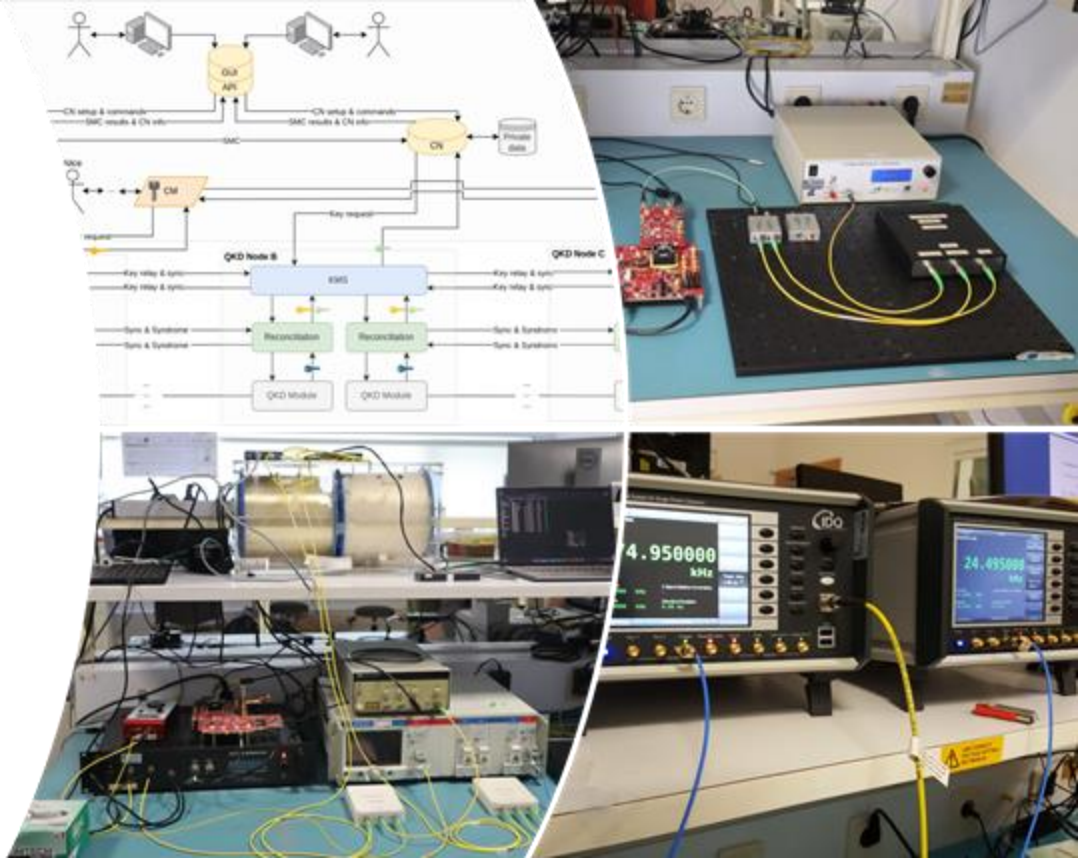
quantum communications

Quantum Key Reconciliation Application



Name(s): Diogo Marto, Vítor Santos, Tiago Pereira, Diogo Cobileac, Tiago Portugal
Research Team: Reconciliation
Role: 3rd Year project
UA Course: LEI - PI
Supervisors:
Armando Nolasco Pinto
Diogo Matos

INSTITUIÇÕES ASSOCIADAS

TÉCNICO LISBOA
universidade de aveiro
U C
Universidade de Coimbra
altice labs
NOKIA
UNIVERSIDADE BEIRA INTERIOR
U.PORTO
ISCTE IUL Instituto Universitário de Lisboa
IPL instituto politécnico de leiria

instituto de telecomunicações

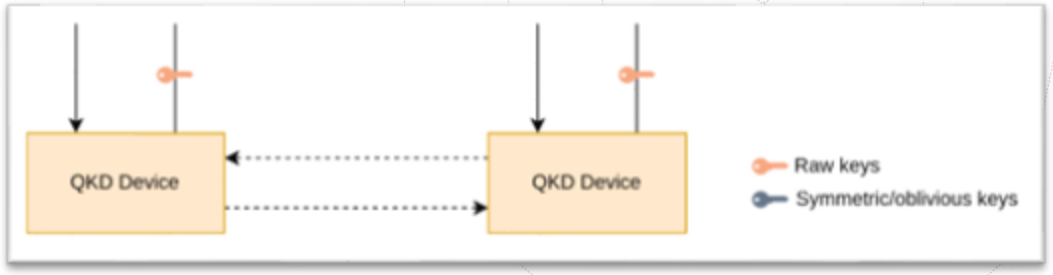
universidade de aveiro

Group Meeting
24 April

Motivation / The Problem Being Addressed

- Physical quantum key generation is not perfectly synchronized

- Raw keys must be corrected, securely transformed into either symmetric or oblivious keys.

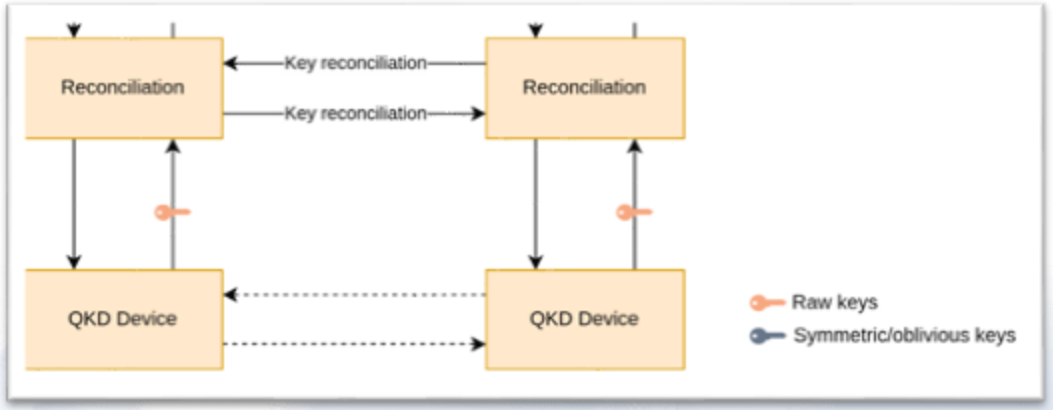


The Proposed Solution / Challenges

- Reconciliation using LDPC algorithm

- C++ implementation using the NetXpto framework to handle signal processing

- Raw key emulation and physical layer comms



Results – Next Steps

Test and compile to both Linux and Windows various previously developed solutions.

Terminal

File Edit View Search Terminal Help

```
##################################################
Rx System Console
##################################################
Local Machine Address: 127.0.0.1
Local Machine Receiving Port: 54001
Remote Machine Address: 127.0.0.1
Remote Machine Receiving Port: 54000
Bypass Parameter Estimation: TRUE
Total Number Of Input Bits: 32204
Estimated BER: 0
Speed (Bits/Sec): 2179.35
Rx: Number Of Calculated Sindromes: 74
Rx: Number Of Validated Sindromes: 72
Rx: Number Of No Matched Sindromes: 31
Rx: Percentage Of No Matched Sindromes: 41.8919
Rx: Number Of Validated Pairs: 36
Rx: Number Of Saved Pairs: 29
Rx: Number Of Discarded Pairs: 7
Rx: Percentage Of Discarded Pairs: 19.4444
```

Terminal

File Edit View Search Terminal Help

```
##################################################
Tx System Console
##################################################
Local Machine Address: 127.0.0.1
Local Machine Receiving Port: 54000
Remote Machine Address: 127.0.0.1
Remote Machine Receiving Port: 54001
Bypass Parameter Estimation: TRUE
Total Number Of Input Bits: 31472
Estimated BER: 0
Tx: Number Of Calculated Sindromes: 144
Tx: Number of Saved Pairs: 29
Tx: Number of Discarded Pairs: 6
Tx: Percentage Of Discarded Pairs: 17.1429
```

Results – Next Steps

- Develop and test an **emulator** capable of simulating raw material for binary and real data.
- Develop a **generic key provider server interface** alongside KMS team for both physical layer comms and KMS comms.
- **Improve upon** the previously developed solutions to obtain a fully connected, functional, multi-machine reconciliation layer.