KroYise oI shJriDQ RDoOZedQe OithheZd IroY others.”

“sePrets” = “secrets”

Guessing

“the HrQe to ACscoUer secrets is deeKZV iDQrJiDed iD hHYJD DJtHre; eveD the ZeJst cHrioHs YiDd is roHsed LV the KroYise oI shJriDQ RDoOZedQe OithheZd IroY others.”

“ACscoUer” = “discover”

Guessing

“the HrQe to discover secrets is deeKZV
iDQrJiDed iD hHYJD DJtHre; eveD the
ZeJst cHrioHs YiDd is roHsed LV the
KroYise oI shJriDQ RDoOZedQe OithheZd
IroY others.”

Why was it so easy?

- Doesn’t hide statistical properties of plaintext
- Doesn’t hide relationships in plaintext (EE cannot match dg)
- English (and all natural languages) is very redundant: about 1.5 bits of information per letter

(~68% of letters are redundant)

  - Compress English with gzip – about 1:6

How to make it harder?

- Cosmetic
- Hide statistical properties:
  - Encrypt “e” with 12 different symbols, “t” with 9 different symbols, etc.
  - Add nulls, remove spaces
- Polyalphbetic cipher
  - Use different substitutions
- Transposition
  - Scramble order of letters

Evolution of cryptography

PORTUGUESE
QUANTUM COMMUNICATION INFRASTRUCTURE

Caeser cipher

It's are simple substitution ciphers. Each letter in the plaintext is shifted a certain number of places down the alphabet.

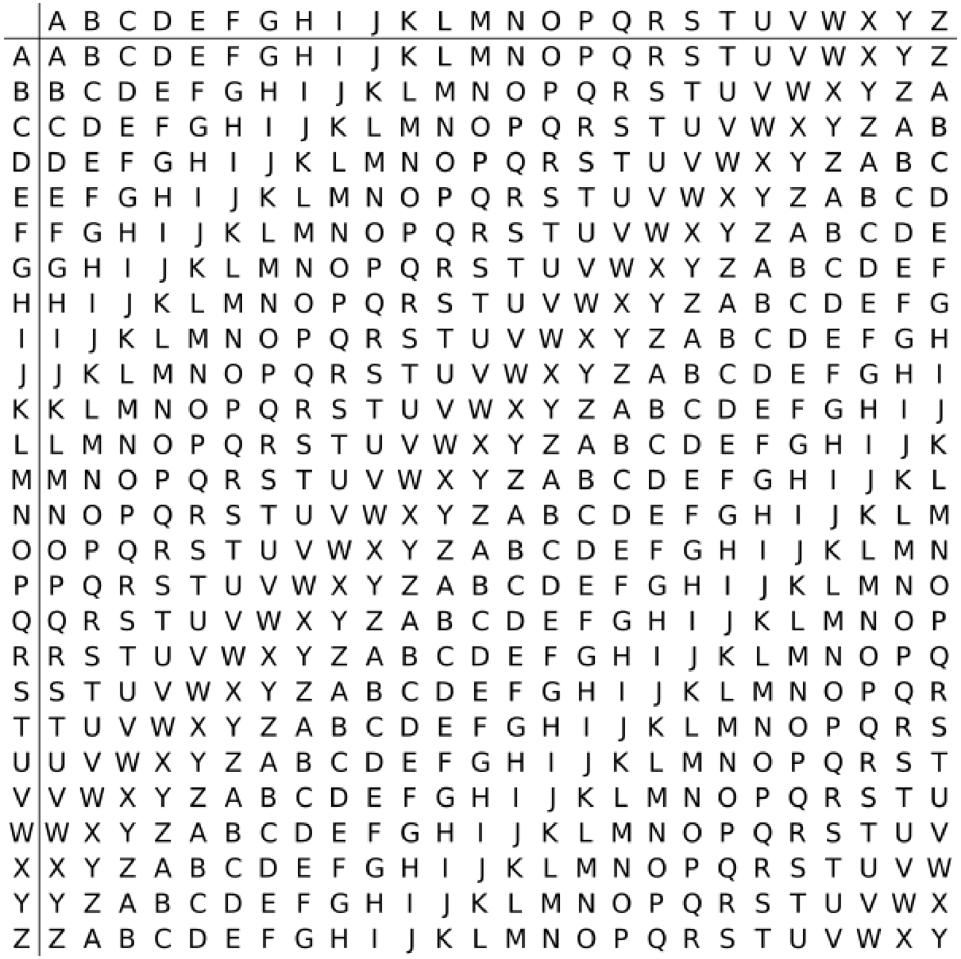
- $C = E_K(P) = P + Key$
- $P = D_K(P) = P - Key$

- Example:
  - Key =12
  - Cifra: Ola => Zcn

Vigenère Cipher

- Vigenère Cipher:
  - A Polyalphabetic Cipher developed in 1553
  - Modification of the substitution Cipher
  - The alphabet is re-scrambled for each letter of the plaintext message
    - Vigenère cipher starts with a 26 x 26 matrix of alphabets in sequence. First row starts with ‘A’, second row starts with ‘B’, etc.
  - Requires a keyword or phrase to start the substitution sequence
    - Each character of the message is combined with the characters of the keyword to find the ciphertext character
  - Considered unbreakable for several centuries.
    - Until 1863

Vigenère Cipher



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Key: ABCDEF AB CDEFA
Plaintext: **CRYPTO** IS SHORT
Ciphertext: **CSASXT** IT UKSWT

Key: BCD EFABCDEFABCD
Plaintext: FOR **CRYPTO**GRAPHY
Ciphertext: GQU **GWYQVR**KWAQJB

Enigma

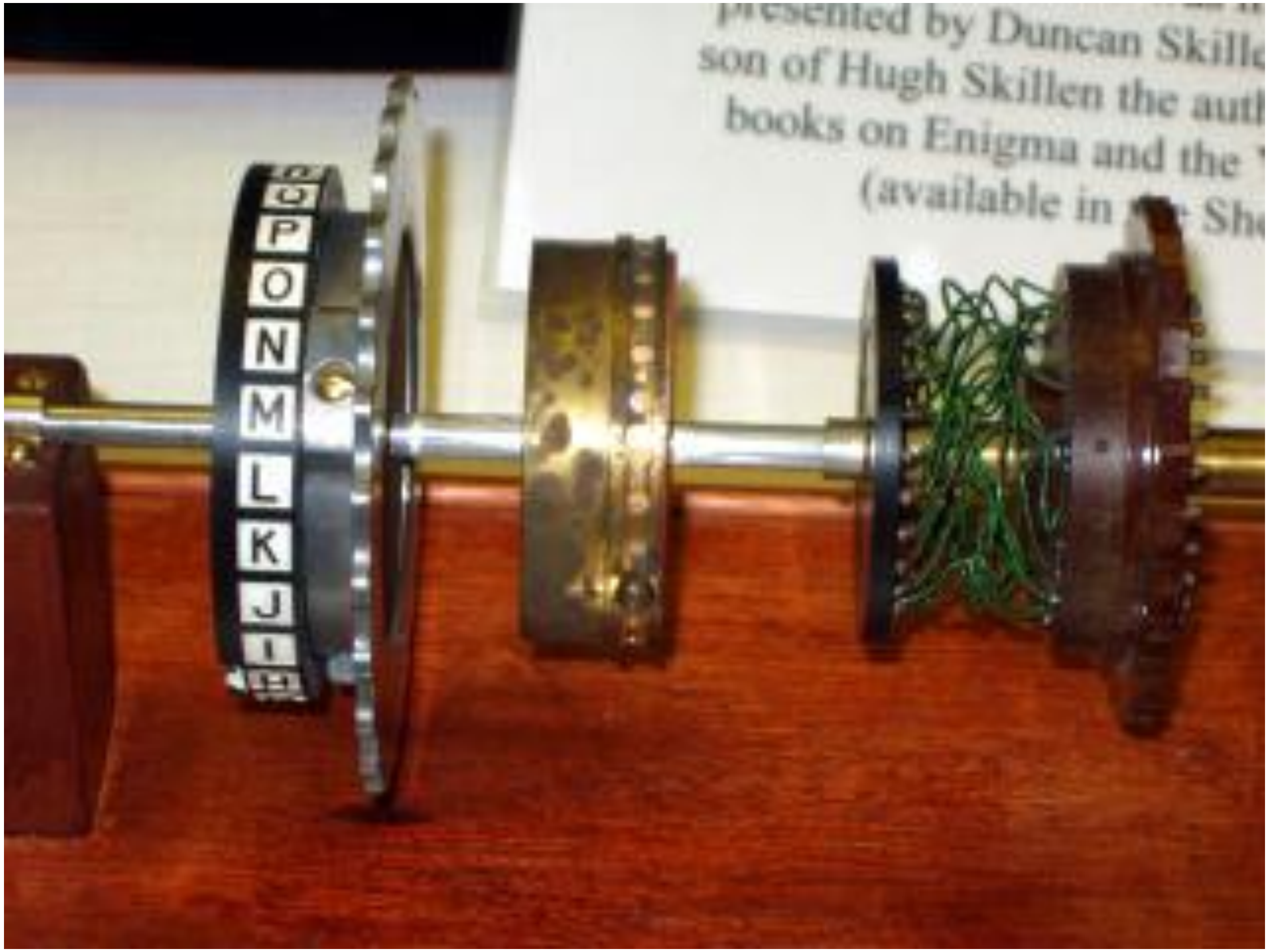
- Invented commercially, 1923
- Used by German Navy, Army, Air Force
- About 50,000 in use
- Modified throughout WWII, believed to be perfectly secure
- Kahn's *Codebreakers* (1967) didn't know it was broken
- Turing's 1940 treatise on Enigma declassified in 1996

Enigma - Rotor Wheel

Simple substitution

No letter maps to itself

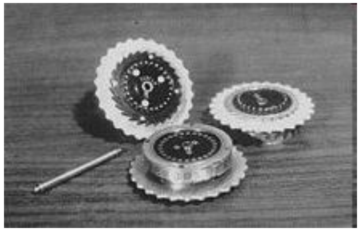
Latch turns next rotor once per rotation



Enigma – Settings (the Key)

- Plugboard
  - Swap pairs of letters
  - Number of plugs varied (≤ 6 until 1939, up to 10 after)
- Rotors
  - Before 1939 – Three rotors (choose order)
  - After – Choose 3 from set of 5 rotors
  - Orientations (3) – start orientations of the 3 rotors
  - Ring settings (2) – when next ring advances
- Reflector
  - Fixed symmetric substitution ($A \rightarrow B \Rightarrow B \rightarrow A$)

    Involution: $R^2 = Identity$



Enigma - Operation

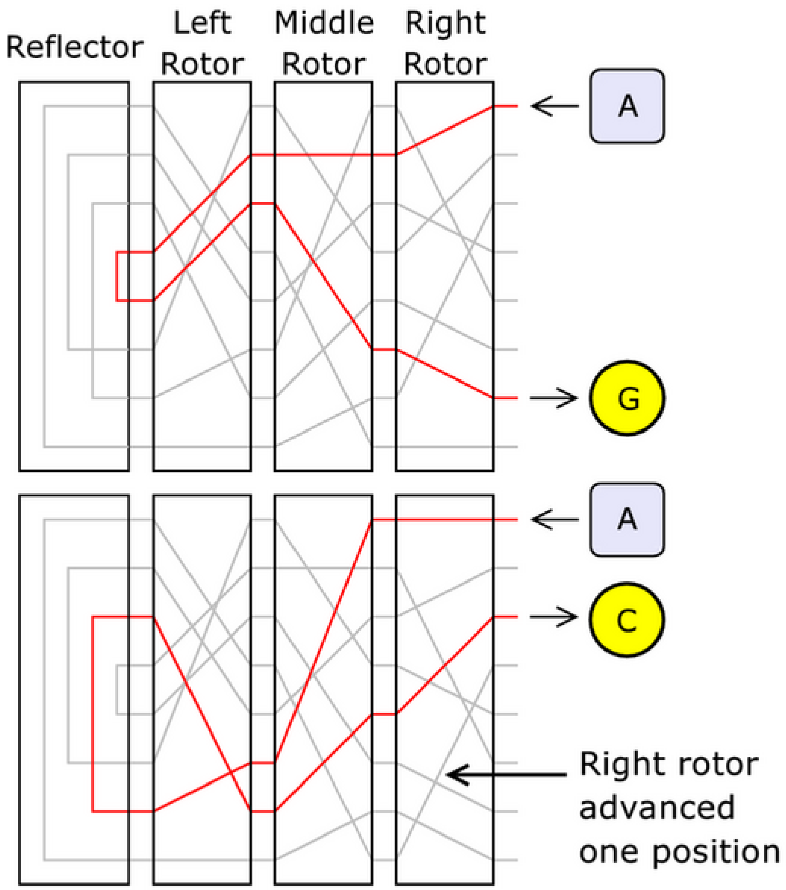
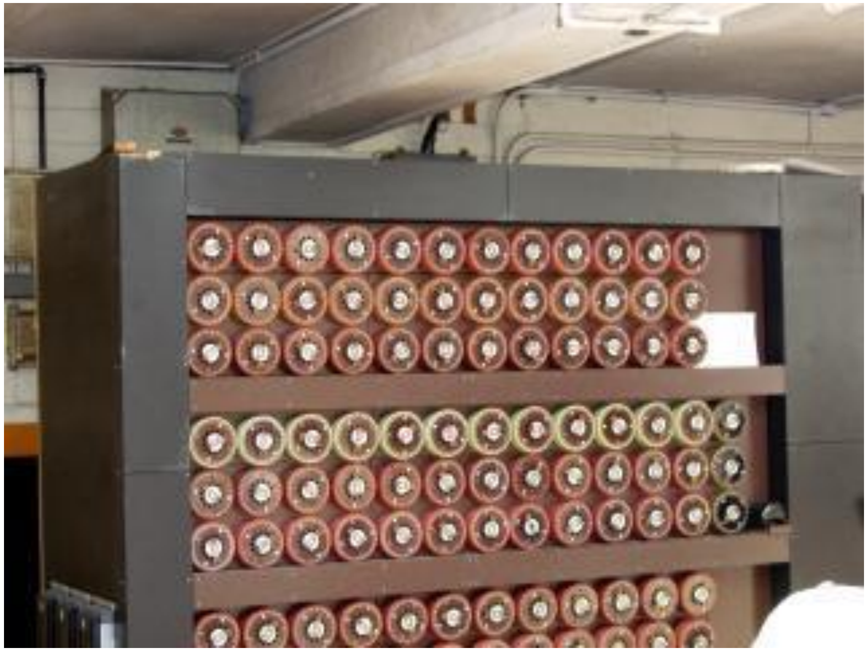


Image from http://en.wikipedia.org/wiki/Image:Enigma-action.png

Bletchley Park

- United Kingdom's main decryption establishment (in 1939)
  - aka Station X
- Alan Turing leads British effort to crack Enigma
- Use cribs ("WETTER" transmitted every day at 6am) to find structure of plugboard settings
- Built "bombes" to automate testing
- 10,000 people worked at Bletchley Park on breaking Enigma (100,000 for Manhattan Project)

Alan Turing's "Bombe"



Steps through all possible rotor positions (26^3), testing for probable plaintext; couldn't search all plugboard settings ($> 10^{12}$); take advantage of loops in cribs

Enigma Cryptanalysis

- Relied on combination of sheer brilliance, mathematics, espionage, operator errors, and hard work
- Huge impact on WWII
  - Britain knew where German U-boats were
  - Advance notice of bombing raids
  - But...keeping code break secret more important than short-term uses

Modern Symmetric Ciphers

A billion billion is a large number, but it's not that large a number.

Whitfield Diffie

Goals of Cipher: Diffusion and Confusion

- Claude Shannon [1945]
- Diffussion:
  - Small change in *plaintext*, changes lots of the *ciphertext*
  - Statistical properties of plaintext hidden in ciphertext
- Confusion:
  - Statistical relationship between *key* and *ciphertext* as complex as possible
- So, need to design functions that produce an output that is diffused and confused

DES Avalanche

```
Input:    ...............................................................*     1
Permuted: .......................................*........................     1
Round 1:  .......*........................................................     1
Round 2:  .*..*...*.....*........................*........................     5
Round 3:  .*..*.*.**..*.*.*.*....**.....**.*..*...*.....*.................    18
Round 4:  ..*.*****.*.*****.*.*......*.....*..*.*.**..*.*.*.*....**.....**    28
Round 5:  *...**..*.*...*.*.*.*...*.***..*..*.*****.*.*****.*.*......*....    29
Round 6:  ...*..**.....*.*..**.*.**...*..**...**..*.*...*.*.*.*...*.***..*    26
Round 7:  *****...***....**...*..*.*..*......*..**.....*.*..**.*.**...*..*
Round 8:  *.*.*.*.**.....*.*.*...**.*...*******...***....**...*..*.*..*...
Round 9:  ***.*.***...**.*.****.....**.*..*.*.*.*.**.....*.*.*...**.*...**
Round 10: *.*..*.*.**.*..*.**.***.**.*...****.*.***...**.*.****.....**.*..
Round 11: ..******......*..******....*....*.*..*.*.**.*..*.**.***.**.*...*
Round 12: *..***....*...*.*.*.***...****....******......*..******....*....
Round 13: **..*....*..******...*........*.*..***....*...*.*.*.***...****..
Round 14: *.**.*....*.*....**.*...*..**.****..*....*..******...*........*.
Round 15: **.*....*.*.*...*.**.*..*.*.**.**.**.*....*.*....**.*...*..**.**
Round 16: .*..*.*..*..*.**....**..*..*..****.*....*.*.*...*.**.*..*.*.**.*
Output:   ..*..**.*.*...*....***..***.**.*...*..*..*.*.*.**.*....*.*.*.**.
```

PORTUGUESE QUANTUM COMMUNICATION INFRASTRUCTURE

Block Ciphers

Block Ciphers

- Stream Ciphers
  - Encrypts small (bit or byte) units one at a time
- Block Ciphers
  - Encrypts large chunks (64–256 bits) at once
- Ciphers we have seen so far:
  - Changing one letter of the message only changes one letter of ciphertext
  - There were classical ciphers that had some diffusion:
    - Vigenère autokey
    - Enigma

AES - Advanced Encryption Standard

- Replacement for DES was needed
  - the standard until 2001
  - 64 bit data block and 56 bit secret key
  - broken in less than 1 day with less than 5k€ (in 2008)
- NIST issued a call for a new AES in 1997
  - AES Requirements:
    - Symmetric block cipher
    - 128-bit data, 128/192/256-bit keys
    - Stronger & faster than triple DES
    - Active life of 20-30 years (+ archival use)
    - Provide full specification & design details
- 15 candidates accepted in Jun 1998

AES Short-list

- After testing and evaluation, short-list of 5 in Aug 1999:
    - MARS (IBM) - complex, fast, high security margin
    - RC6 (USA) - very simple, very fast, low security margin
    - Rijndael (Belgium) - clean, fast, good security margin
    - Serpent (Euro) - clean, slow, very high security margin
    - Twofish (USA) - complex, very fast, high security margin
- Then subject to further analysis & comment
- Saw contrast between algorithms with
    - Few complex rounds vs. many simple rounds
    - Refined existing ciphers vs. new proposals
- The wining cipher was selected in Oct 2000
- Published as FIPS PUB 197 standard in Dec 2001

The Wining Cipher - Rijndael

- Designed by Rijmen-Daemen in Belgium
- Block length: 128, 192, and 256 bits
- Key injection by bitwise XOR
- Does not use a Feistel structure
- An iterated cipher:
  - Operates on entire data block in every round
  - Does not use a Feistel cipher network
- Designed to be:
  - Resistance against all known attacks (at the time)
  - Speed and code compactness on a wide range of platforms
  - Design simplicity

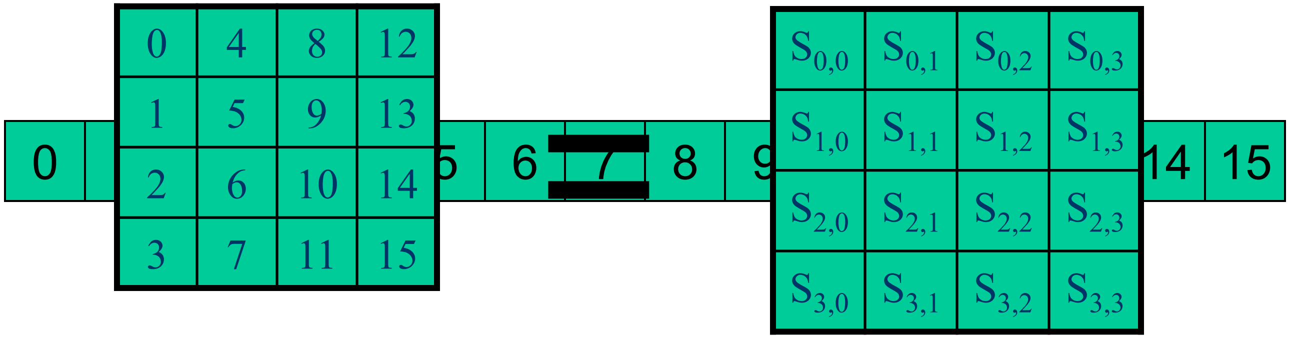
Overall AES/Rijndael characteristics

- Data block of 4 x 4 bytes, the "state"
- Key is expanded to an array of words
- Has 10/12/14 rounds in which the *state* undergoes:
  - substitute bytes (1 S-box used on every byte)
  - shift rows (permute bytes between columns)
  - mix columns (substitute using matrix multiplication of columns)*
  - add round key (XOR state with key material)
- With fast XOR & table lookup implementations
- AES/Rijndael parameters:
  - key size: 128, 192, 256
  - block length: 128, 192, 256
  - round key size: 128

* Initial XOR key material & incomplete last round

AES - Obtaining the *State* Array

Input block → State

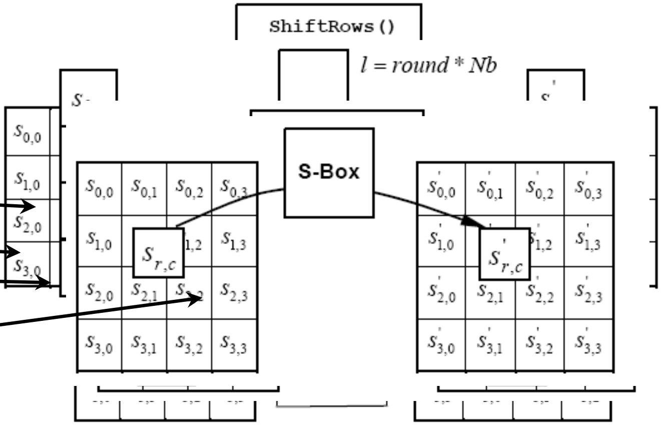


0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

AES - Encryption procedure

```
byte state[4]

state = in

AddRoundKey(state, keySchedule[0])

for round = 1 step 1 to Nr–1 {
   SubBytes(state)
   ShiftRows(state)
   MixColumns(state)
   AddRoundKey(state, keySchedule[round])
}

SubBytes(state)
ShiftRows(state)
AddRoundKey(state, keySchedule[Nr])

out = state
```



ShiftRows()
$l = round * Nb$
S-Box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{r,c}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{r,c}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

No MixColumns

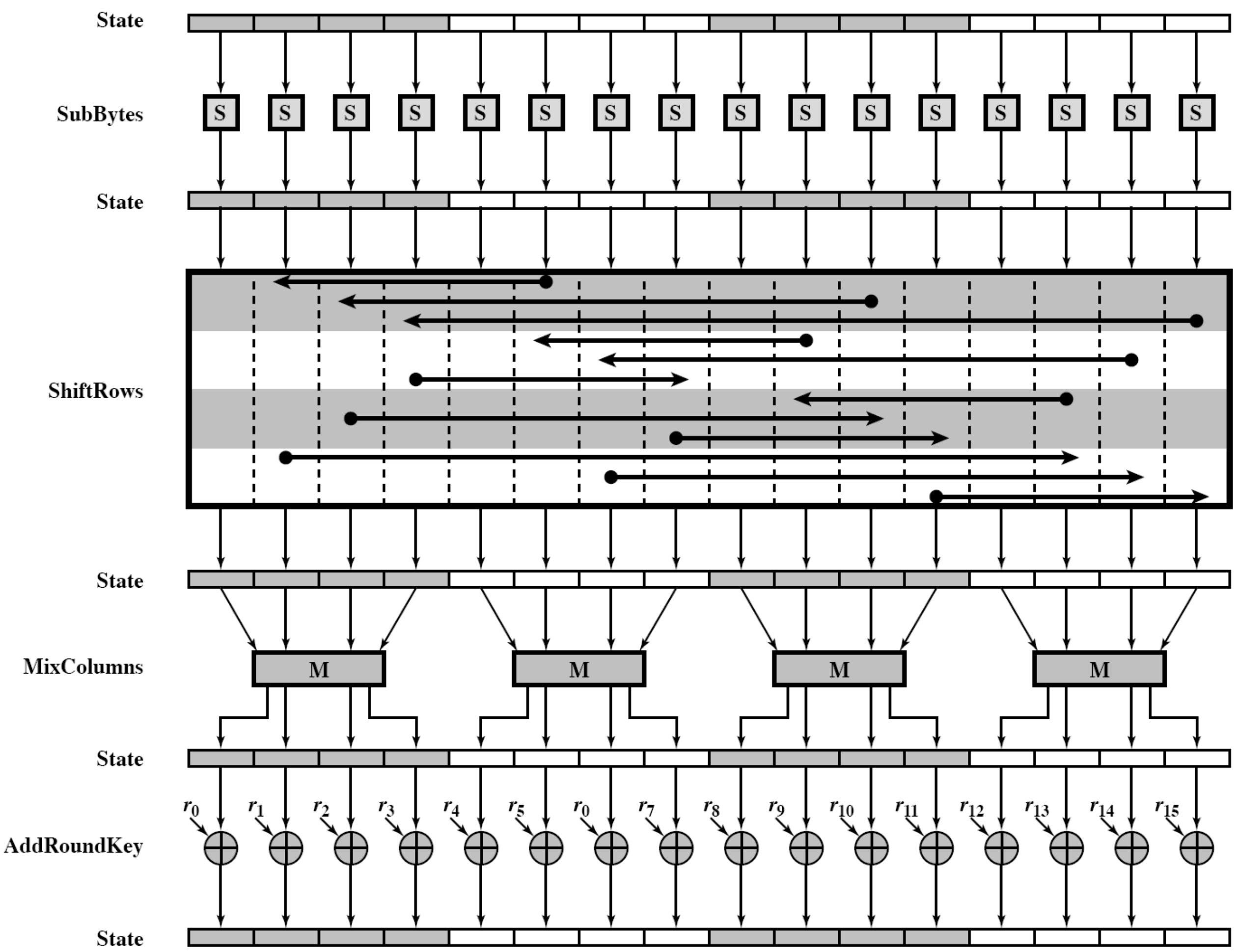
AES - Main Encryption Round

`SubBytes(state)`

`ShiftRows(state)`

`MixColumns(state)`

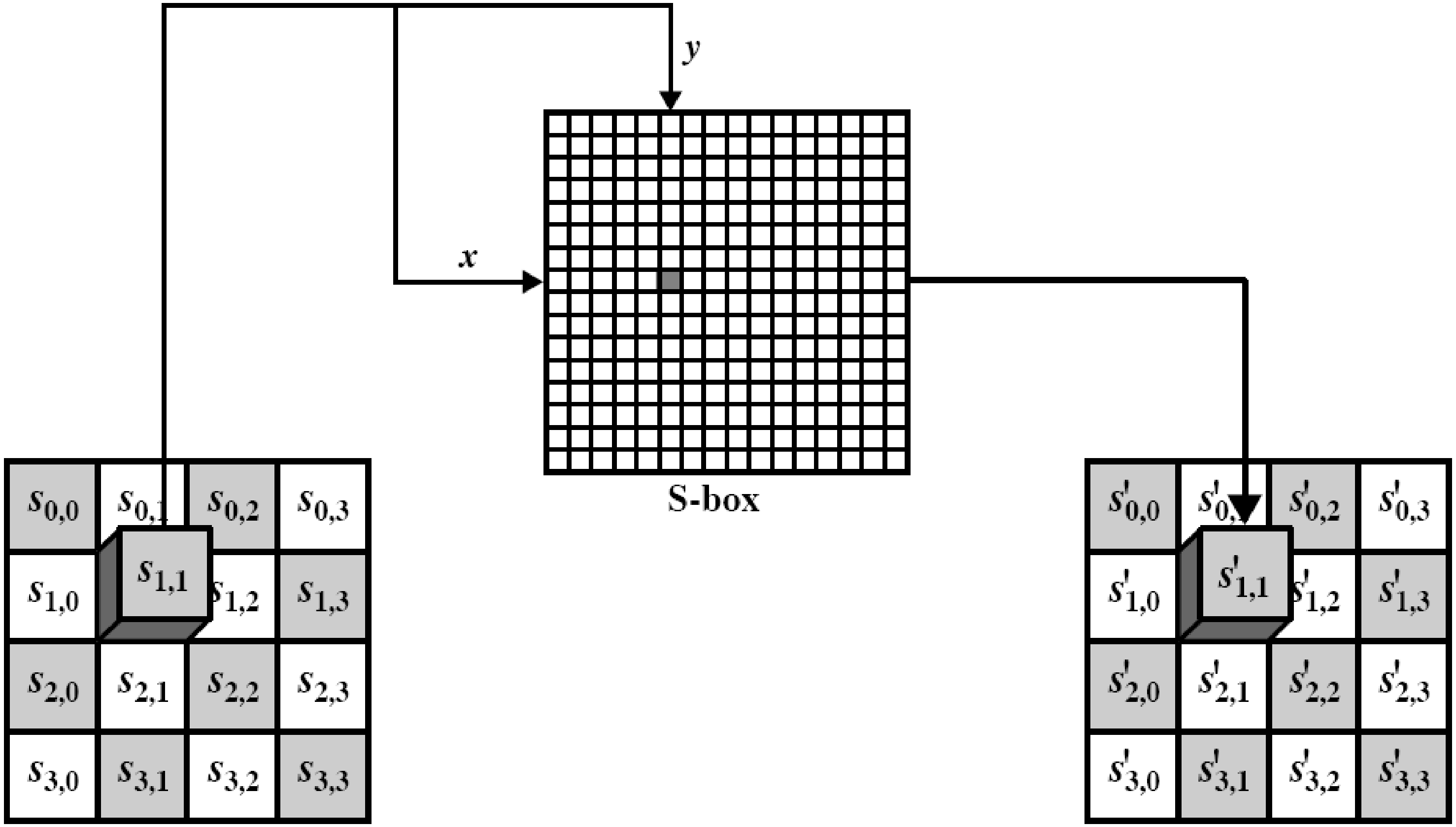
`AddRoundKey(State,`
`    RoundKey)`



AES - Substitute Bytes (SubBytes)

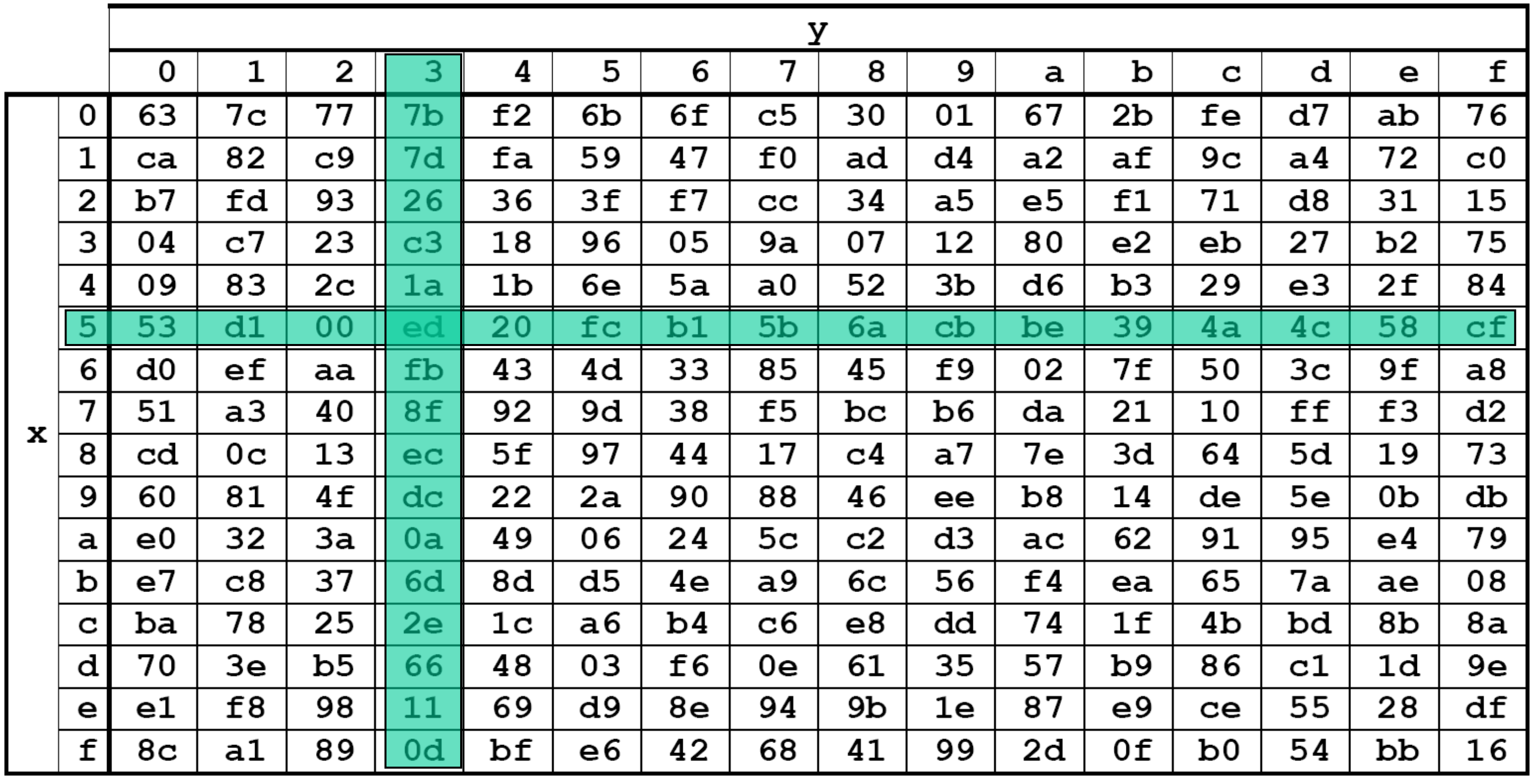
- Simple substitution on each byte of state independently
- Use an S-box of 16x16 bytes containing a permutation of all 256 possible 8-bit values
- Each byte of *State* is replaced by a new byte indexed by row (left 4-bits) & column (right 4-bits)
  - eg. byte {95} is replaced by {2A} in row 9 column 5
- S-box constructed using defined transformation of values in GF(2^8)
- Designed to be resistant to all known attacks

AES - Substitute Bytes


y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

AES - S-Box – Lookup Table

- Replace each byte in the state array with its corresponding value from the S-Box



		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES - Shift Rows

- A circular byte shift in each
  - 1st row is unchanged
  - 2nd row does 1 byte circular shift to left
  - 3rd row does 2 byte circular shift to left
  - 4th row does 3 byte circular shift to left
- Decrypt inverts using shifts to right
- Since state is processed by columns, this step permutes bytes between the columns

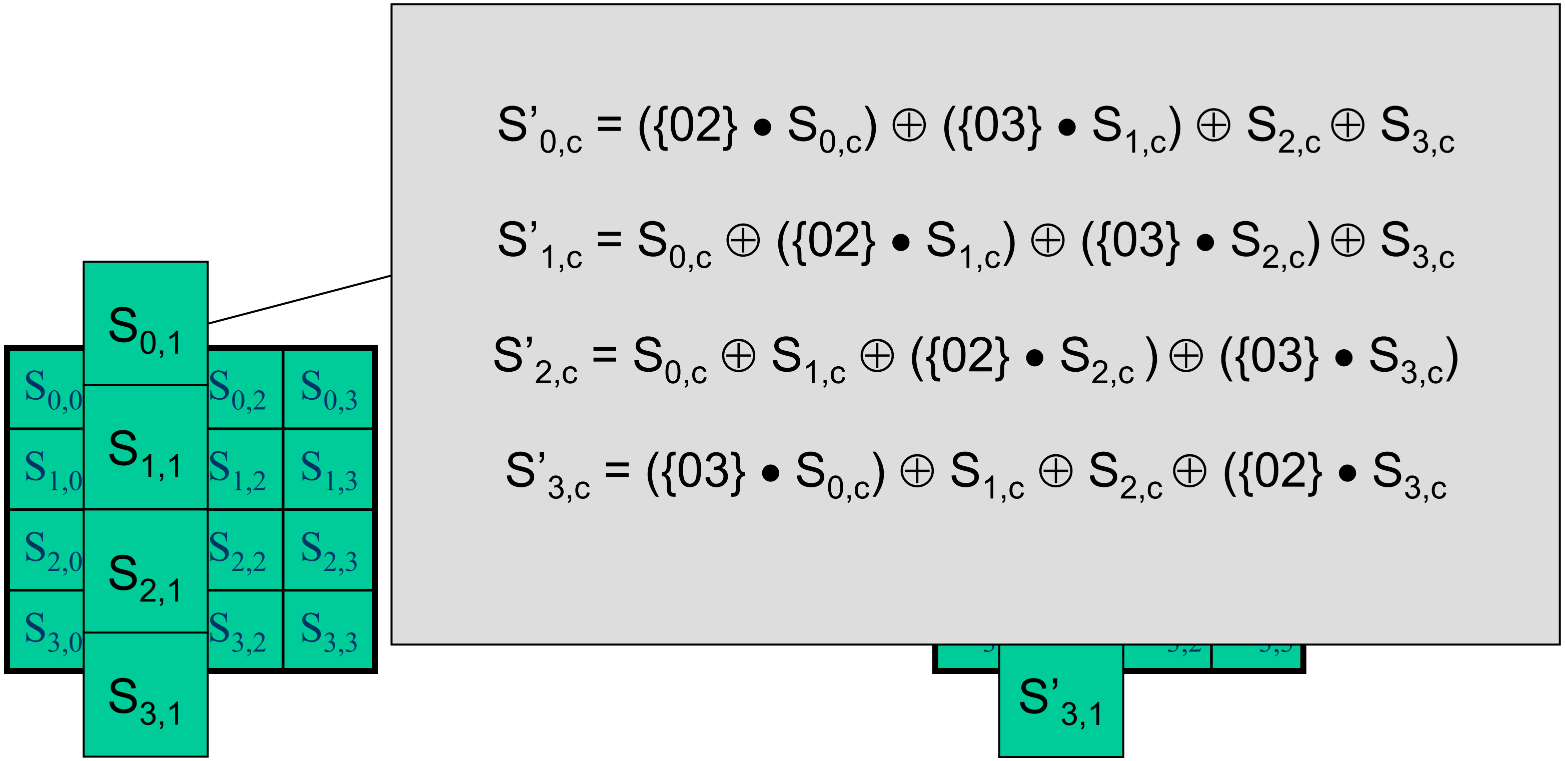
AES - Shift Rows

- Last three rows are cyclically shifted

			$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
		$S_{1,0}$	$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
	$S_{2,0}$	$S_{2,1}$	$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

AES - MixColumns

- Apply MixColumn transformation to each column



$$S'_{0,c} = (\{02\} \bullet S_{0,c}) \oplus (\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$

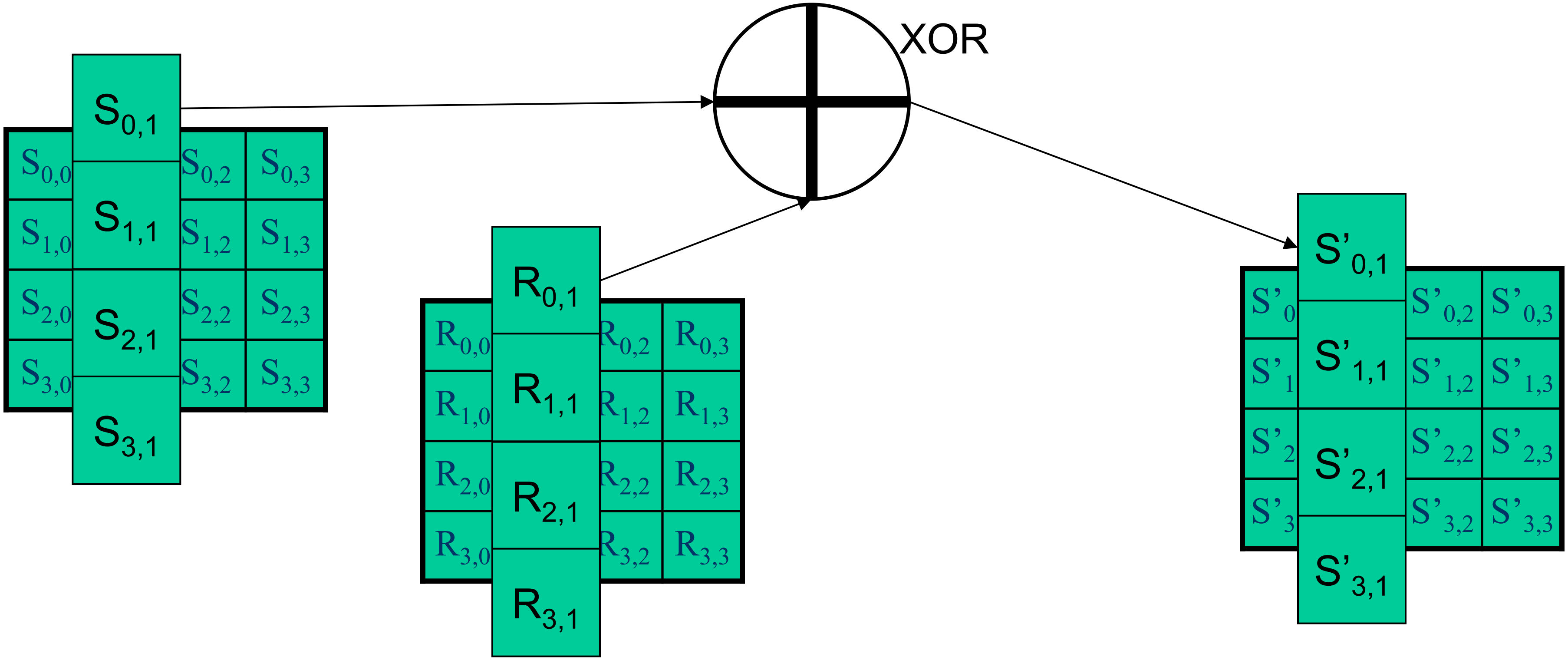
$$S'_{1,c} = S_{0,c} \oplus (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{3,c}$$

$$S'_{2,c} = S_{0,c} \oplus S_{1,c} \oplus (\{02\} \bullet S_{2,c}) \oplus (\{03\} \bullet S_{3,c})$$

$$S'_{3,c} = (\{03\} \bullet S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\} \bullet S_{3,c}$$

AES - AddRoundKey

- XOR each byte of the round key with its corresponding byte in the state array


XOR
$S_{0,1}$
$S_{0,0}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$R_{0,1}$
$R_{0,0}$ $R_{0,2}$ $R_{0,3}$
$R_{1,0}$ $R_{1,1}$ $R_{1,2}$ $R_{1,3}$
$R_{2,0}$ $R_{2,1}$ $R_{2,2}$ $R_{2,3}$
$R_{3,0}$ $R_{3,1}$ $R_{3,2}$ $R_{3,3}$
$S'_{0,1}$
S'_{0} $S'_{0,2}$ $S'_{0,3}$
S'_{1} $S'_{1,1}$ $S'_{1,2}$ $S'_{1,3}$
S'_{2} $S'_{2,1}$ $S'_{2,2}$ $S'_{2,3}$
S'_{3} $S'_{3,1}$ $S'_{3,2}$ $S'_{3,3}$

AES - Key Expansion

- KeyExpasion(key)

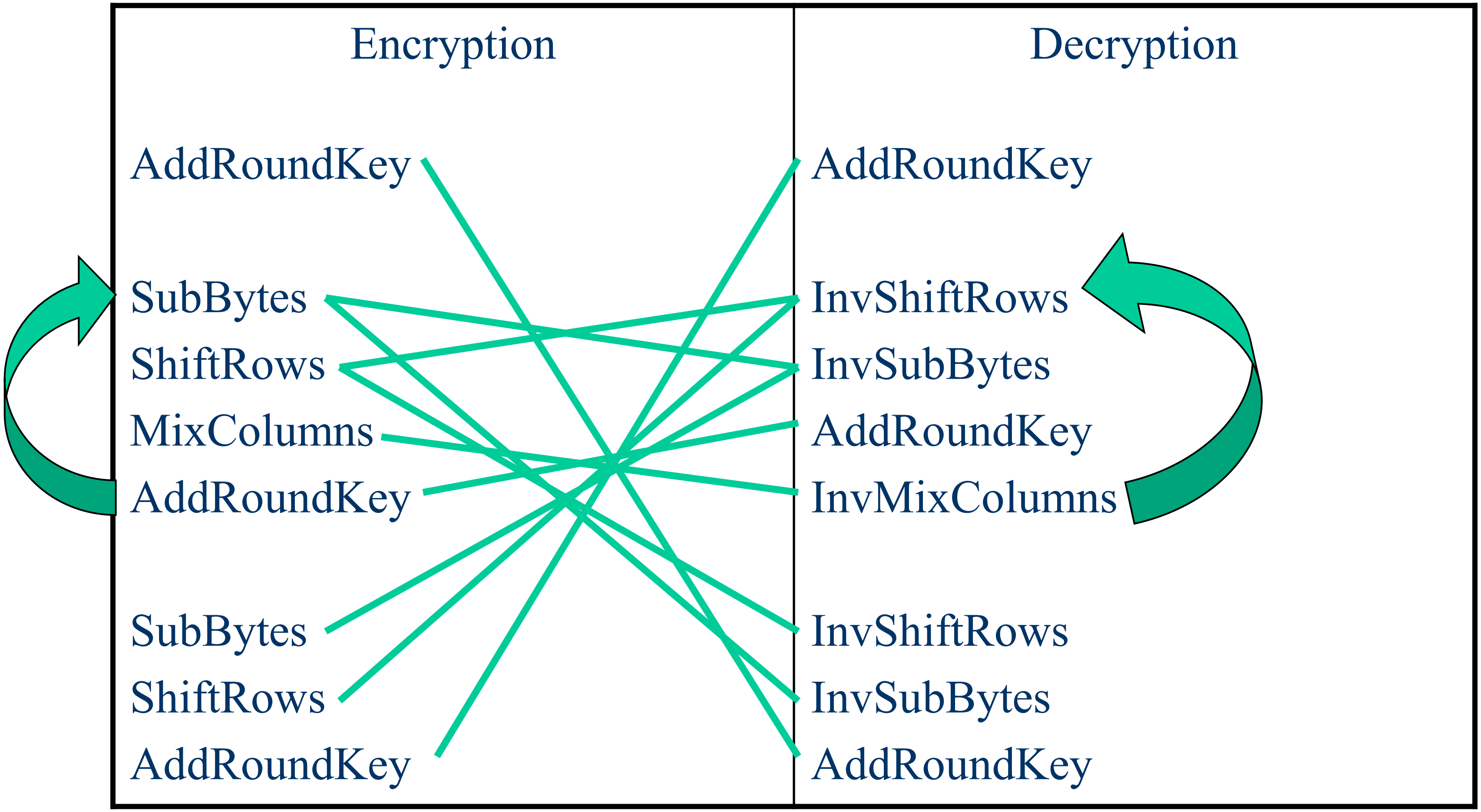
```
RCon[1] ← 0x01000000; RCon[2]  ← 0x02000000
RCon[3] ← 0x04000000; RCon[4]  ← 0x08000000
RCon[5] ← 0x10000000; RCon[6]  ← 0x20000000
RCon[7] ← 0x40000000; RCon[8]  ← 0x80000000
RCon[9] ← 0x01B00000; RCon[10] ← 0x36000000

for i ← 0 to 3 do
   w[i] ← (key[4i],key[4i+1],key[4i+2],key[4i+3])
for i ← 4 to 43 do
   temp ← w[i-1]
   if i ≡ 0 mod 4 then
       temp ← SubWord(RotWord(temp))⊕Rcon[i/4]
   w[i] ← w[i-4] ⊕temp
```

$\mathrm{RotWord}(B_0,B_1,B_2,B_3) = (B_1,B_2,B_3,B_0)$ $\mathrm{SubWord}(B_0,B_1,B_2,B_3) = \mathrm{SubBytes}(B_i),\ i = 0,1,2,3$

AES - Decryption

- AES decryption is not identical to encryption since steps are done in reverse
- But can define an equivalent inverse cipher with steps as for encryption
  - But using inverses of each step
  - With a different key schedule
- Works since the result is unchanged when:
  - Swap byte substitution & shift rows
  - Swap mix columns & add (tweaked) round key

AES - Encrypt *vs* Decrypt



Will AES survive until 2050?

- XSL Algebraic Attacks [Courtois & Pieprzyk 2002]
- 128-bit AES can be written as a system of 8000 quadratic equations with 1600 unknowns
  - Solving those equations breaks AES!
  - Only a few known plaintexts required (but ~2^{100} of work required)

“The XSL attack is not an attack. It is a dream.”

Vincent Rijmen (co-designer of AES)

- New attacks on AES-192 and AES-256 [Alex Biryukov, et al 2009]
  - which require 2^{176} and 2^{119} time, respectively
    - Within certain assumptions!

AES - Summary

- Designing and picking a cipher that will last 50 years is hard
- Mostly predictable advances in computing power
- Rapid but unpredictable advances in cryptanalysis
- Performance/security tradeoff keeps changing:
  - need something that is efficient today and still secure in 2050!!

Other block cipher algorthms

- RC6; Twofish; Serpent; Camellia
  - Block size: 128 bits; Key size:128, 192, or 256 bits
- IDEA
  - Block size: 64 bits; Key size 128 bits
- Threefish
  - Block and Key sizes: 256 to 1024 bits
- Blowfish
  - Block size: 64 bits ; Key size: 32 to 448 bits

RC6

- RC6 characteristics :
  - Block size: 128 bits
  - Key sizes of 128, 192 and 256 bits
  - Number of *rounds*: 20 (depends on the security level)
  - Feistel network based
  - Key Expansion produces the array S[0, … $2r + 3$], of w-bit *round keys.*
- Operations:
  - Data-dependent rotations
  - Modular additions
  - XOR operations
  - Multiplication

RC6 is a patented encryption algorithm

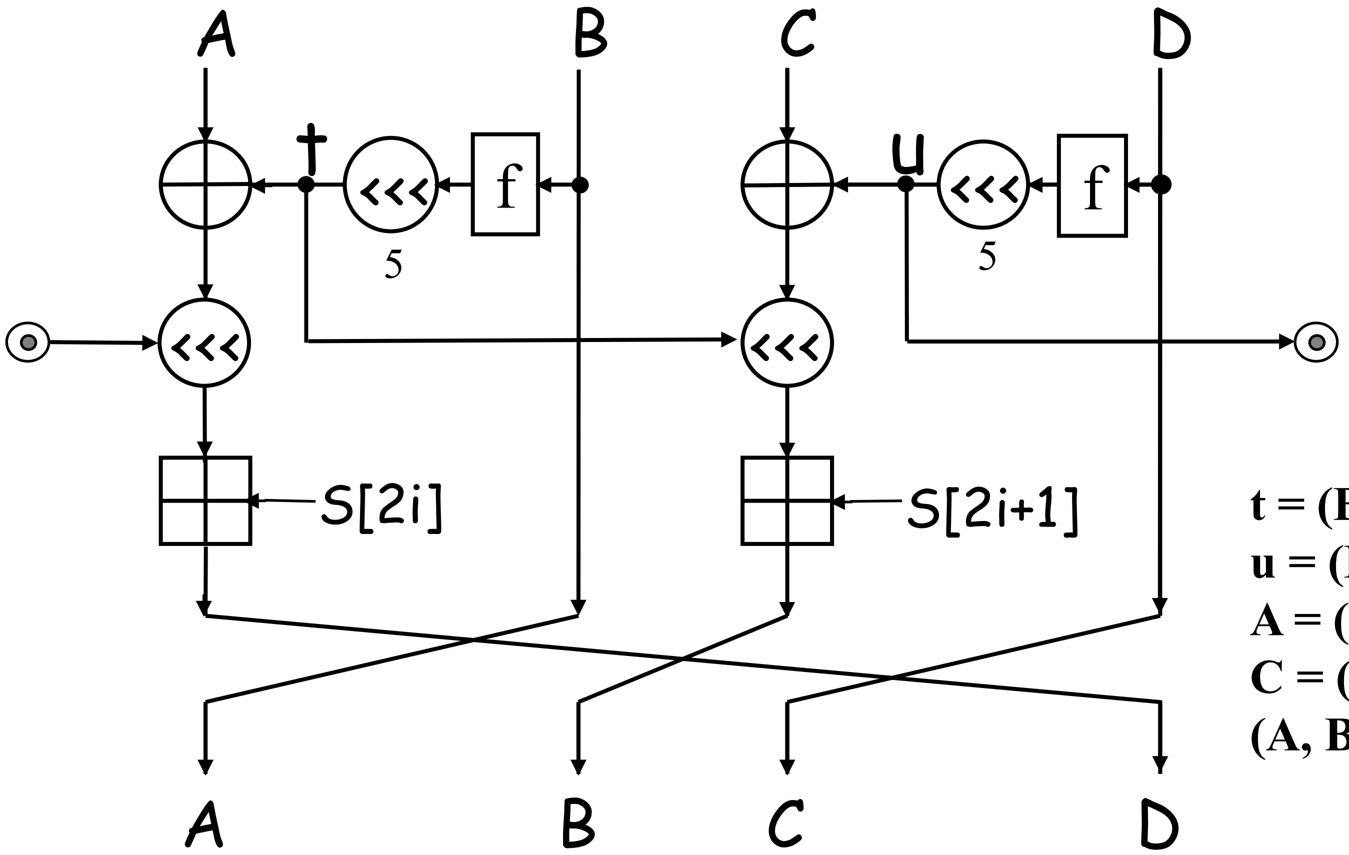
RC6 Encryption

- Augmented RC5 encryption algorithm

```
$B = B + S[0]$
$D = D + S[1]$
for $i = 1$ to 20 do
    $t = (B \times (2B + 1)) <<< 5$
    $u = (D \times (2D + 1)) <<< 5$
    $A = ((A \oplus t) <<< u) + S[2i]$
    $C = ((C \oplus u) <<< t) + S[2i + 1]$
    $(A, B, C, D) = (B, C, D, A)$
$A = A + S[42]$
$C = C + S[43]$
```

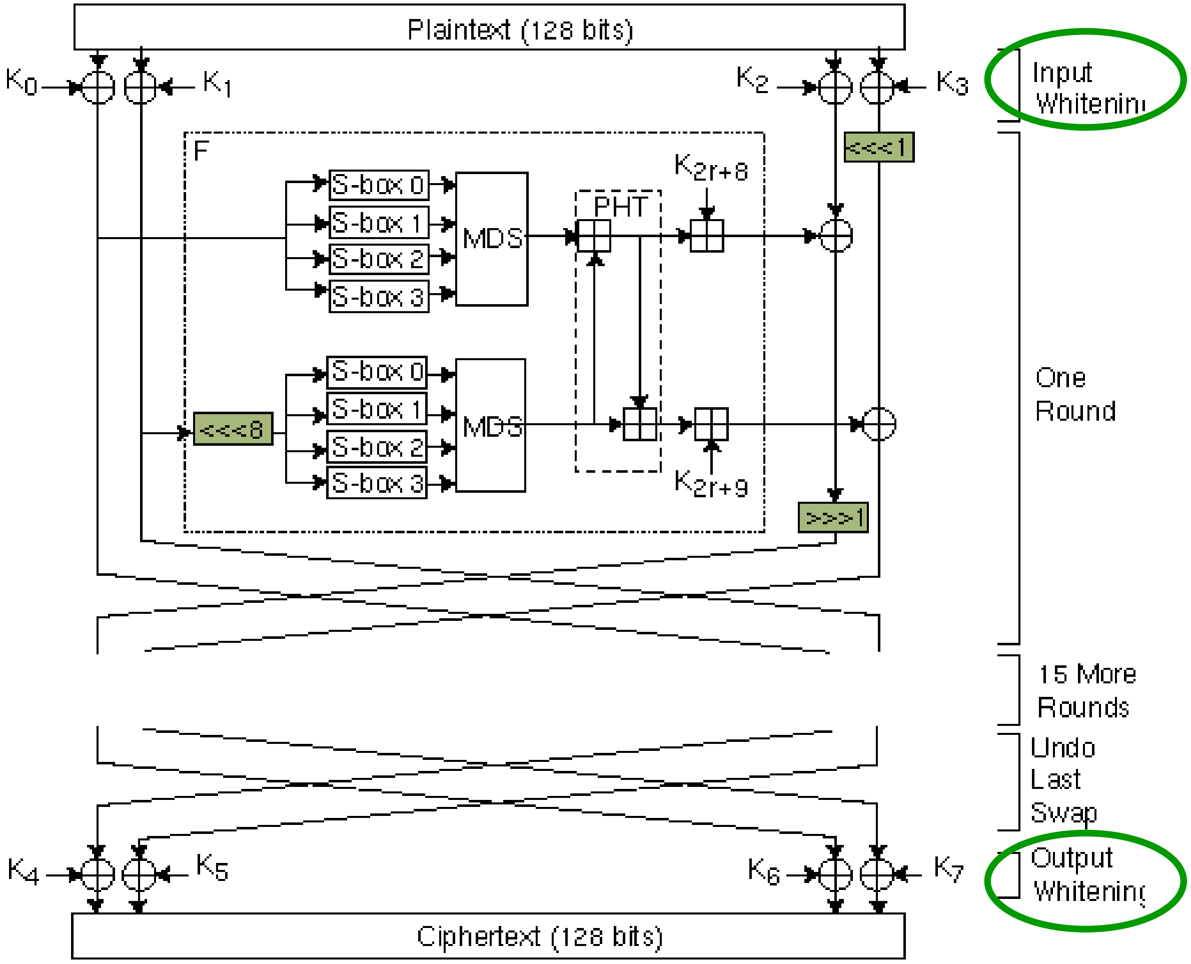
20 rounds for higher security

One Round of RC6



t = (B*(2B + 1)) <<< lg w
u = (D*(2D + 1)) <<< lg w
A = ((A ^ t) <<< u) + S[2i]
C = ((C ^ u) <<< t) + S[2i + 1]
(A, B, C, D) = (B, C, D, A)

Two Fish


Plaintext (128 bits)
K0
K1
K2
K3
Input
Whitenin
F
<<<1
K2r+8
S-box 0
S-box 1
S-box 2
S-box 3
MDS
PHT
<<<8
S-box 0
S-box 1
S-box 2
S-box 3
MDS
K2r+9
>>>1
One
Round
15 More
Rounds
Undo
Last
Swap
K4
K5
K6
K7
Output
Whitening
Ciphertext (128 bits)

Stream Ciphers

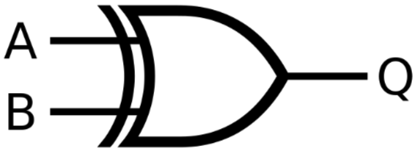
Stream Ciphers

- Mix the plaintext with a secret key
  - Done bit by bit
- Basic operation

Input data	: 1001 1010 0010 1011 … 0
Mix function	: XOR
Encryption Key	: 1101 0100 0101 0001 ….1
Output data	: 0100 1110 0111 1010 ….1
Decryption key	: ????

Perfectly Secure Cipher: One-Time Pad

- Mauborgne/Vernam [1917]



- XOR (⊕):
  - $0 \oplus 0 = 0 \quad 1 \oplus 0 = 1 \rightarrow \quad a \oplus 0 = a$
  - $0 \oplus 1 = 1 \quad 1 \oplus 1 = 0 \rightarrow \quad a \oplus 1 = \text{not } a$

- Encrypt
  - $E(P, K) = P \oplus K = C$
    - P = plaintext; K = key
- Decrypt
  - $D(C, K) = C \oplus K = (P \oplus K) \oplus K = P$

One-Time Pad Problems

- Security is based on the assumption that K is never reused
  - What if one has two encrypted messages:

$$C_1 = P_1 \oplus K \text{ and } C_2 = P_2 \oplus K$$

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K$$

$$= P_1 \oplus P_2$$

- Need to generate truly random bit sequence
  - As long as all messages

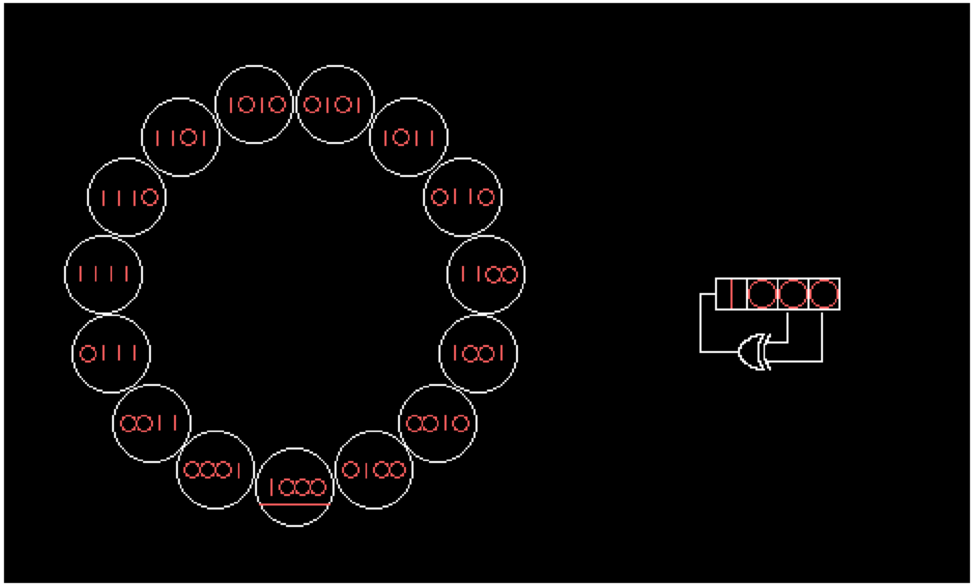
- Need to securely distribute key bit sequence:
  - We can use Quantum Key distribution is available!

Symmetric Stream Ciphers

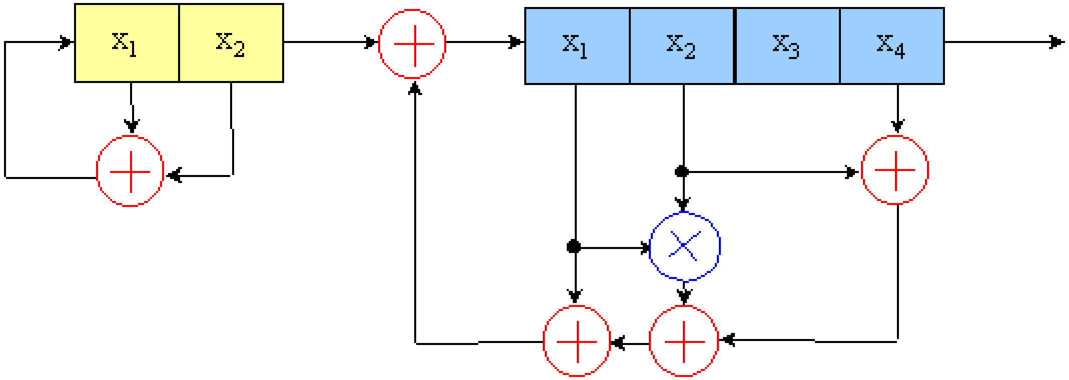
- Used approximations
  - Secure pseudo-random generators
    - Based on LFSRs (Linear Feedback Shift Registers) → next
    - Based on block ciphers → later
    - Other approximations (nonlinear functions, etc.)
  - Usually without self-synchronization
    - Receiver must know when encrypted data begins
- Most common algorithms
  - A5 (GSM)
  - SEAL
  - Trivium
  - Salsa20
  - ChaCha20 (used in HTTPS, OpenVPN)

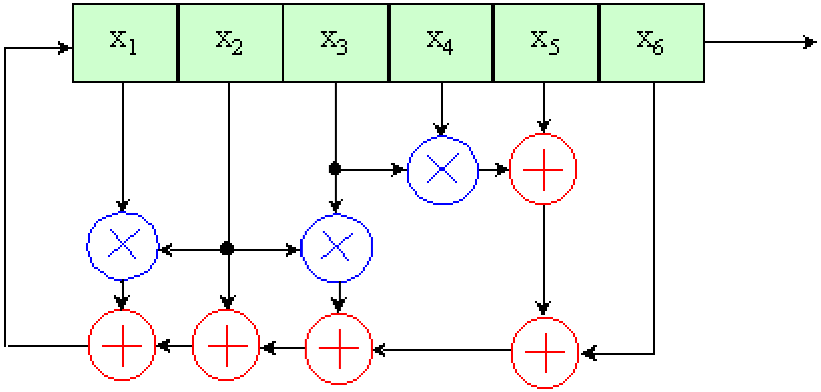
Linear Feedback Shift Register Sequence

- A very simple unsecure example:
  - 4 bit Linear Feedback Shift Register (LFSR)



Non Linear Feedback Shift Register

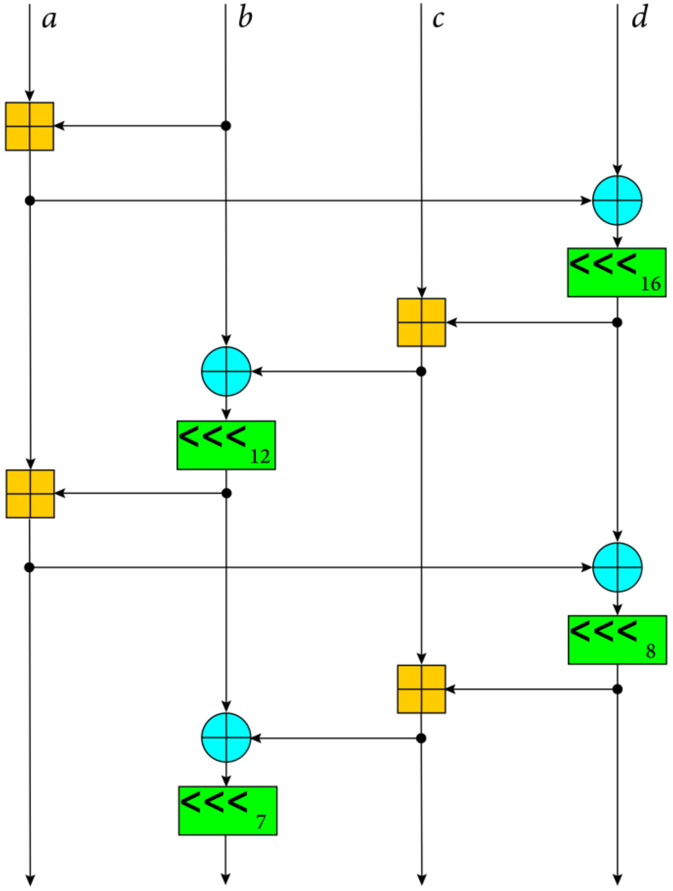




ChaCha20

- ChaCha20
  - Stream Cipher
    - the core processes the key and a counter to produce a keystream
    - each block increments the counter
  - 20 rounds doing basic arithmetic operations
  - Lightweight
    - Particularly in mobile/embedded systems
  - Key sizes of 128 or 256 bits

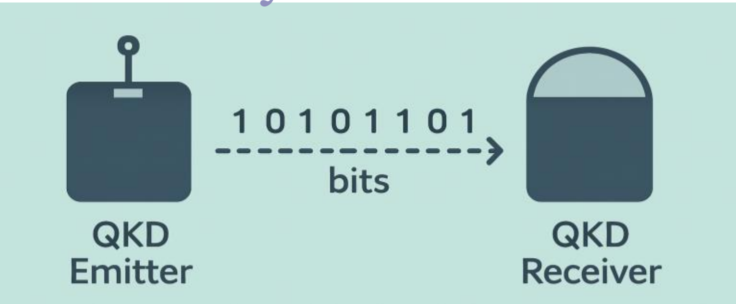
- Used in:
  - HTTPS (TLS)
  - OpenVPN
  - SSH
    - But can be partially attacked



ChaCha20 round computation

The Quantum Key Distribution Approach

- Quantum Key Distribution (QKD)
    - AKA: Quantum Cryptography
  - The Stream cipher key is exchanged by a Quantum System
    - Alice sends random photons
      - either horizontal (0) or vertically polarized (1)
    - Bob receives these random photons / bits
  - We know have random bit to be used as keys
    - the Encryption Key
      - aka, the keystream!



Acknowledgments

Prof. David Evans @ University of Virginia
Cryptology - Principles and Applications

Prof. Hyunsoo Yoon @ KAIST
Cryptography & Network Security

Prof. Tim van der Horst @ BYU
Kent Seamons @ BYU
Computer Security

CARLOS **PIRES**

Carlos Pires has graduated in Physical Engineering from the Faculty of Sciences of the University of Lisbon and, by the same university, he did a master's degree in Physical Engineering. In 2007, he started his duties at the Speed Laboratory of the National Metrology Laboratory, of the Portuguese Institute for Quality. In 2015, assumes the functions of head for the Time and Frequency domain, having as main function to carry out and disseminate the second, as well as to provide traceability to the unit at national level. He currently serves as Chair of the Time and Frequency Technical Committee (TC-TF) of EURAMET.

ABSTRACT

SECURE TIME TRANSFER

ABSTRACT

This presentation discusses the concepts and techniques of time and frequency transfer, with a particular focus on secure time transfer. The dissemination of time is a prerequisite for the availability of correct time within a country, which is essential for diverse applications. These range from Positioning, Navigation and Timing (PNT) in defence and sensing to fundamental scientific applications like the definition of constants and relativistic geodesy. Requirements for timing and synchronization vary widely, from milliseconds (ms) to nanoseconds (ns) with stability of 1×10^{-11} to 1×10^{-13} for some applications, to nanoseconds (ns) to picoseconds (ps) with stability of 1×10^{-13} to 1×10^{-16}, reaching picoseconds (ps) and better (1×10^{-18}) for the most demanding applications. Techniques for time and frequency transfer are diverse. These include two methods recommended by the BIPM (Bureau International des Poids et Mesures) to compare the national reference time scales to the international reference time scale UTC (Coordinated Universal Time). The Common-View method and the Two-Way Satellite Time and Frequency Transfer (TWSTFT) can be used to link entities such as UTC(IPQ), NIST, and PTB. Optical Carrier offers the best ultra stable frequency service performances, characterized by low noise, no interference, and excellent reciprocity. It has been operated in different setups, including dark channel and dark fibre, though it typically requires frequency combs for end-users and highly trained personnel. ELSTAB is another method that distributes time and frequency services using active cancellation with electronic delays. White Rabbit PTP is presented as an easy-to-use and affordable option, providing time and frequency services with performances only slightly better than GNSS.

Secure time transfer is a crucial aspect, ensuring not just precise time, but trustworthy time. This process synchronizes clocks between systems or devices in a way that protects against tampering, spoofing, or unauthorized manipulation of time data. It is vital for systems requiring precise and trustworthy timestamps, such as financial systems, military operations, critical infrastructure (e.g., power grids, aviation), and blockchain/cryptographic protocols. Key aspects of secure time transfer include: Authentication to ensure that time source is legitimate, Integrity to guarantee that time data has not been modified in transit, Confidentiality to protect time transfer data from interception, Accuracy to maintain high-precision synchronization, and Resilience to detect and resist attacks like GNSS spoofing/jamming, delay attacks, and man-in-the-middle attacks. Common protocols for secure time transfer include Network Time Protocol (NTP) with authentication extensions like Network Time Security (NTS), and Precision Time Protocol (PTP) with security profiles (e.g., IEEE 1588 with secure extensions).More advanced, quantum-secure time transfer explores properties of quantum mechanics. Main approaches include:

- Quantum Key Distribution (QKD) + Classical Time Protocols: QKD uses quantum properties of photons to securely distribute encryption keys, which are then used to authenticate and encrypt time transfer data. Any eavesdropping attempt on the quantum channel reveals the intrusion.

- Two-Way Quantum Time Transfer: Similar to classical two-way methods, but enhanced by sending single photons or entangled particles. It uses quantum correlations to measure precise delays and detect tampering, allowing sub-nanosecond timing accuracy with high tamper resistance.

- Entanglement-Based Synchronization (experimental): This uses quantum entanglement between particles at two locations. The time correlation of entangled states enables clock synchronization without requiring direct signal transmission, offering potential for ultra-secure and covert synchronization.

Secure time transfer

PTQCI
PORTUGUESE
QUANTUM COMMUNICATION INFRASTRUCTURE

SI
kg
m
s
A
K
mol
cd
h
c
Δν
e
k
N_A
K_cd

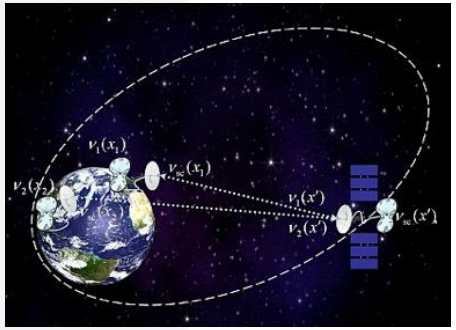
Instituto
Português
da Qualidade

Time and frequency transfer

Sensing/Defense:
Positioning, Navigation and Timing

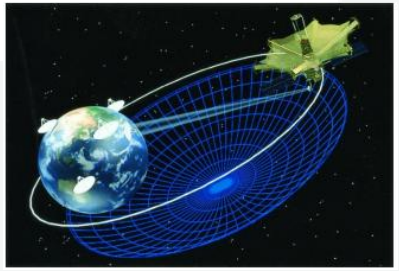
Requirements:
Timing and syntonisation:
ms to ns; 1×10^{-11} to 1×10^{-13}

Fundamental Scientific Applications
Definition & Variations in fundamental constants

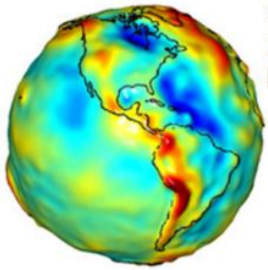


Requirements:
Timing and syntonisation:
Best possible

Very Long Baseline Interferometry

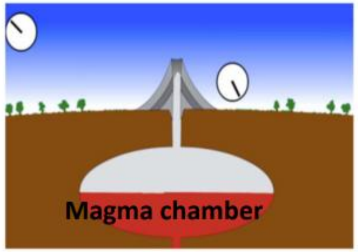


Requirements:
Timing and syntonisation:
ns to ps; 1×10^{-13} to 1×10^{-16}



10 $^{-18}$
1 cm
height

Relativistic geodesy

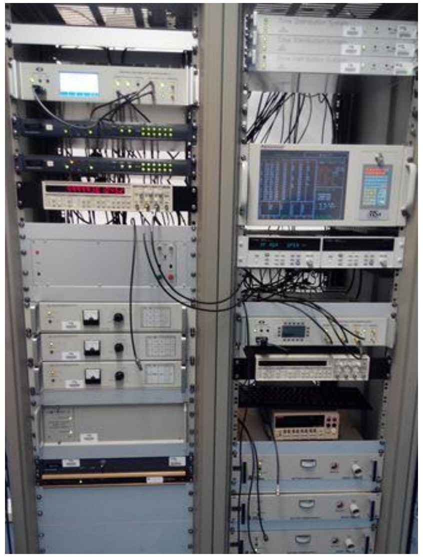


Gravity Sensor

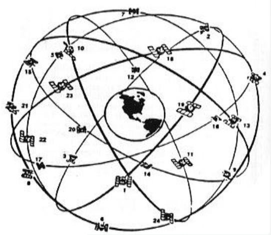
Requirements:
Timing and syntonisation:
ps; 1×10^{-18} and better

Time and frequency transfer

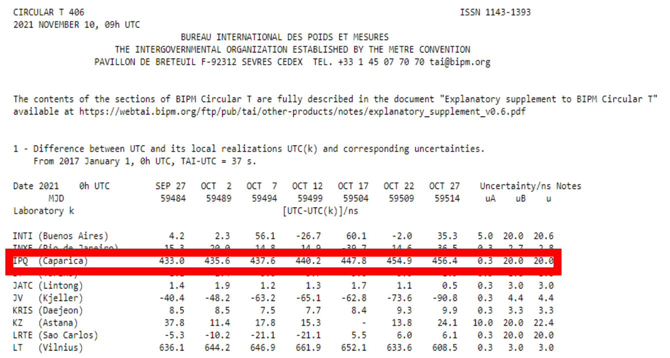
Time transfer



Common-View method



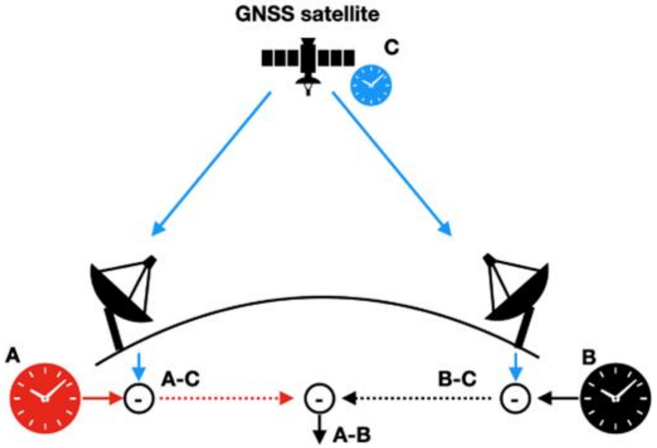
GNSS



```
CIRCULAR T 406                                                    ISSN 1143-1393
2021 NOVEMBER 10, 09h UTC
                              BUREAU INTERNATIONAL DES POIDS ET MESURES
                     THE INTERGOVERNMENTAL ORGANIZATION ESTABLISHED BY THE METRE CONVENTION
                 PAVILLON DE BRETEUIL F-92312 SEVRES CEDEX  TEL. +33 1 45 07 70 70 tai@bipm.org


The contents of the sections of BIPM Circular T are fully described in the document "Explanatory supplement to BIPM Circular T"
available at https://webtai.bipm.org/ftp/pub/tai/other-products/notes/explanatory_supplement_v0.6.pdf


1 - Difference between UTC and its local realizations UTC(k) and corresponding uncertainties.
    From 2017 January 1, 0h UTC, TAI-UTC = 37 s.

Date 2021    0h UTC        SEP 27   OCT  2   OCT  7   OCT 12   OCT 17   OCT 22   OCT 27    Uncertainty/ns Notes
       MJD                  59484    59489    59494    59499    59504    59509    59514     uA    uB    u
Laboratory k                                    [UTC-UTC(k)]/ns

INTI (Buenos Aires)           4.2      2.3     56.1    -26.7     60.1     -2.0     35.3    5.0  20.0  20.6
INXE (Rio de Janeiro)        15.3     20.0     14.8     14.9    -39.7     14.6     36.5    0.3   2.7   2.8
IPQ  (Caparica)             433.0    435.6    437.6    440.2    447.8    454.9    456.4    0.3  20.0  20.0
IT   (Torino)               [illegible]
JATC (Lintong)                1.4      1.9      1.2      1.3      1.7      1.1      0.5    0.3   3.0   3.0
JV   (Kjeller)              -40.4    -48.2    -63.2    -65.1    -62.8    -73.6    -90.8    0.3   4.4   4.4
KRIS (Daejeon)                8.5      8.5      7.5      7.7      8.4      9.3      9.9    0.3   3.3   3.3
KZ   (Astana)                37.8     11.4     17.8     15.3       -      13.8     24.1   10.0  20.0  22.4
LRTE (Sao Carlos)            -5.3    -10.2    -21.1    -21.1      5.5      6.0      6.1    0.3  20.0  20.0
LT   (Vilnius)              636.1    644.2    646.9    661.9    652.1    633.6    608.5    0.3   3.0   3.0
```

→ UTC(IPQ)

GNSS time-transfer

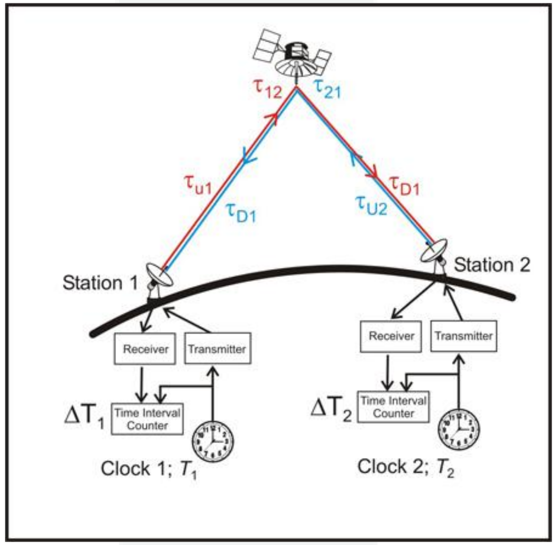


NIST

$$A - B - (d_A - d_B) = [A - GNSS - d_A] - [B - GNSS - d_B]$$

Time and frequency transfer

TWSTFT



PTB

$$\mathrm{TIC(B)} = \mathrm{B} - \mathrm{A} + d_{TA} + d_{AS} + d_{SAB} + d_{SB} + d_{RB} + S_A$$

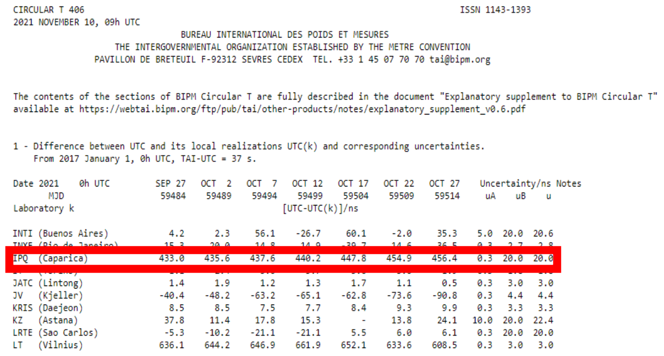
$$\mathrm{TIC(A)} = \mathrm{A} - \mathrm{B} + d_{TB} + d_{BS} + d_{SBA} + d_{SA} + d_{RA} + S_B$$

$\mathrm{A} - \mathrm{B} = [\mathrm{TIC(A)} - \mathrm{TIC(B)}] / 2$	TIC readings
$+ (d_{TA} - d_{RA}) / 2 - (d_{TB} - d_{RB}) / 2$	Earth station equipment
$+ (d_{AS} - d_{SA}) / 2 - (d_{BS} - d_{SB}) / 2$	Propagation delay
$+ (d_{SAB} - d_{SBA}) / 2$	Delay in satellite
$- 2\omega\,Ar/c^2$	Sagnac effect

NIST: https://www.nist.gov/pml/time-and-frequency-division/time-distribution/two-way-satellite-time-and-frequency-transfer

UTC(IPQ)

CIRCULAR-T

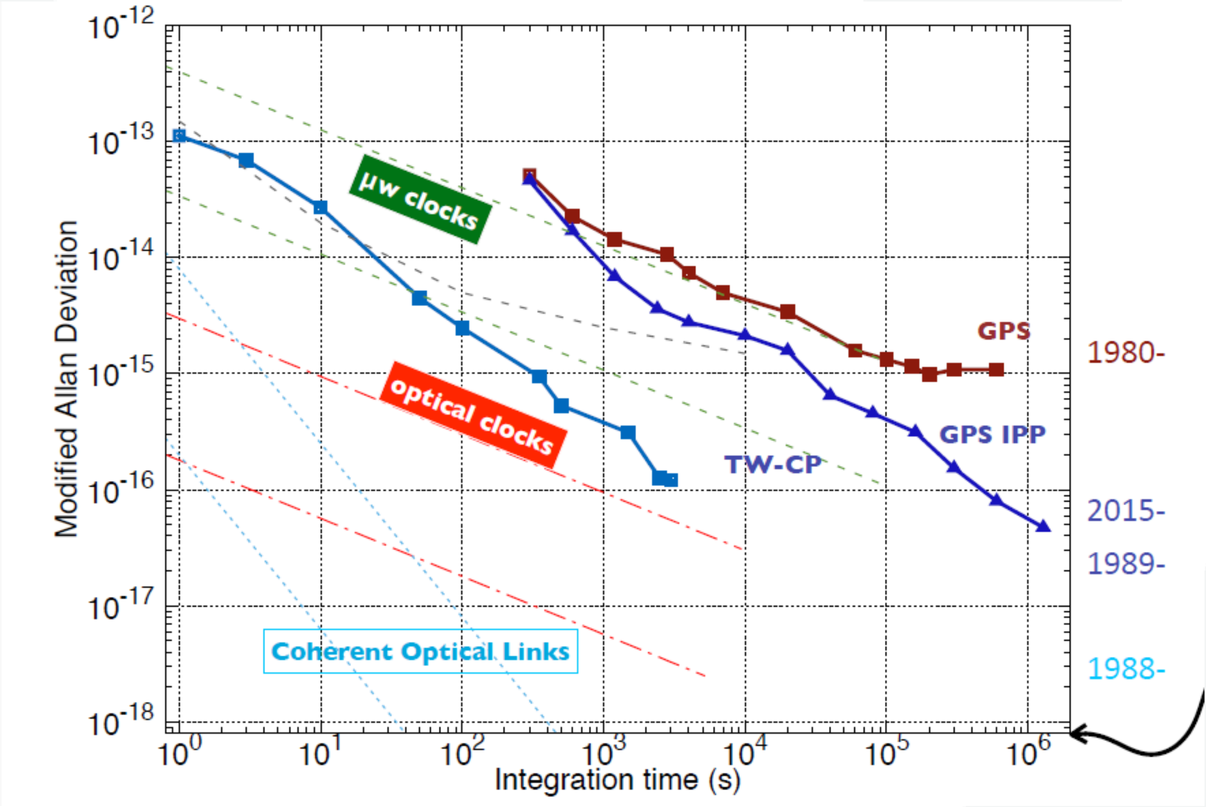


```
CIRCULAR T 406                                                        ISSN 1143-1393
2021 NOVEMBER 10, 09h UTC
                              BUREAU INTERNATIONAL DES POIDS ET MESURES
                     THE INTERGOVERNMENTAL ORGANIZATION ESTABLISHED BY THE METRE CONVENTION
                  PAVILLON DE BRETEUIL F-92312 SEVRES CEDEX  TEL. +33 1 45 07 70 70 tai@bipm.org


The contents of the sections of BIPM Circular T are fully described in the document "Explanatory supplement to BIPM Circular T"
available at https://webtai.bipm.org/ftp/pub/tai/other-products/notes/explanatory_supplement_v0.6.pdf


1 - Difference between UTC and its local realizations UTC(k) and corresponding uncertainties.
   From 2017 January 1, 0h UTC, TAI-UTC = 37 s.

Date 2021    0h UTC         SEP 27   OCT  2   OCT  7   OCT 12   OCT 17   OCT 22   OCT 27    Uncertainty/ns Notes
      MJD                    59484    59489    59494    59499    59504    59509    59514     uA    uB    u
Laboratory k                                        [UTC-UTC(k)]/ns

INTI (Buenos Aires)            4.2      2.3     56.1    -26.7     60.1     -2.0     35.3    5.0  20.0  20.6
INXE (Rio de Janeiro)         15.3     20.0     14.8     14.9    -39.7     14.6     36.5    0.3   2.7   2.8
IPQ  (Caparica)              433.0    435.6    437.6    440.2    447.8    454.9    456.4    0.3  20.0  20.0
[illegible]
JATC (Lintong)                 1.4      1.9      1.2      1.3      1.7      1.1      0.5    0.3   3.0   3.0
JV   (Kjeller)               -40.4    -48.2    -63.2    -65.1    -62.8    -73.6    -90.8    0.3   4.4   4.4
KRIS (Daejeon)                 8.5      8.5      7.5      7.7      8.4      9.3      9.9    0.3   3.3   3.3
KZ   (Astana)                 37.8     11.4     17.8     15.3        -     13.8     24.1   10.0  20.0  22.4
LRTE (Sao Carlos)             -5.3    -10.2    -21.1    -21.1      5.5      6.0      6.1    0.3  20.0  20.0
LT   (Vilnius)               636.1    644.2    646.9    661.9    652.1    633.6    608.5    0.3   3.0   3.0
```

Time and frequency transfer

IPQ

Motivations for time and frequency dissemination



O. Lopez *et al.*, CRAS, 16 (5), pp. 459-586 (2015) (2015)

GOAL for the SI second redefinition

Fiber links

Pro

- Low noise
- No interference
- Excellent reciprocity
- Low optical noise

Contra

- Point to point
- Cost

Time and frequency transfer

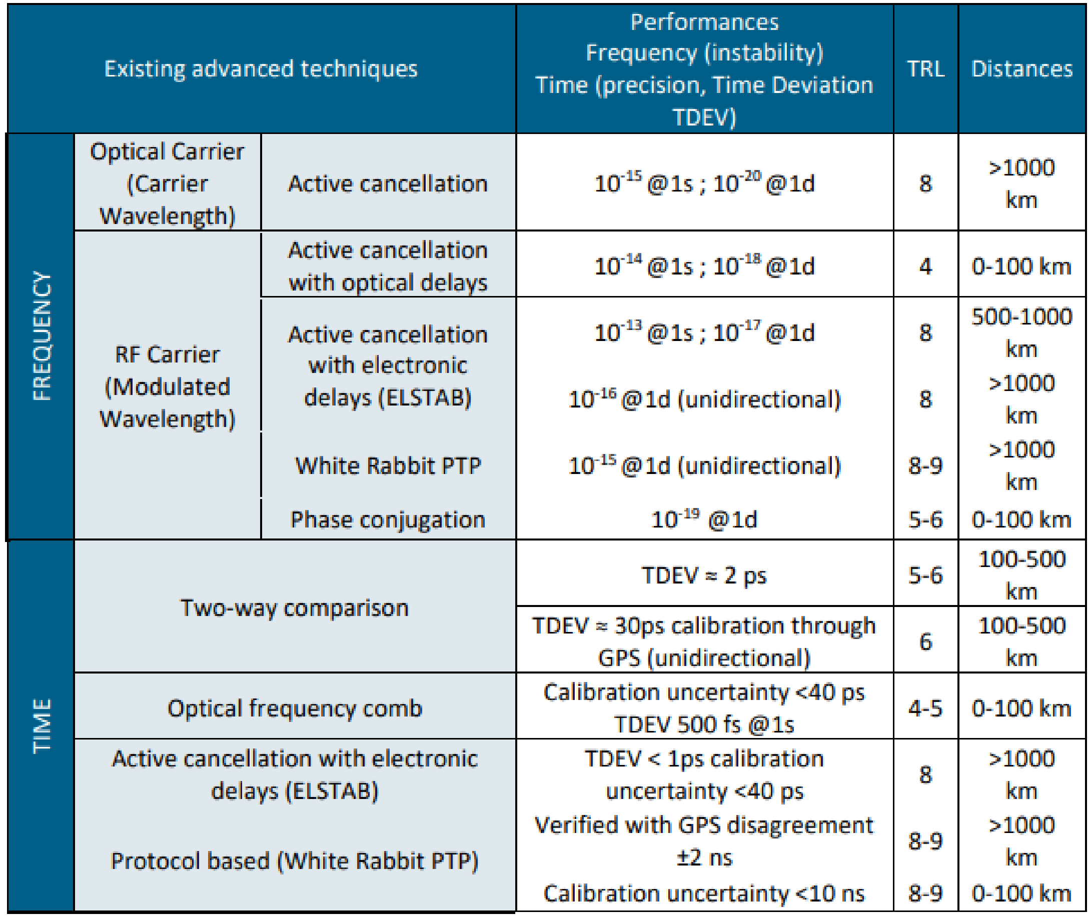
Techniques for time and frequency dissemination

The dissemination of legal time is the prerequisite for the availability of the correct time in the country

Techniques	Advantages	Disadvantages
Optical Carrier	• Best ultrastable frequency • service performances. • Has been operated in different • setups (dark channel and dark • fibre).	• A limited number (but more demanding) of end-users because frequency combs are required to use the distributed signal. • Industrialized equipment is designed to work @ 194.4THz in C-Band. • Alternative systems using other frequencies are being deployed and are to be tested in the real field. • Requires highly trained personnel.
ELSTAB Active cancellation with electronic delays	• Distributions Time and Frequency services. • Wavelength is fixed but can be chosen all over C-Band to fit any ITU channel.	• Even greater performances might be required for the most demanding end users (optical clock comparisons).
White Rabbit **PTP**	• Easy to use. • A wide range of potential endusers. • Time and Frequency service. • Affordable prices.	• Performances only slightly better than GPS.

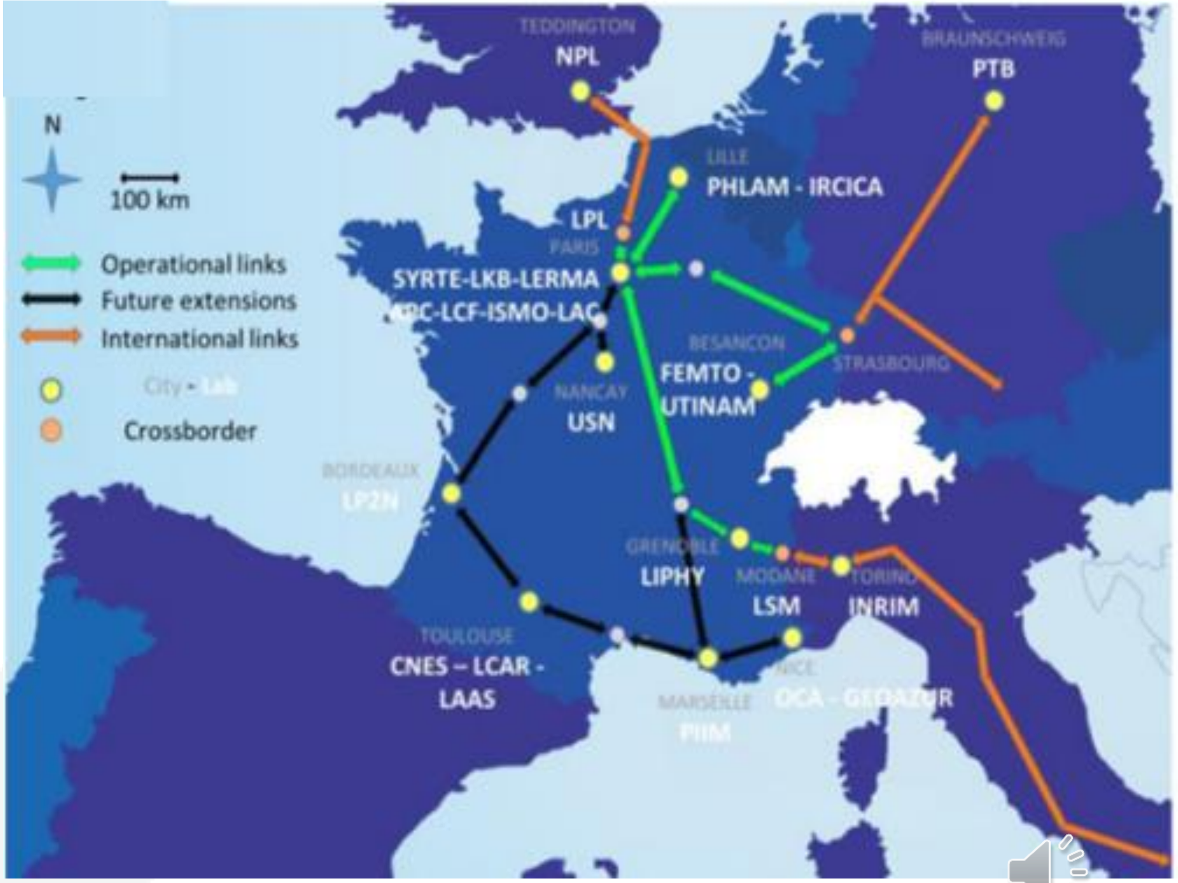
Time and frequency transfer

Time and frequency dissemination



Existing advanced techniques			Performances Frequency (instability) Time (precision, Time Deviation TDEV)	TRL	Distances
FREQUENCY	Optical Carrier (Carrier Wavelength)	Active cancellation	10^{-15} @1s ; 10^{-20} @1d	8	>1000 km
	RF Carrier (Modulated Wavelength)	Active cancellation with optical delays	10^{-14} @1s ; 10^{-18} @1d	4	0-100 km
		Active cancellation with electronic delays (ELSTAB)	10^{-13} @1s ; 10^{-17} @1d	8	500-1000 km
			10^{-16} @1d (unidirectional)	8	>1000 km
		White Rabbit PTP	10^{-15} @1d (unidirectional)	8-9	>1000 km
		Phase conjugation	10^{-19} @1d	5-6	0-100 km
TIME	Two-way comparison		TDEV ≈ 2 ps	5-6	100-500 km
			TDEV ≈ 30ps calibration through GPS (unidirectional)	6	100-500 km
	Optical frequency comb		Calibration uncertainty <40 ps TDEV 500 fs @1s	4-5	0-100 km
	Active cancellation with electronic delays (ELSTAB)		TDEV < 1ps calibration uncertainty <40 ps	8	>1000 km
	Protocol based (White Rabbit PTP)		Verified with GPS disagreement ±2 ns	8-9	>1000 km
			Calibration uncertainty <10 ns	8-9	0-100 km

GEANT



https://doi.org/10.1088/1367-2630/abe79e

Secure time transfer

Secure time transfer ensures not just precise time — but trustworthy time

Secure time transfer is the process of synchronizing clocks between systems or devices in a way that protects against tampering, spoofing, or unauthorized manipulation of time data. This is crucial for systems where precise and trustworthy timestamps are essential, such as in:

- Financial systems
- Military operations
- Critical infrastructure (e.g., power grids, aviation)
- Blockchain and cryptographic protocols

Secure time transfer

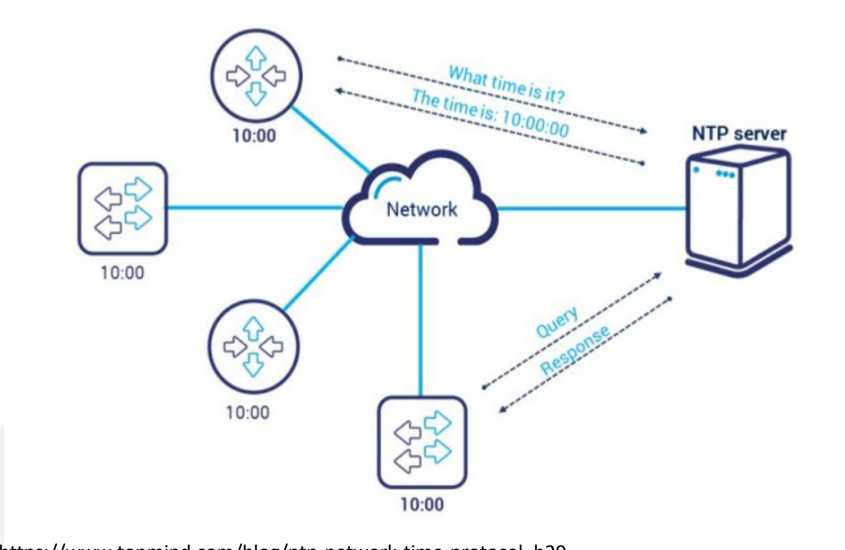
Key Aspects of Secure Time Transfer

- Authentication: Ensures that the time source is legitimate and hasn’t been spoofed (e.g., a fake GPS signal).
- Integrity: Guarantees that time data hasn't been modified in transit.
- Confidentiality (sometimes): Protects time transfer data from being intercepted or analyzed.
- Accuracy: Maintains high-precision synchronization between devices or systems.
- Resilience: Detects and resists attacks such as:
    - GPS spoofing/jamming
    - Delay attacks (introducing latency to manipulate timestamps)
    - Man-in-the-middle attacks

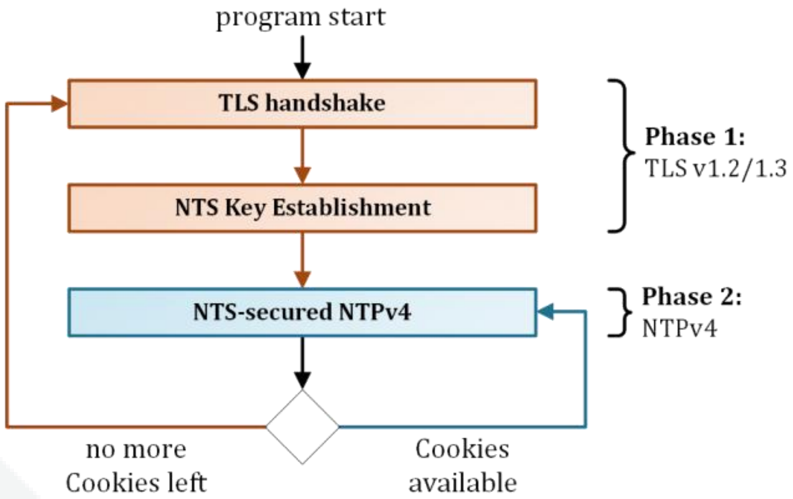
Secure time transfer

Common Protocols and Technologies

- NTP (Network Time Protocol) with authentication extensions (e.g., NTS – Network Time Security)



https://www.tonmind.com/blog/ntp-network-time-protocol_b29

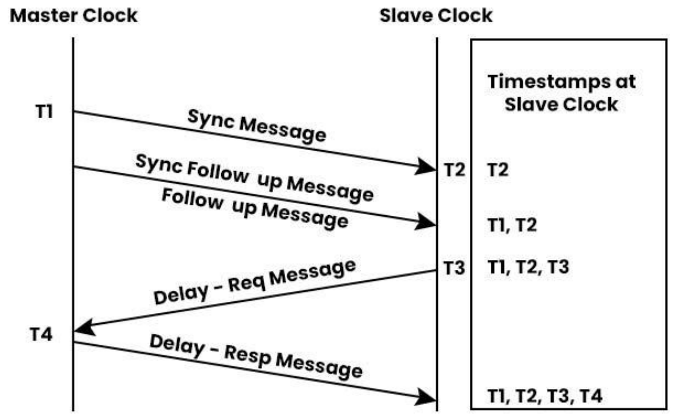


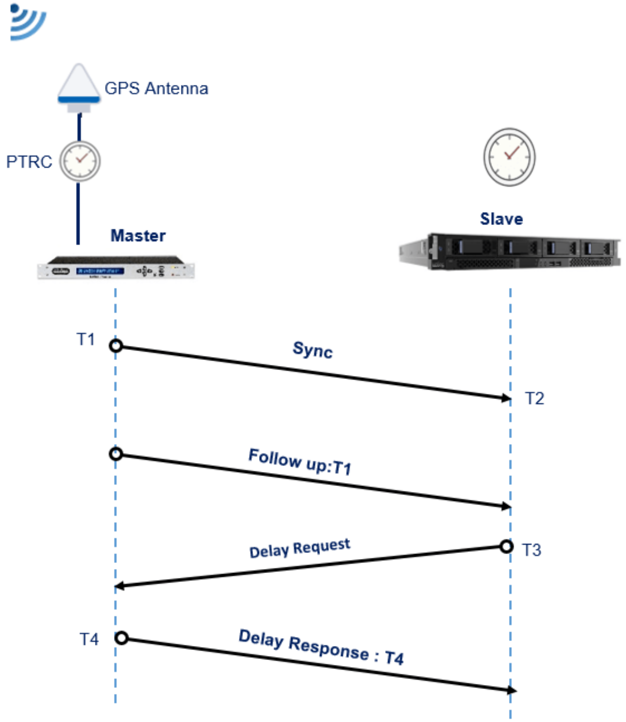
Network Time Security: new NTP authentication mechanism, Martin Langer, 2019

Secure time transfer

Common Protocols and Technologies

- PTP (Precision Time Protocol) with security profiles (e.g., IEEE 1588 with secure extensions)





Secure time transfer

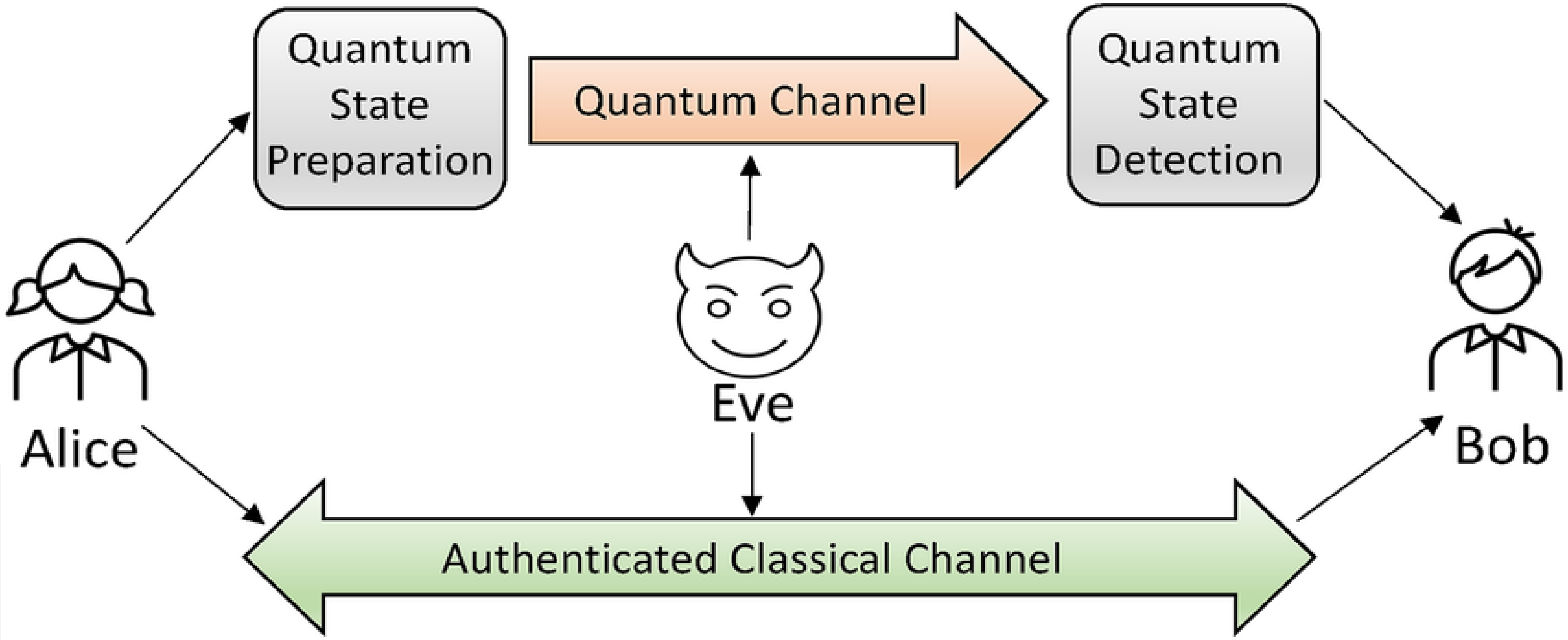
Quantum-secure time transfer

Main Approaches:

- Quantum Key Distribution (QKD) + Classical Time Protocols
  - QKD uses quantum properties of photons (e.g., polarization) to distribute encryption keys securely. These keys are then used to authenticate and encrypt time transfer data (e.g., over NTP or PTP). Any eavesdropping attempt on the quantum channel alters the quantum state, revealing the intrusion.
- Two-Way Quantum Time Transfer
  - Similar to classical two-way time transfer but enhanced by sending single photons or entangled particles. Uses quantum correlations to measure precise delays and detect tampering. Allows sub-nanosecond timing accuracy with high tamper resistance.
- Entanglement-Based Synchronization (experimental)
  - Uses quantum entanglement between particles at two locations. Time correlation of entangled states enables clock synchronization without needing direct signal transmission. Currently experimental but could offer ultra-secure, covert synchronization.

Secure time transfer

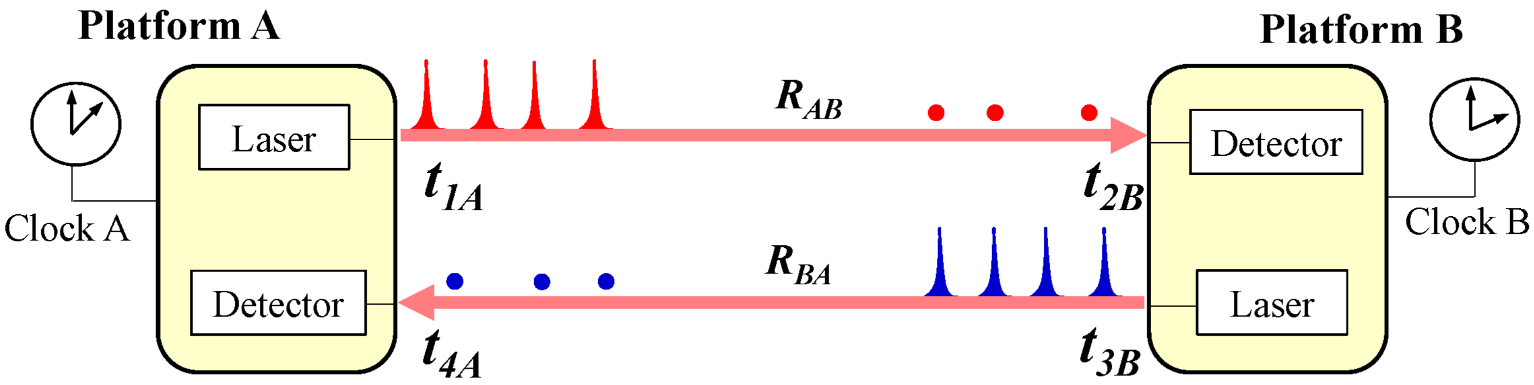
Quantum Key Distribution (QKD) + Classical Time Protocols



https://doi.org/10.1049/qtc2.12044

Secure time transfer

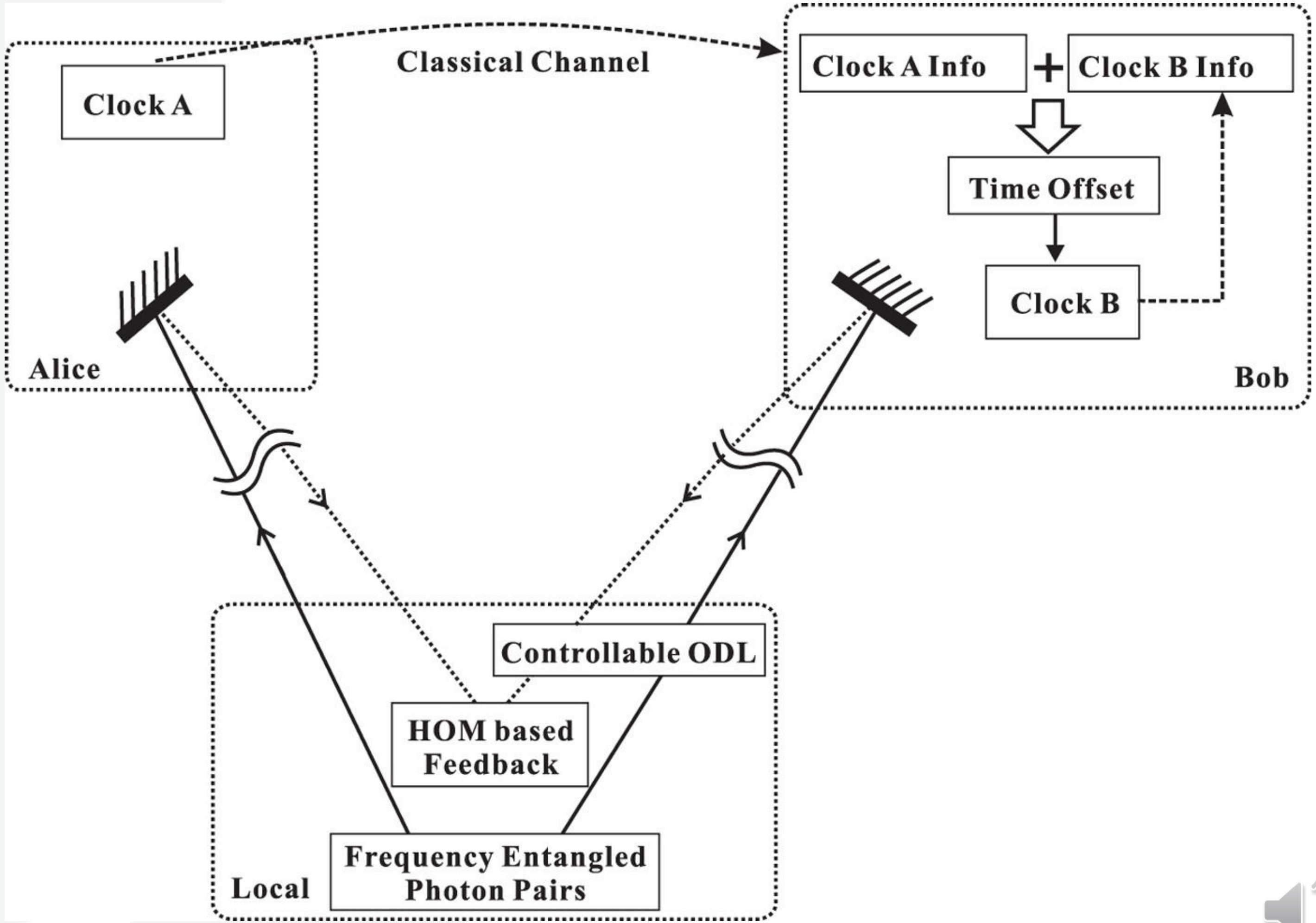
Two-Way Quantum Time Transfer



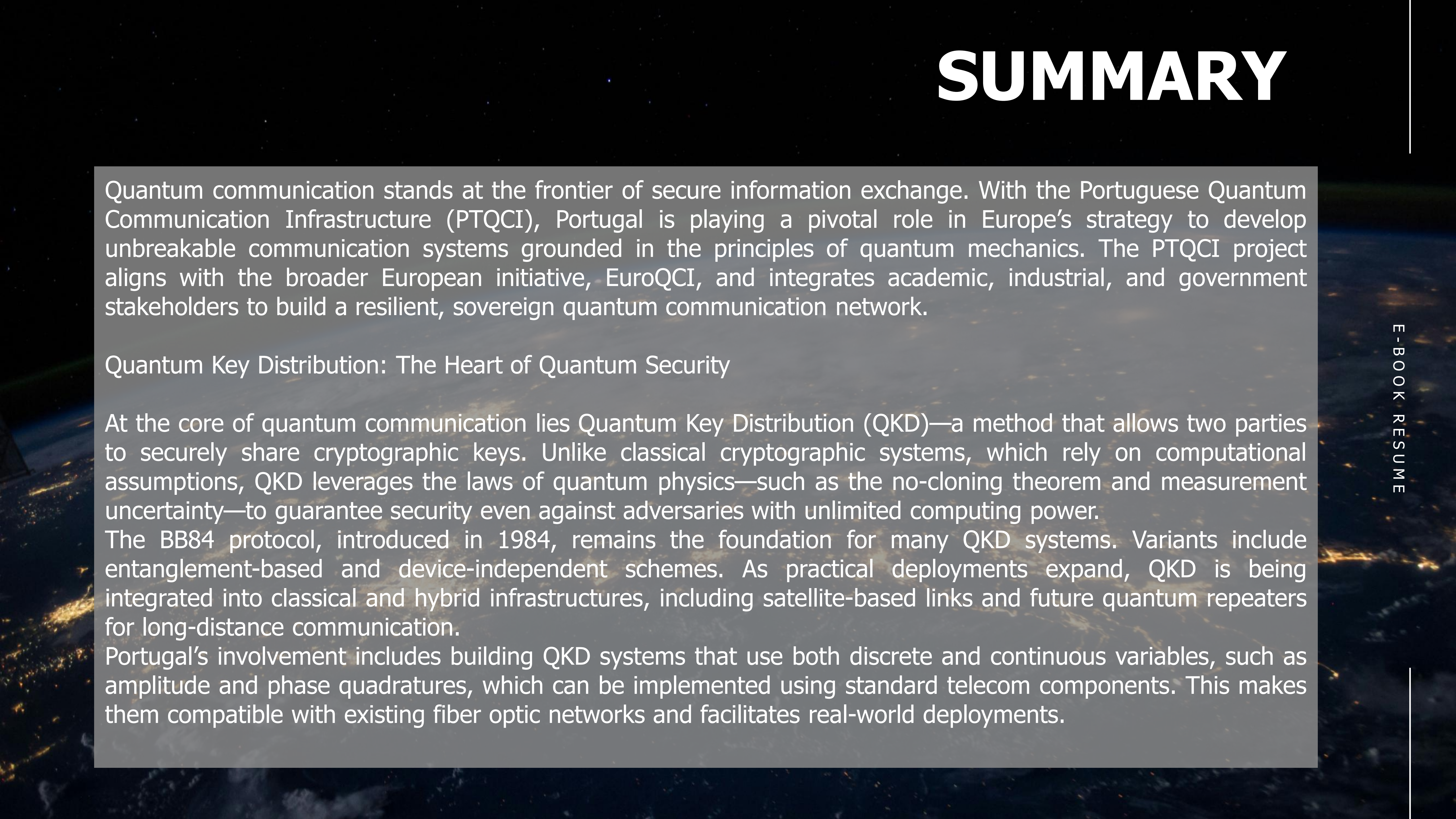
https://doi.org/10.3390/photonics11111028

Secure time transfer

Entanglement-Based Synchronization



https://doi.org/10.1038/srep30453



SUMMARY

Quantum communication stands at the frontier of secure information exchange. With the Portuguese Quantum Communication Infrastructure (PTQCI), Portugal is playing a pivotal role in Europe’s strategy to develop unbreakable communication systems grounded in the principles of quantum mechanics. The PTQCI project aligns with the broader European initiative, EuroQCI, and integrates academic, industrial, and government stakeholders to build a resilient, sovereign quantum communication network.

Quantum Key Distribution: The Heart of Quantum Security

At the core of quantum communication lies Quantum Key Distribution (QKD)—a method that allows two parties to securely share cryptographic keys. Unlike classical cryptographic systems, which rely on computational assumptions, QKD leverages the laws of quantum physics—such as the no-cloning theorem and measurement uncertainty—to guarantee security even against adversaries with unlimited computing power.

The BB84 protocol, introduced in 1984, remains the foundation for many QKD systems. Variants include entanglement-based and device-independent schemes. As practical deployments expand, QKD is being integrated into classical and hybrid infrastructures, including satellite-based links and future quantum repeaters for long-distance communication.

Portugal’s involvement includes building QKD systems that use both discrete and continuous variables, such as amplitude and phase quadratures, which can be implemented using standard telecom components. This makes them compatible with existing fiber optic networks and facilitates real-world deployments.

E-BOOK RESUME

SUMMARY

Going Beyond QKD: Broader Quantum Cryptography

The field is rapidly evolving to encompass more than just QKD. Emerging protocols like quantum oblivious transfer, secure multi-party computation, and quantum digital signatures represent the next frontier. However, the security analysis of these advanced protocols remains an open problem, demanding further theoretical and experimental research.

Researchers like Ricardo Faleiro explore the philosophical underpinnings of quantum information, highlighting how fundamental quantum concepts enable new forms of secure communication. His work reinterprets classic ideas like Wiesner’s Conjugate Coding in the context of modern protocols like 1-out-of-2 Oblivious Transfer.
Composable Security: Building Trustworthy Systems

Mariano Lemus introduces the Universal Composability (UC) framework—a robust method for defining and proving security in complex cryptographic systems. UC allows for modularity, meaning that if a component (like QKD) is proven secure, it can be reused safely in larger systems without introducing vulnerabilities.
This framework uses a formal system of "machines" and ideal functionalities, ensuring that even under adversarial conditions, protocols behave securely from an external observer’s perspective. Such rigor is essential as quantum protocols are deployed in real-world, heterogeneous environments.

E-BOOK RESUME

SUMMARY

Portuguese Leadership and Infrastructure Development

Professor Armando N. Pinto, a leading figure in quantum communications, emphasizes Portugal's role as an innovator in photonic systems and protocol development. The Instituto de Telecomunicações (IT) and University of Aveiro are key research centers contributing to national and international projects. Portugal's active participation in EuroQCI demonstrates its commitment to European strategic autonomy in secure communications.

The PTQCI leverages existing fiber infrastructure to create a scalable, quantum-safe network, with planned extensions to the Portuguese islands and interoperability with Spain. The approach promotes a hybrid cryptographic model, blending quantum and post-quantum classical methods.

GNS and National Security

Coronel Paulo Santos outlines the role of Portugal’s National Security Agency (GNS) in leading the PTQCI effort. GNS ensures that the infrastructure meets national and EU security standards, accredits entities handling classified information, and oversees risk management.

A significant focus of GNS is on public trust. Through community outreach, education, and transparent governance, GNS aims to demystify quantum technologies and ensure that their deployment enhances—not undermines—citizen confidence in digital systems. Portugal’s strategic autonomy is bolstered by relying on European-developed technologies, minimizing dependence on external vendors.

SUMMARY

Cutting-Edge CV-QKD Systems

Gustavo Anjos discusses the implementation of Continuous Variable QKD (CV-QKD) systems, which use modulated coherent light and homodyne detection instead of single photons. This approach allows for higher key rates and easier integration with conventional telecom systems.

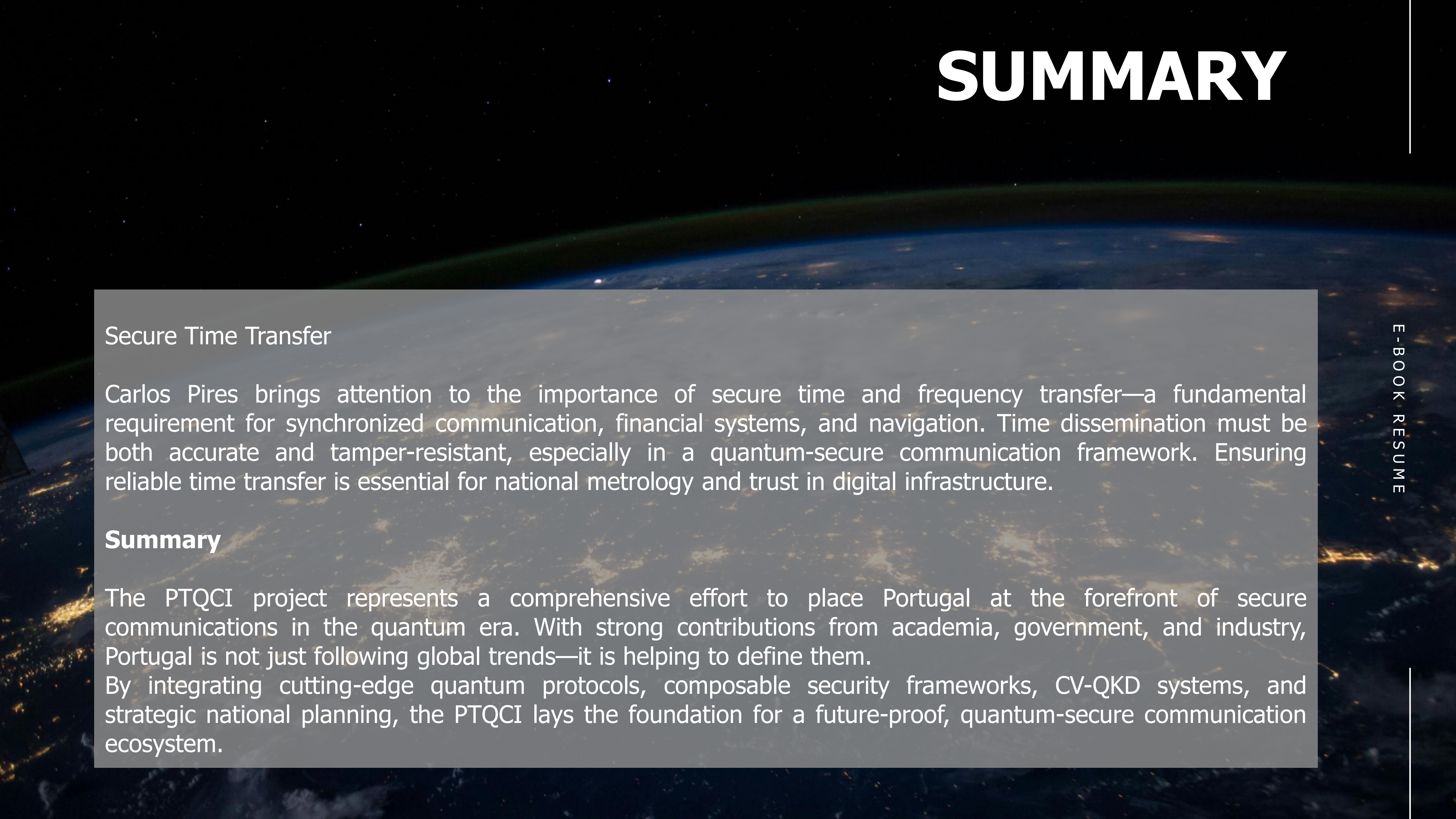
Security in CV-QKD is maintained through rigorous calibration (e.g., noise estimation) and intensive post-processing (error correction and privacy amplification), often accelerated by GPUs or FPGAs. These systems are increasingly embedded in Software Defined Networking (SDN) environments, allowing for programmable, scalable, and automated key distribution across complex networks.

Cryptographic Foundations

Ricardo Chaves provides an accessible introduction to cryptography, tracing its history from ancient substitution ciphers to modern block and stream ciphers. He explores the theoretical concept of the one-time pad, its perfect security, and the practical challenges of key distribution—challenges that QKD can overcome.

His talk also covers the evolution of encryption technologies, including the development of the Advanced Encryption Standard (AES) and stream ciphers like ChaCha20. Chaves stresses the importance of aligning encryption methods with the value and sensitivity of data, advocating for a balance between security and efficiency.

E-BOOK RESUME



SUMMARY

E-BOOK RESUME

Secure Time Transfer

Carlos Pires brings attention to the importance of secure time and frequency transfer—a fundamental requirement for synchronized communication, financial systems, and navigation. Time dissemination must be both accurate and tamper-resistant, especially in a quantum-secure communication framework. Ensuring reliable time transfer is essential for national metrology and trust in digital infrastructure.

Summary

The PTQCI project represents a comprehensive effort to place Portugal at the forefront of secure communications in the quantum era. With strong contributions from academia, government, and industry, Portugal is not just following global trends—it is helping to define them.
By integrating cutting-edge quantum protocols, composable security frameworks, CV-QKD systems, and strategic national planning, the PTQCI lays the foundation for a future-proof, quantum-secure communication ecosystem.