Cryptographie quantique
Théorie et Pratique

Applications de la Physique Quantique
IMT Atlantique
28 Décembre 2022

Romain Alléaume
romain.alleaume@telecom-paris.fr

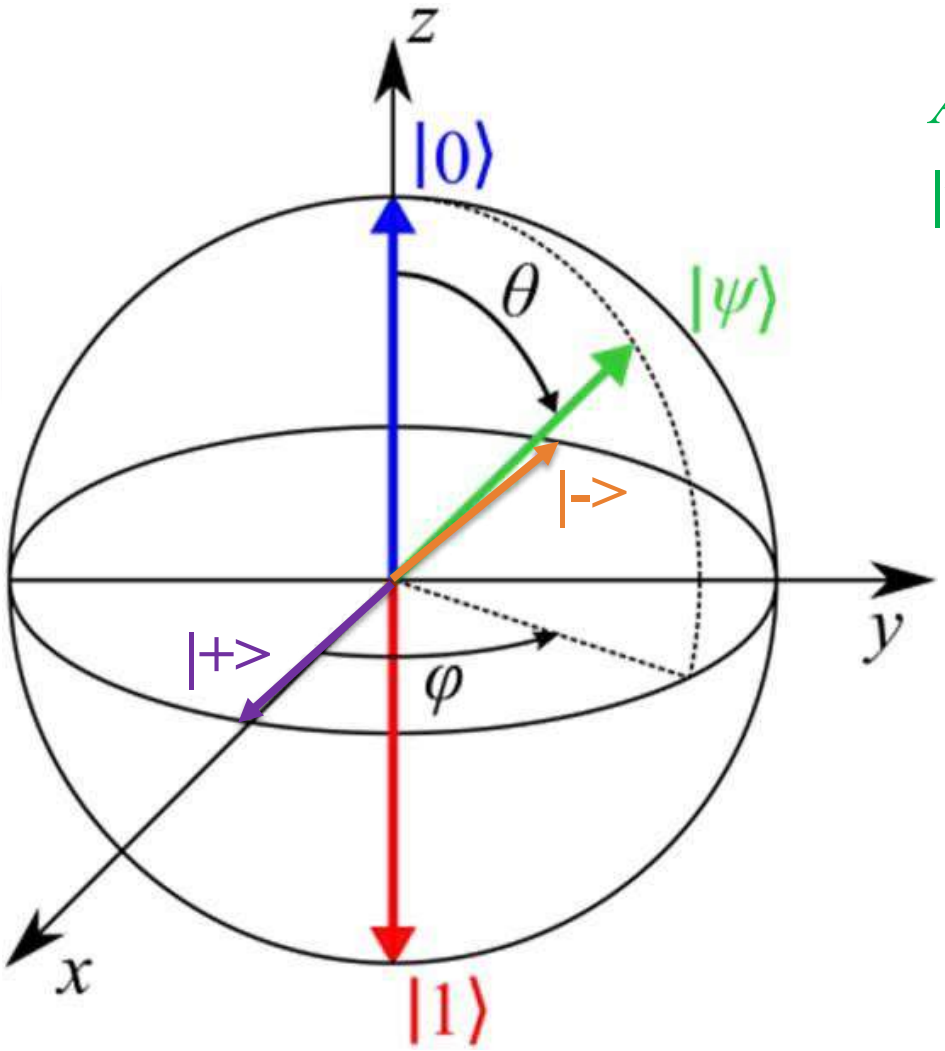
Plan du cours

- Principe de la Distribution Quantique de Clé (QKD)
- Cryptographie quantique et cryptographie classique
- Real-World QKD

Principe de la QKD
(distribution quantique de clé)

Protocole BB84

Représentation des états à 1 Qubit
Sphère de Bloch



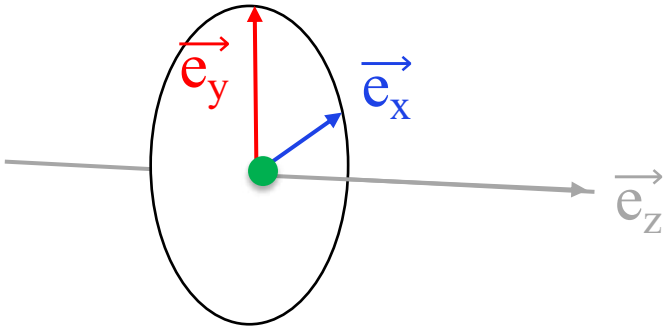
Arbitrary Qubit

$|\psi\rangle = \{ \cos\theta\ |0\rangle + \sin\theta\ e^{i\varphi}\ |1\rangle \}$

Z basis : { |0> , |1>}

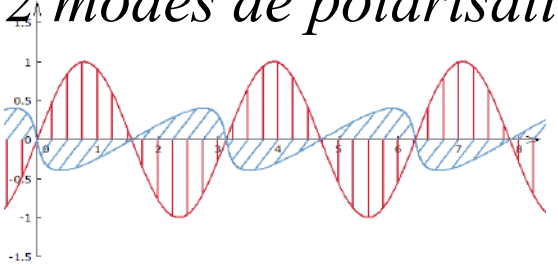
X basis : { |+>=(| |0> +||1>√2
|-> = |0> -|1>√2}

1 photon encodé en polarisation = 1 polarization qubit



$$\vec{\varepsilon} = \varepsilon_x \vec{e}_x + \varepsilon_y \vec{e}_y$$

2 modes de polarisation

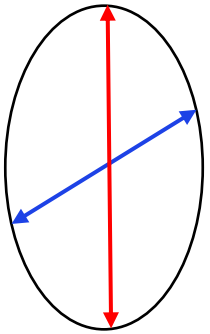


$$\vec{E}(\vec{r},t) = A\,\vec{\varepsilon}\,e^{i\vec{k}.\vec{r}-\omega t}$$

2-dim Hilbert space

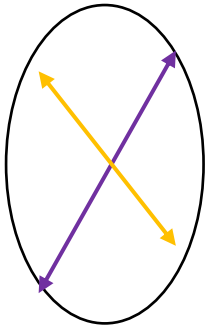
$$|\psi\rangle = \{\cos\theta\,|0\rangle + \sin\theta\;e^{i\varphi}\,|1\rangle\}$$

Z basis : { |0> , |1>}



Horizontal / Vertical Polarization

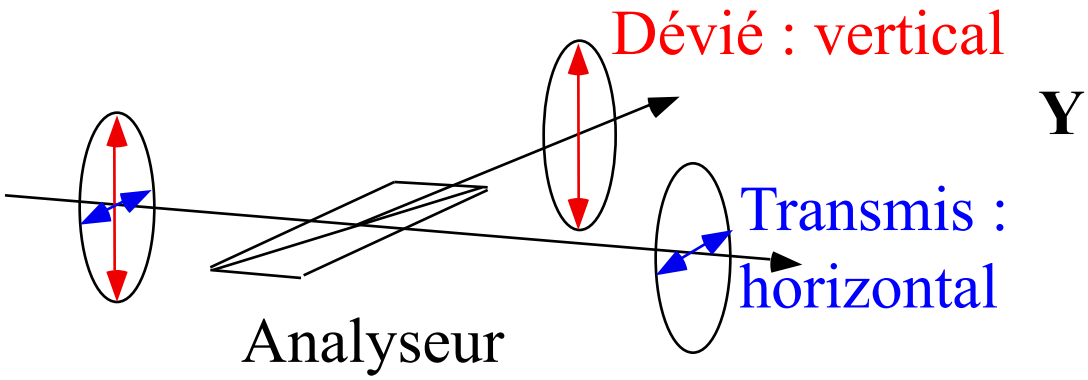
X basis : { |+>=(| |0> +||1>√2
|-> = |0> -|1>√2}



π/4 or 3 π /4 Polarization

Mesure d'un qubit encode en polarisation

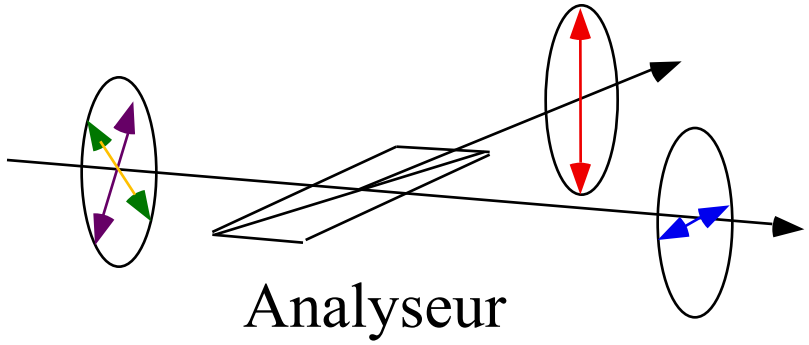
- Un analyseur de polarisation donne 2 résultats : transmis ou dévié
- Une détection conjointe sur les deux sorties permet de déterminer avec certitude l'état du photon polarisé dans la même base que la base d'analyse



H(X|Y) = 0

- Si la polarisation et la base d'analyse diffèrent, le résultat de mesure devient aléatoire (50 % - 50 % pour la base à 45°)

|+>=(|0>+|1>)/√2
ou
|->=(|0>-|1>)/√2



H(X|Y) = 1

QKD Security <= No-cloning theorem (Zurek 1982)

No cloning theorem: **It is impossible to copy an unknown quantum state,** $\psi \not\rightarrow \psi \cdot \psi$

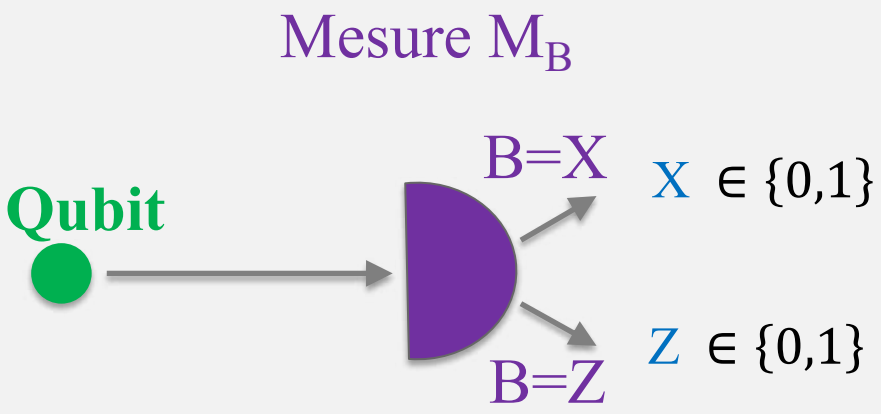
Proof

$$\begin{aligned} |0\rangle &\rightarrow |0,0\rangle \\ |1\rangle &\rightarrow |1,1\rangle \end{aligned} \Rightarrow \quad |0\rangle + |1\rangle \rightarrow |0,0\rangle + |1,1\rangle$$

$$\neq (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$$

Contradiction!

Autre façon de prouver la sécurité de la QKD: relations d'incertitude



$$H(X|B) + H(Z|B) \geq 1$$

(Massen Uffink 1988)

Precursor of quantum crypto: Quantum Money

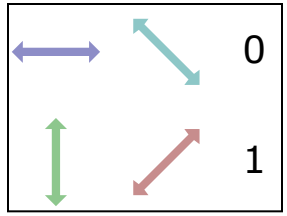
Uncloneable Quantum Banknotes
Wiesner, 1969 .. Published 1983

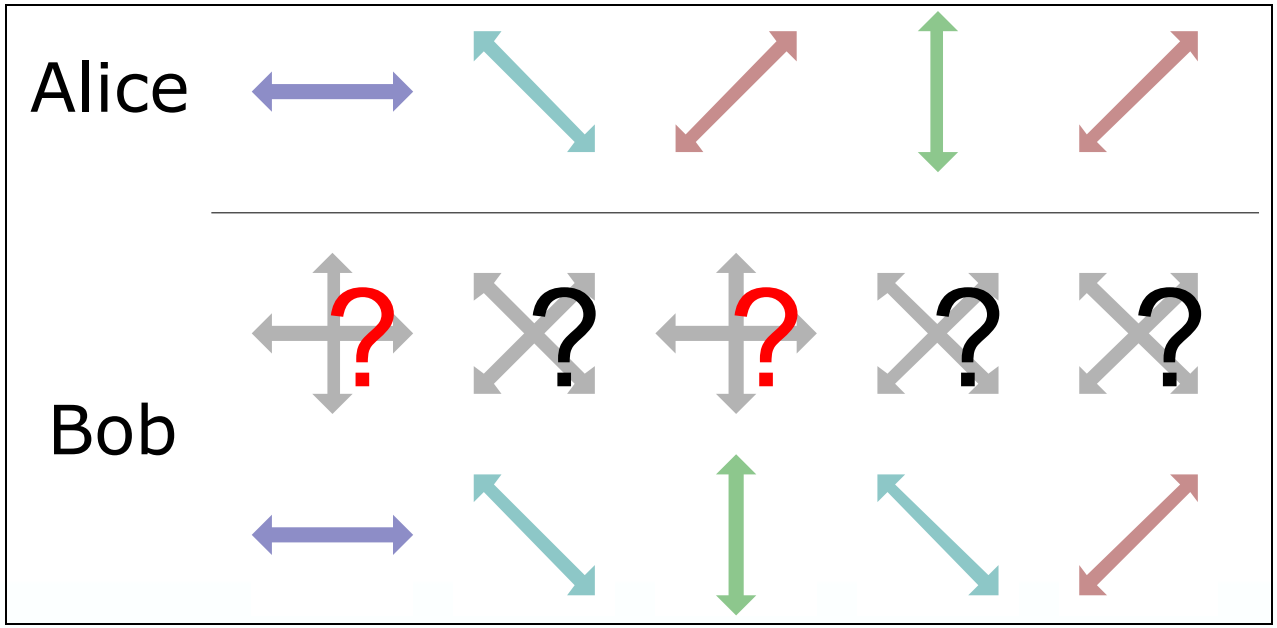
Crucial ideal: Conjugate Coding
Encode 1 bit into 1 qubit using 2 complementary basis

Rectangular basis (Z) :  = |0> or  = |1>

Diagonal basis (X)  =|+> =(|0>-|1>)/√2 or  =|-> =(|0>+|1>)/√2

BB84: Transmission

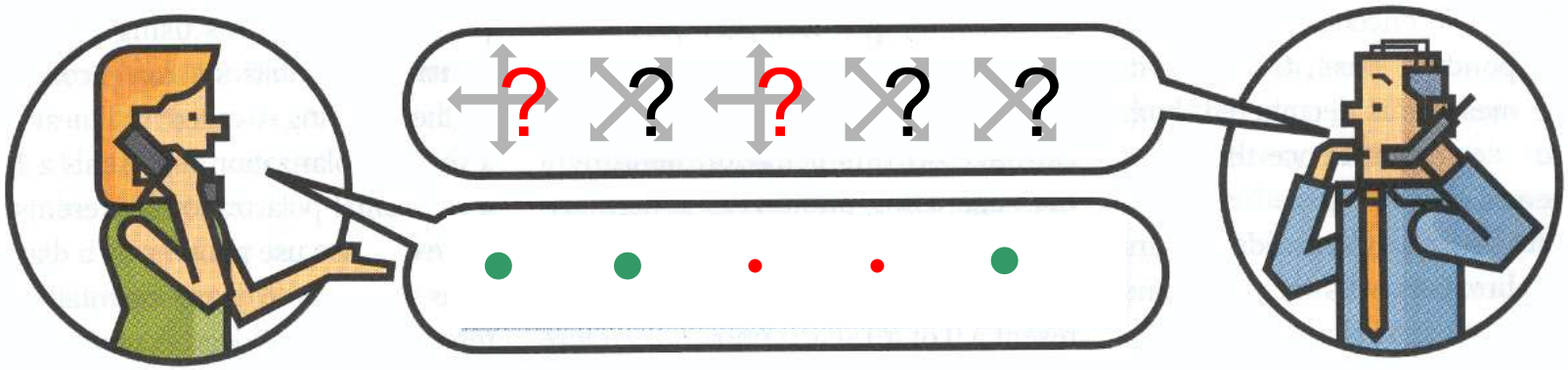




Dessins issus de IEEE Spectrum

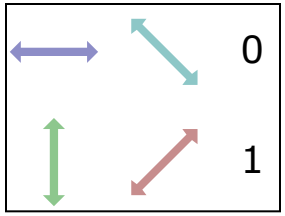
BB84: Tamisage/ Sifting

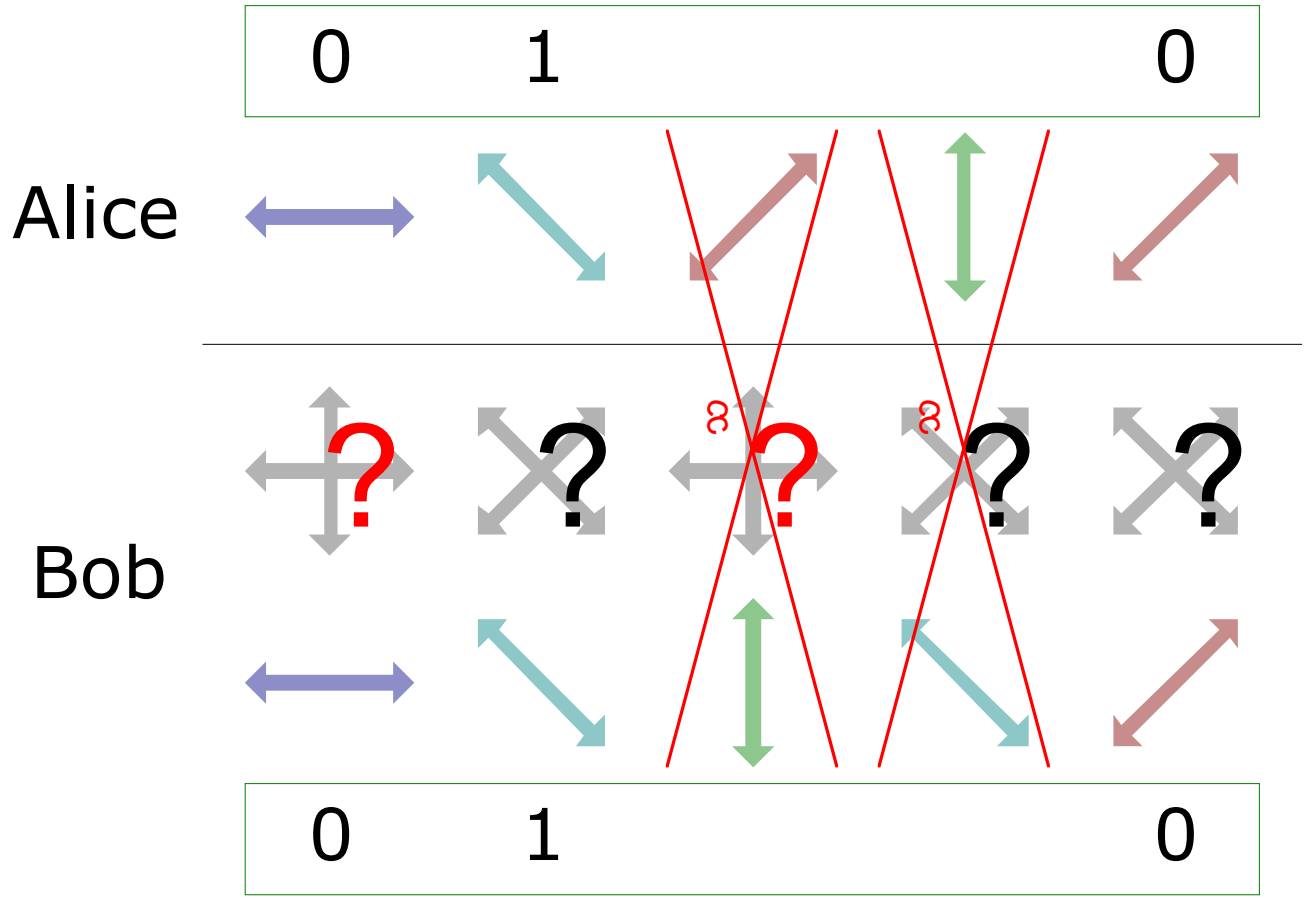
- Eliminer les mesures qui ne correspondent pas
  - Utilisation d'un canal **public**

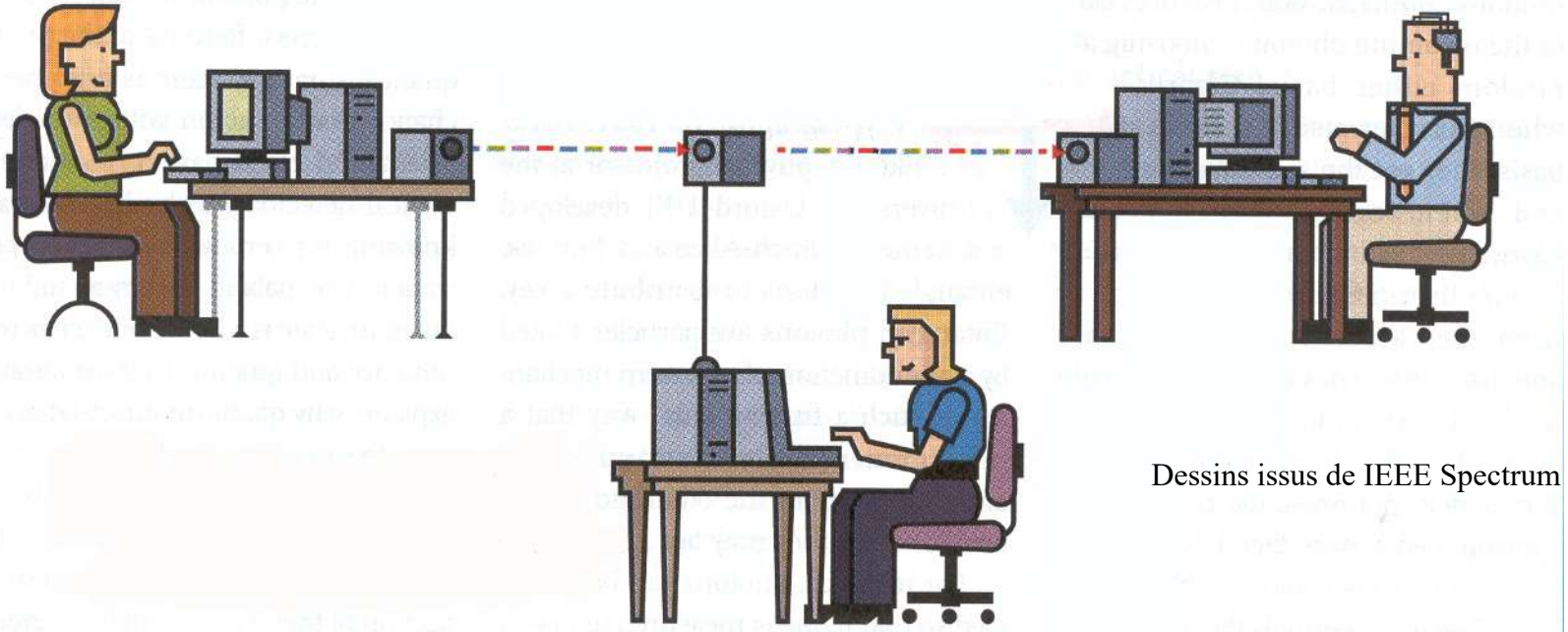


Dessins issus de IEEE Spectrum

BB84: Partage de la Clé







Dessins issus de IEEE Spectrum

Questions:

- Quel est l'effet d'un espionnage sur la ligne ?

- Cas de l'Attaque Intercept-Resend:
  Eve agit comme Bob et renvoie état mesuré
  ➔ Quel taux d'erreur ?

Distillation de clé de la clé en QKD
Etapes dite de Réconciliation

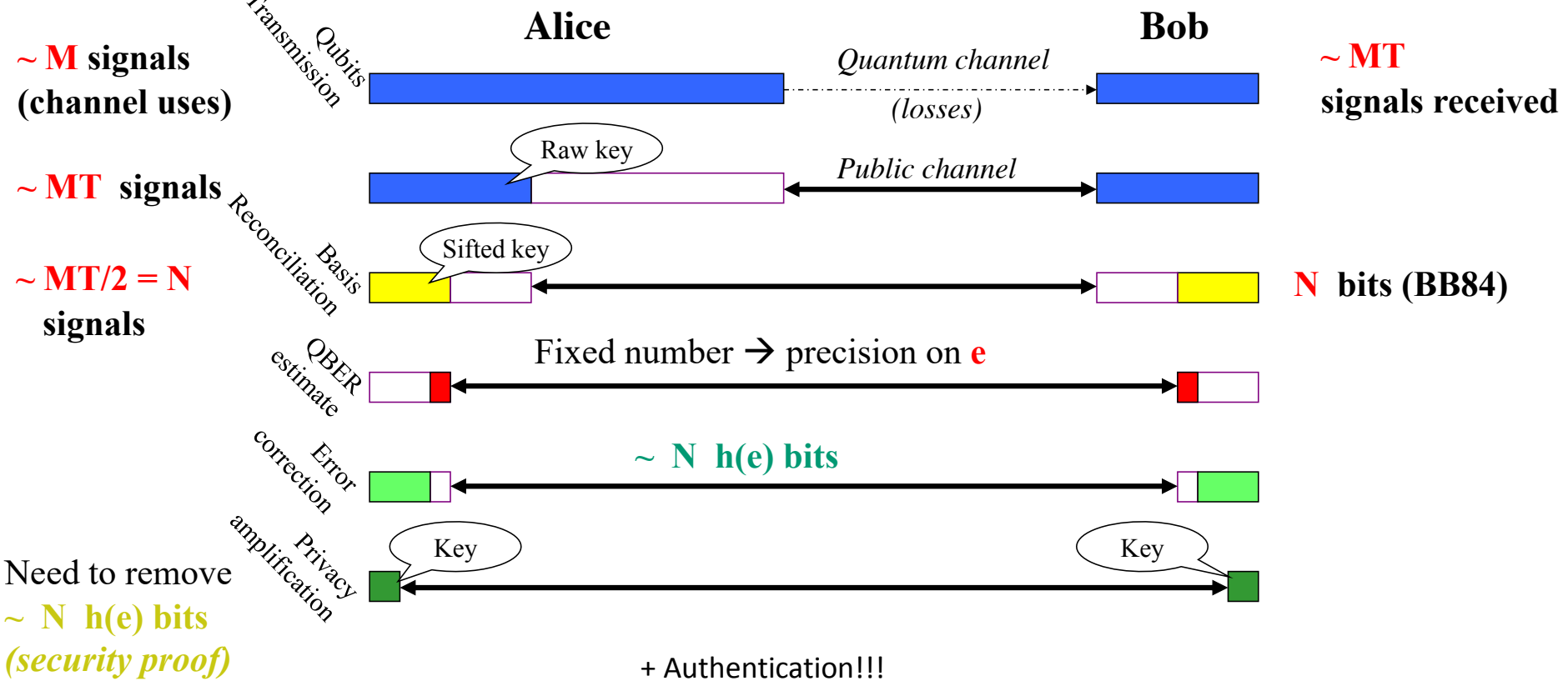
2 Etapes Purement classiques : réalisée sur le canal classique authentique, à partir des données brutes, classiques de XA et XB)

1. **Correction d'Erreur** : utilisation du canal classique et d'un code correcteur d'erreur pour s'accorder sur une chaine identique (par exemple XA), en révélant le moins d'information possible sur le canal classiques => XA'=XB'

2. **Amplification de confidentialité**: permettant d'extraire un **secret commun** (de taille plus petite que les données brutes), totalement découplé de l'attaquant ➔ **clé finale**

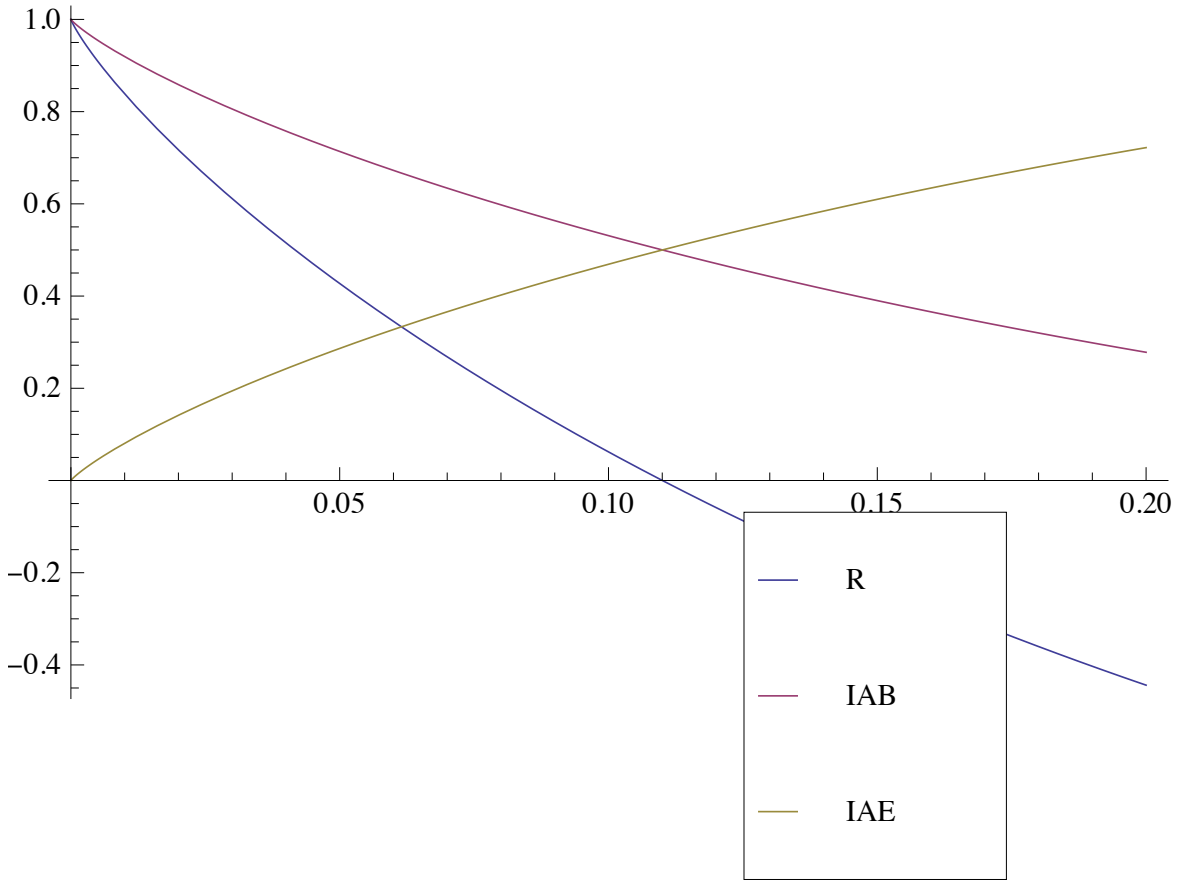
   Repose par exemple sur l'utilisation de fonctions de hachage universelles

The steps to a secret key



Key Rate $_{BB84}$ per ch.use ~ T (1-2 h(e)) (general attacks)

BB84 Secure key rate against general (coherent) attacks

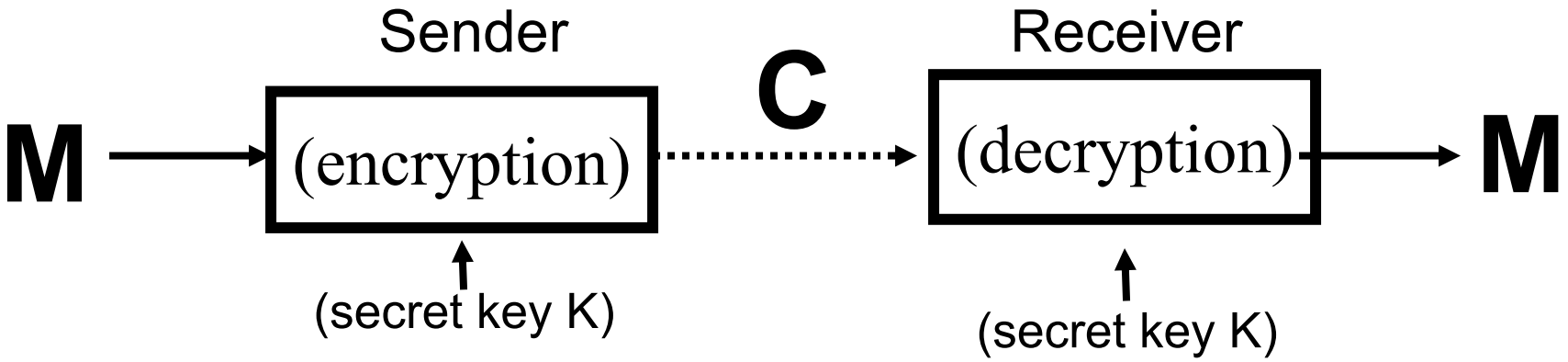


BB84 : $R_{(\text{secure key rate})} \sim n\,(1\text{-}2\,h(\text{QBER}))$

Taux d'erreur tolérable maximal ~11 %

Cryptographie quantique et cryptographie classique

Symmetric-Key Cryptography



- **Private/secret/symmetric key** cryptography uses **one** key
- Same key shared by both sender and receiver => **Symmetric**

- **Applications:**
  - Encryption
  - Authentication (with Message Authentication Codes)

- ***Challenge: Key Distribution Problem***
  (in particular over large network)

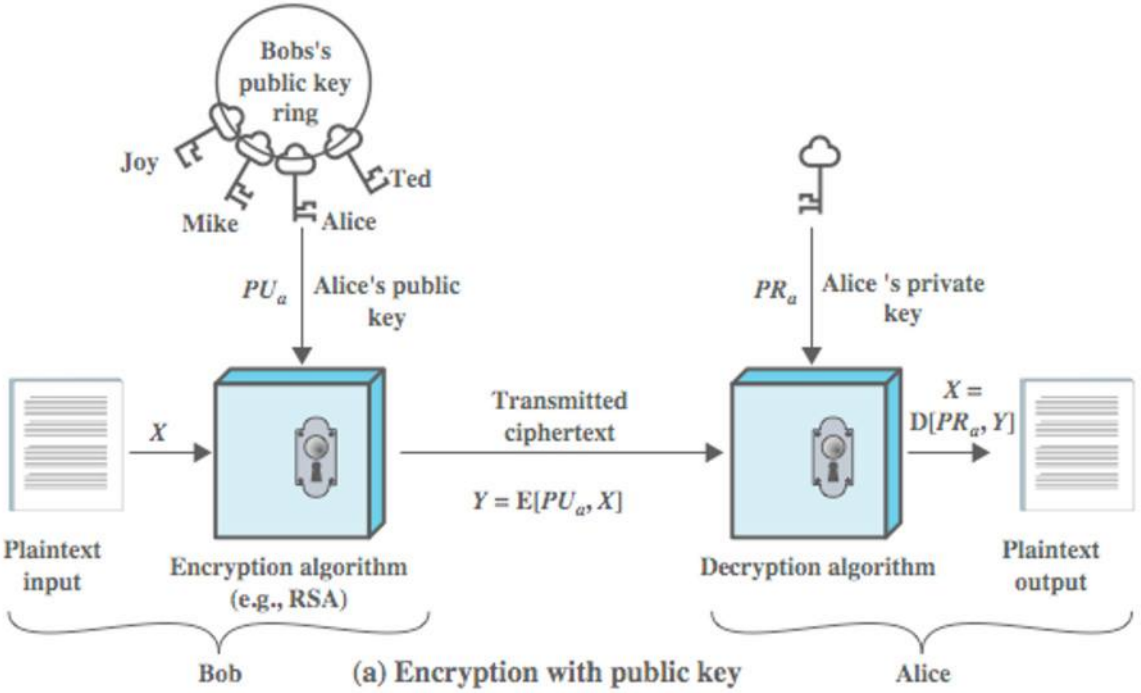
Public-Key Cryptography

- Uses **two** keys – a public & a private key
- **Asymmetric** since parties are **not** equal
- Uses clever application of number theoretic concepts to function
  - Example:
    - Factorize 48770428682337401 => **hard problem**
    - Is 223092871 a factor of 48770428682337401? (yes !) => **easy problem**

Public-key encryption (decryption)

Applications
- Key distribution
- (Digital signature)

➔ **Security Foundations of Internet**



Cryptographie: Symétrique vs. asymétrique

Chiffrement symétrique (à clé secrète)

- Pros
  - Clé courte (~100 bits)
  - Chiffrement / déchiffrement rapide
- Cons
  - Distribution sécurisée de la clé
- Utilisation
  - Chiffrement de grand volume de données
- Exemples d'algorithmes
  - AES
  - DES

Chiffrement asymétrique (à clé publique)

- Pros
  - Pas nécessaire d'échanger la clé secrète (seule la clé publique est publiée)
- Cons
  - Clé longue (~ 1000 bits)
  - Calcul intensif
- Utilisation
  - Distribution de clés secrètes
  - Signature numérique
- Exemples d'algorithmes
  - RSA
  - Diffie-Helman

Modern cryptography : computational assumptions

Example1: Hardness of breaking AES128 encryption

Assumptions: AES (block cipher) is a secure one-way function

➔ Best attack is exhaustive search, requires 2^{128} operations

Example2: Hardness of factoring

Assumption: Best known factoring algorithm (General Field Number Sieve) is **sup-exponential**

Factoring large number N, requires Exp [O($(\ln n)^{1/3}$)] operations

Remark: what about pratical computing power ?

(individu, ~10 k$)

1 GHz * 100 (parallélisation) * 1 an ~ 2^{52}

(grande organisation type NSA ~1000 M$)

10 Petaflops * 1 an ~ 2^{78}

Sécurité inconditionelle // Information Theoretic Security

Def: Un algo de chiffrement ***(E,D)*** sur (K,M,C) verifie la condition de **confidentialité parfaite (perfect secrecy) si**

$$\forall m_0, m_1 \in M \quad (|m_0| = |m_1|) \quad \text{et} \quad \forall c \in C$$

$$Pr_K[E(k,m_0)=c] = Pr_K[E(k,m_1)=c]$$

where $k \xleftarrow{R} K$

➔ **Sécurité au sens de la théorie de l'information (pas d'hypothèse computationnelle)**

➔Connaissant un texte chiffré c, on ne peut dire si message est m_0 ou m_1 pour tout m_0 ou m_1

➔ Quelle que soit puissance adversaire, n'apprend RIEN sur message à partir de texte chiffré c

One Time Pad OTP – Masque Jetable (Vernam 1917)

$\mathbf{M=C=K=\{0,1\}^n}$

Chiffrement

$C = E(k, m) = k \oplus m$

Déchiffrement

$D(k, c) = k \oplus c$

Msg M: 0 1 1 0 1 1 1 ⊕

Key K: 1 0 1 1 0 1 0

Ciphertext

C: 1 1 0 1 1 0 1

Shannon (1949): OTP vérifie la propriété de sécurité inconditionnelle

Key distribution problem and public-key crypto

Shannon positive result (1949):

- One-Time-Pad verifies the perfect secrecy condition

Shannon negative result (1949):

- Perfect secrecy condition requires $|K| \geq |M|$

➔ Secret-key distribution problem

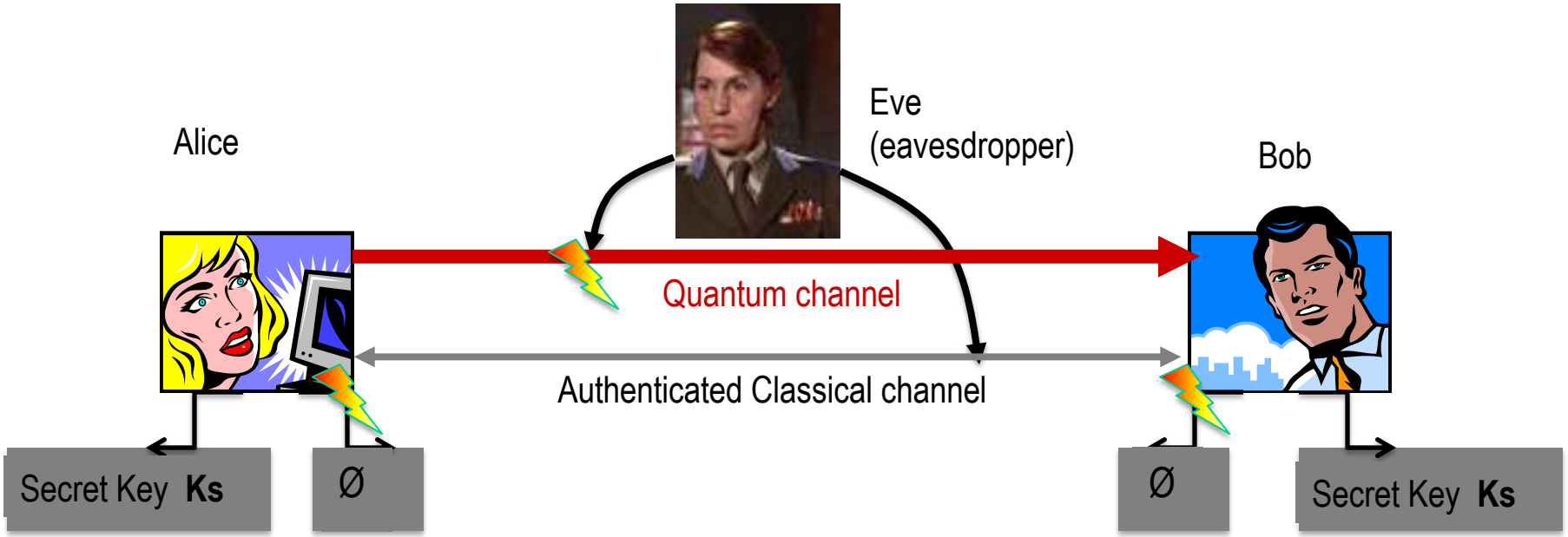
➔ Information-theoretic security considered non-practical

Public-key cryptography

- Diffie-Hellman 1976
- RSA 1978

Current solution to the key distribution problem

Quantum Key Distribution (QKD): general setting



- Intuition for security:
  Any measurement by Eve leads to detectable perturbation by Alice/Bob

- **Specificity: Information-Theoretic Security (ITS)** [Unconditional Security]
  - No assumption about Eve computational power
  - « Future-proof »

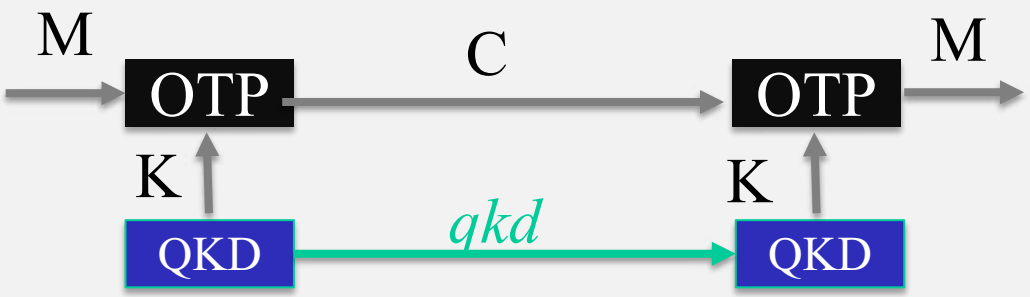
QKD combined with encryption: Secure Communication

One-Time Pad rekeying

☺ ITS

➔ Perfect Secrecy

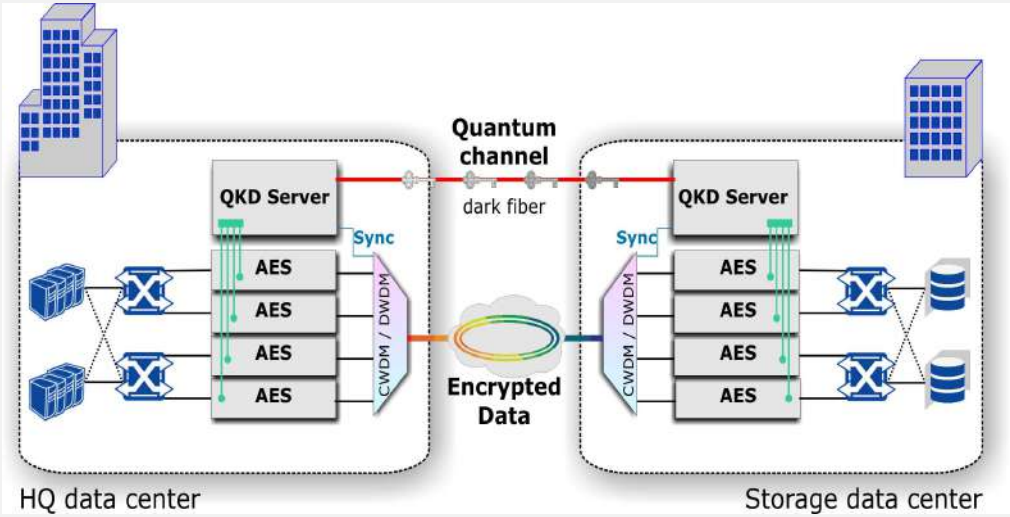
☹ Rate = QKD Rate ≤ 1Mb/s



AES Rekeying

☺ High Rate ~ 10 Gb/s

☹ Less Security Gain



QKD mostly useful when long-term security is needed

Long-term secrets
- Industry, IP
- Military
- Governmental

Personal Data
- Medical record
- Genomic
- Private

Computational Cryptography
Based on hardness of mathematical problems

Generic Vulnerability (incl. PQC)

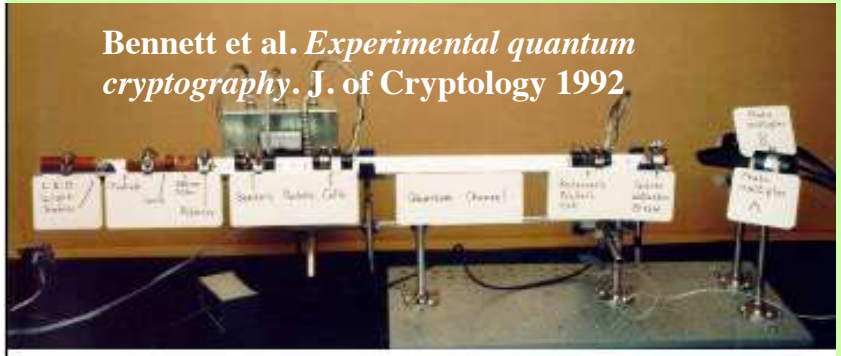
Harvesting Attack
"Intercept now, decrypt later "

NSA Bullrun program

Real-World QKD

From QKD pioneers to first QKD networks

Early 90's: Pionneering work in USA and UK



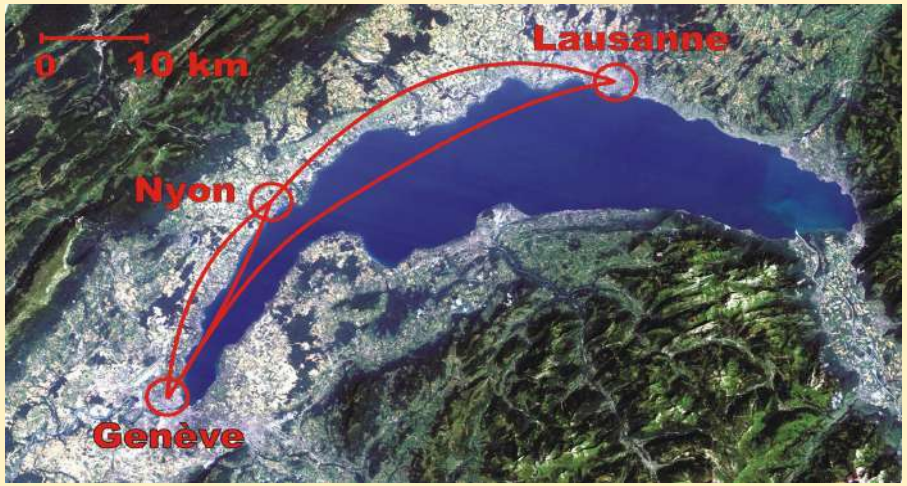
Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

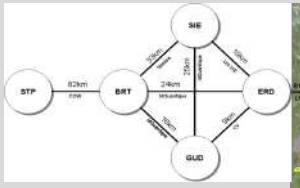
End 90's: QKD outside of the lab



2000 -2010: First QKD networks deployments

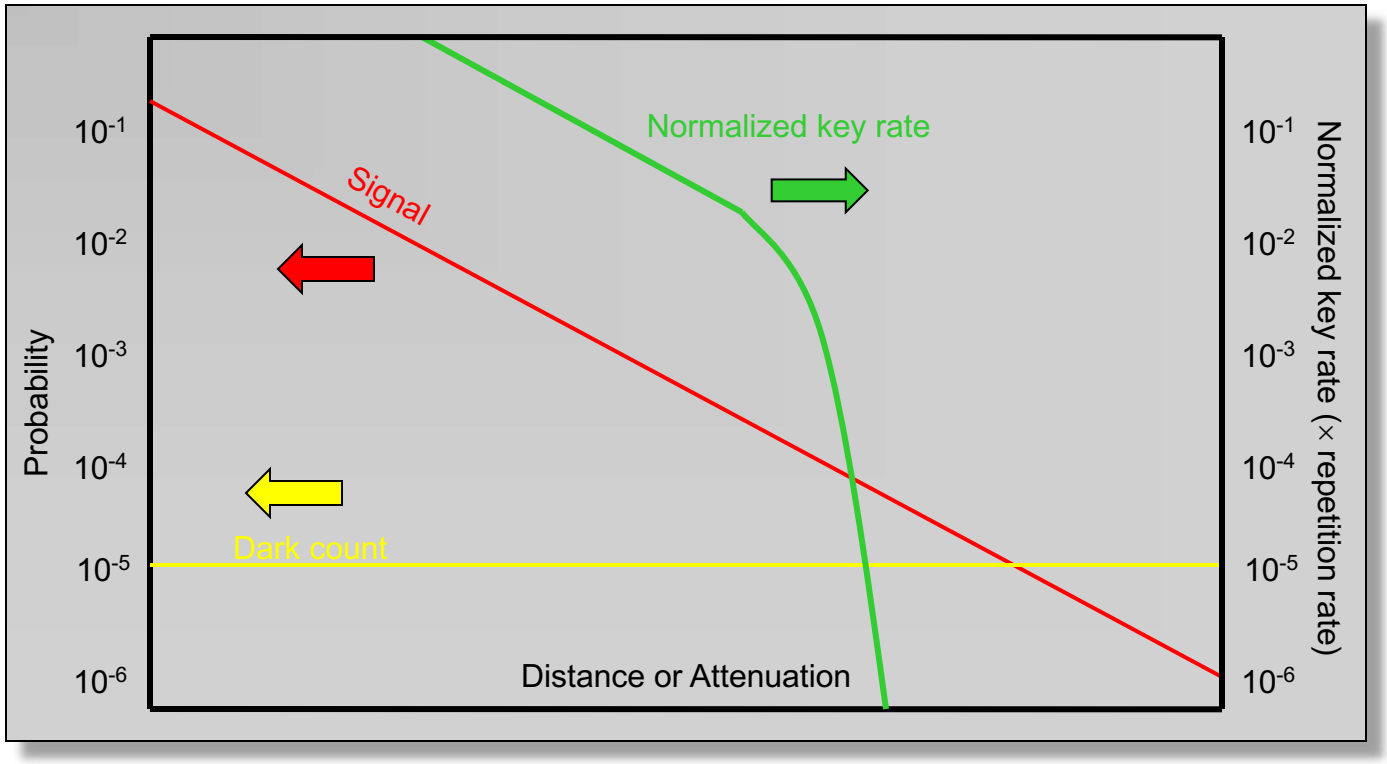
2004 DARPA BBN QKD Network (Boston)

2008 First European QKD Network Vienna



SECOQC

Performance of a QKD System in a nutshell

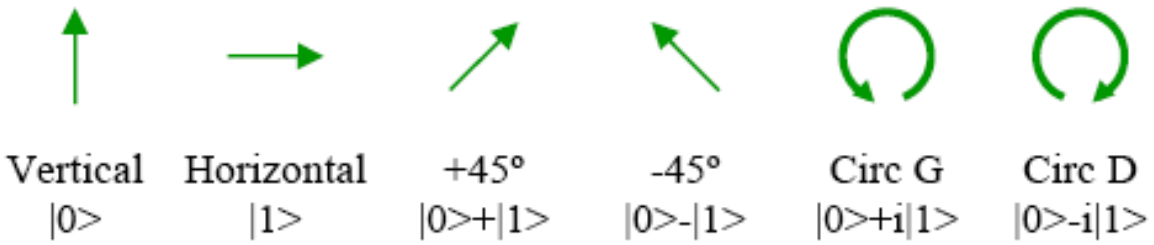


- Performance of a QKD system: number of secret bits per second = key rate
- Key rate decreases with distance / attenuation
  - Transmission probability of a photon decreases exponentially
  - Error probability (from dark count) is constant
- Key distillation causes key rate breakdown

Practical QKD systems
(Discrete Variable QKD)

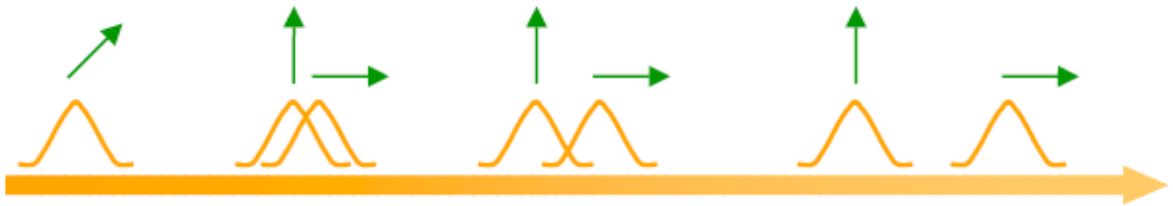
Polarization encoding in fiber

Photon polarization



Pros: Simple encoding
Simple detection (extincition ratio of polarizing cube > 10^5)

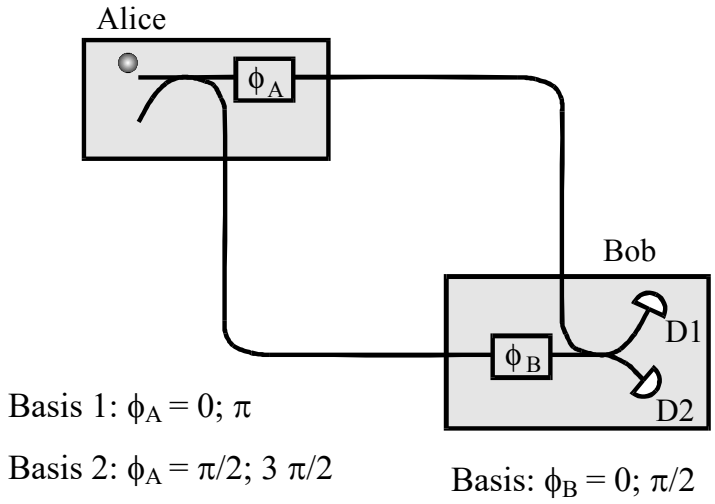
Cons: Slow modulation (max 10 MHz)
Polarization Mode Dispersion in fibers



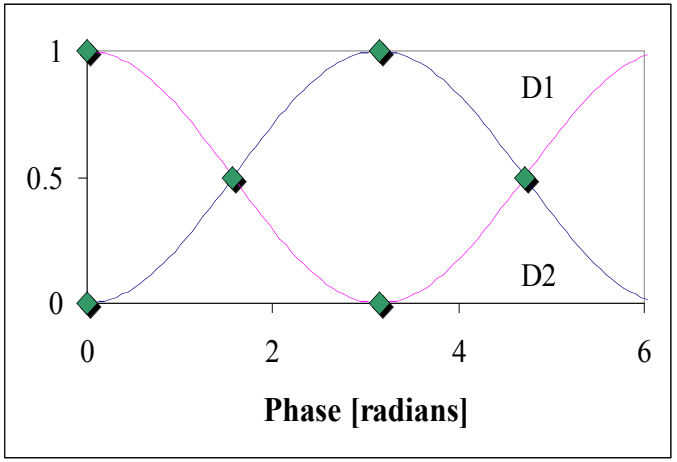
=> Polarization coding (without active tracking) is usually a bad choice on optical fibers

Time-bin encoding

Single-photon interference with Mach-Zender



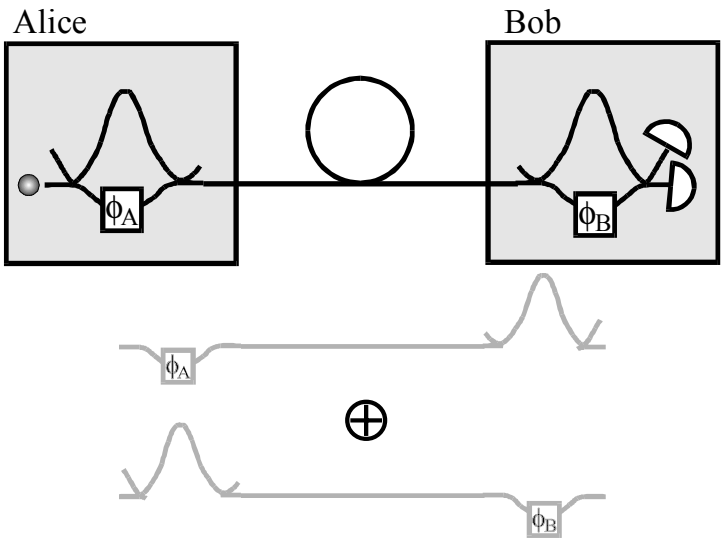
$$I = I_{max}(1 + cos(\phi_A - \phi_B))$$

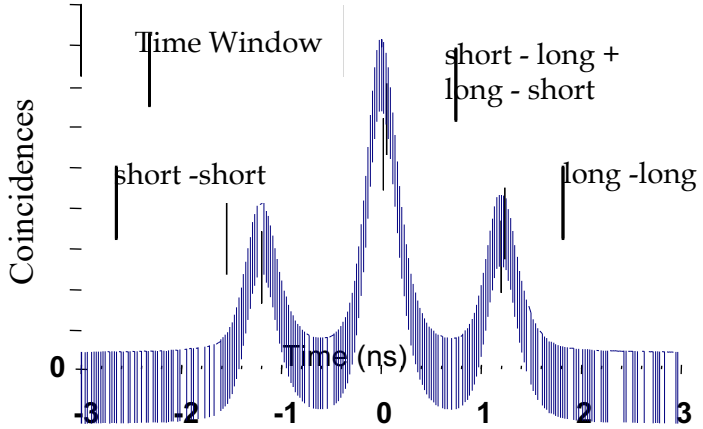


Bases

Compatible:	Alice $\phi_A \Rightarrow D_i$	Incompatible: Alice and Bob ??
$(\phi_A - \phi_B = n\pi)$	Bob $D_i \Rightarrow \phi_A$	$(\phi_A - \phi_B = \pm\pi/2)$

Time-bin for phase coding on long distance





Problems:

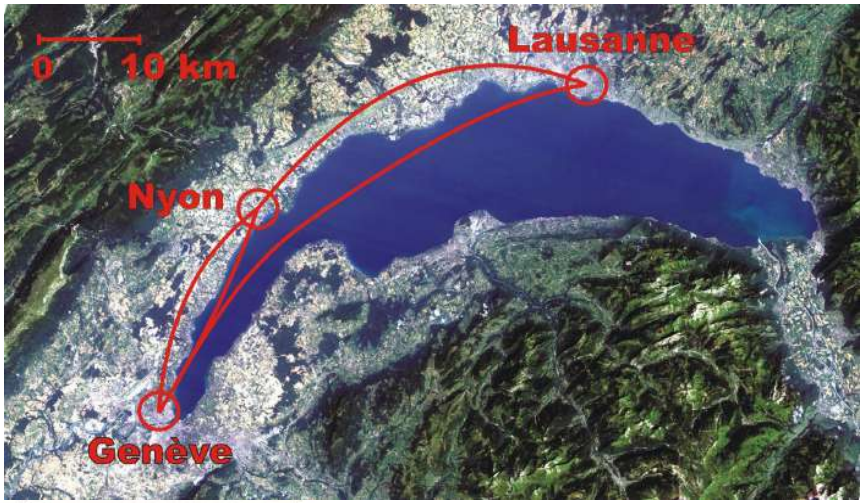
- stabilization of the path difference → active feedback control
- stability of the interfering polarization states

Stability of a 20 km long interferometer?

The Plug-&-Play configuration: Telecom distances reached

- Round-trip system, with Faraday rotators
- Simplicity, self-stabilization J.Mod.Opt. 47, 517, 2000

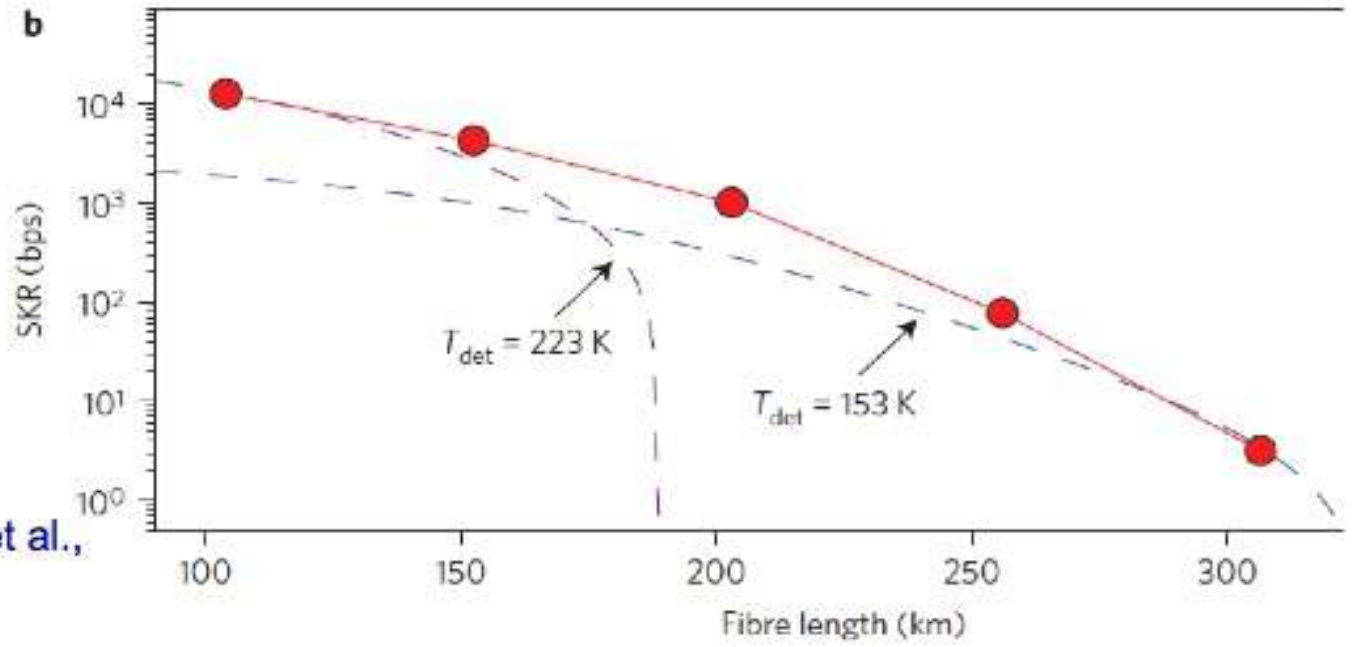
(GAP Optique - Gisin group)



(Clavis IdQ 2005, Bob) 3U - 4U, 19'' racks

QKD over 307 km with real time secret key distillation and InGaAs APDs

- Integration into ATCA blades
- Standard telecom format

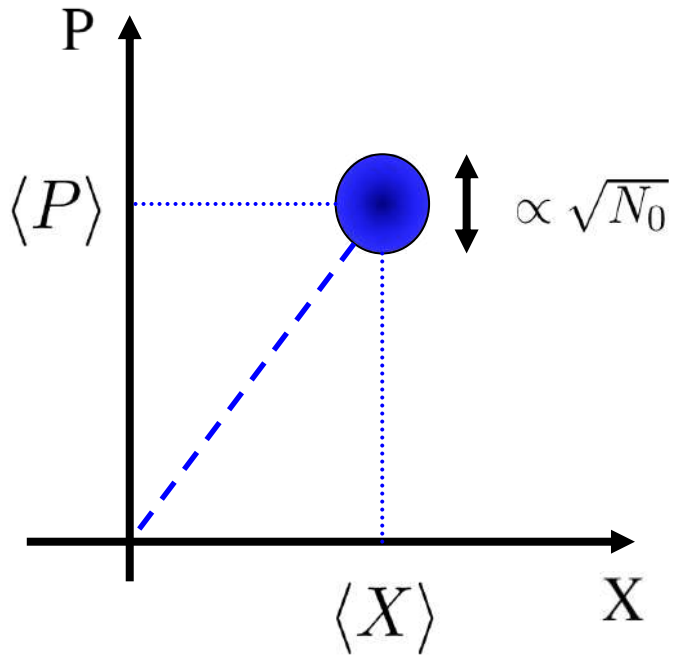


B. Korzh, C. W. Lim et al.,
Nature Photonics
9, 163-168 (2015)

GAP Quantique

CV-QKD
(Discrete Variable QKD)

Encoding information on light quadratures: Continuous Variables

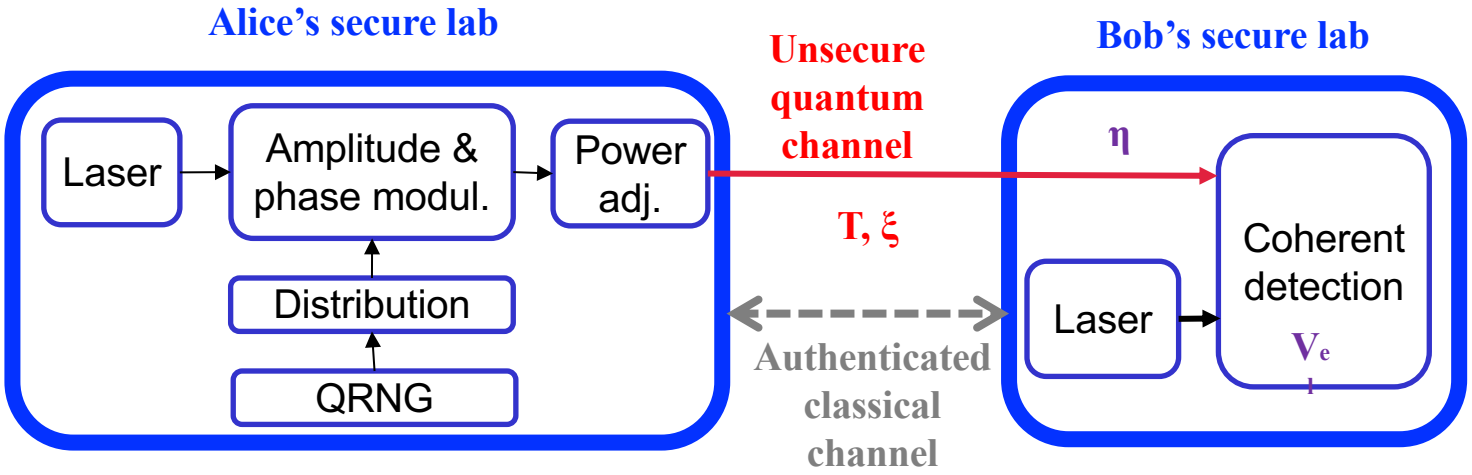


$$\left[\hat{X}, \hat{P}\right] = 2iN_0$$

$$\Delta X \Delta P \geq N_0$$

N_0 : bruit de photon

CV-QKD typical set-up



I. Alice generates a random distribution of variance V_A

II. The channel introduces losses. Transmittance **T**

III. The detector has noise (V_{el}) and limited efficiency **η**

IV. Imperfections (excess noise) **ξ**

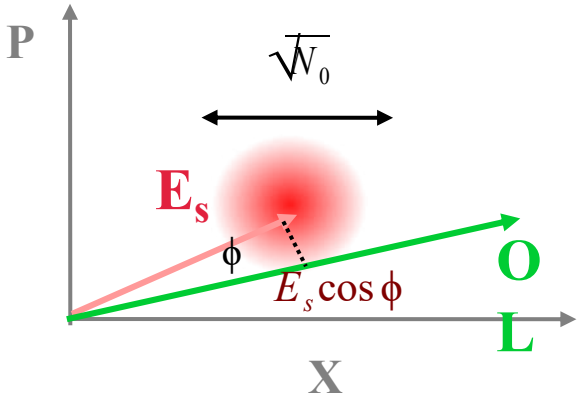
Calibrated or Estimated during protocol execution

ξ is attributed to the attacker (Eve)

Encoding information and sending information

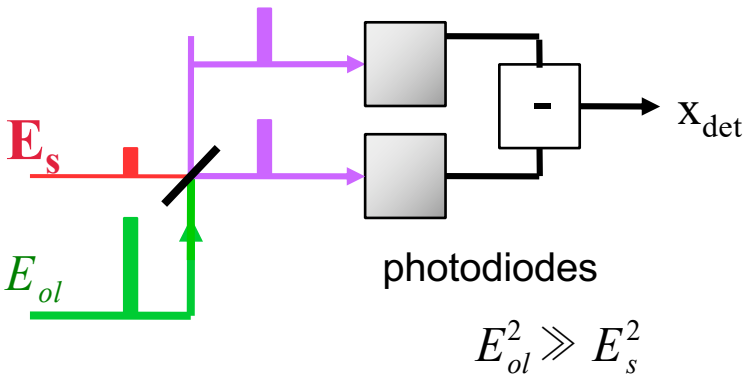
Coherent state encoding is a practical choice

➔ **Use standard laser, phase modulator and amplitude modulator to modulate quadratures x_A,p_A**



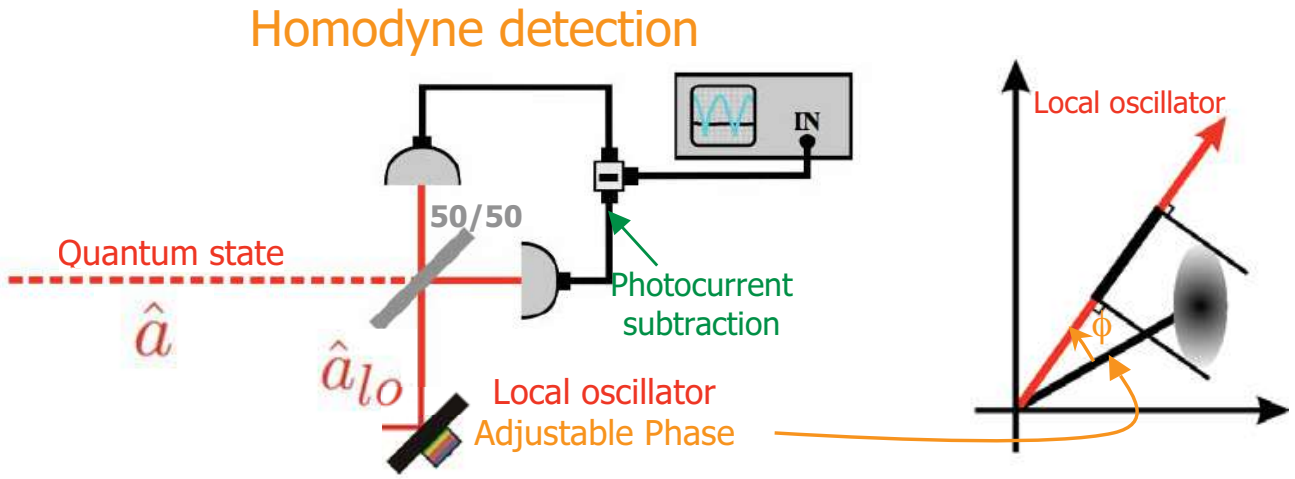
➔ **Coherent receiver at reception**
(homodyne or heterodyne)

Modulating OL phase
➔ choice of quadrature measurement



Homodyne Measurement noise: shot noise N_0 + electronic noise v_{elec}

Measuring quadrature: homodyne



- Annihilation operators of the mixed modes: $\hat{a}_1 = \frac{\hat{a} + \hat{a}_{lo}}{\sqrt{2}}$ $\hat{a}_2 = \frac{\hat{a} - \hat{a}_{lo}}{\sqrt{2}}$

- After subtraction, the resulting photocurrent operator is:

$$\hat{N}_- = \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2 = \hat{a}^\dagger \hat{a}_{lo} - \hat{a}_{ol}^\dagger \hat{a}$$

- Mean Value and variance for $|\psi\rangle \otimes |\alpha e^{i\phi}\rangle$:

$$\langle \hat{N}_- \rangle = \alpha \langle \psi | \hat{a}^\dagger e^{i\phi} + \hat{a} e^{-i\phi} | \psi \rangle = \alpha \langle \psi | \hat{p}_\phi | \psi \rangle$$

$$V(\hat{N}_-) = \alpha^2 V(\hat{p}_\phi) + \langle \psi | \hat{a}^\dagger \hat{a} | \psi \rangle$$

For large photon number in lo:

$$V(\hat{N}_-) \simeq \alpha^2 V(\hat{p}_\phi)$$

Credit : Julien Laurat

☺ **CV-QKD can be implemented with standard telecom components**

😐 **Specific requirements:**

- Need to share a Phase reference
- Noise Homodyne receiver noise:

➔ V_{elec} (electronic thermal noise) << N_0 (Shot Noise)

➔ **« Shot noise limited receiver »**

☺ **Shot noise limited coherent receivers are commercially available**

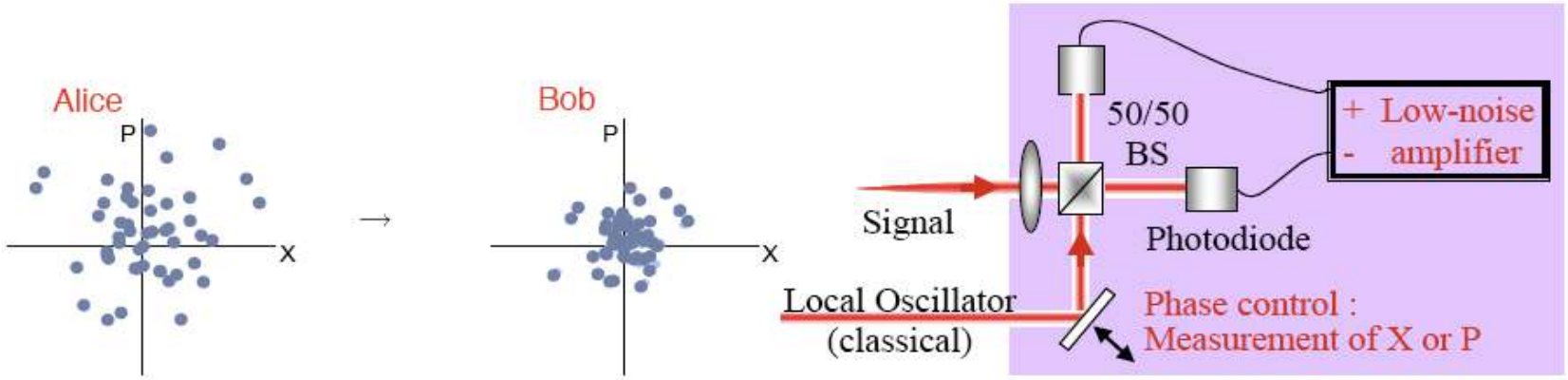
Exalos
380 MHz
bandwidth

Wieserlabs
400 MHz
bandwidth

Thorlabs
100MHz -> 1
GHz bandwidth

Finisar
CPRV
Several GHz
bandwidth

Gaussian Modulated Continuous Variable QKD



Alice encodes continuous information in amplitude and phase by sending randomly modulated coherent states with a Gaussian distribution.

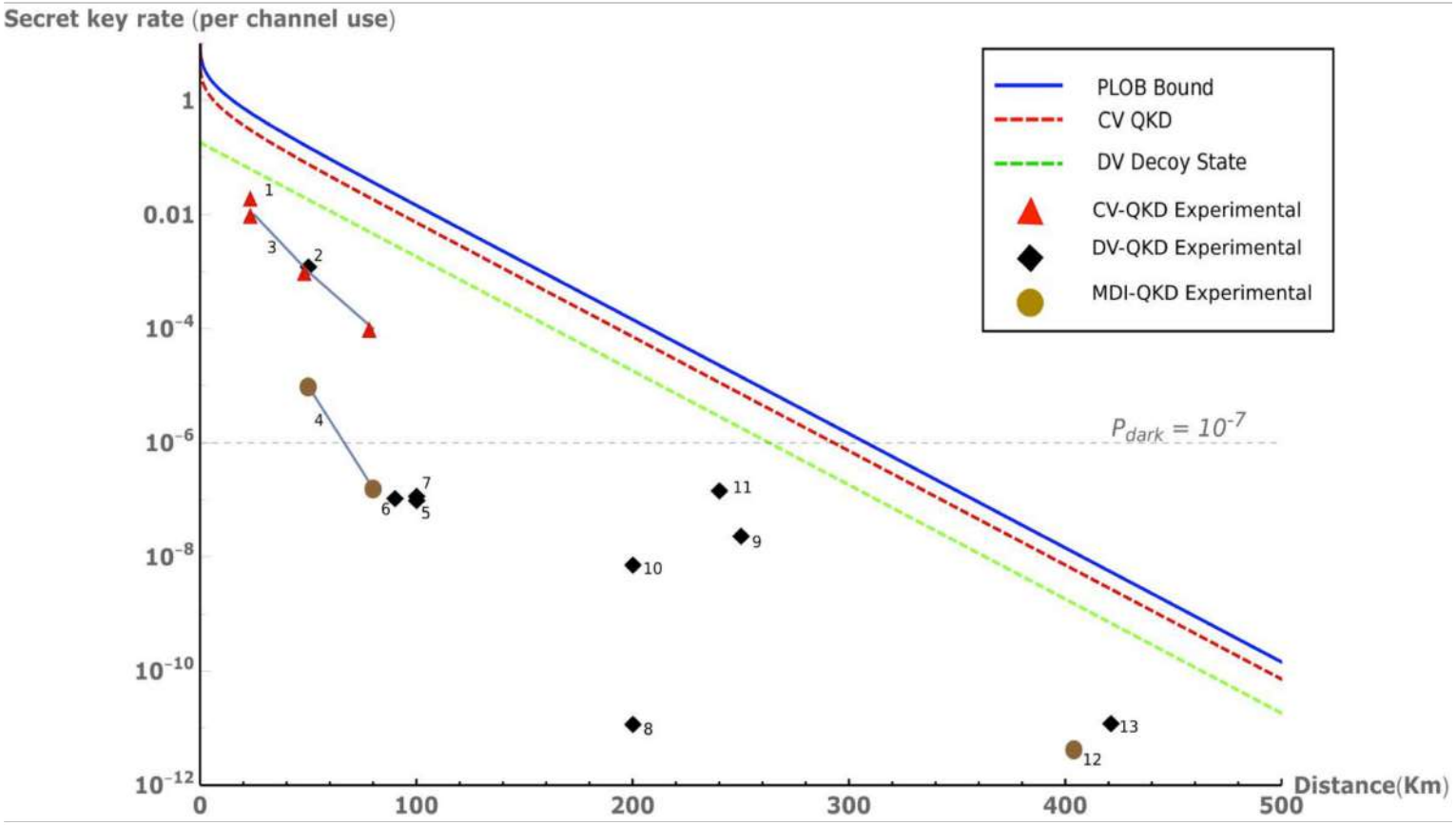
Bob uses a homodyne (interferometric) detection.

Grosshans, Grangier, PRL 88 057902

CV and DV technology: some elements of comparison

DV-QKD	CV-QKD
Long reachable distance achievable with current detectors Typically 150 km- 200 km can be reached (1 bit/s limit around ~**300 km**)	More sensitive to loss Distance limit demonstrated: - 25 km in 2010 ~ **150 km** in 2020
☺ DV-QKD key rate is not too sensitive to reconciliation efficiency	CV-QKD has more complex post processing, ➔ Need for specific highly efficient error correction codes
Single photon detectors ☹ Need to be cooled	Coherent detectors ☺ Can be operated at room temperature
Single photon detectors are sensitive to stray light => WDM integration requires high filtering	Coherent detector act as high-finess filters => well fit for WDM integration
No need of phase reference (phase randomization is actually better for security)	Need of a shared phase reference between Alice and Bob ➔ can be deal with DSP in high speed systemss

Overview: Achieved QKD performance vs theoretical bound



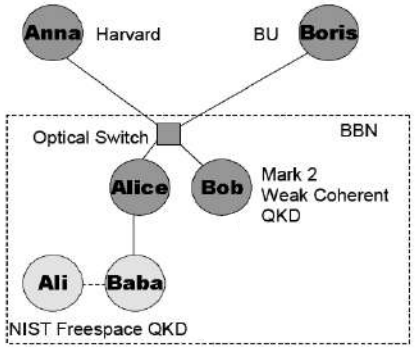
Cooling detectors to very low temperature

Dmax can reach *(rque: R(Dmax) ~1 bit/s)*

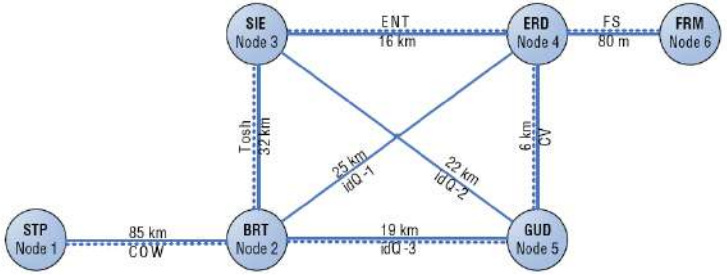
400 km, lab environment, low-loss fiber, superconducting detector
250 km, lab environment, dark fiber, avalanche photodiode
150 km, field deployment, dark fiber, avalanche photodiode
~ 100 km, field deployment, WDM , avalanche photodiode / CV receiver

QKD Networks – overview of major prototypes

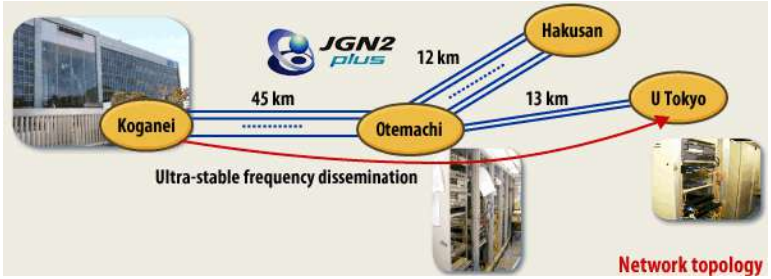
DARPA – BBN **2005**



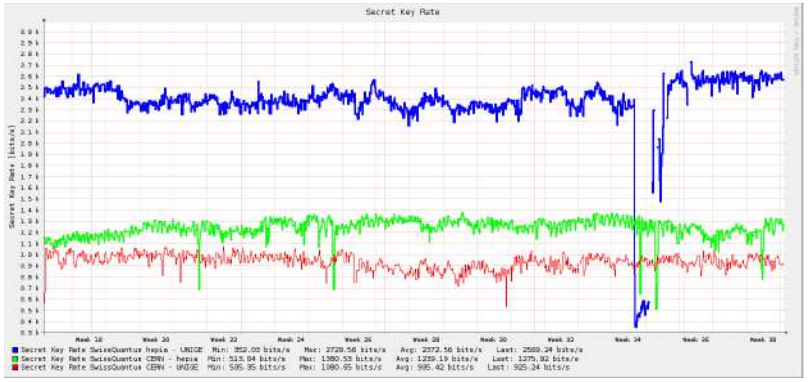
SECOQC **2008**



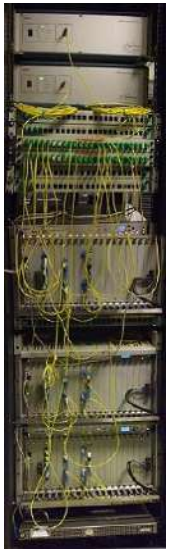
Tokyo QKD Network **2010**

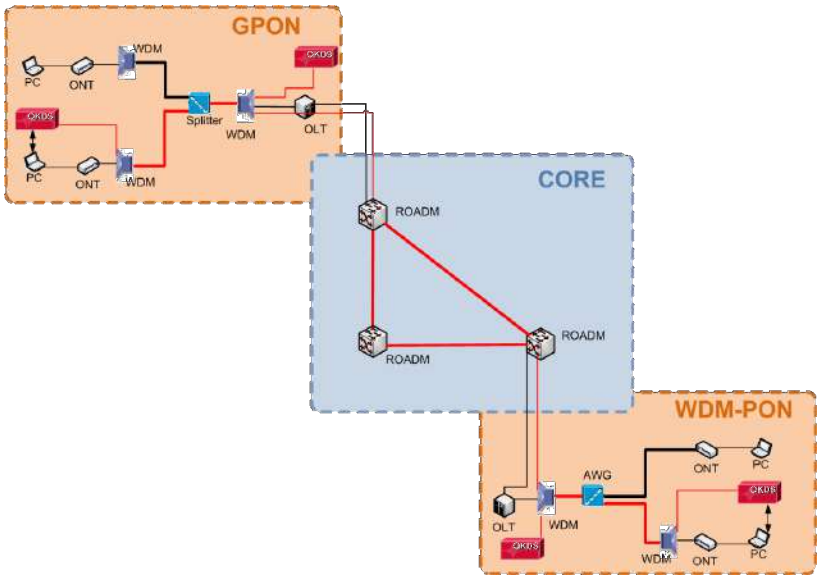


Testbeds to move further towards real-life industrial use of QKD



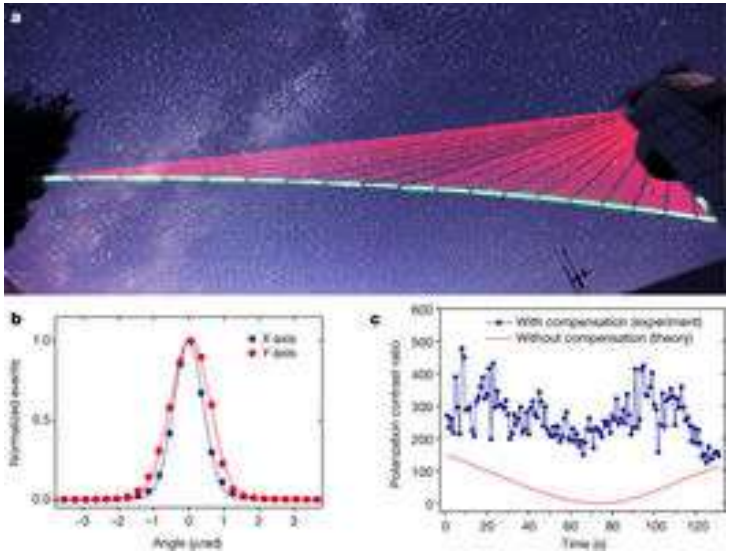
SwissQuantum: Stable operation from April 2009 to November 2009

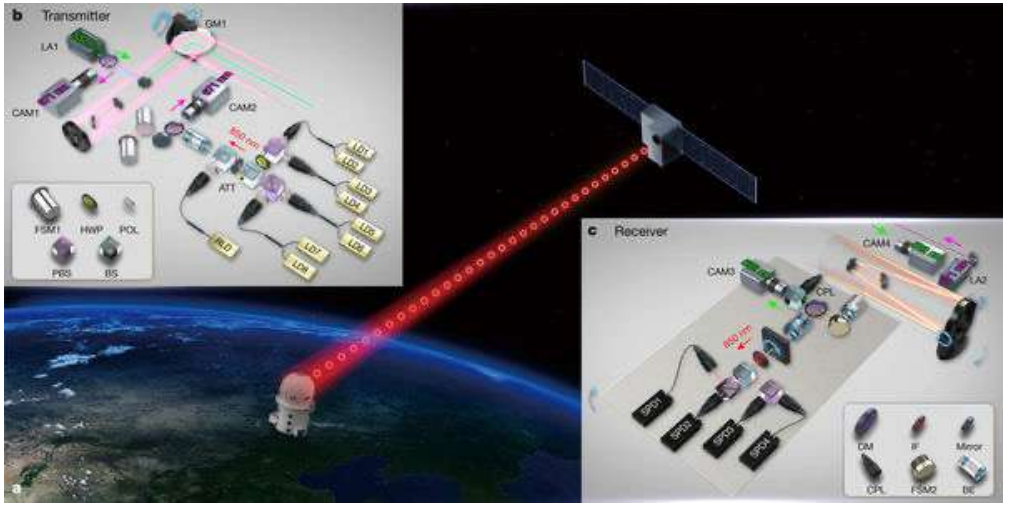




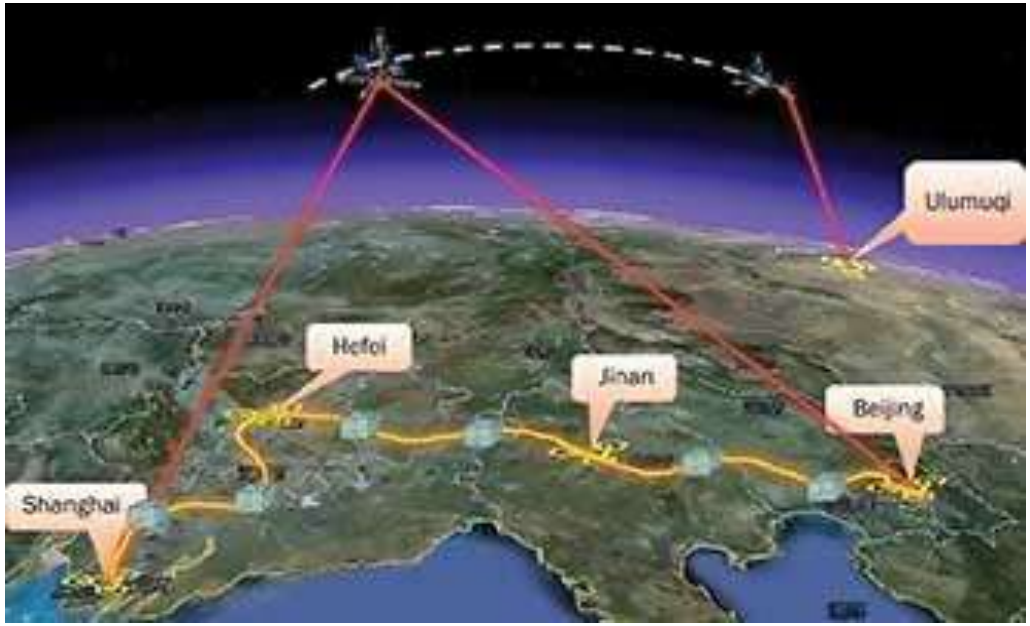
The Madrid QKD Test-Bed: WDM + optical network integration

2012-17: Major steps demonstrated in China
Q Satellite (Micius) + Large-scale Ground QKD network





- Bell violation over 1200 km
- Ground to satellite QKD



2000 km QKD Network
+ Highly connected Nodes
➔ QKD industry

QKD industry: global acceleration, strong drive in Asia

- Significant Q Comm industry in **China**: QuantumCTek, Qasky, Quantum Cas Networks,…

-Toshiba (JP and UK)

➔ high rate QKD, market release in 2020

- SK Telecom acquires IDQuantique(Feb 2017)

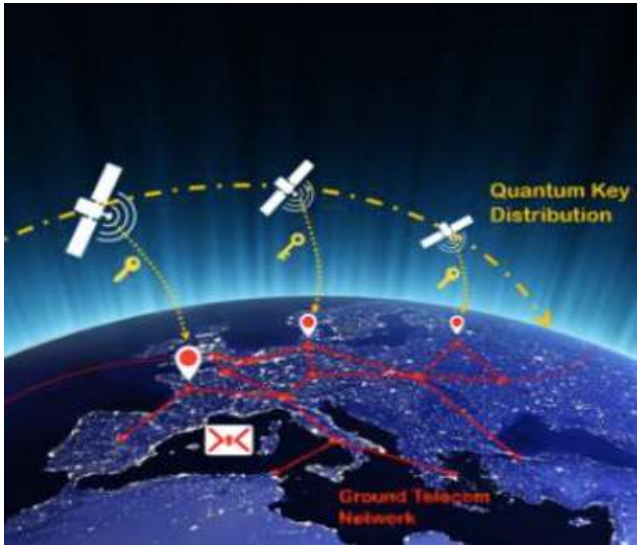
➔ Deploy to strengthen security of 5G Network

-QuantumXChange launches commercial QKD service in NYC-Boston

-SeQureNet had a commercial activity In (FR, JP, USA, CN)

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

European Quantum Communication Infrastructure (EuroQCI)



Initiated by the European Commission in 2019

Aims at the **deployment**, by **2030**, of a pan-European **publicly controlled secure quantum communication infrastructure** linking selected EU strategic sites by using **both terrestrial and space links**.

Signature of the 27 EU countries
Important foreseen investments in FP9 [Digital Europe]

Telecom Paris *participates in two successive industry-driven EuroQCI Studies, for the European Commission*

- ***QOSAC*** *(Jan-Oct 2020)*
- ***QSAFE-QCI4EU*** *(Mar 2021- Jun2022)*

➔ ***(Job) Opportunities for Future Quantum Engineers, in Europe !***

Some Future Challenges
and
Research directions

Telecom Paris impliqués dans 2 projets du Quantum Technology Flagship, pilier Q Communications, depuis 2018

CiViQ

Continuous Variable Quantum Communication

European Quantum Technology Flagship Project: 2018-2021

21 Partners, 3 years, 10 M€ budget

Q Comm R&D, Telecom Manufacturers, Network Operators

ICFO · AIT Austrian Institute of Technology · MPL Max Planck Institute for the Science of Light · Politécnica · International Campus of Excellence · VLC Photonics · Nokia Bell Labs · Mellanox Technologies · NEXTWORKS Engineering Forward · T · cnrs · Telecom ParisTech · Une école de l'IMT · Inria inventors for the digital world · University of York · Palacký University Olomouc · DTU · Fraunhofer Heinrich-Hertz-Institut · coriant · QUSIDE · HUAWEI · orange · Telefónica

OPENQKD

European QKD Testbed

European Quantum Technology Flagship Project: 2019-2022

38 Partners, 3 years, 15 M€ budget

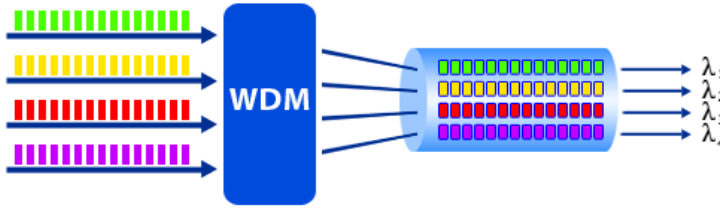
QKD and Encryption Suppliers, Telecom and Aeorospace industry, Standardization bodies, QKD and Network R&D, Early Adopters

➔ 16 Test Sites **(incl. Paris)** Use-case demonstrations, Standards

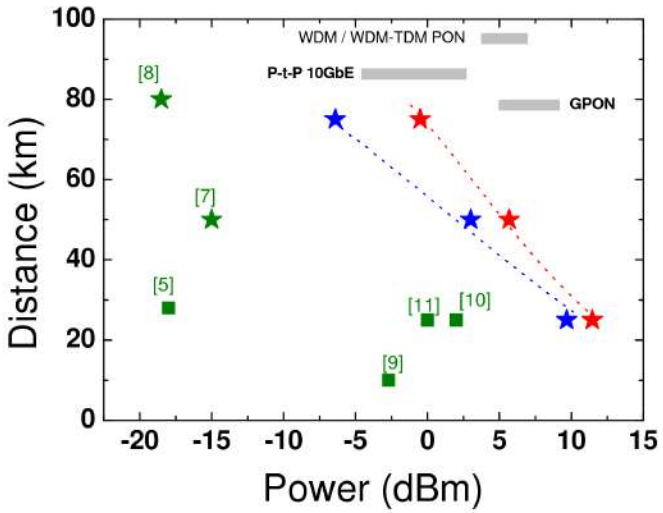
➔ ***Precursor of Euro QCI***

Towards Mass-Market QKD

WDM integration of CV-QKD



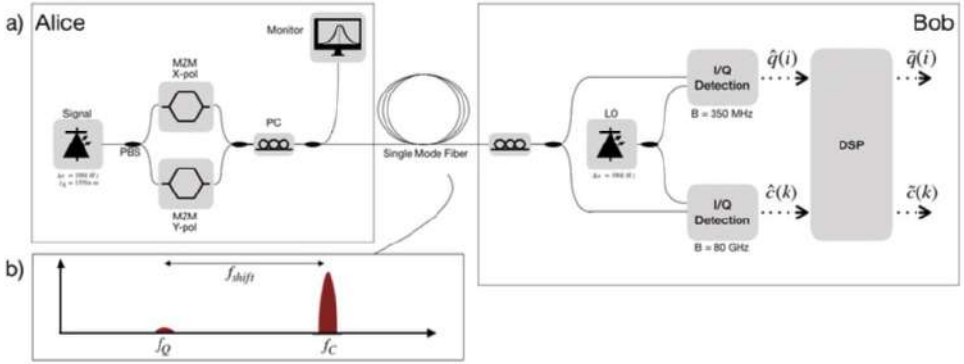
R. Kumar, H. Qin and RA
Coexistence of continuous variable QKD with intense DWDM classical channels.
New Journal of Physics, 17(4), 043027. (2015).

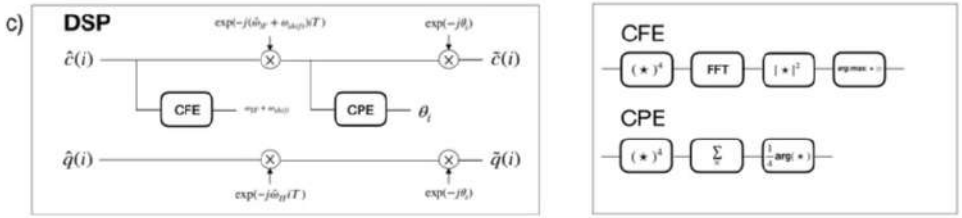


CV-QKD strong WDM coexistence (10 dBm @ 25 km) favored by coh detection

Convergence with classical coherent comm systems

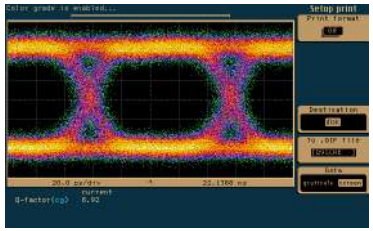
"Local" Local oscillator with affordable laser / modulator

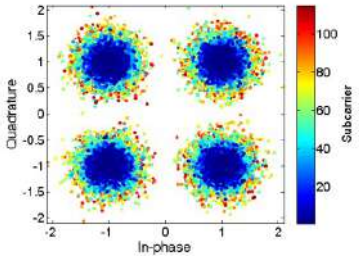




Adrien Marie and RA
*Self-coherent phase reference sharing for continuous-variable quantum key distribution Phys. Rev. A **95**, 012316, (2017)*

Q Communication over a state-of-the-art optical communication platform (Telecom Convergence)





Collaboration avec équipe GTO- Telecom Paris (Yves Jaouen, Cédric Ware)

Plateforme 40 Gb/s à l'état de l'art + détecteurs cohérents « quantiques »

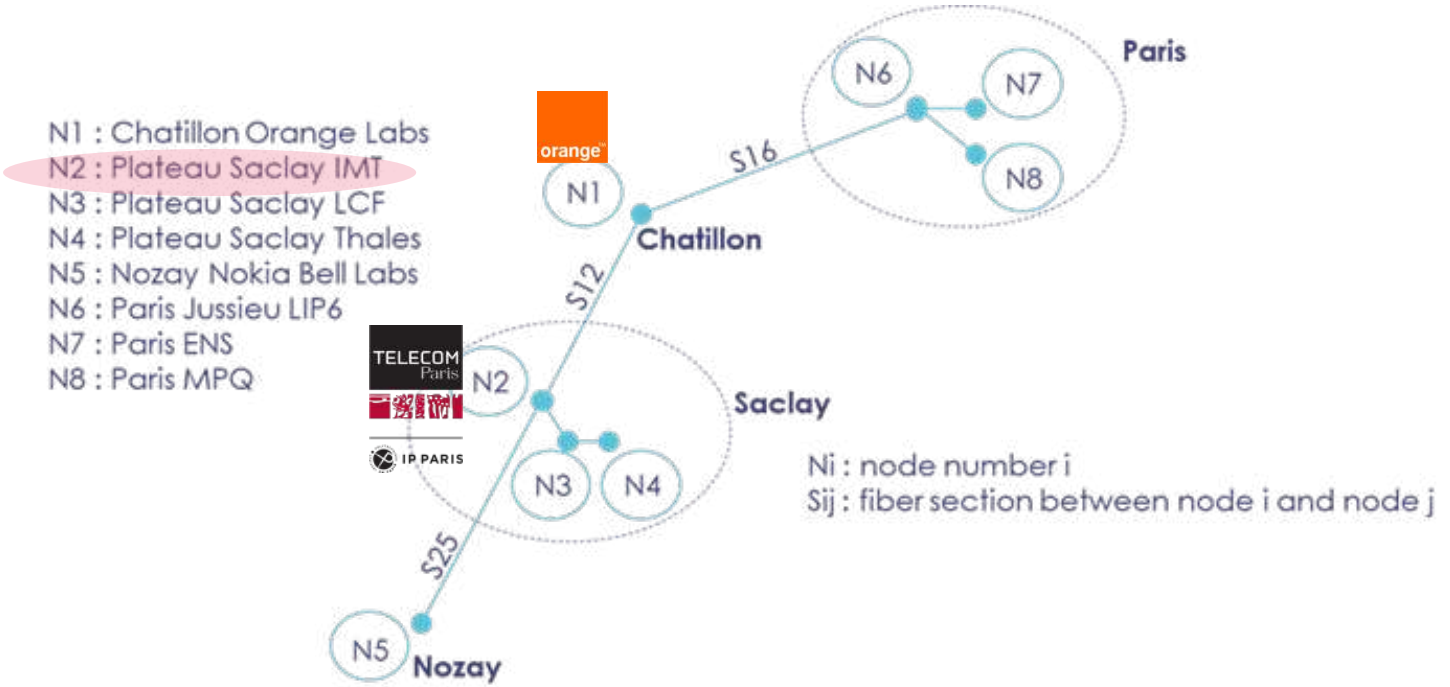
Quantum Communication Network Deployment and Testbed in Paris Region

ParisRegion QCI 2021-2023
Projet Région IDF, mostly industry
Orange (Coord), Thales, Nokia, Kets, Quandela, VeriQloud, IOGS, LIP6, Telecom Paris.

ParisQCI: 2021-2024
Projet SIRTEQ SYNERGIE
mostly academic (Q Internet)
LIP6 (coord), MPQ, LKB, C2N, LCF, Telecom Paris.

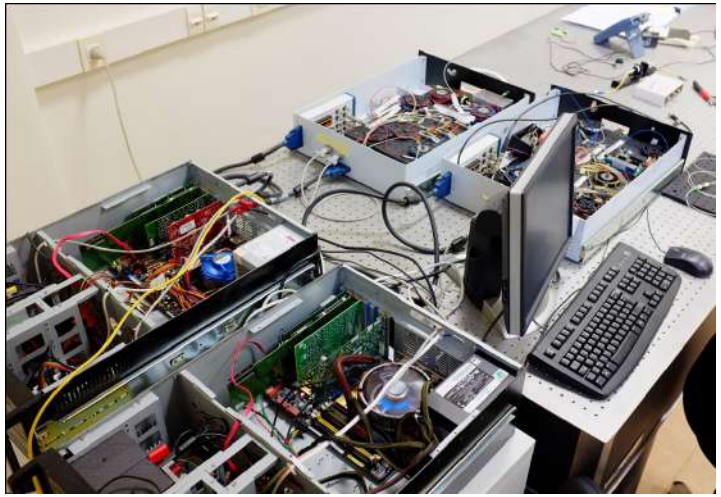
Network operated By Orange
Deployment launched Q2 2021

→ *First step towards national French Q network (with UCA Nice) in EuroQCI*

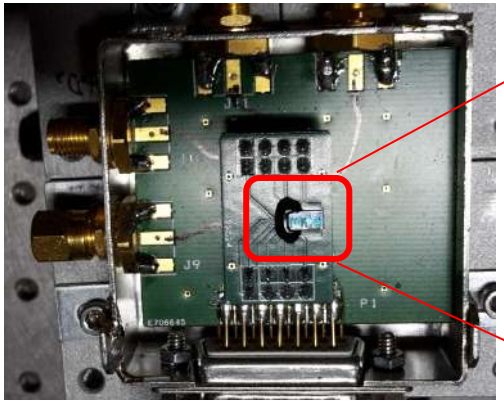


Photonic integration of QKD technology

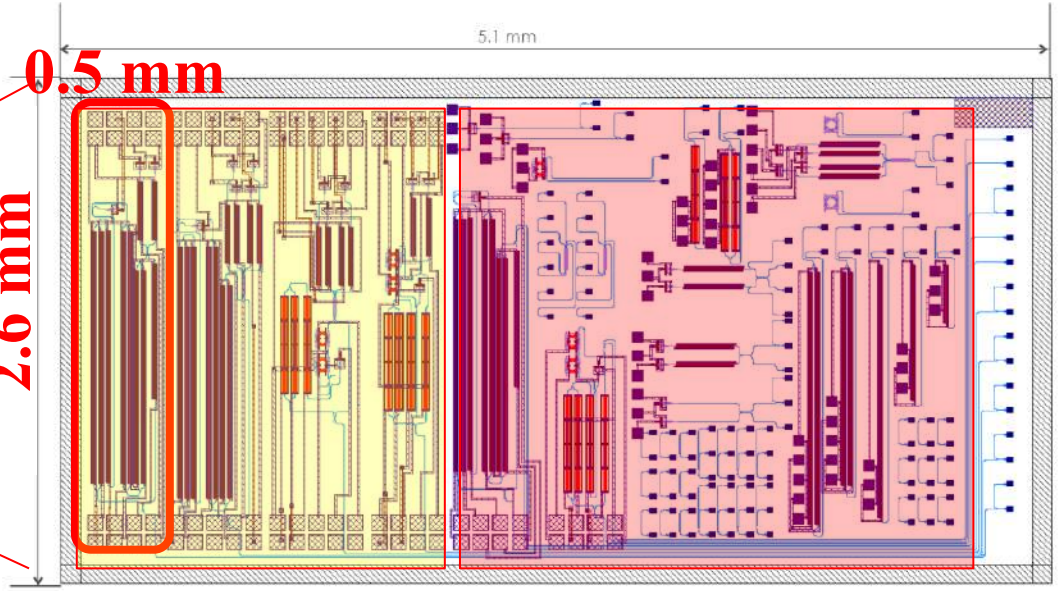
Integration allows for scalable, low cost quantum cryptographic implementations



Smaller, cheaper, CMOS-compatible



OPSIS – IME Foundry



nature photonics

Letter

Nature Photonics **4**, 686 - 689 (2010)
Published online: 29 August 2010 | doi:10.1038/nphoton.2010.214

Subject Category: Quantum optics

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen[1,2], Carlos Wiechers[3,4,5], Christoffer Wittmann[3,4], Dominique Elser[3,4], Johannes Skaar[1,2] & Vadim Makarov[1]

Press release

Vulnerability in commercial quantum cryptography tackled by international collaboration

August 29, 2010

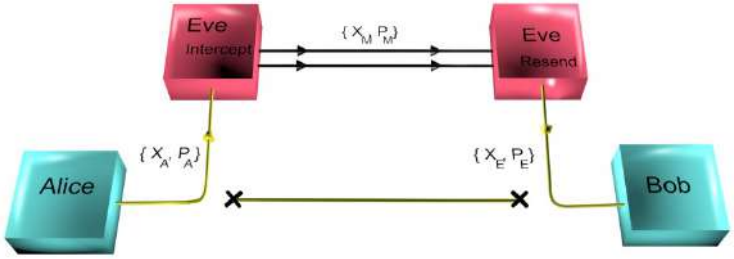
The Norwegian University of Science and Technology (NTNU) and the University of Erlangen-Nürnberg together with the Max Planck Institute for the Science of Light in Erlangen have recently developed and tested a technique exploiting imperfections in quantum cryptography systems to implement an attack. Countermeasures were also implemented within an ongoing collaboration with leading manufacturer ID Quantique.

Attacks on QKD implementations are possible ➔ Implementation Security Challenge

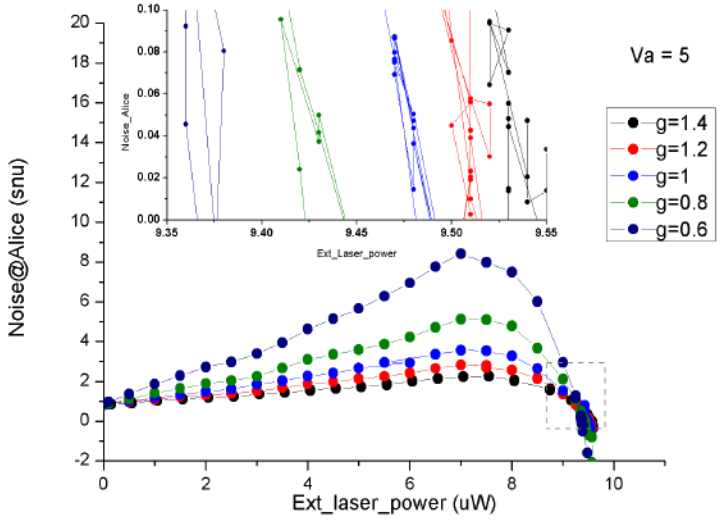
- Large pulse attack (Trojan horse)
  - Back reflection intense pulse — Vakhitow et al 2001
  - OTDR/OFDR — Gisin et al. 2006
- Side channel
  - Detector flash back — Linares et al 2001
  - Spectral, temporal source properties — Nauerth et al 2011
- Detector efficiency mismatch
  - Temporal mismatch — Zhao et al . 2008
  - Superlinear detector response — Lydersen et al 2011
- Active detector control
  - Steer actively quenched APD — Makarov et al 2009
  - Photoelectrical blinding — Lydersen et al 2010

Build Certified QKD (Q Hardware) Implementations

Security Evaluation of QKD implementation



Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alléaum
Experimental vulnerability analysis of QKD based on attack ratings
arXiv:2010.07815



ETSI QKD Industry Standardization Group

International group of experts (academics & industry)

- Metrology, Q Comm Device Characterization
- QKD and Networking: interfaces, deployment parameters
- **Implementation Security and Certification**

OPENQKD (Flagship project 2019-2022)

- Quantum Hacking
- **Protection Profile for QKD**

OPEN QKD

European QKD Testbed

European Quantum Technology Flagship Project: 2019-2022

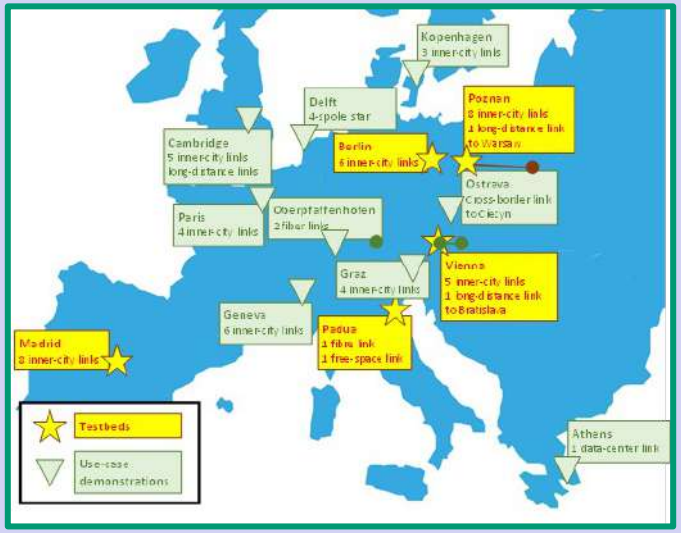
38 Partners, 3 years, 15 M€ budget

QKD and Encryption Suppliers, Telecom and Aeorospace industry, Standardization bodies, QKD and Network R&D, Early Adopters

- **4 Test-Beds and 16 Test Sites (incl. Paris)**
- **Use-case-driven demonstrations**

(government, health, cloud, telecom, satelite)

- **Standardized interfaces**
- **Security Certification**
- **Kick-start a competitive European QKD industry**

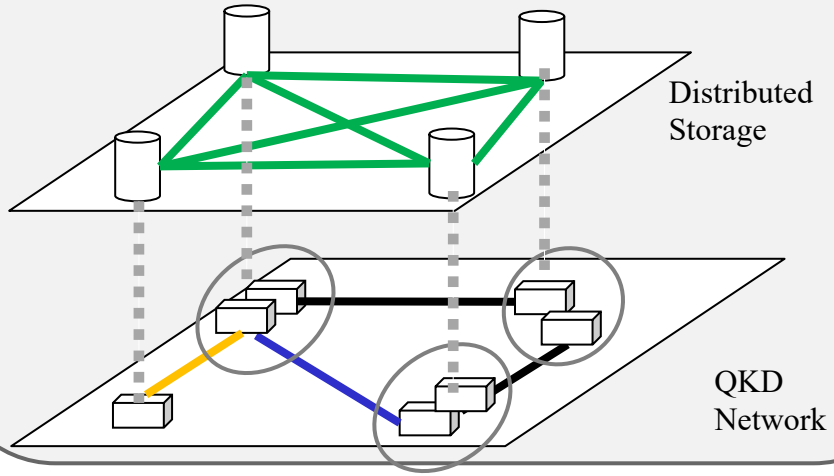


Long-Term Secure Storage

Need:
Confidentiality (integrity, availability) over 30+ years

Principle: Proactive Secret Sharing
➔ Protects against storage node corruption

Requirements:
- Distributed Storage Infrastructure
- Secure Communication with ITS
  - *Impossible Classically*
  - ➔ ***QKD + OTP***



Initial demonstration

Braun, Johannes, J. Buchmann et al. "LINCOS: A storage system providing long-term integrity, authenticity, and confidentiality." *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 2017.

+ 2 OpenQKD Use-Cases & Pilot implementations in Japan

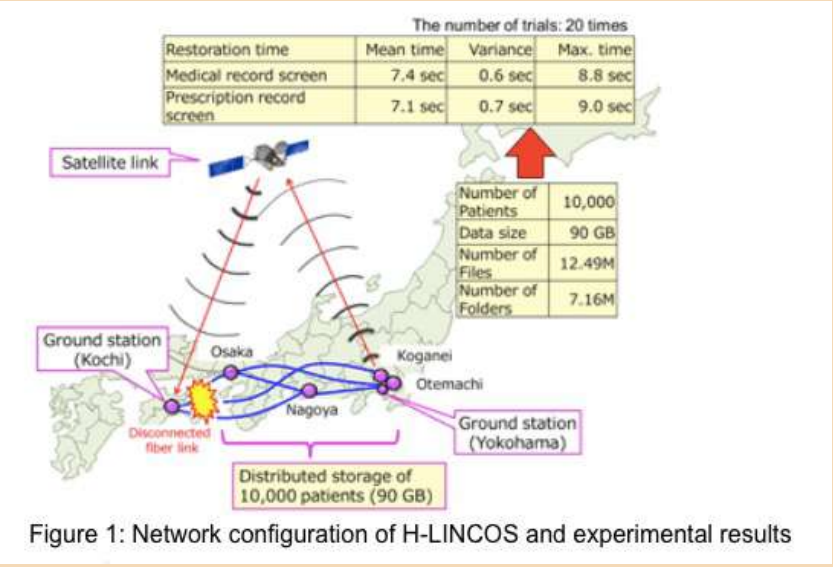
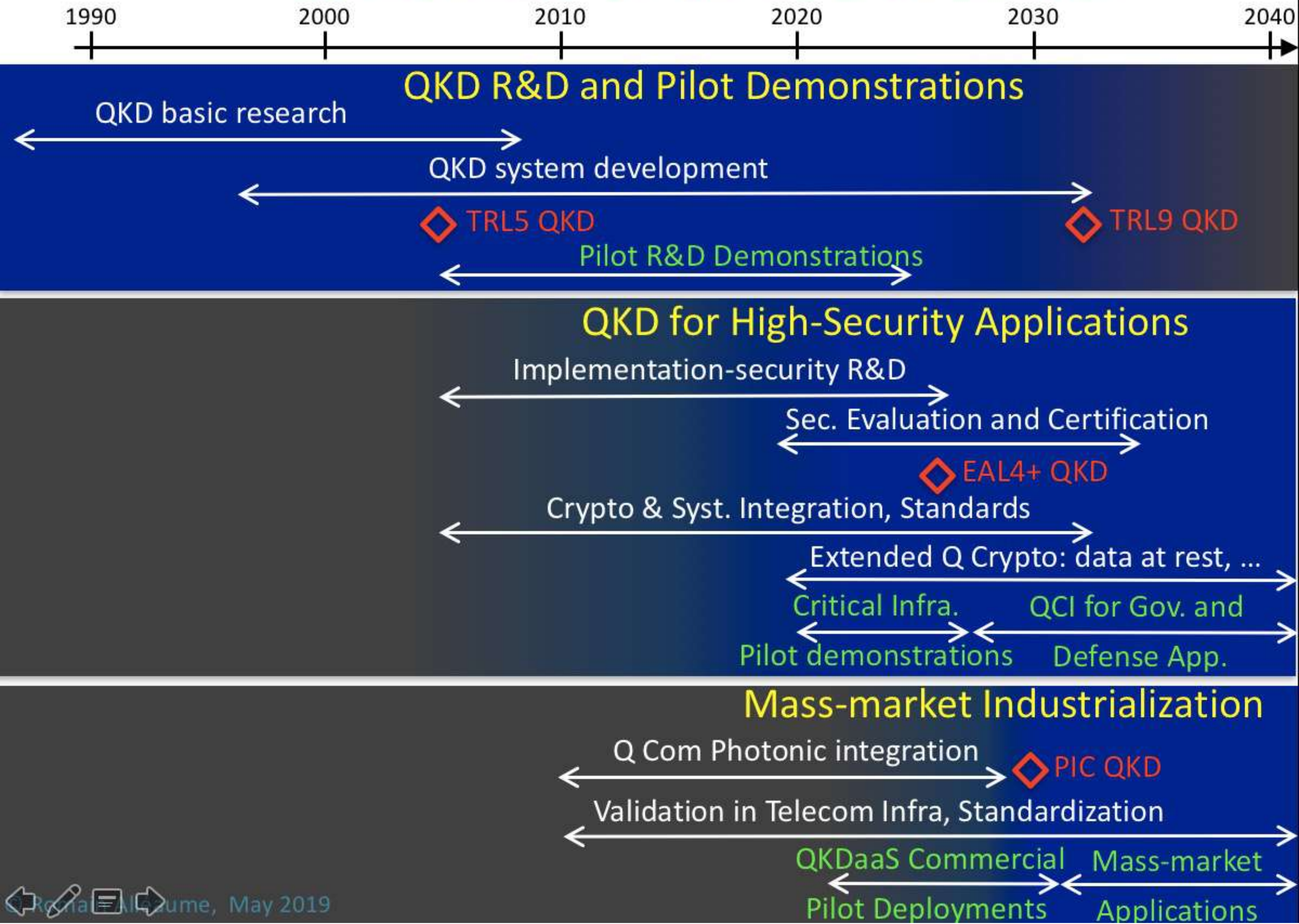
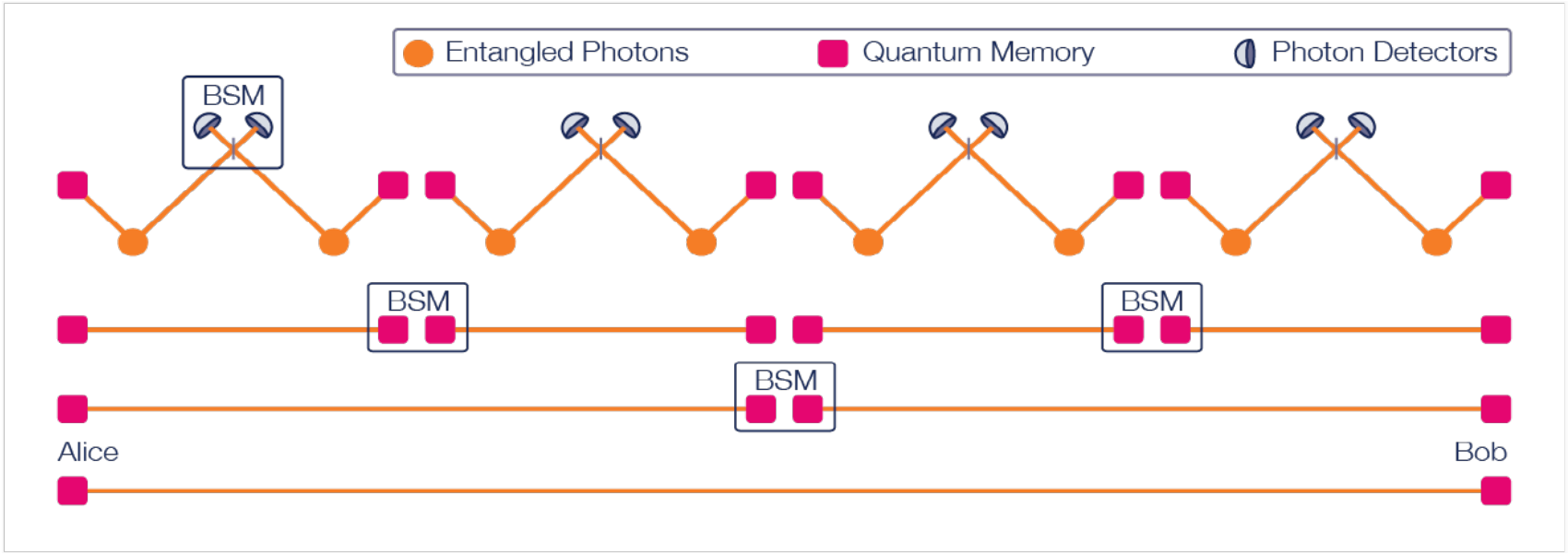


Figure 1: Network configuration of H-LINCOS and experimental results

QCI: ROADMAP FOR QKD INDUSTRIALIZATION



Long-term vision for Q networks: Quantum Internet



Planned demonstration in 2021: Early network of Entangled Q memories

Quantum Internet Alliance Flagship Project

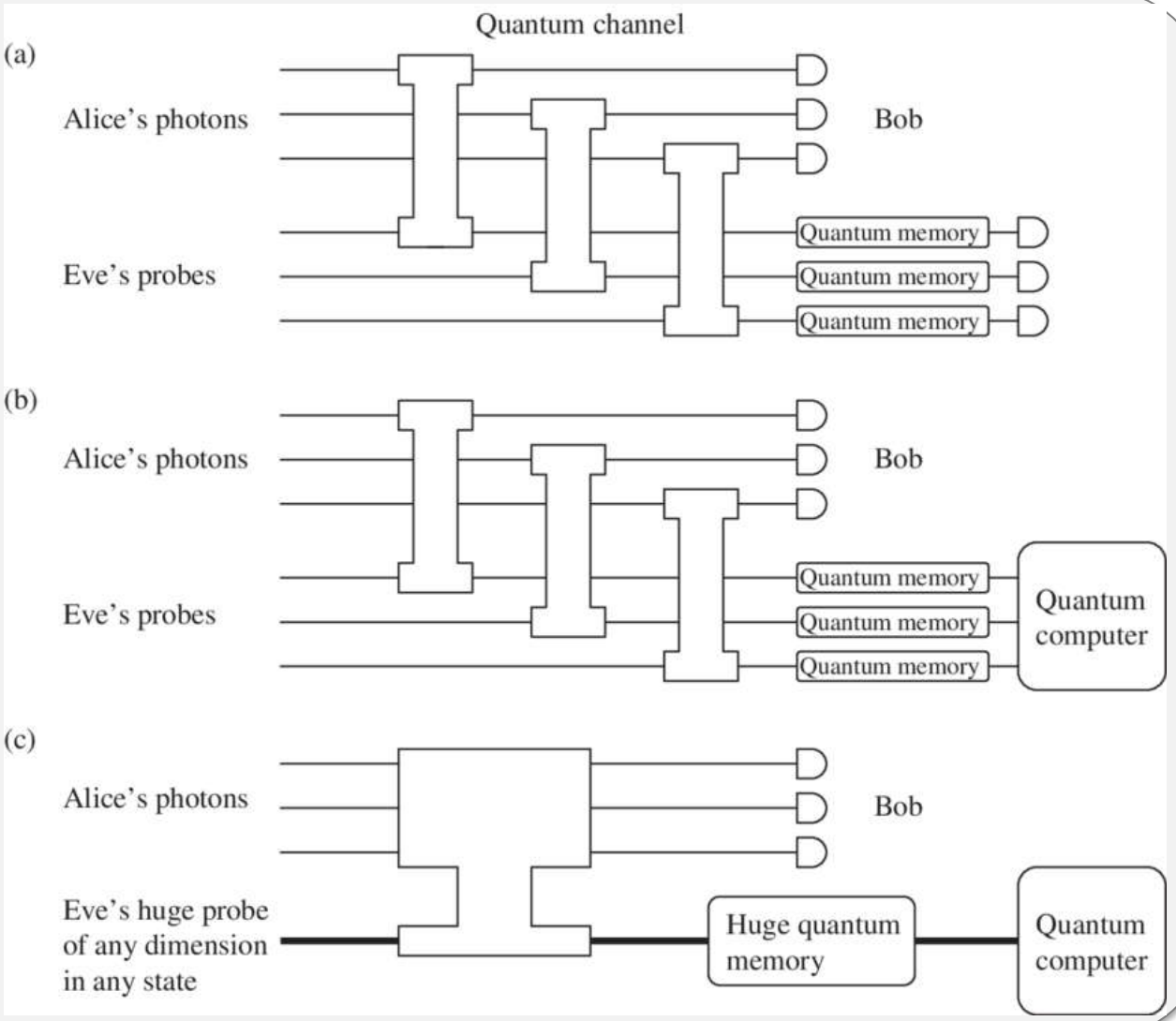
Bonus:
Let's go more Quantitative / Technical about QKD Security

Différentes classes d'attaque d'Eve envisageables

Attaques individuelles:
interaction **indiv** et mesure **indiv** Eve

Attaques collectives :
interaction **indiv** et mesure **jointe** Eve

Attaques cohérentes:
interaction et mesure **arbitraires** Eve



Security proofs are known for the early QKD protocols, but remain an active domain of research

Secure key rate: (depends on Eve attack powr)

Main idea : Csiszar Körner, (for classical correlated data X_A, X_B, X_E),

$R(X_A ; X_B \| X_C) \geq$

$\max [\quad I(X_A ; X_B) - I(X_A ; X_E) \quad , \quad I(X_B ; X_A) - I(X_B ; X_E) \quad]$

- **Direct reconcilation: $R \geq I(X_A ; X_B) - I(X_A ; X_E)$**
- Reverse reconciliation: $R \geq I(X_B ; X_A) - I(X_B ; X_E)$

Generalization to quantum attacker, (collective attacks), Devetak Winter

- Direct reconcilation: $R \geq I(X_A ; X_B) - \chi(X_A ; \rho_E)$
- Reverse reconciliation: $R \geq I(X_B ; X_A) - \chi(X_B ; \rho_E)$

$\chi(X_A ; \rho_E)$: Holevo bound on accessible information on X_A, given ρ_E

Exercice : Individual attacks

We consider Intercept-Resend attacks on BB84:

- With proba α Eve measures in her basis (see text)
- With proba $1-\alpha$ Eve does nothing

1) Attack in the basis $\{0, \pi/2\}$, $\{\pi/4, 3\pi/4\}$

- What is the QBER, (Quantum Bit Error Rate) as a function of α ?
- What mutual information IAE Eve can obtain about Alice's information ?
- What is the maximal tolerable value of α and thus of the noise ?

2) Compare BB84 intercept-resend attacks in basis $\{0, \pi/2\}$, $\{\pi/4, 3\pi/4\}$ and in Breidtbart basis $\{\pi/8, 5\pi/8\}$

Solution Exercice

BB84

Secret key rate

When Eve performs, with probability *alpha*, intercept-resend attacks in the BB84 basis the secret key rate is $R = I_{AB} - I_{AE} = 1 - h(\alpha/4) - \alpha/2$.

Breidbart

Secret key rate

In the Breidbart basis $\{\pi/8, 5\pi/8\}$ we thus have the following secret key rate

$$R_{Breidtbardt} = 1 - h(\alpha/4) - \alpha \times (1 - h(\sin^2(\pi/8)))$$