UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

QUANTUM COMMUNICATIONS HUB

EPSRC
Engineering and Physical Sciences Research Council

Quantum Communications (and their implications for Information Security)

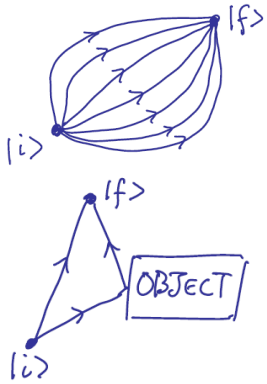
The Quantum Communications Hub
Director: Professor Tim Spiller

UNIVERSITY of York

New Quantum Technologies

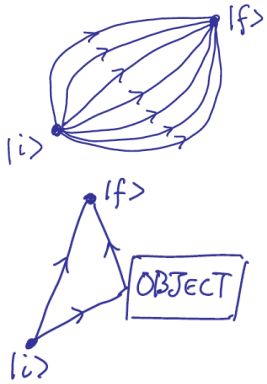
- Quantum technologies form a whole new technology sector.
- These technologies handle information in a radically different manner from their conventional counterparts, because their operation is underpinned by fundamental features of quantum physics.
- Due to this, quantum technologies have novel abilities and the potential to outperform their conventional counterparts.
- Examples, particularly relevant for security…

New Quantum Technologies



- Quantum Superposition (of calculations) enables better computing!
- Quantum entanglement enables better sensing and imaging!
- Quantum uncertainty enables new secure communications!

New Quantum Technologies



- Quantum Superposition (of calculations) enables better computing!
- Quantum entanglement enables better sensing and imaging!
- Quantum uncertainty enables new secure communications!

- Utilises light as the carrier…

National Network of Quantum Technologies Hubs

The four Hubs:

- Quantum Technology Hub in sensors and metrology:
  Birmingham-led; focus on atoms

- Quantum Enhanced Imaging (QuantIC):
  Glasgow-led; focus on light

- NQIT Networked Quantum Information Technologies:
  Oxford-led; focus on ion traps and photonics

- Quantum Communications Hub:
  York-led; focus on QKD applications

Quantum Communications Hub

- £24M funding (capital and recurrent) + £2M additional capital.

- Our vision is to develop new technologies that will reach new markets, enabling widespread use and adoption in many scenarios – from government and commercial transactions through to consumers and the home.
- Through our technology demonstrators we will welcome trial or pilot tests, as part of our user engagement programme.

Quantum Communications Hub: Partners

Academic partners:

- York (lead), Bristol, Cambridge, Heriot-Watt, Leeds, Royal Holloway, Sheffield, Strathclyde

Industrial partners:

- R&D: Toshiba Research Europe Ltd. (TREL), BT and the National Physical Laboratory (NPL)
- Network: ADVA, ID Quantique, NDFIS
- Supplier/Consultancy (optical): Oclaro, ID Quantique
- Collaboration/Consultancy (microwave): Airbus, L3-TRL
- Start-ups (exploitation): Qumet, KETS (Bristol), Cryptographiq (Leeds/IP Group)
- Standards/Consultancy: ETSI, GCHQ (NCSC)
- User engagement: Bristol City Council, Knowle West Media Centre, Cambridge Science Park, Cambridge Network Ltd, BT Adastral Park

Partnership Resource:

- Cambridge Quantum Computing, Glasgow/QuantIC, Oxford/NQIT, National STEM Learning Centre, York Science Education Group

Quantum Key Distribution (QKD)

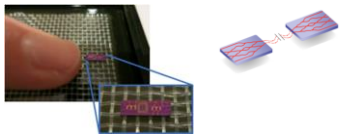
Secure sharing of a key between two parties (Alice and Bob!)

- The quantum part is the distribution of the key, with a promise from quantum physics that only Alice and Bob have copies.
- Once distributed, the (non-quantum) uses of the key(s) cover a wide range of secure information tasks: communication or data encryption, financial transactions, entry, passwords, ID/passports…
- The keys are consumables (use once only for security), so need regular replenishment, which is “quantum”.

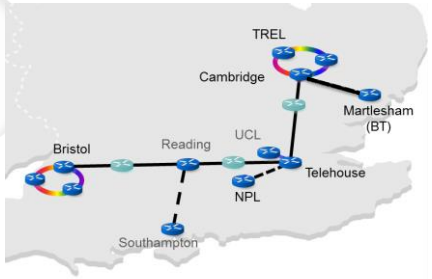
Quantum Communications Deliverables

- Handheld Alice (credit-card size or 'phone compatible) for consumer applications

- Chip-based Alice and then Bob modules



- Establishment and operation of the UK Quantum Network and user-engagement



- "Next-generation" (beyond QKD) technologies demonstrated on the UKQN

New Quantum Technologies and their implications for Information Security

- Cryptanalysis with quantum computers will render PKI (RSA, elliptic curves…) vulnerable.
- New quantum sensors will enable us to detect and image things beyond current limits.
- Despite both of these, new secure quantum communications technologies are being developed. New mathematical encryption techniques immune to quantum computer attack are also being sought.

- Secure communications in the future may well be based on a combination of new quantum and conventional technologies – "quantum safe".

Further Quantum Information

- The Quantum Communications Hub:
- www.quantumcommshub.net/

- The UK National Quantum Technologies Programme:
- http://uknqt.epsrc.ac.uk/

- Quantum Technologies: Blackett Review
- https://www.gov.uk/government/publications/quantum-technologies-blackett-review

- QT Showcase: QEII Centre London, Friday 15 November 2019
- https://qtshowcase2019.eventbrite.co.uk