UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UK QUANTUM TECHNOLOGY HUB

FOR QUANTUM COMMUNICATIONS TECHNOLOGIES

ANNUAL REPORT

2015 2016

QUANTUM
COMMUNICATIONS
HUB

Contents

Special thanks to all contributors:

Erika Andersson, Klitos Andrea, Gerald Buller, Emilio Hugues-Salas, Rupesh Kumar, Georgia Mortzou, Reza Nejabati, Kenny Paterson, John Rarity, Andrew Shields, Timothy Spiller, Mark Thompson, Adrian Wonfor.

Thanks to the following for kindly providing images: Professor Erika Andersson, Professor Gerald Buller, Dr Robert Collins, Dr Andrew Shields, Dr Adrian Wonfor, the Centre for Quantum Photonics (Quantum Engineering Technology Labs) University of Bristol, the Quantum Europe 2016 conference organising team, the National Institute of Information and Communications Technology in Japan.

Foreword

As part of the wider UK National Quantum Technologies Programme, the Quantum Communications Hub is delivering new quantum technologies for secure data services applicable to commercial, consumer, defence and government markets. Our technology delivery strategy during the initial five-year period of the UKNQT Programme is to focus on taking proven quantum key distribution (QKD) technologies and advancing these to commercial-ready status.

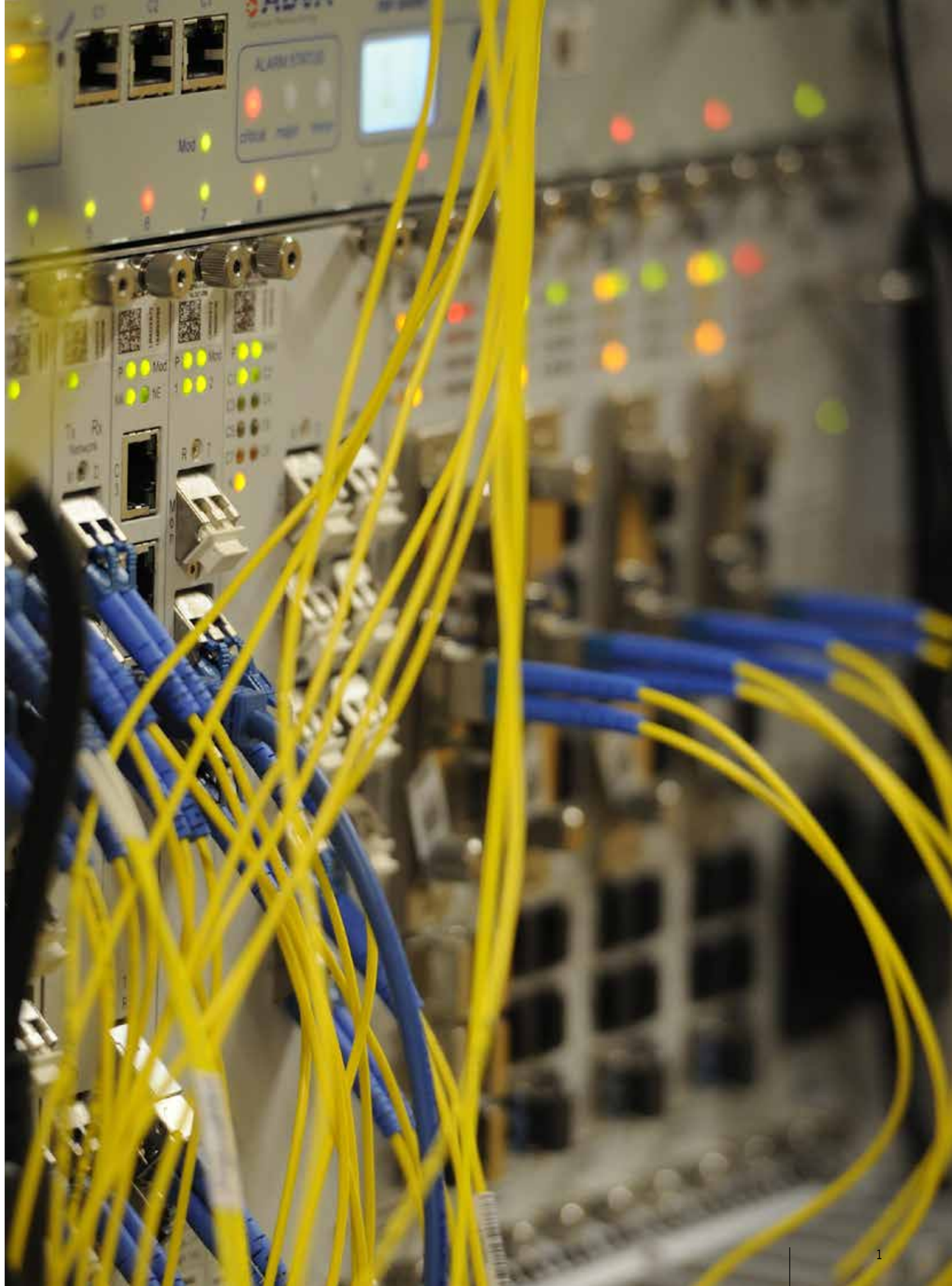
This second year has been one of consolidation and growth for our Hub, during which time we have achieved major technology breakthroughs. We have developed a credit-card size transmitter unit for many-to-one applications, and initial key-exchange trials with the receiver are now underway. We have performed the world's first demonstration of chip-to-chip QKD, with very competitive performance. We have consolidated the record (200G) bandwidth for sending quantum keys and encrypted data down the same fibre, while construction of the UK's first Quantum Network is well underway.

The Hub has also demonstrated major advancements with next generation applications. Invention of a new protocol for quantum digital signatures has taken this work from laboratory experiments to a real demonstrator, and a huge (1000-fold) increase in key rate has been achieved with measurement device independent (MDI) QKD. Despite challenges to procurement and recruitment, we have met or exceeded our two-year deliverables, and so we are well on course towards the five-year targets.

At the same time, we remain aware of, and sensitive to, the growing importance of information security, the evolving world landscape and its implications for this security, and the development and progress of other quantum communications activities worldwide. Data security raises a range of issues for individuals, companies and governments, so in addition to our expanding user engagement, we have a very active programme of public engagement, extending appreciation of the issues and implications of the new technologies.

We look forward to continuing our technology delivery for the benefit of the UK, and enhancing the UK's leadership and standing in quantum communications on the world stage.

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.

»SECURITY«

Introduction

The Quantum Communications Hub is a technology research and development consortium of UK Universities, private sector companies and public sector stakeholders. It is funded by the UK National Quantum Technologies Programme, an original government investment of £270 million, aiming to facilitate the commercialisation of newly emerging quantum technologies. Part of a Network of four Quantum Technology Hubs, this Hub's 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) systems, we aim to advance these to a commercialisation-ready stage. We are also advancing new directions and applications, developing prototype "next generation" (beyond basic QKD) quantum communications technologies.

We are delivering three major advances to QKD technologies, each in a separate technology theme:

- Short-range, free-space, QKD systems. These technologies will enable many-to-one, short-range, quantum-secured communications, for consumer, commercial and defence markets.
- "QKD-on-a-chip" modules: scaled down and integrated QKD component devices, for producing robust, miniaturised sender, receiver and switch systems. 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 (UKQN), which integrates QKD into secure communication infrastructures at access, metropolitan and inter-city scales. This advance will enable device and system trials, integration of quantum and conventional communications, and – critically –demonstrations for engagement of users, stakeholders, customers, the media and the wider public.

Furthermore we are undertaking investigative and experimental work in "next generation" quantum communications technologies, including: (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.

Summary of the second year

The second year was marked by significant technological progress and expansion of both our interests and the partnership. Our vision for the three main technology themes continued its timely focus on the QKD technologies closest to commercialisation. Our portfolio in next generation quantum communications technologies continued to evolve flexibly, within the overall vision of quantum solutions that will address various current technological limitations, or offer new applications and services. We started the Hub with some recognised capability gaps; for example, we did not have (Hub-) internal development programmes for new source and detector component technologies and we did not have an R&D thread for quantum communications in space. Our vision is evolving to include relevant new work, using the flexibility that exists in Hub resources, including funding available for new developments, the so-called partnership resource fund. Examples include: in collaboration with the NQIT Hub, take-up of an active guidance project that will contribute to short-range, free-space QKD and also to QKD technologies for space; movement of Hub resources to support semiconductor sample growth in the Cavendish Laboratory for Hub investigators working on source and detector devices; building on a workshop that we organised at ESA Harwell and follow-on meetings with stakeholders and potential partners, we are now actively developing a Hub strategy for QKD technology in space and on satellites (or high altitude platforms), leading towards feasibility studies, technology demonstrations and collaborative projects.

International engagement and impact on policy

International collaboration is the natural route for major space or satellite projects and provides an example of our strategy and ambition as a global centre of excellence. Hub investigators have provided significant input to the EU Quantum Manifesto, leading to the Quantum Flagship. We have established collaborative links with major national centres, notably NICT in Japan. Our growing international standing is reflected by the invitations to lead two major international conferences in 2017, QCRYPT (to be hosted in Cambridge) and the ETSI Quantum Safe Workshop (to be hosted in London).

To date we have organised and hosted a range of cluster events, contributed to EU and wider international policy meetings. We had a strong presence on the Blackett Review expert panel for quantum technologies, and Hub investigators have undertaken a broad spectrum of public engagement activities. The metro(politan)-networks of the UK Quantum Network in Bristol and in Cambridge, along with the network link to BT's Adastral Park Research and Innovation cluster (separately funded by an EPSRC capital award), will be providing the foci for major piloting and demonstration activities with industry.

Secure quantum communications are the subject of specific attention in a number of different countries worldwide. Using the very strong international links of our academic and industry partners, the Hub is engaging with individuals, institutions and companies involved in various international initiatives, whilst being aware that there may be common or diverging interests (and International Traffic in Arms Regulations – ITAR – or export control considerations), for both development and exploitation. This breadth of initial engagement is aimed at ensuring that the UK benefits from knowledge of, and where appropriate, collaboration with, activities worldwide that are relevant to the Hub's remit. Standards, policy and earlier-stage research (as opposed to later-stage, commercially focused, development) thus form the preferred routes for the Hub's international engagement strategy.

There are numerous significant QKD network initiatives worldwide, with either common or overlapping interests to those of the Hub. These include R&D; engineering and implementation of QKD systems; industrial engagement and partnerships; commercial imperatives; standards, regulation and legal frameworks; social and political complexities of securing data in the modern world. These matters are of varying weight and priority in the different countries where QKD networks have been or are being built – by governments, industry, research institutions, or a combination of all. Significant networks exist in North America, Europe and Asia – this geographical spread reflects the importance attached to QKD networking around the world. These networks differ from each other in various ways - from age, size and purpose; equipment and protocols; current status and future plans; nature and strength of collaborations. The Hub has established, or is in the process of establishing, productive relationships with relevant international QKD activities.

Public engagement and outreach

Central to the National Quantum Technologies Strategy is creation of the "right social and regulatory context" for quantum technologies. This is particularly relevant for quantum communications, as data security raises a plethora of issues for individuals, institutions, companies and governments. To promote open discussion on the technologies and services we are delivering, the Hub's strategy incorporates educational, public and user engagement activities, and cross-Hub coordination. Highlights include: consultation on educational materials for use in secondary schools; production of public engagement videos and filmed interviews with stakeholders; participation in numerous public engagement events through talks, panel discussions, debates and demos (Times Cheltenham Science Festival, York Festival of Ideas, Pint of Science, Illuminations); school visits; use of social media (YouTube, Twitter) – all to relate the work of the Hub to a wider audience. High-profile, public technical demonstrations of the technologies developed in the Hub are part of our detailed user engagement strategy. More activities are planned in 2017 and beyond, using the UK Quantum Network.

Future plans

Looking ahead, the Hub will build upon existing commitments to develop prototypes and demonstrators from across its technology themes. Arrangements are in place to demonstrate a system (QKD-enabled device talking to an ATM) in a high-profile showcase banking environment, a first step towards piloting adoption within the financial services industry. Chip-scale integration of QKD has stimulated significant industry interest, and the company created to exploit it (KETS) has made a very promising start, with the technology attracting commercial interest including licensing. We will continue to develop next generation quantum communications technologies with longer lead times, and pipeline these for demonstration within the Hub's initial 5-year programme.

Another vital aspect of our work over the next three years will be acceleration of user engagement. The UK Quantum Network will play a major role in widening and deepening engagement: a platform for demonstrating our technologies, trial services to consumer, commercial and government users, and the active participation of early adopters. The Hub's strategy for commercialisation is to develop and maintain a variety of options across a range of users – from large service providers and technology companies through SMEs to start-ups. This was embedded in the initial Hub consortium and continues to evolve.

Since the start of the Hub the role of BT has expanded significantly, and through the company's international partner networks, we are also establishing links with service providers in other countries. The contributions of Toshiba (via TREL) and ID Quantique to the Hub, and particularly to the UK Quantum Network and its recent extension, continue to develop.

Plans for new developments include an extension of the UK Quantum Network. A significant step towards this was achieved by securing substantial industry collaboration and additional EPSRC capital funding for connecting the quantum network in Cambridge to BT's Research and Innovation ICT cluster at Adastral Park in 'Silicon Fen', stimulating industrial exploitation of the network by facilitating direct connection of companies to it. The network will be publicly demonstrated in 2017, including commitment to invite manufacturers of systems from around the world to connect them to the network to demonstrate interoperability.

The Hub also has ambitions to support, promote and demonstrate industry-focused developments in new areas of QKD, subject to current review of options and feasibility. These include, notably, CV-QKD and Satellite-QKD – both of which have strong industrial pull; the former for use in metro-scale networks, the latter for distances beyond optical fibre capability and necessitating international collaboration.

The Partnership

National Cyber Security Centre
a part of GCHQ

TOSHIBA
Leading Innovation

HERIOT WATT UNIVERSITY

ADVA Optical Networking

AIRBUS DEFENCE & SPACE

Cambridge Network

UNIVERSITY OF CAMBRIDGE

BRISTOL CITY COUNCIL

BT

ROYAL HOLLOWAY UNIVERSITY OF LONDON

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

NPL
National Physical Laboratory

UNIVERSITY of York

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 Team

Includes, in addition to the Management Team, the Senior Co-Investigators listed below, 27 Research associates, 19 PhD students, a business development manager, project co-ordinator 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
- Dr Stefano Pirandola

BT
- Dr Andrew Lord

Toshiba Leading Innovation
- Dr Andrew Shields

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

Overview: **The Second Year**

Having established the necessary administrative, contractual and operational machinery of the Hub, work in the second year focused on achieving major technology breakthroughs primarily towards the development of miniaturisation prototypes and installation of infrastructure for the quantum network. This R&D work was firmly embedded in a programme of parallel activities including industry and user engagement stakeholder events, training workshops, scientific conferences, policy roundtables, and numerous public engagement initiatives. The defining features of the second year have been growth and expansion across the partnership: new collaborating partners and aligned projects (through allocation of partnership resource); new doctoral students (through EPSRC's training partnership scheme); expanding UK Quantum Network infrastructure (through work on an additional £2m EPSRC capital equipment grant); strengthened international links; a more ambitious Hub vision exploring gaps in UK space capability and satellite links.

Specifically, in the second year, we have:

- Made significant progress across all technology themes
- Organised four expert workshops on Quantum Digital Signatures, Continuous Variable QKD, QKD in Space and Microwave QKD
- Led the organisation of the 2nd National Quantum Technologies Showcase with more than 600 delegates from the UK and abroad
- Initiated work on the extension to the UK Quantum Network project, linking Cambridge with BT's Adastral Park research facility
- Invested in a number of partnership resource projects that demonstrated clear potential to enhance delivery of the Hub's core outputs
- Strengthened links with the modern cryptography community through two training workshops organised by partner Royal Holloway for members of the Hub
- Made available 18 EPSRC PhD studentships for graduates wishing to pursue further study in quantum technologies
- Contributed significantly to the Government Office for Science Blackett Review for Quantum Technologies
- Expanded our international engagement activities through collaborative meetings and exchange visits in Japan, and exploratory talks with research groups in Canada, Austria, Germany, Italy, and South Korea on quantum networks and quantum satellite communications
- Continued to impact policy through direct contributions to various European Commission policy debates and round tables, including the €1bn EU Quantum Flagship investment programme
- Continued our work with industrial standards development bodies in particular for optical component characterisation for QKD and implementation security for QKD systems
- Been invited to host two major international conferences in 2017: the 7th International Conference on Quantum Cryptography (QCrypt 2017) and the 5th ETSI/IQC International Workshop on Quantum Safe Cryptography
- Expanded our public engagement activities through numerous school visits, science festival appearances, general talks
- Published 36 peer-reviewed papers, book chapters and conference abstracts and submitted another 17 papers for peer review
- Delivered more than 100 presentations on our work at various conferences, workshops, industry and user engagement events, both in the UK and abroad
- Adopted the use of social media such as Twitter and YouTube in order to support user engagement and knowledge transfer activities, as well as our wider public engagement

Technology Development:
Progress in the Second 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.

Application Space: 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.

Connecting Alice to Bob: 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. Our initial scheme for establishing an optical link between the devices is to use a card slot-inspired mechanical design which positions the end of an optical fibre on the handheld transmitter into focussing optics which are aligned to the receiver detectors. This arrangement is sufficient for system operation. However, as part of the partnership resource funding of this project, we have started a collaboration with the University of Oxford (NQIT Hub) to adapt their active alignment system to the front of our Quantum ATM. The active alignment uses a bright beacon signal to monitor hand position jitter and adjustable tip-tilt mirrors to compensate – allowing for true handheld operation.

Handheld Transmitter (Alice): The transmitter is roughly the size of a chip and pin card authenticator device such as Barclays' PINSentry, the electronics are USB powered and interfaced and we are investigating either basic mobile phone integration (as a clip-on module) or adding a small system-on-chip processor to the next generation prototype. The device emits 2.1ns optical pulses at a repetition frequency of 100MHz. In parallel to this work, we are investigating hardware methods of generating secure random numbers on the device which will also be included in later prototypes.

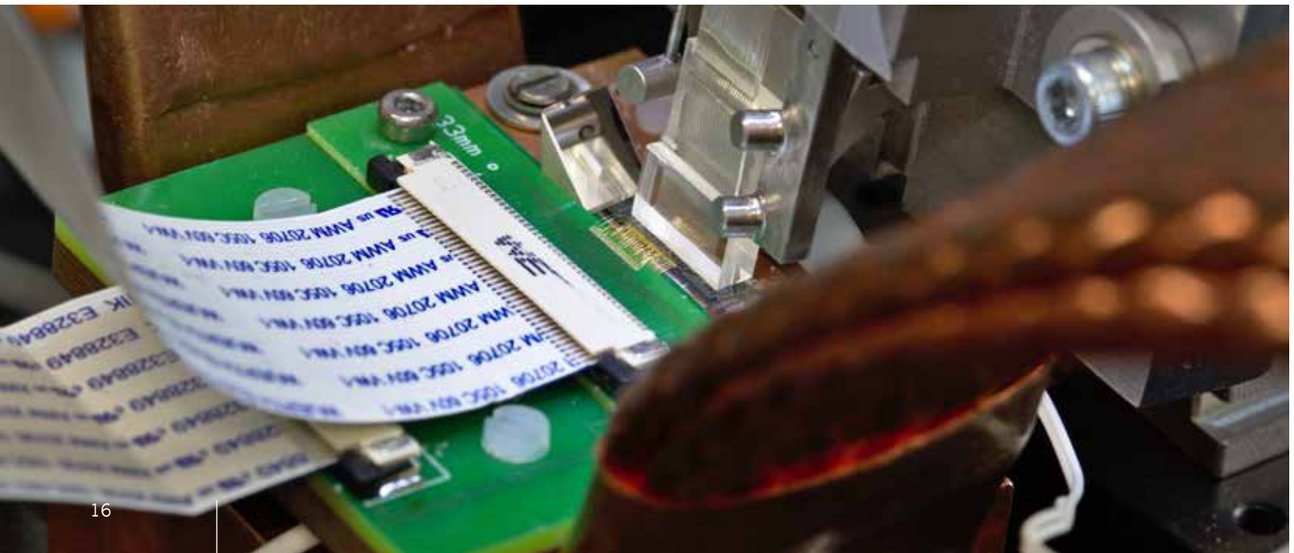
Quantum ATM (Bob): We currently have a prototype Quantum ATM ready which contains optical and electronic hardware for characterising the input light and performing the required processing for QKD. The main characterisation performed is to correct the misalignment between the transmitter's and the receiver's polarization bases which is induced by the fibre based mode filter in the transmitter. This is performed by measuring the incoming light in H/V, D/A and R/L bases and calculating the wave-plate angles for a wave-plate based polarization controller on the input of the receiver. The QKD processing will be performed by a modular software suite, currently in development in conjunction with the technology theme 3 efforts in Bristol. This suite will standardise certain common aspects of different QKD protocols to improve reliability and help with integrating these devices into a wider QKD network.

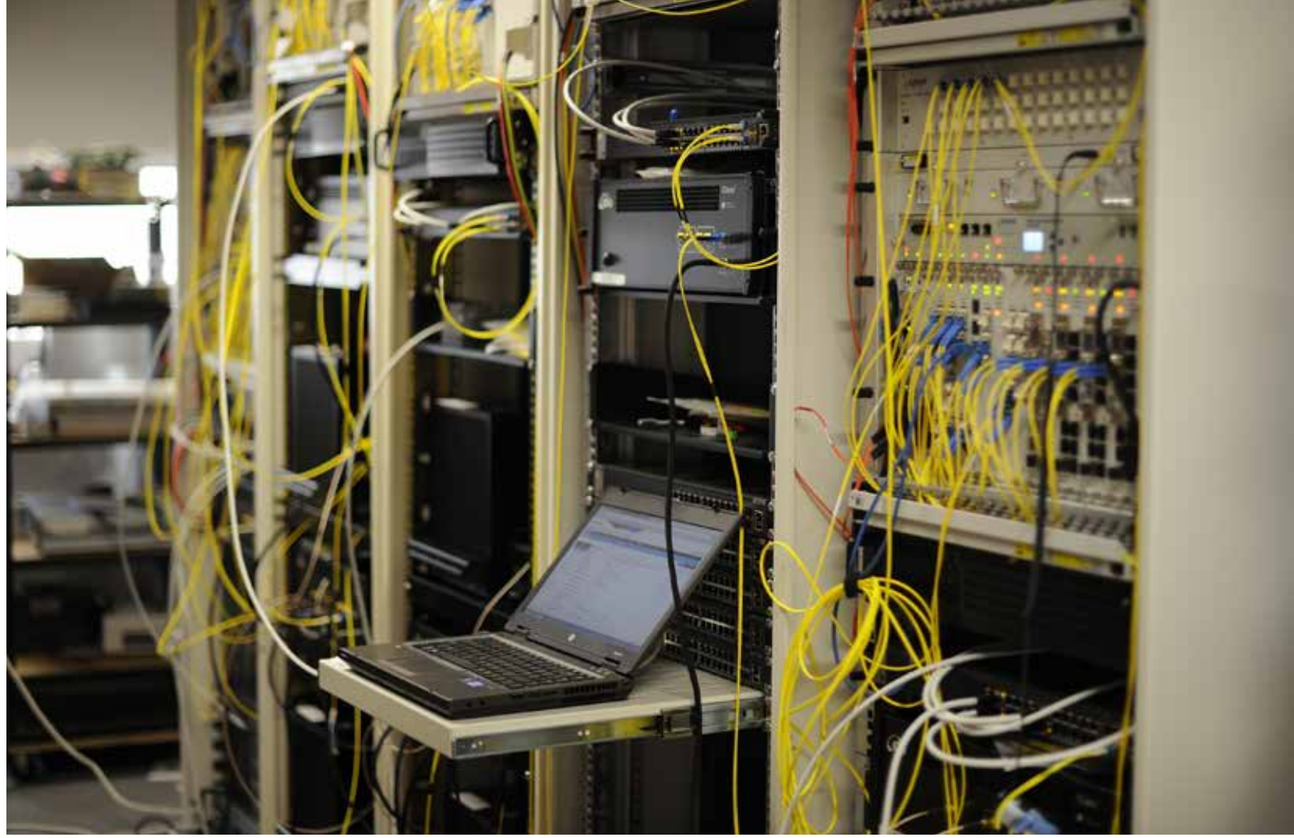
Theme 2: Chip-Scale QKD Technology (led by Prof. Mark Thompson)

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.

The World's First Chip-to-Chip QKD: Progress towards these goals has been rapid, with successful fabrication and demonstration of the world's first chip-to-chip QKD demonstration. The two chips used to demonstrate the point-to-point link integrate all of the photonics required (bar the single photon detectors) onto monolithic devices. This included an InP transmitter chip (Alice), with on-chip lasers, photodiodes and phase modulators, and an SiON receiver chip (Bob). This technology demonstrated performance comparable to current state-of-the-art and commercial devices, with an enormously reduced footprint and ultimately fabrication cost, all in a platform conducive to mass-manufacture. We have also demonstrated quantum-enhanced technologies in silicon-on-insulator waveguide platforms – reducing the footprint further and potentially allowing integration of control electronics onto the device itself. The team has developed a method for overcoming the non-ideal characteristics of phase modulators in silicon, to implement a number of fast QKD protocols and encodings. Additionally, a quantum random number generator has been demonstrated in this technology, based on quantum homodyne detection, allowing for high speed, high fidelity random numbers – a vital component of modern security systems, but also with wider application potential.

Practical Integrated Devices: With this key technology established, we are continuing to push performance of the devices and deploy these in real-world scenarios, progressing towards building autonomous QKD systems for deployment in the Bristol-is-Open (BiO) metro network based on these integrated devices. Additionally, we have investigated the budgets for loss and cross-talk and how these influence the transmission distance of QKD systems, with the aim of designing and ultimately implementing a quantum secured router (QSR). Significant progress has been made on development and characterisation of both the classical and QKD switching elements required for such a router. Finally, we continue to develop next-generation devices with increased performance. Examples include demonstrating Measurement Device Independent (MDI) QKD for increased security and Wavelength-Division-Multiplexed (WDM) QKD for increased key rates. Having characterised and operated our GHz Silicon QKD Transmitter devices, we have extended our previous chip-to-chip work with initial demonstration of Wavelength-Division-Multiplexed (WDM) QKD with integrated photonics.





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

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

UK Quantum Network (UKQN): Fibres have now been installed for the Cambridge metro network part of the UKQN, connecting TREL on the Cambridge Science Park, CAPE (the Centre for Advanced Photonics and Electronics) on Cambridge West Site, the Engineering Department and the University Central Network Hub. The first QKD equipment has been installed on the network by TREL and found to operate stably with a secure bit rate of over 3 Mb/s for a 10.6 km (4.2dB loss) link. Equipment for the other links is also ready and further testing is underway. In addition, QKD has been performed on a 1.1 km test link between two buildings in Bristol, as a precursor to setting up the Bristol metro network part of the UKQN. With respect to the longer distance links that will be used to connect these metro networks, QKD tests have been performed on the long distance National Dark Fibre Infrastructure Service (NDFIS) links, initially connecting Cambridge to Duxford, and Bristol to Bradley Stoke.

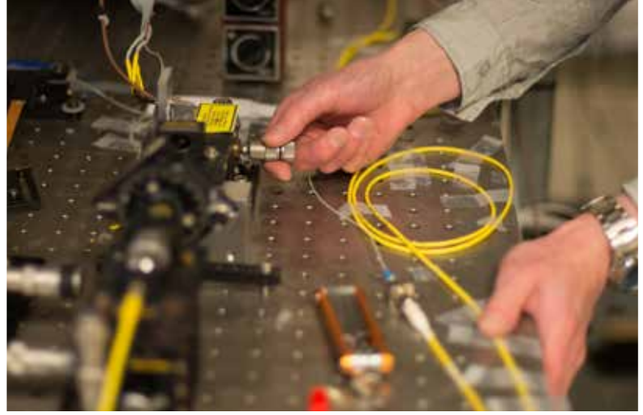
NFV and SDN with QKD: The University of Bristol have made an experimental demonstration of secure Network Function Virtualisation (NFV) orchestration over an emulated Software Defined Network (SDN). This NFV orchestration was secured by time-sharing ID Quantique Clavis 2 QKD systems. This work is the basis of ongoing development and planning for incorporating QKD into the Bristol is Open metro network. BT are a key industrial partner in this work, due to the interest in securing the deployment of Network Functions to reprogrammable commodity hardware, in order to make future communications networks flexible and securely reconfigurable by their service-providers.

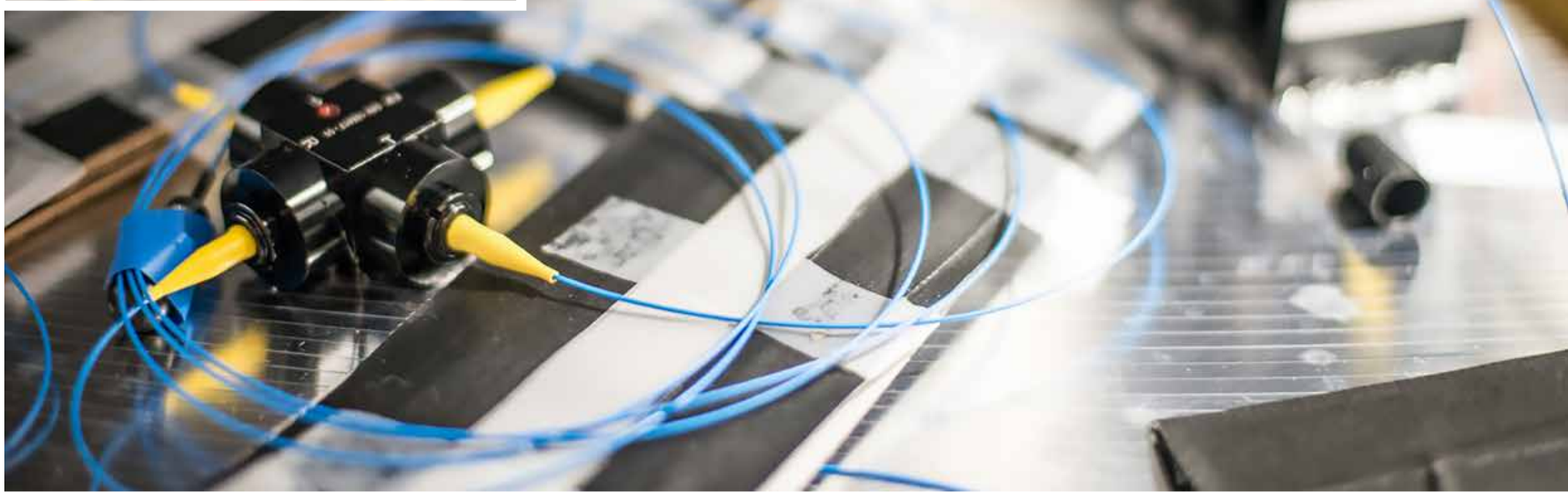
Orthogonal Frequency Divisional Multiplexing: Our colleagues in the University of Leeds have developed new optical orthogonal frequency division multiplexing (OFDM) techniques for QKD systems. They have shown that the total throughput as well as the resilience to the background noise from the data channels can be enhanced. They have also developed optimal methods for wavelength allocation in hybrid dense-wavelength division multiplexing (DWDM) links, combining data and quantum channels.

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

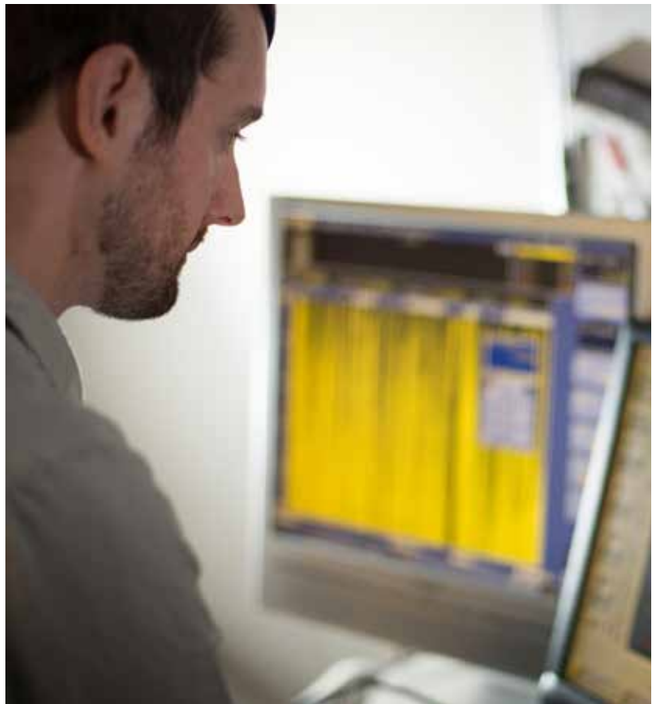
Aim: To explore new approaches, applications, protocols and services – to open up new markets for quantum communications beyond key distribution alone. The sub-themes have been reviewed and revised regularly, based upon progress to implementation, demonstration and technology. The initial sub-themes 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.

Quantum Digital Signatures: The first two years have seen considerable developments in quantum digital signatures (QDS), used to guarantee message integrity and non-repudiation with information-theoretical security, and complementary to the confidentiality provided by quantum key distribution (QKD). In the short lifetime of the Hub, QDS has progressed from short range (a few metres) laboratory-based experiments, through to demonstrations in installed dark fibre over 10's of km, enabled by major recent Hub developments in QDS protocols. This year also saw the first demonstration of MDI-QDS. 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.





Amplifiers and Repeaters: The state comparison amplifier (SCAMP) experiment has been developed to address increased gain (in excess of 9), and implement a practical feedforward approach to increased success rate. A close interaction of theoretical and experimental groups has allowed a detailed theoretical model to predict future amplifier designs. The first designs for miniaturised chip-based SCAMP implementations are now being progressed. The quantum relay using an entangled LED source has been demonstrated over 1km of fibre in the laboratory. Both the coherent state amplifier and quantum relay will now progress to more practical versions, better suited to deployment on the UK Quantum Network.



Measurement Device Independent Quantum Key Distribution (MDI-QKD): We have performed experimental demonstrations of high bit rate MDI-QKD, this protocol being designed to foil attacks on the detectors used for QKD. This involves performing two-photon interference of light signals generated by the two parties wishing to form a key. By making joint measurements of the pulses from both parties, it is possible to establish correlations between the parties and thereby form a shared key. Previous demonstrations of MDI-QKD have been limited to very low bit rates due to the difficulty of generating indistinguishable laser pulses from distinct sources at high rates. However, the recent work by TREL demonstrated a new laser seeding technique to generate such indistinguishable pulses from ordinary laser diodes at GHz rates. This has enabled a demonstration of MDI-QKD with key rates in excess of 1 Mb/s for the first time – an improvement over previous experiments by between 2 and 6 orders of magnitude.

Single-Photon Sources: Building on our recent realisation of a method to deliver on-demand, electronically synchronised, indistinguishable single photons to a quantum network, we are currently using so-called spin-lambda systems to develop a single photon source with perfect purity (e.g. all excess photons are suppressed). Preliminary results point to the world's "purest" single photon source, which we are using to investigate the indistinguishability of photons separated by large time delays. In addition, we have recently realized ultra-bright and scalable single photon sources in a layered semiconductor material. We are currently improving the sample fabrication that will enable enhanced single photon coherence and integration into chip-based QKD transmitters, based on silicon or non-linear platforms such as lithium niobate.

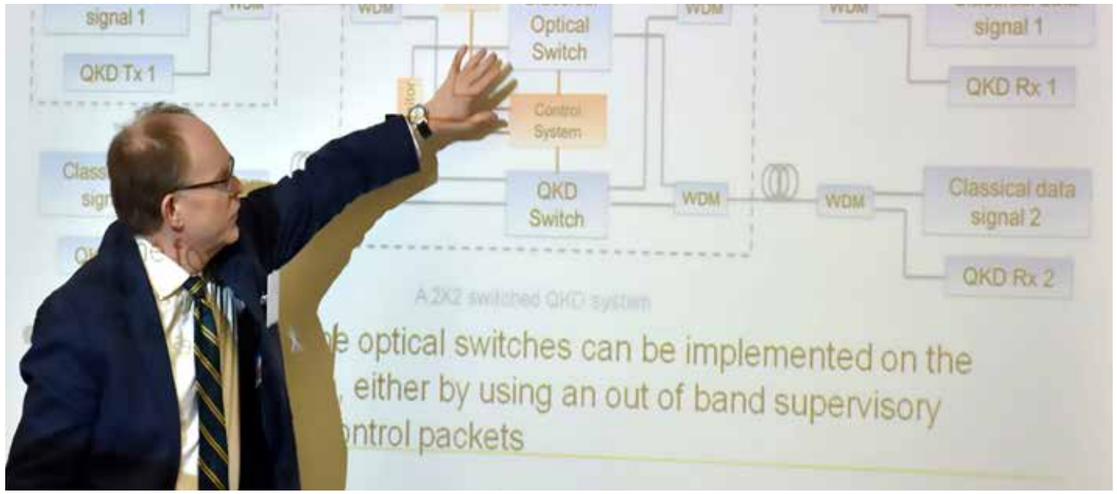
Highlight on

2nd UK-Japan Quantum Technologies Workshop

A first UK-Japan quantum technologies workshop took place in Tokyo in May 2015, funded by the British Embassy. A number of common interests were identified between the UK National Quantum Technologies Programme and various initiatives in Japan, primarily the national ImPACT programme (Impulsing Paradigm Change Through Disruptive Technologies) delivered by the Japan Council for Science, Technology and Innovation. The focus of ImPACT on close collaboration between academia and industry was particularly relevant, with quantum communications singled out as particularly likely to benefit from strategic collaborations between the two countries.

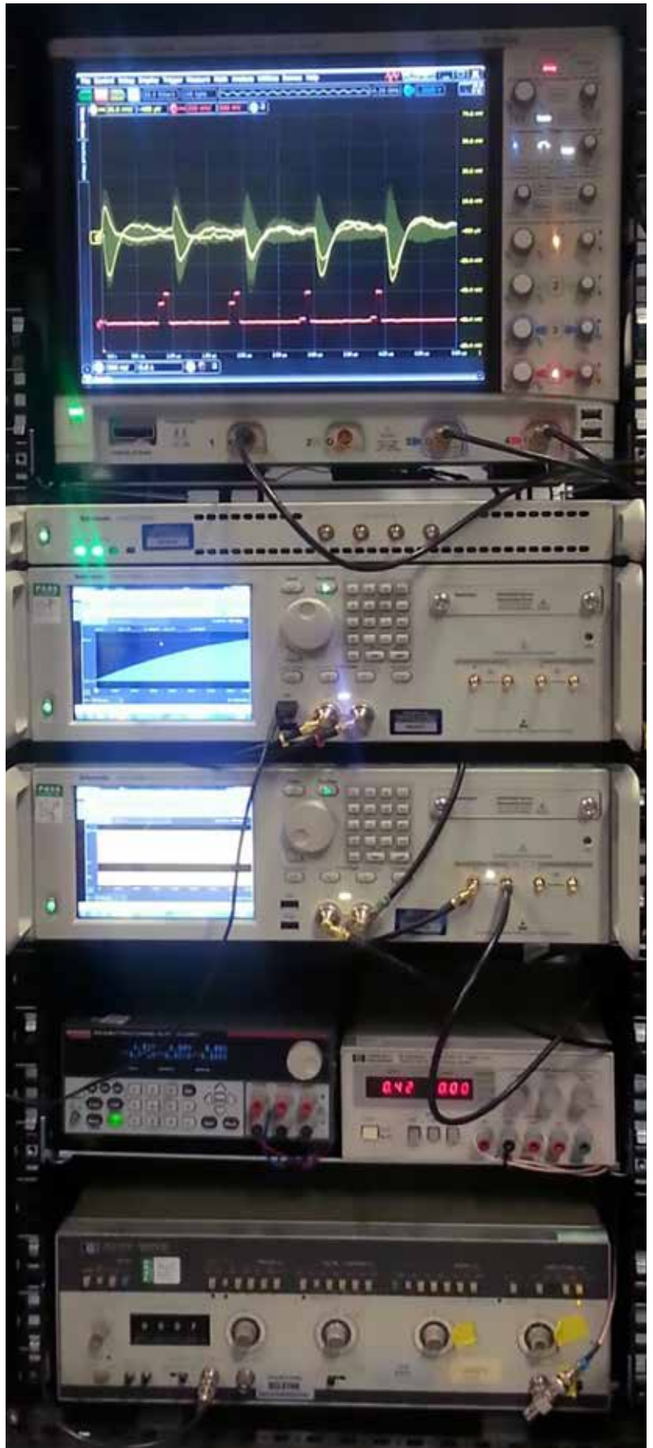
To this end, a second workshop was organised in spring 2016, funded in part by the Foreign Commonwealth Office and specifically focused on quantum communications. The meeting was co-chaired by the Hub Director, Tim Spiller, and Masahide Sasaki, Distinguished Researcher in Japan's National Institute of Information and Communications Technology (NICT). A number of senior Hub investigators from the Universities of Bristol, Cambridge and Heriot Watt were invited to present talks on their work along with colleagues from partners BT, ID Quantique and Toshiba (TREL). The Japanese delegation included senior researchers from the Universities of Hokkaido, Gakushuin and Tokyo, with key figures also from NICT, Toshiba Japan, NTT (the leading Japanese telecommunications company) and information technology company NEC. Topics covered included field trials of QKD in the UK and Japan; security analysis of QKD schemes; optical communications in space; quantum safe cryptography; security certification for QKD implementation; QKD-AES hybrid systems; quantum digital signatures, and collaboration with industry.

The workshop was very successful resulting in an agreed plan for follow-up actions, including a number of collaborative research agreements, and commitment to continue the annual workshops.



Highlight on

Continuous Variable Quantum Key Distribution



An expanding area of interest for the Hub is Continuous Variable Quantum Key Distribution (CV-QKD), a potentially high performance technique that utilises both the amplitude and phase of light to carry information. CV-QKD relies on continuous modulation of orthogonal components of the electromagnetic field (quadratures) which can be measured with coherent homodyne or heterodyne detectors. This is in contrast to the discrete encoding of information into photons that is used in conventional QKD. Recent demonstrations have shown CV key distribution at increased transmission distances, 80km and 100km, a higher key rate and network field deployment. A most appealing aspect of CV-QKD is that it can use existing telecommunications equipment which is readily available within well-resourced research laboratories and which is also in common use industry-wide. However, despite its ability to yield high secure key generation per channel use, the current lower clock rate and data processing complexities affect commercial interests and thence widespread use of CV-QKD systems in secure data communication networks.

The Hub has initiated exploratory activities aimed at the realization of commercially viable CV-QKD propositions, with colleagues in partner institutions Universities of Cambridge and York taking the lead in this effort. To support this initiative, a first scoping workshop was organised in Cambridge in early 2016. The workshop introduced the concept of information encoding on light, its security aspects, information decoding using deliberate detectors and, finally, secure key generation for cryptographic purposes. The first outcome of this workshop has been a feasibility study of a new high-speed CV-QKD system undertaken by the Universities of Cambridge and York, in parallel with the realization of an experimental demonstration using the UK Quantum Network as the testbed.

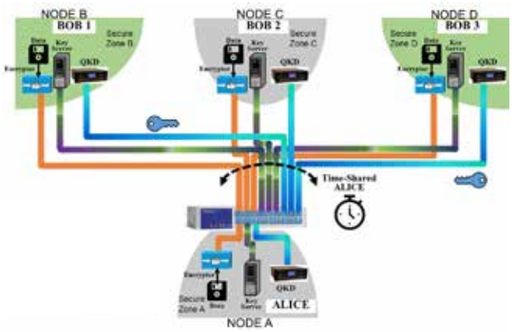
Plans are underway to expand this body of work in 2017, focusing on the construction of a physical CV-QKD system and its network implementation.

Highlight on

Quantum-Secured Network Function Virtualisation

2016 marked a significant development in the Hub's quantum networking efforts, as colleagues from the High Performance Networks (HPN) and the Centre of Quantum Photonics (CQP) groups at the University of Bristol, working closely with BT's Optical Research team, demonstrated experimentally, for the first time, a secure optical network architecture that combines Network Function Virtualisation (NFV) orchestration and Software-Defined Networking (SDN) control with QKD technology.

NFV is a highly desirable proposition in network architecture design and management, aiming to replace purpose-built hardware appliances (e.g. routers, firewalls, load balancers) with software running on off-the-shelf standard IT network infrastructure. When deployed successfully, it is cheaper to run, minimises space requirements, while it also offers all the "plug and play" advantages of a superimposed system on existing machinery, notably up/down-scaling flexibility to changing system demands. SDN is similarly an adaptable, manageable and cost-effective network architecture approach, and the two concepts, while distinct, can be applied in a complimentary fashion to mutual benefit.



Time-Shared QKD
Supported by Software-Defined Networking (SDN)

Our Bristol and BT colleagues have taken this approach one step further, by deploying NFV and SDN in implemented experimental setups in combination with QKD technology. This approach was specifically designed to test resistance to security breach issues experienced by standard NFV when associated network functions stored in a remote data centre were transferred as virtual functions across the network. The parallel addition of SDN technology added a cost-efficient method for time-sharing the QKD systems and served to highlight the ease in which these systems can be integrated with a NFV platform. The results were very positive, demonstrating a particular ETSI-NFV inter-DC architecture designed on a QKD compatible optical network test-bed to provide enhanced security capabilities for Virtual Network Function distribution across datacentres and a novel SDN-based resource-scheduling method for time-sharing a single QKD-Bob between multiple QKD-Alice units. Furthermore, it was shown that this solution could be implemented over longer distances by applying a multi-hop (trusted-node) approach to distribute keys on the network. Results demonstrate that a standard single-mode fibre link of up to 25 km can be secured using quantum encryption for NFV MANO operations with a simultaneous SDN control, showing a minimum quantum bit error rate of 5.3%.

This body of work was presented in detail at the 42nd European Conference and Exhibition on Optical Communication (ECOC 2016) in Düsseldorf, Germany and a full journal paper was published in the IEEE Journal of Lightwave Technology in April, 2017. Full results are described in this paper:

A. Aguado et al. "Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources", IEEE Journal of Lightwave Technology. Vol. 35, No. 8, April, 2017. Pp. 1357 – 1362

Highlight on

Quantum Digital Signatures

We take it for granted that the messages and emails we send are not tampered with. But just as a hand-written signature on a document gives some confidence that the document is genuine, digital messages also need to be signed to guarantee that they haven't been forged or tampered with.

Schemes for digitally signing messages exist, and are now so widely used that the European Union has granted digital signatures the same legal standing as their handwritten counterparts. However, the security of the "public-key" signing methods we commonly use is only computational. This means that it relies on the intractability of certain mathematical calculations, such as factoring large composite (non-prime) numbers. Thus in principle, in the future signed messages could be forged with enough computational effort, or the realisation of a quantum computer.

Alternatively, more secure schemes both for encryption and signatures can rely on secret keys shared between senders and recipients. Hub researchers have developed an efficient way to sign messages using shared secret keys, distributed in a particular way between senders and recipients. The shared secret signing keys can be generated using quantum key distribution (QKD). The length of the key that is needed for signing messages scales only as the logarithm of the length of the message, making "quantum signatures" a very attractive application for quantum key distribution.

Against the higher security one has to accept some disadvantages. Anybody can verify a message signed using a "public-key" signature. But when signatures are based on shared secret keys, then only recipients who are part of the network can verify messages. Nevertheless, there may be applications where the greater security outweighs this drawback, or certain messages might only ever need to be sent within a relatively small network.

We are also developing methods for "quantum signatures" that don't rely on shared secret keys. Instead they directly rely on the fact that even a technically perfect quantum measurement cannot determine what an unknown quantum state is. For example, if a sender passes a weak light pulse through a polarising filter, which only they know the orientation of, then only the sender will be able to know exactly what the polarisation of the light is.

These quantum states serve as "signature states". Later on, when sending a signed message, only the legitimate sender can give information that exactly matches the previously distributed signature states, meaning that only they can sign messages.

Previous initial experimental demonstrations of quantum signatures, at Heriot-Watt University, have been followed by demonstrations in collaboration with the Max Planck Institute for the Science of Light, Erlangen and the University of St Andrews, with researchers in Hefei, China and the University of Vigo, Spain, and with Toshiba Research, Cambridge and the University of Vigo. A collaboration between researchers at Heriot-Watt, the Japanese National Institute of Information and Communications Technology (NICT), and the Nippon Telegraph and Telephone Corporation (NTT) successfully demonstrated transmission of quantum digital signatures over optical fibre attenuation equivalent to 134 km, the longest transmission distance to date. The demonstration used 90 km of installed optical fibre in the Tokyo metropolitan optical fibre network plus controlled attenuation to simulate additional fibre length, and a prototype commercial system. It is planned that these demonstrations will lead to future use of quantum digital signatures within the UK Quantum Network being built by the Hub. Details on the experimental efforts can be read in full in this paper:

Collins RJ et al. Experimental transmission of quantum digital signatures over 90-km of installed optical fiber using a differential phase shift quantum key distribution system. Optics Letters 2016; 41(21): 4883-4886 DOI: 10.1364/OL.41.004883

Highlight on

International Satellite QKD Technologies Workshop

The Quantum Communications Hub held a specialist workshop in June 2016 on satellite quantum key distribution at the European Space Agency's ECSAT – European Centre for Space Applications and Telecommunications at Harwell. The workshop was focused on the use of satellite communications for QKD - a combination of technologies that offers possibilities for quantum-secure communications over very large distances.

The workshop brought together the leading figures from the international academic community, industrial/commercial interests, and public stakeholders from both the EU and UK. Contributors included the pre-eminent satellite QKD specialists Paolo Villoresi (University of Padova), Rupert Ursin (Vienna Centre for Quantum Science & Technology), Christoph Marquardt (Max Planck Institute for the Science of Light), and Thomas Jennewein (University of Waterloo, Canada), as well as experts from Airbus, BT, ID Quantique and ESA itself. Participants included the UK's National Physical Laboratory, the Satellite Applications Catapult, and the EU's Joint Research Centre, as well as Hub university and industry partners. Themes covered ranged from quantum communication activities at ESA, experimental work and satellite-based quantum links, options on upgrading existing laser communication terminals for satellite quantum communications, to CubeSats (miniaturised satellites comprised of multiple cubic elements) for space quantum hardware development and how QKD from space could be harnessed into the existing infrastructures for customer service.

The workshop was part of a wider Hub initiative to explore options for active UK participation in collaborative satellite QKD R&D that will contribute to demonstrations/pilots in which there is increasing global scientific and commercial interest. Micius is the world's first quantum satellite, part of the QUESS (Quantum Experiments at Space Scale) research project by the Chinese and Austrian Academies of Sciences, and designed to facilitate a series of long-distance experiments for the development of quantum encryption and teleportation technologies. The seminal launch of Micius in August 2016 has provided a shift in global momentum in this area.

This shift in momentum was recognised at an end-of-year "Quantum Technology – Implementations for Space" international workshop at ESTEC (European Space Research and Technology Centre) in Noordwijk, the Netherlands, where the Hub was invited to attend and contribute to the discussion. The importance of quantum developments in space was acknowledged, the extent of existing efforts in Europe and Canada recognised, and the need for cross-country collaboration heralded as the way forward in parallel to increasing national initiatives for the development of sovereign capability in quantum space missions. The Hub, in terms of expertise, application focus and breadth of partnership, is now ideally placed to shape a strategy for QKD technology in space and on satellites (or high altitude platforms), leading towards feasibility studies, technology demonstrations and international collaborative projects.

Highlight on

Blackett Review of Quantum Technologies

Copyright: Dan Tsantilis & EPSRC

In 2016, Professor Sir Mark Walport, the Government Chief Scientific Adviser, and Professor Sir Peter Knight convened a panel of experts from academia and industry to write the Blackett Review, "The Quantum Age: technological opportunities". This review introduces the whole range of quantum technology sectors, with global context but also specific reference to the UK activities and the future potential for the UK economy. In order to progress the UK National Quantum Technologies Programme and take the next steps towards realising this economic potential, the review identifies a series of eleven recommendations across the various technology sectors.

Quantum communications is one of the technology sectors that features in this Blackett Review, and investigators and partners from the Quantum Communications Hub provided significant contributions through the expert panel. The communications section of the review explains the concepts of both quantum and mathematical approaches to future communications that will be resilient to attack with new quantum computer technologies, when these emerge. Near and longer term applications are considered, along with a forward look towards future quantum networking and quantum communications in space.

The recommendations of this Blackett Review aimed directly at the communications sector are: additional collaborative work focused on joint technical development and integration of quantum and mathematical cryptography; pilot trials of quantum key distribution (QKD) with realistic data in realistic environments; continuation of work on standards and testing, leading to accreditation, and with engagement to relevant industry and end-user sectors such as finance and communications. The Quantum Communications Hub already has activities underway in all these directions; for example, pilot QKD trials are a key focus of our user engagement strategy. The Hub will therefore be playing a major role in the delivery of these Blackett Review recommendations.

The review can be accessed at: https://www.gov.uk/government/publications/quantum-technologies-blackett-review

Highlight on

Quantum Europe and the EU Flagship Programme

Since the first year of the Hub's lifetime and throughout 2016, the Hub Director and senior colleagues have been engaged in policy debates and high level briefings, both domestically and in the EU, focusing on the transformative potential of quantum technologies for societal and economic impact and the identification of initiatives to drive innovation and commercialisation. The result of these consultations in the UK has been the publication of the Blackett Review into quantum technologies (The Quantum Age: technological opportunities – see relevant section). In Europe, a first successful outcome at the end of 2015 was the Pact for Innovation, an initiative signed at the end of the 7th European Innovation Summit by all participants, intent on supporting and enhancing a direct collaboration between stakeholders and policy makers. By far, though, the landmark policy achievement in 2016 was the publication of a Quantum Manifesto and the accompanying announcement of the €1 billion Quantum Flagship programme at the Quantum Europe conference in the spring of that year.

The Quantum Manifesto is a joint publication by a select team of European quantum experts setting the strategic foundations for a common approach to harnessing the potential of quantum technologies for sustainable and long-term benefit for the European economy. Written at the invitation of Mr. Günther Oettinger, Commissioner for Digital Economy and Society, and Mr. Henk Kamp, Minister of Economic Affairs in The Netherlands, the country holding the Presidency of the Council of the European Union at the time, the Manifesto acknowledged that quantum technologies had reached a point of considerable maturity and potential market readiness, as evident from the significant level of investment in this emerging sector globally. The prime recommendation of the Quantum Manifesto was a call to all Member States and the European Commission for investment of up to €1 billion over 10 years through a Flagship-scale programme in quantum technologies as part of the European Horizon 2020 research and innovation framework programme. A formal announcement confirming the investment was made a month later, in May 2016, in Amsterdam at the Quantum Europe conference.

Apart from the importance of the level of the investment, and the commitment and confidence in the potential of quantum technologies it signifies, it is crucial to note the debt that the Quantum Manifesto owes the UK National Quantum Technologies Programme. Key goals mention creating "a favourable ecosystem of innovation and business creation for quantum technologies", facilitating "a new level of coordination between academia and industry to move advances in quantum technologies from the laboratory to industry" and creating "a new generation of quantum technology professionals" – all founding principles of the UK national programme and its National Strategy for Quantum Technologies.

Our Quantum Communications Hub team supported the aims of the Manifesto, took part in the Quantum Europe conference at the invitation of the organisers and remains committed to contributing to the success of this initiative for cross-collaboration and strengthening innovation.

Highlight on

2nd National Quantum Technologies Showcase

Copyright: Dan Tsantilis & EPSRC

The National Quantum Technologies Showcase is the flagship user engagement event for the national programme, intended to highlight the impact and market readiness of the multi-million investment through live technical demonstrations to a select audience of government officials, leading industry figures, representatives of public sector bodies and the media. The Quantum Communications Hub, working with a group of stakeholders from the national programme (representatives from the other National Quantum Technology Hubs, the EPSRC, the National Physical Laboratory, the Knowledge Transfer Network, Innovate UK, BEIS, and Dstl) led the organisation of the 2016 event, with marked success.

Over 600 delegates registered to attend the event at the Queen Elizabeth II Centre in London in November 2016. Innovate UK organised a reception the night before for a number of distinguished international guests and leading stakeholders of the national programme from across sectors: academia, government, industry and the public sector. The reception took place at Lancaster House with a welcoming address given by the Rt. Hon. Tobias Ellwood MP. This select audience attended also the showcase the next day, when the programme for the day consisted of a combination of talks and some 40 live demonstration sessions.

The event was used as the platform for both the launch of the Blackett Review into quantum technologies by the Government Office for Science, and the announcement of the winners of the £19m Innovation Fund competition for commercialisation of quantum technologies. Professor David Delpy, Chair of the UK National Quantum Technologies Programme, welcomed everyone and chaired the plenary session. Proceedings started with the Government's Chief Scientific Adviser, Sir Mark Walport, introducing the Blackett review ("The quantum age: technological opportunities") to a full auditorium, followed by a panel of experts presenting a session on quantum technology applications for government and industry. Professors Muffy Calder (University of Glasgow) and Sir Peter Knight (national programme strategic advisory board) and Drs Helen Margolis (National Physical Laboratory) and Richard Murray (Innovate UK, Emerging Technologies and Industries) presented talks on all sections of the report (quantum clocks, imaging, sensing and measurement, computing and simulation, communications, commercialisation), followed by a Q&A session with members of the audience. Professor Delpy then announced the winners of the Innovation Fund competition into quantum technologies and invited representatives from some of the successful projects on stage to provide short summaries of their vision. The afternoon session focused on perspectives from the industry. Talks were given by BT's managing director of Research & Innovation, Dr Tim Whitley ("Purposeful innovation: converting cutting-edge science into commercial technology"), and the CEO of Photon Force Ltd, Dr Richard Walker ("Spinning out innovation: an entrepreneur's perspective") – followed again by a discussion and more questions from the audience.

Throughout the day and especially during the networking lunch and breaks, delegates were encouraged to visit the technology demonstrations laid out over two exhibition floors. Exhibits included technologies developed in the four National Quantum Technology Hubs and the National Physical Laboratory, Dstl, as well as industrial partners, funded through Innovate UK for projects focused on the commercialisation of quantum technologies. The Quantum Communications Hub participated with three exhibits showcasing low-cost, short-range quantum key distribution; integrated quantum key distribution; and quantum encryption.

Development of Industrial Standards for Quantum Key Distribution

Industrial standards are essential for ensuring the interoperability of equipment and protocols in complex systems, as well as stimulating a supply chain for components, systems and applications through the definition of common interfaces. Without standards there would be no global networks for fibre optic and mobile communications, or low cost consumer electronics based on reliable and widely available components from multiple suppliers. New standards are therefore required to integrate quantum communications into networks and to stimulate its commercialisation.

The Quantum Communications Hub is at the forefront of developing industrial standards for QKD, through the leading roles of partners Toshiba Research Europe Ltd (TREL) and the National Physical Laboratory (NPL) within the European Telecommunications Standards Institute (ETSI). Andrew Shields, research lead of the Quantum Communication Networking technology theme and a member of the Hub Management Team, is the Chair of the ETSI Industry Specification Group (ISG) for QKD. Along with the other members of the ISG, TREL and NPL have been working on the first standards for quantum communications.

During the first two years of the Hub, partners TREL and NPL have driven work on two areas within the ETSI ISG. NPL, acting as Rapporteur, and TREL contributed to work on characterisation of components used in QKD systems. Standards in this area will stimulate a supply chain for such components, through the definition of common interfaces and requirements. These will define markets for specialist devices such as photon sources and detectors. All this opens up new opportunities for component manufacturers, whilst providing hardware vendors with a broader and more reliable supply base. NPL led the production of the ISG document in this area which was published in May 2016 as ETSI Group

Specification QKD011 Component characterisation: characterising optical components for QKD. TREL have led work in the ISG on implementation security of QKD systems. Although the protocols for QKD can be proven information theoretically secure, small deviations of real world systems from the theoretical model can open potential vulnerabilities, called side channels. The ISG are therefore working on understanding the potential imperfections of real QKD systems, analysing the potential side channel and attack vulnerabilities that these introduce, and advising on countermeasures suitable to mitigate against the threats.

It is very natural that work focuses upon implementation of security issues, as there are now sophisticated QKD prototypes with a high level of technology readiness. Side channels are a feature of all cryptographic equipment, and are therefore also a challenge for systems based on computational complexity. However, quantum cryptography provides a particularly elegant solution to the implementation security problem. Privacy Amplification allows information theoretic security to be restored, even for imperfect QKD systems, provided that the extra information available to an adversary due to the flaws can be measured. The work in the ISG has therefore concentrated on metrology of real world QKD systems and theoretical work on relating this to the potential information available to Eve.

The first type of active attack to be analysed in detail is the so-called Trojan Horse Attack, in which an adversary shines bright light into the QKD system and tries to gain information from the back-reflections without causing any disturbance. Work in the ISG has demonstrated that this attack can be rendered totally ineffective by adding a few passive components – a filter and optical isolator – to a QKD transmitter. TREL have acted as Rapporteur for a draft Group Specification on this subject which should be published in the near future.

Expanding the Partnership Through Collaboration with Industry

The Hub strategy for commercialisation of new secure communications technologies and services is to develop and maintain a spectrum of routes. This is essential because, while specific technologies could be commercialised via a range of technology companies (large, SME, start-up), services are delivered through large service providers, and, with these, access to supply chains and a large customer base. At the same time, the breadth of the UK National Quantum Technologies Programme, the national investment initiative which the Hub is part of, acts as a powerful incentive for a number of global corporations to seriously consider the market opportunities that the UK can offer in the area of quantum technologies.

In 2015 the Hub submitted a proposal for expansion of the UK's quantum network (UKQN) infrastructure to link Cambridge with Adastral Park, BT's research base at Martlesham Heath near Ipswich (see "Future Research Directions" in the first Hub Annual Report, 2014-15). The successful award of £2M for this expansion of the UKQN has enabled work to commence on the Cambridge to Adastral Park link, in parallel with the development of the Cambridge metro(politan) section of the UKQN. Both of these parts of the UKQN are progressing well and it anticipated that both will be operational in late 2017, facilitating two years of operation and user engagement during the remaining two years of phase one of the UK National Quantum Technologies Programme.

The Cambridge to Adastral Park link has been designed specifically to open up quantum communications to a range of potential end users and thus to expand the Hub Partnership. The Adastral Park site includes BT's R&D laboratories and extensive showcase and demonstration facilities, but in addition a wide range of other companies as part of the wider Innovation Martlesham cluster (see "Highlight on The Adastral Park Cluster" in the first Hub Annual Report, 2014-15). Over 70 companies working in communications and ICT, including multi-nationals (e.g. Cisco, Intel, Huawei, Alcatel-Lucent, Nokia) have a presence at Adastral Park. Linking this site to the UKQN thus provides a wide range of opportunities for user engagement, development of quantum secure applications, expansion of the Hub partnership, and delivery of the Blackett Review recommendation of QKD trials with realistic data in realistic environments.

It is also important to note that expansion of the Hub partnership is occurring through expansion and development of the roles undertaken by founding industrial partners, as the Hub evolves. The development of the metro network sections of the UKQN in Bristol and in Cambridge, along with the links between these and the extension to Adastral Park, has expanded the roles of Hub partners such as ADVA, BT, Toshiba (through TREL) and Swiss SME ID Quantique SA (IDQ). All these companies are playing a growing part in the establishment of the wider UKQN, and in the case of IDQ this has contributed to their establishment in late 2016 of an official UK office. All this clearly points to the UK's growing R&D reputation in this area, and the future market potential.

Partnership Resource Investment

The disruptive potential of quantum technologies for applications in areas not currently obvious was recognised early on in the context of the UK National Quantum Technologies Programme, and resulted in additional investment across the network of hubs in the form of flexible funding – the partnership resource. 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 in the second year. Examples include:

The Quantum NODE

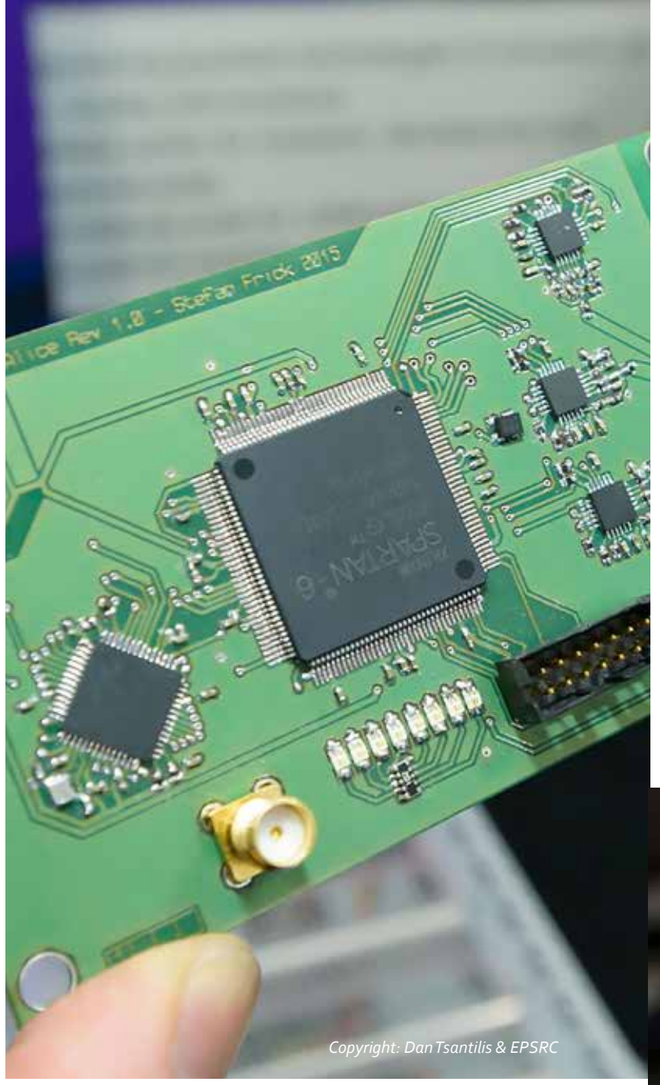
(University of Bristol, University of Glasgow, BT)

This project seeks to establish the foundations for developing a quantum NODE (Quantum Network Operational Device rEceiver) Architecture, using silicon-based waveguide circuits with integrated superconducting nanowire single photon detectors (SNSPDs). This new node-based network architecture will dramatically reduce the resources required for secure quantum communication networks, relieving the users from the need to have bulky and costly high performing detectors, and concentrating these expensive resources into a single central location. Integrated photonics approaches will be utilised to significantly reduce the technology footprint, whilst simultaneously enabling scaling. The proposal builds on a highly successful existing collaboration between the University of Bristol and the University of Glasgow, expanding their joint activity on integrated quantum photonics for quantum computing supported by an EPSRC programme grant. BT will provide their networking expertise to deploy a NODE network demonstration at Adastral Park – proving a compelling quantum NODE demonstrator for the Quantum Communications Hub. Proof-of-principle prototypes of this NODE concept will be demonstrated, targeting fully integrated NODE devices suitable for scaling up to support many users in later development stages.

Flexible Quantum Wireless System

(University of Bristol, University of Oxford/NQIT Hub)

Quantum Key Distribution (QKD) is a cryptographic scheme which provides an unrivalled level of data security. This project specifically investigates practical application of QKD in securing short-range wireless communication between a terminal such as an Automatic Teller Machine (ATM) and a handheld device (e.g. mobile phone), complementing the existing Theme 1 activity in the Hub. This quantum security model can be extended to mobile phone payment and other indoor wireless applications. The consortium (the Universities of Bristol and Oxford [NQIT Hub]) has existing effort in quantum wireless security. Oxford has a project (funded by Innovate UK) in specifically studying the feasibility of a quantum wireless system with hand-movement tracking capability; while Bristol (Quantum Communications Hub) is leading the Theme 1 Hub work in developing next generation credit card with quantum enhanced security. Both partners are working together to develop a flexible platform for future quantum wireless technology.



Copyright: Dan Tsantilis & EPSRC

Wide angle receivers for long-distance free-space QKD (a precursor to satellite QKD)

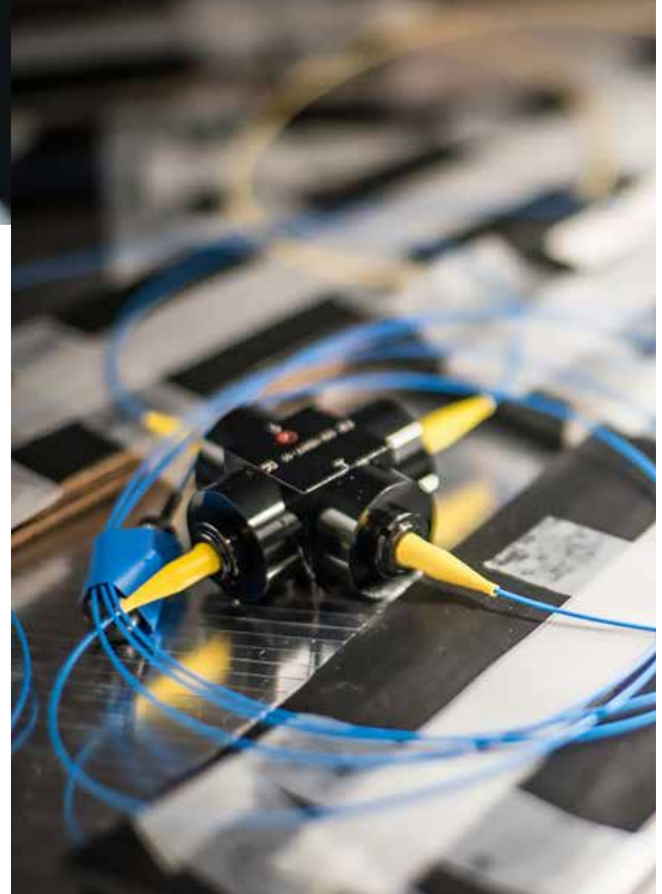
(Heriot Watt University)

The biggest challenge to overcome in long-distance QKD is optical loss. Current mission designs foresee separate optical telescopes, light sources and detectors for the quantum channel and the classical guiding beacon, which strains the stringent size and payload limitations any space mission is subject to. A new design is proposed, that combines quantum key detection and pointing-and-tracking hardware into a single receiver. The goal is to build up a quantum receiver for time-bin qubits with a large field of view, and that will provide spatial information for pointing and tracking directly from the quantum signal. This project reflects the growing interest in quantum communications in space.

High speed (100 Gbps) encrypted optical communication system based on Quantum Key Distribution and fast Optical Code scrambling

(Heriot Watt University, University of Bristol)

Quantum key exchange will be used to seed optical code scrambling (OCS), in order to provide significantly enhanced security at high speed (>100 Gbps) data rates. The resources and expertise from three groups at Heriot Watt University and University of Bristol will be combined. The High Performance Networks (HPN) group at Bristol are providing the 100 Gbps test-bed, and access to the national dark fibre facility (NDFIS) along with the "Bristol is Open" network facility. Bristol are also providing relevant technical support. HWU are setting up and operating the quantum key distribution system, while they will also implement and set up the OCS sections and carry out the 100 Gbps OC transmission experiments at Bristol facilities.



Frequency down-conversion to telecom wavelengths of on-demand indistinguishable single photons from a quantum dot

(Heriot Watt University)

This project is aiming to realize the world's brightest on-demand telecom wavelength source of single photons. This will be achieved by frequency down-conversion of single photons, emitted on-demand from a single InGaAs quantum dot at 950 nm wavelength, to the telecom C-band (1550 nm wavelength) using periodically poled lithium niobate (PPLN) crystals for difference of frequency generation. Success will enable ground-breaking next generation quantum communication technology demonstrations, including experiments in hybrid single photon entanglement and teleportation, and quantum digital signatures and QKD.

Training

Quantum Meets Modern: Hub Training Days on Modern Cryptography

The interaction between modern cryptography and the security community on the one hand, and the quantum technology propositions on the other, is extremely important. This is particularly so as we get closer to delivery of actual products and infrastructure, which will be competing with those currently available for use by industry, the government and the wider public. Awareness of the necessity for interaction and proper dialogue with the cryptographic community is instilled in our Hub, which counts on colleagues from partner Royal Holloway University of London (RHUL) to provide the expertise needed to bridge this divide. To this end, RHUL's Information Security Group, a recognised Academic Centre of Excellence in Cyber Security Research (ACE-CSR) by EPSRC and the National Cyber Security Centre, organised two training days for Hub researchers in 2016 to facilitate a dialogue and exchange of ideas on the capabilities of existing (classical/conventional) systems, so that valid comparisons could begin to take place between these and their quantum equivalents.

The training workshops took place in April and December of 2016 with the aim of providing a broad overview of modern cryptography for Hub researchers, who generally speaking have a Physics background and limited exposure to cryptography as it is currently viewed in the Computer Science and Mathematics communities. The intention was to equip Hub researchers with a sense of how cryptography is used in real applications and how we build security assurance for cryptographic algorithms and protocols. A secondary aim was to provide Hub researchers with a solid technical foundation and a recognised terminology that can be used when talking about cryptography both inside the Hub and within the wider cybersecurity community.

The first session, focused on provable security, with RHUL colleagues explaining the methodology by which security proofs for complicated protocols are obtained by making assumptions on simpler components and then providing security reductions from the security of the complex protocols down to the security of those simpler components. This was followed by a seminar on public key cryptography, covering the basics of public key encryption, digital signatures, and Diffie-Hellman key exchange, delivered by RHUL's Kenny Paterson. Finally, a guest speaker from GCHQ talked about public key infrastructures and the importance of key management in building a working cryptographic deployment.

While this first workshop covered symmetric cryptography and introduced public-key cryptography, the focus of the second session was more on applications. Using two case studies, the TLS and EMV protocols, the debate was honed into how "real-world" protocols combine various cryptographic primitives, their design and evolution, and the practical aspects that come into play in such large-scale systems. Kenny Paterson continued with coverage of public key cryptography, Mike Ward from the banking industry (MasterCard) gave an overview of cryptographic aspects of payment system security, and Thyla van der Merwe from RHUL talked in detail about the cryptographic design of the TLS protocol, this being one of the main secure communications protocols used on the Internet today for protecting online commerce, web browsing and e-mail.

Throughout both days there was lively discussion and comparison of "classical" cryptography and quantum techniques. We plan to run a third session in autumn 2017 with a focus on modern cryptographic techniques that are designed to resist quantum computers -- so called post-quantum cryptography.

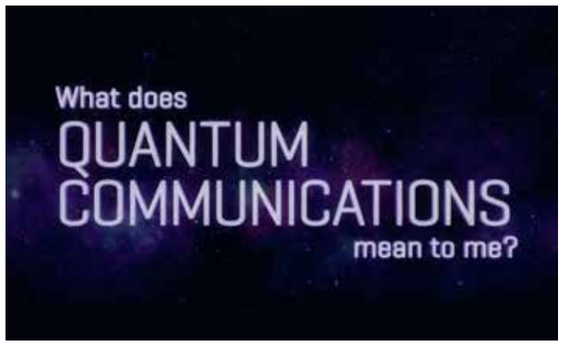
Public Engagement and Outreach

Engagement with the public remained a focus of Hub activity throughout 2016. Our approach to communicating our work to different audiences took various forms, from participating in popular science events to using social media as a platform for outreach.

Working alongside the NQIT Hub, our Hub partners in the University of Bristol took part in the Cheltenham Science Festival with two demonstrations explaining to school children the different properties of light and how these are used in optical fibres for communications. Older visitors were encouraged to visit and learn more about quantum photonic chips and were given the opportunity to closely inspect their structure under microscope.

At the same event, our colleague Professor Kenny Paterson from Royal Holloway University of London gave public talks and took part in panel debates on cryptography, surveillance and the nature of privacy in the modern world. Other colleagues took part in similar outreach events across the partnership: Pint of Science, the Big Bang Fair and Festival of Ideas talks, school visits, summer schools.

More similar activities are planned for 2017 with participation in events such as Soapbox Science, a public outreach platform for promoting women scientists and their work, Women in STEM and the New Scientist Instant Expert science festival.



At the same time and with partial support from the EPSRC, our Hub worked with Spectrecom to produce a short video explaining the concept of quantum communications for non-specialist audiences. The video, titled "The Face of Quantum Communications Technology" is available to watch along with related content on the Hub's newly launched YouTube channel (search Quantum Communications Hub within YouTube) – a platform for openly sharing audio-visual material relevant to our work. Business audiences may be more interested in a series of video interviews with various national programme stakeholders (Hub directors, industrial partners, technologists), produced by the Hub and available to access there; as well as, the "Stimulating Applications and Market Opportunities" video describing the key role of industry in the UK national quantum technologies programme. A Twitter project feed (@QCommHub) was also launched in the same year as a key communication channel between our team and the fellow research, industrial, business, STEM, education, media and general public communities.

Looking ahead, the Hub is looking forward to participating along with the other Hubs in an EPSRC funded public dialogue exercise, aiming to help build an understanding of public concerns, aspirations and priorities for the future development and deployment of quantum technologies. We will also continue to present our work, giving the public the opportunity to witness the technologies under development at appropriate outreach events. In parallel, we also aim to explore closer working with schools to expand the presence of quantum technologies in the curriculum.

APPENDICES

Peer reviewed publications and conference proceedings

Aguado A, Hugues-Salas E, Haigh PA, Marhuenda J, Price AB, Sibson P et al. First Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources. In: 42nd European Conference and Exhibition on Optical Communication (ECOC 2016). Institute of Electrical and Electronics Engineers (IEEE). 2016. p. 512-514

Aguado A, Hugues-Salas E, Haigh PA, Marhuenda J, Price AB, Sibson P, Kennard JE, Erven C, Rarity JG, Thompson MG, Lord A, Nejabati R & Simeonidou D. Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources. Journal of Lightwave Technology 2016; 99 DOI: 10.1109/JLT.2016.2646921

Albrecht MR, Degabriele JP, Hansen T & Paterson KG. A Surfeit of SSH Cipher Suites. ACM Conference on Computer and Communications Security - CCS 2016, Vienna, Austria, 24-28 October 2016. DOI: 10.1145/2976749.2978364

Albrecht MR & Paterson KG. "Lucky Microseconds: A Timing Attack on Amazon's s2n Implementation of TLS". EUROCRYPT (1) 2016: 622-643. DOI 10.1007/978-3-662-49890-3_24

Al-Khuzheyri R, Dada AC, Huwer J, Santana TS, Skiba-Syzmanska J, Felle M, Ward MB, Stevenson RM, Farrer I, Tanner MG, Hadfield RH, Ritchie DA, Shields AJ & Gerardot BD. Resonance fluorescence from a telecom-wavelength quantum dot. Appl. Phys. Lett. 2016; 109: 163104 DOI: 10.1063/1.4965845

Amiri R, Wallden P, Kent A & Andersson E. Secure quantum signatures using insecure quantum channels. Phys. Rev. 2016, A 93:032325. DOI: 10.1103/PhysRevA.93.032325

Arrazola JM, Wallden P & Andersson E. Multiparty quantum signature schemes. Quant. Inf. Comput. 2016; 16:435

Bahrani S, Razavi M & Salehi JA. Optimal wavelength allocation in hybrid quantum-classical networks. Proc. European Signal Processing Conf., EUSIPCO 2016, Budapest, Aug.-Sept. 2016

Bahrani S, Razavi M & Salehi JA. Crosstalk Reduction in Hybrid Quantum-Classical Networks. Scientialranica Transactions 2016; D:23 (6). pp. 2898-2907. ISSN 1026-3098

Bahrani S, Razavi M & Salehi JA. Orthogonal Frequency-Division Multiplexed Quantum Key Distribution. Orthogonal frequency division multiplexed quantum key distribution in the presence of Raman noise. Proc. SPIE 9900, Quantum Optics, 99001C (April 29, 2016). DOI:10.1117/12.2227982

Bonneau D, Silverstone JW & Thompson MG. (Book chapter). Book title: Silicon Photonics III (2016), Chapter: Silicon Quantum Photonics. DOI: 10.1007/978-3-642-10503-6_2

Branny A, Wang G, Kumar S, Robert C, Lassagne B, Marie X, Gerardot BD & Urbaszek B. Discrete quantum dot like emitters in monolayer MoSe2: Spatial mapping, magneto-optics and charge tuning. App. Phys. Lett. 2016; 108:142101. DOI: 10.1063/1.4945268

Coles RJ, Price DM, Dixon JE, Royall B, Clarke E, Fox AM, Kok P, Skolnick MS & Makhonin MN. Chirality of nanophotonic waveguide with embedded quantum emitter for unidirectional spin transfer. Nature Communications 2016; 7: 11183. DOI:10.1038/ncomms11183

Collins RJ, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Sasaki M, Andersson E & Buller GS. Photonic quantum digital signatures operating over kilometer ranges in installed optical fiber. SPIE Proceedings 2016; 9996, Article Number 999604. DOI: 10.1117/12.2241502

Collins RJ, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Andersson E, Buller GS & Sasaki M. Experimental transmission of quantum digital signatures over 90-km of installed optical fiber using a differential phase shift quantum key distribution system. Optics Letters 2016; 41(21): 4883-4886 DOI: 10.1364/OL.41.004883

Croal C, Peuntinger C, Heim B, Khan I, Marquardt C, Leuchs G, Wallden P, Andersson E & Korolkova N. Free-space quantum signatures using heterodyne detection. Phys. Rev. Lett. 2016; 117:100503. DOI: 10.1103/PhysRevLett.117.100503

Dada AC, Santana TS, Malein RNE, Koutroumanis A, Ma Y, Zajac JM, Lim JY, Song JD & Gerardot BD. Indistinguishable photons with flexible electronic triggering. Optica 2016; 3(5):493-498. DOI: 10.1364/OPTICA.3.000493

Degabriele JP, Paterson KG, Schuldt JCN & Woodage J. Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results. CRYPTO (1) 2016: 403-432. DOI 10.1007/978-3-662-53018-4_15

Donaldson RJ, Collins RJ, Kleczkowska K, Amiri R, Wallden P, Dunjko V, Jeffers J, Andersson E & Buller GS. Experimental demonstration of kilometer-range quantum digital signatures. Phys. Rev. 2016, A 93: 012329 – Highlighted as Editor's Suggestion DOI: 10.1103/PhysRevA.93.012329

Iten R, Colbeck R, Kukuljan I, Home J & Christandl M. Quantum Circuits for Isometries. Phys. Rev. 2016; A 93: 032318 DOI: 10.1103/PhysRevA.93.032318

Jin RB, Fujiwara M, Shimizu R, Collins RJ, Buller GS, Yamashita T, Miki S, Terai H, Takeoka M & Sasaki M. Detection–dependent six–photon Holland–Burnett state interference. Scientific Reports 2016; 6, Article number 36914 DOI: 10.1038/srep36914

Joo J, Elliott M, Oi DKL, Ginossar E & Spiller TP. Deterministic amplification of Schrödinger cat states in circuit quantum electrodynamics. New J. Phys. 2016;18: 023028. DOI: 10.1088/1367-2630/18/2/023028

Kok P. Photonic Quantum Information Processing. Contemporary Physics 2016: 1178472. DOI:10.1080/00107514.2016.1178472

Kumar S, Brotons-Gisbert M, Al-Khuzheyri R, Branny A, Ballesteros-Garcia G, Sanchez-Royo JF & Gerardot BD. Resonant laser spectroscopy of localized excitons in monolayer WSe2. Optica 2016; 3(8):882-886. DOI: 10.1364/OPTICA.3.000882

Lim Y, Joo J, Spiller TP, Jeong H. Loss-resilient photonic entanglement swapping using optical hybrid states. Phys. Rev. 2016; A 94: 062337 DOI: 10.1103/PhysRevA.94.062337

Lo Piparo N & Razavi M. Memory-Assisted Quantum Key Distribution Immune to Multiple-Excitation Effects. In Conference on Lasers and Electro-Optics, OSA Technical Digest (2016) (Optical Society of America, 2016), paper JTu5A.6. DOI: 10.1364/CLEO_AT.2016.JTu5A.6

Malein RNE, Santana TS, Zajac JM, Dada AC, Gauger EM, Petroff PM, Lim JY, Song JD & Gerardot BD. Screening Nuclear Field Fluctuations in Quantum Dots for Indistinguishable Photon Generation. Phys. Rev. Lett. 2016; 116:257401. DOI: 10.1103/PhysRevLett.116.257401

Ottaviani C, Laurenza R, Cope TPW, Spedalieri G, Braunstein SL & Pirandola S. Secret key capacity of the thermal-loss channel: improving the lower bound (2016). Proc. SPIE 9996, Quantum Information Science and Technology II, 999609. DOI: 10.1117/12.2244899

Ottaviani C. & Pirandola S. General immunity and superadditivity of two-way Gaussian quantum cryptography. Sci. Rep. 2016;6: 22225 DOI: 10.1038/srep22225

Paterson KG & van der Merwe T. Reactive and Proactive Standardisation of TLS. Security Standardisation Research (SSR). In: Chen L, McGrew D, Mitchell C (Eds.), Security Standardisation Research, Third International Conference, SSR 2016, Gaithersburg, MD, USA, December 5–6, 2016, Proceedings

Pirandola S & Braunstein S. Physics: Unite to build a quantum Internet. Nature 2016; 532:169–171. DOI:10.1038/532169a

Puthoor IV, Amiri R, Wallden P, Curty M & Andersson E. Measurement-device-independent quantum digital signatures. Phys. Rev. 2016; A 94:022328. DOI: 10.1103/PhysRevA.94.022328

Ragy S, Jarzyna M & Demkowicz-Dobrzanski R. Compatibility in Multiparameter Quantum Metrology. Phys. Rev. 2016; A 94: 052108 DOI: 10.1103/PhysRevA.94.052108

Sapienza L, Al-Kuzheyri R, Dada AC, Griffiths A, Clarke E & Gerardot BD. Magneto-optical spectroscopy of single charge-tunableInAs/GaAs quantum dots emitting at telecom wavelengths. Phys. Rev. 2016; B 93:155301. DOI: 10.1103/PhysRevB.93.155301

Wang J, Bonneau D, Villa M, Silverstone JW, Santagati R, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner MG, Natarajan CM, Hadfield RH, O'Brien JL & Thompson MG. Chip-to-chip quantum photonic interconnect by path-polarization interconversion. Optica 2016, 3(4):407-413. DOI: 10.1364/OPTICA.3.000407

Wang ZW & Braunstein SL. Higher-dimensional performance of port-based teleportation. Sci Rep. 2016, 6: 33004. DOI: 10.1038/srep33004

Papers submitted for peer review

Elmabrok O & Razavi M. (2016) Wireless Quantum Key Distribution in Indoor Environments. arXiv:1605.05092

Iten R & Colbeck R. (2016) Smooth Manifold Structure for Extreme Channels. arXiv: 1610.02513

Iten R, Colbeck R & Christandl M. (2016) Quantum Circuits for Quantum Channels. arXiv: 1609.08103

Knott PA, Proctor TJ, Hayes AJ, Ralph JF, Kok P & Dunningham JA. (2016) Local versus Global Strategies in Multi-parameter Estimation. arXiv:1601.05912

Laurenza R & Pirandola S. (2016) General bounds for sender-receiver capacities in multipoint quantum communications. arXiv:1603.07262

Lo Piparo N, Razavi M & Munro WJ. (2016) Measurement-device-independent quantum key distribution with nitrogen vacancy centers in diamond. arXiv:1603.03623

Pearce ME, Campbell ET & Kok K. (2016) Optimal Quantum Metrology of Distant Black Bodies. arXiv:1612.04828

Pirandola S. (2016) Optimal Performance of a Quantum Network. arXiv:1601.00966v1

Pirandola S. (2016) Capacities of repeater-assisted quantum communications. arXiv:1601.00966

Pirandola S, Laurenza R, Ottaviani C & Banchi L. (2016) Fundamental Limits of Repeaterless Quantum Communications. arXiv:1510.08863

Pirandola S & Lupo C. (2016) Ultimate precision of adaptive quantum metrology. arXiv:1609.02160

Raffaelli F, Ferranti G, Mahler DH, Sibson P, Kennard JE, Santamato A, Sinclair G, Bonneau D, Thompson MG & Matthews JCF. (2016) An On-chip Homodyne Detector for Measuring Quantum States and Generating Random Numbers. arXiv:1612.04676

Santana TS, Ma Y, Malein RNE, Bastiman F, Clarke E & Gerardot BD. (2016) Generating indistinguishable photons from a quantum dot in a noisy environment. arXiv: 1612.04427

Sibson P, Kennard J, Stanisic S, Erven C, O'Brien JL & Thompson M. (2016) Integrated silicon photonics for high speed quantum key distribution. arXiv:1612.07236

Vinay SE & Kok P. (2016) Practical repeaters for ultra-long distance quantum communication. arxiv:1607.08140

Weilenmann M & Colbeck R. (2016) The entropy vector method is unable to certify non- classicality in line-like causal structures. arXiv:1603.02553

Weilenmann M & Colbeck R. (2016) Non-Shannon inequalities in the entropy vector approach to causal structures. arXiv:1605.02078

Scientific presentations at conferences and workshops

Aguado A, Hugues-Salas E, Haigh PA, Marhuenda J, Price AB, Sibson P, Kennard J, Erven C, Rarity JG, Thompson MG, Lord A, Nejabati R & Simeonidou D. Contributed talk ("First Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources") at the European Conference on Optical Communications (ECOC 2016), Düsseldorf, Germany, 18 – 22 September 2016

Aguado A, Martin V, Lopez D, Peev M, Martinez-Mateo J, Rosales JL, de La Iglesia F, Gomez M, Hugues-Salas E, Lord A, Nejabati R & Simeonidou D. Poster presentation ("Quantum-Aware Software Defined Networks") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, 12-16 September 2016

Amiri R, Wallden P & Andersson E. Poster presentation ("Imperfect oblivious transfer") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, 12-16 September 2016

Andersson E. Invited talk ("Secure quantum signatures – a practical quantum technology") at the 2nd UK-Japan Technology Workshop (Quantum Communications), Tokyo, Japan, 15-18 March 2016.

Andersson E. Invited talk ("Secure signatures - a practical quantum technology") at the Quantum technology challenges for the 21st century research workshop, Kavli Royal Society Centre, 11-12 May 2016

Bahrani S, Razavi M & Salehi JA. Contributed talk ("Optimal Wavelength Assignment in Hybrid Quantum-Classical DWDM Networks") at the Quantum Communication, Measurement and Computation Conference, Singapore, July 2016

Bahrani S, Razavi M & Salehi JA. Contributed talk ("Optimal wavelength allocation in hybrid quantum-classical networks"), at European Signal Processing Conf (EUSIPCO) 2016, Budapest, September 2016

Buller GS. "Progress in quantum communications technologies at the UK Quantum Technology Hub", Keynote address to SPIE Security + Defence, Edinburgh, UK, 26-29 September 2016

Burenkov V. Poster presentation ("Metrology for Quantum Key Distribution") at the Royal Society discussion meeting on Quantum technology for the 21st century, Royal Society, London, 9-10 May 2016

Burenkov V, Szwer D, Patel P, Chunnilall C & Sinclair A. Poster presentation ("Metrology for Quantum Secure Communications") at the 6th International Conference on Quantum Cryptography (QCrypt), Washington DC, 12-16 September 2016

Burenkov V. Poster presentation ("Metrology for Quantum Secure Communications") at the 4th ETSI/IQC Workshop on Quantum Safe Cryptography, Toronto, 19-21 September 2016

Colbeck R. Invited seminar ("Quantum circuits for quantum operations") at University College London, London, UK, 2 March 2016

Colbeck R. Invited seminar ("Quantum circuits for quantum operations") at University of Maryland, USA, 7 September 2016

Colbeck R. Invited seminar ("Tutorial on device-independent randomness generation") at the 6th International Conference on Quantum Cryptography (QCrypt 2016), Washington DC, USA, 12-16 September 2016

Colbeck R. Invited talk ("Entropic constraints on causal structures") at the "Quantum phenomena -- between the whole and the parts" international workshop, Sopot, Poland, 22 September 2016

Collins RJ. Invited talk ("Experimental quantum digital signatures: A personal perspective of the first four years") at the Quantum Free-space and Fiber Optics Communications and Cryptography session of the Meeting on Quantum Communication and Quantum Imaging, Berlin, Germany, 23-26 August 2016

Collins RJ, Donaldson R, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Wallden P, Dunjko V, Sasaki M, Andersson E, Jeffers J & Buller G. Poster presentation ("Kilometer Transmission Range Quantum Digital Signatures") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, 12-16 September 2016

Collins RJ. Contributed talk ("Photonic quantum digital signatures operating over kilometer ranges in installed optical fiber") at SPIE Security + Defence, Edinburgh, UK, 26-29 September 2016

Croal C, Thornton M, Peuntinger C, Heim B, Khan I, Marqurdt C, Leuchs G, Wallden P, Andersson E & Korolkova N. Poster presentation ("Free-Space Quantum Signatures Using Heterodyne Measurements") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, 12-16 September 2016

Elmabrok O & Razavi M. Poster presentation ("Quantum-Classical Access Networks with Embedded Optical Wireless Links") at the IEEE GLOBECOM 2016 Freedom Through Communications Workshop, Washington D.C., USA, 4-8 December 2016

Erven C. Invited talk ("KETS – Our Entrepreneurial Journey in Quantum Cryptography, so far…") at the PICQUE Bristol Young Scientist Conference on quantum information with photons, Bristol, 4 – 6 April 2016

Erven C. Invited talk ("Quantum Communications and Networks in Bristol") at the Bristol Quantum Information Technologies workshop, Bristol, 6 – 8 April, 2016

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") at QCMC2016, Singapore, 4-8 July 2016

Kennard J. Invited talk ("Quantum Communications in Bristol") at the 2nd UK-Japan Technology Workshop (Quantum Communications), Tokyo, Japan, 15-18 March 2016

Kennard J. Invited talk ("Integrated Quantum Photonics") at the Quantum UK 2016, Birmingham, UK, 20 – 22 September 2016

Kok P. Invited talk ("Quantum metrology and quantum imaging") at the Recent Advances in Quantum Metrology workshop, Warsaw, Poland, 2 March 2016

Kumar R. Invited talk ("Distributing Secret Keys with Quantum Continuous Variables") at CV-QKD workshop, University of Cambridge, Cambridge, UK, 16 February 2016

Kumar R. Invited talk ("Communication with Quadrature: Quantum Converges to Classical") at the Quantum UK 2016 conference, Birmingham, UK, 20-22 September 2016

Kumar S. Invited talk ("Resonance fluorescence and laser spectroscopy of three-dimensionally confined excitons in monolayer WSe_2") at the Meeting on Quantum Communication and Quantum Imaging, Berlin, Germany, 23-26 August 2016

Kumar R. Poster presentation ("Continuous Variable Quantum Key Distribution with Displaced Coherent States", co-authored with Tang X, Asif R, Wonfor A, Penty R, Savory S & White IH) at the 6th International Conference on Quantum Cryptography (QCrypt16), Washington DC, USA,12-16 September 2016

Kumar R, Tang X, Asif R, Wonfor A, Penty R, Savory S & White IH. Poster presentation ("Practical Challenges in Classical Coherent Receivers for Detecting High Speed CV-QKD Signals") at the 6th International Conference on Quantum Cryptography (QCrypt16), Washington DC, USA, 12-16 September 2016

Laing A. Invited talk at the Quantum Europe conference, Amsterdam, the Netherlands, 17 May 2016

Laurenza R. Contributed talk ("General bounds for sender-receiver capacities in multipoint quantum communications") at Quantum Roundabout 2016, University of Nottingham, 6th – 8th July 2016 & IQIS 2016 – 9th Italian Quantum Information Science Conference, Rome, 20-23 September 2016

Laurenza R. Invited talk ("Benchmarks for secure and quantum communications") at SPIE Security + Defence Symposium, Edinburgh, UK, 26-29 September 2016

Lo Piparo N, Razavi M & Munro WJ. Contributed talk ("Simple and Efficient Memory-Assisted Quantum Key Distribution") at Quantum Communication, Measurement and Computation Conference, Singapore, July 2016

Lo Piparo N, Razavi M & Munro WJ. Contributed talk ("Toward feasible long-distance quantum communications systems") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, September 2016

Lord A. Invited talk at industrial engagement innovation workshop organised by Innovate UK in London, 25 February 2016

Lord A. Invited talk ("Quantum Communications: A BT Perspective") at the 2nd UK-Japan Technology Workshop (Quantum Communications), Tokyo, Japan, 15-18 March 2016

Lowndes D, Frick S, Collins R, Hart A, Linares-Vallejo E, Maini N & Rarity JG. Contributed talk ("Low cost, short range, free space quantum key distribution") at the Photon16 conference, Leeds, UK, 5 – 8 September 2016

Marhuenda J. Presentation ("Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared QKD Resources") at invited visit to the UK General Communications Headquarters (GCHQ) on quantum key distribution with NFV and SDN

Newton E, Everitt M, Wilson F & Varcoe B. Poster presentation ("Central Broadcast Quantum Cryptography") at the Cambridge Wireless TEC workshop, Cambridge, UK, 14 September 2016

Ottaviani C. Invited talk ("Measurement-Device-independent quantum conferencing with continuous variables") at 2st Trustworthy Quantum Information conference (TyQI2016), Shanghai Institute for Advanced Studies, Shanghai, China, 27 June – 1 July 2016

Ottaviani C. Research visit and seminar ("Quantum cryptography with continuous variables: unconditional security in point-to-point and end-to-end configuration") at Beijing University of post and telecommunications, 2 July – 7 July 2016

Ottaviani C. Invited talk at the workshop 'Photons Beyond Qubits', Palacky University, Olomouc, Czech Republic, October 3-5 2016

Paterson K. Invited talk ("Authenticated Encryption") at a Winter School on IoT Security, Tenerife, 25-29/01/16

Paterson K. "Cryptographic Vulnerability Disclosure – the Good, the Bad, and the Ugly", series of research seminars given at University of Oxford (10/2/16), University of California, San Diego (24/2/16), and at UCL (7/4/16)

Paterson K. Invited talk ("Cryptography for Cloud Security") at the $(ISC)^2$ SecureCambridge Conference on Securing the Virtual Organization, Cambridge, UK, 5 April 2016

Paterson K. Series of talks on "Authenticated Encryption" at a Norwegian Winter School on Information Security, Finse, Norway (24-29/4/16)

Paterson K. Invited talk and panel participation at the AWACS ("A Workshop About Cryptography Standards") single-day workshop in Vienna, focusing on the work of the Crypto Forum Research Group (CFRG), a Research Group of the IRTF which he co-chairs. Vienna, Austria, 8 May 2016

Paterson K. Invited seminar talks ("AE Security for SSH") at the "Summer school on real-world crypto and privacy", Sibenik, Croatia, June 5–10, 2016

Penty R. Invited talk ("Extending quantum research networks to industry and other users") at the 2nd UK-Japan Technology Workshop (Quantum Communications), Tokyo, Japan, 15-18 March 2016

Pirandola S. Invited talk ("Fundamental Limits of Repeaterless Quantum Communications") at the RACQIT (Recent advances in continuous variable quantum information theory) 2016 conference, UniversitatAutònomaBarcelona, Spain, 6-8 June 2016

Pirandola S. Invited talk (""Fundamental limits of repeaterless quantum communications") at the 6th International Conference on Quantum Cryptography (QCrypt 2016), Washington DC, USA, 12-16 September 2016

Pirandola S. Invited talk ("The ultimate rates of quantum communications") at the IQIS 2016 – 9th Italian Quantum Information Science Conference, Rome, Italy, 20-23 September 2016

Price A, Aguado A, Hugues-Salas E, Haigh E, Sibson P, Marhuenda J, Kennard J, Rarity J, Thompson M, Nejabati R, Simeonidou D & Erven C. Poster presentation (""Towards the Deployment of Quantum Key Distribution Systems in a Software Defined Networking Environment") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, 12-16 September 2016

Price AB, Aguado A, Hugues-Salas E, Haigh PA, Sibson P, Marhuenda J, Kennard J, Rarity JG, Thompson MG, Nejabati R, Simeonidou D & Erven C. Contributed talk ("Practical Integration of Quantum Key Distribution with Next-Generation Networks") at the International Conference for Young Quantum Information Scientists, Barcelona, Spain, 19 – 21 October 2016

Puthoor I, Amiri R, Wallden P, Curty M & Andersson E. Poster presentation ("Measurement-Device-Independent Quantum Digital Signatures") at the 6th International Conference on Quantum Cryptography (QCrypt) 2016, Washington DC, USA, 12-16 September 2016

Ragy S. Contributed talk ("High-rate device-independent quantum randomness generation") at Quantum Roundabout young researchers' conference, Nottingham, UK, 6-8 July 2016

Rarity JG. Invited talk ("Nanophotonics, two-level systems and quantum information") at the TU, Berlin, Germany, 27 Jan 2016

Rarity JG. Invited talk ("Open challenges for optical quantum technologies") at the Quantum Technology Challenges for the 21st Century workshop, Chicheley Hall (Royal Society), UK. May 2016

Rarity JG. Invited talk ("Bristol Satellite QKD") at the Satellite Quantum Key Distribution workshop, ESA, ESTEC Harwell Campus, Didcot, UK, 2 June 2016

Razavi M. Invited talk ("Memory-assisted quantum key distribution") at Sharif University of Technology, May 2016

Razavi M. Invited talk ("Memory-assisted quantum key distribution") at Tsinghua University, China, July 2016

Razavi M. Invited talk ("Trust-free quantum key distribution at regional scales", co-authored with Lo Piparo N, Elmabrok O, Ghalaii M, Panayi C, Fazelian M, Salehi JA & Munro WJ) at the SPIE Security + Defence Symposium, Quantum Information Science and Technology Conference, Edinburgh, UK, September 2016

Shields A. Invited talk ("Quantum communications in telecom networks") at the Quantum technology for the 21st century research workshop, Royal Society, London, 9-10 May 2016

Shields A. Invited talk at the 4th ETSI/IQC workshop on Quantum Safe Cryptography, Toronto, Canada, 19-21 September 2016

Sibson P, Kennard J, Stanisic S, Erven C, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner MG, Natarajan CM, Hadfield RH, O'Brien JL & Thompson MG. Contributed talk ("Quantum Key Distribution with Silicon Integrated Photonics") at the Photon16 conference, Leeds, UK, 5 – 8 September 2016

Sibson P, Kennard J, Stanisic S, Erven C & Thompson MG. Contributed talk ("Integrated Silicon Photonics for Quantum Key Distribution and Wavelength-Division-Multiplexed QKD with Integrated Photonics") at the QCrypt 2016 conference, Washington DC, USA, 12 – 16 September 2016

Spiller T. Invited talk on quantum communications technologies and the Quantum Communications Hub as part of a meeting organised by NPL (EMTECH Quantum Technologies Briefing Seminar; 24/02/16)

Spiller T. Invited talk ("National Network of Quantum Technologies Hubs: Developments with the UK Quantum Communications Hub") at the 2nd UK-Japan Technology Workshop (Quantum Communications), Tokyo, Japan, 15-18 March 2016

Spiller T. Invited talk ("Quantum secure communication technologies") at the Quantum technology challenges for the 21st century research workshop, Kavli Royal Society Centre, UK, 11-12 May 2016.

Spiller T. Invited talk ("Quantum Communications Hub") and panellist during the Quantum Europe conference, Amsterdam, The Netherlands, 17-18 May 2016

Spiller T. Keynote address ("Quantum Communications and the UK National Quantum Technologies Programme") at the IPAQS Symposium, Heriot Watt University, Edinburgh, UK, 19 May 2016

Spiller T. Presentation ("Quantum Communications Hub") for Gareth Davies, Director-General for BIS, during visit at the University of York, York, UK, 10 June 2016

Spiller T. Invited talk at the single-day quantum technologies workshop on Defence & Security organised by the Government Office for Science, KTN, UK National Quantum Technology Hub in Sensors and Metrology and the University of Birmingham, BEIS, London, UK, 25 October 2016

Tang X, Asif R, Kumar R, Wonfor A, Penty RV & White IH. Poster presentation ("Optically switched multi-user quantum key distribution") at the Quantum UK 2016 conference, Birmingham, UK, 20-22 September 2016

Tang X, Asif R, Kumar R, Wonfor R, Savory S, Penty RV & White IH. Poster presentation ("Getting the best out of balanced homodyne detectors for high speed continues-variable quantum key distribution") at the Quantum UK 2016 conference, Birmingham, UK, 20-22 September 2016

Thompson M. Invited talk ("Quantum Technology Enterprise Centre at Bristol & Cranfield Universities") at the PICQUE Bristol Young Scientist Conference on quantum information with photons, Bristol, 4–6/04/16

Thompson M. Invited talk ("Integrated quantum photonics") at the Quantum technology challenges for the 21st century research workshop, Kavli Royal Society Centre, UK, 11-12 May 2016

Thompson M. Invited talk ("Silicon Quantum Photonics") at the European Conference on Integrated Optics, Warsaw, Poland, 18 – 20 May 2016

Thompson M. Invited talk ("Silicon Quantum Photoincs") at the Silicon Summer School, Ghent, Belgium, 1 September 2016

Varcoe B. Invited talk ("National Network of Quantum Technologies Hubs: Quantum Communications Hub") at the "Cybersecurity and the Emerging Field of Quantum Computing" workshop, Science & Innovation Network, Villa Wolkonsky, Rome, 18 May 2016

Vergheese Puthoor I. Invited talk ("Measurement-Device-Independent Quantum Digital Signatures") at the 4th ETSI/IQC Workshop on Quantum Safe Cryptography, Toronto, Canada, 19-21 September 2016

Vinay S. Poster presentation ("High-fidelity quantum repeaters") at the Quantum Roundabout conference, Nottingham, UK, 6-8 July 2016

Wilson F, Everitt MCJ &Varcoe BTH. Poster presentation ("Integrating CVQKD with existing satellite networks") at Photon 16, University of Leeds, Leeds, 5 - 8 September 2016

Wilson F, Newton E, Everitt M, Varcoe B. Poster presentation ("Integrating QKD with existing communications systems") at the Photon 2016 international conference, Leeds, UK, 5-8 September 2016

Wonfor A. Invited talk ("Integrated optical switches and short pulse generation using a generic integration platform") at 2016 IEEE Photonics Conference, Hawaii, USA, 2-6 October 2016

Selected Public Engagement Activities

Colbeck R. Public engagement talk ("Keeping secrets") in the Quantum Pub session of Pint of Science festival, York, 24 May 2016

Gerardot B. Delivery of an outreach seminar ("Changing the Lightbulb") to approximately 300 secondary school students throughout Scotland, May 2016

Lord A. Technical demonstrations of the Hub's quantum key distribution systems for quantum communications by our industrial partner BT, for the general public at the New Scientist Live public engagement event, London, UK, 22-25 September 2016

Lord A. Technical demonstrations of the Hub's quantum key distribution systems for quantum communications by our industrial partner BT, for industrial audience at the "Powering the Global Connected Society" industrial engagement event, London, UK, 18-20 October 2016

Paterson gave a talk introducing RHUL's research capability at the GCHQ CyberInvest event, Westminster (8/3/16)

Paterson K. Invited 90-minute class on "Binary" to a group of 20 year 6 schoolchildren at Archdeacon Cambridge Primary School, Twickenham, 26 May 2016

Paterson K. Participation in a Times Cheltenham Science Festival panel session on Privacy and Surveillance, Cheltenham, UK, 10 June 2016

Paterson K. Short talks (x 2) on cryptography at RHUL's "Exploring Mathematics" day, 28 June 2016

Paterson K. Invited 2-hour masterclass on "Cryptography - Everywhere" to a group of 30 lower sixth form students at Esher College, Surrey, 6 July 2016

Ragy S. Public engagement talk ("Keeping secrets with a side of quantumness") in the Quantum Pub session of Pint of Science festival, York, 24 May 2016

Spiller T. Invited talk ("A Quantum Leap for York") at the York Talks 2016 (Research in the Spotlight) event, York, (6/01/16)

Spiller T. Invited talk ("Quantum Communications Technologies") at the Physics Review journal 25th Anniversary event. University of York, York, 19 October 2016

Selected Media Coverage

QECDT student wins renowned Erwin Schrödinger Prize; University of Bristol news item, posted 29 January 2016. Available to access at http://www.bristol.ac.uk/physics/news/2016/qecdt-prize.html

The quantum clock is ticking on encryption – and your data is under threat; WIRED online article including interview with KETS researcher, Philip Sibson, posted October 2016. Available to access at http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption

Has The Age Of Quantum Computing Arrived? Interview with Tim Spiller, posted on D/SRUPTION on 18th October 2016. Available to access at https://disruptionhub.com/age-quantum-computing-arrived/

Bristol's quantum chip goes on display at the Science Museum; Techspark online news item, posted on 15 December 2016. Available to access at: https://techspark.co/bristols-quantum-chip-goes-display-science-museum/

China's 2,000-km Quantum Link Is Almost Complete, IEEE news item including commentary by Tim Spiller, posted on 26 October 2016. Available to access at http://spectrum.ieee.org/

Quantum Leaps in Quantum Technology, The Naked Scientists podcast, posted on 11 November 2016. Available to access at https://www.thenakedscientists.com/podcasts/special/quantum-leaps-quantum-technology

The arrival of 5G, cognitive radio and the future of connectivity, The Guardian news piece, published on 8 December 2016. Available to access at:

https://www.theguardian.com/media-network/2016/dec/08/5g-cognitive-radio-future-connectivity-business

A quantum leap towards the market, news item on electrooptics.com, posted on 5 May 2016. Available to access at:

https://www.electrooptics.com/feature/quantum-leap-towards-market


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

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.