The practical quantum cryptography dilemma (and some ideas to address it)

Workshop on Implementation Attacks on QKD Systems - BSI & T-System

June 30 2021

Romain Alléaume – romain.alleaume@telecom-paris.fr

The Black Paper prophecy (Scarani, Kurtsiefer 2009)

arXiv.org > quant-ph > arXiv:0906.4547

Search...

Help | Advanced

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

The laws of physics play a crucial role in the security of quantum key distribution (QKD). This fact has often been misunderstood as if the security of QKD would be based only on the laws of physics. As the experts know well, things are more subtle. We review the progresses in practical QKD focusing on (I) the elements of trust that are common to classical and quantum implementations of key distribution; and (II) some threats to security that have been highlighted recently, none of which is unredeemable (i.e., in principle QKD can be made secure). 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; those who pursue ultimate security may have to suspend their claims of usefulness.

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;

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

Situation in 2021

☺ **Quantum Cryptography is still United and Roaring**

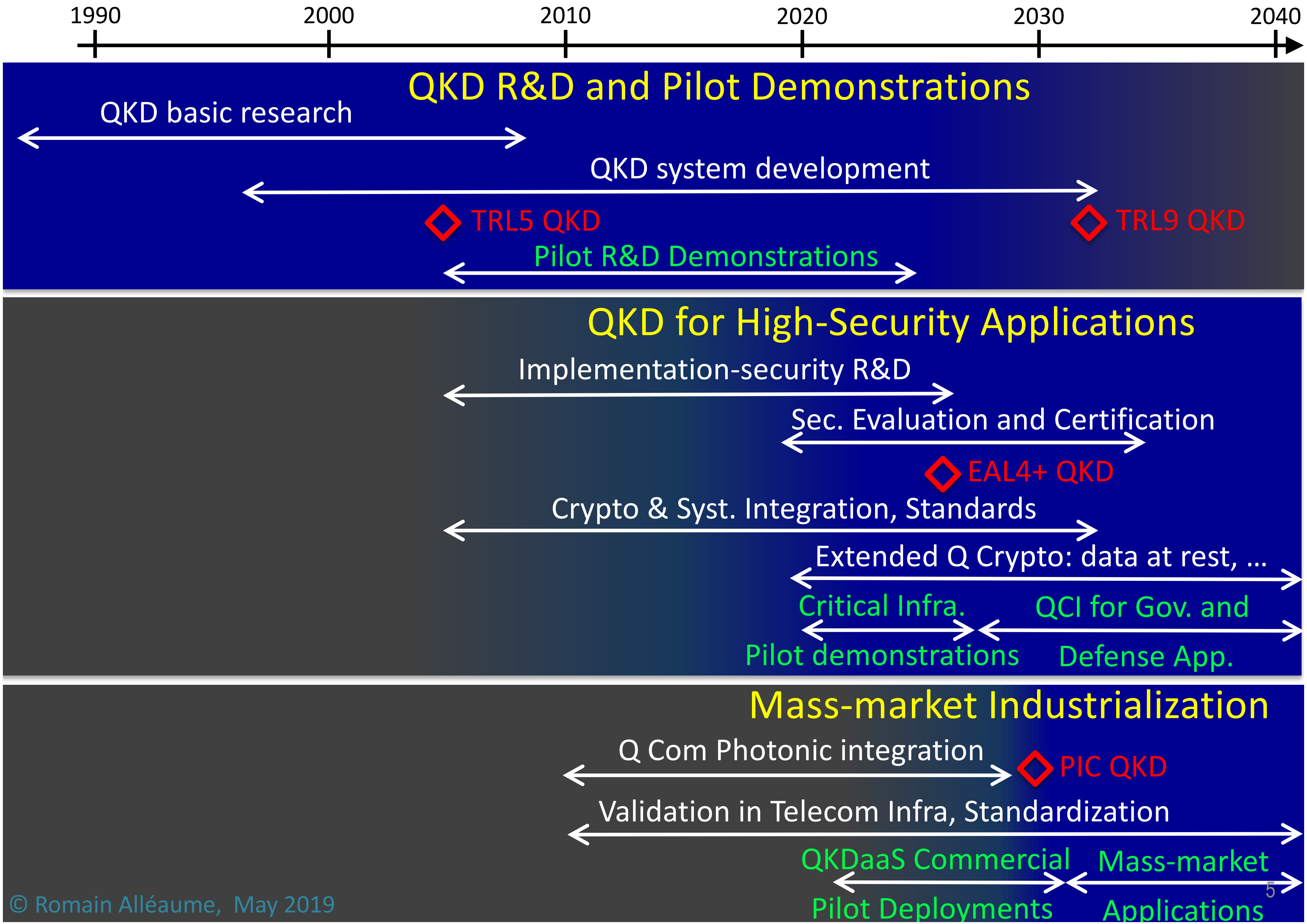
- ➢ Significant technological progress in maturity (TRL) and performance (rate, distance)
- ➢ Significant progress on the theory side (security proofs, ultimate limits, quantum repeater theory, etc..)

☹ **Real-world applicability of Quantum Crypto not yet clear**

- ☹ Cultural gap between classical and quantum cryptography (disjoint objectives ?)
- ☹ Difficult to define a strategic vision for « practical quantum cryptography »

Why has the « Black Paper prophecy » not yet come true ?

Reason 1: Quantum Crypto (QKD) was mostly at research stage



© Romain Alléaume, May 2019

Reason 2: Because splitting has a high cost,

and it is actually not clear whether Quantum Crypto should be willing to pay it or not

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

absolute security, and abstract quantum crypto may not directly apply to real systems (because of imperfections)

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

if practical Quantum Crypto cannot reach absolute security,

What Type of Security then ?

This talk:

Take a closer look at the practical cryptography side

1) What level of security can we claim in practice?

What methodology can we use to evaluate and certify QKD implementations?

Relation with theoretical security

2) The practical quantum crypto dilemma, and some ideas to address it:

Thoughts about QKD System design and certification

Quantum Computational Timelock

1) What level of security can we claim in practice?

- What methodology can we use to evaluate and certify QKD implementations ?
- Relation with theoretical security

scientific reports

Check for updates

OPEN

Experimental vulnerability analysis of QKD based on attack ratings

Rupesh Kumar[1], Francesco Mazzoncini[2], Hao Qin[3] & Romain Alléaume[2]✉

Published in May 2021

arXiv:2010.07815

- **Illustrate that Common Criteria Vulnerabilty Analysis (VAN) methodology, is well suited for QKD**

- **Position QKD within the cybersecurity landscape (not as an exception)**

Attack Rating / Attack Potential

- Reference: CEMV3

Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5 (2017). URL https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

- Use some standardized methodology to compute the **Attack Potential**, associated to an attack Path

Attack Potential (AP) = metric to assess attack difficulty

High AP ⇔ High Difficulty to perform the attack

Tables used in the article (adapted from CEMV3)

Expertise	
Laymen	0
Proficient	3
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
Equipment	
Standard	0
Specialized	4
Bespoke	7
Multiple bespoke	9

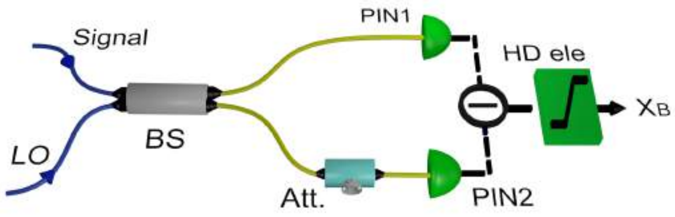
Table 1: Table for the evaluation of the Attack Potential [3]

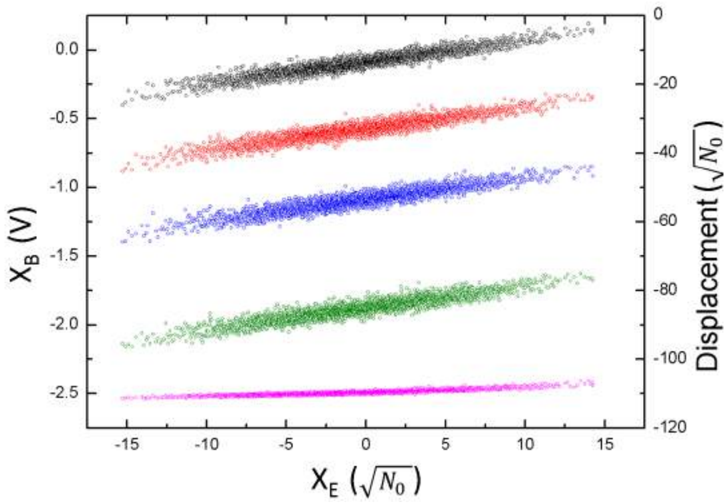
Rating	AP Range
Basic	0 – 10
Moderate	11 – 15
High	16 – 19
Beyond High	20 – ∞

Table 2: Semi-qualitative scale for attack rating. This scaling is adapted with respect to the Common Criteria [3]

Not considered in the article: **Elapsed Time** (not easily applicable to lab system)

Saturation Attack on CV-QKD





Homodyne detection has a limited Output Range

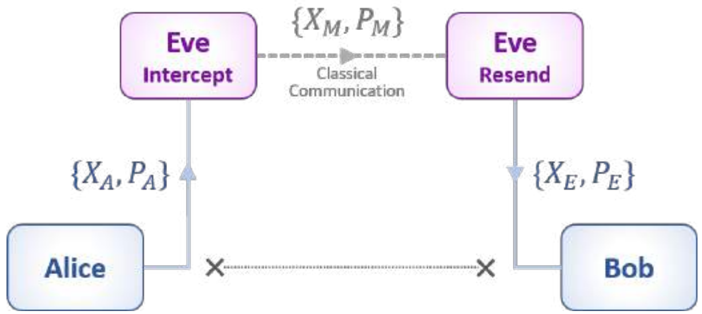
➔ Saturates for High Quadrature values

[1] Qin, H., Kumar, R. & Alleaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Physical Review A* **94**, 012325 (2016).

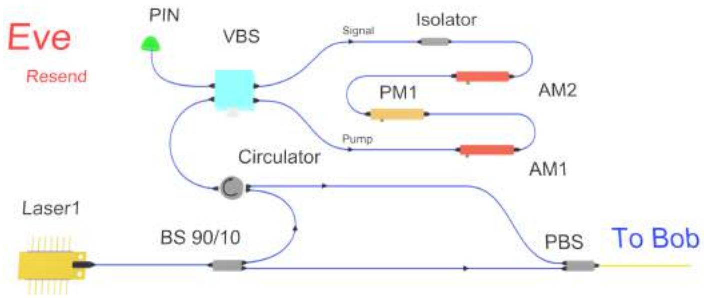
[2] Qin, H., Kumar, R., Makarov, V. & Alleaume, R. Homodyne-detector-blinding attack in continuous variable quantum key distribution. *Phys. Rev. A* **98**, 012312 (2018).

Saturation Attack:

- Actively induce Saturation
- Intercept-Resend Attack



Two (Saturation) Attack Paths

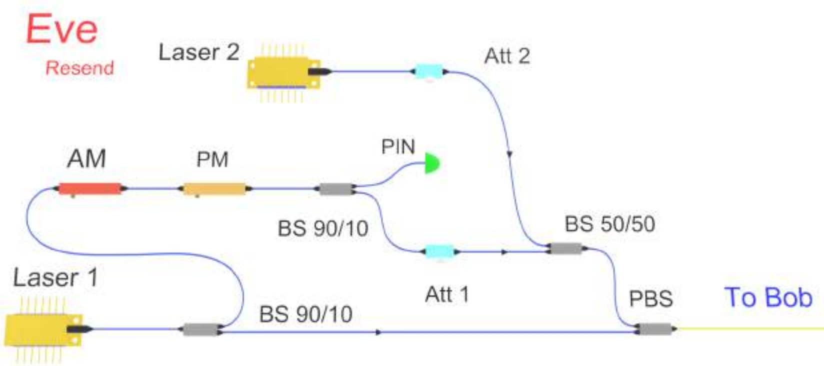


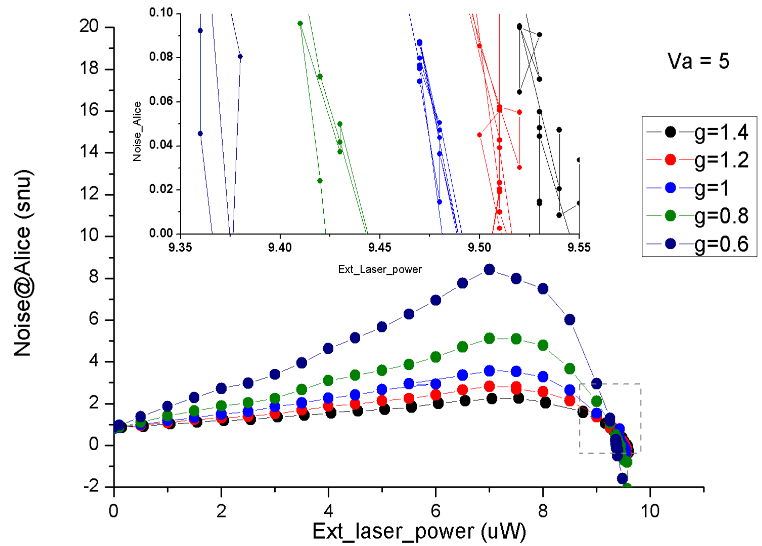
Induce Coherent Displacement

- Same-mode attack
- Eve must be phase –locked with Alice-Bob: *Sagnac Loop*
- ***Challenging !***

Incoherent Blinding

- External laser
- Good attack control demonstrated by tuning laser power



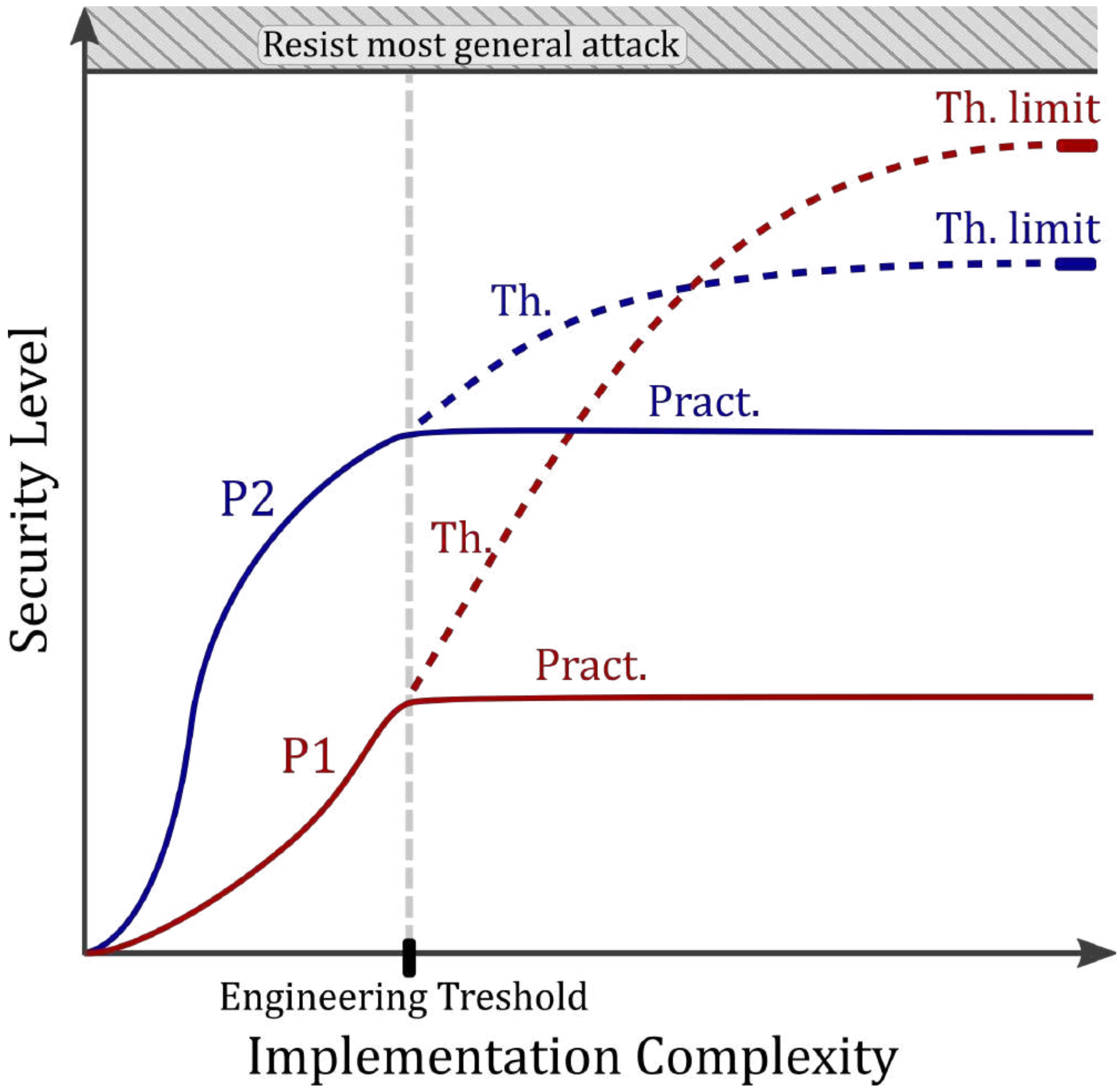


Rating the two attack paths

	Resources	Attack Potential					Rating	Experimental results
Coherent Attack	Interferometric setup for coherent displacement	Exp	KoT	WoO	Equip	**AP**	**Beyond High**	✓ Noise model experimentally characterized × Attack not feasible under noise model
		6	3	10	7	**26**		
Incoherent Attack	External laser and attenuator	Exp	KoT	WoO	Equip	**AP**	**Moderate**	✓ Attack experimentally demonstrated
		3	3	4	4	**14**		

Expertise / Knowledge of the TOE / Window of Opportunity / Equipment

The QKD system with the strongest proof may not be the more secure one



What security guarantee can we obtain from QKD implementation evaluation / certification ?

Practical Security < Theoretical Security ~ Absolute Upper Bound

Role of Evaluation (incl. Vulnerability Analysis VAN)

⇒ Verify resistance against ~ all Attacks up to some AP level

⇒ Provides confidence in a **Lower bound on Practical Security**

Importance of minimizing Implementation Complexity

- Increase Practical Security
- Reduce gap with Theoretical Security

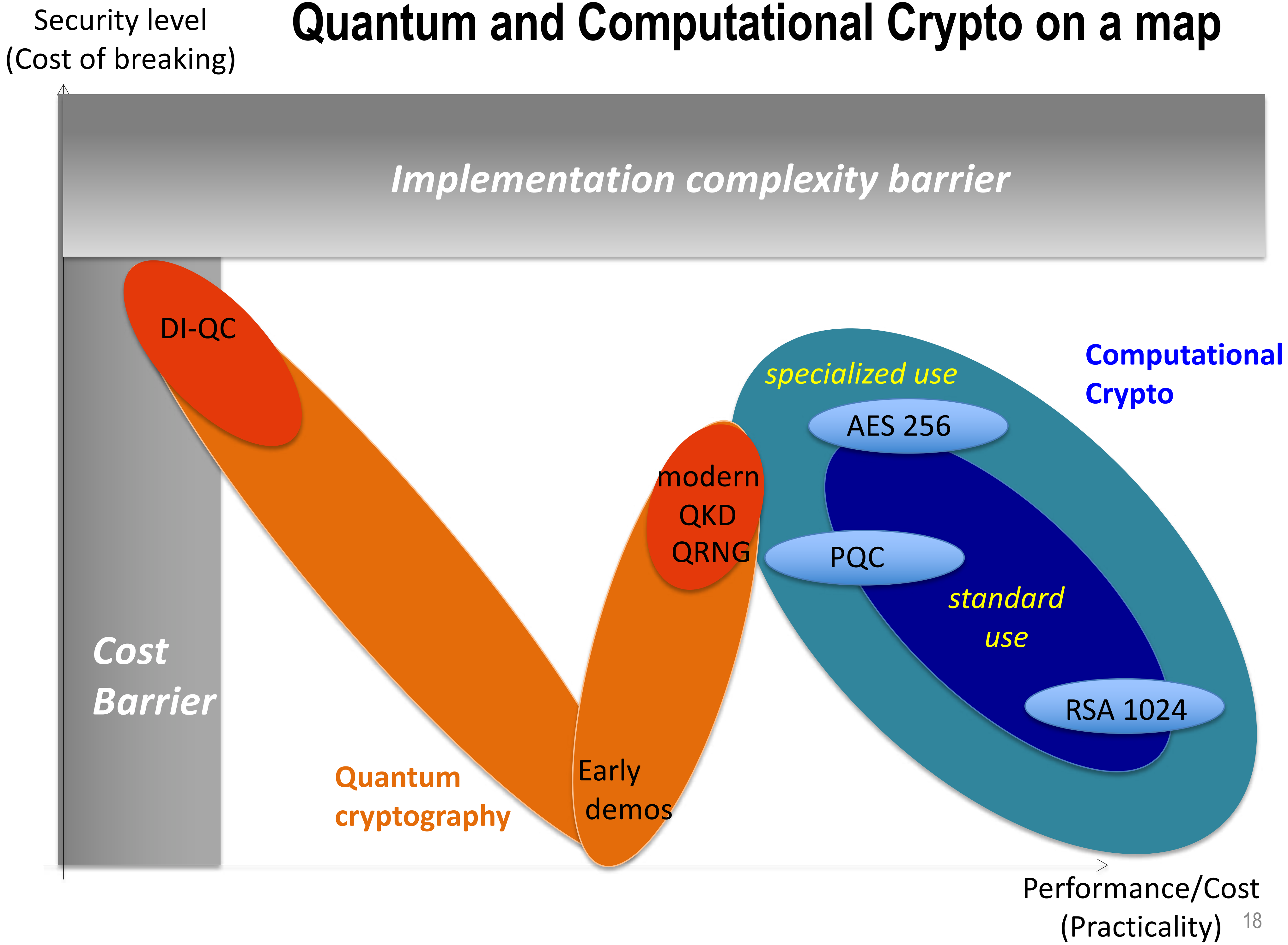
➔ **New optimization route for QKD protocols and implementations (at fixed implementation complexity)**

2) The practical quantum crypto dilemma, and some ideas to address it:

Thoughts about QKD System design and certification

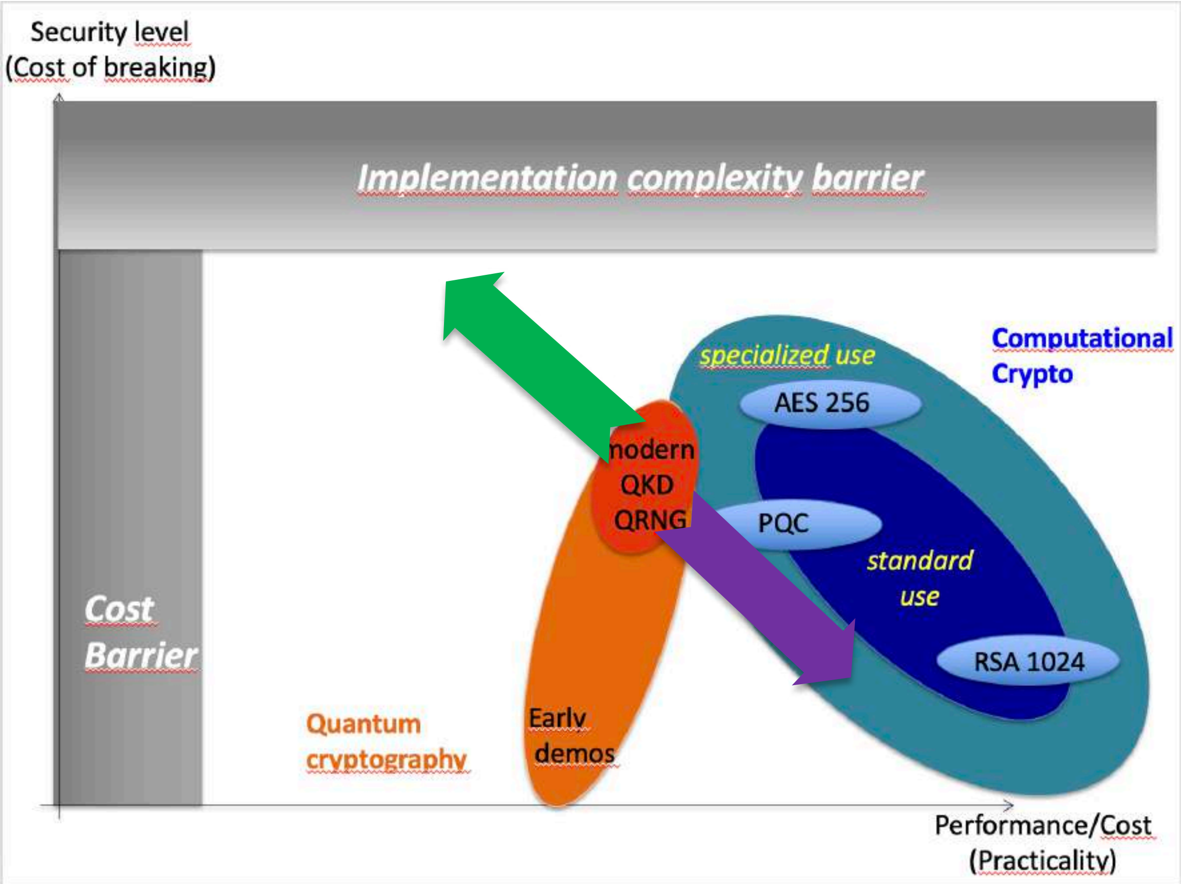
Quantum Computational Timelock

Quantum and Computational Crypto on a map



- 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

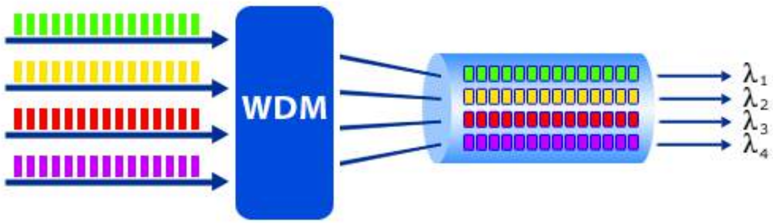


Practical Quantum Cryptography Dilemma:

Obvious next steps towards practicality have negative side-effects

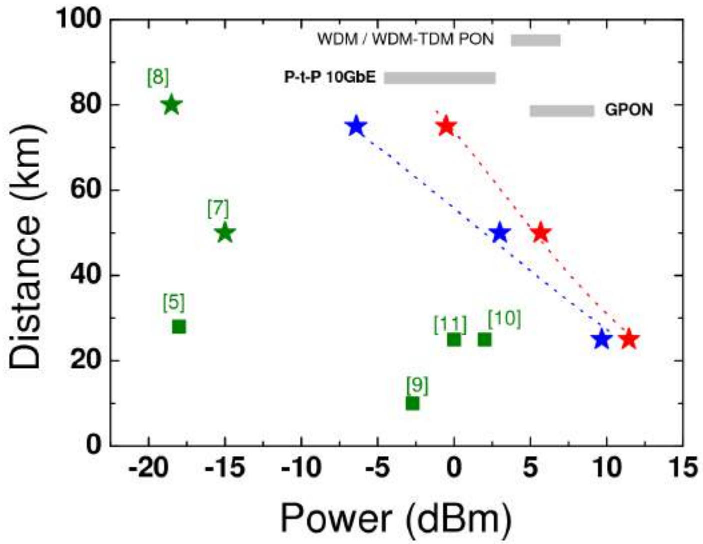
Technology Upgrade bring new security challenges
Example: CV-QKD Technology Upgrade

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).

➔ Bring Cost Down // Noise up



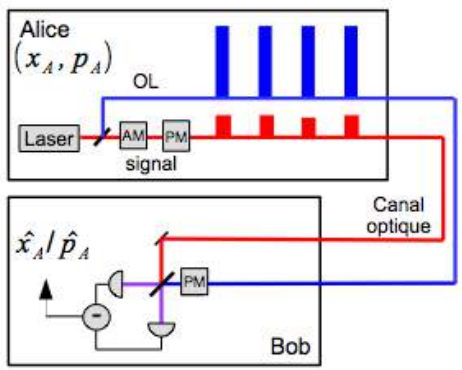
CV-QKD
strong WDM
coexistence
(10 dBm @ 25 km)
favored by
coh detection

Coherent Q Com System Design

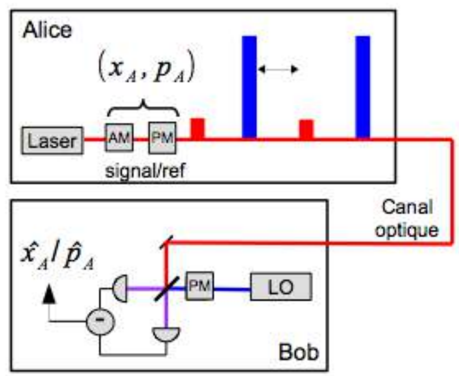
"Local'' Local oscillator (LLO)

➔ *Removes TLO Loophole*
➔ *High Speed*

➔ *Loss tolerance down*
➔ *Calibration complexity up (DSP)*



Transmitted LO



Local LO = LLO

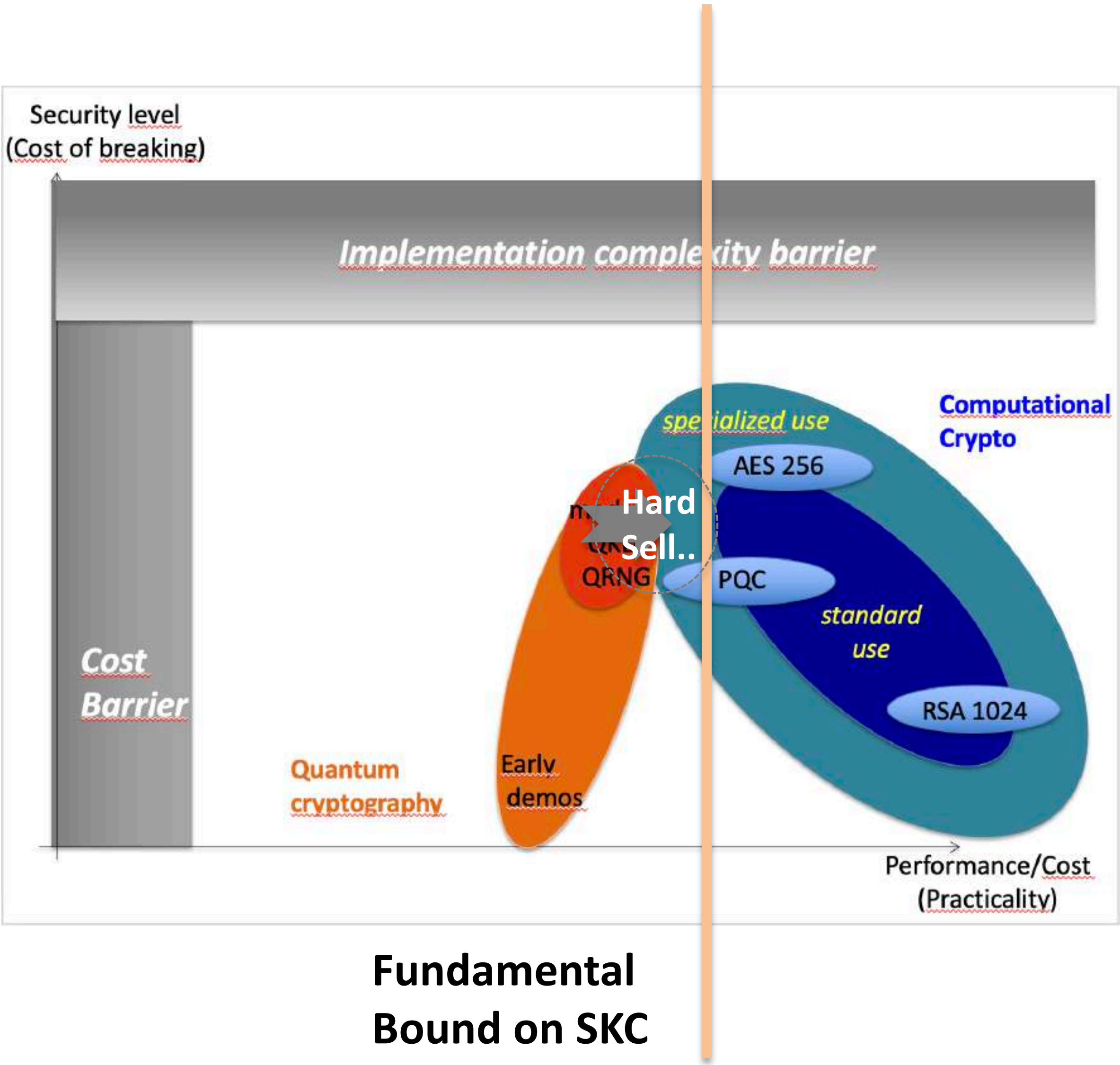
How to address Practical Quantum Cryptography Dilemma ?

- Improve System Design, by jointly addressing (co-design)
  - Performance / Cost
  - Security

- **Further Thoughts**
  - Which Quantum Hardware generation should we certify:
    - 19’’ Rack QKD ? Chip-based QKD ?
  - Complexity of QKD certification is very high: **break down the problem**
    - Start with QRNG (cf UK) (and wait for chip-based QKD ?)
    - Separate (start with ?) the work on classical part of QKD on selected trusted hardware platforms)➔ clarify physical trust assumptions (PP)
    - Isolate «qcrypto building blocks » for which we can have
      - High engineering quality (high performance / low complexity)
      - Strong security assurance possible

Practical QKD Dilemma 2:

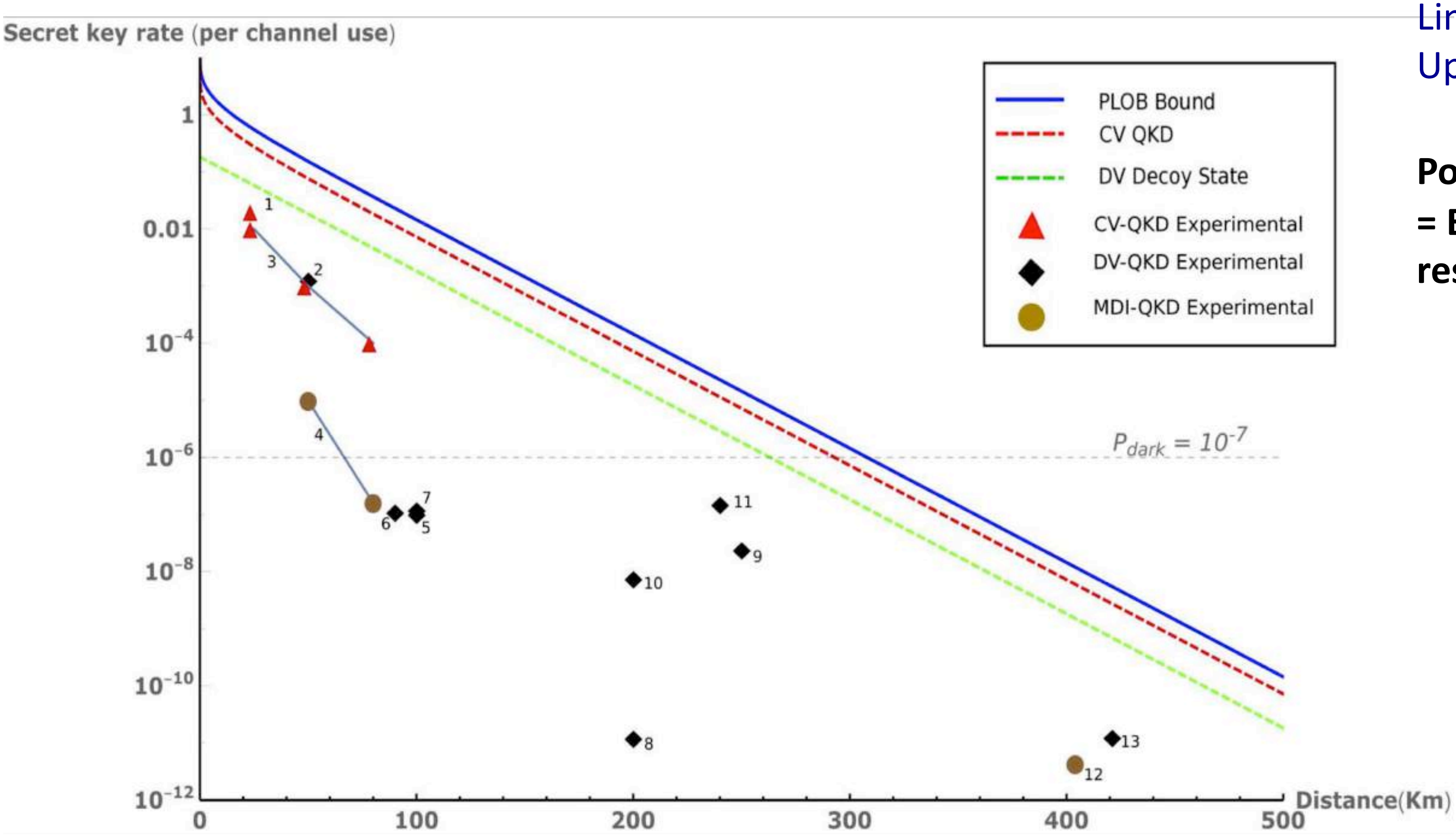
Fundamental limits of repeaterless QKD may limit applications to small niche



Fundamental Bound on SKC

e.g.
Secure Comm with QKD+OTP

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



Lines =
Upper bounds

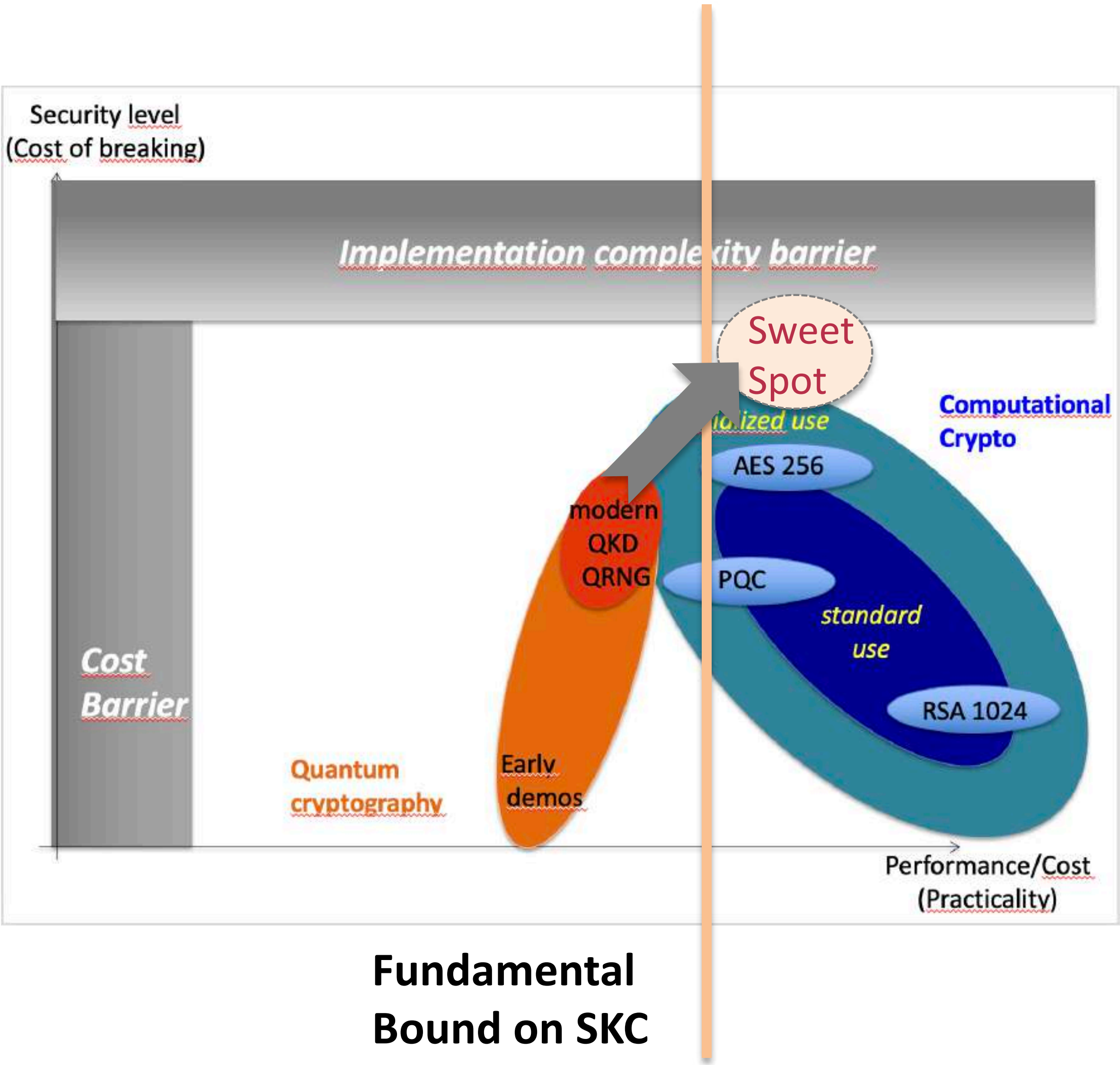
Points
= Experimental results

Room for performance improvement is limited

Escape the practical Quantum crypto dilemma

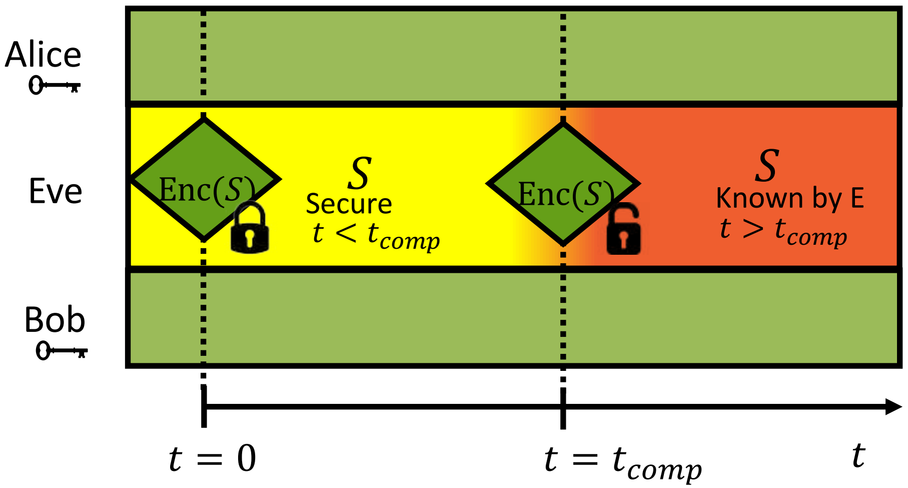
➔ *Requires to « break » the fundamental (repeaterless) SKC bounds*

➔ *(Q Repeaters) or Change the setting / model*

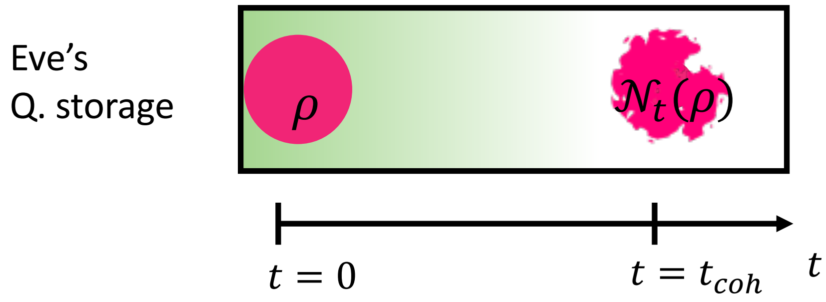


Quantum Computational Timelock (QCT) Security Model

1. Short term secure encryption:



2. Time-limited quantum storage:



$$||\mathcal{N}_t(\rho) - \frac{\mathbf{I}_d}{d}|| \leq \frac{1}{d^2}, \qquad \forall t > t_{dcoh}$$

- State of the art $t_{coh} \approx \mathcal{O}(1)\ sec$
- Top secret (AES Encryption) : $t_{comp} \approx 10^8\ sec$

➡ $\boldsymbol{t_{coh} \ll t_{comp}}$

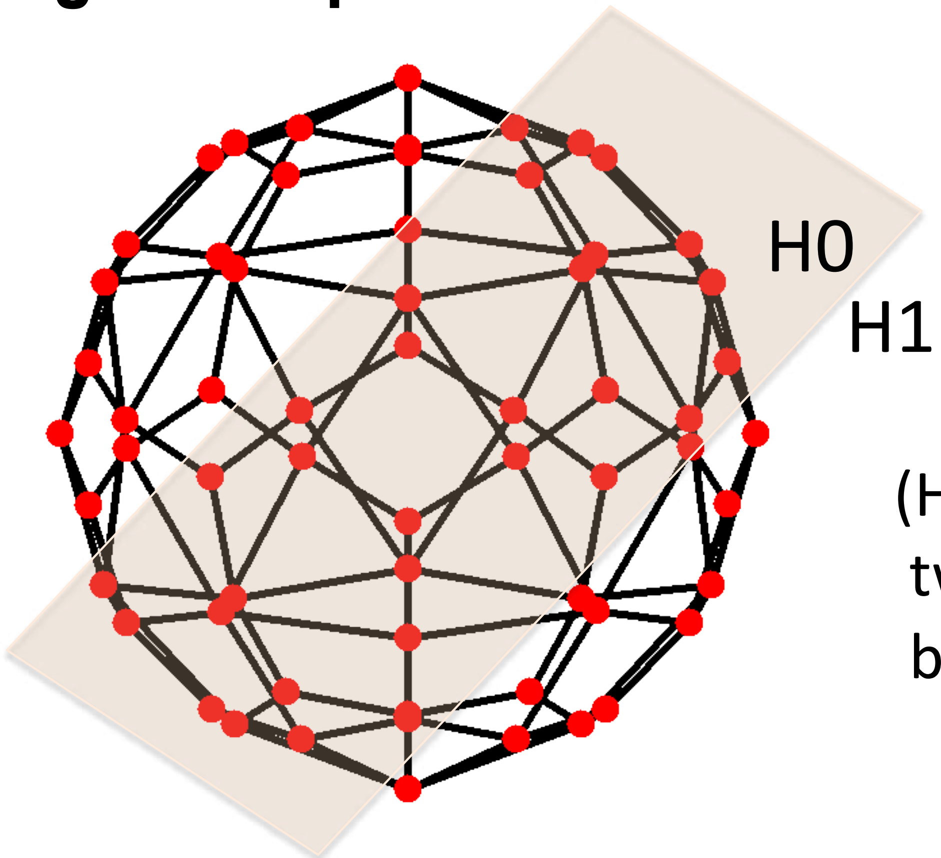
Likely to hold in the near / mid-term

How to design a KD protocol in the QCT model ?

High dimensional (d>>1) quantum encoding

e.g d=64

(artistic view)



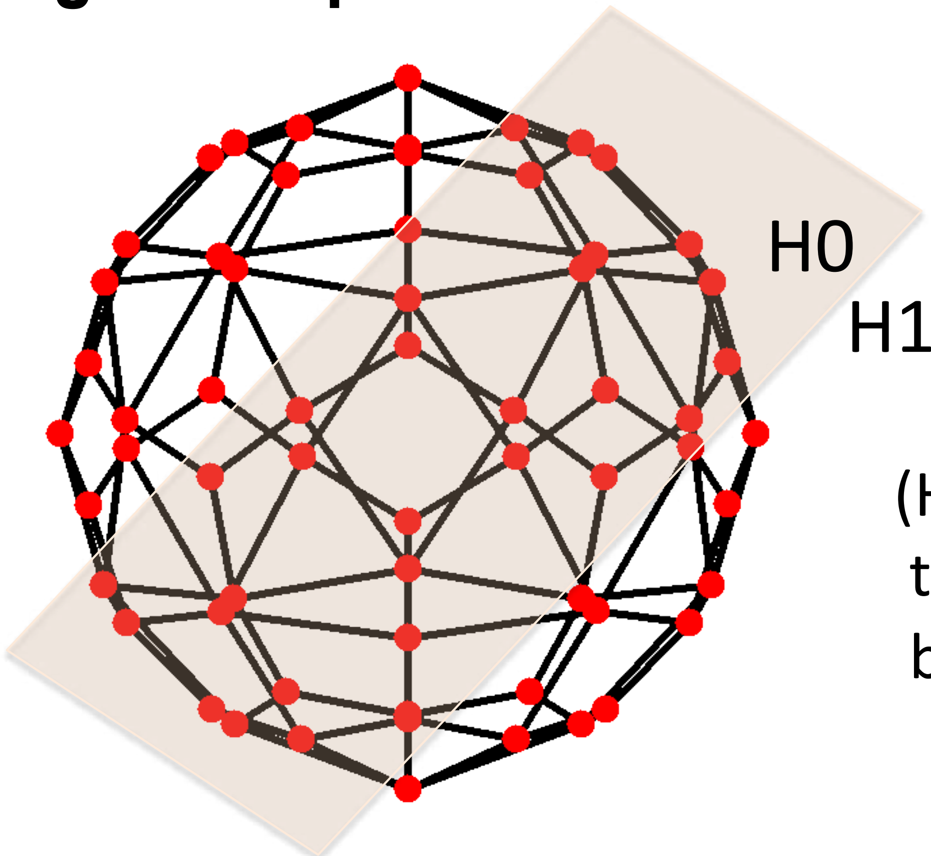
(H0,H1): partition in two d/2-dimensional boolean subspaces

How to design a KD protocol in the QCT model ?

High dimensional (d>>1) quantum encoding

e.g d=64

(artistic view)



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

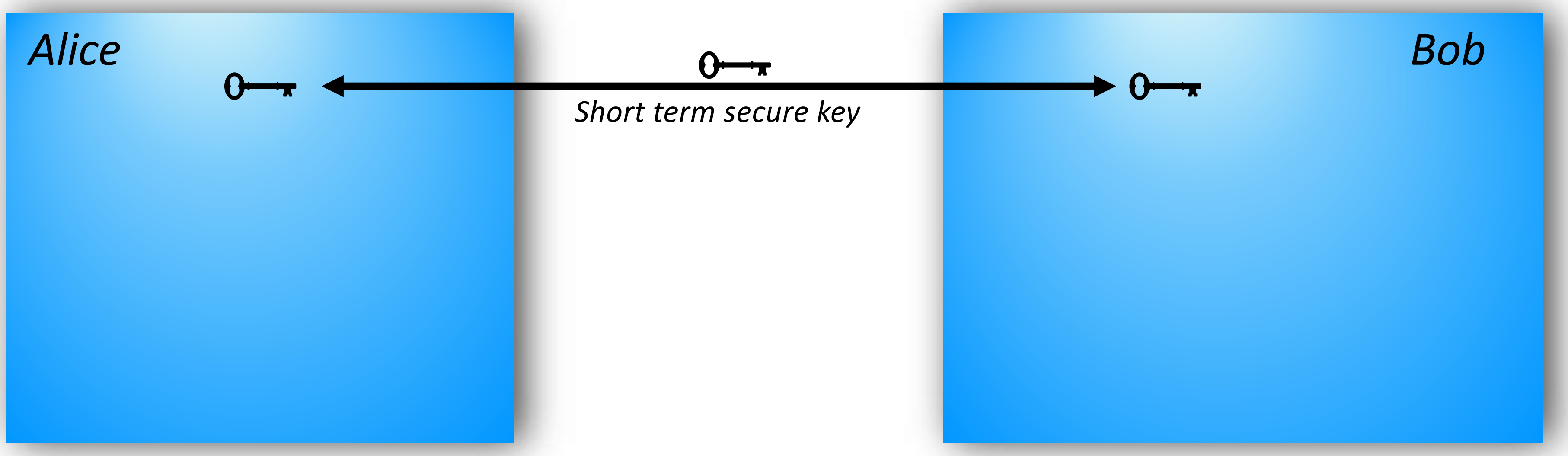
High-level idea for q cryptographic protocol:

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

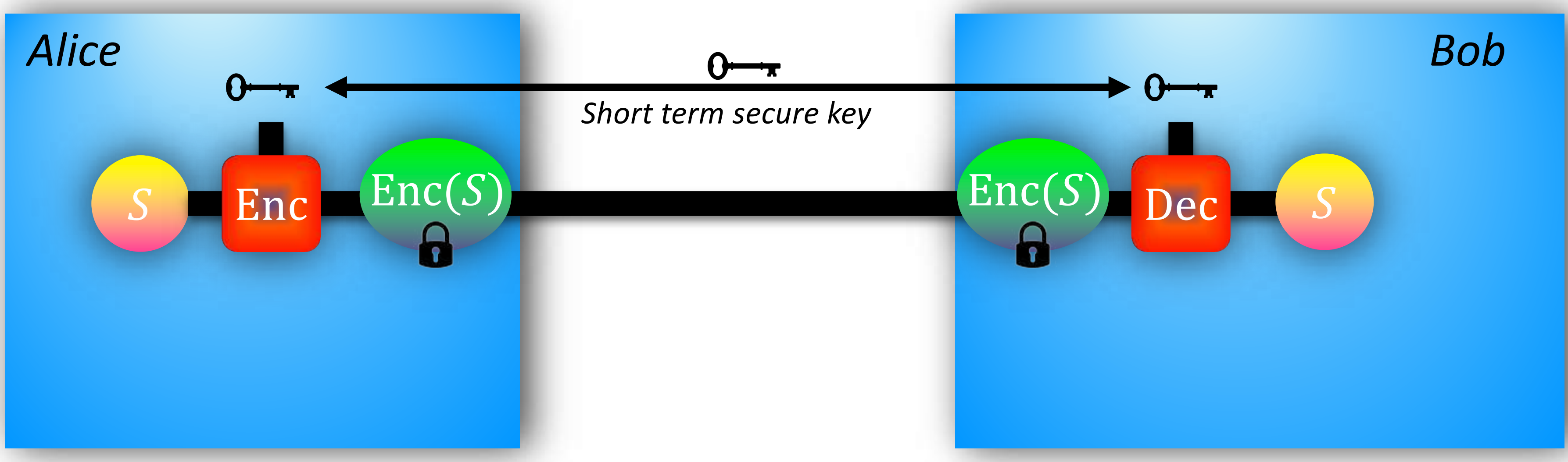
If one knows S ➔ can decode b *(measurement (H0,H1))*

If does not know S ➔ cannot guess b (what measurement ?)

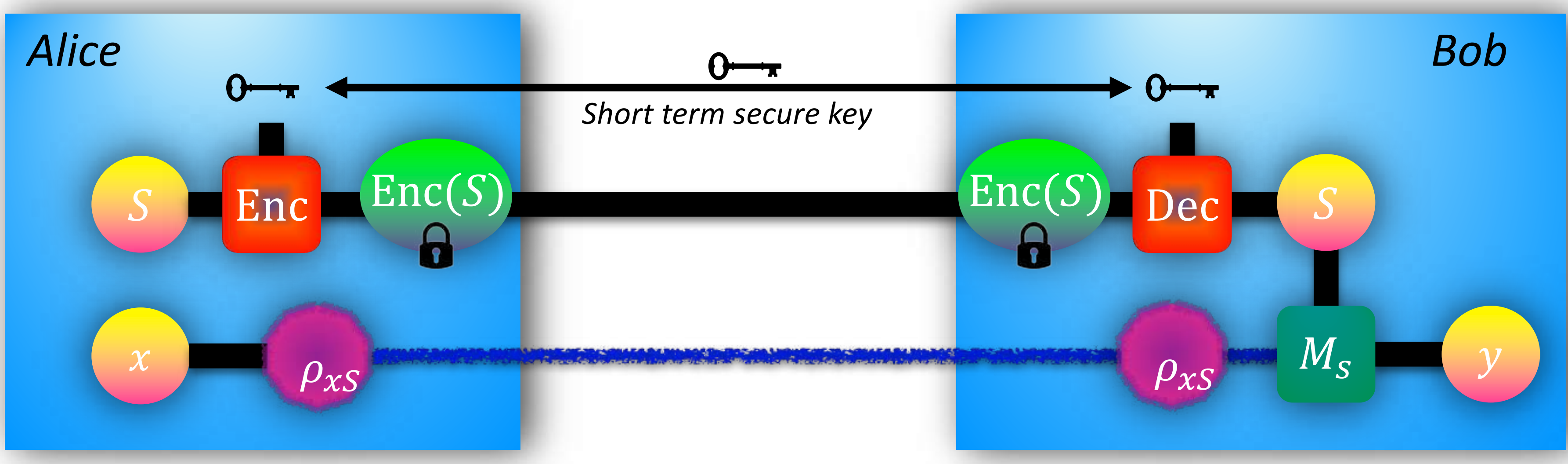
Quantum Computational Time-lock (QCT)



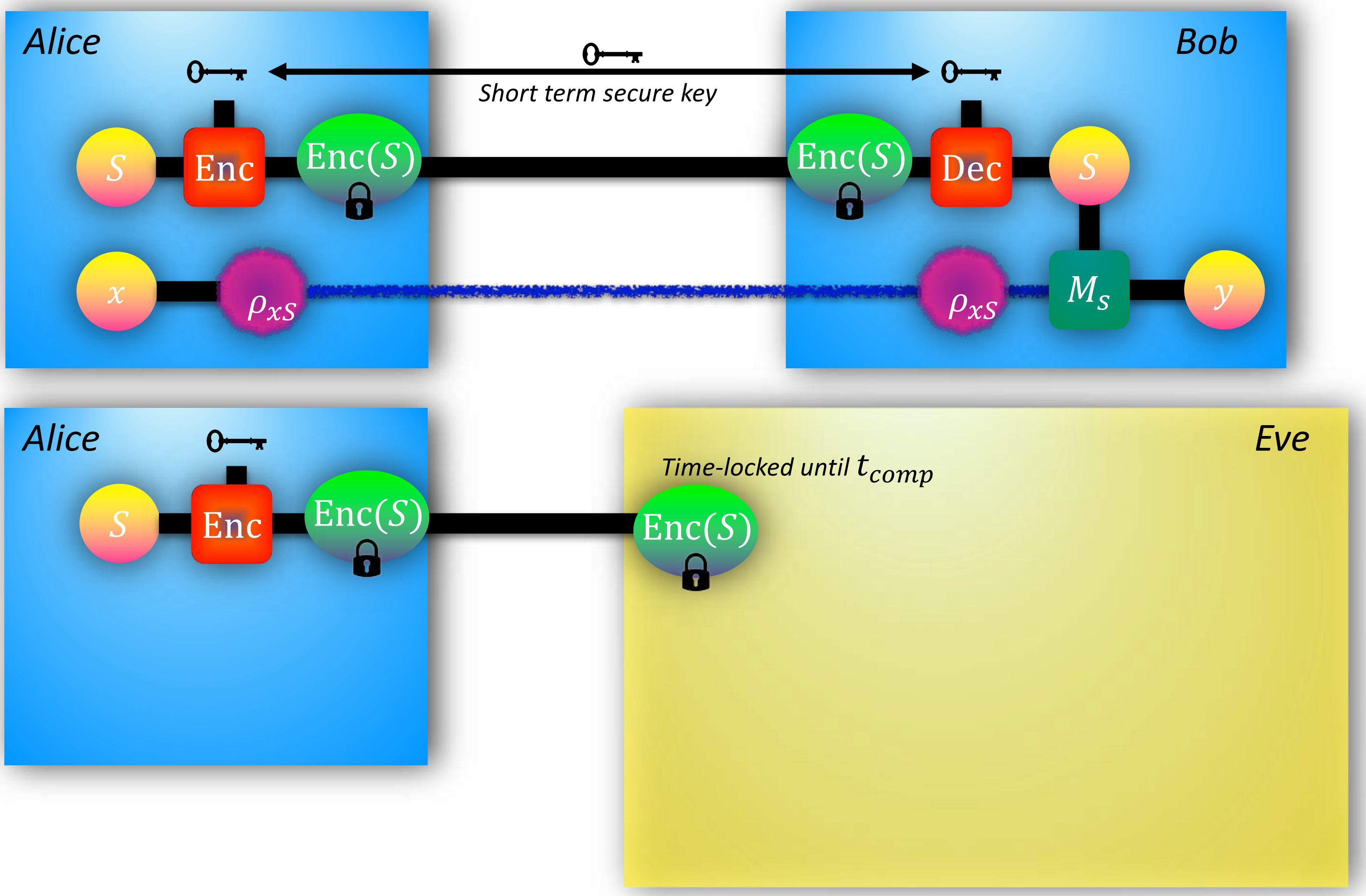
Quantum Computational Time-lock (QCT)



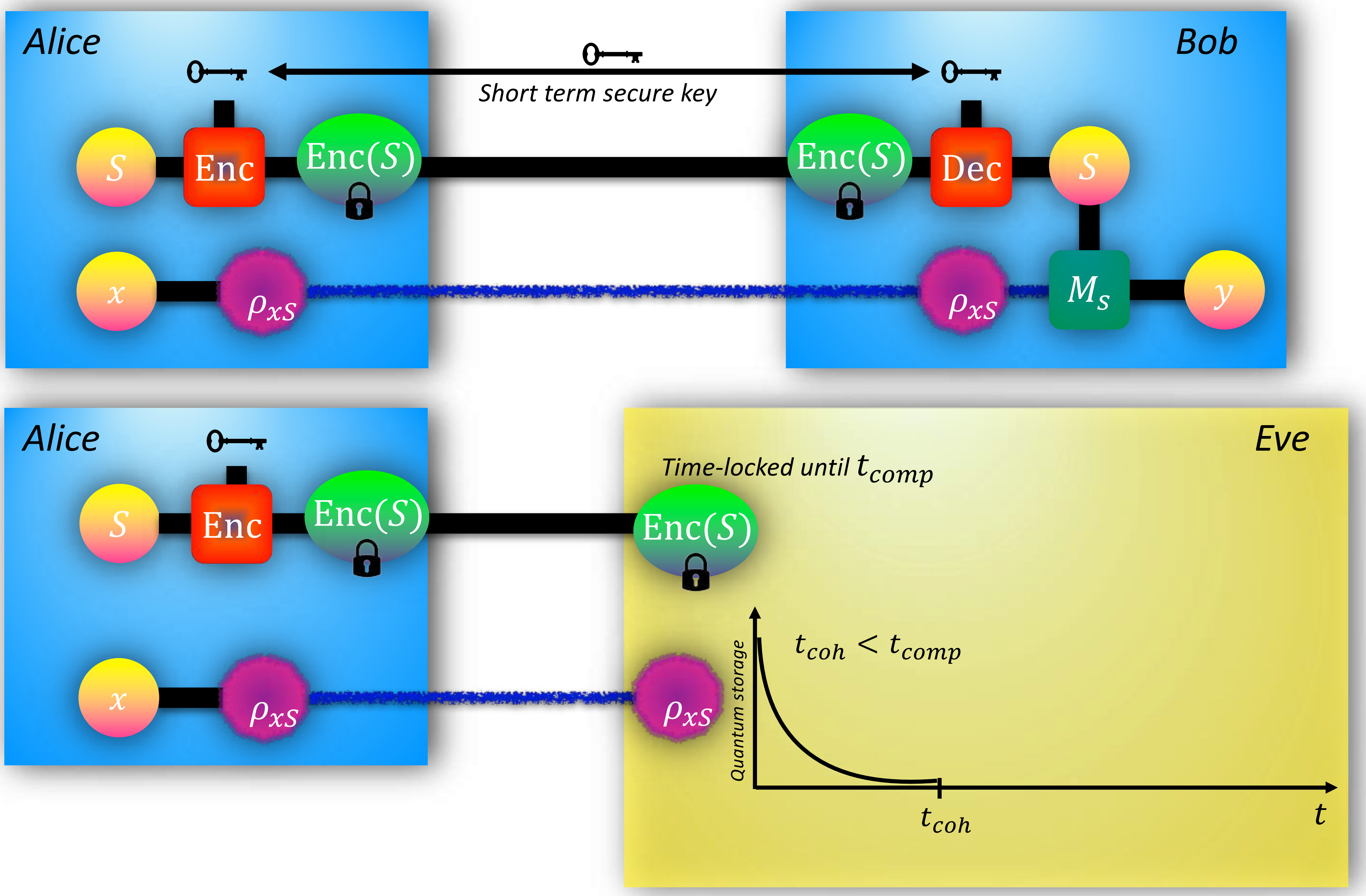
Quantum Computational Time-lock (QCT)



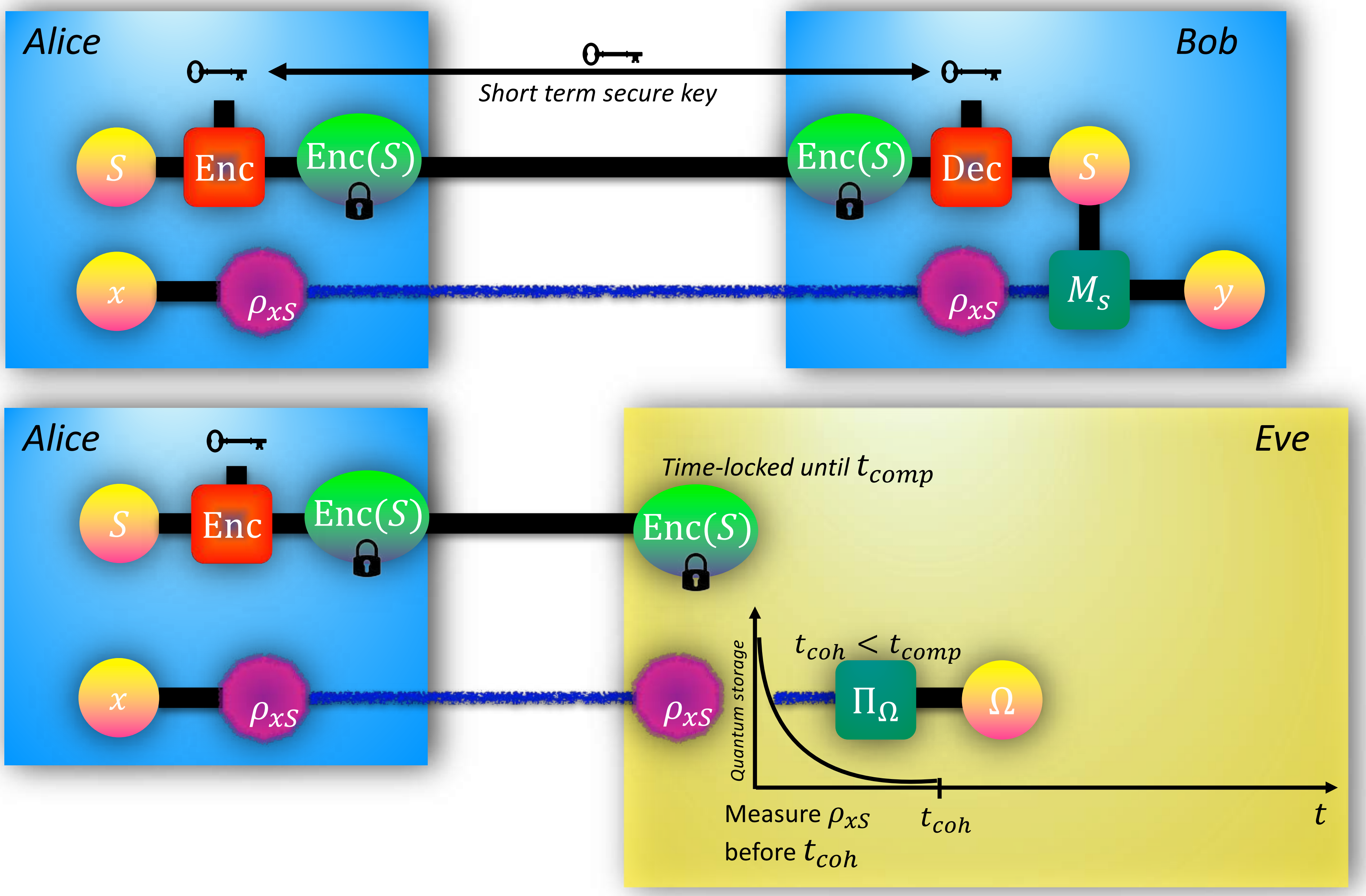
Quantum Computational Time-lock (QCT)



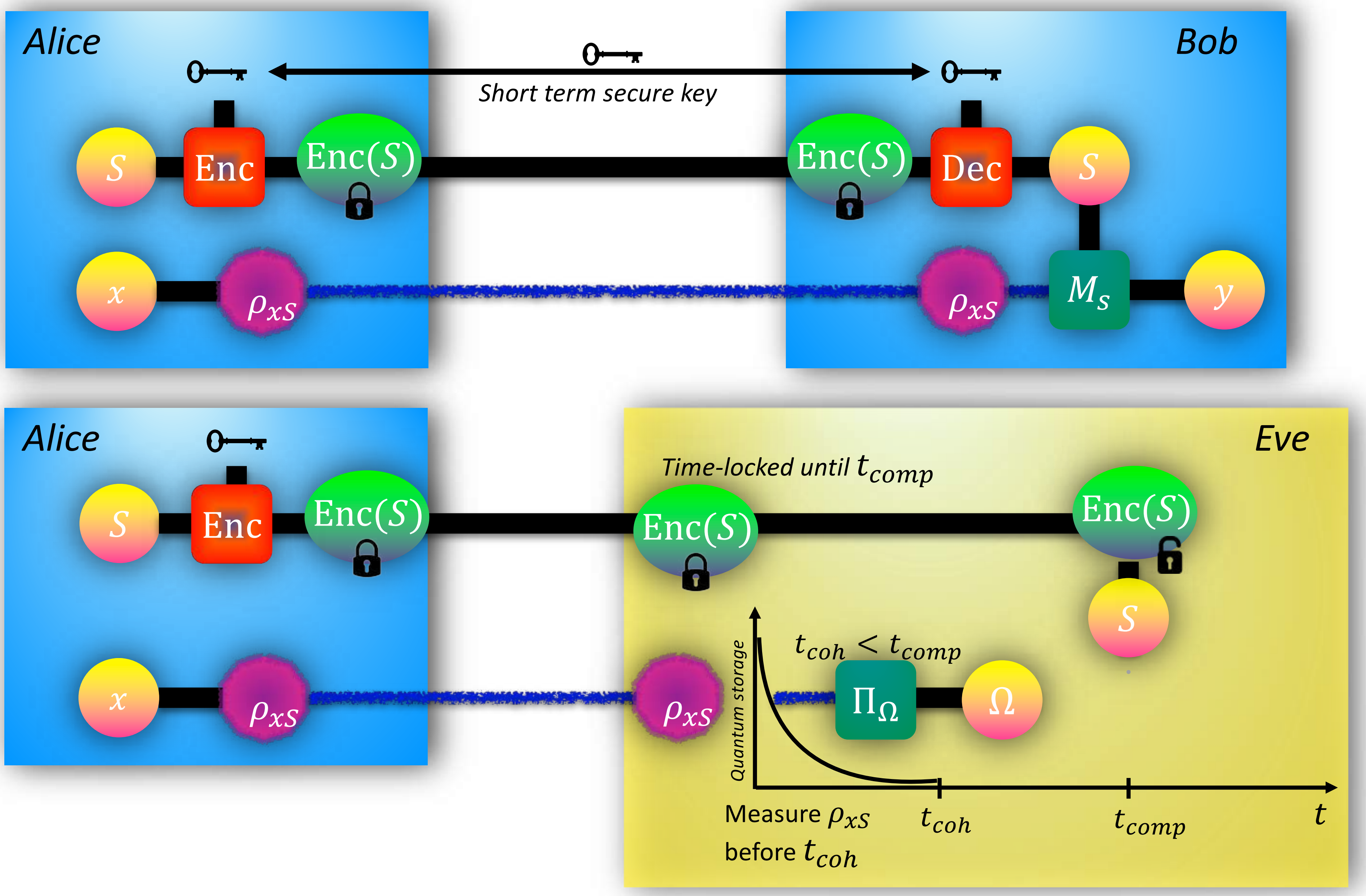
Quantum Computational Time-lock (QCT)



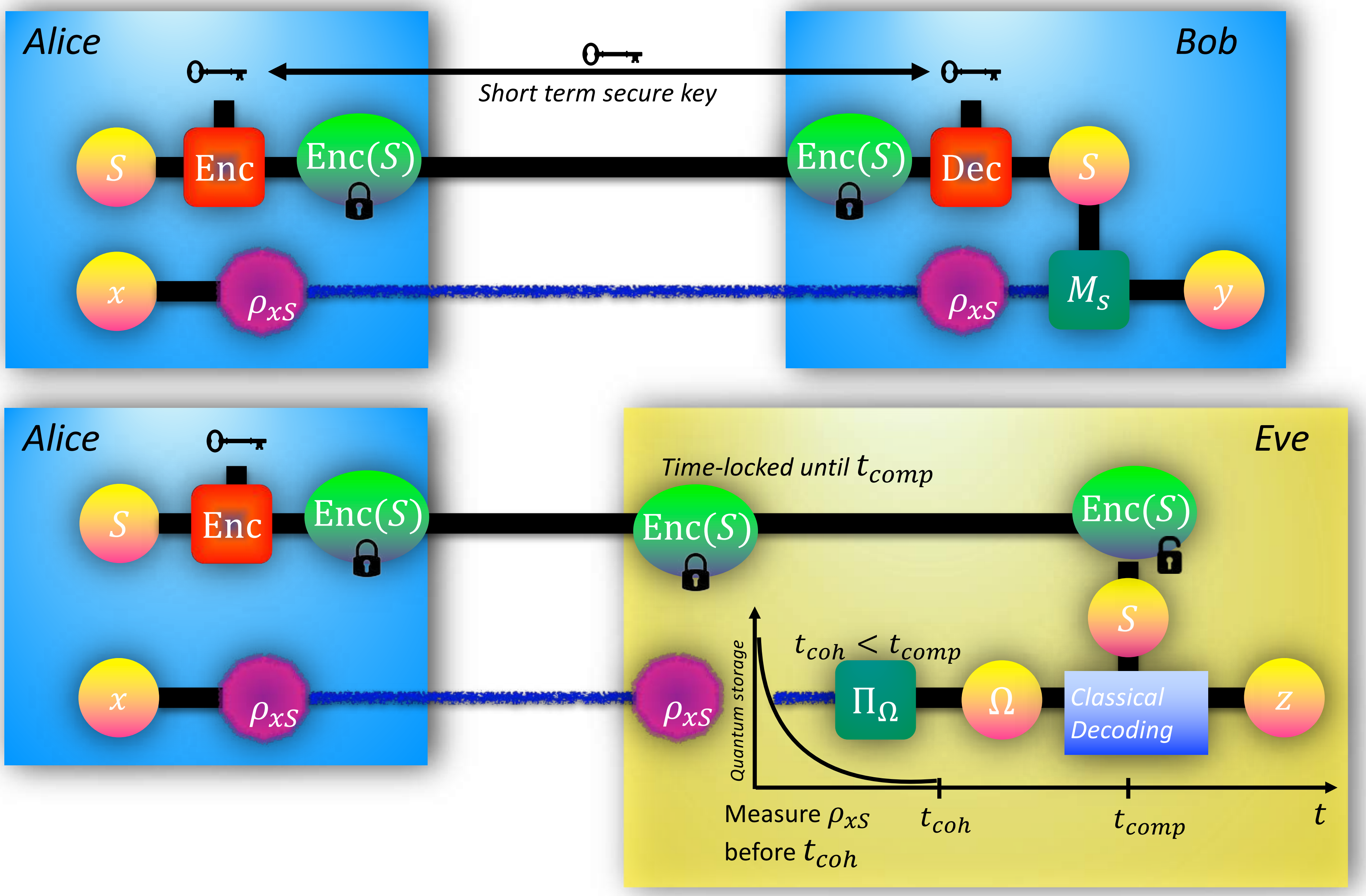
Quantum Computational Time-lock (QCT)



Quantum Computational Time-lock (QCT)



Quantum Computational Time-lock (QCT)



Key distribution using QCT: MUB-QCT arXiv:2004.10173

Encoding a bit $x \in \{\mathbf{0}, \mathbf{1}\}$ on a $d = 2^N$ dimensional quantum state ρ_A using full set of *Mutually Unbiased Bases (MUBs) and a set of pair-wise independent permutation.*

Alice chooses a MUB: U_θ , $\theta \in [d+1]$,
and a pair-wise independent permutation P_σ , $\sigma \in [\Lambda_d], (\Lambda_d = 2^{d-1})$.

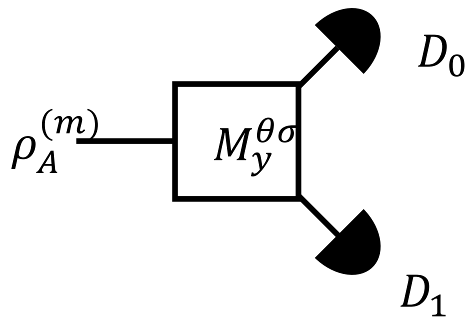
Randomization w.r.t Eve

Encode a random bit $x \in \{0,1\}$ on the d-dimensional quantum system A as:

$$\rho_A = \frac{1}{|\theta||\sigma||r|}\sum_{\theta\sigma r} P_\sigma U_\theta |i_{xr}\rangle\langle i_{xr}| (P_\sigma U_\theta)^\dagger,$$

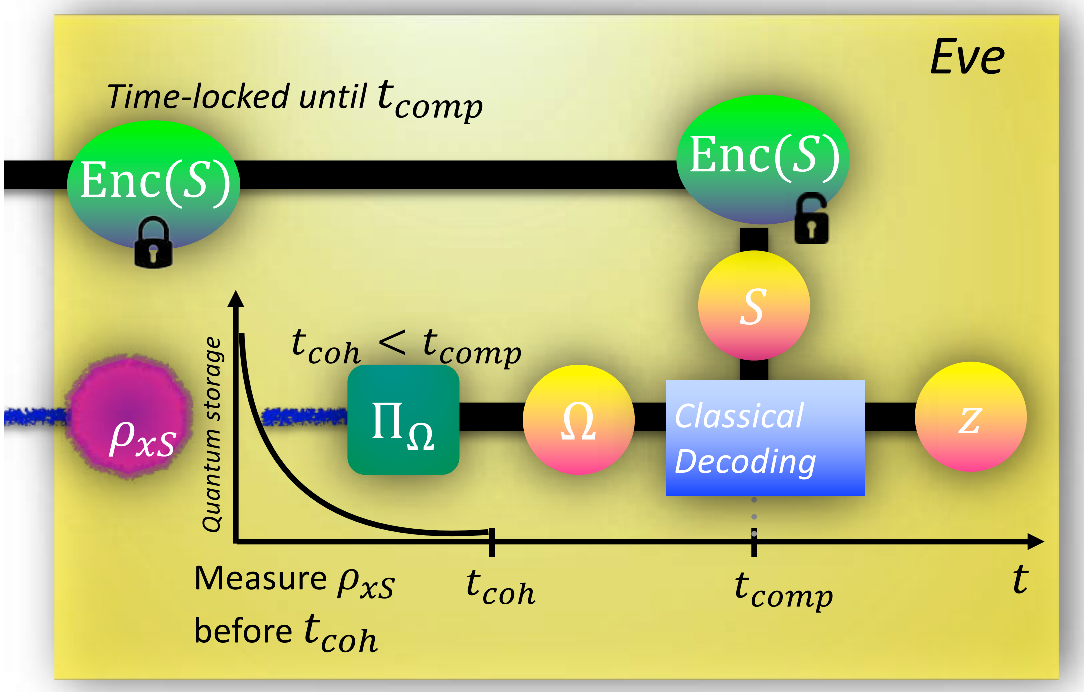
where $i_{xr} = x \times \frac{d}{2} + r$, for $r \in [d/2]$.

- Bob's Measurement: measure using U_θ & P_σ



Security Analysis:
Reduction to Strong Q-C Randomness Extractor

Reduction of Eve's strategy:



- **Quantum Computational Timelock Security Model**

  - ☑ No gain in delaying Eve measurement.
  - ☑ ➔ Eve measures without knowing S

Protocol drives Eve into implementing

- $\{U_\theta P_\sigma : \theta \in [d+1], \sigma \in [\Lambda_d]\}$ forms a "STRONG" Quantum to Classical randomness extractor.

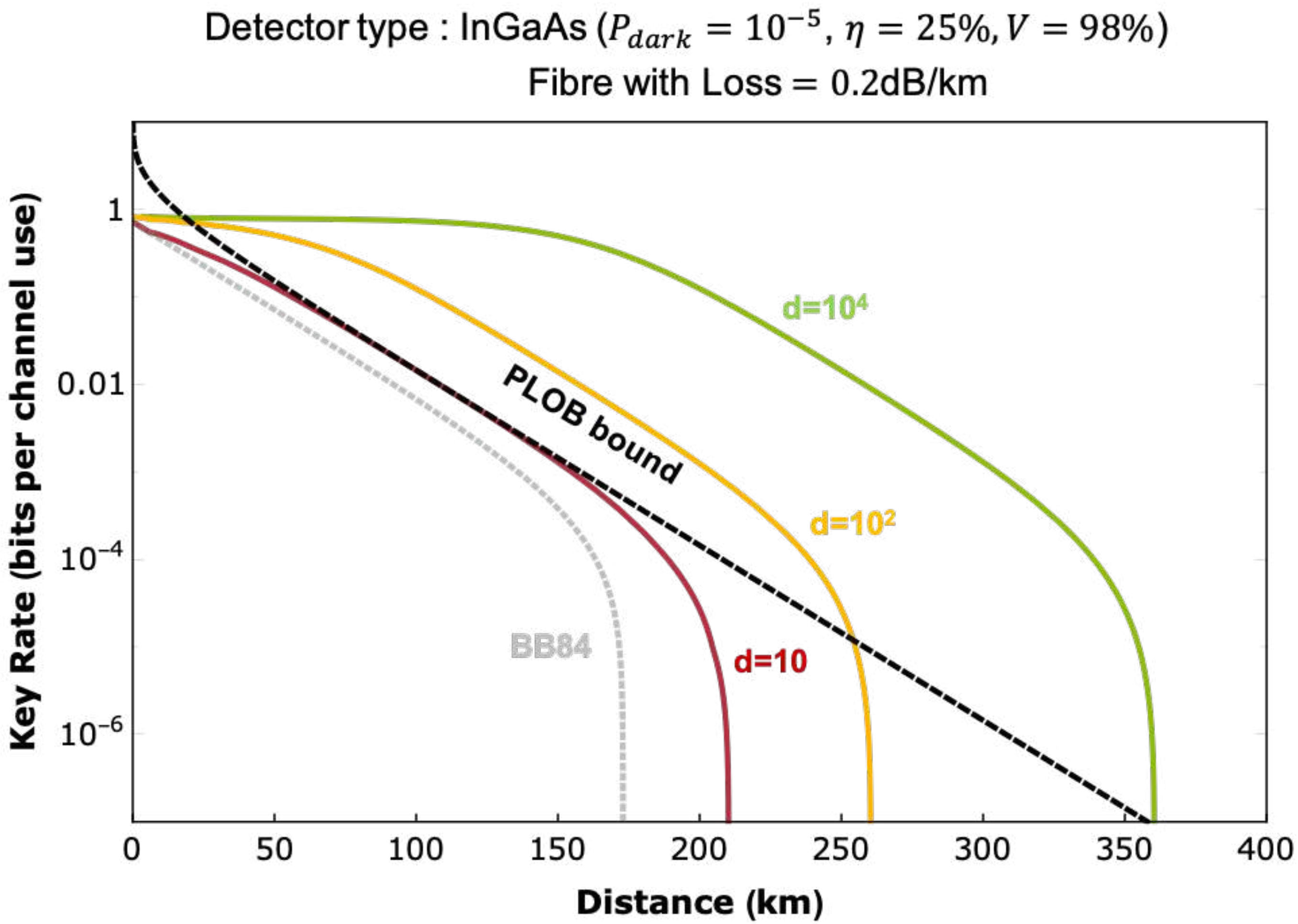
  (M. Berta et.al., IEEE Trans. Info. Theo. 60, 1168 (2014))

  ➔ Eve measurement outcome z is strongly decoupled from x (even after S is revealed)

Pguess(X|E) = ½ + o(1/d)

Performance of MUB - QCT protocol

Generalization to with coherent states (m), and high dimensional (n modes) encoding
Assuming non-adaptative attacks: **Pguess(X|E) = ½ + o(m/d)**



Secure KD with O(n) photons / ch use

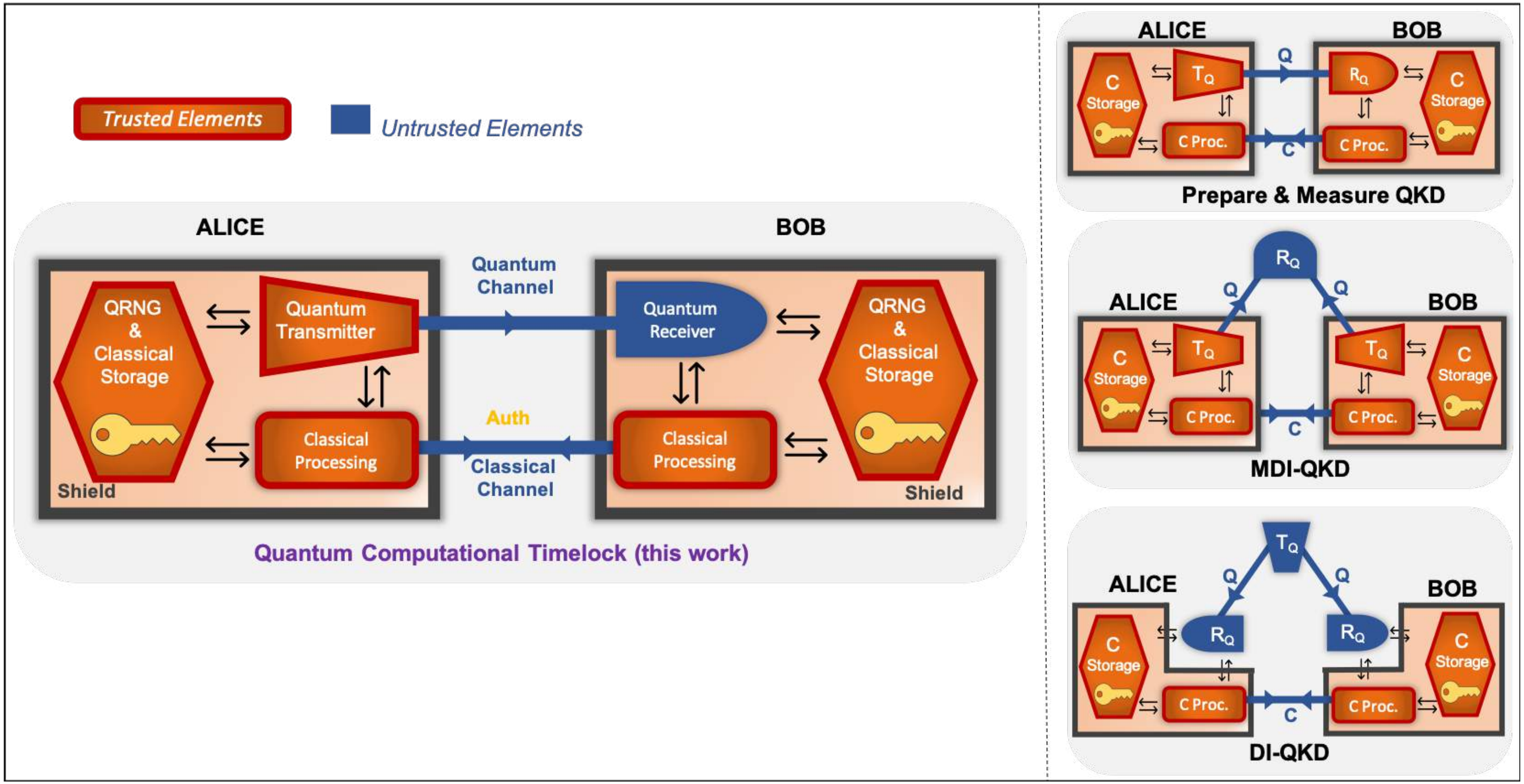
➔ Longer reach

➔ Higher rates than QKD

Significant ***performance gain for large n*** *(multimode regime)*

Challenge: find proof techniques valid against general attacks for multiple photons/ch use.

Another Advantage of QCT : Reduced Trust at Bob side



Conclusion and perspectives

Practical Quantum Cryptography Dilemma can be addressed, to a certain extent.
Beneficial to focus on a subset of mature enough questions

- Place Security – Performance Tradeoff at the heart on quantum crpto System Engineering
- Use of a restricted number of Trusted Hardware Plateforms for QKD classical processing

- **Explore new security models**
    - Trade-off between relaxed security assumptions and performance / trust gain that can be obtained
    - **Everlasting Security (ES)** relaxation ***highly relevant in practice***
    - **QCT** = (ES + Noisy Storage) => ***may bring significant extra gain***