Quantum-Computational Hybrid Cryptography based on the Boolean Hidden Matching Problem

Workshop Boolean Functions and Applications
June 21, 2019

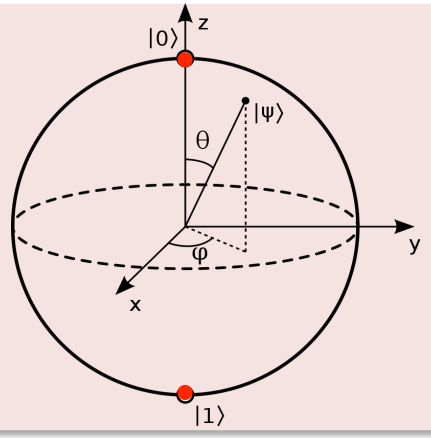
Romain Alléaume

Relation btw **quantum cryptography** and boolean functions ?

Quantum bit (Qbit) ⇔ SU(2) ⇔ Point on the Block Sphere

|0>, |1> : orthogonal vectors of SU(2)

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi}\,sin(\theta/2)|1\rangle$$

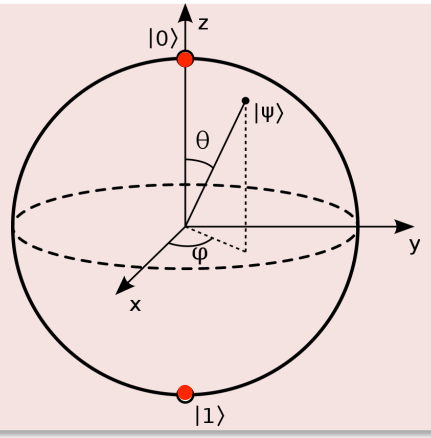


Relation btw **quantum cryptography** and boolean functions ?

Quantum bit (Qbit) ⇔ SU(2) ⇔ Point on the Block Sphere

|0>, |1> : orthogonal vectors of SU(2)

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi}\,sin(\theta/2)|1\rangle$$



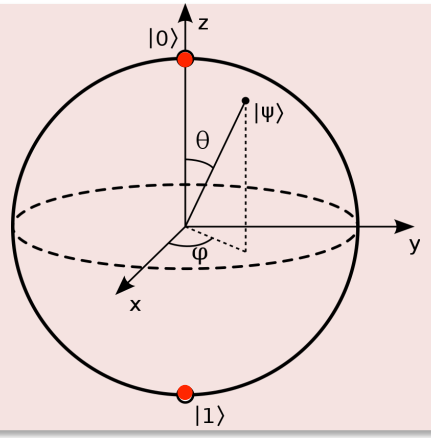
Holevo Theorem (73): the classical capacity of n qubits is at most n bits

Relation btw **quantum cryptography** and boolean functions ?

Quantum bit (Qbit) ⇔ SU(2) ⇔ Point on the Block Sphere

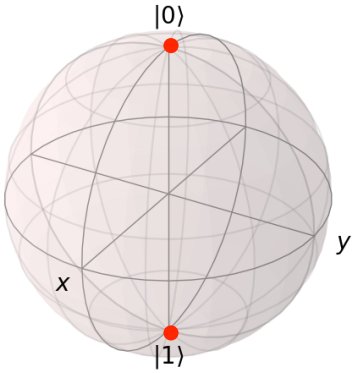
|0>, |1> : orthogonal vectors of SU(2)

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi}\,sin(\theta/2)|1\rangle$$

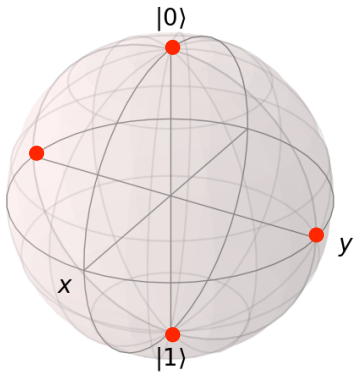


Holevo Theorem (73): the classical capacity of n qubits is at most n bits

{|0>, |1> } ⇔ F_2 ⇔ 1 classical bit



BB84 QKD encoding: {|0>, |1>, |+>, |-> }



1 bit max capacity

Zero-error eavesdropping Impossible

=>(…) Security

“Quantum” is a frontier for computational cryptography

“When elementary quantum systems … are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media.”

Charles H. Bennett et Gilles Brassard (1984)

“Quantum” is a frontier for computational cryptography

“When elementary quantum systems … are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media.”

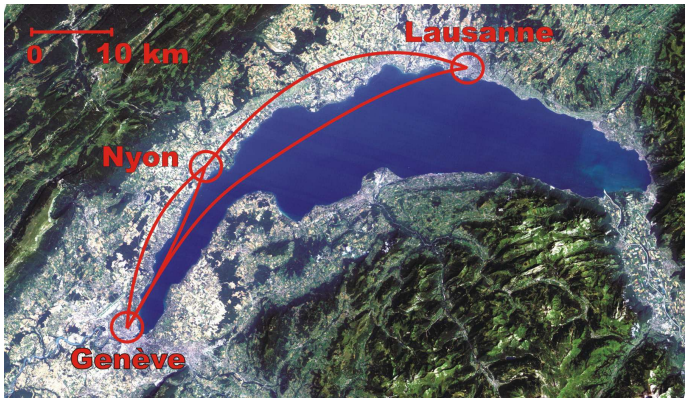
Charles H. Bennett et Gilles Brassard (1984)

- Key Distribution: QKD (BB94, E91, GG02, DI-QKD, MDI-QKD, etc..)
- Randomness Generation: QRNG, DI-QRNG
- Secure multi-party computation: Bit commitment, OT, Blind QC

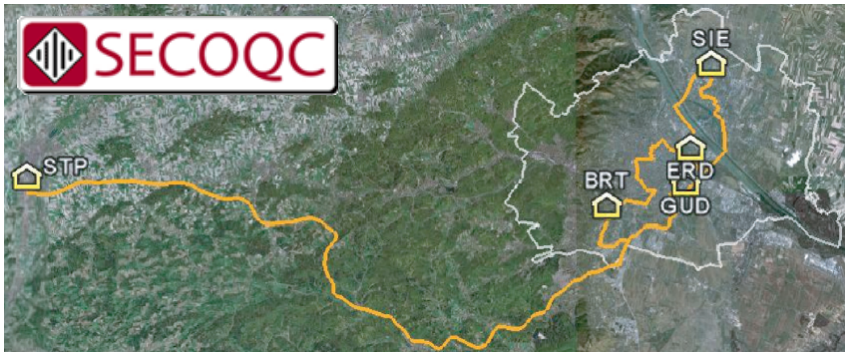
Common point: realize some existing cryptographic functionalities <u>without</u> computational assumption:

ITS security = Unconditional Security

Quantum Key Distribution: large-scale deployment in view

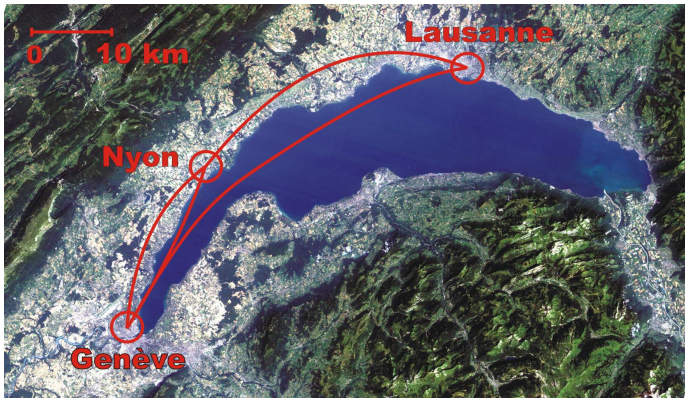


Geneva-Lausanne QKD link (1998)

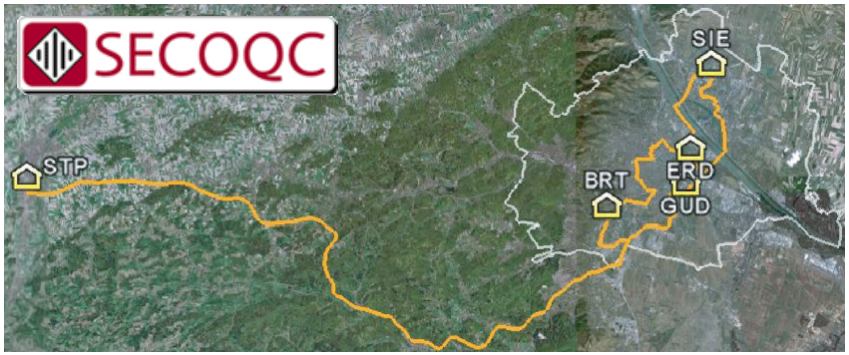


First European QKD Network, Vienna (2008)

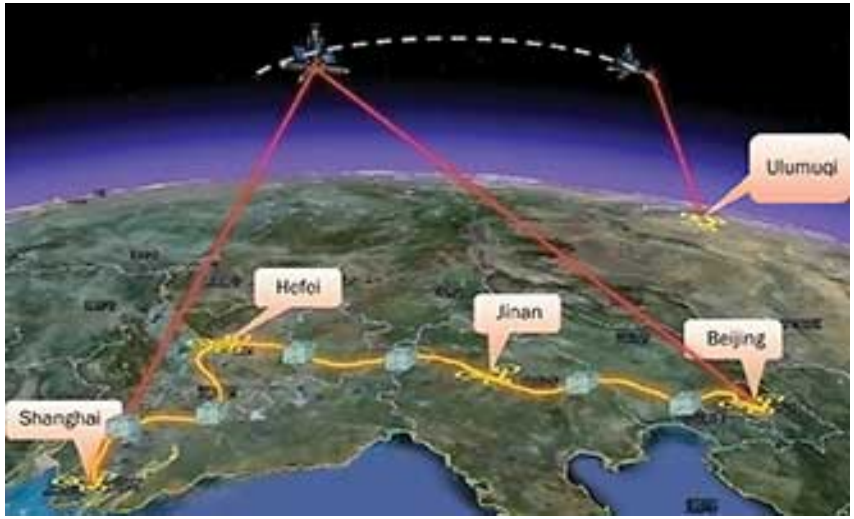
Quantum Key Distribution: large-scale deployment in view



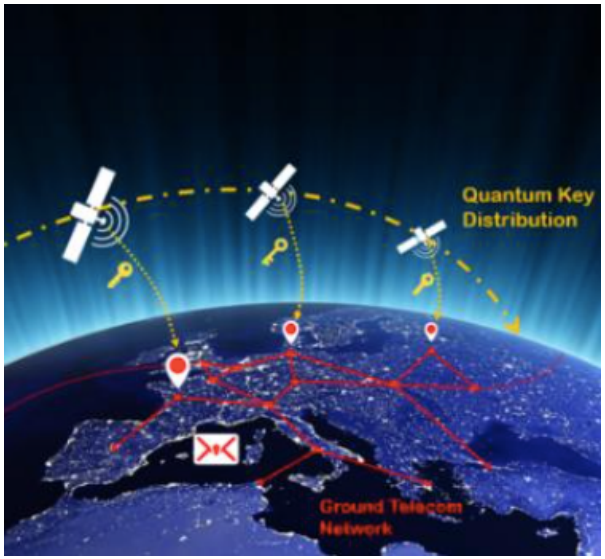
Geneva-Lausanne QKD link (1998)



First European QKD Network, Vienna (2008)



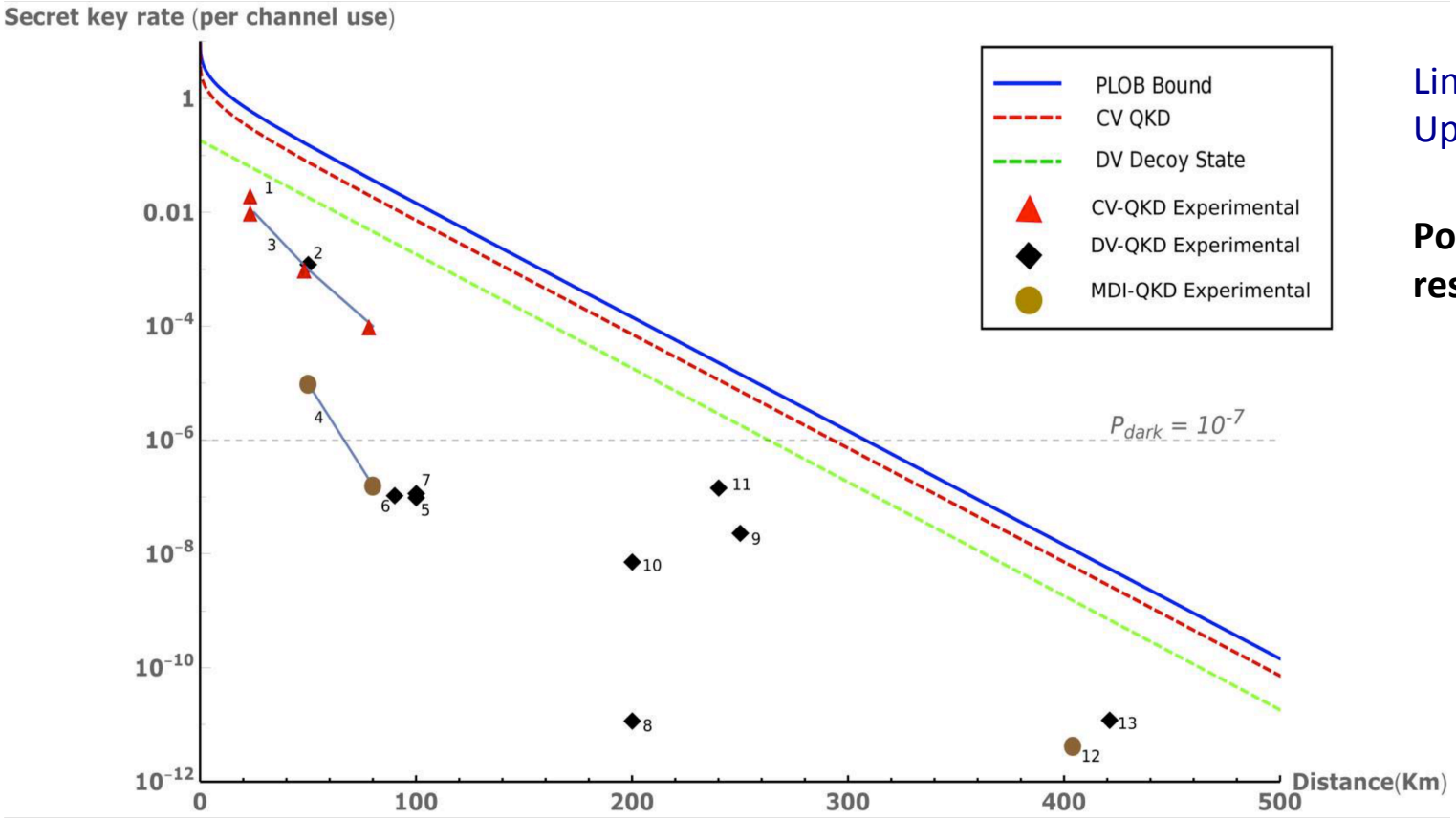
Q Satellite Micius (2016)
2000 km Ground QKD Network (2018)



QUANTUM FLAGSHIP

European Quantum Communication Infrastructure: deployment planned by 2030

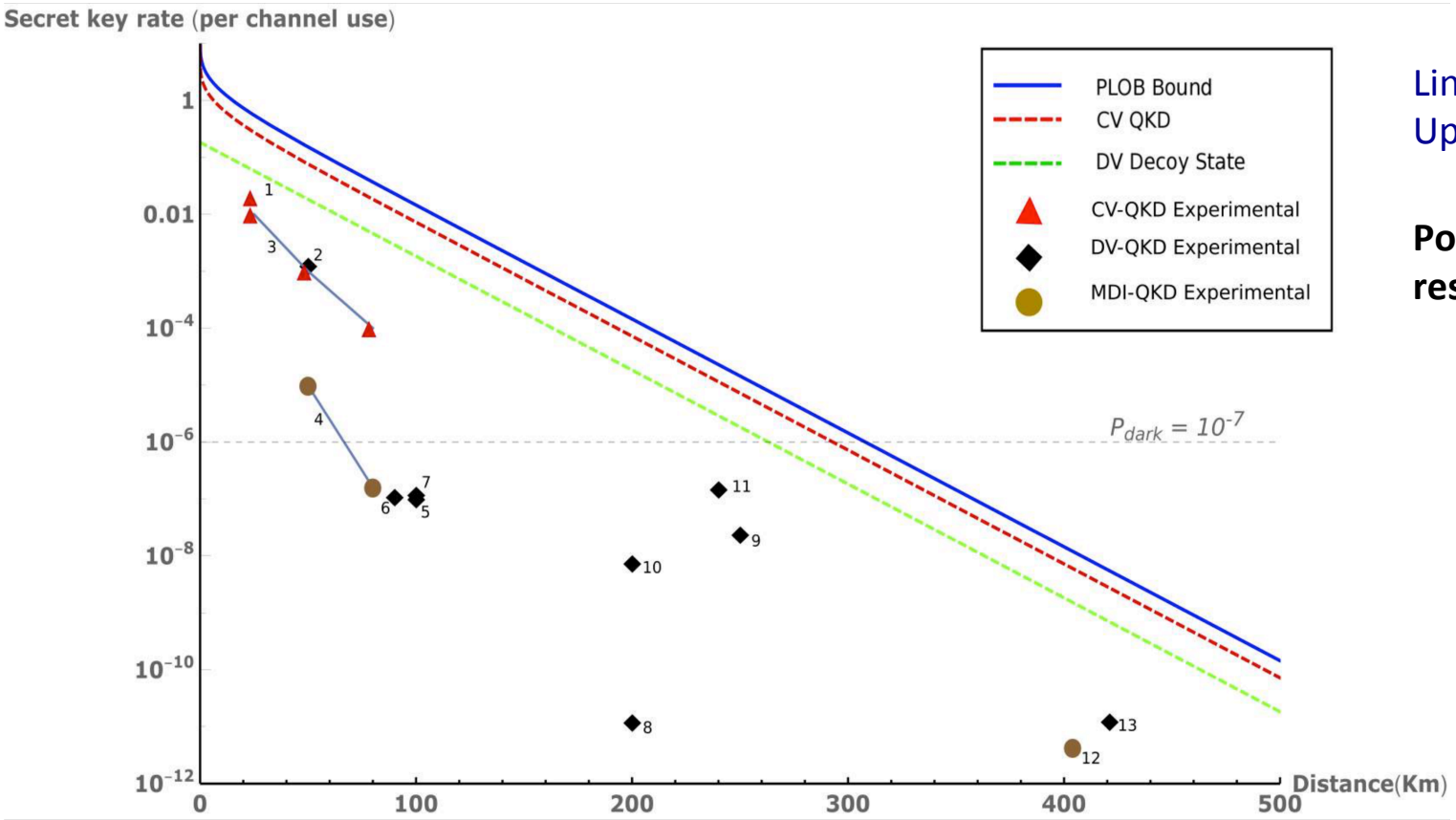
Challenge: fundamental rate-loss trade-off (PLOB bound)



Lines =
Upper bounds

Points = Experimental results

Challenge: fundamental rate-loss trade-off (PLOB bound)



Lines =
Upper bounds

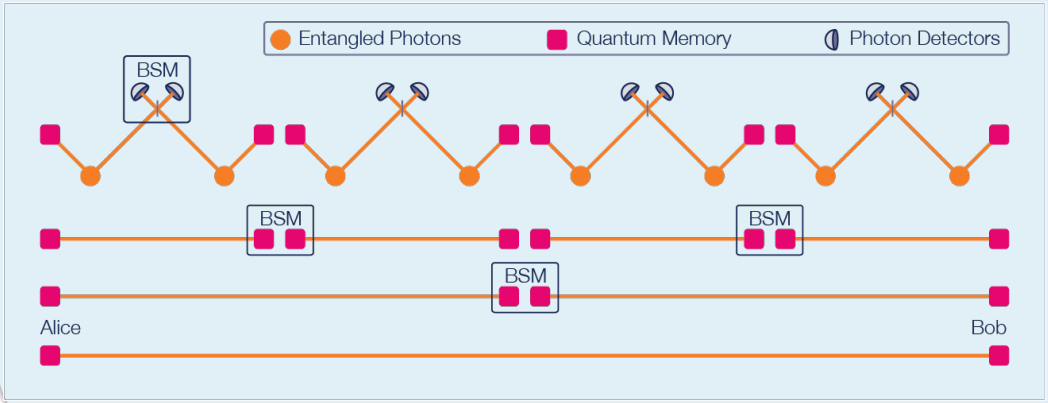
Points = Experimental results

Maximum Distance depends on conditions *(i.e Dmax such that R(Dmax) ~1 bit/s)*

400 km	lab environment	low-loss fiber	supra-conducting detector
240 km	lab environment	dark fiber	avalanche photodiode
150 km	**field deployment**	**dark fiber**	**avalanche photodiode**
<100 km	field deployment	WDM	avalanche photodiode

Breaking the rate-loss fundamental barrier

Quantum Repeaters



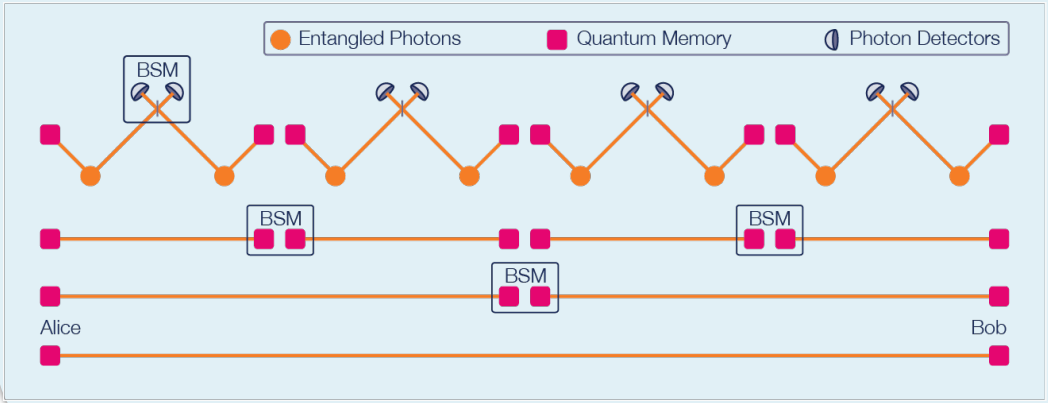
QUANTUM FLAGSHIP

QIA

Quantum Internet Alliance project

Breaking the rate-loss fundamental barrier

Quantum Repeaters



QUANTUM FLAGSHIP

QIA

Quantum Internet Alliance project

This work: Quantum-Computational Hybrid Cryptography

Use computational assumptions to boost quantum cryptography

- Implementable with current technology *(no quantum memory, no repeaters)*
- Change of security model
  - Relax unconditional security requirement
  - Keep core cryptographic advantage: everlasting security

Quantum Computational Hybrid (QCH) Security Model

Assumption 1 : **Short-term-secure encryption exists**

Legitimate users can use a (computationally-secure) symmetric encryption scheme indisguishable from a random function during a time at least τ_{enc}

Assumption 2 : **Noisy Quantum Storage**

Quantum memory decoheres within a time $\tau_{coh} << \tau_{enc}$

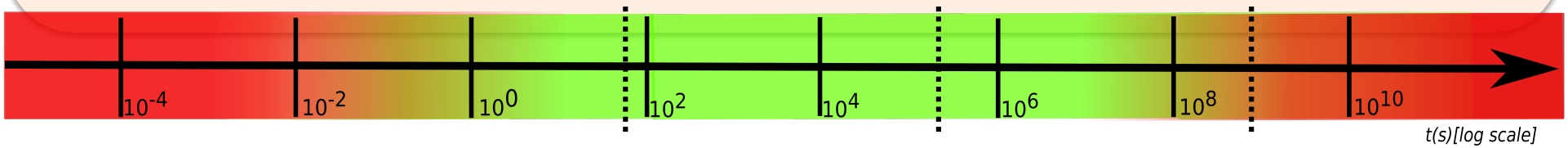
Quantum Computational Hybrid (QCH) Security Model

Assumption 1 : **Short-term-secure encryption exists**

Legitimate users can use a (computationally-secure) symmetric encryption scheme indisguishable from a random function during a time at least τ_{enc}

Assumption 2 : **Noisy Quantum Storage**

Quantum memory decoheres within a time $\tau_{coh} << \tau_{enc}$



~min

1 Day

25 years

Quantum memory requirements:

- Quantum regime
- High Capacity:
- efficiency
- dimensionality
- fidelity

$\Rightarrow t_{coh} < 10^{-2}$ s

Record T1 time for light storage

Heinze et.al., PRL 111, 033601 (2013)

Top Secret
AES-256 Encryption

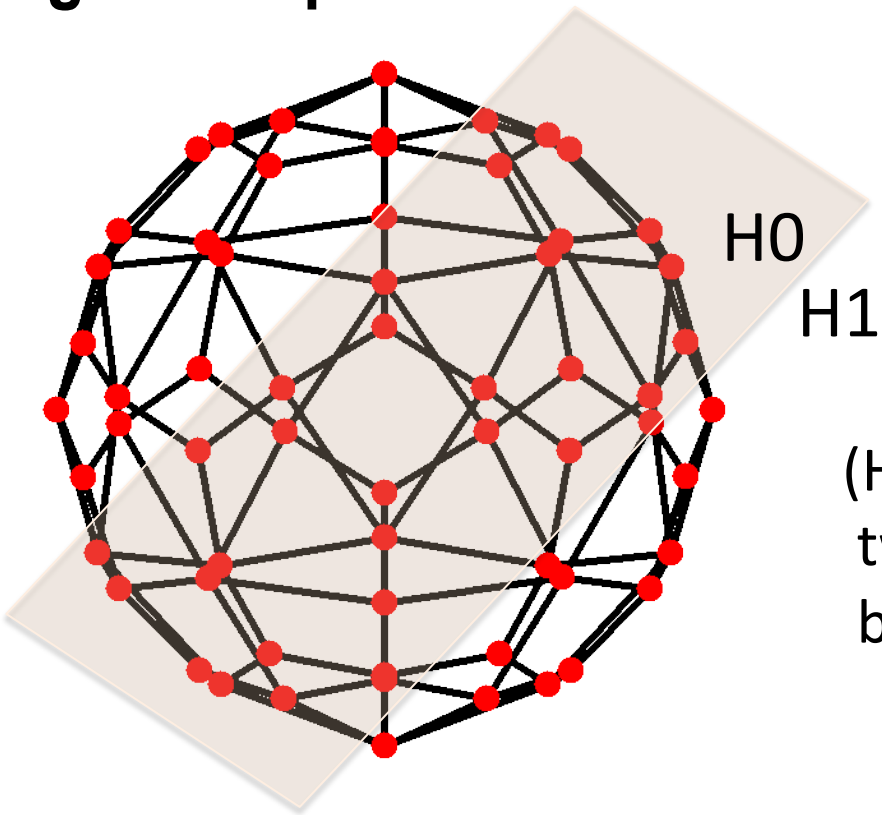
Barker, NIST SP 800-57 Pt. 1 Rev. 4 (2016)

How to design a KD protocol in the QCH model ?

High dimensional (d>>1) quantum encoding

e.g d=64

(artistic view)



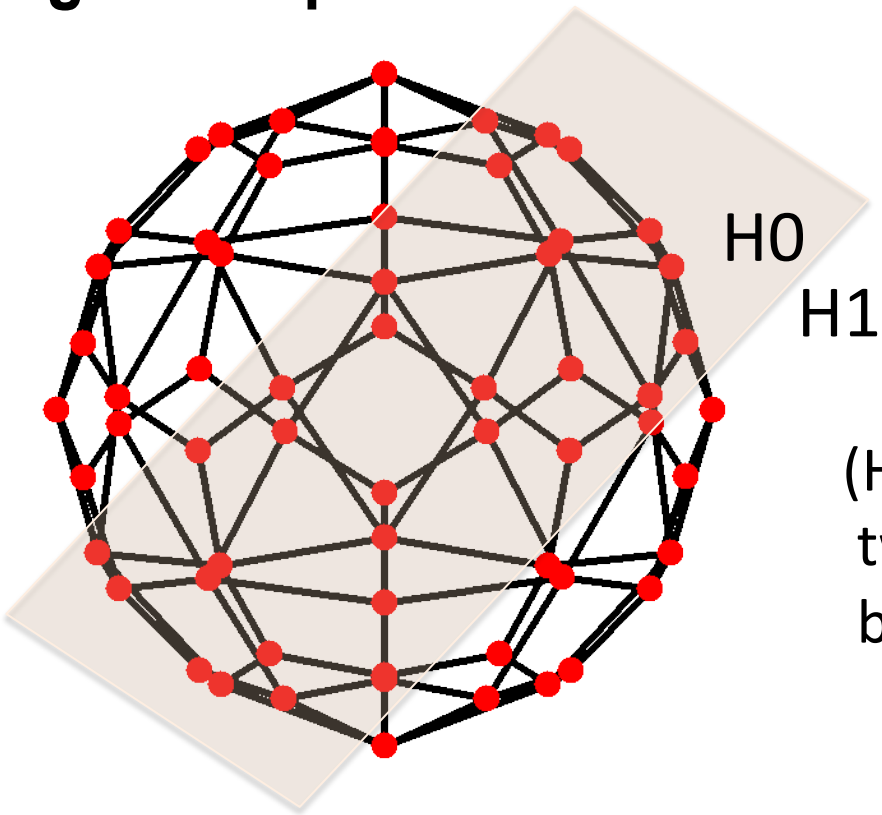
(H0,H1): partition in two d/2-dimensional boolean subspaces

How to design a KD protocol in the QCH model ?

High dimensional (d>>1) quantum encoding

e.g d=64

(artistic view)



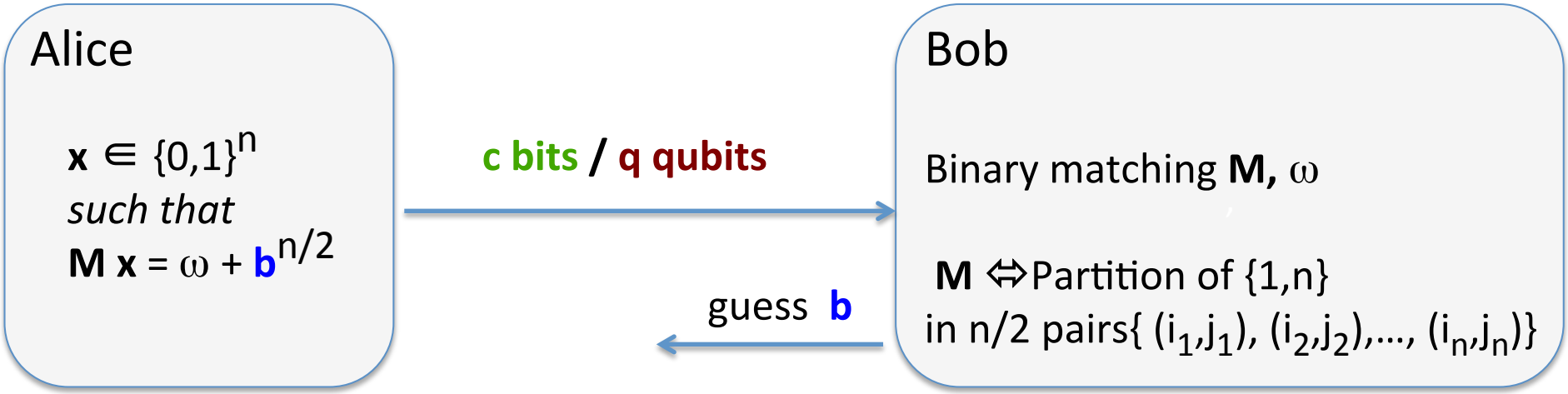
(H0,H1): partition in two d/2-dimensional boolean subspaces

High-level idea for q cryptographic protocol:

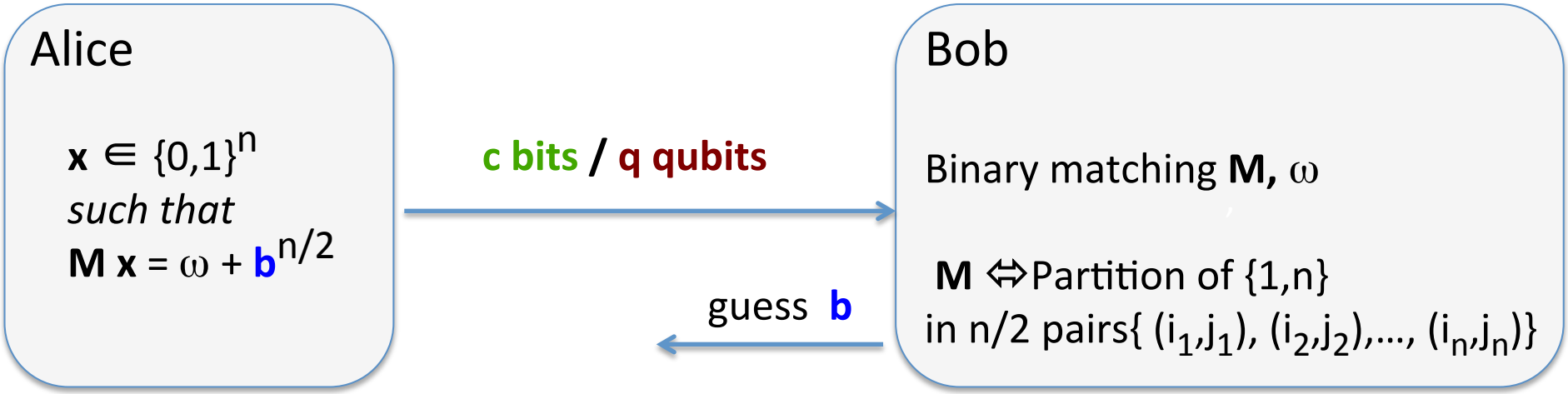
- **Encrypt and send (H0,H1)**
- **Encode 1 bit b** as a q state $|\phi_x\rangle$ that belongs to H0 or H1

If one knows (H0,H1) ➔ can decode b *(measurement (H0,H1))*
If does not know (H0,H1) ➔ cannot guess b (what measurement ?)

Boolean Hidden Matching (BHM)



Boolean Hidden Matching (BHM)



Reference

Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald De Wolf.
Exponential separations for one-way quantum commun complexity, with appl. to cryptography.
ACM Symposium on Theory of Computing 2007.

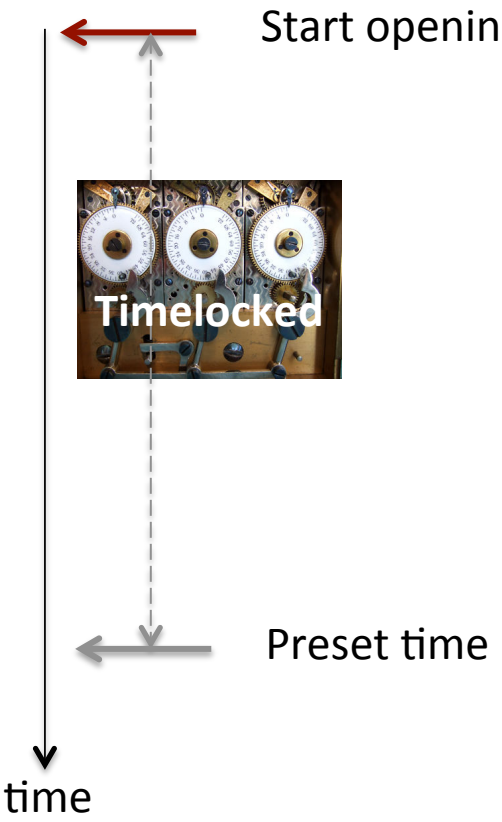
Classical One-way computational complexity of BHM **$O(\sqrt{n})$ bits**

Quantum One-way computational complexity of BHM **log(n) qubits**

- Alice sends $|\psi_x\rangle = \Sigma_{i=1..n} (-1)^{xi} |i\rangle$
- Bob measures according to matching M : projections $P_k^{(\pm)}$ on $|i_k\rangle \pm |j_1\rangle$

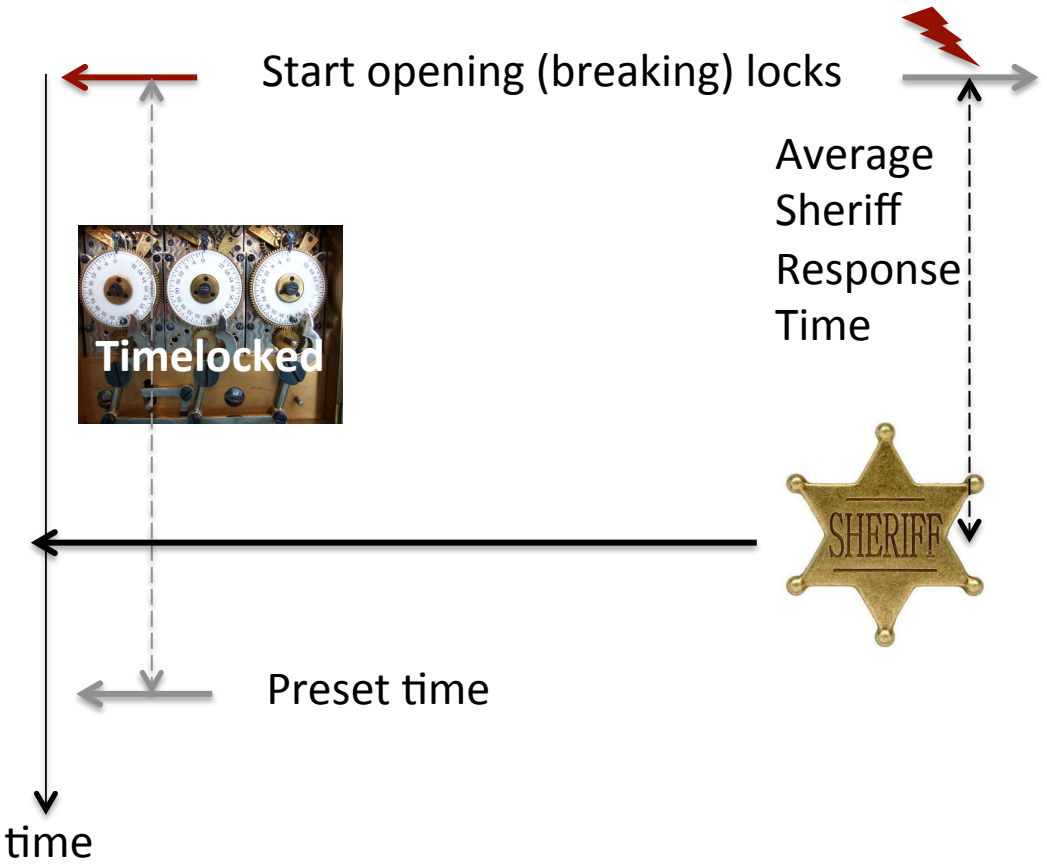
New Q Crypto framework : Quantum Computational Timelock (QCT)

The **timelock** is a timer designed to prevent the opening of a vault until it reaches a preset time.
Very strong security when combined with external security mechanism (e.g. Sheriff)



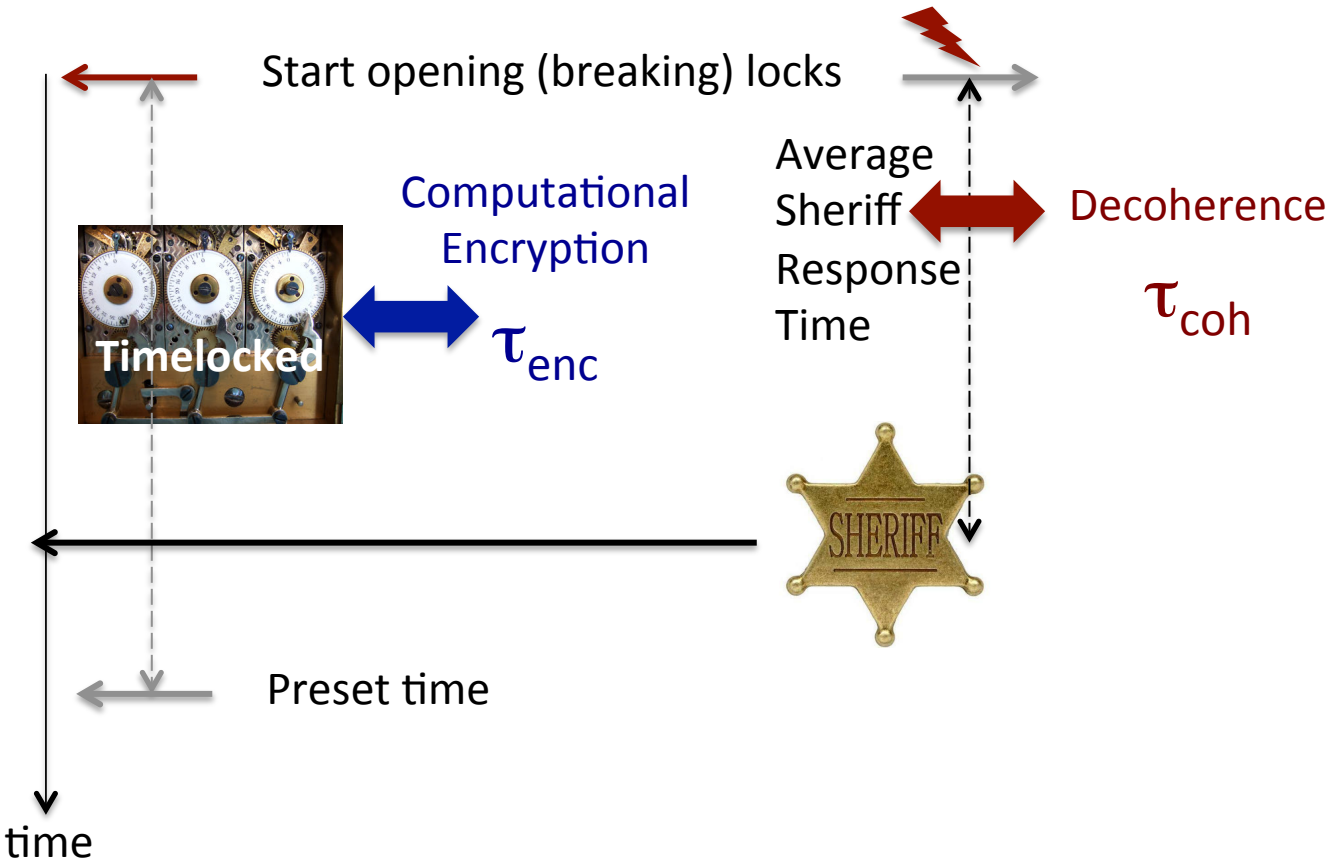
New Q Crypto framework : Quantum Computational Timelock (QCT)

The **timelock** is a timer designed to prevent the opening of a vault until it reaches a preset time.
Very strong security when combined with external security mechanism (e.g. Sheriff)



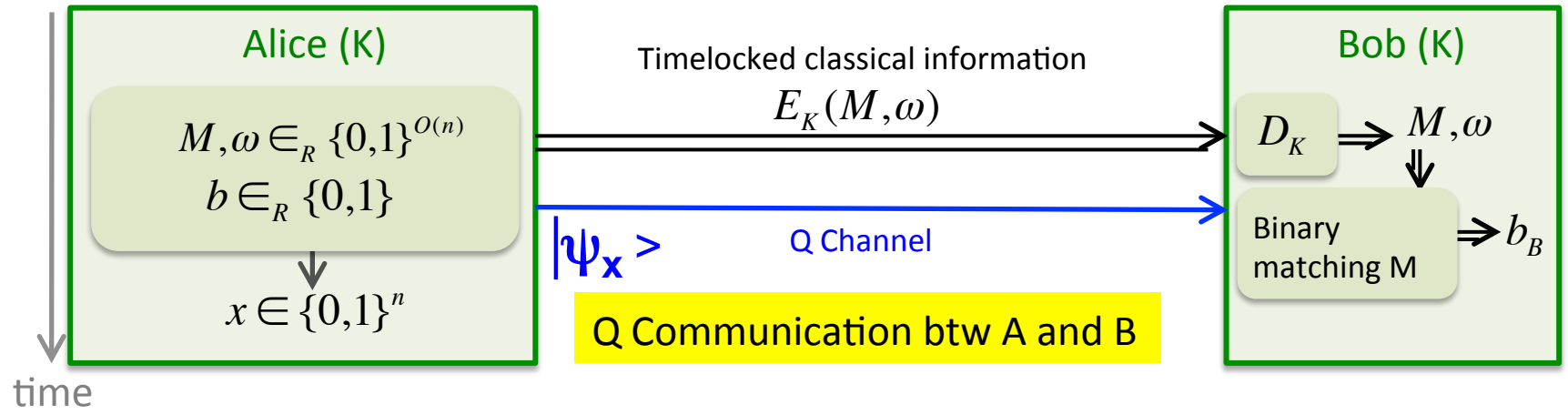
New Q Crypto framework : Quantum Computational Timelock (QCT)

The **timelock** is a timer designed to prevent the opening of a vault until it reaches a preset time.
Very strong security when combined with external security mechanism (e.g. Sheriff)

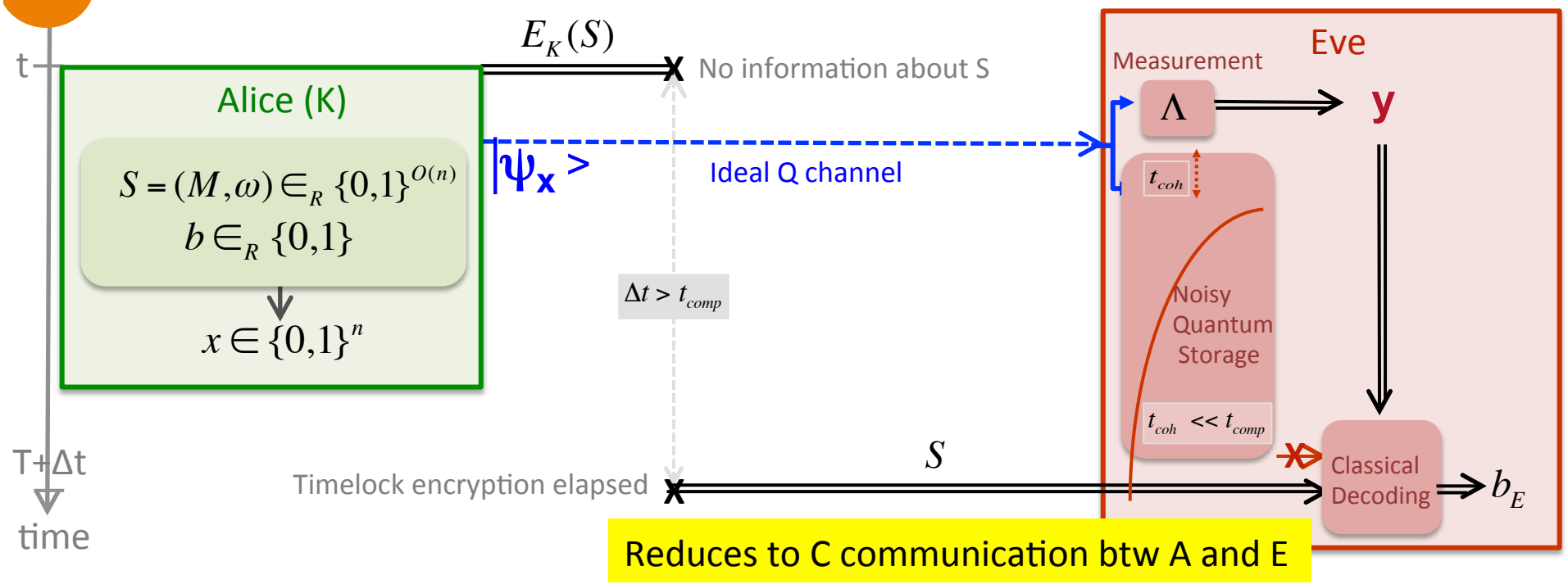


A-B

QCT leads to reduction (C/Q separation) to Hidden Matching

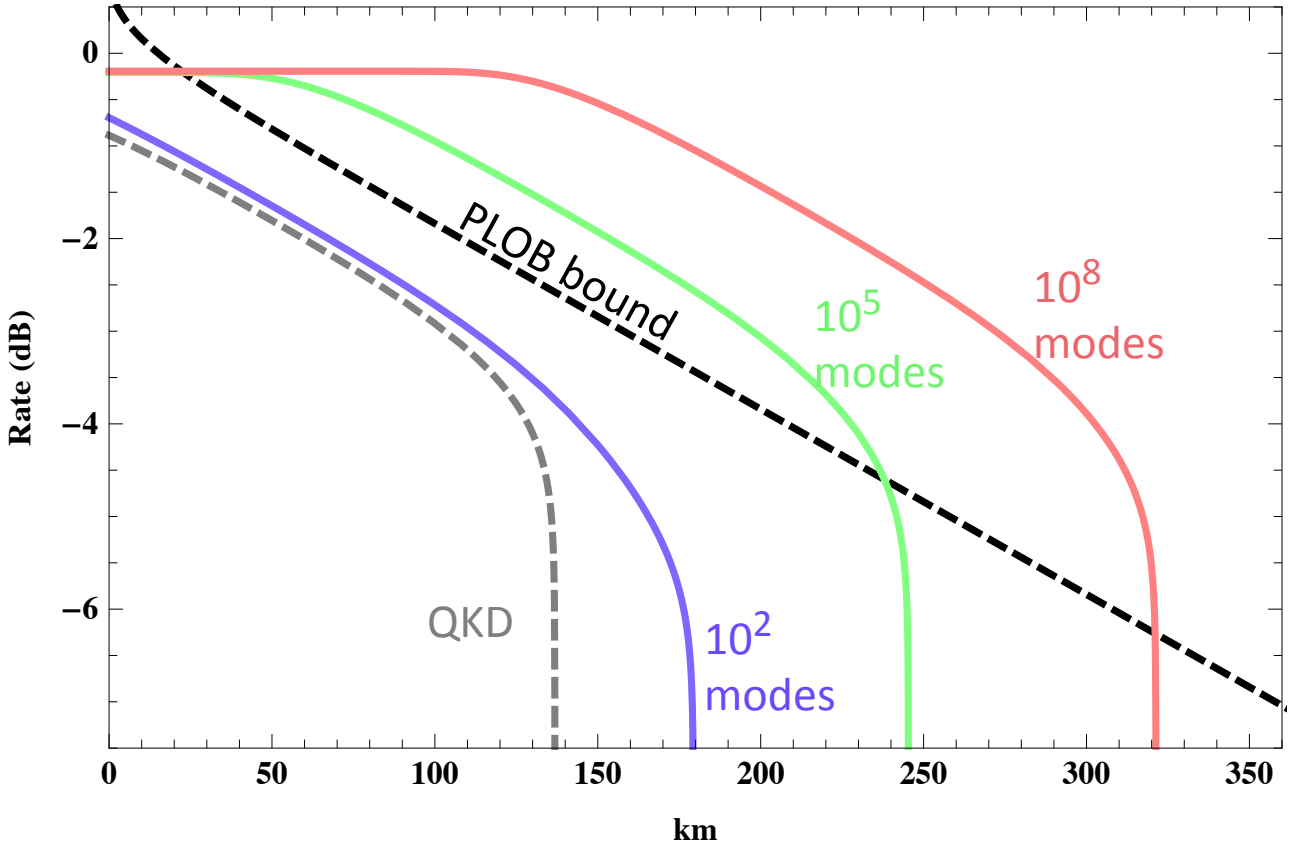


A-E



Performance of Hidden Matching - QCT protocol

Implementable with coherent states, with high dimensional (n modes) encoding



Reduction to BHM:

Secure KD with O(√n) photons / ch use

➔ Longer reach

➔ Higher rates than QKD

Granted Patent **EP**15305017.4 **WO**2016110582

ROMAIN ALLÉAUME, COMMUNICATIONS WITH EVERLASTING SECURITY FROM SHORT-TERM-SECURE ENCRYPTED COMMUNICATION

Conclusion and perspectives

Q Crypto can be boosted by ephemeral computational assumptions

- ***Everlasting security in noisy storage model***
- Improved performances
- Improved functionalities: 1 to N KD ; no need to trust Bob

Future work and Open questions

Experimental Implementation (*ongoing work, frequency encoding*)

Is a better scaling achievable ? *(e.g, rate scales like 0(n))*

➔ Explore alternative constructions and connections with:

- Communication complexity
- Locally decodable codes
- Randomness extractors
- *Other techniques from cryptography and coding ?*