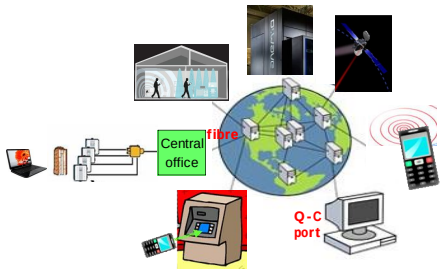
29 Dec 2016

Quantum Communications Technologies: Now and the Future

Mohsen Razavi

Institute of Microwaves and Photonics
School of Electronic and Electrical Engineering
University of Leeds

Quantum-Classical Networks: The Grand Vision



Supporting multiple users, at any distance
classical or quantum,

A glance of the future!

quantum secure

Fiber-to-the-home

* Make sure your QT router is on!

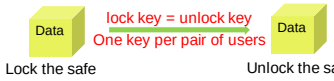
QT: Quantum Telecom

Cryptography 1-0-1

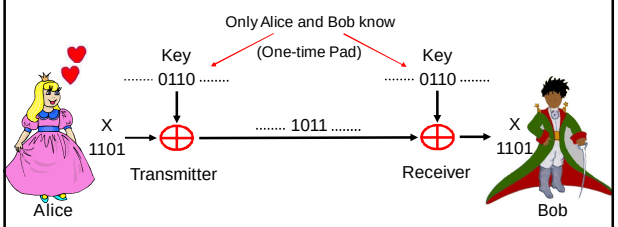
Secure Communication: How two parties can securely communicate?

Two general approaches

- Symmetric-key cryptosystems



Symmetric-key Example: One-time Pad



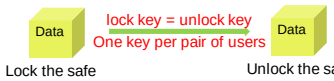
But, how to distribute the secret key to begin with?

Cryptography 1-0-1

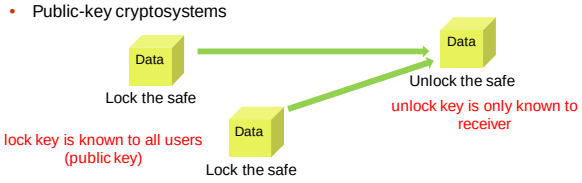
Secure Communication: How two parties can securely communicate?

Two general approaches

- Symmetric-key cryptosystems

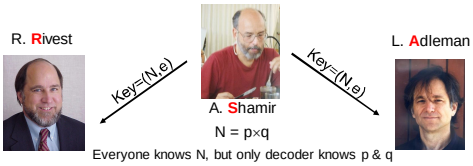


- Public-key cryptosystems



Public-Key Example: RSA Protocol

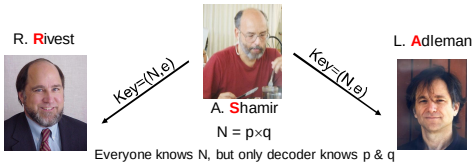
- RSA public-key cryptosystems (1977)



One ideally can exchange a secret key using public key crypto.

Public-Key Example: RSA Protocol

- RSA public-key cryptosystems (1977)



One ideally can exchange a secret key using public key crypto.

Just one issue: RSA is not quantum safe!

Shor's Algorithm: Super-efficient Factoring

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

classical $O((\log N)^{(\log N)^{1/3}}) \longrightarrow O((\log N)^3)$ **quantum**

For the best **known classical** algorithm

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

Summary So Far

- By shrinking the size of electronic devices, we reach a regime in which quantum mechanical laws will rule.
- In that regime, a new paradigm for computing can be developed: Quantum Computing
- There are certain problems for which quantum computers definitely outperform classical computers, e.g., search algorithm
- There are certain problems that quantum computers outperform the best known classical algorithms, e.g., factoring problem.
- A quantum computer can break RSA cryptosystem: a serious threat
- Any cryptosystem that relies on computational complexity, is threatened by technological advancements; many historical examples

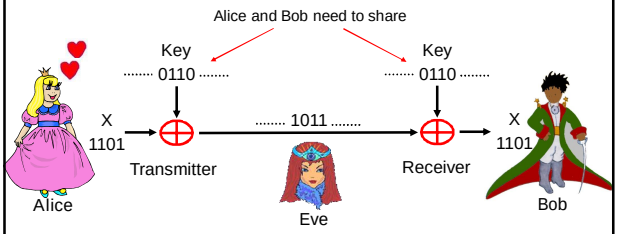
Question: What can be done?

Future-proof Security

- **Key idea:** If we want to be immune against advancement of our computers, our security should not rely on computational complexity
- It could, instead, rely on the laws of nature that are not expected to change with time
- The most reliable model we currently have for the nature is based on quantum mechanics; so, let's develop some *quantum cryptography* tools
- In particular, let's exchange the secret key that we need for our cryptographic protocols in a quantum way.
- Let's develop

Quantum Key Distribution (QKD)

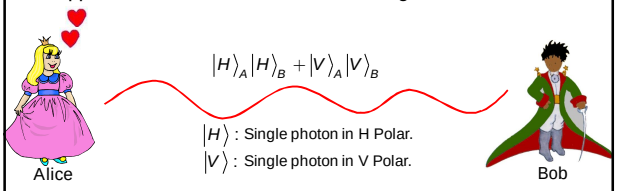
Quantum Key Distribution (QKD)



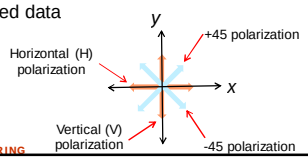
- Key Objective: Alice and Bob want to exchange a secret key in such a way that any eavesdropping attempt can be detected.
  - In cryptography, Eve considered to have all imaginable computational power; she has full control over the channel, too
  - Eve's goal is not to disrupt the connection (no info for her), but to steal information without being detected (like a spy)

Entanglement-Based QKD

- Suppose Alice and Bob share an entangled state

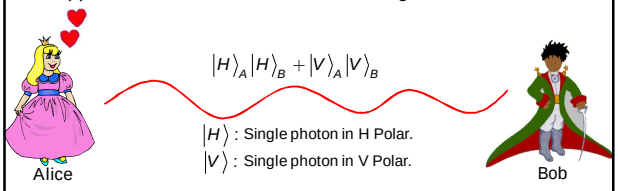


- They can each measure their photon in H-V basis to get random but correlated data



Entanglement-Based QKD

- Suppose Alice and Bob share an entangled state

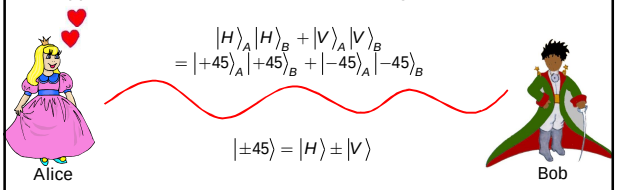


- They can each measure their photon in H-V basis to get correlated data
- But what if Eve has entangled a photon with Alice-Bob state?

$$|H\rangle_A|H\rangle_B|H\rangle_E + |V\rangle_A|V\rangle_B|V\rangle_E$$

Monogamy of Entanglement

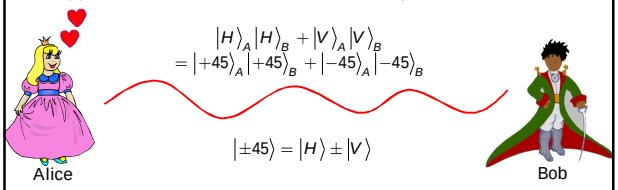
- Suppose Alice and Bob share an entangled state



- Every now and then, they should measure in ±45 basis

Monogamy of Entanglement

- Suppose Alice and Bob share an entangled state



- Every now and then, they should measure in ±45 basis
- Monogamy of Entanglement: Only a true bipartite entangled state gives correlated data no matter what basis is chosen (so long as Alice and Bob both measure in the same basis)

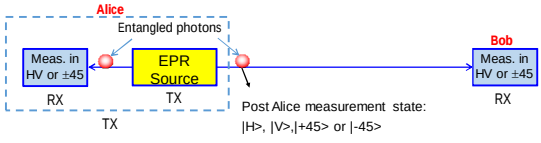
$$|H\rangle_A|H\rangle_B|H\rangle_E + |V\rangle_A|V\rangle_B|V\rangle_E$$
$$\neq |+45\rangle_A|+45\rangle_B|+45\rangle_E + |-45\rangle_A|-45\rangle_B|-45\rangle_E$$

The rest of the protocol

- Q: How do we make sure that Alice and Bob has chosen the same measurement basis?
- A: Sifting; they have to communicate over a public channel and exchange basis data → Sifted key
- Q: How Alice and Bob know that they are talking to each other?
- A: they need to authenticate their messages → They need a secret key in advance → QKD is a key extension protocol
- Q: What if there are errors in the system?
- A: We can use error correction techniques → Identical key
- Q: What if some information is leaked to Eve?
- A: We can use privacy amplification techniques to reduce Eve's information about the key → Secret key
- Q: What if too much information is leaked to Eve?
- A: We can abort the protocol → No key!

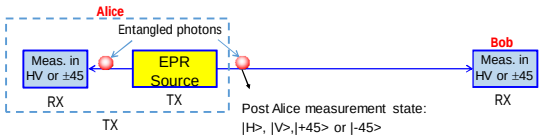
Can we do QKD without Entangled Photons?

- Suppose Alice has an EPR Source

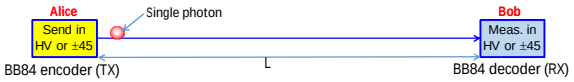


Can we do QKD without Entangled Photons?

- Suppose Alice has an EPR Source

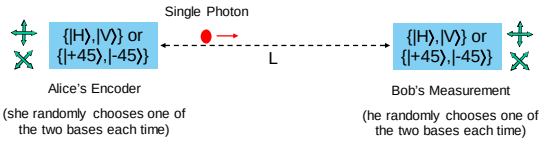


- We can then alternatively just encode a single photon and send it to Bob



BB84 (Bennett-Brassard 1984) Protocol

- Bennett-Brassard Protocol (BB84)
- First, for the ideal channel

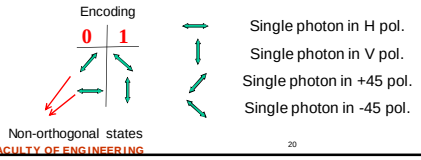


Alice's Encoder

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

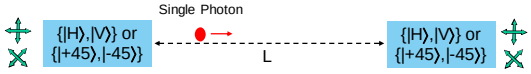
Bob's Measurement

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



QKD: Practical Issues

- Bennett-Brassard Protocol (BB84)



Alice's Encoder

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

Bob's Measurement

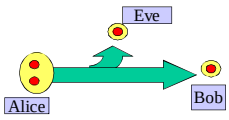
(he randomly chooses one of the two bases each time)

- Security: any tampering with the single photon can be detected by Alice and Bob
- Information encoded on a single photon (phase or polarization)

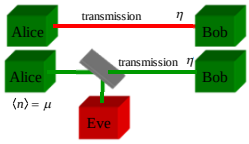
Single-Photon Communications

Challenge 1: Single-photon Generation

- Q1: How to generate single photons? Use 2-level transitions
- Q2: Do we need to generate exact single photons? Not really. We can use weak laser pulses, but with a trick.



Multi-photon signals

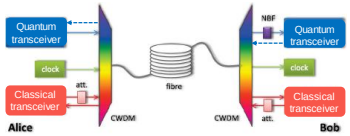


Beam splitting attack

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

Challenge 2: Shared Infrastructure

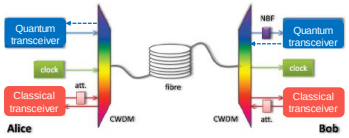
- For cost efficiency, QKD must share infrastructure with classical networks.
- Classical channels carry strong signals; even a small leakage could mask our single photons.



[PRX 2, 041010 (2012)]

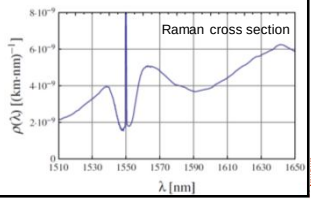
Multiplexing Quantum and Classical in WDM Setups

- Coexistence of classical and quantum signals over the same medium



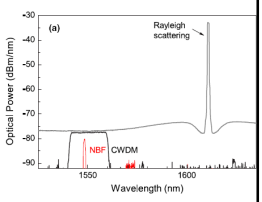
[NJP 12, 063027 (2010)]

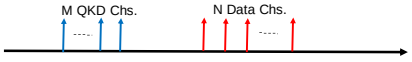
- Key challenge: Raman scattering



Solutions used

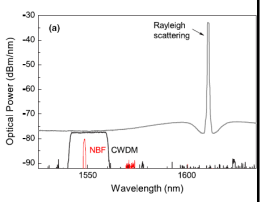
- Extensive filtering: narrowband filters with 15 GHz bandwidth has been used
- Proper time gating: We leave the detector on only when we expect a photon; pulse widths around 100 ps
- Power control: We set the data channels power to the minimum required to meet a BER target
- **Wavelength allocation:** Conventionally lower wavelengths are assigned to QKD channels





Solutions used

- Extensive filtering: narrowband filters with 15 GHz bandwidth has been used
- Proper time gating: We leave the detector on only when we expect a photon; pulse widths around 100 ps
- Power control: We set the data channels power to the minimum required to meet a BER target
- **Wavelength allocation:** But the wavelength assignment can be optimised to reduce cross talk

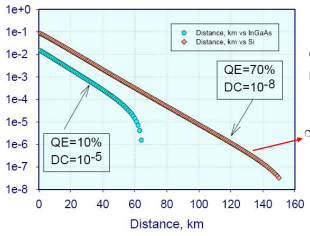


[Scientia Iranica, (2016)]

Challenge 3: Loss

- Our single photons should travel through the channel and reach Bob
- Our best option for an optical channel is optical fibre with a typical loss of 0.2 dB/km. That is 20 dB loss for a 100-km-long channel.

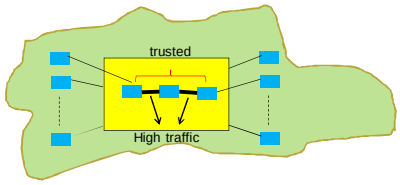
Prob. of generating a single key bit for a weak laser pulse



QE: Quantum efficiency
DC: Dark count

$\propto \exp[-L / L_{att}]$

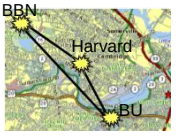
Long-distance QKD: Short-term Solution



One possible architecture for the core network: a mesh of **trusted** interconnected nodes

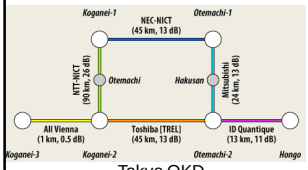
- Keys can be exchanged between neighboring nodes; they can then securely relay the original key
- Drawback: Majority of intermediate nodes must be trusted
- Possible solution: We can exchange key via multiple routes; if nodes are non-cooperative, the trust requirement can be alleviated.

Trusted-Node QKD Networks: Implementations



DARPA QKD Network, 2004

SECOQC QKD Network, 2008

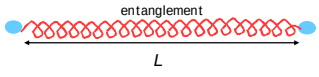


Tokyo QKD Network, 2010

China Beijing-Shanghai link coming soon …

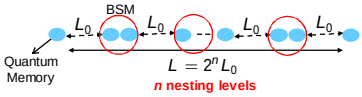
Long-distance QKD: Long-term trust-free solution

- If we want to be trust-free, we can use entanglement-based QKD
- Then the question is how to extend entanglement over long distances
- Direct distribution has no luck!



$R(L) \propto \exp[-\alpha L]$ ← Channel loss

- Let's break the link into multiple shorter sublinks



Briegel, Dür, Cirac & Zoller, PRL 1998

$R(L) \propto \exp[-\alpha L_0]$

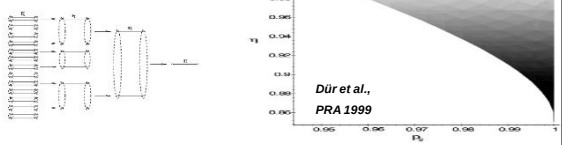
Different Approaches to Quantum Repeaters

$L = 2^n L_0$

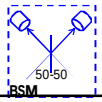
n nesting levels

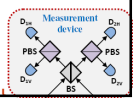
Briegel, Dür, Cirac & Zoller, PRL 1998

- Deterministic: BSM and purification processes are all deterministic, although, not necessarily, error free



- Probabilistic: BSM or purification processes are probabilistic; we sometime get inconclusive results
  - Rely on linear optics & photodetection





1000-km Repeater Link

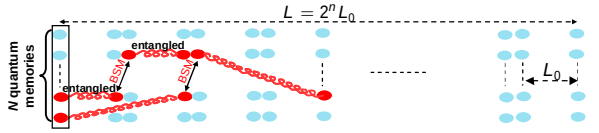
Probabilistic Quantum Repeaters

- Single-memory per node
  - 1. attempt to simultaneously distribute entanglement between adjacent pairs
  - 2. perform as many informed BSMs as possible at nesting level 1; send the results to the next nesting station; the same for higher nesting levels
  - 3. release memories after use
  - Go to step 1

In order to do BSM2, the two BSM1 must succeed, and BSM2 must know about that

- **Repeat period** limited by initial entanglement distribution to L_0/c
- Transmission delay to inform one nesting level of the result of the previous one → required **coherence time** scales with the total transmission delay
- The success rate is low

Multiple-Memory Configuration

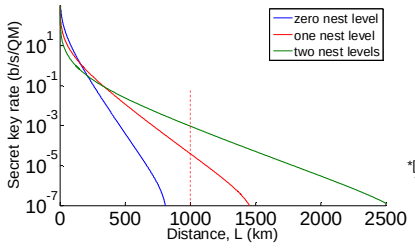


MR, M. Piani, and N. Lütkenhaus, PRA **80,** 032301 (2009)

- Successive mode of operation with cycle period $T_0 = L_0/c$:
  - 1. attempt to simultaneously distribute entanglement between unused pairs of memories over shortest segments
  - 2. perform as many informed BSMs as possible according to nesting protocol
  - 3. release memories after use
  - Go to step 1
- Key Figures of Merit
  - Required coherence time
  - Required #memories for a desired rate, or $\frac{\text{Key Rate}}{\text{\# mems}}$

Quantum Repeaters: Required # Memories

- How many memories needed for 1 key bit/s at 1000 km?
  - Entanglement-distribution scheme relies on single photon sources with a double-photon probability as low as 0.0001 [PRA **76,** 050301 (2007)]



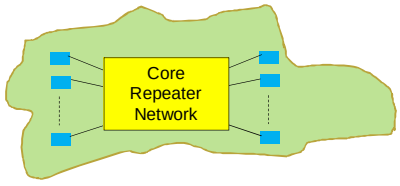
QE = 0.93*
$T_2 \rightarrow \infty$
and other optimistic assumptions

*[Nature Photon. **7,** 210 (2013)]

- We still need 1000 logical memories

Quantum Repeaters: Required # Memories

- How many key bit/s do we need to generate in a network setup?

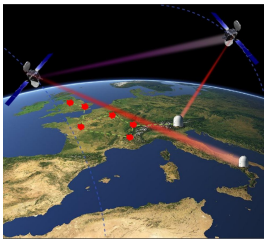


Design Criteria:

- Any two users can exchange a secret key
- It is desired to not rely on trusting intermediate nodes
- Classical and quantum signals both use the same infrastructure
- Low-cost components at the user's end

Long-distance QKD: mid-term solutions

- There are other classes of quantum repeater with better performance but even more demanding requirements
- In the next talk, we will look at mid-term solutions that can offer some advantages despite device imperfections: memory-assisted QKD
- Other Mid-term solutions: satellite QKD



Future Trends in Quantum Communications

NOW

1M key bits/s over
50 km of fiber

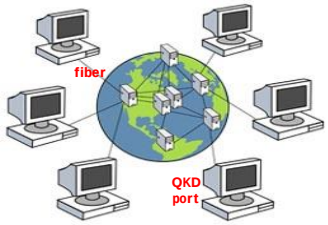
Used in Geneva
voting system (2007)

SOON LATER

Prototype built by
HP Labs Bristol

Future Trends in Quantum Communications

- **Bringing QKD to daily life**
  - Increasing key generation rate, MHz → GHz, by improving the sources, the detectors, and protocols
  - Reducing the cost and the size
  - QKD networks
- **Beyond QKD protocols**



Summary

- New Quantum Applications are on the rise. They will affect
  - How securely we can exchange information
  - How precisely we can measure
  - How fast we can compute
- Quantum Communications
  - Enables secure communications in the quantum era
  - Teaches us about the fundamental limits of our systems
  - And takes us beyond that by teleporting us to new horizons!
  - But, it will not replace our high-data-rate systems!
- If you are interested, PhD positions are available via the European project QCALL.

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME
QUANTUM COMMUNICATIONS HUB
HORIZON 2020

PhD Positions in Europe!

QCALL is a European Innovative Training Network (ITN) that offers 15 extremely well-funded PhD positions on various topics related to quantum communications

- 3 years of funded PhD research with annual salaries > €43k and research budget > €60k per student
- Dedicated schools on QKD and quantum networks + complementary-skill training + extensive internship/placement programmes
- Eligibility: meeting mobility criterion + being an early-stage researcher
- PhD start date: Early 2017 – Oct 2017; Deadline for application: **15 Jan 2017**

http://www.qcall-itn.eu

Partners:

- **ID Quantique:** 1 project on quantum hacking; contact *F Brussieres*
- **Telecom ParisTech:** 1 project on Hybrid CV QKD; *R Alleaume*
- **Toshiba Research Europe Ltd:** 2 projects on MDI-QKD and Integration; *A Shields*
- **University of Dusseldorf:** 2 projects on repeaters and multipartite entanglement; *D Bruss*
- **University of Geneva:** 2 projects on QKD and quantum memories; *H Zbinden*
- **University of Leeds:** 2 projects on MDI-QKD and repeaters; *M Razavi* (**Coordinator**)
- **University of Padova:** 2 projects on satellite QKD and QRNGs; *P Villoresi*
- **University of Pierre and Marie Curie:** 1 project on beyond-QKD protocols; *E Diamanti*
- **University of Vigo:** 2 projects on security of QKD and beyond-QKD protocols; *M Curty*
- Plus collaborative partners at **BBN**, **Heriot-Watt**, **Inria**, **IQC**, **Madrid**, **Max Planck** & **NTT**