Towards Quantum Internet

Evolution of Quantum Cryptography

Kari Seppänen

VTT Technical Research Centre of Finland Ltd

22 May, 2023 **VTT – beyond the obvious**

Outline

Topics covered today:

- Quantum key distribution (QKD)
- Quantum Internet
- Current State-of-the-Art
- QKD deployments

Quantum key distribution

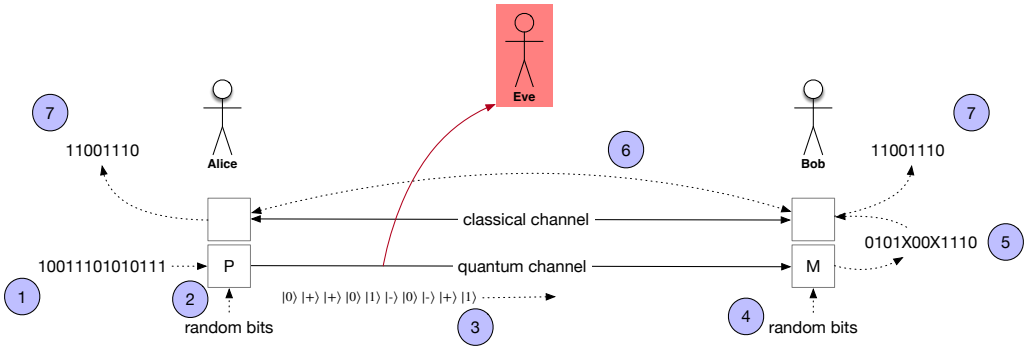
Quantum Information

A very short introduction

- Qubit (or quantum bit): basic unit of quantum information
  - linear combination of basic states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (note: $\alpha, \beta \in \mathbb{C}$)
- Quantum measurement
  - gives a single bit of information $\{0,1\}$, e.g., measuring in standard basis $\{|0\rangle, |1\rangle\}$, probability of getting 0 is $P(0) = |\alpha|^2$, and $P(1) = |\beta|^2$ (note: $|\alpha|^2 + |\beta|^2 = 1$)
  - measurement alters the state of qubit, if result is 0 then state is $|0\rangle$
- No-cloning theorem: it is impossible to create an independent and identical copy of an arbitrary unknown quantum state
- Quantum entanglement
  - quantum state of each particle cannot be described independently of the quantum state of the other particle(s)
  - the outcome of the measurement on one qubit will always be correlated to the measurement on the other qubit

Prepare and measure QKD

BB84 protocol



Prepare and measure QKD

BB84 protocol

1. Alice generates random bit-stream b (preferably with QRNG)
2. Alice generates single photon and encodes each bit b_i using randomly chosen basis
   - e.g. random bit = 0 $\Rightarrow 0 \mapsto |0\rangle, 1 \mapsto |1\rangle$ and random bit = 1 $\Rightarrow 0 \mapsto |+\rangle, 1 \mapsto |-\rangle$
   - note: $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
3. Generated qubits are transfered to Bob via quantum channel
4. Bob selects measurement basis randomly
5. Measurement results are feed to key distillation
6. In key distillation, Alice and Bob agree which bits can be used, perform error correction, and privacy amplification
   - some bits are used for error rate estimation to detect Eve
7. Resulting key can be used for encryption

Prepare and measure QKD

BB84 protocol

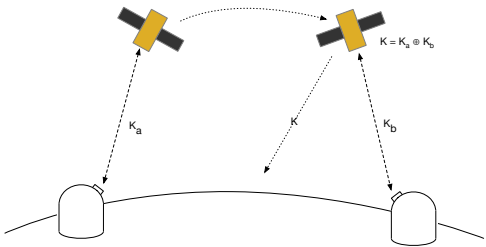
Eavesdropper Eve does not know which basis Alice has used to encode qubit

- Measurement gives only one bit of information and does not reveal if Eve selected correct basis, e.g., measuring $|+\rangle$ in standard basis will give $P(0) = P(1) = \frac{1}{2}$
- Measurement cannot be repeated as 1st measurement alters the qubit state
- Eve cannot clone qubit (no-cloning) to perform multiple measurements or to send Bob a copy of the original qubit
- $\Rightarrow$ if Eve captures Alice's qubit, measures it, and perpares a new qubit for Bob, there will be errors that can be detected

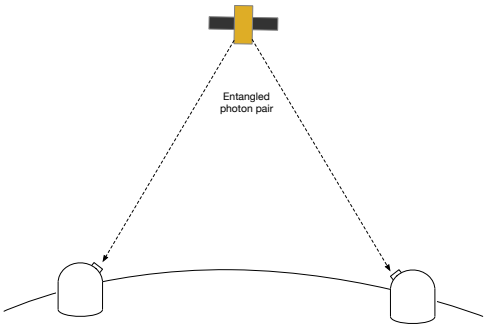
Alternative QKD protocols

- Entanglement based QKD (E92)
  - Utilizes entangled photon pairs – if Alice and Bob make measurement in the same basis they get 100% same result
  - Alice and Bob select measurement base randomly ($\{0, \pi/8, \pi/4\}$, $\{-\pi/8, 0, \pi/8\}$ respectively)
  - After measurements, bases are announced and Alice and Bob know what bits they can use for secret key and rest can be used to detect Eve
- (Measurement) Device Independent ((M)DI-)QKD, Twin-Field (TF-)QKD
  - Alice and Bob both send weak signals to measurement device where they interfere
  - Measurement results can be made public as only Alice and Bob know what bases they have used
- Continuous Variable (CV-)QKD
  - Utilizes coherent optical transmitters, weak pulse, bases e.g. AM & PM

Satellite QKD



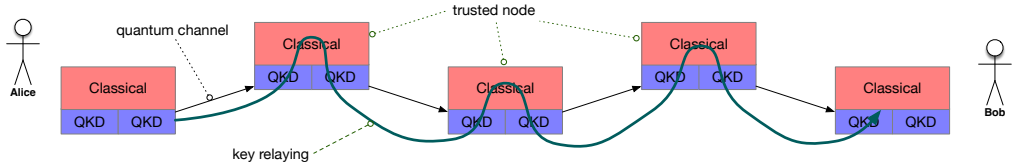
Typical LEO QKD concept



GEO QKD with quantum entanglement(e.g. HISPASAT led CARAMUEL)

Challenges

Short-comings of current systems



- Validation, operability, etc.
- Point-to-point quantum channels, max range ~50-100+ km
  - Key relaying is needed for QKD networks & longer ranges
  - Long-term solution: quantum repeaters

- Implementation (side-channels)
- Statistical single-photon sources
  - Reduces efficiency, security risk
  - Practical deterministic single-photon sources
- Detectors
  - SPAD efficiency, noise
  - SNSPD are still bit unpractical

Quantum Internet

Quantum Internet

The quantum internet is a network of quantum computers that will someday send, compute, and receive information encoded in quantum states. The quantum internet will not replace the modern or “classical” internet; instead, it will provide new functionalities such as quantum cryptography and quantum cloud computing.

Quantum Internet

Development steps (Wehner2018)

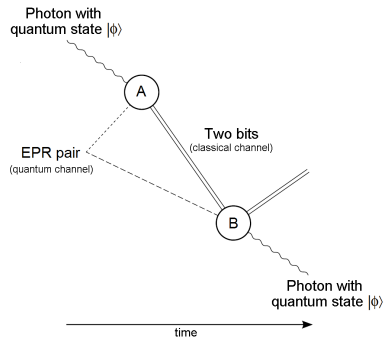
1. Basic QKD is possible
2. End users can prepare and measure the qubits
3. Quantum repeaters and entanglement distribution
4. Quantum repeaters gain the capability of storing and manipulating entangled qubits in the quantum memories
5. Quantum repeaters can perform error correction
6. Distributed quantum computing relying on more qubits

Quantum cryptography beyond QKD

- Everlasting security
  - QKD, limited-quantum-storage protocols
- Quantum functionalities
  - encryption of quantum messages in the information-theoretic, entropic and computational settings
  - quantum secret sharing
  - multi-party quantum computation
  - authentication of quantum messages
  - two-party secure function evaluation
  - quantum anonymous transmission
  - quantum one-time programs
  - quantum homomorphic encryption
- Key recycling
- Quantum uncloneability
  - uncloneable encryption, quantum copy-protection and revocable time-release encryption
- Leakage resilience using quantum techniques
- Quantum cryptanalysis
- Merkle puzzles in a quantum world

Quantum repeaters

- Based on quantum teleportation
  - Sender and receiver share EPR pair
  - Sender prepares quantum state $|\phi\rangle$ and performs Bell State Measurement (BSM) (erases states at the sending end)
  - Measurement result (two bits) is sent to receiver who now knows what measurement to perform to replicate $|\phi\rangle$
- Linking multiple entangled pairs via successive pair-wise BSM for repeater chains



GFDL, https://commons.wikimedia.org/w/index.php?curid=116768547

Where are we today

Technologies

Some examples

- Quantum entanglement
  - Sources are commercially available
  - *“Qubit teleportation between non-neighbouring nodes in a quantum network”*, 2022, https://doi.org/10.1038/s41586-022-04697-y
  - Entanglement distribution in Qunnect’s GothamQ spanning from Brooklyn to Manhattan, 2023
    - Quantum entanglement as a service
- Quantum repeaters
  - Plans to demonstrate repeaters in QKD testbeds within couple of next years
- Quantum memory
  - Qunnect: first sale of commercial, room temperature quantum memory 2021
- Quantum network:
  - QuTech: first entanglement-based quantum network connecting three nodes 2021

QKD deployments

EuroQCI initiative

European Quantum Communication Infrastructure

Joint agreement signed by all EU countries for secure QCI spanning whole EU

- QKD technology developed in H2020 projects
  - OpenQKD, 8TAVO, Civiq etc.
- 2023-2025: national testbeds, QKD technology ecosystem
- 2025-2027: cross-border connections incl. satellite,
  - Satellite component in cooperation with ESA
- Test and certification system
- -2030: operational EU wide QKD network

NaQCI.fi

National Quantum Communication Infrastructure in Finland

National EuroQCI project in Finland, started Jan 2023

- Cinia, CSC, Erillisverkot, and VTT (coordinator)
- Public demo network at Helsinki area
  - Demo events, hands on workshops, development and testing platform
- Governmental test network
  - Southern Finland, later links to Estonia and Sweden
- VTT's QKD development system
  - DV-QKD system built from components; own software
- Goals
  - Prepare for next EuroQCI phases
  - Educate staff to design, deploy and operate QKD networks
  - Reach out for potential users and developers

Rest of the World

- UK: commercial trial by BT & Toshiba, satellite QKD
- Switzerland: early adopter, banking, voting
- South-Korea: large scale test network, mobile network infra, industry
- Japan: Tokyo QKD network since 2010, plans for global network
- USA: focus on quantum entanglement networks (this far, QKD is the only practical application)
- Singapore: terrestrial network 2020, plans for global satellite QKD
- China: 2000 km QKD key-relay network Beijing–Shanghai, satellite QKD

Summary

Summary

- QKD promises to provide unbreachable security
  - Commercial devices are available but with limitations
  - Existing deployments worldwide
- QKD development will converge with Quantum Internet
- Many Quantum Internet building blocks already demonstrated
  - Some technologies are moving out from laboratories
- Quantum Internet will enable many new quantum cryptography schemes
- Are we on the edge of rapid development phase?

VTT

beyond
the obvious

Kari Seppänen
Email: kari.seppanen@vtt.fi
Twitter:
LinkedIn: https://fi.linkedin.com/in/kariseppanen