UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME

UK QUANTUM TECHNOLOGY HUB

FOR QUANTUM COMMUNICATIONS TECHNOLOGIES

ANNUAL REPORT

2016 2017

QUANTUM
COMMUNICATIONS
HUB

Contents

Special thanks to all contributors:

Klitos Andrea, Gerald Buller, Christopher Chunnilall, Caroline Clark, Roger Colbeck, Chris Erven, Jake Kennard, Georgia Mortzou, John Rarity, Andrew Shields, Philip Sibson, Tim Spiller, Mark Thompson, Adrian Wonfor.

Thanks to Iris Choi, Caroline Clark, Andy Hart, David Lowndes, Kantar Public, Adrian Wonfor, the Quantum Photonics Laboratory team at Heriot Watt University, and Emma Smith and the Centre for Quantum Photonics team at the University of Bristol for kindly providing images.

Foreword

The Quantum Communications Hub, led by the University of York, is a technology research and development consortium of Universities, industrial partners and public sector stakeholders. Funded through the UK National Quantum Technologies Programme, its main aim is to exploit fundamental laws of quantum physics for the development of secure communications technologies and services.

Technological progress in 2017, our third operational year, was sustained and built upon previous developments. We continued to develop QKD technologies over short distances and in free-space while also adding hand tracking functionality to terminal devices, through a collaboration with the NQIT Hub. Following our world first chip-to-chip QKD demonstration, we fabricated and successfully demonstrated a range of integrated devices including high performance QKD transmitters in the silicon-on-insulator platform; we also continued to explore the incorporation of compactness with high performance in quantum random number generators. Various links across the UK's first quantum network are gradually becoming operational, demonstrating long-term stability coupled with generation of high secure key rates successfully trialled on the Cambridge metropolitan network, in parallel with secure tunnel applications and successful distributed denial of service mitigation using software defined networking on the Bristol equivalent. In the next generation technologies theme, work focused on the development of a miniaturised optical chip-based state comparison amplifier designed for enhanced performance, as well as the implementation of a quantum relay using a quantum dot emitter aimed at securing compatibility with optical communications networks.

With technological progress on track and ahead of targets, 2017 marked a strengthening of our user engagement activities across the board: we organised two major international events, the 7th International Conference on Quantum Cryptography in Cambridge and the 5th ETSI/IQC Quantum Safe workshop in London, while also taking part in the third national quantum technologies showcase. We invested in many more projects using our partnership resource funding, expanding the capabilities and expertise of the Hub ahead of further future developments, including as part of a possible second phase of the national programme. And we continued to engage with the public, through numerous science festivals demonstrations and talks, and more importantly, by contributing along with the rest of the Hub Network to a specially designed and commissioned public dialogue exercise.

We are excited to be sharing our work with you and look forward to further engagement opportunities in the future.

Professor Timothy P. Spiller, MA PhD CPhys FInstP
Director, UK Quantum Technology Hub for Quantum Communications Technologies
Director, York Centre for Quantum Technologies

Quantum Key Distribution

Fundamental to the Hub's objectives is Quantum Key Distribution (QKD), a currently available technology for the secure distribution of secret keys, which can be used for data encryption and other applications. Standard communication scenarios usually involve transmitter and receiver units, traditionally described as "Alice" and "Bob" respectively. Quantum physics dictates that at the scale of individual particles (such as photons which are the particles that comprise light), their quantum properties cannot be measured without being unavoidably and irrevocably disturbed from their original state. This means that no interceptor (or hacker – routinely described as "Eve" in such scenarios) can eavesdrop on quantum transmissions, without their presence becoming known to Alice and Bob. This disturbance is due to quantum uncertainty and it is a fundamental feature of quantum physics. It underpins all current work in the field of quantum secure communications.

Although immediately detectable, the presence of an eavesdropper can still be disruptive, for example through denial of service attacks. Nevertheless, when service is not denied, from the information communicated Alice and Bob can distil random data (the "key") that only they know. QKD systems generate such shared secret keys, which can then be used for data encryption and other applications based on conventional communication techniques. The key generation, distribution and replenishment is underpinned by quantum uncertainty, thus offering to any two communicating parties security based on the laws of quantum physics.

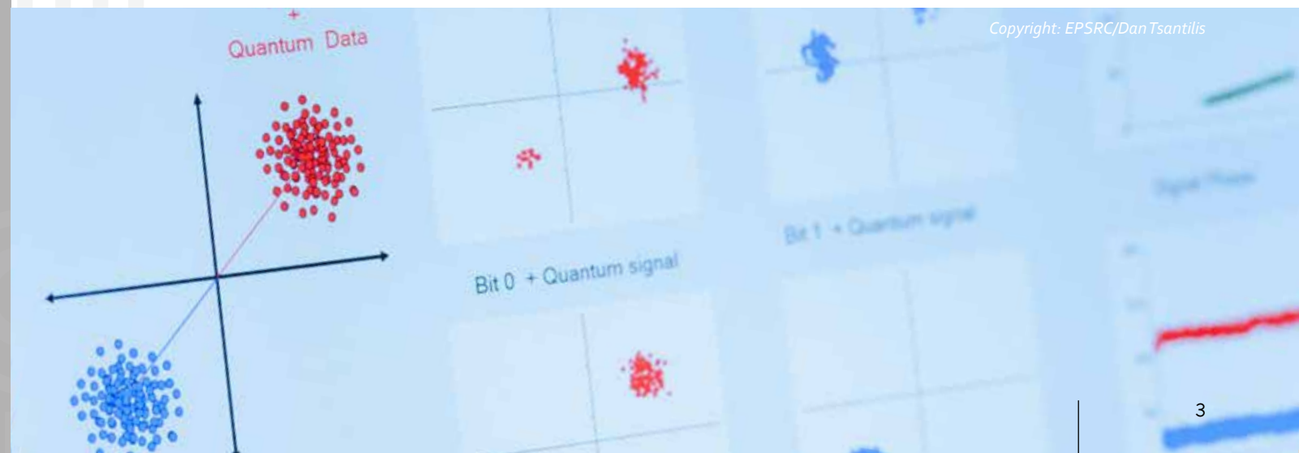
Introduction

The Quantum Communications Hub is a £24m technology research and development consortium of UK Universities, private sector companies and public sector stakeholders, funded as part of the UK National Quantum Technologies Programme. Our vision is to develop quantum secure communications technologies for new markets, enabling widespread use and adoption – from government and commerce through to consumers and the home. Using proven concepts such as quantum key distribution (QKD), our objective is to advance these to a commercialisation-ready stage. Specifically, we are delivering:

- **Short-range, free-space, QKD systems:** these technologies will enable many-to-one, short-range, quantum-secured communications, for consumer, commercial and defence markets. We are working to deliver a credit card sized QKD transmitter linked to a rack-size (wall mounted ATM-like) QKD receiver to allow secure key sharing between a phone and terminal with minimal modification of phone hardware.
- **"QKD-on-a-chip" modules:** scaled down and integrated QKD component devices, for producing robust, miniaturised sender, receiver and switch systems - "QKD-on-a-chip" modules. These advances address cost, energy-efficiency and manufacturability issues, to enable widespread, mass-market deployment and application of QKD.
- **Establishment of a UK Quantum Network:** which integrates QKD into secure communication infrastructures at access, metropolitan and inter-city scales. We are building metro-scale networks in Bristol and Cambridge and will link these to the National Physical Laboratory in London utilising the National Dark Fibre Infrastructure Service (NDFIS), to form a UK Quantum Network. This national facility will be used for device and system trials, integration of quantum and conventional communications, and demonstrations for stakeholders, end users and the wider public.

Furthermore, we are undertaking work in **"next generation" quantum communications technologies,** so approaches which go beyond current QKD technologies and address some of their limitations. We are exploring: (i) development and implementation of quantum signatures and other protocols in order to address areas of the security application space not covered by QKD; (ii) development of quantum amplifier and repeater demonstrators, addressing the current distance limitations of QKD; (iii) development of measurement-device-independent (MDI) QKD technologies, to address some of the side channel vulnerabilities that exist in current QKD implementations. Side channel and security analysis, novel protocols, network architecture design and analysis, virtualisation and modelling are additional areas being pursued to support the Hub technology goals.

In combination, these four technology themes are designed to deliver our vision, both establishing a quantum communications technologies industry for the UK and feeding its future expansion, diversification and sustainability.



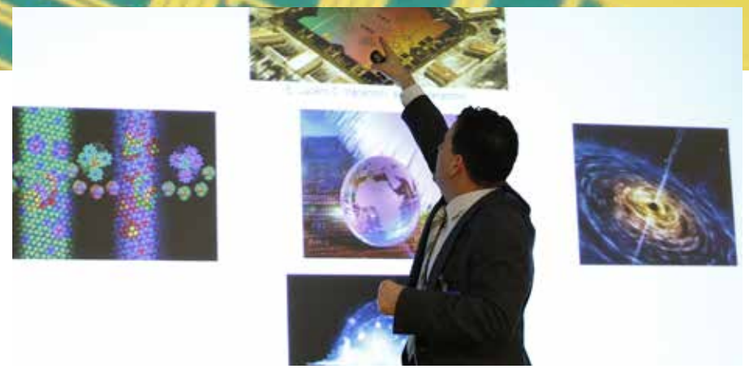
Overview: The Third Year

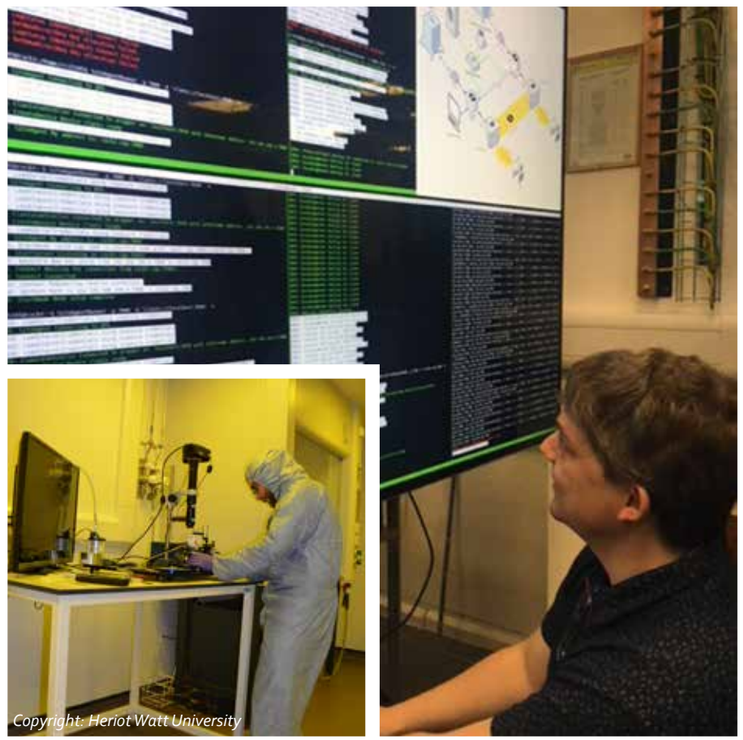
With the technical work progressing well ahead of targets, in the third year we placed the focus firmly on user and external engagement: QCrypt'17, the 5th ETSI/IQC quantum safe workshop, the 3rd national showcase were all major events which we co-organised and where the Hub had the opportunity to demonstrate technical achievements to date. At the same time, the partnership continued to grow through: new partners brought in via our flexible resource funding; the extension of the Cambridge to Adastral Park quantum link, which is nearing completion; and a number of new doctoral students who have joined the Hub through the doctoral training partnerships funding scheme.

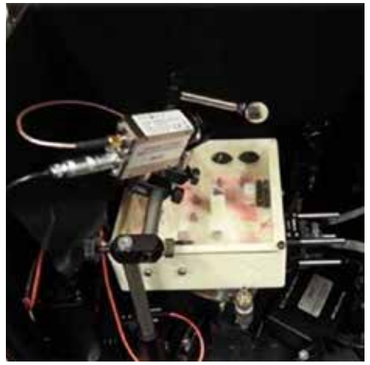
In the third year we have:

- Continued to make significant progress across all technology themes
- Installed QKD equipment on three links along the Cambridge metro network and have been running the system with high rates of secure keys and without any user interruption for more than 6 months
- Completed preparatory work on the infrastructure of the Cambridge to Adastral Park quantum network link in advance of deployment of equipment in the field for testing
- Hosted the largest ETSI/IQC Quantum Safe Cryptography Workshop to date in London
- Organised the annual Qcrypt research conference – the major international event in quantum cryptography, and the largest to date, attended by over 300 delegates
- Took part in a major public dialogue exercise commissioned by the Engineering and Physical Sciences Research Council on attitudes towards quantum technologies
- Funded a major 2-year programme of work to deliver in collaboration with the whole Network of Hubs a quantum ambassadors scheme of class-based activities for secondary school students and educators
- Invested over £500k in new partnership resource projects
- Established nine PhD studentships on subjects relevant to the work of the Hub through the EPSRC's Doctoral Training Partnerships scheme
- Continued to develop international links with research visits to Italy and the US
- Delivered presentations on our work in more than 70 conferences, workshops, industry and user engagement events, both in the UK and abroad
- Published more than 30 research papers, book chapters, and conference abstracts, and submitted a further 16 for peer review
- Participated in numerous public engagement events while continuing to disseminate our work through social media

Copyright: University of Bristol







Copyright: Heriot Watt University

The Partnership

Heriot-Watt University

National Cyber Security Centre
a part of GCHQ

TOSHIBA
Leading Innovation

AIRBUS
DEFENCE & SPACE

ADVA
Optical Networking

Cambridge Network

University of Cambridge

Bristol City Council

BT

Royal Holloway University of London

Cambridge Quantum Computing

IDQ
FROM VISION TO TECHNOLOGY

University of Leeds

ETSI

NDFIS
National Dark Fibre Infrastructure Service

OCLARO

KETS
QUANTUM SECURITY

University of Strathclyde Glasgow

The University Of Sheffield.

University of Bristol

TRL Technology
one step ahead

University of York

NPL
National Physical Laboratory

STEM
LEARNING

University of York
Science Education Group

QUANTUM COMMUNICATIONS HUB

Management & Leadership

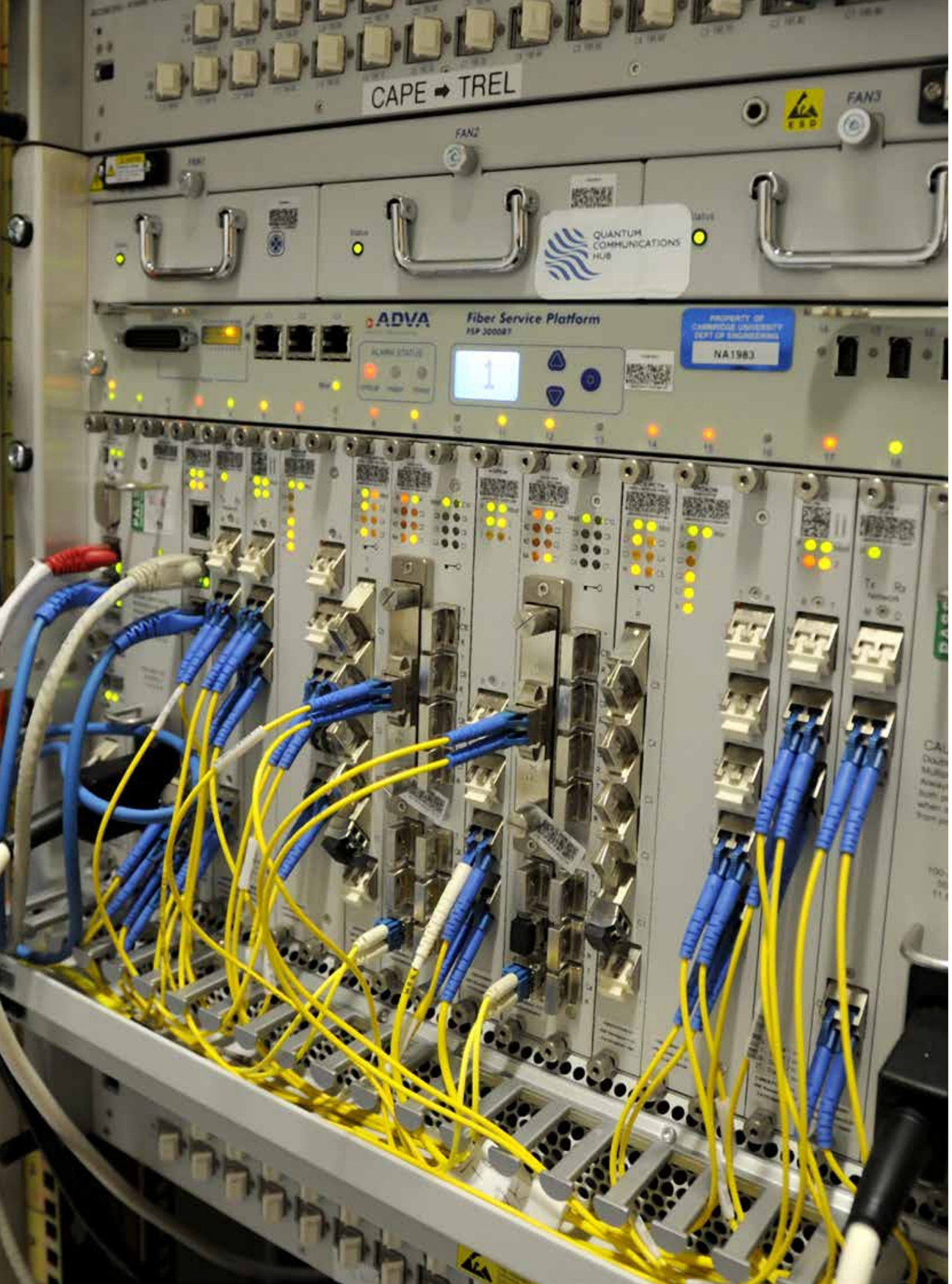
Tim Spiller, MA PhD CPhys FInstP, is Professor of Quantum Information Technologies at the University of York, founding Director of the York Centre for Quantum Technologies (since 2014), and Director of the Quantum Communications Hub. Prior to this appointment, he was at the University of Leeds in the roles of Head of the Quantum Information Group and Director of Research for the School of Physics and Astronomy. Prior to 2009, Spiller was Director of Quantum Information Processing Research at HP Labs Bristol – an activity that he established in 1995 – and a Hewlett-Packard Distinguished Scientist. He has spent 35 years researching quantum theory, superconducting systems and quantum hardware and technologies. He led HP's strategy on the commercialisation of QIP research, and is an inventor on 25 patents linked to quantum technologies and applications.

John Rarity, MSc PhD FRS, is Professor of Optical Communications Systems and Head of the Photonics Group in Electrical and Electronic Engineering at Bristol. He is a founding father of quantum technologies (QT), including the first experiments in path entanglement, QKD, multiphoton interference and quantum metrology, recognised by the 1994 IoP Thomas Young Medal. He has been reviewer/advisor for EU projects and prestigious international projects. He has contributed to the formation of QT research in Europe through various advisory panels (Pathfinder, ACTS), and has led EU consortia, and teams in several large projects. He and colleagues were awarded the Descartes Prize in 2004 for the project QuComm. He has published >120 papers with >9000 citations. He holds an ERC Advanced fellowship, and in 2015 Rarity was awarded an EPSRC established career fellowship, while he was also elected a Fellow of the Royal Society.

Mark Thompson, MSc PhD, is Professor of Quantum Photonics, Director of the Quantum Engineering Centre for Doctoral Training at Bristol and Deputy Director of the Centre for Quantum Photonics. He holds an EPSRC Early Career Fellowship and is pioneering the emerging field of silicon quantum photonics. He has over ten years' industrial experience in photonics, working with Corning Cables Ltd, Bookham Technology Ltd and Toshiba, and was awarded the 2009 Toshiba Research Fellowship. He is world-leading in the development of advanced integrated quantum circuits, and was awarded the 2013 IET researcher award for his contribution to this field.

Andrew Shields, PhD FInstP, FREng, is Assistant Managing Director at TREL Cambridge Research Laboratory. He directs Toshiba's R&D in Quantum Information Technology, heading a world-class team of around 30 scientists and engineers. He has extensive experience of leading large EU programmes in quantum technologies, and in particular QKD network technology development and quantum device work for long-distance quantum communications. He is the Chair and co-founder of the Industry Specification Group for Quantum Key Distribution of ETSI (the European Telecommunications Standardisation Institute). In 2013, he was elected a Fellow of the Royal Academy of Engineering and awarded the Mott Medal by the IoP.

Gerald Buller, PhD FInstP FRSE, is Professor of Physics and has served as founding Head of the Photonics and Quantum Sciences Research Institute at Heriot-Watt University. He has worked in single-photon physics for over 25 years and in quantum communication systems for over 20. He has led experimental teams which demonstrated the first fibre-based GHz QKD scheme in 2004 and the first quantum digital signatures scheme in 2012. He has been PI on a range of collaborative research projects funded by the EU, European Space Agency, DSTL, QinetiQ, CERN, etc., including the EQUIS European collaboration. In 2015, he was awarded an EPSRC Established Career Fellowship in Quantum Technology.



The Project Partners

Includes, in addition to the Management Team, the Senior Co-Investigators listed below, over 30 Research Associates, and over 20 PD students, a business development manager, a project manager and support staff at partner institutions.

University of Bristol
- Dr Christopher Erven
- Dr Anthony Laing
- Dr Reza Nejabati
- Professor Dimitra Simeonidou

Royal Holloway University of London
- Professor Kenny Paterson

University of Cambridge
- Professor Richard Penty
- Professor Ian White
- Dr Adrian Wonfor

The University Of Sheffield.
- Dr Pieter Kok

Heriot-Watt University
- Professor Erika Andersson
- Professor Brian Gerardot

University of Strathclyde Glasgow
- Professor John Jeffers

University of Leeds
- Dr Mohsen Razavi
- Professor Ben Varcoe

University of York
- Professor Samuel Braunstein
- Dr Roger Colbeck
- Professor Stefano Pirandola

BT
- Professor Andrew Lord

Toshiba Leading Innovation
- Dr Andrew Shields

NPL National Physical Laboratory
- Dr Christopher Chunnilall
- Dr Alastair Sinclair

Technology Development:
Progress in the Third Year

Theme 1: Short-Range, Free-Space QKD Technologies (led by Prof. John Rarity)

Aim: To advance existing "consumer" QKD demonstrations at the University of Bristol, progressing to integrated, practical and affordable Alice and Bob units with their supporting hardware and software. For lower frequency microwave systems, we will produce practically secure Alice and Bob units with their supporting hardware and software.

This theme focuses on the development of QKD technologies over short-range distances and in free space. This technology is designed for widespread use; the distribution of secrets to the public for daily, low-bandwidth cryptography purposes such as internet banking. The system comprises a handheld transmitter which is small and cheap (<£10) which docks to a larger, more expensive (£2k) fixed terminal - analogous to an ATM. In the last year, and as part of a collaborative partnership resource project with the NQIT Hub, we have added hand tracking functionality to the terminal device which removes the requirement for physical contact between transmitter and receiver – "contactless QKD".

The receiver optics split incoming light into three bases (H/V, D/A, R/L) which can fully characterise incoming light and feedback signals into correction wave plates to adjust for any basis misalignment, including axial rotation which is not corrected for by the hand tracking system. The aim is to enable a user to share a few hundred kilobits of key in approximately four seconds. This is comparable to the time someone might spend at an ATM performing conventional financial transactions.

The technologies developed in this theme will directly enable a wide range of users to exchange secure keys with a centralized location. A useful application of this would be to place receiver terminals at nodes of a high-speed fibre optic quantum network. This would allow users to establish secure keys with each other across the high-speed network with relatively cheap devices. We are investigating potential real-world applications of this technology.

Additionally, the technology of miniaturizing a QKD source to a low size, weight and power (SWaP) has potential in other applications such as satellite or drone-based communications. These schemes translate well from the handheld paradigm, for example, where there are relatively numerous nanosatellites which must be small and cheap, communicating with a ground station which has fewer SWaP restrictions.

Theme 2: Chip- Scale QKD Technology (led by Prof. Mark Thompson)

Aim: This theme focuses on using integrated quantum optics to develop chip-scale QKD devices. This approach, leveraging the expertise at the University of Bristol, allows for small footprint, low power devices, enabling sophisticated, high performance communications security systems. In collaboration with industry, existing semiconductor fabrication infrastructure is utilised to produce devices that are robust, cost-effective and commercially viable. The aim is to produce devices and systems using these principles to enable demonstration of new technologies and protocols and to produce commercial-ready, quantum-enhanced security systems in a form suitable for mass-manufacture and thus widespread industrial uptake.

Pioneered by Prof. Thompson at the University of Bristol, this chip-scale approach delivers devices with low Size, Weight and Power (SWaP) requirements, ensuring the production of scalable, high performance communications security devices. By partnering with commercial foundries, we are able to leverage existing semiconductor fabrication infrastructure to produce devices which are robust, cost-effective and industrially viable, with significant scope for integration with conventional technologies. The work package aims to produce low SWaP devices and systems not only to demonstrate new protocols and technologies, but also as the core of commercially viable quantum secure communications systems.

Progress towards these goals has been rapid, with a range of integrated devices fabricated and successfully demonstrated. This included the world's first chip-to-chip QKD demonstration. By integrating all of the photonics components required by the protocol (barring the single photon detectors) into sender and receiver chips, we were able to produce cheap, robust and low SWaP, industrially fabricated devices with performance comparable to state-of-the-art devices. These devices have formed the core of an internally developed stand-alone QKD system, with custom control electronics, software and packaging all developed to accelerating the graduation of this technology from the lab to real world scenarios. Further to this, the University of Cambridge has also leveraged this technology with the aim of demonstrating a quantum secure router (QSR). This is a critical component for deploying QKD devices in real world networks – able to switch both classical data and QKD channels, whilst maintaining the fidelity of both.

We have also produced high performance QKD transmitters in the Silicon on Insulator (SOI) platform. Significantly cheaper, scalable and lower SWaP than the InP and SiON technologies used previously, SOI is a desirable material in which to perform quantum secure protocols that could be produced on a mass-manufacturable scale. By overcoming the non-ideal characteristics of fast switches in silicon, we have been able to demonstrate GHz-rate encoding and transmission of QKD keys. Additionally, we have leveraged this platform to develop quantum random number generators (QRNGs) – a crucial cryptographic primitive - leveraging quantum random sources such as vacuum fluctuations and laser phase fluctuations to produce highly compact, high performance QRNGs conducive to mass manufacture. Finally, we continue to leverage the integrated photonics technology to improve the performance and practicality of the systems using integrated technology. For example, we have demonstrated Wavelength-Division-Multiplexed (WDM) by combining signals from two devices, with improved devices fabricated and under test. Similarly, we are able to use these same devices to perform next generation protocols such as Measurement Device Independent (MDI) QKD, linking across to theme 4.

Theme 3: Quantum Communication Networking (led by Dr Andrew Shields)

Aim: Theme 3 incorporates core Hub network developments and includes the work on industrial standards. The major deliverable of this theme is the UK Quantum Network (UKQN).

The goal of this theme is to develop technology for ubiquitous application of quantum security in communication networks, addressing the vital issues of telecom and cryptographic integration. It is distinguished from previous quantum network deployments in not requiring dedicated 'dark' fibre for the quantum signals. It aims to develop solutions for metro-core, access, and backbone networks and build a UK Quantum Network (UKQN), to serve as a test-bed for the technology developed in our Hub, and as a focus for application development, international standardisation and user engagement.

We've already reported that TREL QKD equipment has been installed on the Cambridge Quantum Network on three links between the Science Park, Cambridge West Site and the University Engineering Department in town. In an extended trial, the QKD system operating between the nodes on the Science Park and the Engineering Department has run continuously for 6 months without user intervention, distributing 47Tb of secure key, at an average rate of 3 Mb/s. Meanwhile we installed the DWDM Data Transport system (made by ADVA Optical Networking) between the sites in Cambridge, and tested wavelength divisional multiplexing of QKD and data traffic on a single fibre. For the data bandwidth used in this test (100 Gb/s), we see negligible reduction in the QKD secure key rate.

In Bristol, the University team have developed a secure tunnel application which was successfully demonstrated during the 2017 National Quantum Technologies Showcase, in London. We have also experimentally demonstrated distributed denial of service (DDOS) mitigation over a QKD-based network using software defined networking (SDN). As part of ongoing work, Bristol is developing a quantum path algorithm as well as a key management platform targeting the implementation of quantum security over the Bristol city network, Bristol-is-Open, in the short-term period, and NDFIS (the National Dark Fibre Infrastructure Service), in the longer term.

To enable compatibility of the QKD and Data Transport equipment, Toshiba and ADVA developed an application programming interface (API) for transferring keys from a QKD system to any application requiring keys. The API uses well-known REST-based protocols. This interface was implemented by both parties in their equipment and a successful plug test was made in the Cambridge network. In the tests, the AES encryption key used by the data transport system was refreshed by quantum keys every few seconds. Results were presented at the QCrypt conference in Cambridge in September 2017. We have further proposed the REST-based key delivery interface to the ETSI Industry Specification Group (ISG) for QKD, who have agreed to start a new Work Item to write a Group Specification defining the interface. An early draft of the document was presented to the ISG in December 2017.

In the last year, we also reported the first field trial of QKD on the NDFIS network on a loop-back between Cambridge and Duxford. This was made using a TREL system designed for metro networks. TREL have now developed 4 QKD systems designed for the long-distance links spanning Cambridge-London-Bristol. These systems are designed to tolerate higher loss over the quantum channel.

Theme 4: Next Generation Quantum Communications (led by Prof. Gerald Buller)

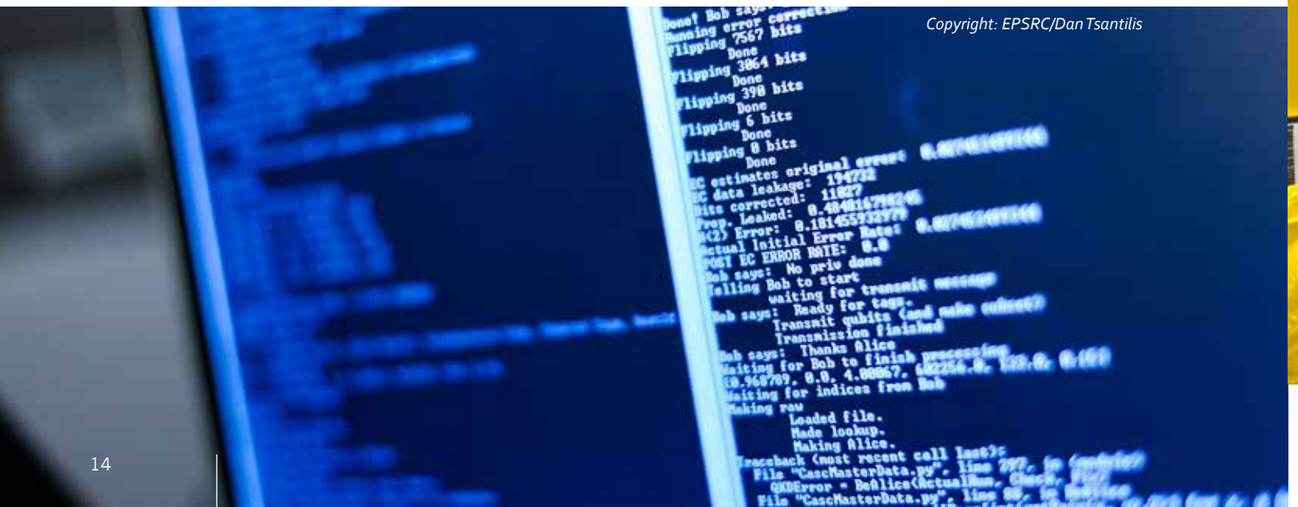
Aim: To explore new approaches, applications, protocols and services – to open up new markets for quantum communications beyond key distribution alone. The sub-themes have been reviewed and revised regularly, based upon progress to implementation, demonstration and technology. The initial sub-themes include quantum digital signatures, multiple-user scenarios, quantum relays/ repeaters/ amplifiers and device-independent technologies. The hardware developed here will feed into themes 1-3, to accelerate progress from the laboratory to the UK Quantum Network and eventual commercialisation.

The information theoretically secure guarantees of message integrity and nonrepudiation offered by quantum digital signatures (QDS) are complementary to the confidentiality provided by quantum key distribution. In the last year, the Hub has built on its previous track record in developing new theories and advancing the experimental feasibility of QDS to extend the transmission distance to over 100 km of installed dark optical fibre. In parallel, the Hub conducted the first experimental demonstration of measurement device independent (MDI) QDS. This demonstration applied the techniques developed through the Hub's ongoing progress in MDI QKD to realise a quantum network architecture, where the nodes were fully connected using a minimum amount of physical links. The central node of the network could act either as a totally untrusted relay, or as a trusted recipient directly communicating with the end users via QKD. The Hub remains the world leader in QDS, and now major international laboratories are starting to work in the field, including Max Planck Institute (Erlangen), NICT (Tokyo), and Jian-Wei Pan's group in China.

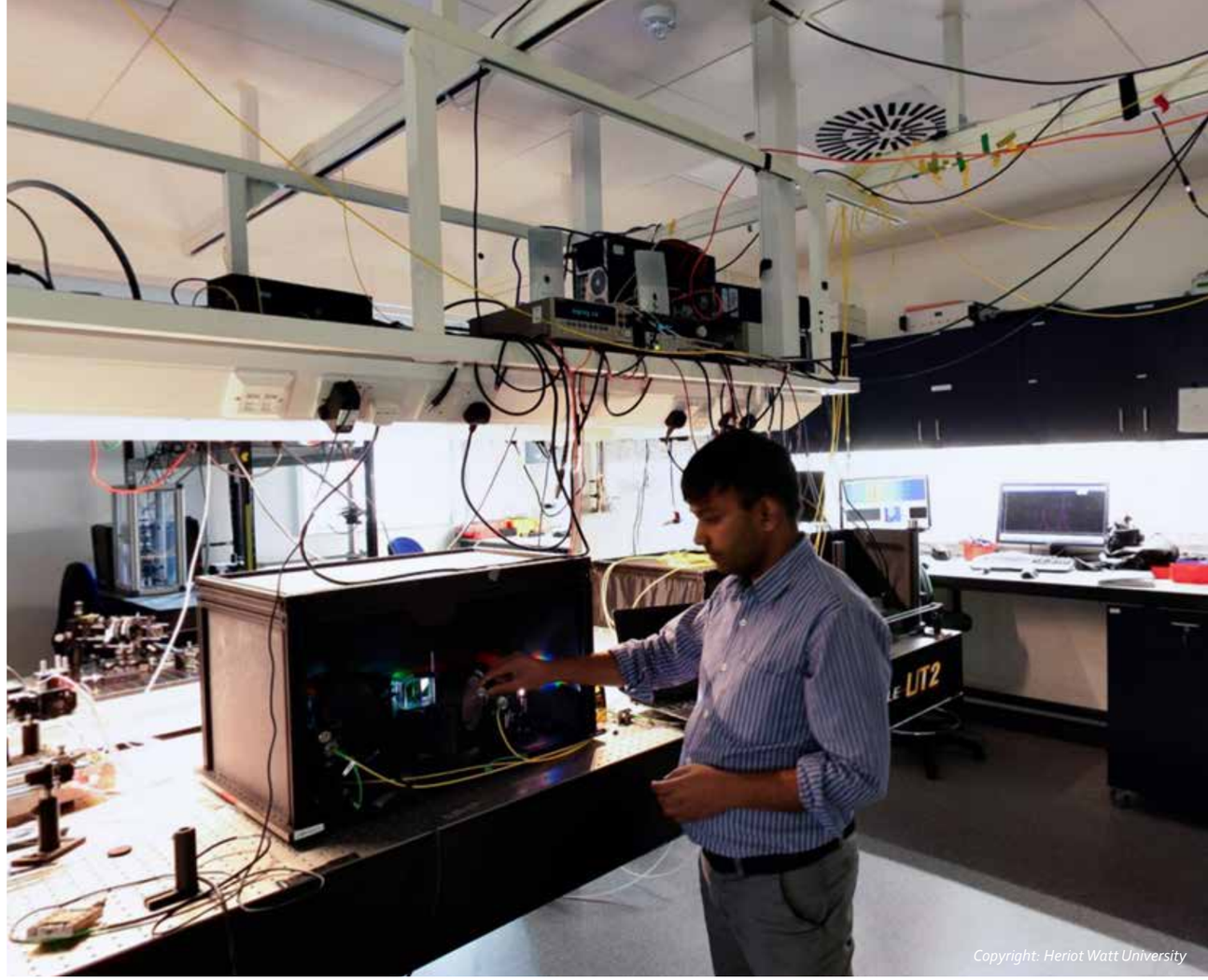
With regard to amplifiers and repeaters, ongoing work on the state comparison amplifier (SCAMP) has led to a practical feedforward approach that offers enhanced success rate over previous implementations. A miniaturised optical chip-based SCAMP has been developed and tested and offers the prospect of enhanced performance compare to larger scale, bulk optical designs. A close collaboration between theoretical and experimental groups has resulted in the establishment of a detailed theoretical model which can be used to predict the performance of future amplifier designs and experimental prototypes of many of these designs are undergoing initial testing.

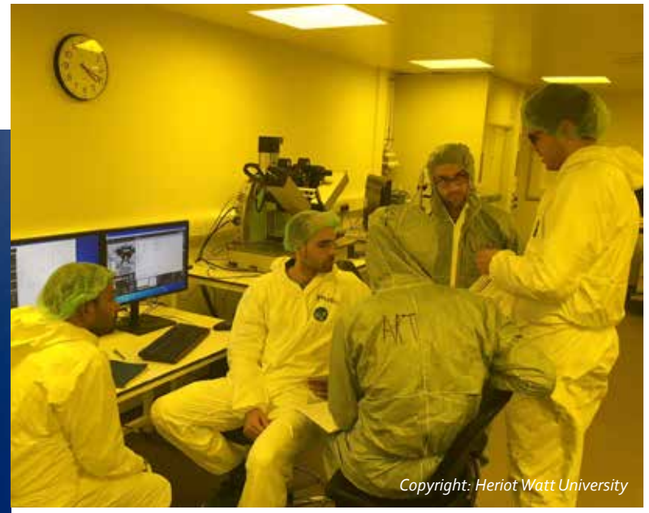
A quantum relay has been implemented by TREL and the University of Cambridge using a Quantum Dot (QD) emitter generating entangled photon pairs in the telecom O-band, making the system compatible with existing optical telecommunication networks. High fidelities for operation with a standard 4-state protocol were achieved and the system was tested for robustness against spectral drifts typical for commercial telecom laser diodes. Furthermore, non-classical teleportation for arbitrary input states was demonstrated. In preparation for field deployment of the technology, a dedicated loopback link in the Cambridge network was established for running first preparatory experiments over installed fibre. The growth of new wafer material with QDs emitting in the telecom O-band is still ongoing but showed first promising results. For the electric operation of telecom devices, new fabrication designs were investigated.

Building on our recent realization of ultra-bright and scalable single photon sources in a layered semiconductor material, we have designed heterostructure devices that enable loading electrons or holes one-by-one



Copyright: EPSRC/Dan Tsantilis


Copyright: Heriot Watt University


Copyright: Heriot Watt University

(via Coulomb blockade). This ability enables access to a spin-photon interface, which we are currently exploring for coherence. Future applications would be in quantum repeaters. Additionally, we have exploited the potential to combine 2D semiconductor single photon sources and CMOS compatible photonic chips to create hybrid quantum photonic chips. Our first-generation chip includes a single photon emitter coupled to an on-chip waveguide with a beam-splitter for on-chip Hanbury Brown and Twiss interferometry. Finally, we have pushed a single photon source based on III-V quantum dots with perfect purity (e.g. all excess photons are suppressed) towards the highly desirable target of perfectly indistinguishable emissions. Such sources can underpin both quantum communication and photonic quantum simulation.

Highlight on:

Chip-based Quantum Key Distribution

2017 marked a significant development in the Hub's miniaturised chip-based technology, as colleagues from the University of Bristol, demonstrated the world's first chip-based QKD system.

Complex cryptography protects our bank accounts and identities from fraud, allowing us to safely buy and sell online without ever leaving the comfort of our living rooms. But the potential introduction of ultra-powerful quantum computers renders our personal information vulnerable to direct attacks, even information that is stored today and decrypted in the future. Hub researchers at the University of Bristol's QETLabs have developed tiny microchip circuits which use light and optical communications to provide a level of security enhanced by the laws of quantum physics. These devices distribute cryptographic keys between users by transmitting single particles of light, using the properties of entanglement, superposition, and the absolute randomness provided by quantum behaviour, which is reproducible by no other means.

Principal investigator Professor Mark Thompson said: "The system we have developed allows information to be exchanged using single photons of light in a quantum state. If an eavesdropper hacks your transmission, they will cause the fragile quantum states to collapse and the system will alert you to their presence and terminate the transmission."

This work, published in the February 2017 issue of Nature Communications, has demonstrated the world's first chip-to-chip quantum secured communication system, using microchip circuits just a few millimetres in size. The international collaboration, including researchers from Bristol, Glasgow and NICT in Japan, used commercial semiconductor chip manufacturers to make their devices – in much the same way as Intel pattern silicon to make the latest central processing units (CPUs). However, instead of using electricity these miniaturised devices used light to encode information at the single photon level, providing encryption keys with an unlimited lifetime.

Lead author Dr Philip Sibson, added: "Our research opens the way to many applications that have, until now, been infeasible. The technology is miniaturised for handheld devices, has enhanced functionality for

telecommunications networks, and employs cost-effective manufacturing to feasibly deploy quantum key distribution technology in the home."

The Bristol team have continued to develop this technology, demonstrating an innovative design that allows the same functionality in a complementary metal-oxide-semiconductor (CMOS) compatible process, appearing in the February issue of Optica. By manufacturing this generation of in-standard silicon, this paves the way for direct integration with microelectronic circuits. This will ultimately lead to integration in every day electrical devices, such as laptops and mobile phones. Dr Chris Erven explained: "As part of the UK Quantum Communications Hub, we are in the process of deploying these devices throughout the heart of the Bristol City fibre-optic network, allowing us to test out these ultra-secure communications systems in real-world scenarios."

P. Sibson *et al*. Chip-based Quantum Key Distribution. Nature Communications 8, 13984 (2017)

P. Sibson *et al*. Integrated silicon photonics for high-speed quantum key distribution, Optica Vol. 4, Issue 2, pp. 172-177 (2017)

Highlight on:

Operability of the Cambridge Metropolitan Quantum Network

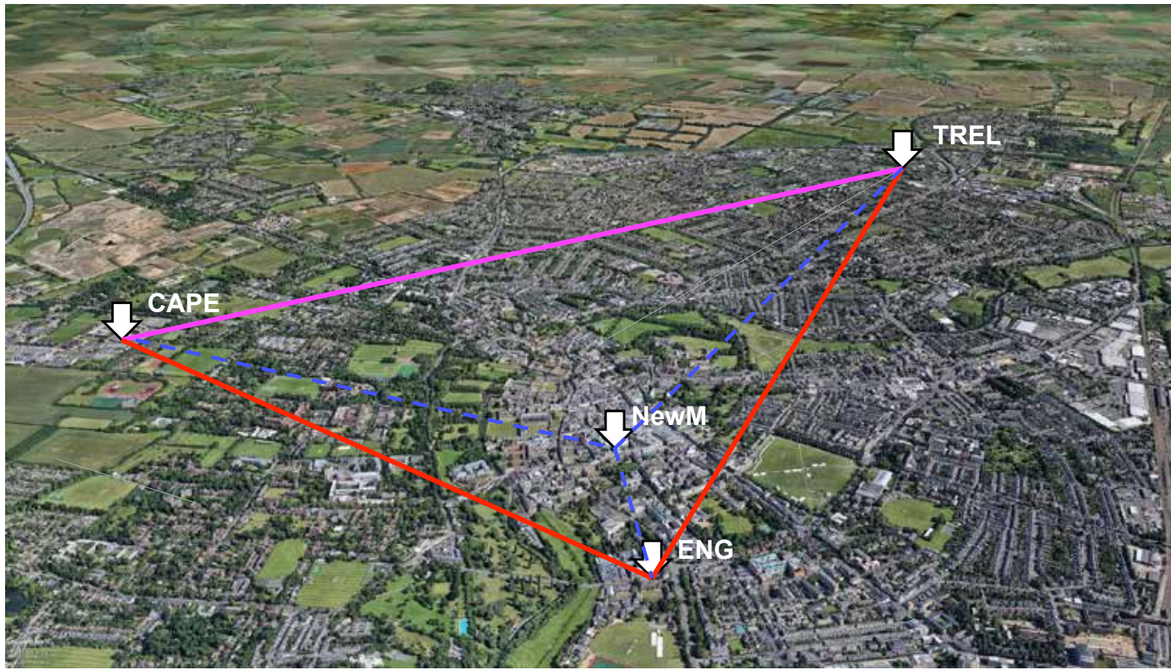
The Cambridge quantum network (CQN) is a four-node metropolitan quantum secured optical communication network connecting 3 sites within the University of Cambridge and Toshiba Research Europe's laboratories (TREL) on the Cambridge Science Park.

The CQN provides secure communication using 100Gb/s optical channels between three of the four nodes. Each of these channels is secured using TREL quantum key distribution systems. These systems generate secure keys at rates in excess of 2 Gb/s on all links; the QKD systems feed their keys via a key management layer to the AES 256 secured 100Gb/s transmission systems from ADVA networking.

This network enables the provision of ten 10Gb/s data channels between each of the main nodes at Electrical Engineering and the main Engineering Department at the University of Cambridge and at TREL. It is additionally planned to add quantum secured access networks to locations at Electrical Engineering and TREL, enabling many different users and services to operate over the network.

Furthermore, the CQN node at Electrical Engineering forms a gateway for the UK Quantum Network via the EPSRC-funded National Dark Fibre Infrastructure Service (NDFIS) - a time-shared dark fibre resource (provided by the Janet Aurora 2 fibre platform). This key facility will eventually enable the linking of the CQN with its equivalent – the metropolitan network in Bristol. This work is underway, with the first two sections, between Cambridge, London and Reading currently being scheduled for imminent deployment.

An additional and exciting development is the imminent completion of the extended link of the UK's Quantum Network between the Department of Electrical Engineering at Cambridge and BT's Research Labs at Adastral Park, near Ipswich. This will enable the Hub to test commercially available systems and will provide a method of producing design rules which enables migration from a research network to a commercially deployable quantum secured communication service.



Copyright: 2017 Google, Infoterra Ltd + Bluesky, Getmapping plc, The Geoinformation group, Mapdata ©2017 Google. Image courtesy of Dr Andrew Shields, TREL.

Highlight on:

Assurance/Certification of Physical Quantum Random Number Generators

Random numbers are important in many branches of science, from simulating meteorological scenarios to generating cryptographic keys. Using a low-quality random number generator can be detrimental, making the results of a simulation misleading, or leading users to believe in the security of a poor key. Thus, validation of random number generators is important. Unfortunately, this is not an easy task. Testing the outputs of such a device can expose some types of flaw but it is impossible, through tests on the output candidate random numbers alone, to certify that these are fit for purpose. For example, two devices generating random numbers could output the same sequence of numbers, which pass all the randomness tests. To avoid this clearly undesirable potential for matching random sequences, the physical process by which the numbers are generated needs to be random.

As far as we know, the only way to generate fundamentally random numbers is to use quantum processes. Furthermore, the technological requirements for such a device are much lower than for other quantum technologies. As a result, quantum random number generators (QRNGs) are already on the market, with several others under development. Recognising this, the Quantum Communications Hub has funded a Partnership Resource project to kick-start work on validation of the "quantumness" (and hence randomness) of the underpinning physical processes. QRNG technology is unlikely to become widely used without such assurances.

As a first step, a scoping workshop was held at the National Cyber Security Centre (NCSC) at the end of August 2017, bringing together interested parties to discuss the issues around validation and certification. After the meeting, a concrete proposal was put together focusing on optical quantum random number generators, these being the most developed to date and the basis behind the only commercial products currently available. Taking two devices, one already commercially available and one prototype, the project team will work with the manufacturers to generate an accurate as possible theoretical model of their device before computing the amount of extractable randomness. In parallel, the intent is to develop a general framework for physical testing and analysis such that it can be used with other optical QRNGs, and hence develop UK capability in the area by forming the beginnings of an eventual certification process, fitting with Recommendation 9 of the Blackett Review into quantum technologies.

The project will have direct participation of key UK stake-holders in assurance, verification, accreditation/certification, the National Physical Laboratory with support from NCSC, so as to be informed by:

- the strategic aim of national capability if not leadership in accreditation/certification;
- the necessity of compliance with international standards.

This will increase the likelihood of the results of the project and follow-on work being taken forward into a future accreditation framework, which is the target legacy of this project, and in keeping with Recommendation 9 of the Blackett review*.

* The Quantum Age: technological opportunities, 3rd November 2016 www.gov.uk/government/publications/quantum-technologies-blackett-review

Highlight on:

ETSI/IQC Quantum Safe Workshop, London, 13-15 September 2017

The 5th ETSI/IQC international workshop on quantum-safe cryptography took place in September 2017 at the Westminster Conference Centre, London. The event was jointly co-organised by ETSI, the European Telecommunications Standards Institute, and the IQC, the University of Waterloo's Institute of Quantum Computing (Canada), with further support provided by the Quantum Communications Hub, which acted as host. The National Cyber Security Centre and CryptoWorks21 training partnership were also supporting partners.

The 3-day workshop is an annual expert stakeholder event aimed at providing a platform for the quantum-safe cybersecurity community to facilitate knowledge exchange and collaboration. This year's event focused on the dependency of modern ICT systems (cloud computing, global payment systems, e-health, critical national infrastructure etc.) on modern cryptography and on the approaches pioneered globally to mitigate the risk posed to it by the advance of quantum computing.

The workshop was structured along executive (13/09) and technical (14-15/09) tracks. The focus on the first day was on the disruptive potential of quantum computing and the technologies available to counteract subsequent threats to existing cyber-security infrastructure. Panel sessions discussed public sector views and threats to governments (with input from the UK's National Cyber Security Centre, Canada's CSE, USA's NIST and NLNCSA Netherlands); critical IT infrastructures (with speakers from Amazon Web Services, Cisco, Microsoft and Huawei); quantum safe products and services; and the importance of standardisation. Discussions during the following two days centred on the current state of quantum-safe cryptography, challenges of cryptographic standardisation on a global scale, the selection criteria for new post-quantum encryption algorithms, and specific government and industry requirements. A world tour session offered insights into practical challenges of quantum-safe schemes (from the UK, Japan, the US, Canada, China and the European Quantum Flagship initiative). Specific issues discussed at length included the industry perspective on computational constraints for post-quantum cryptography; high priority use cases; standards for quantum cryptography system devices and for quantum-resistant public-key crypto algorithms; testing, metrics and certification; new applications of post-quantum crypto or quantum key distribution; attempts at cryptanalysis and migration paths.

Keynote addresses were given by Sir Mark Walport, the Government Chief Scientific Adviser and Chief Executive Designate of UKRI; Luke Beeson, BT's Vice-President on Security in UK and Continental Europe; and Sir Peter Knight, member of the Strategic Advisory Board of the UK National Quantum Technologies Programme and Chair of the Quantum Metrology Institute. Professor Tim Spiller, Director of the Quantum Communications Hub, gave an invited talk on the UK perspective and technologies developed in the Hub for quantum-secured communications.

The event was oversubscribed and generated significant media interest, with the Wall Street Journal in particular providing extensive coverage and conducting interviews. All presentations from both executive and technical tracks are available to download from the event website (http://www.etsi.org/news-events/events/1173-etsi-iqc-quantum-safe-workshop-2017).

Highlight on:

QCrypt 2017 – 7th International Conference in Quantum Cryptography

QCrypt is the flagship event in the field of quantum cryptography research, an annual conference for researchers working on all aspects of the discipline, including theoretical and experimental research on possibilities and limitations of secure communication and computation with quantum devices, security challenges posed by quantum computing, and long-distance quantum communication. Following an invitation to submit a proposal, the Quantum Communications Hub was awarded delivery of the 2017 conference. The Hub bid was successful on the basis of the partnership's strength in bringing together multiple institutions and the collective resources and experience necessary to host a major international conference in the UK – an acknowledged focal point of international excellence in cryptography, both current and historic.

The event took place in Cambridge in autumn (West Road Concert Hall, 18-22 September 2017). The city is well known in the community as a major centre for quantum cryptography in the UK. Two of the hub's major partners are located here: the University of Cambridge, and Toshiba Research Europe Ltd. A third, British Telecom, has its global R&D base nearby, in Martlesham Heath. All three partners are central to one of the major developments and demonstrators of the Quantum Communications Hub – a QKD metropolitan network in Cambridge, set up to function as a primary focus for industry engagement (part of the UK's National Quantum Network being built by the Hub – see relevant section in this report). Furthermore, key breakthroughs in recent years have come from Cambridge, including: the first demonstration of QKD over 100 km; the first QKD with secure key rates exceeding 1 Mb/s; protocols for position dependent QKD and bit commitment; first LEDs for generating single and entangled photons and first multiplexing of QKD with 100 Gb/s data signals.

The conference is the major international event in the field, and the 2017 meeting was attended by over 300 delegates from around the world. The event was organised by a Hub team from the Universities of Cambridge and York, led by Professor Richard Penty as Chair of the Local Organising Committee, and Dr Adrian Wonfor as Development Lead. Parallel sessions focused on every aspect of quantum cryptography, from theoretical developments to experimental manifestations: quantum teleportation across metropolitan fibre networking; experimental quantum money; post-quantum cryptography; core and access QKD networks; network coding; quantum authentication and encryption with key recycling; device-independent randomness amplification and privatisation; and many more. Hub researchers participated with over 25 talks, paper presentations and invited tutorials on a range of topics across the full spectrum of the Hub's technology themes. Video recordings of all talks are available through the QCrypt 2017 website (http://2017.qcrypt.net).

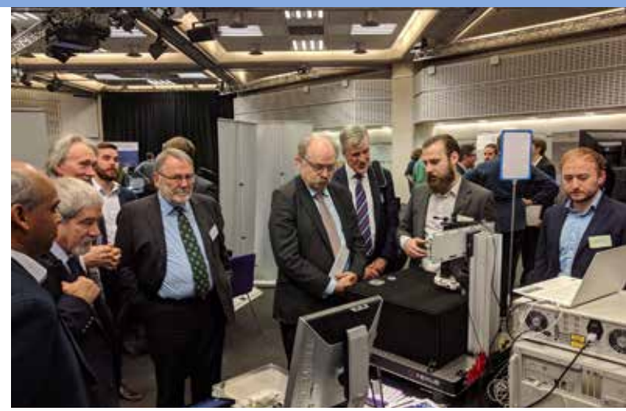
The event was delivered with generous support by a number of sponsors including among others Alibaba, IDQ, SK Telecom, University of Waterloo / IQC, Singapore Centre for Quantum Technologies, Toshiba, and the National Physical Laboratory.

Highlight on:

Hub demonstrations of technology advances at 2017 National Quantum Technologies Showcase

The 2017 National Quantum Technologies Showcase took place on 22 November at the QEII Conference Centre in central London. The third such meeting of its kind, the showcase is the flagship user engagement event of the UK National Quantum Technologies Programme, aimed at highlighting the commercial potential of the emerging technologies for the UK and global economy to representatives of government and industry. This year's event attracted over 600 delegates and included nearly 60 technology demonstrators, covering multiple sectors of the economy: transport, healthcare, defence and security, components and heavy industry, finance, space and communications and future networks.

The Quantum Communications Hub contributed to the organisation of the event, led this year by the EPSRC, and took part with a number of technology demonstrators managed by experimental colleagues at the Universities of Bristol, Cambridge and York, as well as industrial partners Toshiba Research Europe Ltd, BT and ADVA. Our exhibits ranged across the sectors: (i) integrated photonics in the form of chip-based quantum key distribution, offering distinct commercial advantages in terms of enhanced functionality and cost-effective manufacturing; (ii) quantum keys used as a network resource, demonstrating the adaptive functionalities and agile network capabilities resulting from combining QKD security with existing software defined networks (SDN) and network function virtualisation (NFV) principles; (iii) low-cost, short-range QKD for use on handheld devices, enabling cryptographic interaction with ATM-like terminals; (iv) an optical fibre-based transmitter and receiver system for exchanging classical and quantum signals using single laser pulse, for monitoring eavesdropping and generating secure keys for cryptographic purposes; (v) a demonstration of securing data centre links with quantum cryptography over optical fibre networks; (vi) an exhibit highlighting work on the UKQNTel project, the extension arm of the UK's Quantum Network linking major R&D and business clusters in Cambridge with and Adastral Park via optical fibre.



A video about some of the Hub's exhibits at the 2017 showcase can be viewed at the Quantum Communications Hub YouTube channel (searchable within the YouTube platform).

Copyright EPSRC/Dan Tsantilis

Highlight on:

KETS - Venture Capital Funding Competition Winner

KETS Quantum Security Ltd., a start-up company supported by the Hub and aiming to develop integrated quantum photonic platforms for secure data transmissions, has gone from strength to strength and 2017 was marked for further success. Since their top prize award in Bristol's 2015 New Enterprise Competition for their business proposal using quantum cryptography to improve data encryption, KETS have continued to develop their team, technologies and commercialisation strategy. This has involved extensive market research, engagement with large potential customers (such as Airbus and BT), ongoing technology and product development work, and a number of demonstrations at high profile user engagement events, both in the UK and abroad.

KETS's mission is to secure communications using future-proof, scalable, and easily-deployed hardware solutions manufactured with existing semiconductor fabrication processes that can be easily integrated with existing electronics. The company has developed the world's first integrated quantum secured encryption technologies – from quantum random number generators (QRNGs) to full quantum key distribution devices. Its low size, weight, and power (SWaP) solution intends to boost security in applications including defence, telecommunications, and critical infrastructure, with end-users from finance, government, and data centres.

In early 2017, KETS were successful with partners Airbus, ID Quantique, and the Universities of Oxford and Bristol in winning a major Innovate UK grant (Q-DOS Light) to demonstrate quantum secured communication to an Unmanned Aerial Vehicle (UAV). Over the summer, KETS participated in the DCMS Phase 2 Cyber Security Academic Start-Up programme, rapidly evolving its basic QRNG technology into a robust proof-of-principle demonstration showcased in October to industry experts, end users, potential investors, and the public at the DCMS ASI Showcase at Canary Wharf.

In the Autumn, the company was announced as the first of three winners of the prestigious UK TEAC (Telecom Infra Project Ecosystem Acceleration Centre) initiative, judged by a panel of experts from BT, the Telecom Infra Project (TIP) and Facebook. The competition is aimed at SMEs working in the field of telecoms network infrastructure and provides them with access to venture capital partners with a potential pool of £120m, as well as support and expertise from BT - the UK TEAC lead, to facilitate the transition from innovative ideas to market-ready commercial products. As part of the programme, the founding team travelled to Facebook's Annual TIP Summit in Santa Clara, California in November, where they were met with great interest in their technology from industry.

KETS QUANTUM SECURITY

Philip Sibson, CTO of KETS, one of the lead developers of the technology added: "Through initiatives like the TEAC programme and working with the Quantum Communications Hub, we are developing solutions that will underpin the integrity of the UK's future telecommunications infrastructure; we hope to soon ensure the safety of our information in situations ranging from bank transactions to critical infrastructure, and eventually to individuals shopping securely online from the comfort of our own home."

For more information on the work of KETS, visit http://kets-quantum.com

Highlight on:

Satellite Quantum Communications

The Hub continued to explore options for UK development in satellite quantum Communications, an area in which a number of countries have continued to make progress and secured substantial commitments to missions. These include the most dramatic expression of strategic ambition of all by China in 2016, with a very large scale national programme leading to the world's first major quantum communications satellite. Other countries, including Canada, Germany, Japan, Singapore and Switzerland have programmes at various stages of development directed at missions. In addition, the European Space Agency (ESA) confirmed at the end of 2017 commitment to funding both further research and commercially focussed initiatives. This has created possibilities that the UK is now well placed to take advantage of.

Throughout the year, the Hub engaged with the other national programmes, with the aim of identifying appropriate potential partners and collaborations. The purpose of such collaborations is to assist rapid development of UK capability specifically in satellite quantum communications. The UK has relevant existing strengths in industry and research: the former includes a world-class commercial sector building satellites and integrating payloads for the global market; the latter, world-class development in photonics, optical networking, and quantum secure communications, reflected in, and enhanced by, the UK National Quantum Technologies Programme.

In the UK, we worked closely with key stakeholders in space and satellite communications, notably RAL Space and the UK Space Agency, to support alignment of the emergence of satellite quantum communications with established structures and strategies. This is a step towards the creation of strategy and policy for quantum technologies in space – which will include, but not be limited to, satellite quantum communications. The UK landscape itself rapidly changed, with a number of enabling initiatives - including commitment to a new National Satellite Testing Facility at Harwell, and momentum for a new quantum space qualification lab, also at Harwell.

In addition, the Hub itself, with research and industry partners, identified specific requirements for supporting developments around satellite quantum communications. These ranged from optical path modelling of the atmosphere, and identification and assessment of threat assumptions at the ground segment, to a review of current UK industrial capability. The result was a suite of proposals for a number of related feasibility studies to be undertaken in 2018. These would be of inherent research value, as well as providing the foundations for scaled-up development in partnership with industry.

Finally, the Hub actively supported development of international collaborative proposals for satellite quantum communications missions with a significant UK element, the outcome of which will be known in 2018.

Highlight on

Public Dialogue on Quantum Technologies

One of the central tenets of the national programme strategy for quantum technologies is the need to create the right social and regulatory context, through responsible innovation and effective regulation. As part of this effort, the Engineering and Physical Sciences Research Council commissioned in late 2016 a public dialogue exercise with the aim of introducing members of the public to the capabilities of quantum technologies currently under development in the UK, and understanding any concerns, aspirations and priorities relating to their future development and eventual deployment. The tender was won by Kantar Public, an independent social research agency advising on global best practice in public policy, public service delivery and public communications, which over the course of the next year worked with many programme stakeholders to put together an appropriate body of materials for relating the potential of the emerging quantum technologies to the public.

An initial planning workshop attended by stakeholders of the UK National Quantum Technologies Programme, including the directors and many researchers from the four quantum technology Hubs, served as a platform for sharing advice on effective communication with the public and for exploring ideas for use in the dialogue materials. This meeting was followed in autumn 2017 by two waves of reconvened, full-day public dialogue workshops and an interim activity organised by each of the four Hubs with the aim of showcasing their specific technology remit. The workshops were delivered in each Hub's leading institution (the Universities of Birmingham, Glasgow, Oxford and York) with participants including trained facilitators from Kantar, expert stakeholders from each Hub and a diverse (in terms of age, gender, ethnicity, socioeconomic status and interest in science) group of randomly selected members of the public who had no previous knowledge of the subject matter.

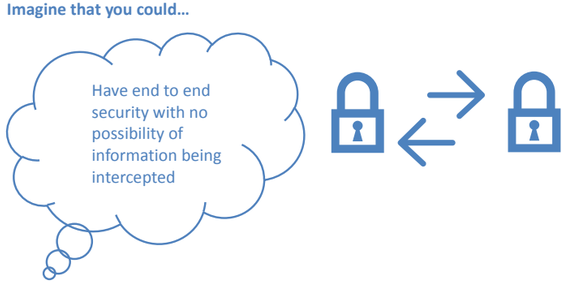
The Quantum Communications Hub workshops were very successful, thanks to a large degree to the enthusiasm and engagement of the participants. Feedback for the interim activity offered (a technical demonstration of quantum secured video transmission between two users and an intercepted hacking attempt, along with a public talk on the principles behind quantum communications delivered by Hub partner BT) was highly positive. Although the potential use of quantum communications applications in the context of a global "arms race" or by criminal/terrorist groups was raised as a concern, overall the group were very vocal about the need for this technology to be prioritised and for UK investment in this area to counteract the threat posed in cybersecurity by developments in quantum computing.

The results of the public dialogue will be made available in a report authored by Kantar Public in 2018.

KANTAR PUBLIC=

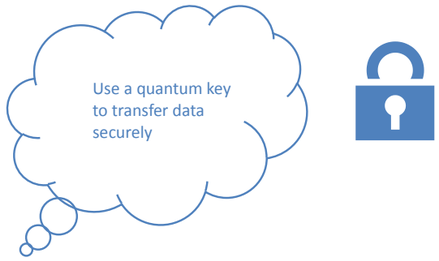
QUANTUM COMMUNICATION

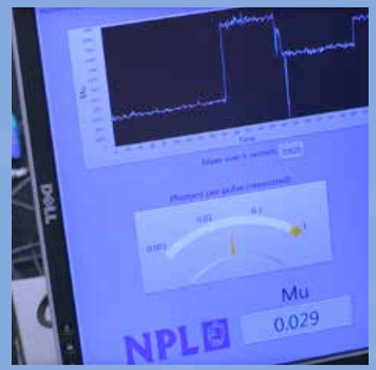
Imagine that you could...

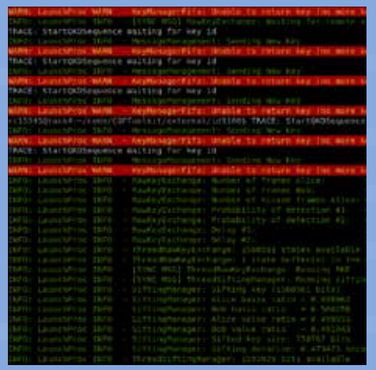


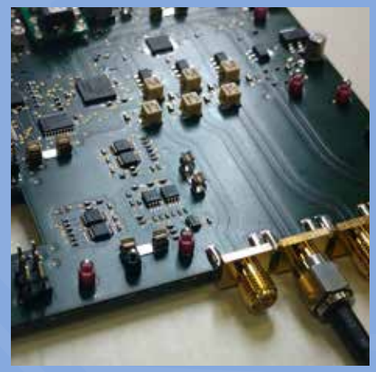
QUANTUM COMMUNICATION KEY

Imagine that you could...



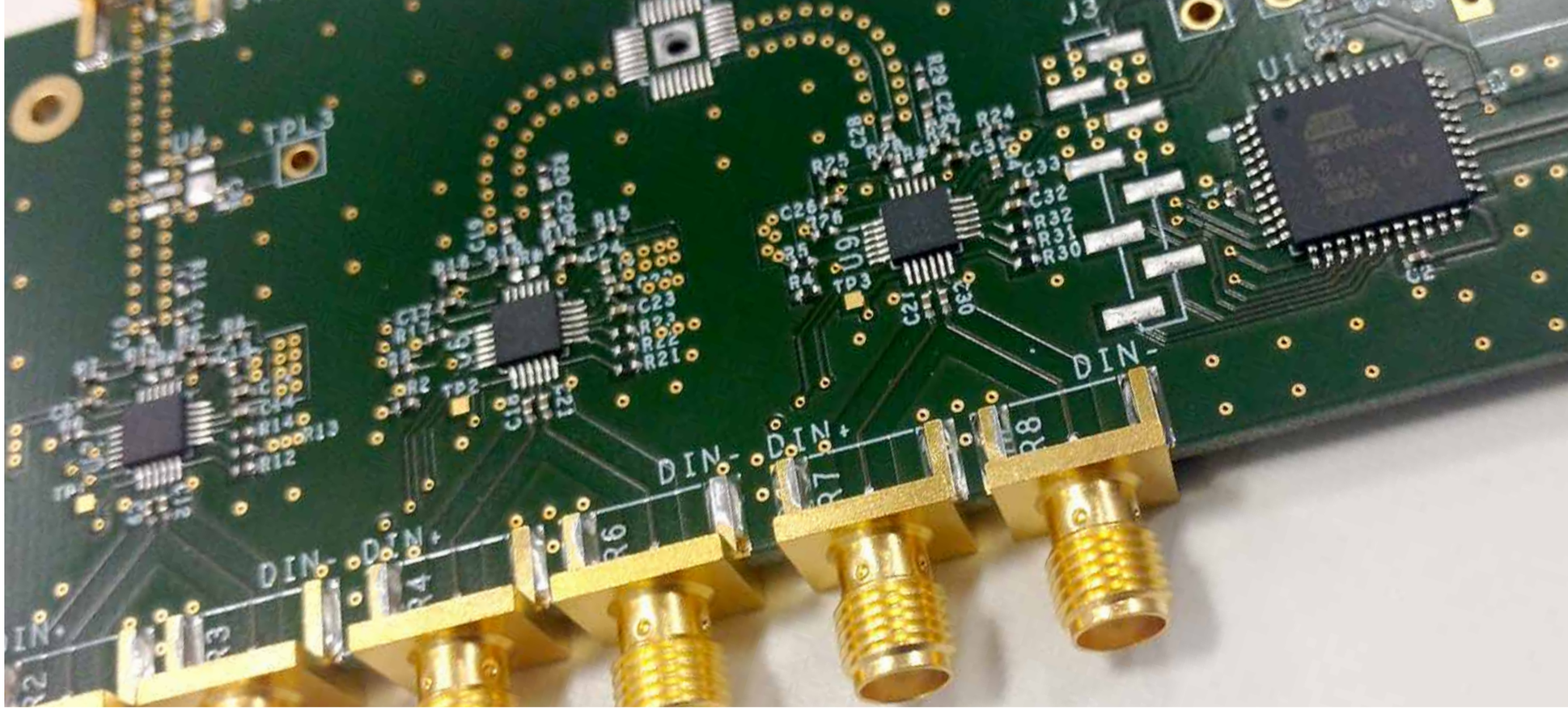






Partnership Resource Investment

The Quantum Communications Hub has allocated funds (Partnership Resource) to support new collaborations which are closely aligned with the work of the Hub and support new capabilities. This additional funding can be strategically invested to: support evolvement of each Hub; bring in new capabilities that are key to Hub success; fund engagement with new partners; respond to new opportunities developed by the national programme; support activities on a significant scale; encourage collaboration between Hubs required to support activity with greater impact; support a high level of user engagement such as workshops, pump-priming and/or networking activities, and responsible innovation.



Using EPSRC guidance in relation to: building new capability; strategic fit; appropriate scale; new partnerships and collaborations; commercialisation potential; measurable deliverables and realistic costs and contributions, the Quantum Communications Hub has: (1) considered proposals from within and outside the partnership for projects related to the core outcomes; (2) committed funding to support activities and events that either relate to the wider national programme, or specifically to major new initiatives linked to opportunities and developments that have arisen since the Hub was proposed; (3) earmarked funding for major new developments, particularly where there is strong industrial engagement.

Through this approach, the partnership fund has been used to support a range of new developments with strategic importance to the Hub. Examples include:

Towards Assurance / Certification of Physical Quantum Random Number Generators

(University of York, National Physical Laboratory)

This project seeks to develop the necessary theoretical and experimental understanding, expertise and techniques to test physical quantum random number generators. The importance of quantum random number generators is widely acknowledged, as is the size of the market for component level devices that are small and cheap enough to be incorporated into small systems, e.g. mobile phones; for authentication purposes e.g. in the Internet of Things; and as essential components in quantum communication systems. Authoritative accreditation of the output is an outstanding issue for QRNGs. Current tests are based on numerical analysis of the output sequence, which cannot provide a confident bound on the independence of the randomness. Stronger certification is possible for physical QRNGs (PQRNGs), since the physical process used to create the output sequence can be theoretically analysed and physically tested. The developed approach will be applied to one or two selected implementations, including a commercial device (adapted to facilitate interrogation).

Quantum Network Token Schemes

(University of Cambridge, Cambridge Quantum Computing)

The project is developing quantum-enabled secure tokens, which can be used on financial and other networks where time is critical and the light speed signalling bound is significant. The tokens allow access authentication and prevent multiple access without involving the delays that cross-checking across the network would require, without requiring long term quantum memory. The plan is to implement these token schemes using quantum key distribution devices and networks developed by Hub partners, in order to demonstrate and optimize them with current quantum technology and identify further gains that could be made by building dedicated devices. Commercialisation of this technology for target markets will be pursued in partnership with Cambridge Enterprise and Cambridge Quantum Computing.

3D Photonic Components for Quantum Optical Communications

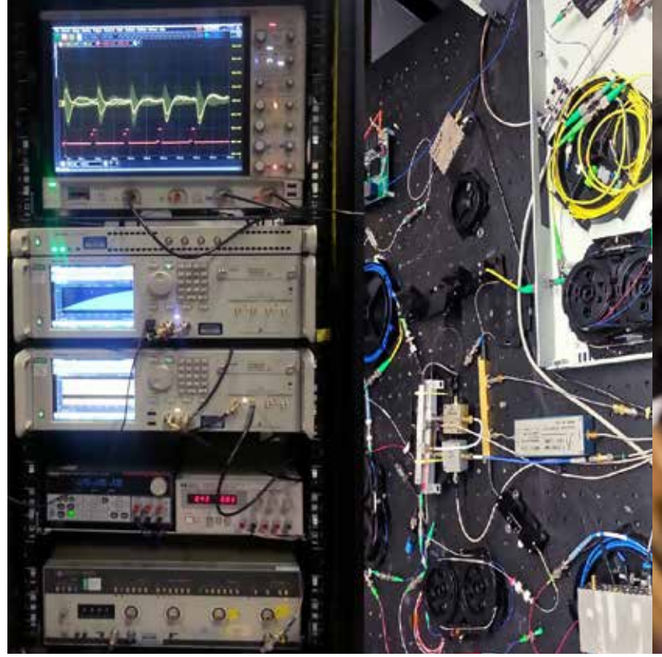
(Heriot Watt University)

This project is designed to take advantage of the world leading expertise at Heriot Watt in the technology of ultrafast laser inscription - a laser writing technology that facilitates the fabrication of three-dimensional optical waveguides inside dielectric materials. The primary goal is to develop 3D integrated multiport interferometers for state elimination measurement in quantum optical fibre communications systems. Such components offer considerable benefits over bulk optic systems, including stability, compactness and manufacturability, with higher throughputs than are currently achievable with other integration platforms e.g. silicon-on-insulator. A secondary and higher risk aim is to investigate the feasibility of developing mode-coupling and sorting components based on "photonic lanterns", for the implementation of space-division-multiplexed quantum communications (both free-space and optical-fibre based). These components can then be used in different communications links, including potential free-space applications with an eye to communicating with orbiting satellites.

The Quantum Ambassadors scheme: inspiring the UK's future quantum community of scientists and engineers

(National STEM Learning Centre, University of York Science Education Group, in collaboration with the Network of UK Quantum Technology Hubs)

The UK Quantum Communications Hub are engaging into a partnership with the National STEM Learning Centre and the University of York Science Education Group to deliver a comprehensive scheme of quantum-related CPD and classroom-based activities for A-level students and their science teachers, with the specific aim of promoting the uptake of STEM subjects, highlighting the benefits and applications of mature quantum technologies and signposting career pathways for science graduates.
The proposed scheme is seeking to increase awareness and understanding of the importance and relevance of quantum technologies to UK society, culture and the economy. Over a 2-year period, the project partners working closely with the other UK Technology Hubs will use the science and technologies of the national quantum technologies programme as a context in which to develop and deliver an inspiring enrichment scheme across the UK. The scheme is UK wide – achieved by a collaborative approach involving a wide network of partners and support organisations.



Copyright: Alex Holland, Marketing, University of York.

CV-QKD at Higher Bandwidth: development of a continuous variable quantum key distribution (CV-QKD) testbed for operation on the Cambridge to Adastral Park network

(University of Cambridge, University of York)

Continuous Variable Quantum Key Distribution (CV-QKD) has recently seen a revival of interest as a potentially high performance technique for secure key distribution, over metro-network scale distances. Demonstration of CV-QKD based on regeneration of reference frame at the receiver shows compatibility with classical coherent detection schemes that are widely used for high bandwidth classical communication systems. Most importantly, seamless integration into existing DWDM classical networks makes it a potentially a highly viable quantum secure key distribution technology over current networks: a most appealing aspect of CV-QKD is that it can use telecommunications equipment which is readily available and which is also in common use industry wide. However, a lower clock rate and certain data processing complexities currently limit commercial interest and thus widespread use of CV-QKD systems in existing secure data communication networks. The aim of this project is to explore the feasibility for demonstration of a CV-QKD system that runs at higher clock rates with enhanced secure key rate, through exploitation of the high bandwidth signal generation and detection systems available within the Cambridge laboratory. An additional aim is to implement key distribution protocols that require reduced complexities in data processing - which is also advantageous towards early commercialisation.

EPSRC Doctoral Training Partnership Studentships in Quantum Technologies

A direct result of the significant investment into the UK's National Quantum Technologies Programme is the need for a creative, adaptable, diverse and networked workforce with the right balance of skills to ensure long-term benefit from new opportunities in this area.

In late 2016, the lead institutions of the Network of Hubs, the Universities of Birmingham, Glasgow, Oxford and York, were awarded additional funding by the EPSRC through the doctoral training partnership (DTP) studentships scheme, to complement the Hub funding and to address this need.

DTP PhD studentships are flexible, fully funded awards designed to support training at the doctoral level in specialist engineering and physical sciences areas that fit the wider funder remit – in this case, the creation of the next generation of skilled quantum scientists.

All such awards were offered for take-up equitably to partners across the Hub consortium on the basis of submission of appropriate projects seeking to expand the Hub capabilities and expertise. The successful programmes were designed to be multidisciplinary in nature, aimed at developing both academic excellence and adaptable, system-based engineering skills through close collaboration with industry. The ultimate aim was for successful candidates to become part of an emergent quantum ecosystem working with many stakeholders to exploit the potential of the new emerging technologies and stimulate a quantum economy.

Topical areas for consideration included quantum communications and wavelength division multiplexing, photonic systems metrology for quantum communications hardware, quantum networking beyond simple point-to-point networks, high-rate communication networks, experimental projects in quantum digital signatures and quantum amplifiers, theoretical projects in quantum communications and quantum information, quantum technologies focusing on the generation of random numbers, integrated quantum key distribution. Studentships were based at multiple partner institutions across the hub partnership, including at industrial partner sites.

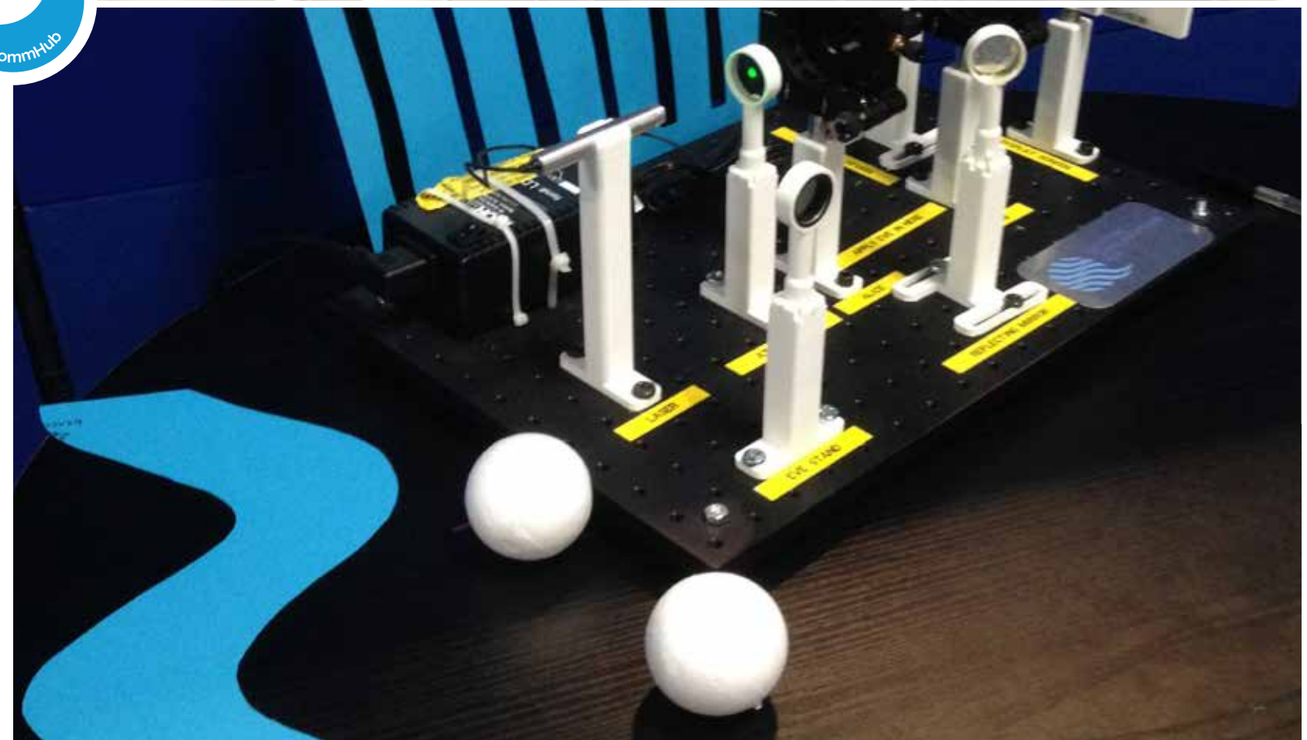
Over the course of the last two years, the Hub has successfully awarded nine such studentships across the partnership – at the Universities of Bristol, Cambridge, Heriot Watt, Strathclyde and York, as well as through secondments to industrial partners such as BT and the National Physical Laboratory.

Public Engagement and Outreach

Engaging with the public developed further as a Hub priority throughout 2017. As well as taking part in the EPSRC commissioned public dialogue, and funding a 2-year targeted school intervention scheme aiming to promote quantum science literacy, Hub members dedicated considerable time designing, preparing and manning technical demonstrations at popular science festivals, giving public talks, engaging with schools and generally promoting the work of the national quantum technologies programme to interested parties.

Particular highlights include: the work of the Heriot Watt University team with select schools in Scotland to devise concept/tutorial questions for Scottish Higher and Advanced Higher students on the topic of quantum theory and its applications; involvement in a series of Women into STEM talks by members of the University of Leeds team; taking part in numerous outreach events (Big Bang, University of Southampton; Soap Box Science Leeds, Pint of Science, York; New Scientist Instant Expert, London; Manchester Science Festival). At the same time, we continued to use social media (Twitter: @QCommHub; YouTube: search for Quantum Communications Hub channel) to reach out and disseminate our work.

Specific mention is merited by Hub colleagues at the University of Bristol's QET Labs, who over the course of the year put together an intense programme of activities, including technical demonstrations at the Cheltenham Science Festival (Splitting the Light Fantastic) and the Royal Society Summer Exhibition (Quantum Computing: Bits to Qubits) – all about the use of light in modern communications, quantum mechanics and the difference between classical and quantum behaviour. This body of work, part of a wider initiative (Quantum in the Crowd) pioneered by Bristol, culminated in late 2017 in QET Labs becoming one of the recipients of the University of Bristol's annual engagement award.



Copyright: University of Bristol

Looking into the future, the Hub will be actively participating in shaping a national quantum technologies programme joint public engagement strategy and series of activities, a particularly exciting development, led by fellow Hub for Quantum Enhanced Imaging (QuantIC) and the team at the University of Glasgow. The initiative will be rolled out over the next year across the Network of Hubs and with involvement from other programme partners such as the National Physical Laboratory and quantum Centres for Doctoral Training (CDTs). The aim is to develop a coherent strategy for engaging with the public through a specially designed website, marketing materials and series of hands-on activities at various science festivals across the country with the view of generating awareness, interest and enthusiasm about the emerging quantum technologies and their potential applications. This body of work will be largely complementary to that of the EPSRC Communications Strategy Group, which is working in parallel with all stakeholders to develop, co-ordinate and implement an integrated communications strategy for the national programme.

APPENDICES

Peer reviewed publications and conference proceedings

Aguado A, Hugues-Salas E, Haigh P, Marhuenda J, Price A, Sibson P, Kennard J & Simeonidou D. Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources. Journal of Lightwave Technology 2017; 8;4: 0733-872

Albrecht MR, Orsini E, Paterson KG, Peer G, Smart NP. (2017). Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts. In Foley SN, Gollmann D, Snekkenes E (Eds.), Computer Security – ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I (Lecture Notes in Computer Science), pp. 29-46

Branny A, Kumar S, Proux R & Gerardot BD. Deterministic strain-induced arrays of quantum emitters in a two-dimensional semiconductor. Nature Communications 2017; 8: 15053 doi:10.1038/ncomms15053

Collins RJ, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Sasaki M, Andersson E, Buller GS. Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution. Scientific Reports 2017; 7: 3235 doi:10.1038/s41598-017-03401-9

Cope TPW, Hetzel L, Banchi L & Pirandola S. Simulation of non-Pauli channels. Phys. Rev. 2017; A 96, 022323. doi:10.1103/PhysRevA.96.022323

Cope T, Pirandola S (2017). Adaptive estimation and discrimination of Holevo-Werner channels. In: Paternostro M (Ed.) Quantum Measurements and Quantum Metrology, 4(1), pp. 44-52

Dada A, Santana T, Koutroumanis A, Ma Y, Park S, Song J, Gerardot B. Experimental triple-slit interference in a strongly driven V-type artificial atom. Phys. Rev. B 96, 081404(R)

Elmabrok O & Razavi M. Quantum-Classical Access Networks with Embedded Optical Wireless Links. In: 2016 IEEE Globecom Workshops. 2016 IEEE Globecom Workshops (GC Wkshps), 04-08 Dec 2016, Washington, DC, USA. doi:10.1109/GLOCOMW.2016.7849014

Elmabrok O, Ghalaii M & Razavi M. Quantum-classical access networks with embedded optical wireless links. J. Opt. Soc. Am. 2018; B 35: 487-499. doi:10.1364/JOSAB.35.000487

Everspaugh A, Ristenpart T, Paterson KG, Scott S (2017). Key Rotation for Authenticated Encryption. In Katz J, Shacham H (Eds.), CRYPTO 2017 (III), Lecture Notes in Computer Science, Vol. 10403. pp. 98-129

Gao Z, Dai B, Buller G & Wang X. Demonstration of 40 Gb/s secure optical communication system based on 40 Gchip/s SPE and symbol overlapping. Contributed talk at Asia Communications and Photonics Conference 2017, Guangzhou, Guangdong, China, 10–13 Nov, 2017

Giacoumidis E, Matin A, Wei J, Doran N & Wu X. Unsupervised Hierarchical Clustering for Blind Nonlinear Equalization in WDM Coherent Optical OFDM. Contributed talk at Asia Communications and Photonics Conference 2017, Guangzhou, Guangdong, China, 10–13 Nov, 2017

Gu M, Pirandola S. (2017) Discord, Quantum Knowledge and Private Communications. In: Fanchini F., Soares Pinto D., Adesso G. (eds) Lectures on General Quantum Correlations and their Applications. Quantum Science and Technology. Springer, Cham, pp. 231-239. doi:10.1007/978-3-319-53412-1_11

Huwer J, Felle M, Stevenson RM, Skiba-Szymanska J, Ward MB, Farrer I, Penty RV, Ritchie DA & Shields AJ. Telecom-wavelength quantum relay using a semiconductor quantum dot. In Conference on Lasers and Electro-Optics (CLEO), OSA Technical Digest (online) (Optical Society of America, 2017), paper FF2E.7. doi:10.1364/CLEO_QELS.2017.FF2E.7

Huwer J, Stevenson RM, Skiba-Szymanska J, Ward MB, Shields AJ, Felle M, Farrer I, Ritchie DA & Penty RV. Quantum-dot-based telecommunication-wavelength quantum relay. Phys. Rev. Applied 2017; 8:024007. doi:10.1103/PhysRevApplied.8.024007

Iten R, Colbeck R & Christandl M. Quantum circuits for quantum channels. Phys. Rev. 2017; A 95: 052316. doi: 10.1103/PhysRevA.95.052316

Kleczkowska K, Vergheese Puthoor I, Bain L & Andersson E. Benchmarking the state comparison amplifier. Phys. Rev. 2017; A 96, 042309. doi:10.1103/PhysRevA.96.042309

Kok P, Dunningham J & Ralph JF. Role of entanglement in calibrating optical quantum gyroscopes. Phys. Rev. 2017; A 95: 012326. doi:10.1103/PhysRevA.95.012326

Laurenza R, Pirandola S. General bounds for sender-receiver capacities in multipoint quantum communications. Phys. Rev. 2017; A96:032318

Lo Piparo N, Razavi M & Munro WJ. Measurement-device-independent quantum key distribution with nitrogen vacancy centers in diamond. Phys. Rev. 2017; A 95: 022338 doi: 10.1103/PhysRevA.95.022338

Lo Piparo N, Sinclair N & Razavi M. Memory-assisted quantum key distribution resilient against multiple-excitation effects. Quantum Sci. Technol. 2018; 3:014009. doi:10.1088/2058-9565/aa9cfb

Ottaviani C, Mancini S, Pirandola S. Gaussian two-mode attacks in one-way quantum cryptography. Phys. Rev. 2017; A95:052310

Papanastasiou P, Ottaviani C & Pirandola S. Finite size analysis of measurement device independent quantum cryptography with continuous variables. Phys Rev 2017; A96:042332 doi:10.1103/PhysRevA.96.042332

Parker RC, Joo J, Razavi M & Spiller TP. Hybrid photonic loss resilient entanglement swapping. J. Opt. 2017; 19:104004. doi:10.1088/2040-8986/aa858a

Pearce ME, Campbell ET & Kok P. Optimal quantum metrology of distant black bodies. Quantum 2017; 1:21. doi:10.22331/q-2017-07-26-21

Pirandola S, Laurenza R, Ottaviani C & Banchi L. Fundamental Limits of Repeaterless Quantum Communications. Nature Communications 2017; 8:15043. doi:10.1038/ncomms15043

Pirandola S & Lupo C. Ultimate precision of adaptive noise estimation. Phys. Rev. Lett. 2017; 118: 100502. doi: 10.1103/PhysRevLett.118.100502

Raffaelli F, Ferranti G, Mahler DH, Sibson P, Kennard JE, Santamato A, Sinclair G, Bonneau D, Thompson MG & Matthews JCF. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. Quantum Sci. Technol. 2018; 3:025003. doi: 10.1088/2058-9565/aaa38f

Roberts GL, Lucamarini M, Yuan ZL, Dynes JF, Comandar LC, Sharpe AW, Shields AJ, Curty M, Puthoor IV & Andersson E. Experimental measurement-device-independent quantum digital signatures. Nat Commun. 2017; 8(1):1098. doi:10.1038/s41467-017-01245-5

Santana TS, Ma Y, Malein RNE, Bastiman F, Clarke E & Gerardot BD. Generating indistinguishable photons from a quantum dot in a noisy environment. Phys. Rev. 2017; B 95: 201410(R). doi: 10.1103/PhysRevB.95.201410

Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner MG, Natarajan GM, Hadfield RH, O'Brien JL & Thompson M. Chip-Based Quantum Key Distribution. Nat Commun 2017; 8:13984. doi:10.1038/ncomms13984

Sibson P, Kennard JE, Stanisic S, Erven C, O'Brien JL & Thompson MG. Integrated Silicon Photonics for High-Speed Quantum Key Distribution. Optica 2017; 4(2): 172-177. doi: 10.1364/OPTICA.4.000172

Vinay S & Kok P. Practical quantum repeaters for ultra-long distance quantum communication. Proc. SPIE 10118, Advances in Photonics of Quantum Computing, Memory, and Communication conference X 2017; 101180E. doi: 10.1117/12.2250497

Vinay SE & Kok P. Practical repeaters for ultra-long distance quantum communication. Physical Review 2017; A 95, 052336. doi:10.1103/PhysRevA.95.052336

Weilenmann M & Colbeck R. Analysing causal structures with entropy. Proc. R. Soc. 2017; A473: 20170483. doi:10.1098/rspa.2017.0483

Wonfor A, Cheng Q, Penty RV & White, Integrated optical switches and short pulse generation using a generic integration platform. In 2016 IEEE Photonics Conference (IPC), Waikoloa, HI, 2016, pp. 226-227. doi:10.1109/IPCon.2016.7831053

Yin H-L, Wang W-L, Tang Y-L, Zhao Q, Liu H, Sun X-X, Zhang W-J, Li H, Vergheese Puthoor I, You L-X, Andersson E, Wang Z, Liu Y, Jiang X, Ma X, Zhang Q, Curty M, Chen T-Y & Pan J-W. Experimental measurement-device-independent quantum digital signatures over a metropolitan network. Phys. Rev. 2017; A 95:042338. doi:10.1103/PhysRevA.95.042338

Zhang Z, Zhao Q, Razavi M & Ma X. Improved key rate bounds for practical decoy-state quantum key distribution systems. Phys. Rev. 2017; A 95: 012333. doi:10.1103/PhysRevA.95.012333

Papers submitted for peer review

Albrecht MR, Orsini E, Paterson KG, Peer G, Smart NP. Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts. Cryptology ePrint Archive: Report 2017/354 ia.cr/2017/354

Amiri R, Abidin A, Wallden P & Andersson E. Unconditionally Secure Signatures, Cryptology ePrint Archive: Report 2016/739, ia.cr/2016/739

Bahrani S, Razavi M & Salehi JA. Wavelength Assignment in Hybrid Quantum-Classical Networks. arXiv:1701.08270

Braun D, Adesso G, Benatti F, Floreanini R, Marzolino U, Mitchell MW, Pirandola S. Quantum enhanced measurements without entanglement arXiv:1701.05152

Elmabrok O, Ghalaii M & Razavi M. Quantum-Classical Access Networks with Embedded Optical Wireless Links. arXiv:1707.02280

Everspaugh A, Paterson K, Ristenpart T & Scott S. Key Rotation for Authenticated Encryption. eprint.iacr.org/2017/527

Iten R & Colbeck R. Smooth Manifold Structure for Extreme Channels. arXiv: 1610.02513

Lacharité MS, Minaud B & Paterson KG. Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage. Cryptology ePrint Archive: ia.cr/2017/701

Laurenza R, Braunstein SL & Pirandola S. Finite-resource teleportation stretching for continuous-variable systems. arXiv:1706.06065

Lupo C, Ottaviani C, Papanastasiou P & Pirandola S. Composable Security of Measurement-Device-Independent Continuous-Variable Quantum Key Distribution against Coherent Attacks. arXiv:1704.07924

Miller CA, Colbeck R & Shi Y. Keyring models: an approach to steerability. arXiv:1706.09275

Newton E, Ghesquiere A, Wilson FL & Varcoe BTH. Quantum Secrecy in Thermal States. arXiv:1711.06592

Ottaviani C, Lupo C, Laurenza R & Pirandola S. High-rate quantum conferencing and secret sharing. arXiv:1709.06988

Ottaviani C, Mancini S, Pirandola S. Gaussian two-mode attacks in one-way quantum cryptography. arXiv:1703.07683

Papanastasiou P, Weedbrook C & Pirandola S. Continuous-variable quantum key distribution in fast fading channels. arXiv:1710.03525

Ren S, Kumar R, Wonfor A, Tang X, Penty R & White I. Reference Pulse Attack on Continuous-Variable Quantum Key Distribution with Local Local Oscillator. arXiv:1709.10202

Scientific presentations at conferences and workshops

Andersson, E. Invited talk "Secure signatures- a practical quantum technology" at SPIE Security & Defence, 26-29 Sep 2016, Edinburgh, UK

Andersson, E. Invited talk "Secure signatures- a practical quantum technology" at a Workshop on Quantum Technology, 13-15 Dec 2016, Chalmers, Gothenburg, Sweden

Andersson E. Invited talk at Conference for Undergraduate Women in Physics, Brasenose College Oxford, 24-26 Mar 2017

Andersson, E. Invited talk "Quantum cryptography beyond quantum key distribution" at the SEPnet school on Quantum Technologies 24-26 Apr 2017, Liphook, UK

Chunnilall C. Traceable Measurements to Enable Certification of QKD Security. Invited talk at 5th ETSI/IQC Quantum Safe Workshop, London, UK, 13-15 Sep 2017

Chunnilall C, Kirkwood R, Patel P & Sinclair A. The development of accurate measurements to provide assurance for QKD technologies. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Chunnilall C. Standards – with special reference to quantum communications. Invited talk at the 2017 National Quantum Technologies Showcase, London, UK, 22 Nov 2017

Colbeck R. Assurance for quantum random number generators. Invited talk at MIQC2 symposium, Cambridge, UK, 20 Sep, 2017

Colbeck R. Entropic constraints on causal structures. Invited talk at Frontiers of quantum information physics workshop, Santa Barbara, United States, 13 Oct, 2017

Collins R, Amiri R, Fujiwara M et al. Quantum Digital Signatures Transmitted Over a Channel Loss Equivalent to 134 km. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Cope T & Colbeck R. Exploiting no-Signalling Extremal Distributions to find Bell Inequalities. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Cope T, Hetzel L, Banchi L & Pirandola S. Teleportation Simulation of non-Pauli Channels. Poster presentation at CEWQO 2017 - 24th Central European Workshop on Quantum Optics, Dtu Lyngby, Denmark, 26-30 June 2017

Cope T, Hetzel L, Banchi L & Pirandola S. Teleportation Simulation of non-Pauli Channels. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Ding M, Wonfor A, Cheng Q, Penty RV & White IH. Scalable, Low-Power-Penalty Nanosecond Reconfigurable Hybrid Optical Switches for Data Centre Networks. Poster presentation at CLEO: Applications and Technology 2017, San Jose, California, United States, 14–19 May, 2017

Ding M, Wonfor A, Cheng Q, Penty RV & White IH. Emulation of a 16×16 Optical Switch Using Cascaded 4×4 Dilated Hybrid MZI-SOA Optical Switches. Contributed talk at CLEO: Applications and Technology 2017, San Jose, California, United States, 14–19 May, 2017

Donaldson R, Mazzarella M, Collins R et al. State comparison amplification of optical quantum coherent states. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Elmabrok O, Ghalaii M & Razavi M. Wireless Access to Quantum Networks. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Erven C. Starting up the quantum industry and the importance of ethical tweeting. Keynote address at the Single Photons Single Spins (SPSS II) workshop, Troyes, France, 29 Aug – 1 Sep, 2017

Erven, C. (& Kennard, J.). Invited talk at UK-NL Cyber Security Showcase. Hosted by Department for International Trade – The Netherlands, 30 Nov 2016

Gerardot B. Quantum optics with deterministically positioned quantum emitters in a 2D semiconductor. Invited talk at DPG Spring Meeting, Germany, 19-22 Feb, 2017

Geardot B. Quantum emitters in transition metal dichalcogenides. Invited talk at CNRS & Toulouse University Colloquium, France, 17 May, 2017

Gerardot B. Nuclear Spin Noise Effects on Resonance Fluorescence from Quantum Dots. Invited talk at OSA Incubator Meeting Integrated Semiconductor Quantum Photonic Devices, USA, 4-6 Aug, 2017

Gerardot B. Quantum emitter properties in 2D semiconductors. Invited talk at Rank Prize Symposium on Solid State Nano-Photonics for Quantum Science and Technology, UK, 25-28 Sep, 2017

Geardot B. Two-dimensional single photon sources. Invited talk at 5th international workshop on Engineering of Quantum Emitter Properties, Waterloo Institute for Quantum Computing, Canada, 13-15 Dec, 2017

Ghalaii M, Kumar R & Razavi M. Quantum-Scissor Amplified Continuous-Variable Quantum Key Distribution. Poster presentation at CLEO/Europe-EQEC 2017 (Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference), Munich, Germany, 25-29 June 2017

Ghalaii M, Kumar R, Ottaviani C et al. Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep 2017

Ghesquiere A, Wilson F, Newton E et al. Quantum cryptography using thermal states. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep 2017

Huwer J, Felle M, Stevenson M et al. Quantum-dot-based quantum relay operating at telecom wavelength. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep 2017

Jin, RB., Fujiwara, M., Shimizu, R., Collins, RJ., Buller, GS., Yamashita, T., Miki, S., Terai, H., Takeoka, M. & Sasaki, M. Contributed talk "Detection dependent six–photon NOON state interference", QCMC2016, Singapore, 4-8 Jul 2016

Joo J. Invited talk "A tool box for quantum information technologies" at the GRADnet Quantum Technologies School, Liphook, UK, 24-26 April 2017

Kumar R, Wonfor A, Penty R & White I. Quantum-Classical Transmission on Single Wavelength. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Laing A. Quantum Science and Technologies. Invited talk at the Festival of Physics (IoP) in Bristol, 4 Mar 2017

Laing A. Photonic Quantum Technologies. Invited talk at Quantum 2017, Turin, Italy, 7-13 May 2017

Laing A. Integrated Quantum Photonics. Invited talk at the Heilbronn Focused Research Group on Quantum Computational Supremacy workshop, Bristol, UK, 16 Aug, 2017

Laing A. Photonic Quantum Technologies. Invited talk at 1st Asia-Pacific Workshop on Trapped Quantum Systems, Zhuhai, China, 8-11Dec, 2017

Laurenza R. Contributed talk "Two-way assisted capacities for quantum and private communications" at QIP 2017, Seattle USA, 16-20 Jan 2017

Laurenza, R. & Pirandola, S. Poster presentation "General bounds for sender-receiver capacities in multipoint quantum communications" at CEWQO 2017 -24th Central European Workshop on Quantum Optics, 26-30 Jun 2017, Dtu Lyngby, Denmark

Lupo, C. & Pirandola S. Contributed talk "Ultimate precision bounds for the estimation and discrimination of quantum channels" at CEWQO 2017 -24th Central European Workshop on Quantum Optics, 26-30 Jun 2017, Dtu Lyngby, Denmark

Laurenza R, Braunstein S & Pirandola S. Finite-resource teleportation stretching for continuous-variable systems. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Laurenza R & Pirandola S. General bounds for sender-receiver capacities in multipoint quantum communications. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Lord A, Wakeling J, Spiller T. Quantum Communications. Invited talk at BT Innovation Week 2017, 12-16 June 2017

Lowndes D, Frick S, Harrington B & Rarity J. Low Cost, Short Range Quantum Key Distribution. Poster presentation at CLEO/Europe-EQEC 2017 (Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference), Munich, Germany, 25-29 June 2017

Lupo C, Ottaviani C, Papanastasiou P & Pirandola S. Composable Security of Measurement-Device-Independent Continuous-Variable Quantum Key Distribution against Coherent Attacks. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Mazzarella L, Donaldson R, Collins R et al. Quantum State Comparison Amplifier with Feedforward State Correction. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Ottaviani C, Lupo C & Pirandola S. Poster presentation "Multipartite measurement-device independent quantum conferencing" at CEWQO 2017 -24th Central European Workshop on Quantum Optics, 26-30 Jun 2017, Dtu Lyngby, Denmark

Ottaviani C, Lupo C & Pirandola S. Poster presentation "Microwave quantum cryptography" at CEWQO 2017 -24th Central European Workshop on Quantum Optics, 26-30 Jun 2017, Dtu Lyngby, Denmark

Ottaviani C, Lupo C, Laurenza R & Pirandola S. Multipartite measurement-device independent quantum cryptography: Conferencing and secret sharing. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep 2017

Ottaviani C, Lupo C & Pirandola S. Thermal quantum cryptography: Solutions at the microwave regime. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep 2017

Papanastasiou P, Ottaviani C & Pirandola S. Finite-size analysis of thermal and continuous-variables measurement-device-independent quantum cryptography. Poster presentation at CEWQO 2017 - 24th Central European Workshop on Quantum Optics, Dtu Lyngby, Denmark, 26-30 June 2017

Papanastasiou P, Ottaviani C & Pirandola S. Finite-size analysis of thermal and continuous-variables measurement-device-independent quantum cryptography. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Parker R, Joo J, Razavi M & Spiller T. Hybrid Photonic Loss Resilient Entanglement Swapping. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Paterson, K. The Evolution of Public Key Cryptography in SSL/TLS. Invited talk at 20th International Conference on Practice and Theory of Public-Key Cryptography, Amsterdam, the Netherlands, 28-31 Mar 2017

Paterson, K. Quantum Key Distribution OR Post Quantum Cryptography?. Invited talk at BT Adastral Park event, 3 Feb 2017

Paterson K. Secure storage in the cloud using property preserving encryption. Invited talk at ECRYPT NET 2017 - Workshop on Crypto for the Cloud & Implementation, Paris, France, 27-28 June 2017

Paterson K. Participation in panel discussion on the Importance of Standardisation, during 5th ETSI/IQC Quantum Safe Workshop, London, 13-15 Sep 2017

Paterson K. IRTF update. Invited talk at the 5th ETSI/IQC Quantum Safe Workshop, London, 13-15 Sep 2017

Penty RV, Ding M, Wonfor A & White IH. Scaling of Low Energy InP SOA Based Switches. Contributed talk at Photonics in Switching 2017, New Orleans, Louisiana, United States, 24–27 Jul, 2017

Pirandola S. Ultimate performance of quantum network communications. Invited talk at QCS 2017 - Workshop on Quantum CyberSecurity, Canterbury, UK, 22-23 June 2017

Pirandola S. Capacities of repeater-assisted quantum communications. Invited talk at CEWQO 2017 - 24th Central European Workshop on Quantum Optics, Dtu Lyngby, Denmark, 26-30 June 2017

Pirandola S. Ultimate performance of repeater-assisted quantum communications. Invited talk at 2nd workshop for quantum repeaters and networks. Seefeld, Austria, 25-26 Sep 2017

Price A, Rarity J & Erven C. Quantum Key Distribution Without Sifting. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Puthoor, I. Contributed talk on Measurement-device-independent quantum signatures, QCrypt, 4th ETSI/IQC Workshop on Quantum Safe Cryptography, 19-21 Sep 2016, Waterloo, Canada

Puthoor I. Contributed talk ("Measurement-device-independent quantum digital signatures") at Quantum Information Scotland (QuISco) meeting on 16th June 2017, at the University of St. Andrews, UK.

Raffaelli F, Ferranti G, Mahler D et al. An On-chip Homodyne Detector for Generating Quantum Random Numbers and Measuring Coherent States. Poster presentation at at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Razavi, M. Quantum communications technologies: now and the future. Invited talk at Workshop on Quantum Information Processing, School of Physics, IPM, Tehran, Iran, 27-29 Dec 2016

Razavi, M. Memory-assisted quantum key distribution. Invited talk at Workshop on Quantum Information Processing, School of Physics, IPM, Tehran, Iran, 27-29 Dec 2016

Razavi represented the Hub at the invitation-only Workshop on Quantum Cryptography and Communication Networks and Applications, organised by the European Commission – DG CNECT, Brussels, Belgium, 20 April 2017

Razavi M. From theory to practice: What it takes for quantum repeaters to prove useful? Invited talk at 2nd workshop for quantum repeaters and networks. Seefeld, Austria, 25-26 Sep 2017

Roberts GL, Lucamarini M, Yuan Z et al. Reconfigurable network for quantum digital signatures mediated by measurement-device-independent quantum key distribution. Contributed talk at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Shields A. Quantum communications using semiconductor devices. Invited talk at CEWQO 2017 - 24th Central European Workshop on Quantum Optics, Dtu Lyngby, Denmark, 26-30 June 2017

Shields A. Core and access QKD networks. Invited tutorial at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Shields A. Quantum Communications. Plenary talk at 2017 National Quantum Technologies Showcase, London, UK, 22 Nov 2017

Shields A. UK Quantum Network. Invited talk at 2017 National Quantum Technologies Showcase, London, UK, 22 Nov 2017

Sibson P, Lowndes D, Frick S et al. Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol's Activities in the UK Quantum Communications Hub. Contributed talk at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Spiller T. Quantum technologies and their implications for cyber security. Invited talk at the 'European Cybersecurity: Future Trends and Policy Challenges' international workshop, Oxford, 26-27 January 2017

Spiller T. Quantum Communications Technologies. Invited talk at the GRADnet Quantum Technologies School, Liphook, UK, 24-26 April 2017

Spiller T. UK Perspective: the Quantum Communications Hub. Invited talk at the 5th ETSI/IQC Quantum-Safe Cryptography workshop, London, UK, 13-15 September 2017

Spiller T. The UK Quantum Communications Hub and the implications for Cyber Security. Invited talk at the 2nd UK_NL Cyber Security Showcase, The Hague, The Netherlands, 27 Sep 2017

Spiller T. The UK Quantum Communications Hub. Invited talk at "2nd Quantum Technology – Implementations for Space" workshop at ESTEC, Noordwijk, The Netherlands, 14-15 Nov, 2017

Spiller T. The UK Quantum Communications Hub. Invited talk at 2017 National Quantum Technologies Showcase, London, 22 Nov 2017

Tang X, Wonfor A, Kumar R et al. Crosstalk Limitations on Reconfigurable QKD Networks. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Vinay S, Pearce M & Kok P. The Quantum Trojan Horse Attack. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

White IH, Ding M, Wonfor A, Cheng Q & Penty RV. High Port Court Switch Architectures for Data Center Applications. Contributed talk at Photonic Networks and Devices 2017, New Orleans, Louisiana, United States, 24–27 Jul, 2017

Wonfor A, Dynes J, Kumar R et al. High performance field trials of QKD over a metropolitan network. Poster presentation at Qcrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 18-22 Sep, 2017

Selected Public Engagement Activities

Andersson E. Invited talk at the Conference for Undergraduate Women in Physics, Oxford, 23-26 March 2017.

Andersson, E. Invited talk at New Scientist "Instant Experts" event on quantum physics on 14 Oct 2017, London

Colbeck R. Pint of Science talk ("Do atoms behave randomly?"), 15 May 2017, York

Members of the Bristol University Hub team attended the Manchester Science Festival (26 October 2017), where they presented a hacking demonstration.

The QTEC Labs team took part at the Cheltenham Science Festival (6-11 June 2017) with an exhibit about properties of light.

The QTEC Labs team took part in the Royal Society Summer Science Exhibition (London, 3-9 July 2017) with an exhibit titled: Quantum computing: bits to qubits.

Selected Media Coverage

"Chips with everything – as long as they're quantum", press release posted on 8 December 2016 on the University of Bristol website http://www.bristol.ac.uk/news/2016/december/quantum-chip-science-museum-.html

"Bristol's quantum chip goes on display at the Science Museum", newsitem posted on 15 December 2016 on techspark.co https://techspark.co/bristols-quantum-chip-goes-display-science-museum/

"How quantum mechanics is working to protect security online", University of Bristol press release, 6 March 2017 http://www.bristol.ac.uk/news/2017/march/protect-security-online.html

"How quantum mechanics is working to protect security online", University of Bristol YouTube video, 6 March 2017 https://www.youtube.com/watch?v=EV6xXvF5i2Q&feature=youtu.be&a

"World's first quantum encryption chip developed", newsitem posted on 9 March 2017 on techspark.co https://techspark.co/worlds-first-quantum-encryption-chip-developed/

"Establishing the boundaries of quantum secure communications", University of York press release, 26 April 2017 https://www.york.ac.uk/news-and-events/news/2017/research/qkd-communications-computer/

Hub Director, Tim Spiller, was interviewed by freelance adviser David Shaw for a report titled The Second Quantum Revolution - Action for Business (available to access via LinkedIn https://www.linkedin.com/feed/update/urn:li:activity:6331132380358807553) – November 2017

How to quantum secure optical networks, online news item on www.fibre-systems.com by H. Griesser, Director of Advanced Technology at ADVA Optical Networking (23/10/17 - available to access at https://www.fibre-systems.com/feature/how-quantum-secure-optical-networks

BT, Telecom Infra Project and Facebook announce start-up competition winners, press release announcing KETS as one of three SMEs to be admitted into the UK Telecom Infra Project Ecosystem Acceleration Centre (TEAC). Accessible at http://www.btplc.com/News/#/pressreleases/bt-telecom-infra-project-and-facebook-announce-start-up-competition-winners-2186175 (02/11/17)

TEAC programme connects Bristol spinouts, online news piece published on globaluniversityventuring.com about KETS being admitted into the TEAC programme. Accessible at http://www.globaluniversityventuring.com/article.php/6196/teac-program-connects-bristol-spinouts

Reporter's Phablet: Is It Time To Panic About Quantum Computing's Dark Side? News piece on The Wall Street Journal by Sara Castellanos reporting from London and the ETSI Quantum Safe Workshop (15/09/17). Available to access at https://blogs.wsj.com/cio/2017/09/15/reporters-phablet-is-it-time-to-panic-about-quantum-computings-dark-side/?mod=djemCIO_h (Paywall)

Quantum Promise, feature piece on consumer security online including commentary by T. Spiller on the September issue of TS Today, the online monthly trading standards magazine published by the Chartered Trading Standards Institute. Available to access through: http://portfolio.cpl.co.uk/TS-Today/201709/feature/

Cyber attacks: the response is coming, (with input by Laing/Spiller) online piece published in the technologist.eu, available to access here: http://www.technologist.eu/cyber-attacks-the-response-is-coming/#cmtoc_anchor_id_5

A quantum of security, online feature item published on fibre-systems.com and discussing Hub work on UK's quantum network. Available to access through: https://www.fibre-systems.com/feature/quantum-security

Distinctions and Awards

Professor Gerald Buller, Heriot Watt University was elected Fellow of The Optical Society of America in the Class of 2017 (01/01/17) "for pioneering work in single-photon detection and applications of single-photon technology in three-dimensional imaging and quantum communications" (Engineering and Science Research). Buller collected his award at the CLEO 2017 conference in California in May 2017.

Professor Kenny Paterson was awarded an IACR (International Association for Cryptologic Research) fellowship at EUROCRYPT 2017 in Paris, France. The award was made for Paterson's research and service contributions spanning theory and practice, and for improving the security of widely deployed protocols.

Professor Kenny Paterson became Editor-in-Chief for the Journal of Cryptology in January 2017.

Colleagues in QETLabs at Bristol received the University's 2017 engagement award for their outreach work.

KETS Quantum Security were announced as one of three winners to be admitted to the UK Telecom Infra Project Ecosystem Acceleration Centre (TEAC), based at BT Lab facilities in London's Tech City and Adastral Park, Suffolk.


UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME
UK QUANTUM TECHNOLOGY HUB
FOR QUANTUM COMMUNICATIONS TECHNOLOGIES
ANNUAL REPORT
2014
2015


UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME
UK QUANTUM TECHNOLOGY HUB
FOR QUANTUM COMMUNICATIONS TECHNOLOGIES
ANNUAL REPORT
2015
2016

Quantum Communications Hub
Information Centre
Market Square
University of York
Heslington
York, YO10 5DD
United Kingdom

tel: + 44 (0) 1904 32 4410
enquiries@quantumcommshub.net

www.quantumcommshub.net

The UK Quantum Technology Hub for Quantum Communications Technologies is funded via EPSRC grant no EP/M013472/1.