Secure communications in quantum networks

Eleni Diamanti
LIP6, CNRS, Sorbonne Université
Paris Centre for Quantum Technologies
Quantum communication is the art of transferring quantum information between distant locations

Encoding on properties of quantum states of light
Propagation in optical fibre or free-space channels
Information processing in network nodes (processors, sensors, memories)

Security
Untrusted network users, devices, nodes

Efficiency
Optimal use of communication resources

Applications
Demonstrate provable quantum advantage in security and efficiency for communication and information processing tasks
Network development stages and applications

Functionalities and applications

- Prepare-and-measure QKD, coin flipping, oblivious transfer, position-based cryptography, digital signatures
- Device-independent QKD, certification and verification, secret sharing, conference key agreement, anonymous communication
- Quantum money, secure multiparty computing, leader election
- Blind, delegated and distributed quantum computing, distributed quantum sensing, byzantine agreement

Adapted from S. Wehner et al., Science 2018 & G. Moody et al., J. Phys. Photon. 2022
Modern cryptography relies on assumptions on the computational power of an eavesdropper → symmetric, asymmetric, post-quantum cryptography

Quantum key distribution allows for exchange of sensitive data between two trusted parties with information-theoretic, long-term security guaranteed against an all-powerful eavesdropper → combined with suitable authentication and message encryption algorithms

Key information is encoded on photonic carriers

Analysis of errors due to Eve’s perturbation leads to extraction of secret key
A single-photon QKD protocol – BB84

- **No cloning theorem:** Eve cannot copy the states sent by Alice
- **Heisenberg’s uncertainty principle:** Eve cannot measure in both bases
- **Device independence:** If Alice and Bob share entangled photons less assumptions on devices
- **Practical security:** Deviation from security proof may lead to side-channel attacks
QKD in practice

Performance of **point-to-point, prepare-and-measure** fibre-optic QKD systems


Fundamental **limits in rate and range**

Security: \[ \frac{1}{2} \| \rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E \|_1 \leq \varepsilon \text{ for any } \rho_{A^n B^n E} \]
Discrete and continuous variable QKD

<table>
<thead>
<tr>
<th>Light is:</th>
<th>Discrete Photons</th>
<th>Continuous Wave</th>
</tr>
</thead>
<tbody>
<tr>
<td>We want to know:</td>
<td>their Number &amp; Coherence</td>
<td>its Amplitude &amp; Phase (polar) its Quadratures $X$ &amp; $P$ (cartesian)</td>
</tr>
<tr>
<td>We describe it with:</td>
<td>Density matrix $\rho_{n,m}$</td>
<td>Wigner function $W(X,P)$</td>
</tr>
<tr>
<td>We measure it by:</td>
<td>Counting: APD, VLPC, TES...</td>
<td>Demodulating: Homodyne Detection</td>
</tr>
<tr>
<td>« Simple » States</td>
<td>Fock States</td>
<td>Gaussian States</td>
</tr>
</tbody>
</table>

BB84, Decoy state, COW, DPS, MDI

One or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection, MDI

Coherent state continuous-variable QKD

Single (homodyne) or double (heterodyne) quadrature detection
Trusted (calibrated) noise

Composable, finite size security proof for Gaussian modulation
Adapted to arbitrary discrete constellations at asymptotic limit

A. Denys et al., Quantum 2021
High-rate network-integrated QKD

Compatibility with technology and digital signal processing techniques used in coherent telecom systems

Probabilistic constellation shaped 64 and 256-QAM, dual pol., Nyquist pulses, 50% QPSK pilots, 400 Mbaud, 10 kHz linewidth

With 256-QAM, secret key rate

- 92 Mbit/s @ 9.5 km
- 24 Mbit/s @ 25 km

F. Roumestan et al., OFC & ECOC 2021, 2022, arXiv 2207.11702
Photonic-integrated QKD

**Si receiver photonic chips** from C2N and CEA-LETI

**InP transmitter chips** from HHI-Fraunhofer

---

**Si-PIC CV-QKD receiver platform**

Y. Piétri et al., OFC 2023
Quantum advantage for advanced protocols

Key distribution is central primitive in the **trusted** two-party security model. In other configurations many more **functionalities**

**Unforgeable quantum money**

Wiesner’s original idea (1973) of using the uncertainty principle for security. But needs quantum verification and is not robust to imperfections. Was considered impossible to implement.

New protocol with **classical verification** and ‘BB84’ states. Based on **challenge questions**

\[ S_{pair} = \{ |0, +\rangle, |0, -\rangle, |1, +\rangle, |1, -\rangle, |+, 0\rangle, |+, 1\rangle, |-, 0\rangle, |-, 1\rangle \} \]
Rigorously satisfies security condition for unforgeability
→ quantum advantage with trusted terminal

General security framework for weak coherent states and anticipating quantum memory
→ minimize losses and errors for both trusted and untrusted terminal

Quantum weak coin flipping

Allows two distrustful parties to agree on a random bit, whose value should not be biased.

Classical \rightarrow \text{computational assumptions, quantum} \rightarrow \text{information-theoretic security but fundamental lower bound on bias}

In principle arbitrarily close to zero for weak protocol, where Alice and Bob have a preferred outcome.

Photon number entanglement with heralded single photons, conditional verification step

Quantum advantage in the form of cheat sensitivity maintained over a few kilometres

S. Neves et al., Nature Commun. 2023
Multipartite entanglement verification and applications

Proof-of-principle verification of multipartite entanglement in the presence of dishonest parties


\[ |\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle) \]

Requires very high performance resources
Limited loss tolerance

Application to anonymous message transmission and electronic voting
Verification phase guarantees anonymity and privacy

To counter inherent range limitation due to optical fiber loss → terrestrial and satellite-based networks

Practical testbed deployment allows for interoperability, maturity, network integration aspects and topology, use case benchmarking, standardization of interfaces

Data centre storage and interconnection, protection and resilience of critical infrastructures, governmental communications, finance, telecom operators, medical file transfer

Y.-A. Chen et al., Nature 2021

Trusted node networks
Alice-R: key1, R-Bob: key2, R: key1 ⊕ key2
→ Bob: key2 ⊕ (key1 ⊕ key2) = key1
Benchmarking with commercial systems
IDQ XGR QKD systems
Thales Mistral encryptors

Deployment of quantum memory-based link
Cold atom technology with record high storage-and-retrieval efficiency

Deployment of CV-QKD integrating system-on-chip technology and of entanglement distribution
Feasibility studies for space-based quantum networks

They alleviate the need for long chains of trusted nodes or quantum repeaters
They serve more use cases: remote, isolated or inaccessible locations
Terrestrial and space networks work together and can be fallback options

Downlink channel with turbulence
Probability distribution of transmission efficiency
Payload characteristics of Micius:
pointing error 1 µrad, divergence angle 10 µrad
Ground station characteristics of Matera Laser Ranging Observatory: telescope diameter 1.5 m

Security analysis for a fluctuating channel → fading introduces additional noise
Trade-off between binning of data to reduce variance and finite-size effects

Refined analysis of fibre coupling with adaptive optic system → correcting up to 15 orders optimal for both CV and DV-QKD, for LEO at almost all conditions

D. Dequal et al., npj Quant. Info. 2021
V. Marulanda Acosta et al., arXiv 2111.06747
Analysis of entanglement-based scenario

Trade-offs between visibility time, losses, divergence, pointing, telescope size, atmospheric turbulence, detector efficiency,…

Importance of long simulation duration

L. de Forges de Parny et al., Commun. Phys. 2023
Conclusion and perspectives

Quantum communication networks will be part of the future quantum-safe communication infrastructure.

Such an infrastructure can address a range of use cases with high security requirements in multiple configurations.

The quantum communication toolbox is rich and increasingly advanced.

Quantum technologies need to integrate into standard network and cryptographic practices to materialize the global quantum network vision.

Thank you!