National Network of Quantum Technologies Hubs:

Quantum Communications Hub

Director: Professor Tim Spiller

University of York
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, NDFIS
- Supplier/Consultancy (optical): Oclaro, ID Quantique
- Collaboration/Consultancy (microwave): Airbus, L3-TRL
- Start-ups (exploitation): Qumet (Bristol), Cryptographiq (Leeds/IP Group)
- Standards/Consultancy: ETSI, GCHQ
- User engagement: Bristol City Council, Knowle West Media Centre, Cambridge Science Park, Cambridge Network Ltd
Quantum Communications Hub

Vision:
“To develop new quantum communications (QComm) 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.”

Delivery:
• First generation: Take proven concepts in Quantum Key Distribution (QKD) and advance these to commercial-ready stages. (Work packages 1-3)
• Next generation: Explore new approaches, applications, protocols and services – beyond QKD. (Work package 4)
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 Hub: Work packages

- **WP1** Short Range Consumer QKD  (WP Lead: John Rarity (Bristol))
  - Near infra red, line-of sight
  - Microwave
- **WP2** Chip Scale QKD Components (WP Lead: Mark Thompson (Bristol))
  - Chip scale optics
  - Network switches
- **WP3** Quantum Networks (WP Lead: Andrew Shields (TREL))
  - Quantum Core Networks
  - Quantum Metro Networks
  - Quantum Access Networks
- **WP4** Next Generation QComm (WP Lead: Gerald Buller (Heriot-Watt))
  - Quantum digital signatures
  - Quantum Relays, Repeaters and Amplifiers
  - Device Independent and Measurement-device independent QKD
Quantum Communications Hub: Work packages

Fig 1: The relationship between the Hub Work Packages and activities. Expertise, components and devices will flow between WPs and in from external partnerships and collaborations using the Partnership Resource, all contributing to Tech Transfer.

Tech Transfer and Commercialisation
Expertise, Component and Device Flow
WP1: Quantum secured key exchange for consumers

Could use one-time-pad to protect the PIN.
Generate one-time-pad using quantum secured key exchange.
Key exchange at ATM allows user to ‘top-up’ a personal one-time-pad.
WP1: Why?

- Weekly ‘top-up’ a personal one-time-pad into a personal phone/card.
- Protects against ‘skimming’
- Type your PIN into YOUR device
- Absolute security for PIN online
- Low cost: free to all customers

The competition:

- Present readers provide simplistic security based on ‘toy’ codes.
- In shops: data between card and reader NOT encrypted during a transaction, PIN is sent in the clear!

See [http://www.cl.cam.ac.uk/~sd410/](http://www.cl.cam.ac.uk/~sd410/)
See also google/vodafone: phone=wallet
Bob meets Alice
WP1: The credit card Alice

New System:
Target 3x20x40mm Alice
>100MHz operation
WP1: Flexible receiver and software concept:

Standard 19” rack system with replaceable receiver and software sub-units
WP2 Vision: Chip-based Qcomms devices

Current approach

Integrated quantum photonic Qcomms chip

1mm
WP2: Compact chip-based QKD

- Chip-based devices for:
  - Low cost
  - Compact
  - Energy efficient
  - Mass-manufacture
  - Compatibility with current microelectronic devices

- Hub will target:
  - Fully integrated and packaged QKD devices with control electronics
  - Deployment in real networking situations
WP2: Targeted Applications

- Mobile devices
- Computer networks
- City wide communications network
WP2: Chip-based QKD/WDM switches

- Compact switching device for reconfigurable quantum networks
- InGaAsP devices based on Clos switching architecture
WP3: Quantum Networks

Today: Point-to-point fibre QKD links
WP3: Quantum Networks

- Explore integration of QKD in different network segments (long-haul, metro, access)
- Key management and security analysis of extended trusted node network
- Application development, eg layer 3 encryption, quantum digital signatures
- Multiplex quantum signals on conventional DWDM grid
- Provisioning of quantum and data channels
WP3: UK Quantum Network

- Establish large-scale Quantum Network test-bed in UK

Implemented in stages

- Metro networks in Cambridge and Bristol

- Long-haul network connecting Cambridge-London-Bristol (NDFIS) with possibility to extend

- Access networks providing multi-user connectivity

A focus for application development, industrial standardisation and user engagement

- Potential test-bed for the other QT Hubs and associated projects
WP 4: Emerging Quantum Communications Technologies

Quantum Digital Signatures
*Information Theoretic Secure Digital Signatures*

Quantum Repeaters
*Amplifiers for Quantum Communications Systems*

**Measurement Device Independent Quantum Key Distribution**
*Cryptographic Key Exchange in an Untrustworthy World*
Quantum Comms Hub: Theory and Security Analysis

- Contributes to all four Technology Workpackages:
  - Identify and remove security vulnerabilities at an early stage
  - Contribute to ETSI standards for QKD and other Qcomm systems

- Physical level security analysis
  - Match physical models for analysis to practical implementations
  - Widely applicable channel analysis with side channel information leakage studies
  - Analysis of attacks and countermeasure design

- Protocol level security analysis
  - Analysis of protocol stacks, incorporating low-level quantum and higher level conventional protocols
  - Analysis of practical security advantages of new protocols such as QDS and MDIQKD
  - “Quantum-immune” conventional (classical) protocols

- Hybrid system analysis
  - High speed (Gb/s upwards) systems combine QKD and conventional secure communications protocols, trading unconditional and forward security for speed
  - Detailed security analysis of such hybrid systems (and mitigation against security “loss”) is needed
Quantum Communications Hub: Work package targets

- “Commercial-ready” QKD technologies...
- **WP1 Short Range Consumer QKD**
  - Handheld system, leading to minimal mobile phone modification for Alice
  - Microwave quantum secure communications analysed and demonstrated
- **WP2 Chip Scale QKD Components**
  - Chip scale Alice with semi-bulk Bob, leading to fully packaged chip scale QKD optical modules
  - Network switches demonstrated on the UKQN
- **WP3 Quantum Networks**
  - High bit rate link encryption
  - Quantum Metro Networks demonstrated in Bristol and Cambridge
  - Establishment and operation of the UKQN
- **WP4 Next Generation Quantum Communications**
  - Quantum digital signatures deployed at Metro Network level
  - Quantum Relays/Repeaters for weak pulse QKD demonstrated on UKQN
  - Device Independent and Measurement-device independent QKD deployed at QAN level