28 January 2026

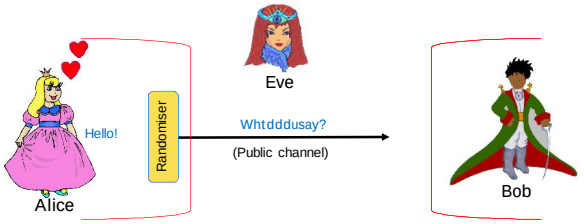
Towards Global Quantum Communications Networks: Data Security in the Quantum Era

Mohsen Razavi

School of Electronic and Electrical Engineering
University of Leeds

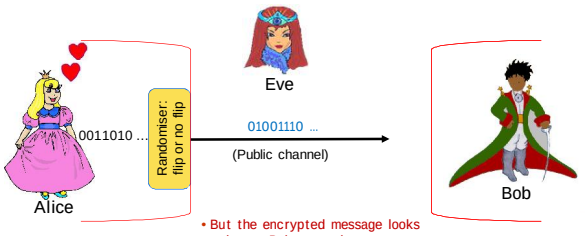
A Key to Secrecy: Randomisation

- Cryptography is the science behind data security
- One of its key tasks: to send *confidential* messages, via a public network, such that no illegitimate party learns about the message
- Key idea: Randomisation
- If what appears on the public channel looks utterly random, then eavesdroppers have a hard time decoding the original message



Example: One-Time Pad

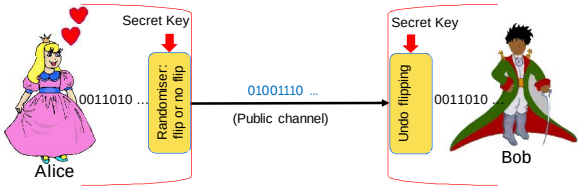
- Suppose Alice's message is in the form of bits: 001101011101 …
- For each bit she can toss a coin:
  - If it comes Head, then she sends the bit as is;
  - If it comes Tail, then she flips the bit before sending
- The output message is fully random; Eve doesn't know which bits have been flipped!



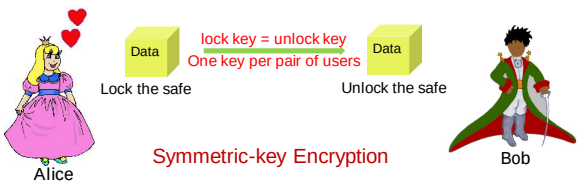
- But the encrypted message looks random to Bob too, unless …

Key Distribution

- Bob needs to know the flip-no-flip sequence in order to undo flipped bits
- In the cryptography jargon, such a flip-no-flip sequence is called a "key", or a secret key. We can think of the key as a sequence of random bits.
- In order to do cryptography in this manner, we need a secure mechanism to exchange the key between legitimate users.



Symmetric Key Cryptography

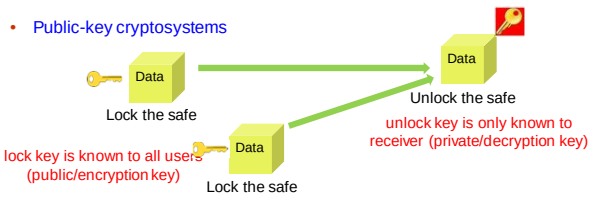


Symmetric-key Encryption

- Challenge: How to distribute secret keys between two parties?
- NB: Some of these parties are effectively our computers and mobiles; they cannot meet in person easily!

Public-key Cryptosystems

- Let's think outside the box!
- Public-key cryptosystems



Locking key ≠ Unlocking key

- A secret key can be generated locally and encrypted using the public key of receiver
- Example: RSA protocol, widely in use, relying on the difficulty of factorisation

Shor's Algorithm: Super-efficient Factoring

- A quantum computer can potentially factor large integer numbers much more efficiently than classical computers. For an integer number *N*,

Classical computer $O((\log N)^{(\log N)^{1/3}}) \longrightarrow O((\log N)^3)$ **Quantum computer**

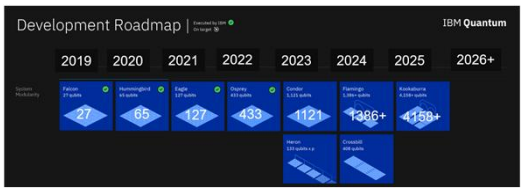
Billions of years for the best **known classical** algorithm

It may only take a few days/hours to factor a 1000-digit number!

P. W. Shor, Algorithms for quantum computation: discrete logarithm and factoring, in Proc. 35th FOCS, 1994.

Summary so far

- Data security relies on public and symmetric key schemes for encryption and authentication
- Public-key schemes are threatened by the advent of quantum computers, and possibly other advanced technologies.
- Quantum computers are on the rise:



- **Question:** Why are we still using them then?
- Some may say, we do not yet have *strong enough* quantum computers

Everlasting Security in Quantum Era

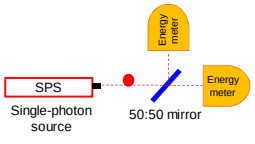
- A hacker with a quantum computer in 100 years from now can go back and decrypt all RSA-encrypted messages sent throughout!
- It's not the case that every secret communication needs to remain secret for ever.
- But, there are personal and private data, as well as sensitive military and governmental information that needs to be kept secure for a long time

Quantum Key Distribution (QKD)

- Challenge: our existing techniques for sharing a secret key, based on public key cryptography, can be broken by quantum computers. How shall we distribute a key securely in the quantum era?
- Solution: Instead of computational complexity, let us rely on the laws of physics as we understand them by Quantum Mechanics!
- Distinct feature: We can detect eavesdropping attempts!

Inherent Randomness in Quantum Systems

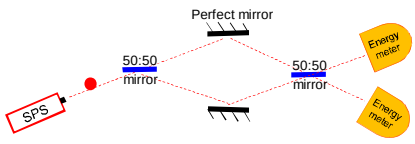
- Let's generate a single photon, and let it go through a 50:50 partial mirror. What do you expect to happen?



- Observations:
  - Only one detector clicks at the time;
  - Any detector could click;
  - If we run the experiment many times, each detector clicks half of the time
- It seems randomness is inherent to quantum systems

The Weird Superposition

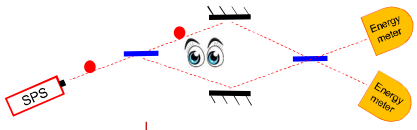
- Now, let's send our single photon through an interferometer. What do you expect to happen?



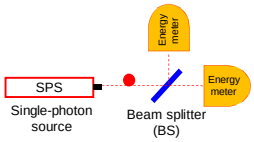
- Observation:
  - Only one detector clicks; the other one never clicks!

The Weirder Measurement Effect

- Now, let's assume we somehow check, in our interferometer, which path the photons has taken. What do you expect to happen?



- if someone meddles with our signal, the outcome could change!

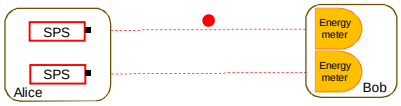


A Simple QKD Protocol

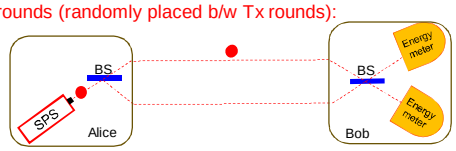
Let's put our learning into action!

Key transmission (Tx) rounds:

- Alice sends a photon through the upper channel to transmit bit 1, or lower channel for bit 0



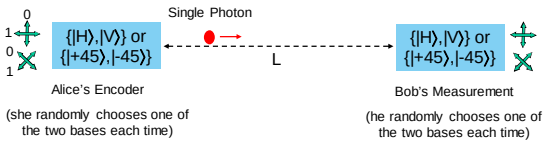
Test rounds (randomly placed b/w Tx rounds):



- If Eve tries to find out which channel carries the photon, she causes error → This can be used to estimate leaked info to Eve.

Point-to-Point QKD: BB84

- Bennett-Brassard Protocol (BB84)



Alice's Encoder

(she randomly chooses one of the two bases each time)

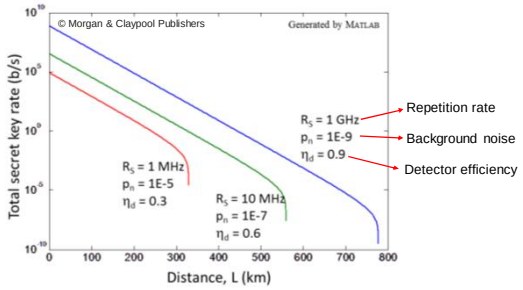
Bob's Measurement

(he randomly chooses one of the two bases each time)

- Security: any tampering with the single photon can be detected by Alice and Bob
- Operational requirement: Information encoded on a single/few photon

Single-Photon Communications

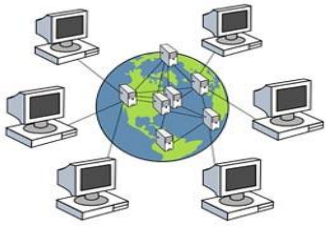
Point-to-Point QKD: Limitations



- Observations:
  - Rate drops exponentially with distance in fibre
  - Security distance drops with background noise
  - Distance record: > 1000 km [Phys. Rev. Lett. 130, 210801, May 2023], but only a few bits/s can securely be exchanged

Grand Vision: Global Quantum Internet

Quantum Internet: Anytime, Anywhere, for Anyone



Grand Objective: To deploy QKD, and other quantum applications,
at the network level by
supporting multiple users
in a cost-efficient way
at any distance

Phased Deployment

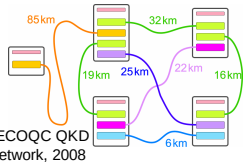
- 1G* Quantum networks: Trusted node approach
  - Integration
  - Multiplexing and Multiple Access
  - Wireless Access
- 2G Quantum networks: Partially trusted approach
  - Satellite QKD
  - Entanglement Based QKD
  - Rate Scaling
- 3G Quantum networks: Trust-free approach
  - Entanglement Based Repeaters
  - Memoryless Repeaters

Now → Near term

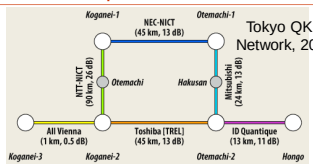
Long term

* Terminology is arbitrary

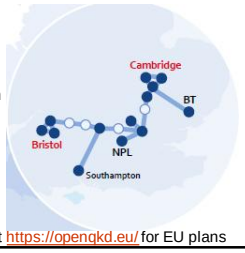
Trusted-Node QKD Networks: Implementations



SECOQC QKD Network, 2008



Tokyo QKD Network, 2010



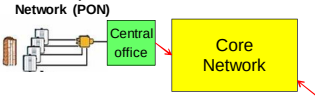
UK Quantum Network, 2018

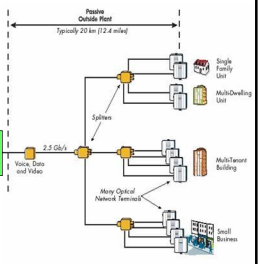
China Beijing-Shanghai link with 32 nodes (~2000 km), 2017

Check out https://openqkd.eu/ for EU plans

Quantum Access Networks

Passive Optical Network (PON)



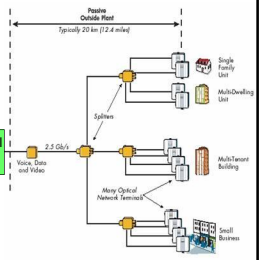


Suitable Platform:

- By the time that QKD is ready for deployment, FTTH is widely available

Quantum Access Networks

Passive Optical Network (PON)



Suitable Platform:

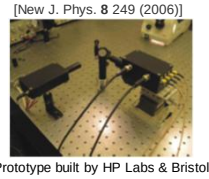
- By the time that QKD is ready for deployment, FTTH is widely available

Challenges for Qcomms:

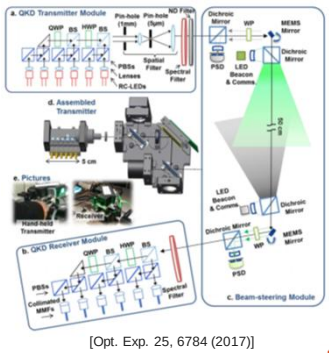
- Co-existence problem: Data and quantum signals must share the same medium; Interference from other quantum/classical users
- Multiplexing and multiple access issues; Inherent splitting loss
- Wireless mode of access: is it possible?

QKD with Handheld Devices: Demonstrations

[New J. Phys. **8** 249 (2006)]



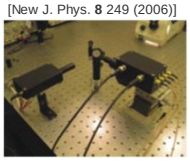
Prototype built by HP Labs & Bristol



[Opt. Exp. 25, 6784 (2017)]

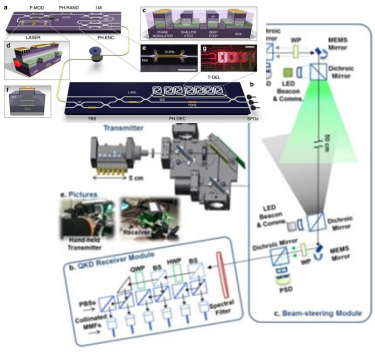
QKD with Handheld Devices: Demonstrations

[New J. Phys. **8** 249 (2006)]



Prototype built by HP Labs & Bristol

[Nature Commun. **8**, 13984 (2017)]



[Opt. Exp. 25, 6784 (2017)]

Phased Deployment

- 1G* Quantum networks: Trusted node approach
  - Integration
  - Multiplexing and Multiple Access
  - Wireless Access
- 2G Quantum networks: Partially trusted approach
  - Satellite QKD
  - Entanglement Based QKD
  - Rate Scaling
- 3G Quantum networks: Trust-free approach
  - Entanglement-based Repeaters
  - Memoryless Repeaters

Now → Near term

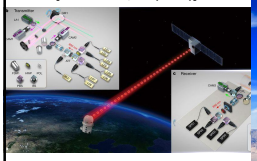
Long term

* Terminology is arbitrary

Satellite-Based QKD

- First QKD satellite, Micius, in orbit!
- 3 breakthrough experiments:
  - QKD between satellite and ground station
  - Teleportation
  - QKD between two cities 7600 km apart

[Nature **549,** 43 (2017)]

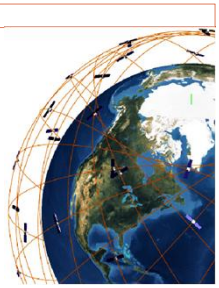


[Nature **549,** 70 (2017)]

[PRL **120,** 030501 (2018)]

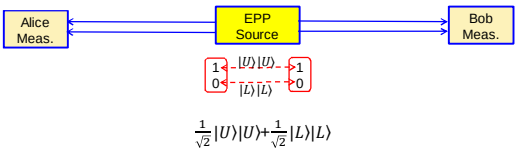
Satellite-Based QKD

- Not without limitations
  - Right now, definitely expensive
  - For LEO satellites, you have about 5 minutes to exchange keys → you need a constellation → even more ambitious
  - Day light could kill you; so far only night operation
  - Weather dependent
  - Not everyone has a large telescope; but such ground stations can be part of the trusted node network
  - The satellite would remain a trusted node in most practical cases
  - There are ways to improve upon the above issues, such as using restricted eavesdropping model, MIMO, adaptive optics, but
    - How about terrestrial solutions?



Let's get back to earth
Alternative Schemes: Entanglement-Based QKD

- QKD with an entangled photon pair (EPP) source

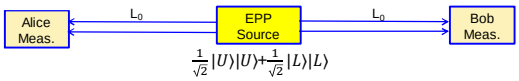


$$\frac{1}{\sqrt{2}}|U\rangle|U\rangle+\frac{1}{\sqrt{2}}|L\rangle|L\rangle$$

- Entanglement is a form of correlation → Ideally Alice and Bob would measure correlated bits
- Monogamy of Entanglement: In order to get information about the key, the third party needs to entangle itself with the above state, but that would break the ideal bipartite entanglement
- Conclusion: Middle party does not need to be trusted.

Entanglement-Based QKD: Key Rate Scaling

- QKD with an entangled photon pair (EPP) source



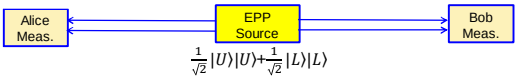
$$\frac{1}{\sqrt{2}}|U\rangle|U\rangle+\frac{1}{\sqrt{2}}|L\rangle|L\rangle$$

$$\text{Key rate} \propto \underbrace{\exp(-\alpha L_0)}_{\eta} \times \exp(-\alpha L_0) \propto \eta^2$$

Can we do any better?

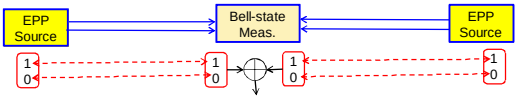
Entanglement-Based QKD

- QKD with an entangled photon pair (EPP) source



$$\frac{1}{\sqrt{2}}|U\rangle|U\rangle+\frac{1}{\sqrt{2}}|L\rangle|L\rangle$$

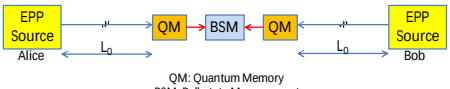
- Entanglement Swapping (Connection) Protocol



The result would tell you how correlated the far end boxes are

Memory-Assisted QKD

- Let's combine EB-QKD with quantum memories

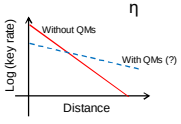


QM: Quantum Memory
BSM: Bell-state Measurement

[PRA **89**, 012301 (2014)]
[NJP **16**, 043005 (2014)]

- Expected benefit: better rate-vs-distance behaviour

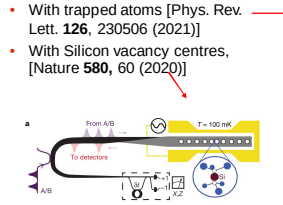
$$\text{Key rate} \propto \underbrace{\exp(-\alpha L_0)}_{\eta}$$

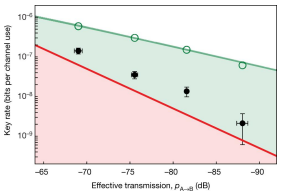


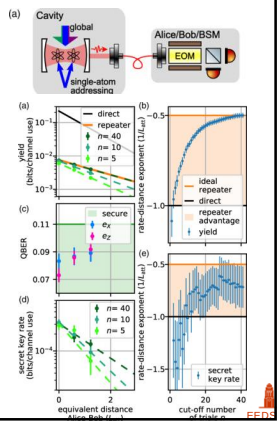
- See also
QST **3,** 014009 (2018);
PRA **96,** 052313 (2017);
PRA **95,** 022338 (2017);
APB **122,** 96 (2016);
JSTQE **21,** 6601010 (2015)

Memory-Assisted QKD Demonstrations

- With trapped atoms [Phys. Rev. Lett. **126**, 230506 (2021)]
- With Silicon vacancy centres, [Nature **580,** 60 (2020)]







Phased Deployment

- 1G* Quantum networks: Trusted node approach
  - Integration
  - Multiplexing and Multiple Access
  - Wireless Access
- 2G Quantum networks: Partially trusted approach
  - Satellite QKD
  - Entanglement Based QKD
  - Rate Scaling
- 3G Quantum networks: Trust-free approach
  - Entanglement Based Repeaters
  - Memoryless Repeaters

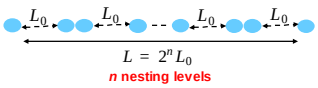
Now → Near term

Long term

* Terminology is arbitrary

Quantum Repeaters

- Objective: to share an entangled state between the far two nodes
- Idea: break the link into shorter segments



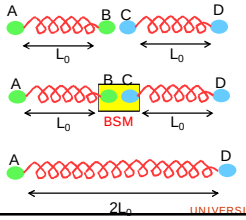
Briegel, Dür, Cirac & Zoller, PRL 1998

- We can then connect the segments by entanglement swapping

Create initial entg & announce it ①

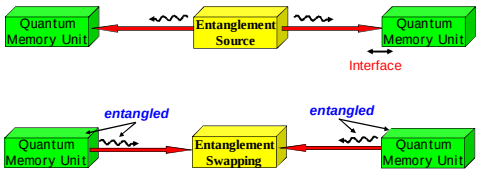
Teleport B to D when both legs are ready ②

Double the distance! ③



Quantum Repeaters: Implementation Challenges

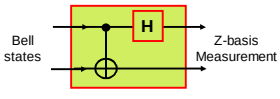
- Heralded Entanglement Generation (HEG): Entanglement is a form of correlation; it cannot be generated out of thin air. It needs to be generated somewhere and then be transferred. That requires photon transmission → susceptible to channel loss → Repeat until Success

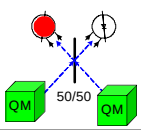


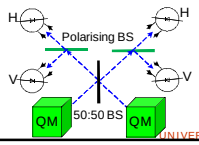
Conjecture: any entanglement distribution technique that relies on photon transmission roughly scales with the loss in any uninterrupted part of the link

Quantum Repeaters: Implementation Challenges

- Heralded Entanglement Generation (HEG): Entanglement is a form of correlation; it cannot be generated out of thin air. It needs to be generated somewhere and then be transferred. That requires photon transmission → susceptible to channel loss → Repeat until Success
- Bell-State Measurement (BSM): This is a two-qubit operation, which means two physical systems need to interact. How to initiate such an interaction between two quantum memories either needs an (optical) interface, and/or is prone to errors.

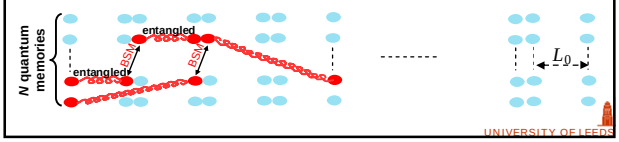






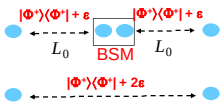
Quantum Repeaters: Implementation Challenges

- Heralded Entanglement Generation (HEG): Entanglement is a form of correlation; it cannot be generated out of thin air. It needs to be generated somewhere and then be transferred. That requires photon transmission → susceptible to channel loss → Repeat until Success
- Bell-State Measurement (BSM): This is a two-qubit operation, which means two physical systems need to interact. How to initiate such an interaction between two quantum memories either needs an (optical) interface, and/or is prone to errors.
- Quantum Memories: That the above two tasks at early stages of quantum repeaters are probabilistic, means that we either incur a lot of waiting time → long coherence times needed, and/or many parallel attempts are needed → need for mass production/control/integration



Quantum Repeaters: Implementation Challenges

- Heralded Entanglement Generation (HEG): Entanglement is a form of correlation; it cannot be generated out of thin air. It needs to be generated somewhere and then be transferred. That requires photon transmission → susceptible to channel loss → Repeat until Success
- Bell-State Measurement (BSM): This is a two-qubit operation, which means two physical systems need to interact. How to initiate such an interaction between two quantum memories either needs an (optical) interface, and/or is prone to errors.
- Quantum Memories: That the above two tasks at early stages of quantum repeaters are probabilistic, means that we either incur a lot of waiting time → long coherence times needed, and/or many parallel attempts are needed → need for mass production/control/integration
- Error Propagation: We need entanglement distillation techniques



Quantum Repeaters: State of the Art

- Heralded Entanglement Generation (HEG): HEG over dozens of km have been demonstrated using atomic ensemble and trapped atom memories (moderate fidelity), and sub-km using nitrogen vacancy centres in diamond (higher fidelity)

Article | Published: 12 February 2020

Entanglement of two quantum memories via fibres over dozens of kilometres

Yong Yu, Fei Ma, Xi-Yu Luo, Bo Jing, Peng-Fei Sun, Ren-Zhou Fang, Chao-Wei Yang, Hui Liu, Ming-Yang Zheng, Xiu-Ping Xie, Wei-Jun Zhang, Li-Xing You, Zhen Wang, Teng-Yun Chen, Qiang Zhang ✉, Xiao-Hui Bao ✉ & Jian-Wei Pan ✉

Nature **578**, 240–245 (2020) | Cite t

Realization of a multinode quantum network of remote solid-state qubits

M. POMPILI ✉, S. L. N. HERMANS ✉, S. BAIER ✉, H. K. C. BEUKERS ✉, P. C. HUMPHREYS, R. N. SCHOUTEN ✉, R. F. L. VERMEULEN, M. J. TIGGELMAN, L. DOS SANTOS MARTINS ✉, I. J. AND R. HANSON ✉ +2 authors | Authors Info & Affiliations

SCIENCE • 16 Apr 2021 • Vol 372, Issue 6539 • pp. 259-264 • DOI: 10.1126/science.abg1919

Article | Open Access | Published: 06 July 2022

Entangling single atoms over 33 km telecom fibre

Tim van Leent, Matthias Bock, Florian Fertig, Robert Garthoff, Sebastian Eppelt, Yiru Zhou, Pooja Malik, Matthias Seubert, Tobias Bauer, Wenjamin Rosenfeld, Wei Zhang ✉, Christoph Becher ✉ & Harald Weinfurter ✉

Nature **607**, 69–73 (2022) | Cite this article

Quantum Repeaters: State of the Art

- Heralded Entanglement Generation (HEG): HEG over dozens of km have been demonstrated using atomic ensemble and trapped atom memories (moderate fidelity), and sub-km using nitrogen vacancy centres in diamond (higher fidelity)
- Bell-State Measurement (BSM): Can be done optically but that would be probabilistic; some memory settings, such as trapped ions/atoms or colour centres (NV or silicon vacancy centres) allow for deterministic gates
- Quantum Memories: we need a device that can interact well with single photons, at the same time having long coherence time, at the same time being able to do gate operations! Top candidates are trapped ions/atoms and colour centres, but none are yet a full package
- Error Propagation: Entanglement distillation can be done probabilistically (demonstrated), but on the long run we need to implement it using quantum error correction techniques. For moderate distances, the requirements are manageable in near-mid term [Phys. Rev. Applied 18, 024041 (2022)], but for longer distances, we need more robust quantum processors.

Different Classes of Quantum Repeaters

	Loss Error	Operational Error	Classical Communication
0G QR	HEG (Probabilistic)	Post-selection	Two way
1G QR	HEG (Probabilistic)	HED (Probabilistic)	Two way
2G QR	HEG (Probabilistic)	QEC (Deterministic)	One way
3G QR	QEC (Deterministic)	QEC (Deterministic)	None

• HEG/D: Heralded Entanglement Generation/Distillation
• QEC: Quantum Error Correction

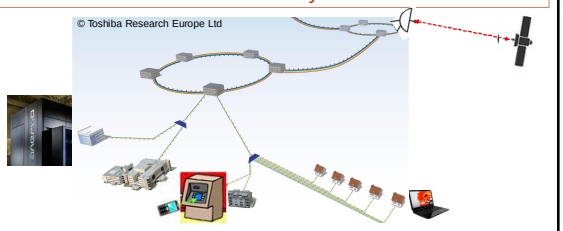
Quantum processing ↓ ↑ Quantum storage

	Features	Requirements
0G QR	Closest to implementation; low rate; could cover ~1000 km	Lots of good memories; linear optics & photodetection
1G QR	higher rates	Deterministic gates w/ errors O(1%); good memories
2G QR	Distillation more resilient to memory errors	Deterministic gates w/ errors O(0.1-1%); good memories
3G QR	Highest rates	High Q Computing; errors O(0.01%); many nodes

The Booming Quantum Industry

- and many more (> 100 listed on Wikipedia)
- Multi-Billion-$ market forecast

Quantum Networks: A Summary



Comms/signal processing
- Access mode (wireless or fibre)
- Multiplexing and multiple-access
- Quantum-classical integration

Network Security
- Inter-generation compatibility
- Trust issue and layered structure
- Standardization and certification

Electronics/integrated optics
- Chip-based devices
- Mass production and end users
- Control

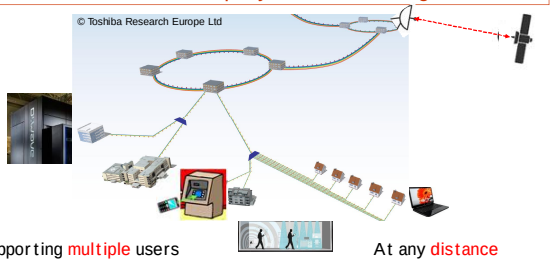
Physics/Computing/Space Comms
- Rate scaling with distance
- Satellite Quantum Comms
- AI influenced solutions

Thank You

QCALL · QUANTUM COMMUNICATIONS HUB · UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME · EPSRC · MARIE CURIE ACTIONS · HORIZON 2020

UNIVERSITY OF LEEDS

Quantum Networks: Deployment Challenges



Supporting multiple users
- Access mode (wireless or fibre)
- Multiplexing and multiple-access

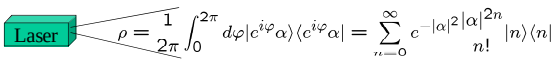
At any distance
- Rate scaling
- Trust issue

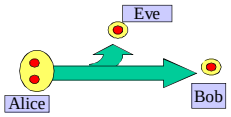
Cost-efficiently!
- Quantum-classical integration
- Chip-based devices
- Mass production and end users
- Inter-generation compatibility

UNIVERSITY OF LEEDS

Single-Photon Sources

- Parametric down-converters
- Quantum dot sources
- Weak laser pulses



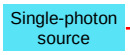


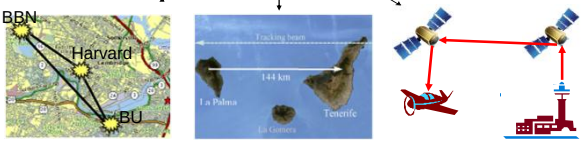
Multi-photon signals

Soln: Use "decoy" states; test channel randomly with different intensities

UNIVERSITY OF LEEDS

Single-Photon Communication: Channels





Fiber-optic channel | Atmospheric channel | Free-space channel

What we have	What we want
QKD over dedicated channel	Over public channels
Cable access	Fibre to the home; wireless access
No standards for hybrid networks	Compatibility with existing optical networks

UNIVERSITY OF LEEDS