Pushing Quantum Optical Receiver Technology Towards Satellite-Mediated Global Quantum Key Distribution

UNIVERSITY OF WATERLOO

Brendon Higgins, Jean-Philippe Bourgoin, Nikolay Gigov, Evan Meyer-Scott, Zhizhong Yan, and Thomas Jennewein

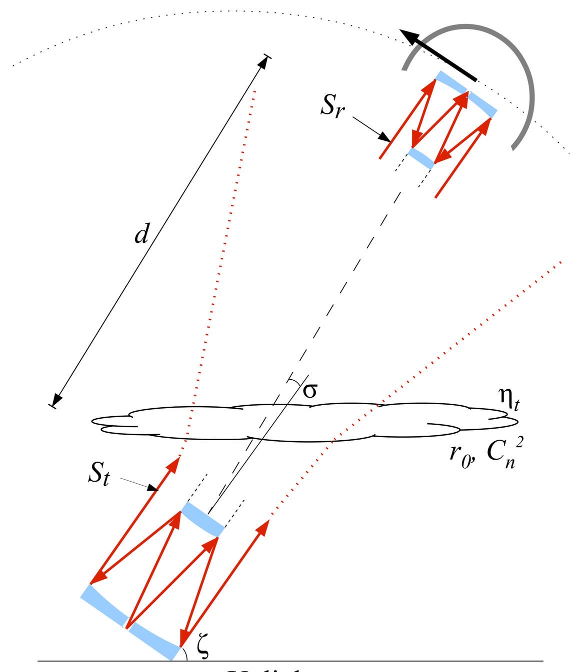
Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada

IQC Institute for Quantum Computing

Introduction: Ground–Satellite Quantum Key Distribution

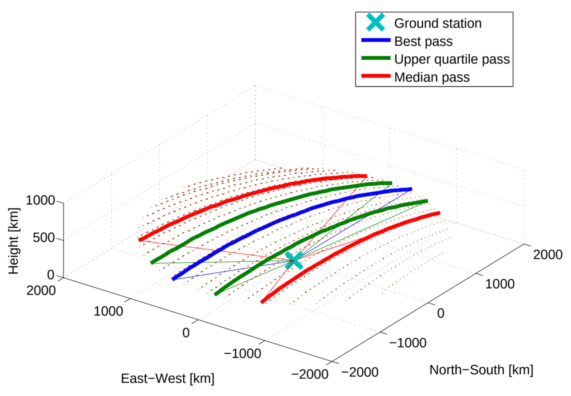
- Transmission losses limit terrestrial QKD and quantum science experiments to distances of order 400 km [1, 2].
- To **overcome terrestrial limits**: Use a *satellite* as a trusted node, making a **global** QKD network.
- Satellite QKD is feasible, either as a quantum **downlink** or an **uplink** [3, 4].
- Uplink (receiver onboard satellite) is less efficient than downlink, but has several advantages:
  - **Simpler** satellite design
  - Lower power, computational, and memory requirements
  - **Flexibility** with the quantum source
  - Allowing **wider scope** for science experiments
- Canadian Space Agency studies culminated in the *Quantum EncrYption and Science Satellite (QEYSSat)* proposal:
  - A single **microsatellite** in noon-midnight low Earth orbit, $h \approx 600$ km.
  - **Uplink**, polarization-encoded single photons, $\lambda \approx 800$ nm.
  - Receiver telescope diameter $D_r \approx 40$ cm.
- Here we outline recent and ongoing laboratory studies towards demonstrating the feasibility of quantum receiver technology for ground–satellite links. We:
  1. Analyze the optical *link efficiency*
  2. Develop and analyze a *quantum-signal*-based polarization alignment protocol
  3. Demonstrate **full QKD** in the *high-loss* regime of a satellite
  4. Investigate the possibility of QKD via *diffusive-screen reflection*
  5. Pursue QKD demonstrations with a **moving receiver**

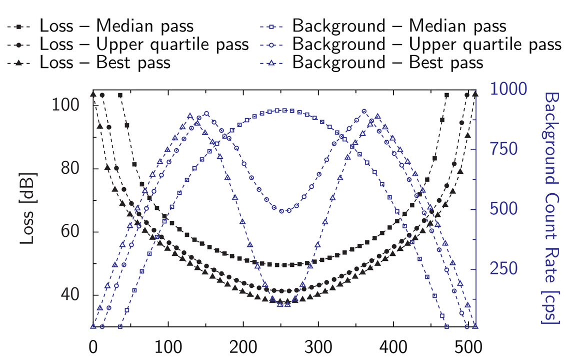
1. Comprehensive Ground–Satellite Link Analysis



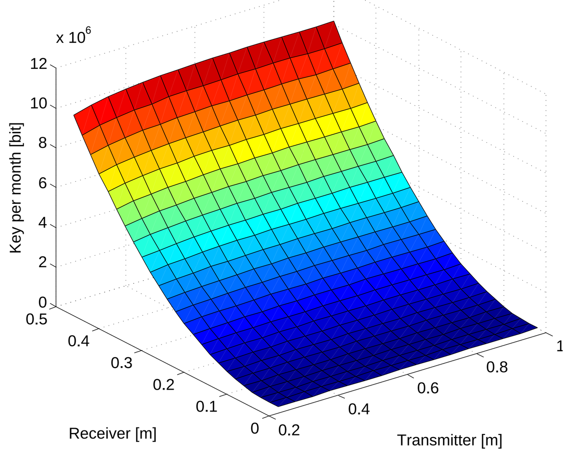
We have developed a **comprehensive** ground–satellite *quantum link model* [4] that takes into account:

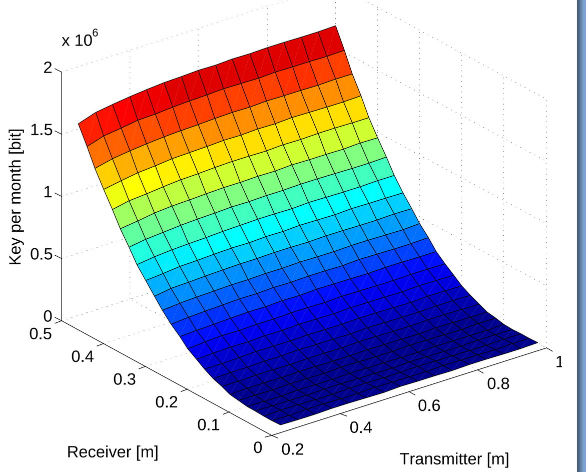
- *Entangled* and *weak coherent pulse* quantum states
- Transmission *wavelength* and pulse frequency
- Transmitter and receiver *telescope sizes* and fields of view
- Up- or down-link propagation
- **Realistic** orbital data
- Atmospheric transmittance and *turbulence*
- Diffraction, optical losses, and pointing error
- Ground site location and **local light pollution**
- Detector dark counts, Earth's thermal radiation, and reflected moonlight
- *Detector inefficiencies* and cloud cover





Top-left: Schematic of the up-link scenario to an orbiting satellite. **Left:** Example orbit passes over a ground station: best (blue), upper-quartile (green), and median (red) passes shown. **Bottom-left:** Determined loss and background (red) for an uplink for each pass. **Bottom-centre:** Accumulated secure key length after one month of operation with a 300 MHz weak coherent pulse source, for various transmitter and receiver telescope sizes. **Bottom-right:** Accumulated secure key length after one month of operation with a 100 MHz entangled pair source.

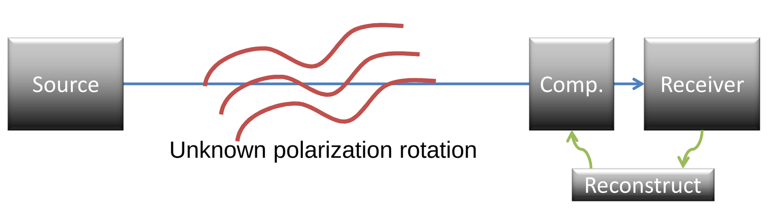




2. Polarization Alignment Based On QKD Signals

High-bandwidth BB84/BBM92 relies on **accurate polarization alignment** of transmitter and receiver, which birefringence and relative orientation will perturb. Classical solutions may be sufficient, but is it possible to align well *only* with the **quantum** signal?

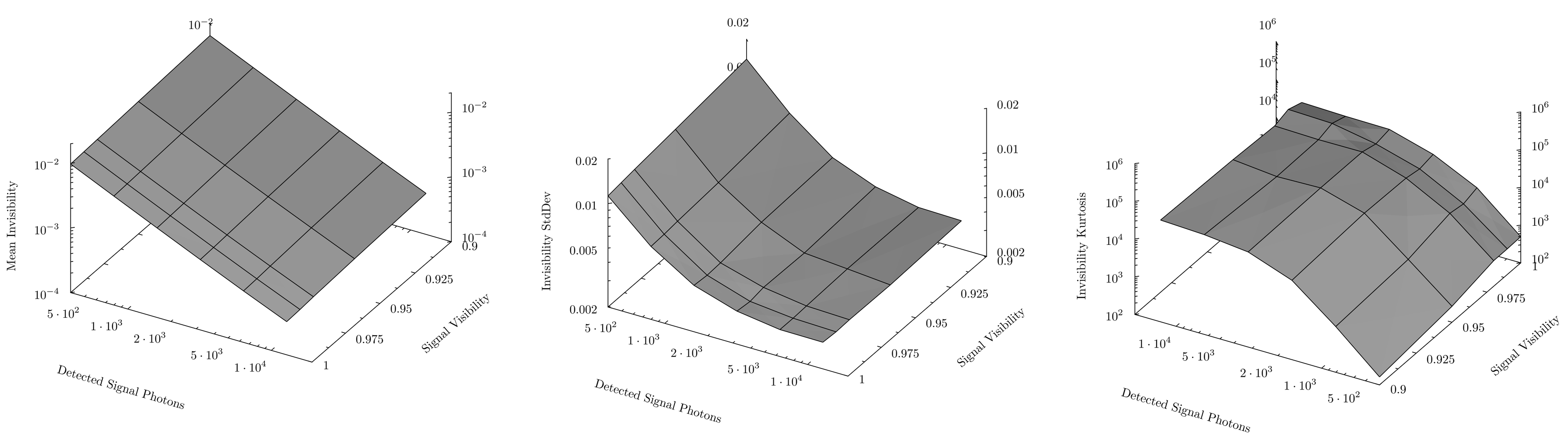
We've developed and assessed the performance of a straightforward *automated polarization alignment protocol*:



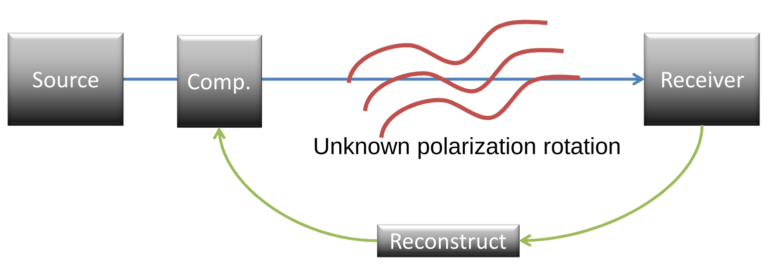
1. A set of known states are sent to the receiver (these can be e.g. standard QKD states)
2. The receiver collects complete-basis* measurement stats.
3. A compensation unitary is determined and applied, via a quarter-, half-, quarter-wave plate triplet

*Conveniently, the requisite change of basis can be achieved using the same wave plate triplet.

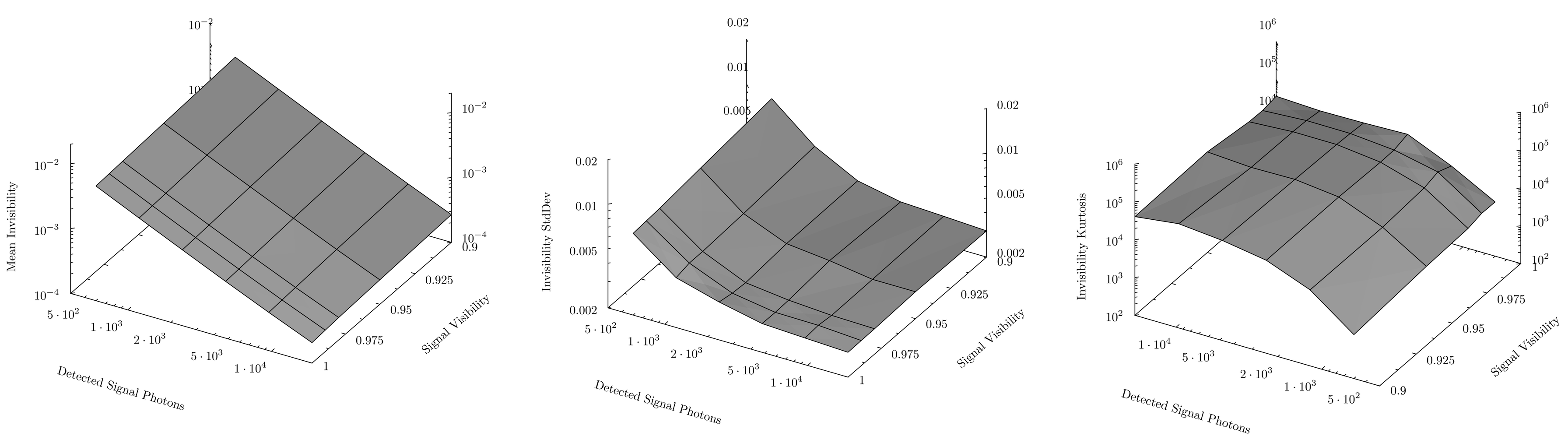
We perform 2^{24} **Monte-Carlo simulations** of this protocol, quantifying performance by visibility reduction:



Above: Invisibility of QKD states after compensation, mean (left), std. dev. (centre), and kurtosis (right).



Moreover, we can **reverse** the protocol by considering measurements as *post-selections*. Here the source produces complete-basis states, the receiver measures in QKD states, and compensation is applied just before leaving the source.

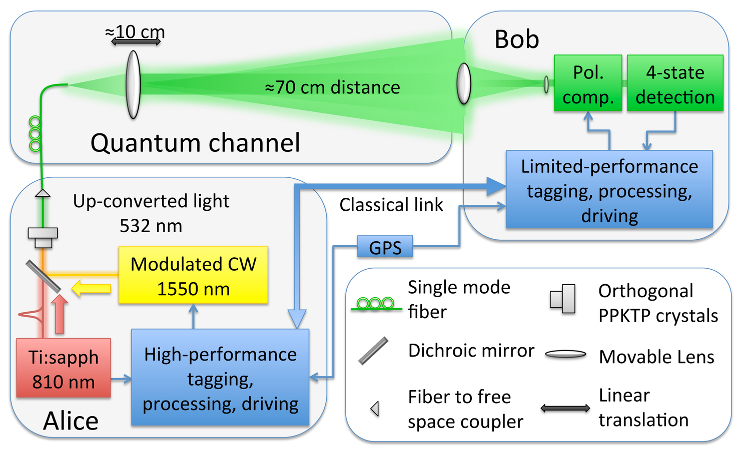


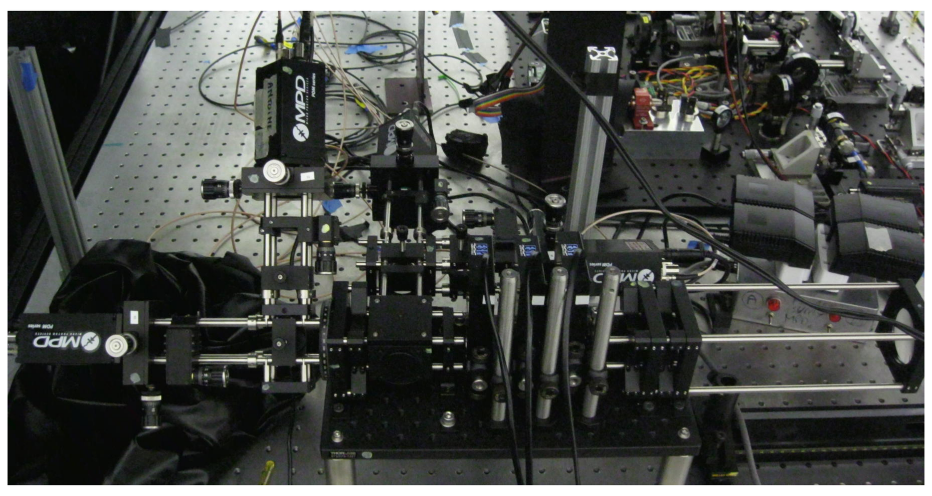
Above: Invisibility of QKD states after compensation in the reversed protocol.

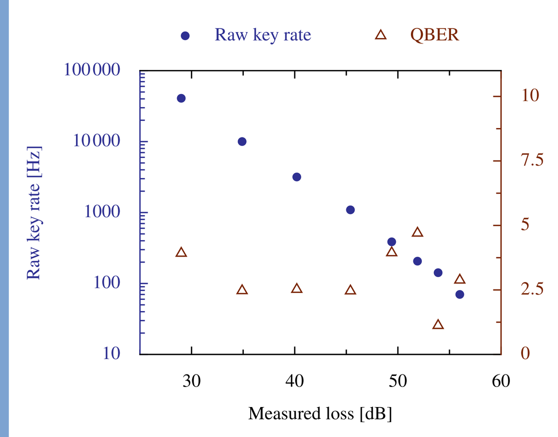
Conclusion: Merely a few **hundred** photons are sufficient to establish *high visibility* for QKD.

3. Experimental High-Loss QKD

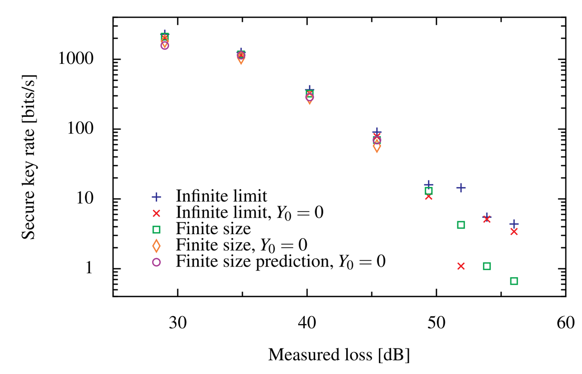
Our previous work demonstrated the *feasibility* of QKD with $\sim$50 dB loss [5]. Here we develop and demonstrate a **complete** QKD system, with chosen algorithms tailored to suit a satellite receiver.





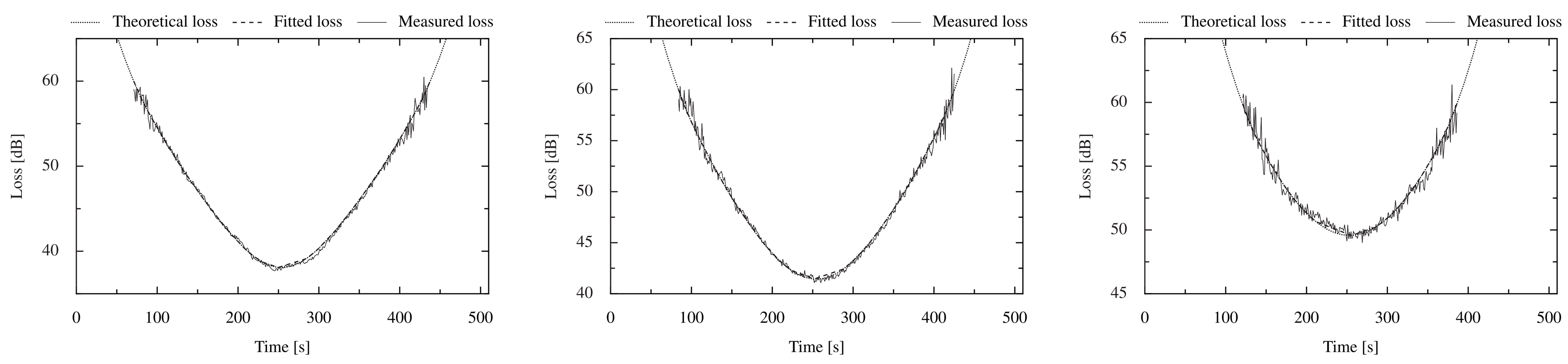


- **Top-left:** Schematic of the apparatus.
- **Top-right:** Picture of the receiver.
- **Left:** Measured raw key rate and QBER for varying losses.
- **Right:** Extracted secure key rates, given various assumptions, for various losses.



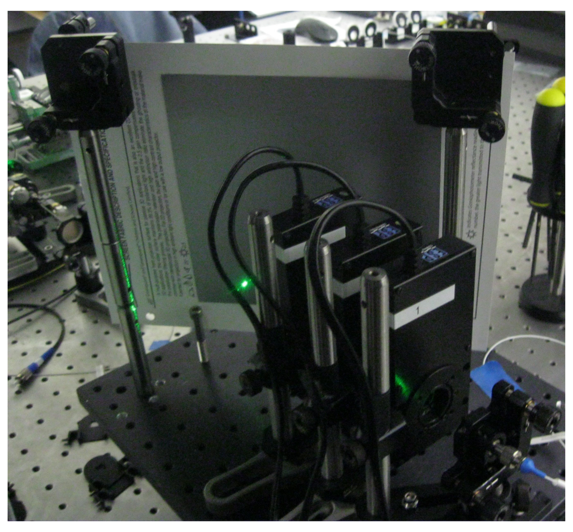
We achieve QKD with up to 56 dB of loss while *including finite-size effects* over 20 min collection.

Further, we take this apparatus and *vary the loss over time*, fitting appropriately such that we construct data corresponding with **realistic orbit losses** (see left): best, upper-quartile, and median, below.



Performing QKD post-processing on these data, we obtain 29423 bits of secure key from a single best pass, 12784 bits from a single upper quartile pass, and 512 bits from a single median pass, including finite-size effects (10σ). (Notably, by combining 2 median passes we generated 4071 secure bits.)

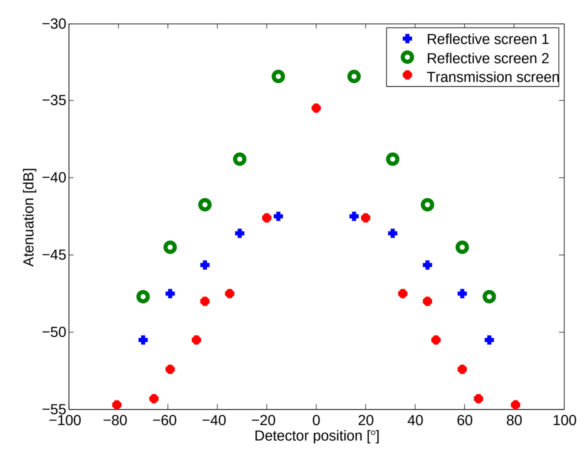
4. High-Loss QKD Spin-off: Diffusive Screen QKD



We are investigating a possible spin-off for high-loss-tolerant QKD: via a **diffusive screen**. This could allow the development of *simple, wireless, multi-access QKD hot-spots* for mobile devices.

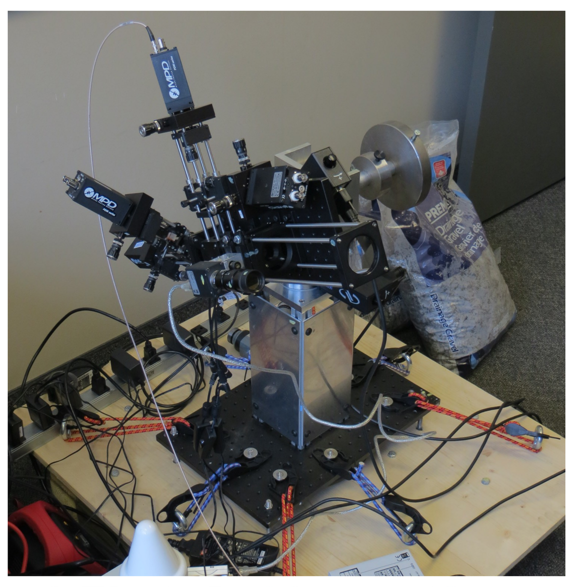
Right: Measured loss profiles of 3 diffusive screen samples (2 reflective, 1 transmissive; 1 cm receiver).

Detector degradation prevents us from performing this experiment presently; new detectors with low dark counts are on the way.



5. In Progress: QKD With A Receiver In Motion

We are presently working to demonstrate QKD with a moving platform. QKD from a moving transmitter has recently been demonstrated [6, 7], but QKD to a moving receiver (as in the QEYSSat proposal) has not.



Our transmitter is located in the dome (above) on the roof of the RAC building, North Campus, with optical access across the surrounding fields. (The source is located in our lab on the ground floor of RAC.) Our receiver (top right) is mounted on a two-axis motorized pointing stage and platform. A diode laser triplet (850 nm) acts as a beacon, with CMOS camera and custom software tracking a duplicate beacon received from the transmitter. This apparatus will then be placed in the tray of a truck (bottom right) and driven, $\sim$600 m distant to the transmitter, at $\approx 1\,^\circ\,\mathrm{s}^{-1}$ relative to the transmitter, *simulating the* $0.1\,^\circ\,\mathrm{s}^{-1}$ *to* $0.7\,^\circ\,\mathrm{s}^{-1}$ *motion of a satellite pass.*

Conclusion

We have demonstrated successful QKD in a **high-loss** regime (3) commensurate with the losses expected of a typical *satellite uplink* (1). With experiments making use of quantum-signal-facilitated polarization alignment (2), current and further work (5) **affirms the feasibility** of satellite QKD and potential spin-off technologies (4).

References

[1] N. Lütkenhaus & A. Shields. *Focus on Quantum Cryptography: Theory and Practice.* New J. Phys. **11**, 045005 (2009).

[2] Z. Yan *et al. An ultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode.* Rev. Sci. Instrum. **83**, 073105 (2012).

[3] A. Tomaello *et al. Link budget and background noise for satellite quantum key distribution.* Adv. Space Research **47**, 802–810 (2011).

[4] J.-P. Bourgoin *et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication.* New J. Phys. **15**, 023006 (2013).

[5] E. Meyer-Scott *et al. How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss.* Phys. Rev. A **84**, 062326 (2011).

[6] S. Nauerth *et al. Air-to-ground quantum communication.* Nature Photonics **7**, 382–386 (2013).

[7] J.-Y. Wang *et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution.* Nature Photonics **7**, 387–393 (2013).