QKD - is it worth it?

Mihai CARABAȘ

University POLITEHNICA Bucharest

Hack.lu

22nd-25th of October 2024

Context

- Quantum Computing breaking asymmetric encryption (Shor's algorithm)

- Why bother now? As qubits are far away? (store information decrypt later)

Context (2)

- QKD = Quantum Key Distribution (EuroQCI)

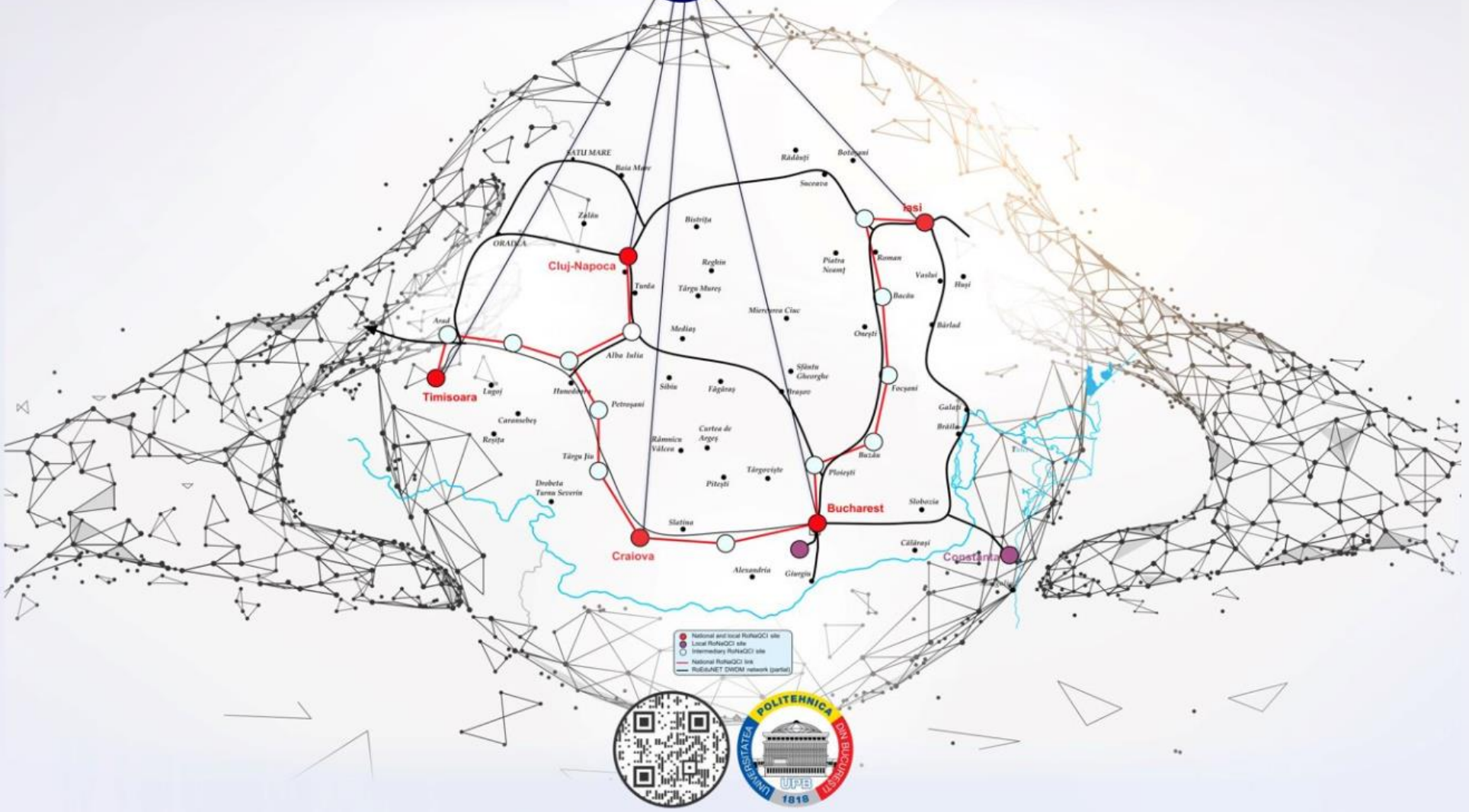
- Quantum-Resistant Cryptographic Algorithms (NIST)

QKD - is it worth?

- QKD = Quantum Key Distribution
  - +: Send encryption keys from one end to another using quantum mechanics properties
  - -: Cannot amplify the quantum channel, integration with classical communication, high costs

Romanian National
Quantum Communication Infrastructure

ronaqci



UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI
UPB
1818