The QEYSSat Mission:

Demonstrating Global Quantum Key Distribution Using a Microsatellite

26th Annual Small Satellites

August 13-16, 2012

I. D'Souza, D. Hudson, C. Evans, E. Choi – COM DEV Ltd.

T. Jennewein – Institute for Quantum Computing, University of Waterloo

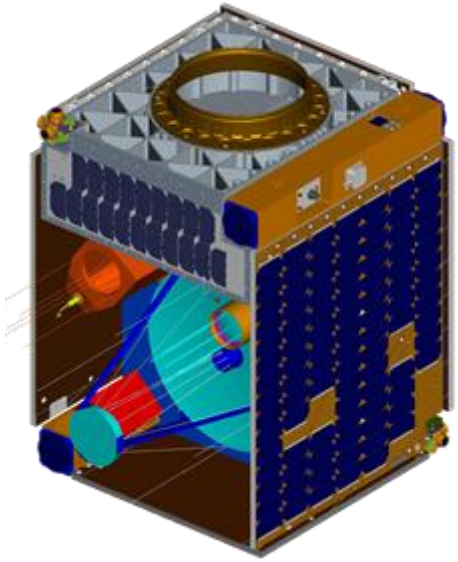
K. Sarda – Space Flight Laboratory, University of Toronto

COM DEV®

QEYSSat: Quantum EncrYption and Science Satellite

- Used to create a quantum link to space
  - individual polarized photons sent from ground to microsatellite
- Demonstrate global quantum key distribution
- Provide platform for long distance entanglement science

- Characterize & optimize the quantum link
- Demonstrate satellite re-keying
- Allow testing of multiple quantum source types
  - single photons / faint laser pulses
  - entangled photons (quantum correlations)

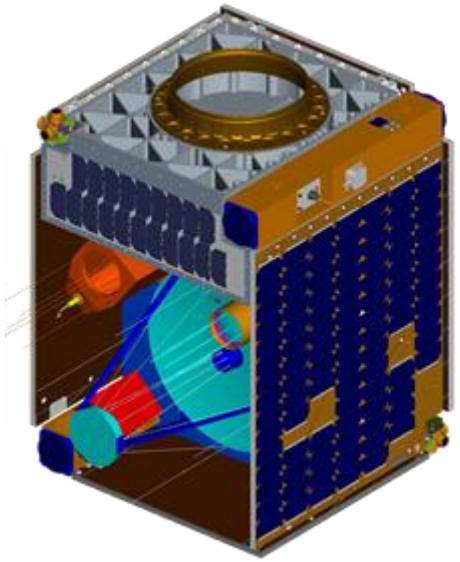


© Canadian Space Agency

COM DEV

Quantum Satellite Proposal

- Studies Performed to date:
  - 2010 Governmental Institution Study on QKD downlink approach.
  - 2010-2011 CSA Study: mission using uplink allows global QKD and science
  - CSA support for advancing the Technical Readiness Levels
  - CSA project for development of key technologies (pointing/tracking)
  - Can be built with all-Canadian industrial partnerships
  - Launch in 3 to 5 years feasible

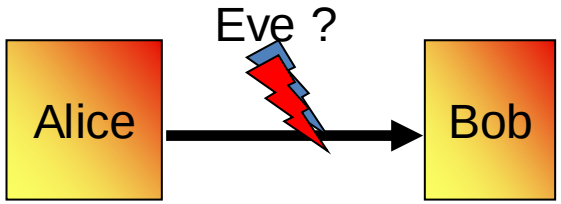


- CSA Contractor, COM DEV Mission Lead, IQC Principal Investigator (Thomas Jennewein)

© Canadian Space Agency

What is Quantum Key Distribution (QKD) ?

- Closes the security loophole of encryption key distribution
  - Security rests on the laws of nature (Uncertainty Principle)
- Key is encoded in quantum states (polarizations of <u>single</u> photons) sent from Alice to Bob
- Eavesdropping impacts quantum state
  - Estimation of bit errors indicates security
  - Security of key is quantifiable
- Secure key does not exist prior to transmission and processing of quantum signal
  - Only known by Alice and Bob



Measurement	Basis Bit	Polarization Bit
→	0	0
↑	0	1
↘	1	0
↗	1	1

© Canadian Space Agency

COM DEV

Why Go to Space?

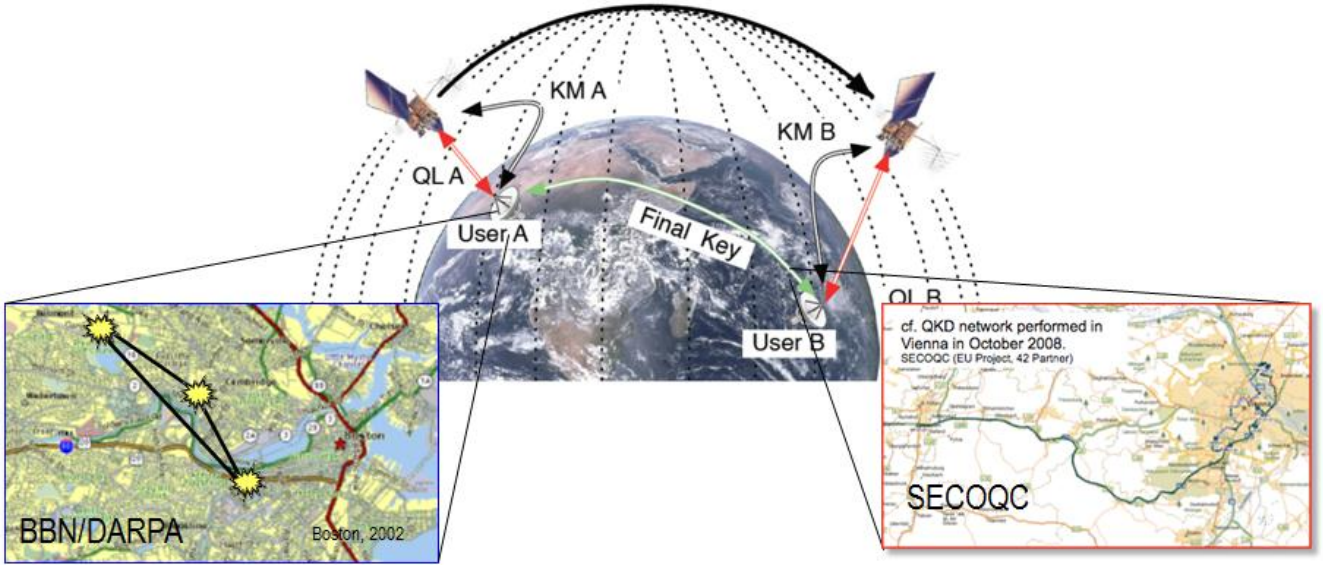
- Maximum quantum link on ground cannot surpass 300 km to 400 km with optical photons
  - Quantum memory & quantum repeaters under development but not expected for perhaps decades
- Quantum Key Distribution (QKD)
  - Distance limits for secure key generation (path length)
  - Provide global coverage for encryption key users
- Fundamental Tests of Quantum Mechanics - Entanglement
  - Distance limits for Bell test (separation of two detectors)
  - Relative speed of entangled photons (effects of relativity)
  - Effect of gravity gradient on entanglement

© Canadian Space Agency

COM DEV®

Key Distribution Concept

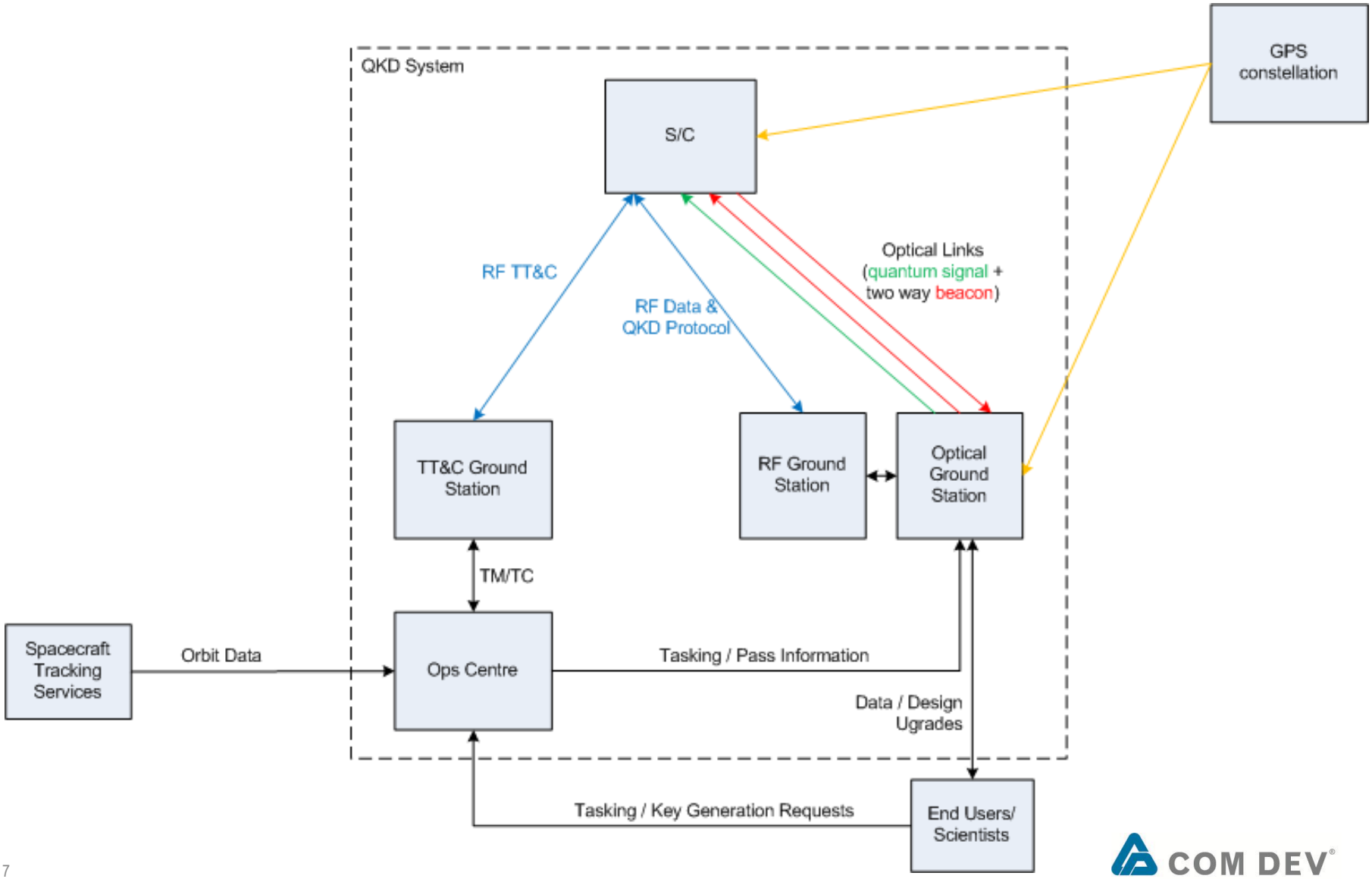
- The satellite generates one secure key with Station A, then a second secure key with Station B
- Unsecure information about the combination of the two keys, allows one station to determine the key of the other
  - Bitwise comparison of two keys calculated (D=XOR(A,B))
  - D transmitted to one station (eg. Station B) which calculates Key A (A=XOR(D,B))
  - Stations A and B use Key A to encrypt their communication



© Canadian Space Agency

COM DEV

System Overview



© Canadian Space Agency

COM DEV

Quantum Link Requirements

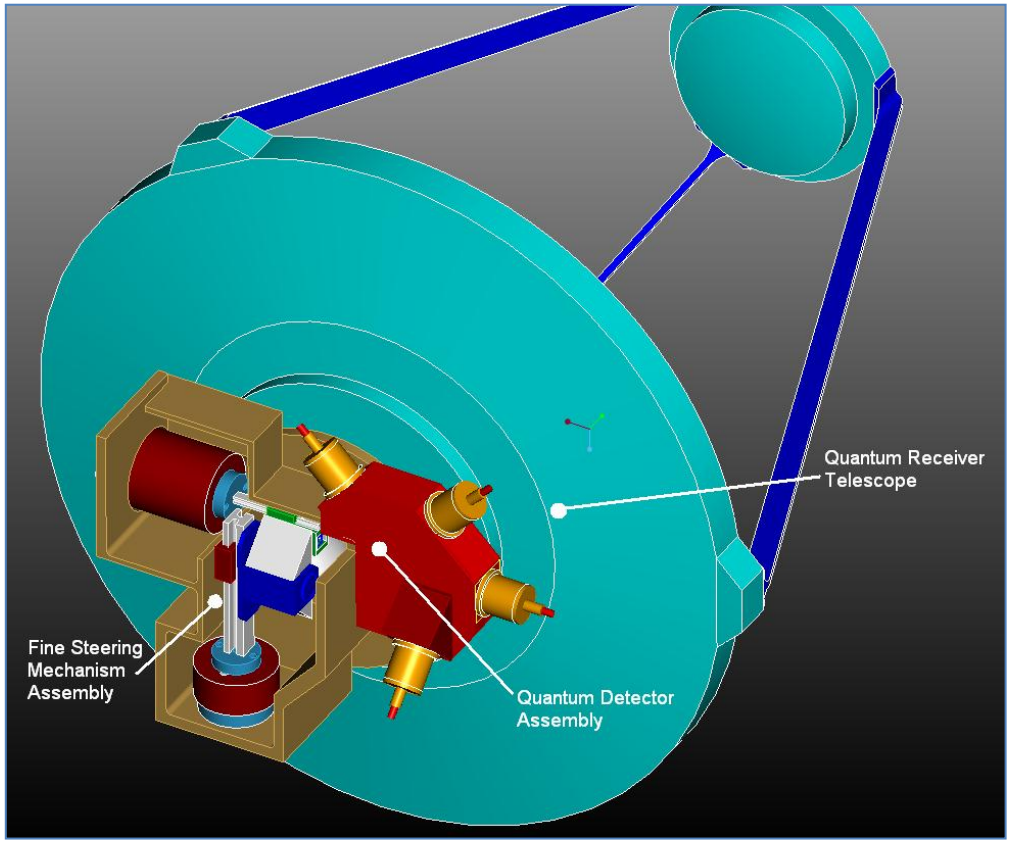
- Photon detection rate
  - Must provide key generation rate which demonstrates a useful operational system
  - Link budget defines receiver aperture size, detector sensitivity, and pointing alignment
- Polarization measurements
  - Polarization maintaining optics
  - Alignment of polarization reference frame between satellite and ground station
- Data logging
  - High speed recording of photon reception times
  - Clock alignment to correlate sent and received times
- Acquisition, Pointing, and Tracking
  - Receiver telescope must find and track the quantum source
  - Receiver and transmitter actively track a beacon target for fine pointing

© Canadian Space Agency

COM DEV

Recent Work – Optical APT

- Payload fine pointing subsystem
- Selection of optimum design for pointing correction mechanism
- Demonstration of concept feasibility
  - Link budgets for beacon target
  - Impact of pointing mechanism on quantum signal
  - Integration of system in payload

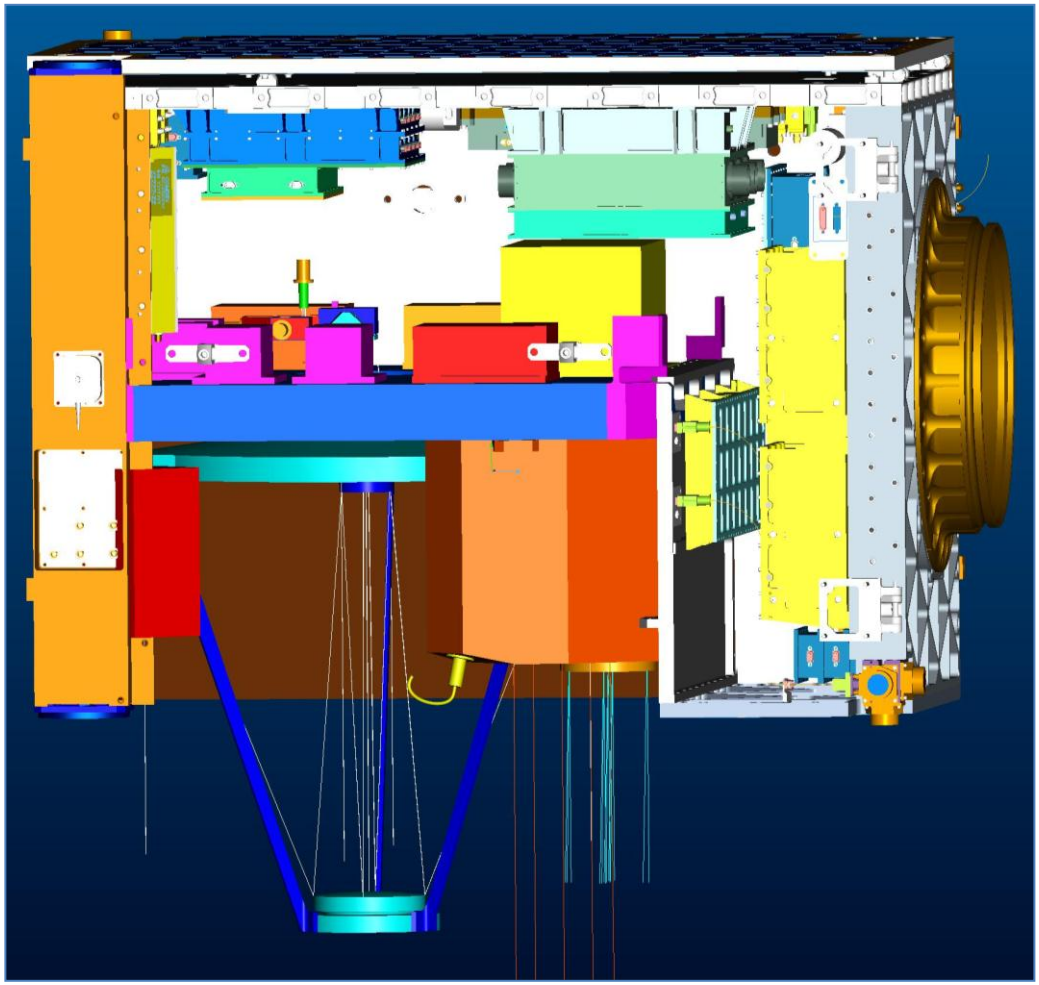


© Canadian Space Agency

COM DEV

Payload Accommodation on AIM Bus

- Secondary mirror extends outside nominal AIM envelope
- CoM in target range for launch requirement
- ADCS upgrades required
- Payload integrated and tested independently
- Volume available for small secondary payload

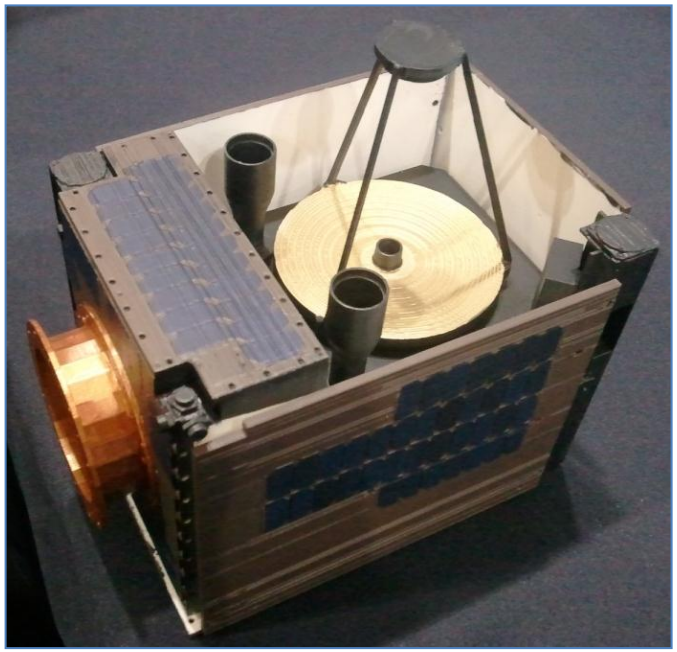


COM DEV®

© Canadian Space Agency

Conclusion

- Implementation of satellite-based QKD will provide encryption key distribution with unconditional security on a global scale
- A microsatellite mission to demonstrate long-range QKD is feasible with current technology and reasonable budgets
- The proposed QEYSSat mission would
  - Demonstrate the feasibility of space based QKD and retire risk
  - Provide a platform for fundamental quantum physics experimentation
  - Provide data on the quantum link in order to optimize a future operational system



© Canadian Space Agency

COM DEV