Feasibility of satellite-to-ground continuous-variable quantum key distribution

Eleni Diamanti
LIP6, CNRS, Sorbonne University

with Daniele Dequal, ASI; Luis Trigo Vidarte, Sorbonne U. & IOGS; Victor Roman Rodriguez, Sorbonne U. & Thales Alenia Space; Anthony Leverrier, INRIA Paris; Pino Vallone, Paolo Villoresi, U. Padova

COAT Workshop, Châtillon, France
2-3 December 2019
Quantum communication

The art of transferring quantum information between distant nodes

Point-to-point secure communication: Quantum Key Distribution

Encoding in properties of quantum states of light

Provides a future-proof, unconditionally secure solution to the key distribution problem for secure message exchange between two trusted parties
## Discrete and continuous variable QKD

<table>
<thead>
<tr>
<th></th>
<th>Discrete variables</th>
<th>Continuous variables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key encoding</strong></td>
<td>Photon polarization, phase, time arrival</td>
<td>Electromagnetic field quadratures</td>
</tr>
<tr>
<td><strong>Detection</strong></td>
<td>Single-photon</td>
<td>Coherent (homodyne/heterodyne)</td>
</tr>
<tr>
<td><strong>Post processing</strong></td>
<td>Key readily available</td>
<td>Complex error correction</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>General attacks, finite-size, side channels</td>
<td>General attacks, finite-size, side channels</td>
</tr>
</tbody>
</table>

BB84, Decoy state, Coherent One Way, Differential Phase Shift, Measurement Device Independent

CV-QKD (one or two-way, Gaussian or discrete modulation, coherent or squeezed states, post selection)
Exploits standard telecom technology

V. Scarani et al, Rev. Mod. Phys. 2009
ED and A. Leverrier, Entropy 2015
State of the art of point-to-point fibre-optic QKD

Inherent range limitation due to optical fiber loss
Quantum networks and Satellite communications

Overcoming channel losses

Trusted node networks

SECOQC QKD network, 2008
South Africa, Swiss, Tokyo, UK QC Hub networks
China 2000 km, 32-node network

OpenQKD – EU Quantum Communication Infrastructure with terrestrial and space segments

LEO Micius: downlink DV-QKD, uplink quantum teleportation, entanglement distribution, videoconferencing across the globe in trusted node-satellite model
Coherent state CV-QKD and model assumptions

**Gaussian modulation**, QPSK, QAM,…

**Heterodyne detection, trusted noise**

Shot noise limited, low noise, high bandwidth

Additional model assumptions:

**Downlink, ground station with 1.5 telescope aperture**

**Circular orbit passing at station zenith**

**Micius performance for pointing and tracking, 3 dB fibre coupling losses**

The excess noise $\xi$ is attributed to the attacker (Eve) – Eve can control $T$ as well

Pilots for phase recovery, narrow linewidth lasers

Classical post-processing steps
Channel model and effect of fading

\[ r: \text{Pointing error + beam wandering} \]
\[ W: \text{Divergence + beam spreading} \]

Main challenge:
Security analysis for a fluctuating channel
Fading introduces an additional noise source

\[ \langle K \rangle = \beta \langle I_{AB} \rangle - f(\langle \Gamma \rangle) \]
\[ \xi_{\text{fading}} = \text{Var} \left( \sqrt{\tau} \right) V_A \]
\[ \xi_{\text{total}} = \xi_{\text{fixed}} + \xi_{\text{fading}} \]

Channel division

To reduce variance of the fading process ➔
Classical beacon to estimate transmission efficiency
‘Binning’ of data according to transmission efficiency, security analysis for each group

![Graph showing Key Rate vs Satellite Perigee](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Symbol</th>
<th>Reference value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pointing error</td>
<td>( \theta_{\text{point}} )</td>
<td>1 ( \mu ) rad</td>
</tr>
<tr>
<td>Divergence angle</td>
<td>( \theta_{\text{div}} )</td>
<td>10 ( \mu ) rad</td>
</tr>
<tr>
<td>Fixed attenuation</td>
<td>( \tau_{\text{fix}} )</td>
<td>5.8 dB</td>
</tr>
<tr>
<td>Electronic noise</td>
<td>( \nu_{\text{el}} )</td>
<td>10% S.N.U.</td>
</tr>
<tr>
<td>Detection efficiency</td>
<td>( \eta )</td>
<td>0.4</td>
</tr>
<tr>
<td>Fixed excess noise</td>
<td>( \xi_{\text{fix}} )</td>
<td>1-5% S.N.U.</td>
</tr>
<tr>
<td>Reference laser power</td>
<td>( P_{\text{ref}} )</td>
<td>100 mW</td>
</tr>
<tr>
<td>Reconciliation efficiency</td>
<td>( \beta )</td>
<td>0.95</td>
</tr>
<tr>
<td>Transmission frequency</td>
<td>( f_{\text{TX}} )</td>
<td>1 GHz</td>
</tr>
</tbody>
</table>
Finite size effects are related to **statistical uncertainties** in parameter estimation.

**Trade-off between finite size and fading noise** in channel division.
Quantum satellite communications will be part of the future quantum-safe infrastructure

CV-QKD is feasible for LEO with realistic assumptions, and provides high throughput

Finite-size effects prevent key generation at higher orbits → increasing transmission rate and using multiple passages may help

Next steps:
Study of inclined orbits, adaptive optics, lab validation, realistic architecture with specific ground stations, measurement device independent configuration