ENTANGLEMENT-BASED QUANTUM COMMUNICATIONS FROM CUBESATS
OVERVIEW

- Background / motivations
- Quantum technologies
- The Quantum threat
- Quantum Key Distribution
- Satellite QKD

- Overview of satellite QKD in Singapore
Quantum Technologies

- Quantum Revolution
- Quantum Technologies
THE SECOND QUANTUM REVOLUTION

Quantum Science

1st Quantum Revolution

weird

Quantum Technologies

Quantum Engineering

2nd Quantum Revolution

resource
QUANTUM TECHNOLOGIES

Q. Computing  Q. Communication  Q. Sensing
The Quantum threat

- Public Key Encryption
- How Quantum Computers threaten it
- Threat timeline
COMMUNICATION NETWORKS USE SATELLITES AND FIBRES
BUT THESE LINKS ARE NOT SECURE AGAINST EAVESDROPPERS
SO WE NEED ENCRYPTION TO GUARD AGAINST EAVESDROPPERS
Public Key Encryption (PKE) is used to Distribute Keys

- Majority of keys are distributed through PKE, which is difficult to crack with today’s technology…

![Diagram of key exchange process]

- Alice sends a message to Bob.
- Bob encrypts the message with his public key.
- Alice receives the encrypted message.
- Alice decrypts the message with Bob’s private key.

Eavesdroppers can access the public key and the encrypted message.
PUBLIC KEY (ASYMMETRIC) CRYPTOGRAPHY

- Security derived from algorithmic complexity
- Public and Private keys rely on operations that are easy to do in one direction but hard in the other.
- $50929 \times 196927 = \, ?$
- Prime factors $10029295183$?
- Basis of RSA cryptography
“The RSA-2048 Challenge Problem would take 1 billion years with a classical computer. A quantum computer could do it in 100 seconds”

Dr. Krysta Svore, Microsoft Research

When will this be possible?

- Reasonable worst case: 2027
- Likely: 2035 or later

According to:

Almost all presently transmitted communications may be accessible on that date!
MOST SECURE SOLUTION IS QUANTUM KEY DISTRIBUTION

QKD is a method for creating \textit{symmetric} keys between remote users

- Fundamentally random numbers “uncrackable”
- Delivered with complete privacy
- Eavedroppers detected
- Automated and scalable
- One time pads or continuously refreshing AES keys
- Global reach
Implementing Quantum key distribution

What infrastructure is needed to deliver QKD keys?
WHAT IS QKD

An optical technology for establishing symmetric strings of truly random bits for two remote users
WHAT IS QKD

An optical technology for establishing symmetric strings of truly random bits for two remote users.
WHAT IS QKD

Any eavesdropper on the channel can be detected.
WHAT IS QKD

Random bit strings can be used as ‘unhackable’ encryption keys

Alice

Bob

101100101011001010111010

101100101011001010111010

Encrypted data sent over internet
SUBSYSTEMS

Alice
- QKD Light source
- Entangled photon pair source

Optical channel

Bob
- QKD receiver
- Single photon detectors

Fibre or free space link
SATELLITE QKD SUBSYSTEMS (EXAMPLES)

Alice
- QKD Light source
- Entangled photon pair source
- Satellite optical terminal

Satellite (Alice)

Optical channel

Ground Station (Bob)
- QKD receiver
- Optical ground station
- Single photon detectors

(b)
COMMERCIAL FIBRE QKD SYSTEMS

IDQ – Cerberis³


Toshiba

Diamanti, E et al. (2016). Practical challenges in quantum key distribution
FIBRE VS SATELLITE

Entanglement distribution via satellite as an alternative:

- Losses scale much more favorably
- Most of the path outside of the atmosphere
- Constellations of orbiting satellites can offer continuous global coverage

Reproduced from: Sheng-Kai Liao et al. Satellite-to-ground quantum key distribution
Satellite QKD

Performing QKD between low earth orbit and ground.
SPACE BASED QKD CONFIGURATIONS
Entanglement distribution over 1200 km

BB84 with key rates of more than 10 kBit/s
ELEMEENTS TO PERFORM SATELLITE QKD

Satellite (Alice)

- Quantum source
- Optical terminal

Alice

- QKD Light source
- Optical channel

Ground Station (Bob)

- Telescope
- Quantum receiver

Bob

- QKD receiver
LEO SATELLITE CONCEPT OF OPERATIONS

Establish high-accuracy optical link
Start transmission quantum signals

During the pass:
Transmission of quantum signal

Ground station receives qubits
Detection events are time-stamped

Cease transmission of quantum signal
Store QKD data on-board for post-processing

Qubits
Pointing beacons, laser comms
BOB: QUANTUM RECEIVER

Image credit: PlaneWave
ENTANGLEMENT DISTRIBUTION: DOUBLE-DOWNLINK

Ground Station (Bob)

Satellite (Alice)

Quantum source

Optical terminal with two telescopes

Telescope

Quantum receiver

Telescope

Quantum receiver

QKD Receiver

Entangled photon source

Optical channel

Optical channel

Optical channel

QKD receiver

Quantum receiver
Satellite QKD in Singapore
OVERVIEW - SATELLITE QKD IN SINGAPORE

• **Beginnings** - *free space QKD*
• **Early missions** – *correlated photon sources on CubeSats*
• **Last mission** – *SpooQy-1, entangled photon source*
• **Next missions** – *Space-to-ground QKD*

• Commercialisation through **SpeQtral**
Beginnings

National University of Singapore
Pre 2010
NUS CENTRE FOR QUANTUM TECHNOLOGIES

Artur Ekert, founding director of CQT 2007 - 2020

Photos Courtesy CQT
CENTRE FOR QUANTUM TECHNOLOGIES

Decoding the quantum universe, designing the quantum future.

- Established December 2007
- First of five national Research Centres of Excellence
- Various associated spin-out companies:

   [Logos of associated companies]

National University of Singapore
ENABLING FUTURE TECHNOLOGIES

Entanglement distribution

Quantum Key Distribution
Quantum Clock Synchronization
Quantum Repeaters
Quantum Internet

Today

Future
Correlated photons

NUS Centre for Quantum Technologies
2012 - 2016
CORRELATED PHOTON SOURCE DEMOS

Produces pairs of photons
Precursor to entangled photon sources

SPEQS – Small Photon Entangling Quantum System

Key challenges
• Miniaturisation and robustness
• Optical alignment
• GM-APD
  • Radiation effects
  • Temperature stability

CORRELATED SOURCE PATHFINDER MISSIONS

2012/13
- Helium filled weather balloon
- Parachute
- Package with photon source & GPS tracker
- VHF beacon
- 37.5km

2014  GomX-2

2015  Galassia

optics payload
The photon pair source that survived a rocket explosion

Zhongkan Tang1, Rakhitha Chandrasekara3, Yue Chuan Tan1, Cliff Cheng1, Kadir Durak1 & Alexander Ling1,2
Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite

Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel K. L. Oi, and Alexander Ling
Entangled photons

NUS Centre for Quantum Technologies
SpooQy-1 3U CubeSat
2019 - 2021
2019: ENTANGLED PHOTON PAIR SOURCE IN CUBESAT
ENTANGLED PHOTON SOURCE

1: laser diode
2: prism pair
3: fluorescence filter
4: BBO1
5: half-wave plate
6: BBO2
7: dichroic mirror
8: long-pass filter
9: YVO4
10: dichroic mirror
11,11': prism pair
12,12': liquid crystal polarization rotator
13,13': interference filter
14,14': avalanche photodetector

Isostatic mounting designs by UNSW Canberra
SPOOQY-1 DEPLOYED 17TH JUNE 2019
Entanglement demonstration on board a nano-satellite


1Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, S117543 Singapore, Singapore
2Current address: Department of Electrical and Electronics Engineering, Ozyegin University, 34794 Istanbul, Turkey
3FHNW University of Applied Sciences and Arts Northwestern Switzerland, School of Engineering, Küstenstrasse 2, CH-5210 Windisch, Switzerland
4University of New South Wales Canberra, School of Engineering and Information Technology, Canberra NSW, Australia
5SUPA Department of Physics, University of Strathclyde, John Anderson Building, 107 Rottenrow East, G4 0NG Glasgow, UK
6Physics Department, National University of Singapore, 2 Science Drive 3, S117542 Singapore, Singapore
7Corresponding author: aitor.villar@nus.edu

Received 6 January 2020; revised 30 April 2020; accepted 25 May 2020 (Doc. ID 387396); published 25 June 2020
Upcoming missions

CubeSat to ground QKD
Launching 2024
Towards detecting Gigacount rates from a polarization entangled photon-pair source

Alexander Lohrmann,¹ Chithrabanu Perumangatt,¹ Aitor Villar,¹ and Alexander Ling¹,²
¹) Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, S117543, Singapore
²) Physics Department, National University of Singapore, 2 Science Drive 3, S117542, Singapore

During the pass:
Transmission of quantum signal

Establish high-accuracy optical link
Start transmission quantum signals

Ground station receives qubits
Detection events are time-stamped

Cease transmission of quantum signal
Store QKD data on-board for post-processing

The ground station performs Quantum Key Distribution with the spacecraft during night-time, cloud-free passes over the ground station in the elevation angle range from 20 to 20 degrees.
SUN SYNCHRONOUS ORBIT (SSO) – ALLOWS GLOBAL COVERAGE

- SSO covers whole globe at same time each day
- Approx noon-midnight SSO required for night time passes
• Each QKD session generates a unique random key
• To link two networks the keys are XOR’d and broadcast
**SATELLITE QKD - VARIOUS USE CASE**

**Direct to User Site**
- Satellite-QKD
- Quantum Ground Station co-located on user site

**Backbone link for QKD networks**
- Satellite-QKD
- Terrestrial FSO and Fibre-QKD links to a network of users (e.g. NQSN)

**User Site**

**Local QKD Network**
SPEQTRAL IS HIRING!

www.speQtral.space/join-us

Particularly seeking:
• QKD specialists
• Key management engineers
• Cyber security specialists
• Grad/post-grad interns

Contact: rob@speqtral.space

Singapore:
• Fully independent country
• English Speaking
• Asian Tiger economy
• City in a garden
• Hub for South East Asian destinations