Everlasting Secure Key Agreement with performance beyond QKD in a Quantum Computational Hybrid security model

Nilesh Vyas, Ramain Alléaume

Telecom Paris, LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

arXiv:2004.10173

Quantum Computational Hybrid Security Model

Comprise of two realistic assumptions:

1. ***Short term secure encryption:*** assumes that there exists an encryption scheme E_k, such that, any adversary running an efficient algorithm in polynomial time can not break it before a computational time t_{comp}.
2. ***Time-limited quantum storage:*** which assumes that any quantum memory decoheres within time $t_{coh} < t_{comp}$.

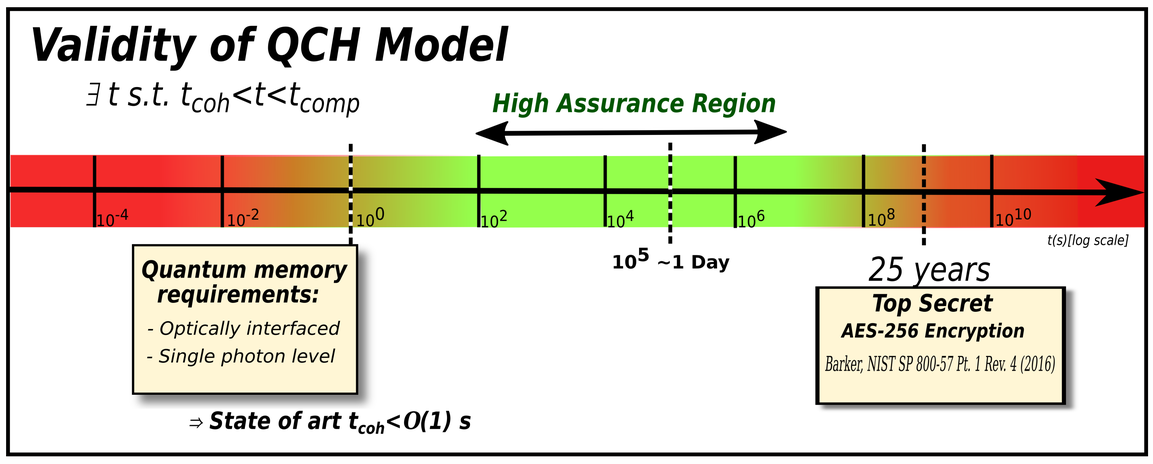


Fig. 1.Validity of QCH security model

Objective

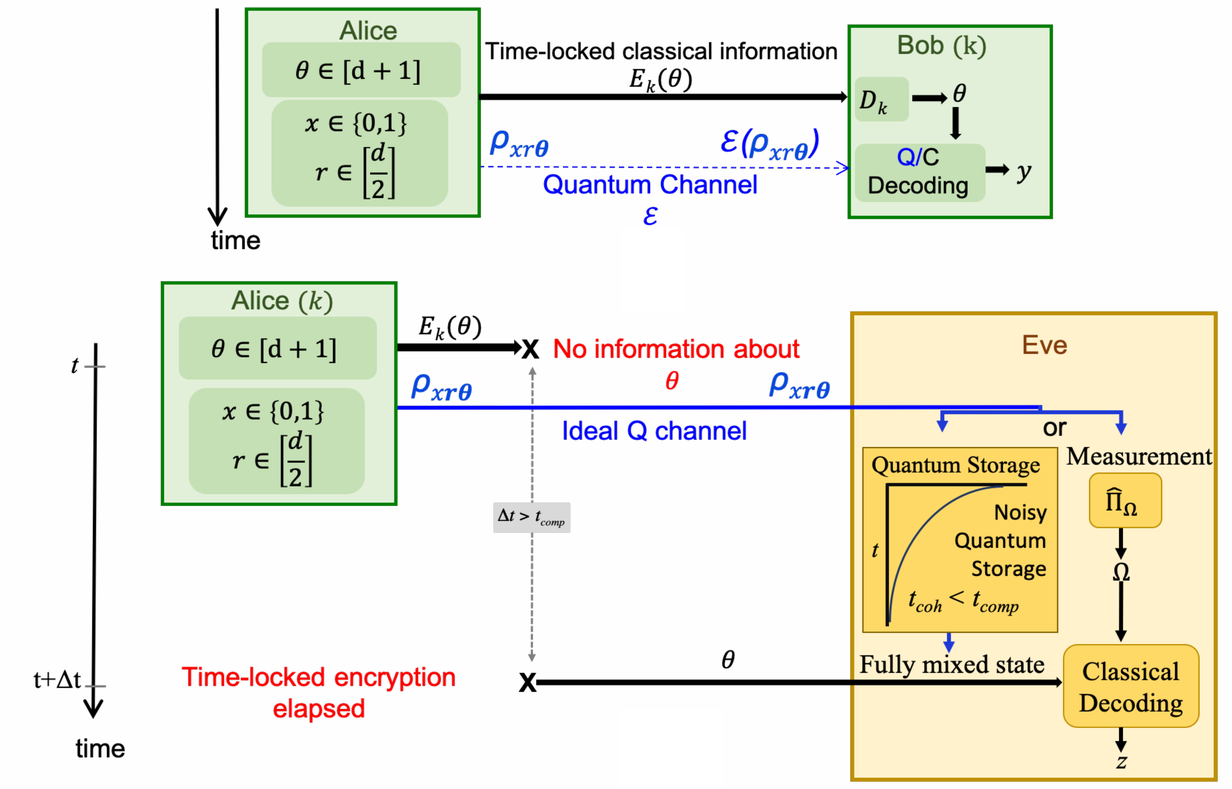
In this work we consider a security model weaker than unconditional security and characterise the gain for quantum cryptography in practicality (i.e. performance and functionality, over cost).

MUB-QCT Key Distribution Protocol

Encoding a bit in a subspace: $(d/2,d/2)$ **random partition of MUB basis vectors in dimension** d

Parameters:

n: channel use, ***k:*** short key shared between Alice and Bob, ***m:*** number of copies sent per channel use.



Best strategy for Eve : **Immediate measurement followed by state discrimination using post-measurement information**

(S.Wehner et.al., Phys. Rev. A 82, 022326)

Results and Analysis

◆ Upper bounding Eve's guessing probability:

Calculating P_{guess} for state discrimination with post-measurement information

❖ **Sending single copy of quantum state per channel use**

$$\Rightarrow \left| P_{guess} - \frac{1}{2} \right| < \frac{1}{\sqrt{d}}$$

❖ **Sending multiple copy of quantum state per channel use (Individual attacks)**

$$\Rightarrow \left| P_{guess}(m) - \frac{1}{2} \right| < \frac{m}{\sqrt{d}} + o\left(\frac{1}{\sqrt{d}}\right)$$

◆ Secret key rate per channel use

$$K \geq I(X;Y) - I(X;Z) \geq H_{\min}(X|Z) - H(X|Y)$$

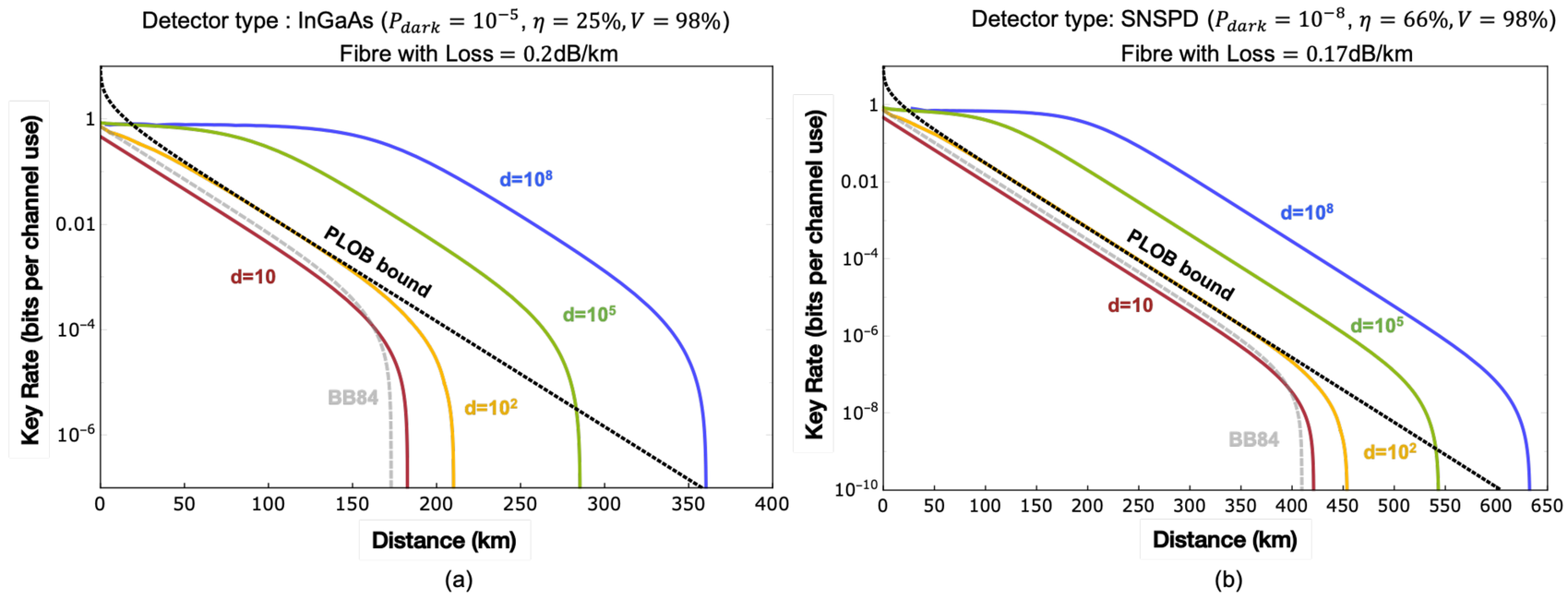


Fig. 3. Key rate per channel use as a function of distance for, (a) Typical QKD Field Deployment (standard fiber, InGaAs single-photon detectors) (b) Experiment in the Lab (low-loss fiber, SNSPDs).

◆ Performance Analysis

☑ **More efficient than QKD**

- ❖ Significant performance boost of $\mathcal{O}(\sqrt{d})$ with fixed hardware.
- ❖ Relaxes the requirement for a very good single-photon detector.
- ❖ High tolerance to channel noise and losses.

☑ **More functionality and practicality**

- ❖ Multi-party key distribution.
- ❖ No need to monitor the disturbances and error rate.
- ❖ MDI-type security guarantee: Security is independent of any trust assumption on the measurement device, provided some additional restrictions.

☑ Ensuring **long term security** guarantee.

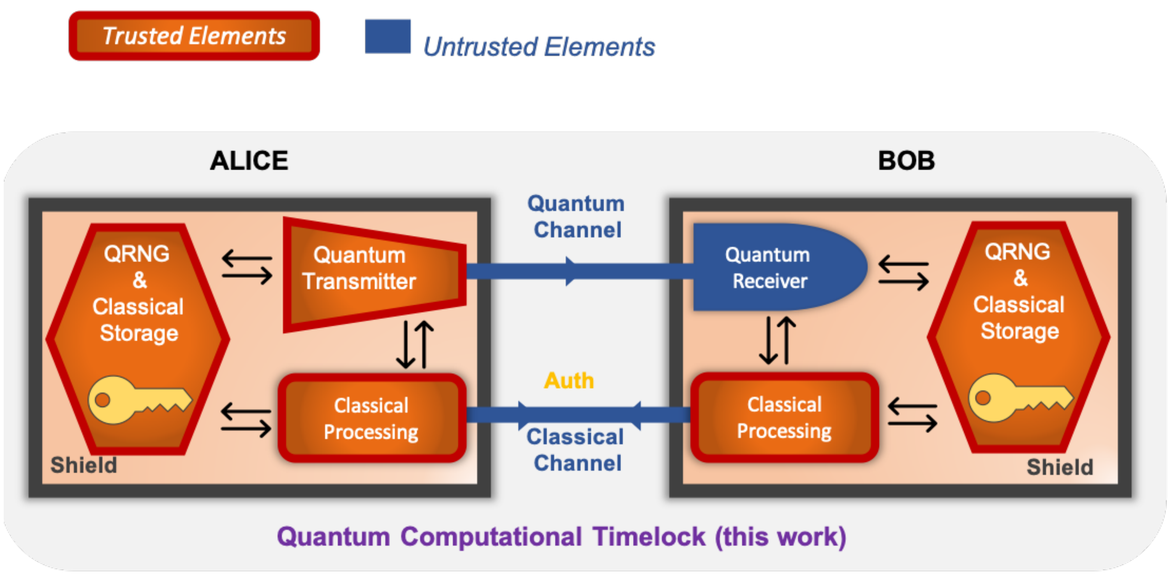


Fig. 4. Trust assumptions on the hardware, required to prove security MUB-QCT key distribution protocols.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Marie Sklodowska- Curie grant agreement No 675662