INSTITUIÇÕES ASSOCIADAS

Continuous Variable QKD System

Gustavo Miranda Castilho dos Anjos

PhD Researcher

PTQCI

7 Mar 2025

OUTLINE

- ❑ FOUNDATIONS
- ❑ CV-QKD PROTOCOL
- ❑ SD-QKD NETWORK
- ❑ CHALLENGES
- ❑ OPPORTUNITIES

FOUNDATIONS

Quantum Physics

Every measure perturbs the system

No perturbation, no measure, no eavesdropper

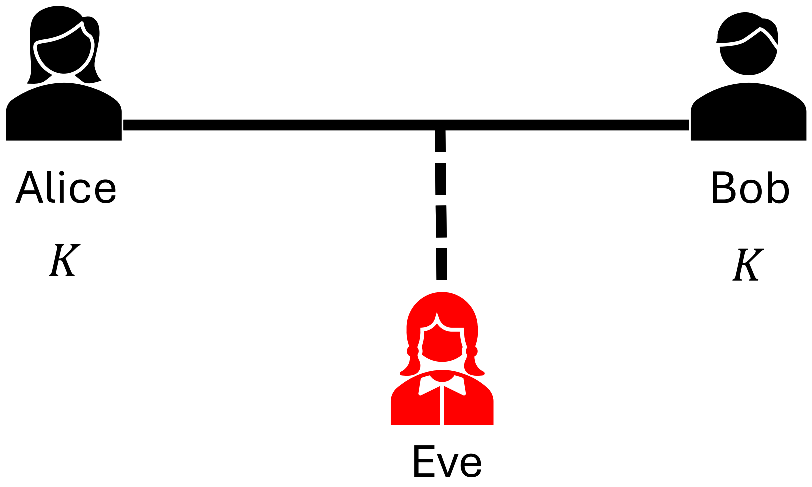
Secret key

Quantum systems can be used for **secret key distribution.**

QKD Protocol: Prepare and Measure

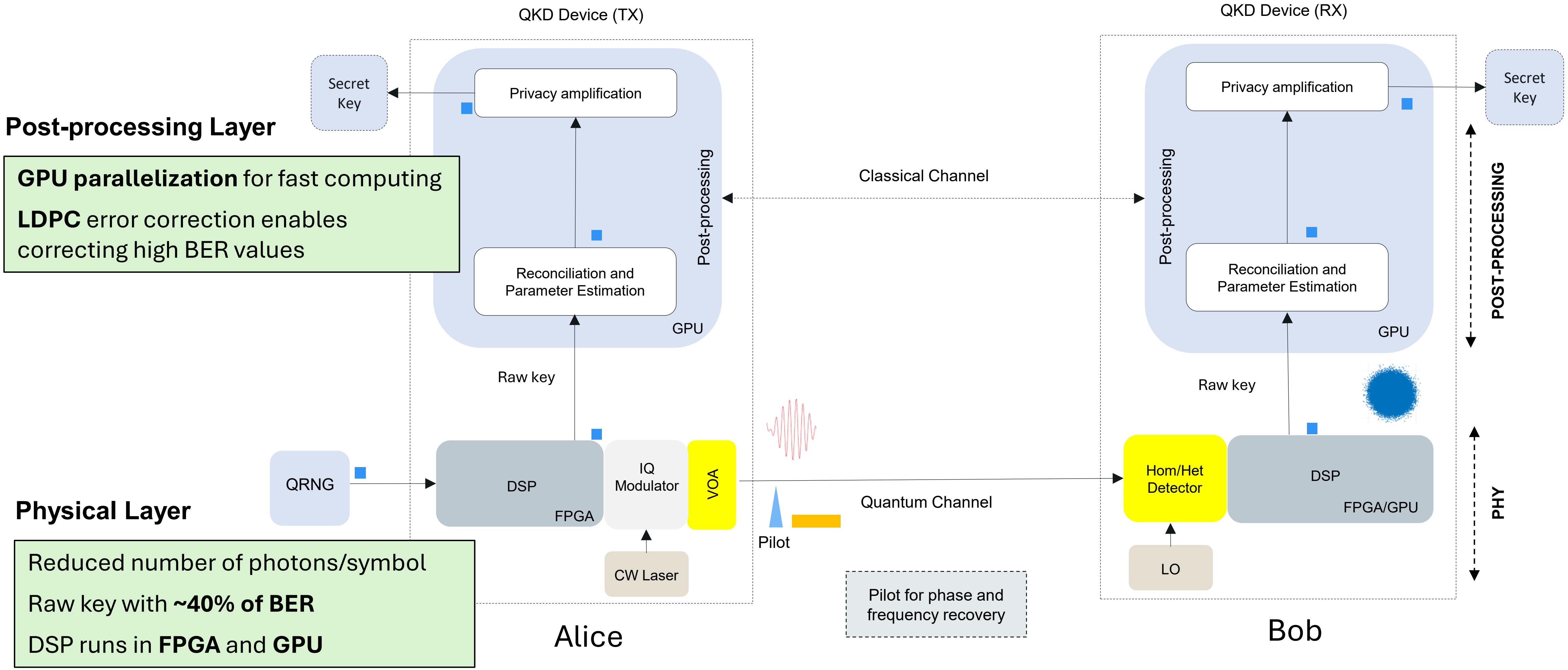
- □ Alice prepares and transmits the quantum key K;
- □ Bob measures the key and checks for Eve signatures;
- □ Key is dropped or reduced if Eve is present;

Eve cannot get the key without being detected



CV-QKD PROTOCOL

The key information (QRNG) is mapped in the phase and amplitude of a continuous wave laser source.



Post-processing Layer

GPU parallelization for fast computing

LDPC error correction enables correcting high BER values

Physical Layer

Reduced number of photons/symbol

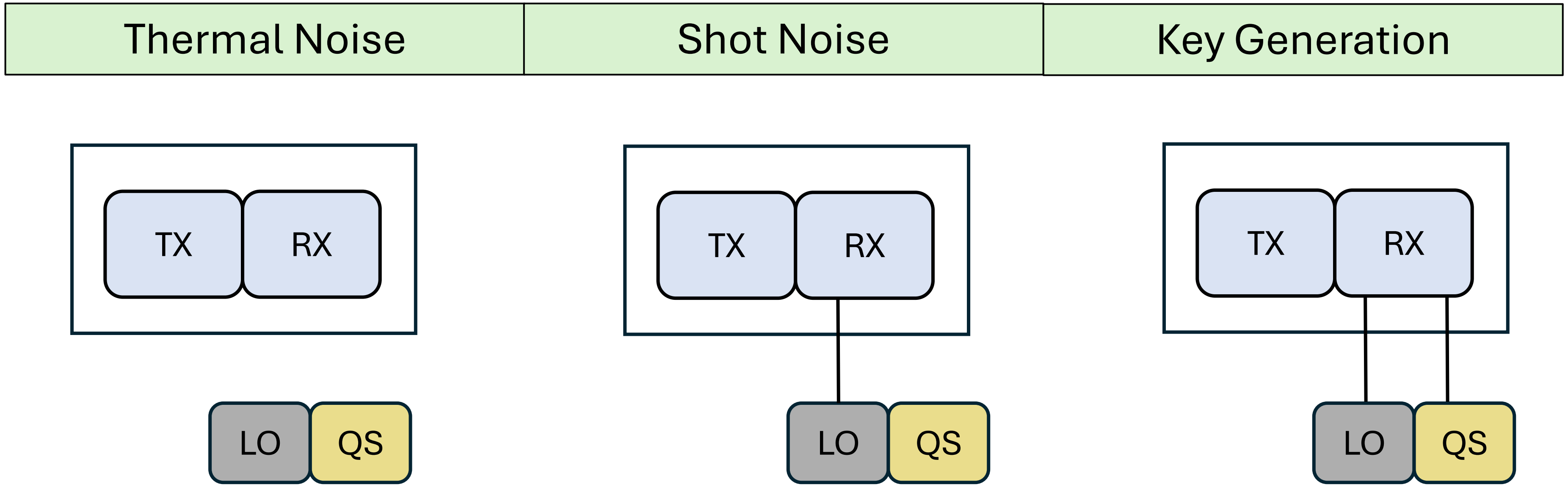
Raw key with **~40% of BER**

DSP runs in **FPGA** and **GPU**

CV-QKD PROTOCOL

Channel monitoring:

System generates keys 1/3 of the time, the other 2/3 for shot and thermal noise calibration.



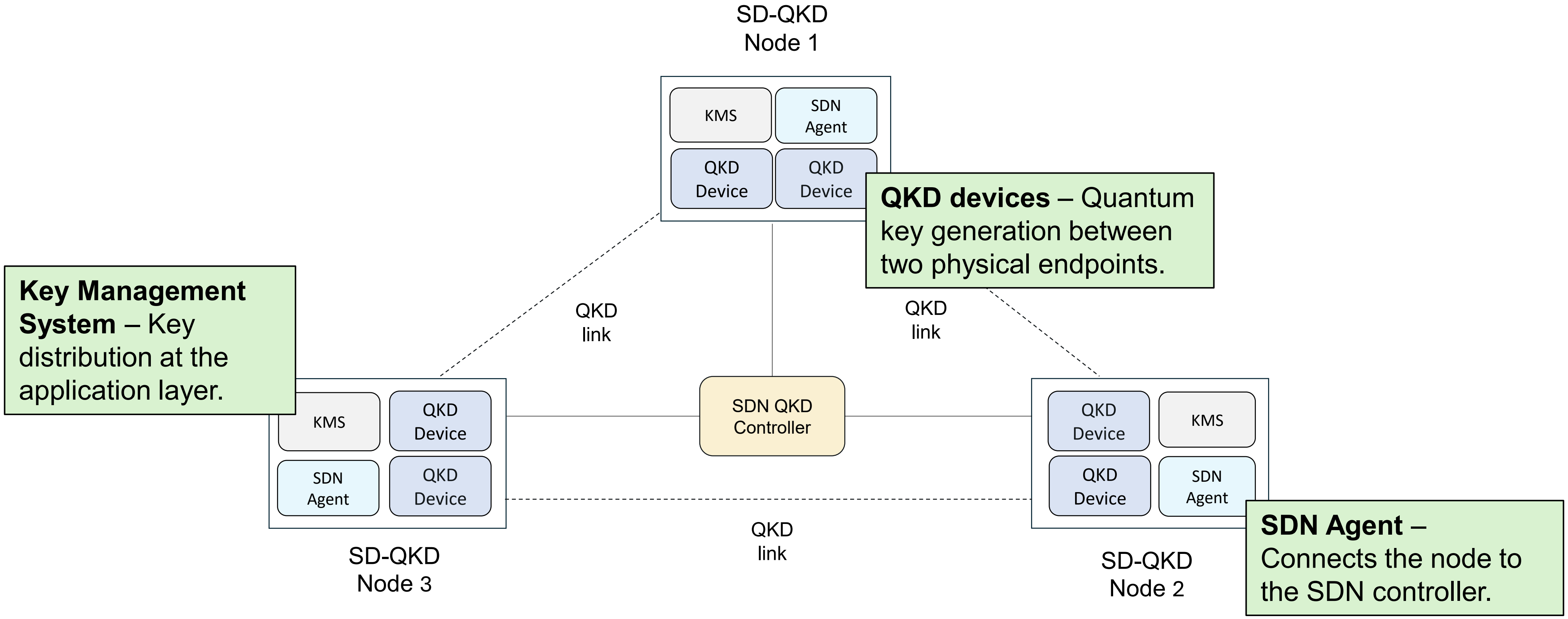
Calibration is essential to real-time quantification of trusted noise.

Eavesdropper signature in the form of excess noise.

SDN-QKD NETWORK

SDN enables centralized control, programming flexibility and scalability of QKD networks.

ETSI15 standard defines the concept of **Software Defined** (SD) – **QKD node**.



QKD devices – Quantum key generation between two physical endpoints.

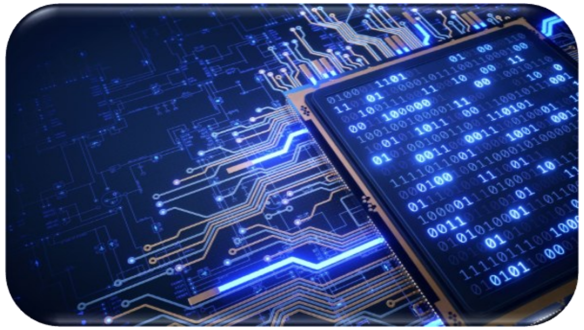
Key Management System – Key distribution at the application layer.

SDN Agent – Connects the node to the SDN controller.

CHALLENGES

Performance limitations

- Secret key rate lower than classical systems (Kbps)
- Distance limitation, 40-50 km (trusted nodes, repeaters)



Implementation complexity

- Faulty hardware implementation susceptible to attacks
- Heavy DSP chains to prepare and measure
- Computationally intensive LDPC reconciliation (QBER~40%)
- Photonics Integration Circuits (PICs) required
- Multidisciplinary topic, complex knowledge integration

OPPORTUNITIES

Promise of unbreakable cryptosystem

Provably secure ITS solution (bits)

Forward secrecy can be ensured

Protocol CV built on top of classical coherent systems

Part of the hardware and algorithms can be reused

Easy integration with classical systems

Emerging market, 50% annual growth