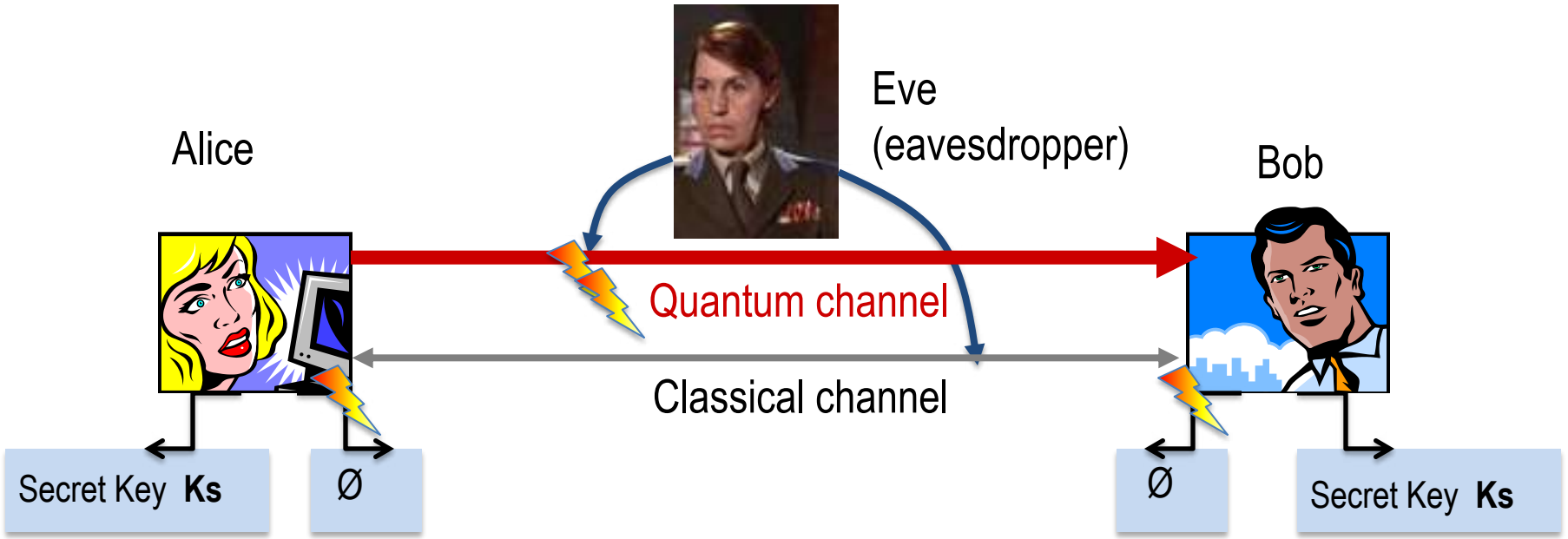
La Cryptographie Quantique à la Croisée des Chemins

Conseil Scientifique INS2I – 28 Septembre 2022

Romain Alléaume
Télécom Paris – Institut Polytechnique de Paris

romain.alleaume@telecom-paris.fr

Quantum Key Distribution (QKD) [Bennett, Brassard 84]

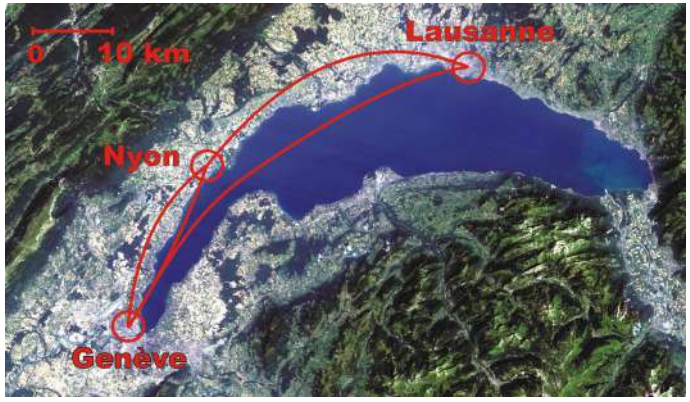


- Security based on **No-Cloning Theorem** and **Uncertainty Principle**
- Error rate statistical monitoring ➔ Bound on information leaked to Eve

QKD provides crypto advantage over computational key establishment techniques:

- no assumptions on Eve's computing power
- future-proof security

QKD Networks in ~ 2000: Real-World Deployments



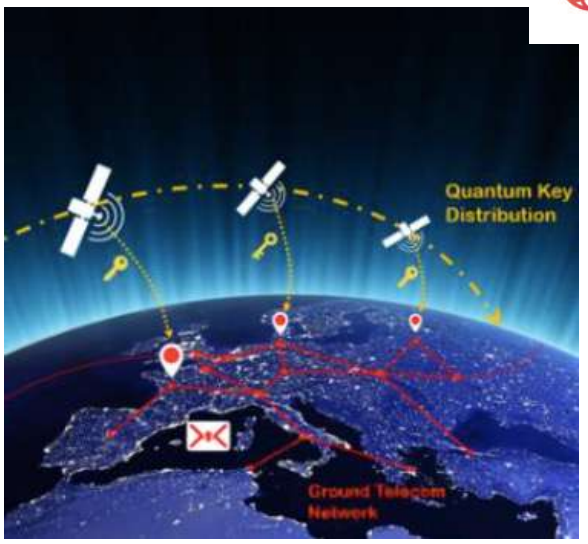
Geneva-Lausanne QKD link (1998)

First European QKD Network, Vienna (2008)

Q Networks in ~2020 Large-scale high TRL

QUANTUM FLAGSHIP

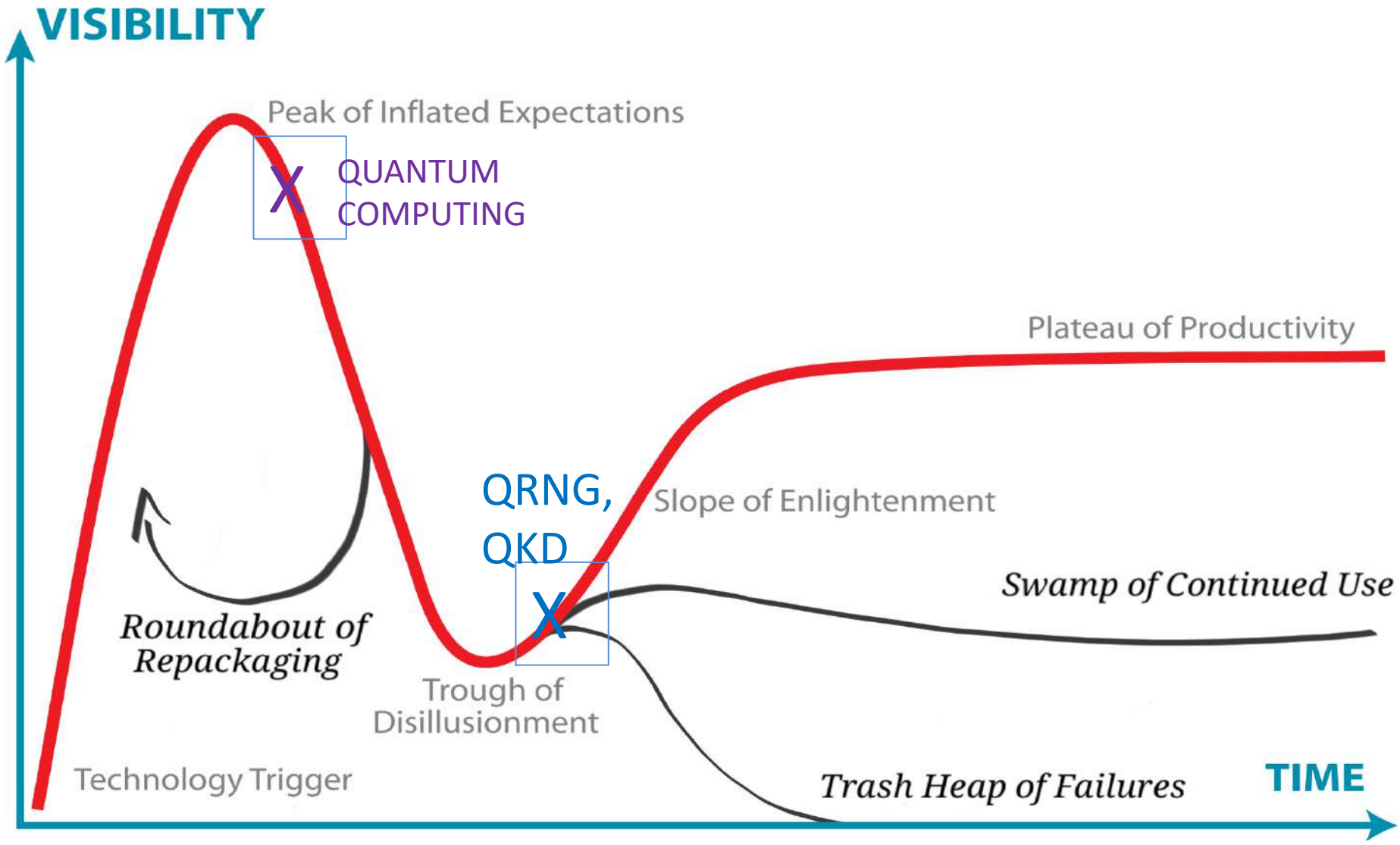
Q Satellite Micius (2016)
2000 km Ground QKD Network (2018) -

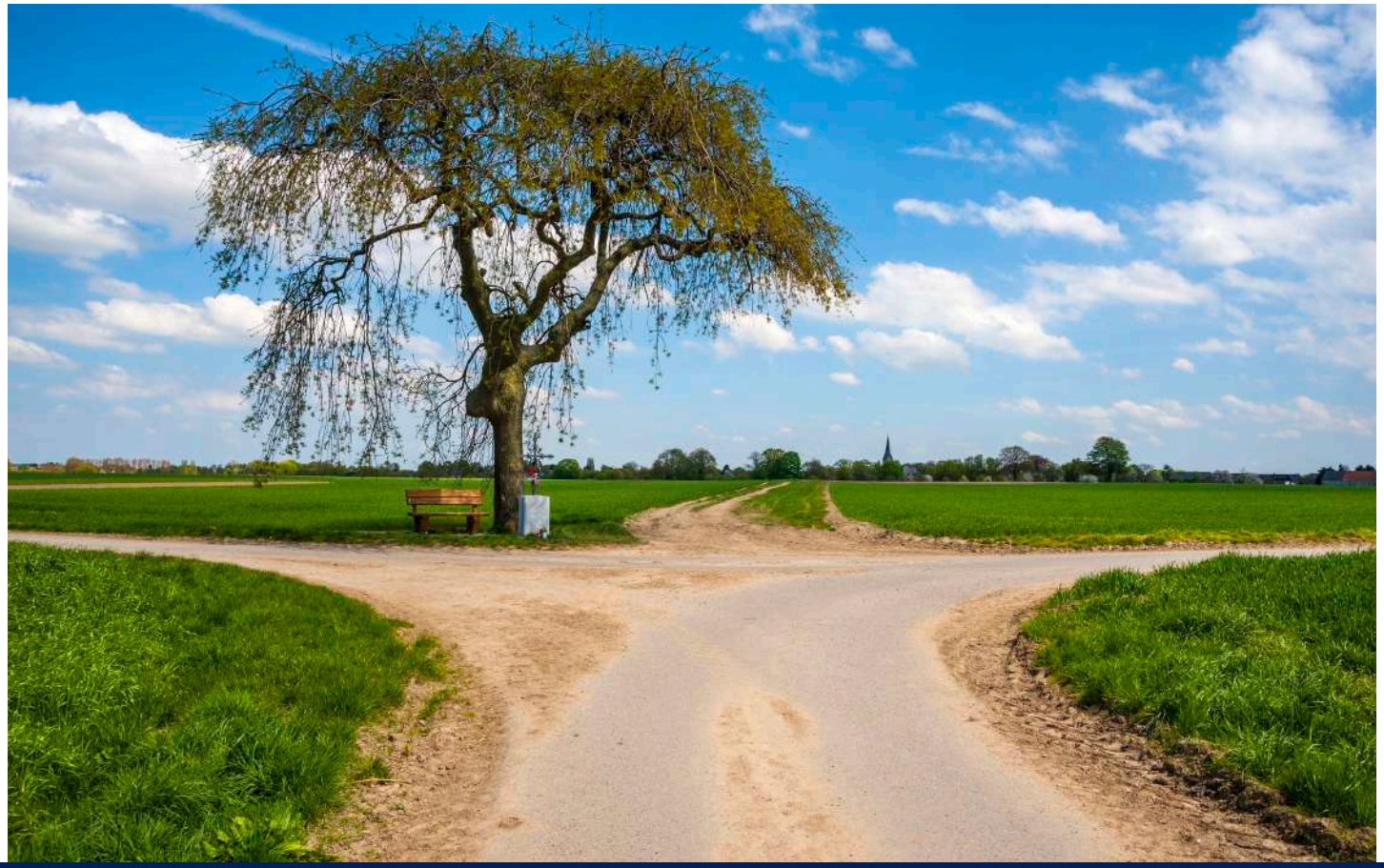


European Quantum Communication Infrastructure: deployment planned by 2030

Which future for (practical) Q Crypto ?

High TRL Q Tech => Real-World Industry ?





Thesis of this talk:

There is a **fork** that

Quantum Cryptography is **not** taking

(but should)

The Black Paper prophecy (Scarani, Kurtsiefer, 2009)

arXiv.org > quant-ph > arXiv:0906.4547

Quantum Physics

[Submitted on 24 Jun 2009 (v1), last revised 20 Apr 2012 (this version, v2)]

The black paper of quantum cryptography: real implementation problems

Valerio Scarani, Christian Kurtsiefer

« This leads us to guess that **the field**, similar to non-quantum modern cryptography, **is going to split in two directions:**

those who pursue practical devices may have to moderate their security claims

Practical QC

those who pursue ultimate security may have to suspend their claims of usefulness. »

Abstract QC

Why not take the fork i.e.
Acknowledge that Abstract QC ≠ Practical QC ?

ITS Security deeply Rooted in QCrypto Program:

"Conventional cryptosystems such as ENIGMA, DES, or even RSA, are based on a mixture of guess work and mathematics. Information theory shows that traditional secret-key cryptosystem cannot be totally secure unless the key, used once only, is at least as long as the cleartext. On the other hand, the theory of computational complexity is not yet well enough understood to prove the computational security of public- key cryptosystems. In this paper we use a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics. In conventional information theory and cryptography it is taken for granted that digital communications in principle can always be passively monitored or copied, even by someone ignorant of their meaning. "
Charles H. Bennett et Gilles Brassard (1984)

- **High symbolic Cost**: (for abstract QC)

Abstract Q Crypto may not directly apply to Real Systems.

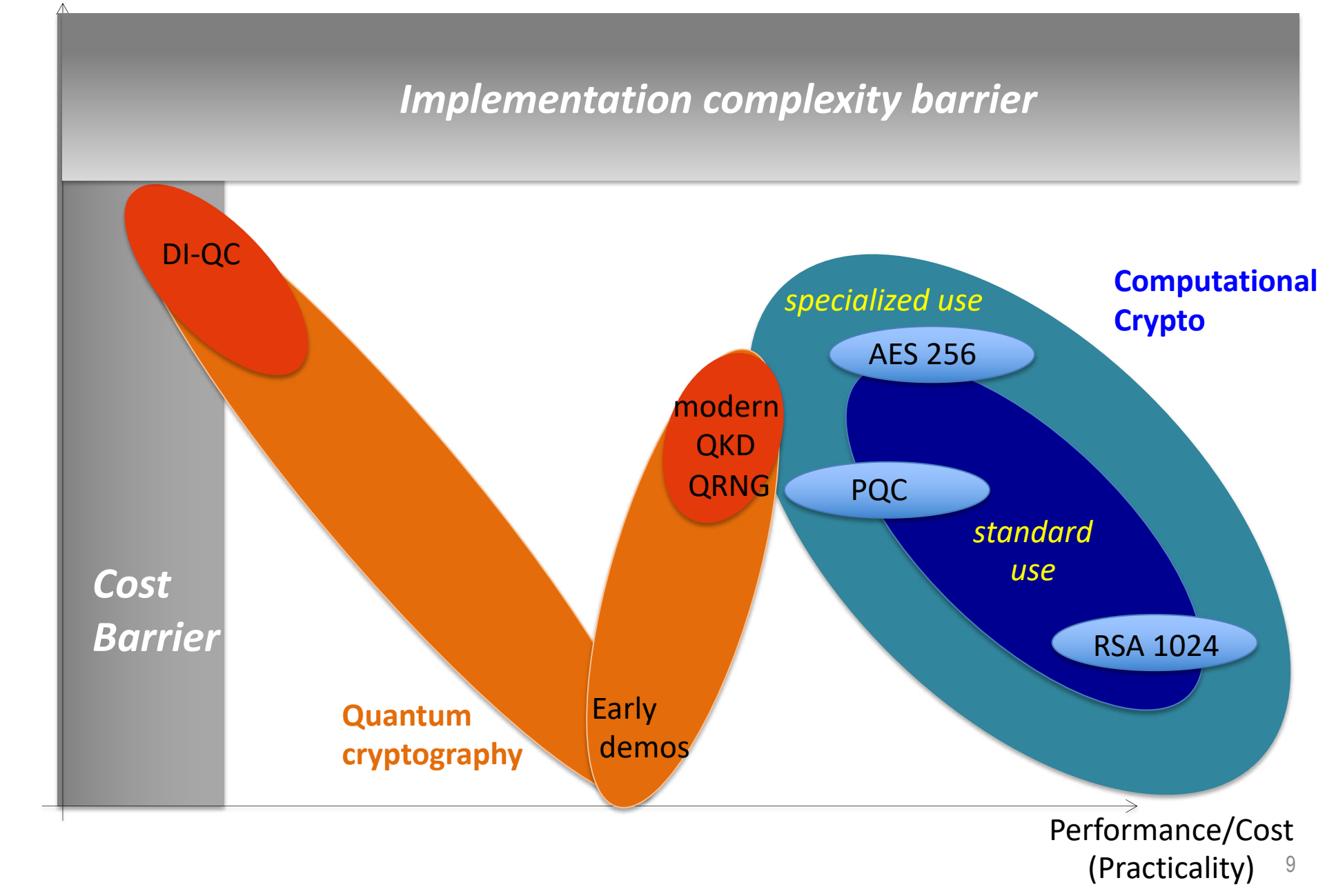
➔ ***Security Proofs cannot guarantee Absolute Security ?***

- **High Ontological Cost**: (for practical QC)

If practical Quantum Crypto cannot reach absolute security,

How is QC positioned in the cryptographic landscape?

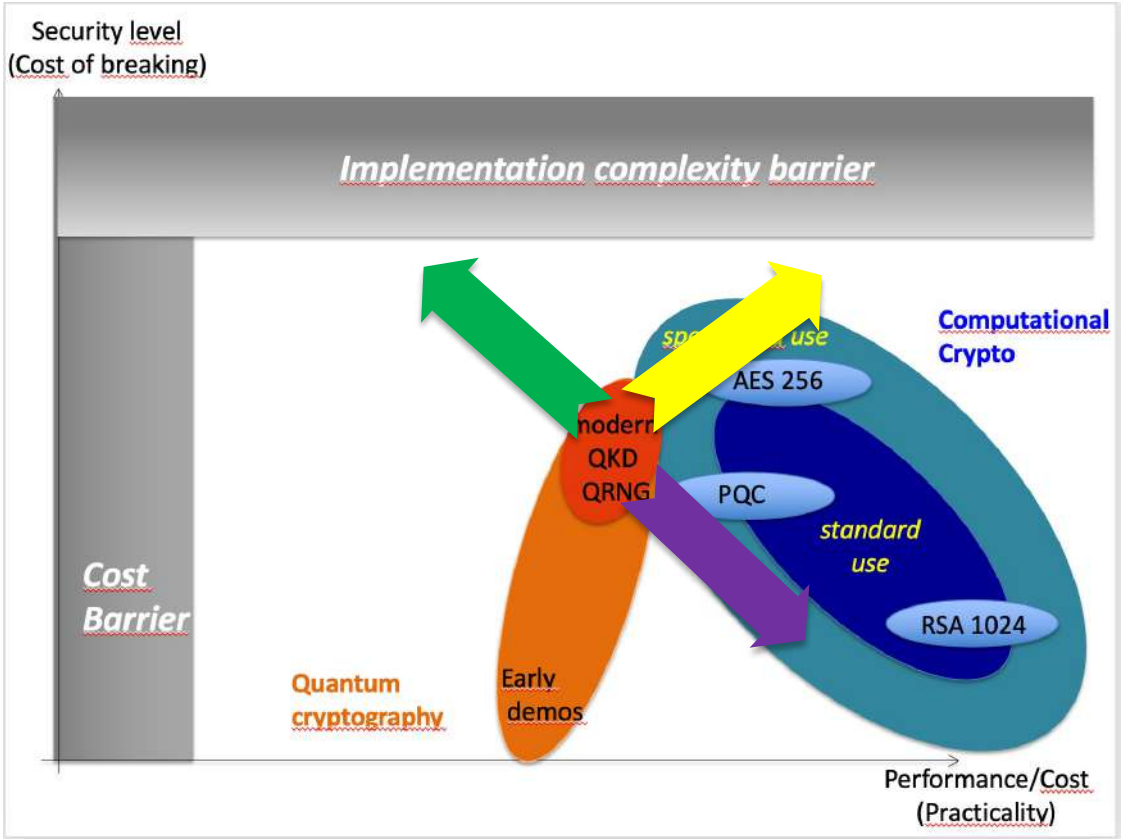
Quantum and Computational Crypto on a map



Practical Quantum Cryptography Dilemma:

Obvious next steps towards practicality have negative side-effects

- Improvements of performance / cost : **technology upgrade, simplification** generally decrease security (at least at short term)
- Increasing implementation security: **countermeasures, security certification** tend to increase cost and decrease performances



Way Forward:

Don't give up!

- ***Work Harder***
- ***Change Rules of the Game***

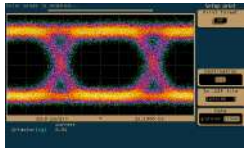
Work Harder: (Some) Quantum Crypto / Comms Research at TELECOM Paris

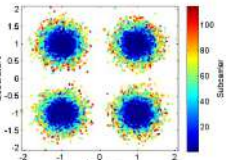
➢ Convergence between classical and quantum communications

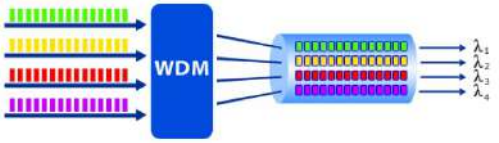
Classical and Quantum Communication with shared hardware

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

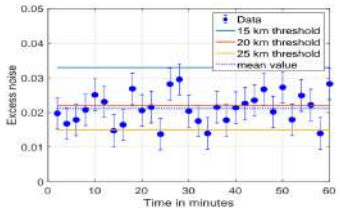
R. Aymeric, C.Ware, Y. Jaouën and RA, Symbiotic joint operation of quantum and classical coherent communications, OFC 2022

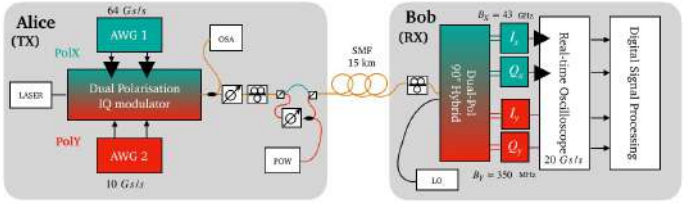




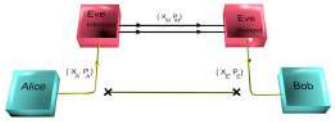


Collaboration with Y. Jaouen GTO group





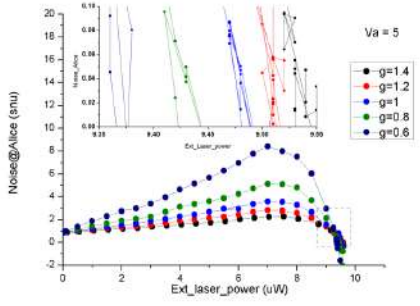
➢ From Q hacking to security certification of QKD implementations



Attacks and Countermeasures

*H. Qin, R. Kumar, and R. A. « Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution », Phys. Rev. A **94**, 012325. (2016)*

R. Kumar, F. Mazzoncini, H. Qin, R. Alléaume, Experimental vulnerability analysis of QKD based on attack ratings. Scientific reports, 11(1), 1-12 (2021).



Protection Profile for QKD

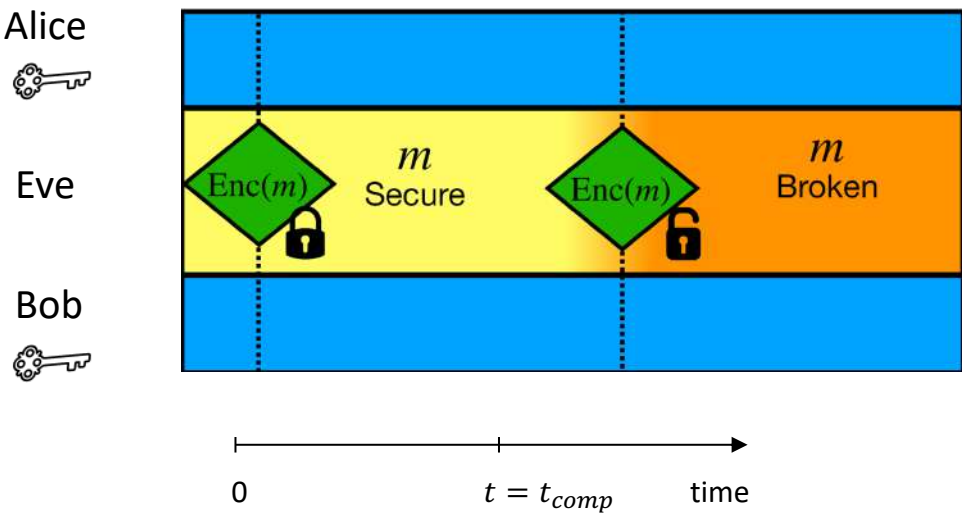
ETSI

OPEN QKD

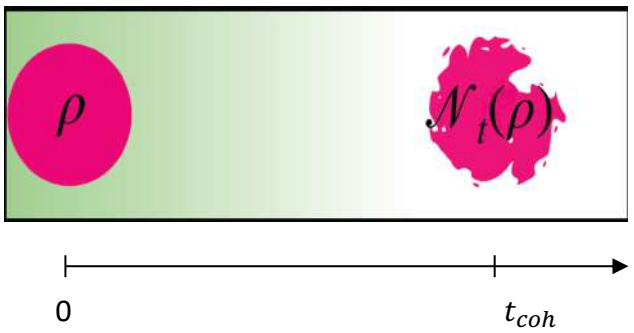
Change the Rules of the Game

QCT Security Model (quantum computational time-lock)

1) Short-term secure encryption



2) Time-limited quantum storage



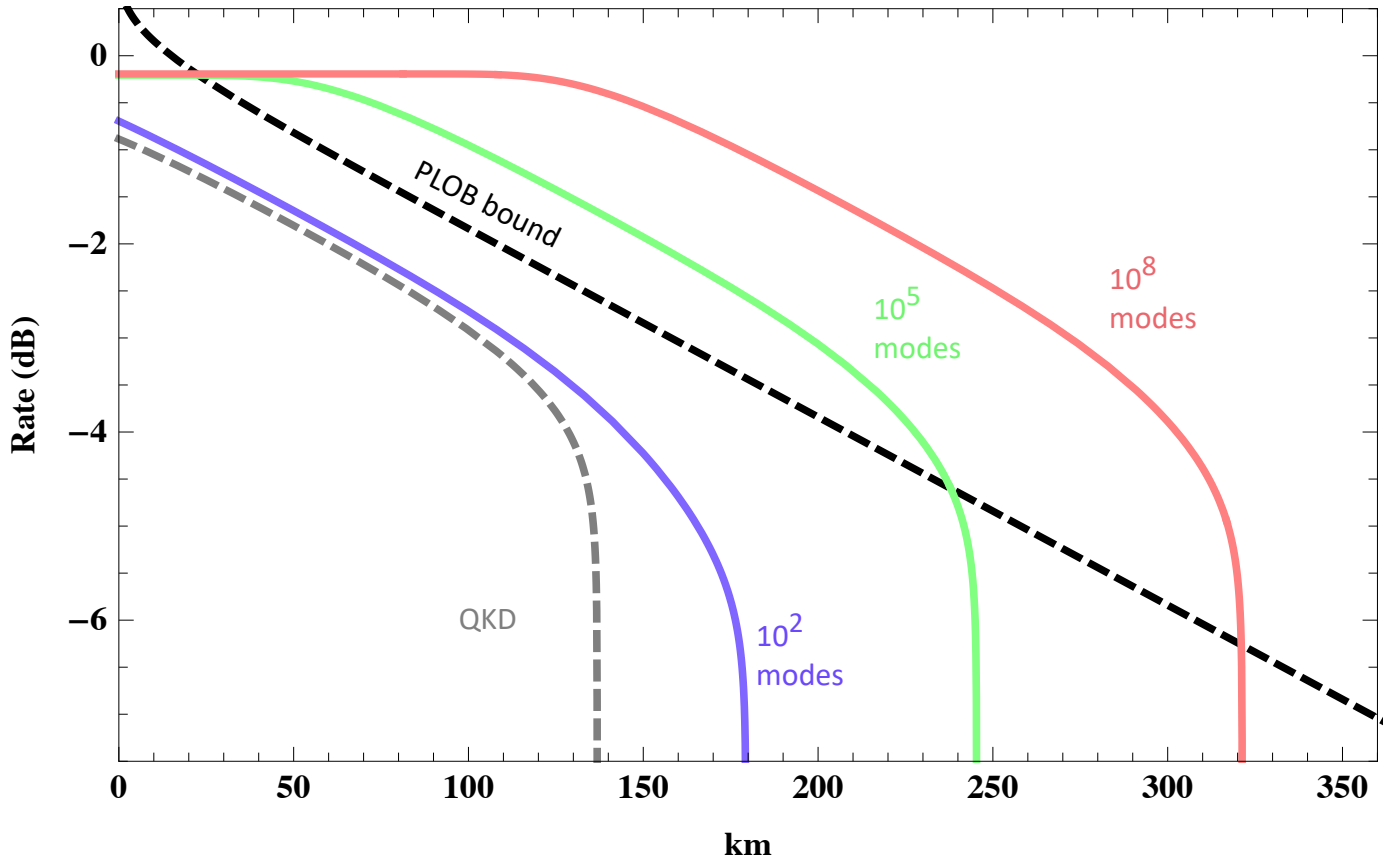
- Top secret (AES Encryption) $t \approx 10^8 sec$
- Coherence time $\approx O(1)\ sec$

$t_{coh} < \mathrm{t_{comp}}$

Very likely to hold (in the future too)

QCT offers Everlasting Security

QCT enables Quantum Cryptography « beyond no-cloning »



arXiv:2004.10173

Nilesh Vyas, RA, *Everlasting secure key agreement from the quantum computational timelock*,

Secure KD with >> 1 photons / ch use

➔ Longer reach & Higher rates than QKD

Contributed Talk at ICQOM 2021

2 Granted Patents **EP**15305017.4 **WO**2016110582

Conclusion - Perspectives

Abstract ≠ Practical Q Crypto

Il faut prendre l'embranchement !

- Continuer à explorer les 2 voies
- Considérer leurs combinaisons

1) Combine Q Crypto and PQC, ***aiming at PQC+QC > PQC***

2) Hybridize Q crypto with computional assumptions
QCT, but also DI-QC with computational assumptions (ArXiv:2204.11353)

3) Quantum-enhanced hardware security
Use ***q crypto protocols*** *to* ***strengthen physical layer security*** *in* ***a provable way***

QSN PARTNERSHIP

Quantum Secure Network Partnership
QT Flagship FPA in Q Communications
2023-2026 (40 partners)

QUANTUM FLAGSHIP