Global Quantum Communication Networks
Ground to Space Quantum Links

Thomas Jennewein
Institute for Quantum Computing & Department of Physics and Astronomy,
University of Waterloo
Thomas.Jennewein@uwaterloo.ca
2019.07.09
Quantum Internet

Quantum internet: A vision for the road ahead

Stephanie Wehner*, David Elkouss, Ronald Hanson

Science 362, 303 (2018)
Quantum Internet may be useful for ...

• **Secure communications (QKD)**
  

• **Quantum Money**

  Wiesner, 1983: long distance entanglement (stored spins)

• **Quantum computing**
  
  • Interfacing between quantum computers
  • Quantum computing “in the cloud”


• **Metrology**
  
  • Clock Synchronisation
  • Telescopes

Quantum Internet – The Infrastructure

Qubit distribution through networks. Multiple different physics systems and channels need to operate together.
Quantum networking *enabler*: Teleportation

QKD (BB1984), Quantum-dense coding (BW 1992), but the breakthrough came with 

Building future quantum networks

- Multiple Qubit technologies – Superconductors, Ions, Photons, etc.
- The final ‘winning’ technology undecided, but
- Networking will be based on photonic systems, e.g.

Monroe group, PRL 100 (2010)

Hansen group, Nature 526 2015)

Quantum Key Distribution

Fixes the loophole of key distribution, where classical keys could be copied or compromised during transport. Only transmit single quanta of light per bit.

L. O. Mailloux et. al. Journal of Cyber Security and Information Systems, 4, 2 – Basic Complexity
Quantum Cryptography with Entangled Photons

Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger

Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria

Sektion Physik, Universität München, Schellingstrasse 4/III, D-80799 München

(Received 24 September 1999)

By realizing a quantum cryptography system based on polarization entangled photons, we highly secure keys, because a single photon source is approximated and the inherent quantum nature of the source is exploited. We implement a novel key distribution scheme that is immune to eavesdropping and allows for a secure key exchange. Our system has two completely independent users separated by 360 m, and at rates of 400–800 bits/s with bit error rates around 3%.

PACS numbers: 03.67.Dd, 42.79.Sx, 89.80.+h

The primary task of cryptography is to enable two parties (commonly called Alice and Bob) to mask confidential messages, such that the transmitted data are illegible to any unauthorized third party (called Eve). Usually this is done using shared secret keys. However, in principle it is always possible to intercept classical key distribution unnoticed. The recent development of quantum key distribution can cover this major loophole of classical cryptography. It allows Alice and Bob to establish two completely secure keys by transmitting single photons (qubits) along a quantum channel. The underlying principle of quantum key distribution is that nature prohibits eavesdropping on the

In any real cryptography by Alice and Bob contains rected by classical error correct. Furthermore, it has been shown that Alice and Bob can share a sufficiently its security by privacy amplification. This allows them to distill a key to a desired level of security.

A range of experiments has demonstrated the feasibility of quantum key distribution in long distance interferometers. A common problem is the transmission of photons.
Findings Fuel Debate

And Thomas Jennewein of the University of Vienna, lead author on the third paper, said that turning those ideas into an off-the-shelf technology was no longer unthinkable: "We realized a complete quantum cryptography system, almost ready to use."

In the Quantum World, Keys to New Codes

"It was first considered as pure philosophy," said Prof. Nicolas Gisin, a physicist at the University of Geneva, who is a co-author of one of the papers. "Now we discuss that these same strange aspects of quantum mechanics can be of some use in securing the Internet, let's say."

The measured properties of entangled particles are, as the name implies, fantastically entwined. It is said that an eavesdropper can always be detected in this way. But if it does allow information to be passed in a secure way, since any measurement of either particle leaves its trace on the other — meaning that an eavesdropper can always be detected, no matter how clever or technically sophisticated. That guarantee of safe passage would allow people at any two sites to share unbreakable codes using quantum entanglement. The experiments demonstrated several versions of this trick, called quantum cryptography. It differs from all traditional cryptography, in which great pains are taken to transmit codes securely or to make them mathematically hard to crack. But spies, with

In disclosing his prostate cancer, Mayor Rudolph W. Giuliani urged men to be tested.
Why Satellites for Long Distance Q-Com?

• Ground-based
  • Practical systems typically 100 km
  • Demonstrations up to to 400 km
  • Optic fibre loss 0.15 dB/km at best
  • Free-space limited due to line-of-sight
  • Commercial Devices available:
    • Note: Optical amplifiers not possible!

• Longer distances:
  • Trusted Repeaters
    (> 1000km networks under way)
  • Long lived Quantum Memories
  • Quantum Repeaters
  • Satellites

Global Quantum Networks?

• A hybrid system may achieve overall best performance
• Satellites and Q-Repeaters
  • Distances up to 20,000 km

K. Boone, Bourgoin, Meyer-Scott, Heshami, TJ, Simon. PRA 91, 052325 (2015),
Entanglement science in space?

• Certain effects may never show up in the parameter space available on ground

• Global Quantum Networks & QKD & Quantum Computing rely on the validity of QM

• Human-operated Bell-tests
  • Earth – Moon or
  • Earth – “Space Ship” on its way to Mars

T. Jennewein, C. Simon, in preparation

• International collaborations will allow community to strengthen Scientific case and output
~2017: Quantum Communication with Satellites
Quantum communication in space is real

Dedicated quantum hardware in Space:

- China (J.W. Pan)
  - Entanglement Distribution over 1200 km! (Science, 2017)
  - QKD from space to ground, (Nature 549, 43–47 (2017))
  - Teleportation (Nature 549, 70–73 (2017))
  - QKD between Beijing and Graz, QKD using Bell-pairs (CLEO 2019)

- Japan (NICT)

- Singapore (A. Ling)
  - Correlated Photon Source onboard CubeSat (Phys. Rev. Applied 5, 054022, 2016), follow up missions launched

Proof of concept demonstrations

- Germany (G. Leuchs): Demonstration of quantum limited states sent from GEO satellite to ground (Vol. 4, No. 6 Optica, 2017)

- Italy (P. Villoresi): Demonstrating a quantum channel from space to ground, (Phys. Rev. Lett. 115, 040502 (2015))

- Canada (T.J.): Airborne demonstration of a quantum communication satellite payload (QST, 2017)

Beijing and Vienna have a quantum conversation
September 2017, [www.physicsworld.com](http://www.physicsworld.com)
http://english.cas.cn/newsroom/news/201709/t20170928_183577.shtml
QHEYSSat (Quantum Encryption and Science Satellite)

Anticipated Timeline:

• 2017 - 2022: Scientific PI Contract, Thomas Jennewein
• Industrial Implementation Contracts Shortly
• Launch 2021/22

Study quantum entanglement between ground and space

• Entangled source on ground. Possible tests:
  
  – Entanglement tests at varying distances and delays, variable height
  – Interfacing with quantum repeater nodes
  – Quantum Teleportation
  – Gravitational decorrelation
  – Special relativity and QM

Timing ambiguity scenario,
New approaches for free-space quantum channels

- Alternative encoding of qubits
- Reference Frame Independent QKD
- HOM interference with structured pulses
Myth: You can only use polarization encoding in free-space quantum communications

Polarization effect of mirrors due to Fresnel-coefficients

- Retardance maps for each mirror element (first three panels) and the cumulative retardance for the entire telescope (last panel).


What about Time-bin encoding in Free-Space?
Unbalanced Interferometer Suitable for Quantum Communications

• Compatibility with Multi-mode Photonic Qubits:
  • 3rd gen system:
  • Visibilities now up to 98% for MMF beam,
  • Throughput ca. 75%

  - Phys. Rev. A 97, 043847 (2018)]
First Outdoor Time-Bin QKD Channel

- 1.2 km outdoor link
- Introduced additional turbulence
- Also introduced depolarization
- Full BB84 protocol

Reference-frame independence

- Challenge for QKD implementations
  - How to align the reference frames (e.g. polarization states at Alice have to match Bob’s)
  - Particular problem in our case is the motion of the telescope
- Realtime Compensation:

![Tomography](image1.png)

![Compensation](image2.png)

Airborne Transmitter, Smith Falls, 2016
Reference Frame Independent

- Tomographic protocols can be used to verify the channel

Raw Key QBER:
\[ Q = 1 - \frac{1}{2} \langle Z_A Z_B \rangle. \]

Channel Verification:
\[ C = (X_A X_B)^2 + (X_A Y_B)^2 + (Y_A X_B)^2 + (Y_A Y_B)^2. \]
Satellite receiver limited to 4 states

- New variant required: 6 – 4 state protocol

Channel Verification:

\[ C = \sqrt{\langle X_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2}, \]

\[
\begin{align*}
\langle \sigma_Z \otimes \sigma_Z \rangle &= (1 - 2Q) \\
\langle \sigma_X \otimes \sigma_X \rangle &= (1 - 2Q) \cdot \cos \theta \\
\langle \sigma_Y \otimes \sigma_X \rangle &= -(1 - 2Q) \cdot \sin \theta \\
\langle \sigma_V \otimes \sigma_X \rangle &= (1 - 2Q) \\
\sigma_V &= (\cos \theta) \sigma_X - (\sin \theta) \sigma_Y
\end{align*}
\]

\[ |\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + e^{-i\phi} |1\rangle_A |0\rangle_B) \]

\[ 4 \text{ States (H, V, D, A)} \]

\[ 6 \text{ stats} – H, V, D, A, L, R \]

\[ \text{Location B e.g. Waterloo} \]

\[ \text{Bob} \]

C will be constantly even for variable angle theta, and if C drops, will reveal Eve!
Experimental Results

The phase is varied by tuning a birefringent element.

Coincidence Counts

Tomography to determine purity of state

\[
Q_{\text{BER}}^{HV} = \frac{1 - \langle Z \otimes Z \rangle}{2} = \frac{N_{\text{bad}}}{N_{\text{total}}},
\]

\[
Q_{\text{BER}}^{\ast \text{Diag}} = \frac{1 - C}{2}.
\]

\[
R \geq Q_{\lambda} \left(1 - f H_2(Q_{\text{BER}}^{HV}) - H_2(Q_{\text{BER}}^{\ast \text{Diag}})\right)
\]
Summary

• Quantum Communication in Space
• Canadian QEYSSat mission, Academic-Gov-Industry partnerships
• Explore new directions for Free-Space Quantum Channels:
  • Time-bin, RFI-QKD, MDI-QKD (not shown today)
Challenges for Quantum Networks

• Efficient and robust q-channels
• Dimensions – power – mass
  • chip scale systems?
• Interfaces / transducers
  • connect channels with stationary qubits
• Long term q-memories
• Routing technology
• Cost
• .....