

# UK QUANTUM TECHNOLOGY HUB

FOR QUANTUM COMMUNICATIONS TECHNOLOGIES



ANNUAL REPORT



2017

2018



QUANTUM  
COMMUNICATIONS  
HUB

# Contents

Foreword by the Director	i
Introduction	3
Overview: The Fourth Year	4
Management & Leadership	7
The project partners	9
Technology Development: Progress in the Fourth Year	10
Highlight: Strategic Development of Satellite Quantum Communications Initiative	16
Highlight: A high-gain and high-fidelity coherent state comparison amplifier	17
Highlight: The Second Phase of the National Quantum Technologies Programme	18
Highlight: 3QN – Towards A New UK Industry for Novel Quantum Receivers in Nascent Satellite QKD Global Markets	19
Highlight: International Engagement – Canada	20
Highlight: Launch of the Cambridge Metro Quantum Network	21
Highlight: The 2018 National Quantum Technologies Showcase	22
Highlight: The MacroPhoton	23
Partnership Resource	24
Public Engagement and Outreach	28
Appendices	30

**Special thanks to all contributors:**  
Klitos Andrea, Gerald Buller, Robert Collins, Ross Donaldson, Chris Erven, Emilio Hugues-Salas, David Lowndes, Georgia Mortzou, John Rarity, Andrew Shields, Tim Spiller.  
Thanks also to our many colleagues, programme partners and collaborators for kindly providing images.

# Foreword

Led by the University of York, the Quantum Communications Hub is exploiting fundamental aspects of quantum physics for the development of new secure communications technologies and services. Part of the UK National Quantum Technologies Programme, the Hub is an evolving consortium of universities, industrial partners and public sector stakeholders. Our main aim is to advance new communications technologies towards commercial readiness.

Progress with our technologies has continued to be strong during 2018, reflected by our presence at the National Showcase event in November. We have further advanced our “consumer QKD” hand-held system, and developed new on-chip devices. It is particularly pleasing to see that two of the four successful proposals for industry-led Industrial Strategy Challenge Fund (ISCF) projects launched in late 2018 are focused on quantum communications with very strong links and partnerships with the Hub. This is a clear sign of progress along the Hub’s trajectory supporting commercialisation.

We have continued to evolve our portfolio of collaborative research and development projects, with a strategic perspective towards future quantum communications in space. A growth area worldwide, this technology direction is crucial to achieve quantum communications over the greatest distances. With research and industry partners, we are establishing foundations for future UK satellite quantum communications based on UK research and development.

June 2018 saw the official launch of the Cambridge metropolitan section of the Hub’s UK Quantum Network (UKQN). This network continues to demonstrate high performance key exchange that is reliable, robust and flexible. Other sections of the UKQN will become fully operational during 2019. The UKQN will provide national capability for demonstrations of new services and end-user engagement.

The importance of engagement – educational and public, in addition to commercial – continues to grow. The Quantum Ambassadors scheme for schools that we established in 2017 for the whole National Programme is now up and running, with very positive feedback. Along with the other Hubs, CDTs and National Programme stakeholders, we are part of Quantum City, a major new public engagement initiative. The MacroPhoton demonstrator developed at Heriot-Watt University is proving to be an excellent “hands-on” public engagement tool. As evidenced from the ISCF project developments, industrial engagement is increasing and we expect the UK Quantum Network to play a key role in accelerating further engagement.

Looking back with pleasure on progress over the last year, we look forward to the next, and the opportunities for both development and engagement across our remit for research and innovation.

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



## Quantum Key Distribution

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

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

## Introduction

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

- **Short-range, free-space QKD systems:** these technologies will enable many-to-one, short range, quantum-secured communications, for consumer, commercial and defence markets. We are working to deliver a credit card sized QKD transmitter linked to a rack-size (wall mounted ATM-like) QKD receiver to allow secure key sharing between a phone and terminal with minimal modification of phone hardware.
- **QKD-on-a-chip modules:** scaled down and integrated QKD component devices, for producing robust, miniaturised sender, receiver and switch systems - "QKD-on-a-chip" modules. These advances address cost, energy-efficiency and manufacturability issues, to enable widespread, mass-market deployment and application of QKD.
- **Establishment of a UK Quantum Network:** which integrates QKD into secure communication infrastructures at access, metropolitan and inter-city scales. We have established metro-scale networks in Bristol and Cambridge and in 2019 will link these utilising the National Dark Fibre Infrastructure Service (NDFIS) to form a UK Quantum Network. This national capability will be used for device and system trials, integration of quantum and conventional communications, and demonstrations for stakeholders, end users and the wider public.
- **Next Generation quantum communications technologies:** approaches which go beyond current QKD technologies and address some of their limitations. We are exploring: (i) development and implementation of quantum signatures and other protocols in order to address areas of the security application space not covered by QKD; (ii) development of quantum amplifier and repeater demonstrators, addressing the current distance limitations of QKD; (iii) development of measurement-device-independent (MDI) QKD technologies, to address some of the side channel vulnerabilities that exist in current QKD implementations. Side channel and security analysis, novel protocols, network architecture design and analysis, virtualisation and modelling are additional areas being explored to support Hub technology goals.

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

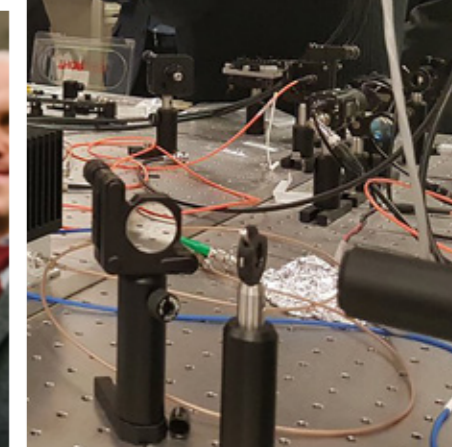
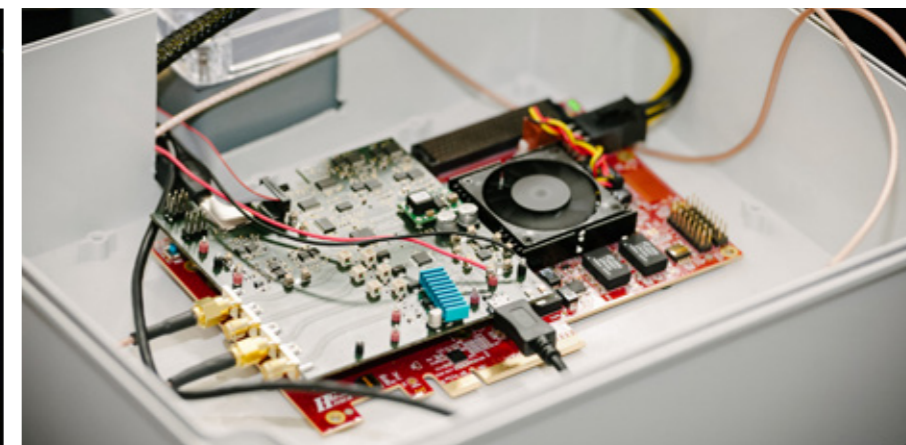


## Overview: the fourth year

A number of work strands reached completion in the fourth year allowing us to start thinking about potential directions during a possible second phase of the national programme. The Cambridge metropolitan network launch was a particular landmark in this regard, the first of four components of a quantum network being built by the Hub. At the same time, a number of new partnership resource projects were funded, paving the way for exploratory work in satellite quantum communications – an area where the Hub has strong interests. By the time, in autumn 2018, the Chancellor announced further investment in the area of quantum technologies over a further five years, the Hub was ready to respond, building on a number of achievements over the last four years, and identifying areas of strategic importance for new development.

In the fourth year we have:

- Completed a number of partnership resource projects, while funding a further six new ones through the investment of more than £1.1M
- Launched the Cambridge metropolitan network
- Participated in an expert quantum technologies mission to Canada organised by Innovate UK
- Launched alongside the rest of the Network of Hubs, NPL and quantum Centres for Doctoral Training a joint public engagement initiative – the Quantum City
- Took part in numerous science festivals and a quantum job fair while also engaging in a variety of outreach activities
- Contributed both written and oral evidence to the Science and Technology Select Committee's Inquiry into Quantum Technologies
- Organised two specialist, senior stakeholder workshops on strategic development of satellite quantum communications
- Sponsored three Quantum Summer Schools for A level and undergraduate students
- Helped to organise and took part in the fourth National Quantum Technologies Showcase with eight demonstrators
- Through many of our academic partners we have been successful in working with industry and securing ISCF funding on two out of the four funded projects in the first Pioneer call: 3QN and AQuaSec
- Delivered more than 70 presentations of our work in various conferences, workshops, industry and user engagement events, both in the UK and abroad
- Published more than 35 research papers, book chapters and conference abstracts, and submitted a further 29 for peer review
- Expanded the partnership with new industrial partners
- Submitted an outline proposal in response to a funding call from the EPSRC for further work as part of the second phase of the national quantum technologies programme



## The Partnership



## 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.



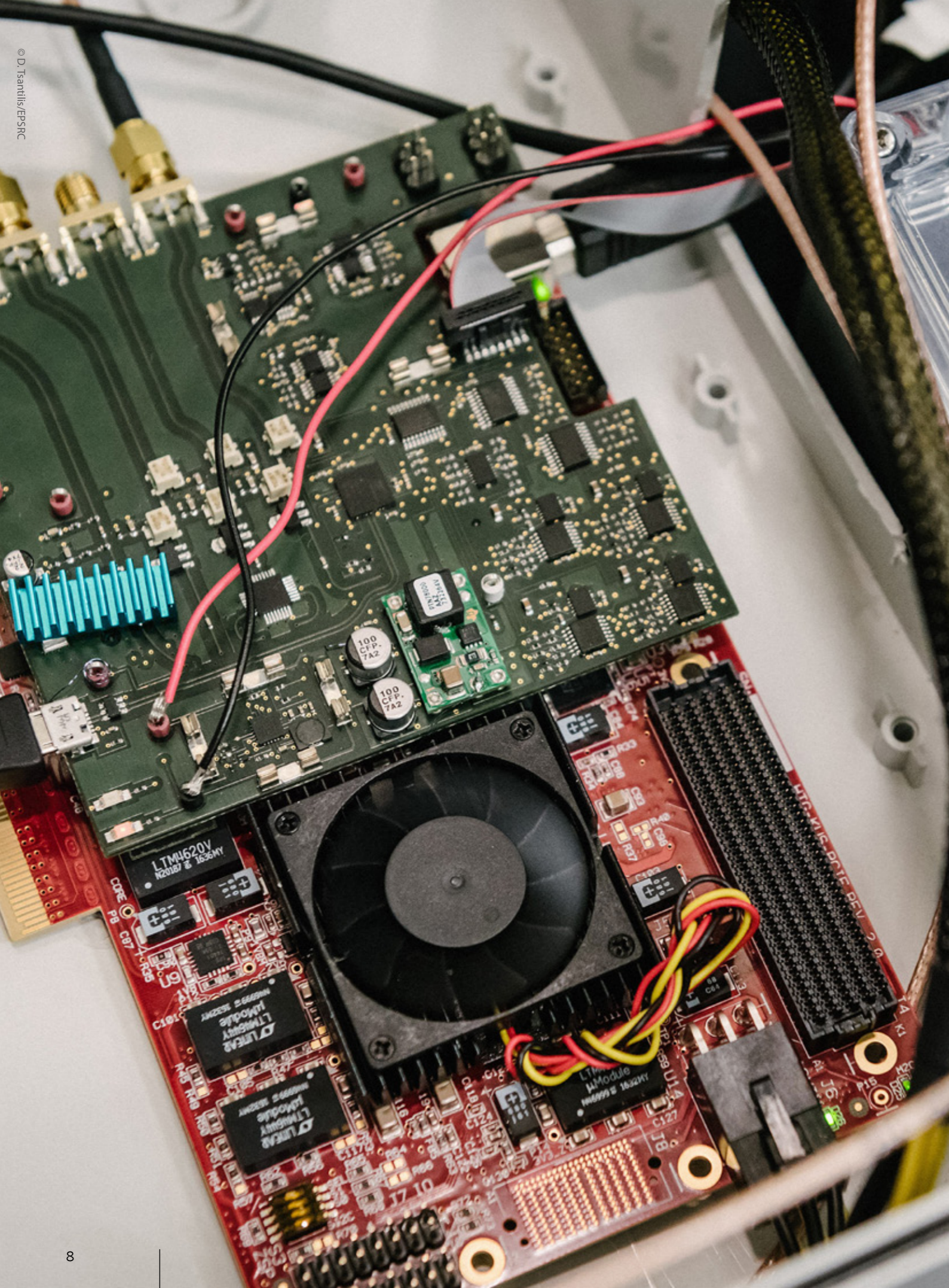
**Mark Thompson**, MSc PhD, is Professor of Quantum Photonics, Director of the Quantum Engineering Centre for Doctoral Training at Bristol and Deputy Director of the Centre for Quantum Photonics. He holds an EPSRC Early Career Fellowship and is pioneering the emerging field of silicon quantum photonics. 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. [N.B. While Professor Thompson is on sabbatical in the US, this work is being supervised by Dr Chris Erven]



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



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



## The Project Partners

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



University of  
BRISTOL

- Dr Christopher Erven
- Dr Anthony Laing
- Dr Reza Nejabati
- Professor Dimitra Simeonidou



- Professor Kenny Paterson



UNIVERSITY OF  
CAMBRIDGE

- Professor Richard Penty
- Professor Ian White
- Dr Adrian Wonfor



- Dr Pieter Kok



HERIOT  
WATT  
UNIVERSITY

- Professor Erika Andersson
- Professor Brian Gerardot



- Professor John Jeffers



UNIVERSITY OF LEEDS

- Professor Mohsen Razavi
- Professor Ben Varcoe



- Professor Samuel Braunstein
- Dr Roger Colbeck
- Professor Stefano Pirandola



- Professor Andrew Lord

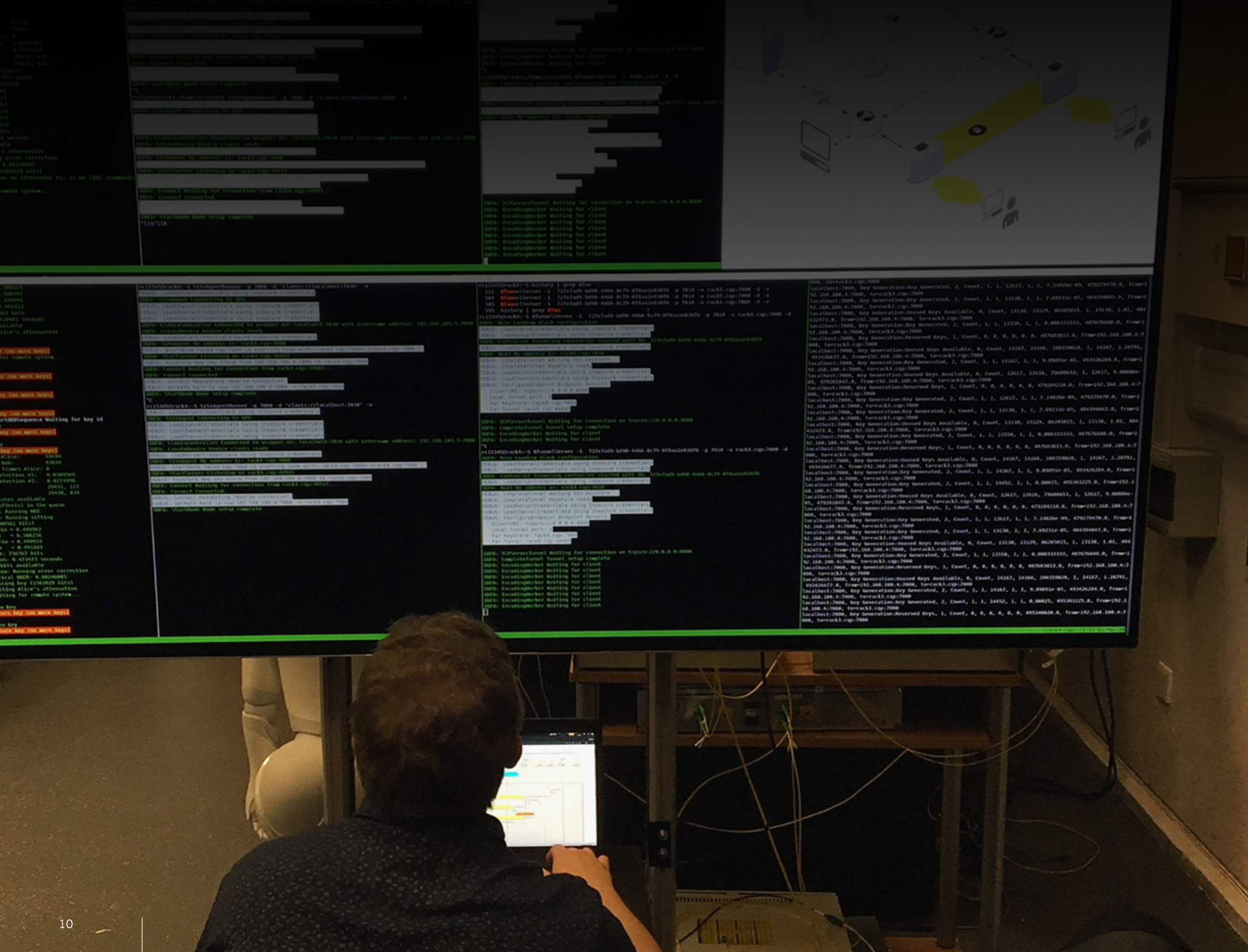


- Dr Andrew Shields



- Dr Christopher Chunnillall
- Dr Alastair Sinclair

# Technology Development: Progress in the fourth 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.*

Theme 1 focuses on the development of QKD technologies over short-range distances and in free space. This technology is designed for widespread use; the distribution of secrets to the public for daily, low bandwidth cryptography purposes such as internet banking.

The system comprises a handheld transmitter which is small and cheap ( $\leq \text{£}10$ ) which docks to a larger, more expensive ( $\text{£}2\text{k}$ ) fixed terminal - analogous to an ATM. The aim is to enable a user to share a few hundred kilobits of key in approximately four seconds. This is comparable to the time someone might spend at an ATM performing conventional financial transactions.

The receiver optics split incoming light into three polarisation bases (H/V, D/A, R/L) which can fully characterise incoming light and feedback signals into correction wave plates to adjust for any basis misalignment, including axial rotation which is not corrected for by the hand-tracking system.

In order for the theme 1 QKD system to be widely applicable, it must be easily integrated into user applications and into a wider infrastructure. To this end, work is underway integrating the devices into a QKD software framework developed at Bristol, initially within theme 3 (see below). This will allow easy integration with other devices also running on the framework and also provision of a documented software interface for applications to access and use QKD keys.

Through a partnership resource project, the QKD transmitter has been modified and integrated with the hand tracking for QKD developed at Oxford University. Also part of this project collaboration is a financial services company that is investigating the applications of QKD to their portfolio.

A second partnership resource project with the University of Strathclyde is investigating nanosatellite-to-ground QKD and the handheld transmitter design is a candidate for a source to fulfil the size, weight and power requirements of a 6U cubesat.



© D. Tsantilis/EPStRC

This work has produced optical devices with a drastic reduction in size, cost and integration complexity, combined with greater robustness. The successful development of QKD transmitter and receiver chips enables smaller form factor QKD solutions, which are simple to integrate into existing server facilities promising to prove to a commercial audience that QKD devices are mature for utilisation.

With a solid achievement in the demonstration of QKD devices fabricated using a chip scale process, the focus has now shifted to the development of more advanced QKD devices aimed at solving some inherent practical limitations of the QKD procedure. Measurement device independent (MDI) technologies aim to reduce the reliance on trustworthy detectors, commonly fabricated by third parties, thereby decoupling the device security from the security of the constituent components. Rapid progress towards MDI key exchange between two on-chip devices has been made. Wavelength division multiplexing (WDM) will increase the utilisation of fibre networks, increasing the efficiency and lowering the cost of QKD networks. WDM has been demonstrated using the mature QKD chips and further progress is being made with the design and fabrication of a new WDM specific chip and a fully packaged receiver device capable of receiving 4 channels, or daisy-chained to receive up to 16. Working closely with the National Physics Laboratory, work has been conducted in characterising and quantifying the quality of operation of the chip scale QKD devices ensuring that future certification standards do not adversely discriminate against chip scale solutions. Together these developments will ensure that on-chip QKD devices are compliant with future mainstream QKD protocols.

The use of Silicon on Insulator (SOI) substrates facilitates even greater benefits of cost and a more diverse supply chain, compared to the indium phosphide (InP) substrates used previously. High performance QKD transmitters based on the SOI platform have been produced. For future feasibility of mass-manufacture, SOI is a desirable material with which to perform quantum secure protocols. By overcoming the non-ideal characteristics of fast switches in silicon, we have demonstrated GHz-rate encoding and transmission of QKD keys with our technologies. Additionally, we have leveraged this platform to develop a number of quantum random number generators (QRNGs) – a crucial cryptographic primitive - leveraging quantum random sources such as vacuum fluctuations and laser phase fluctuations to produce highly compact, high performance QRNGs conducive to mass manufacture.

## Theme 2: Chip-Scale QKD Technology (led by Prof. M. Thompson and Dr C. Erven)

*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.*

Theme 2 focuses on using integrated quantum optics to develop chip-scale quantum key distribution (QKD) devices. It is based on the successful work at the University of Bristol in the design of chip scale quantum optical devices.

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

*Aim: The goal of Theme 3 is to develop technology for ubiquitous application of quantum security in communication networks, addressing the vital issues of telecom and cryptographic integration. It is distinguished from previous quantum network deployments in not requiring dedicated 'dark' fibre. It seeks to develop solutions for metro-core, access, and backbone networks and build a UK Quantum Network (UKQN), to serve as a test-bed for the technology developed in our Hub, and as a focus for application development, international standardisation and user engagement. The UKQN comprises metro-scale networks in Cambridge and Bristol, with a long distance backbone link between these. Here we report on all three aspects of the UKQN.*

Metro-core network - Cambridge Quantum Network (CQN): Last time we reported high-speed network secured quantum encryption in the Cambridge Metro network. This employed the three-link metro architecture composed of three quantum key distribution (QKD) systems forming the quantum layer and a deployed (Toshiba designed) network key exchange layer. The arrangement permitted high-speed applications such as 100G encryptors to efficiently access the quantum keys in the network. This year we report on two major developments building upon these results: (1) 18 months' operation of the quantum layer; (2) key relay in the Cambridge Metro network.

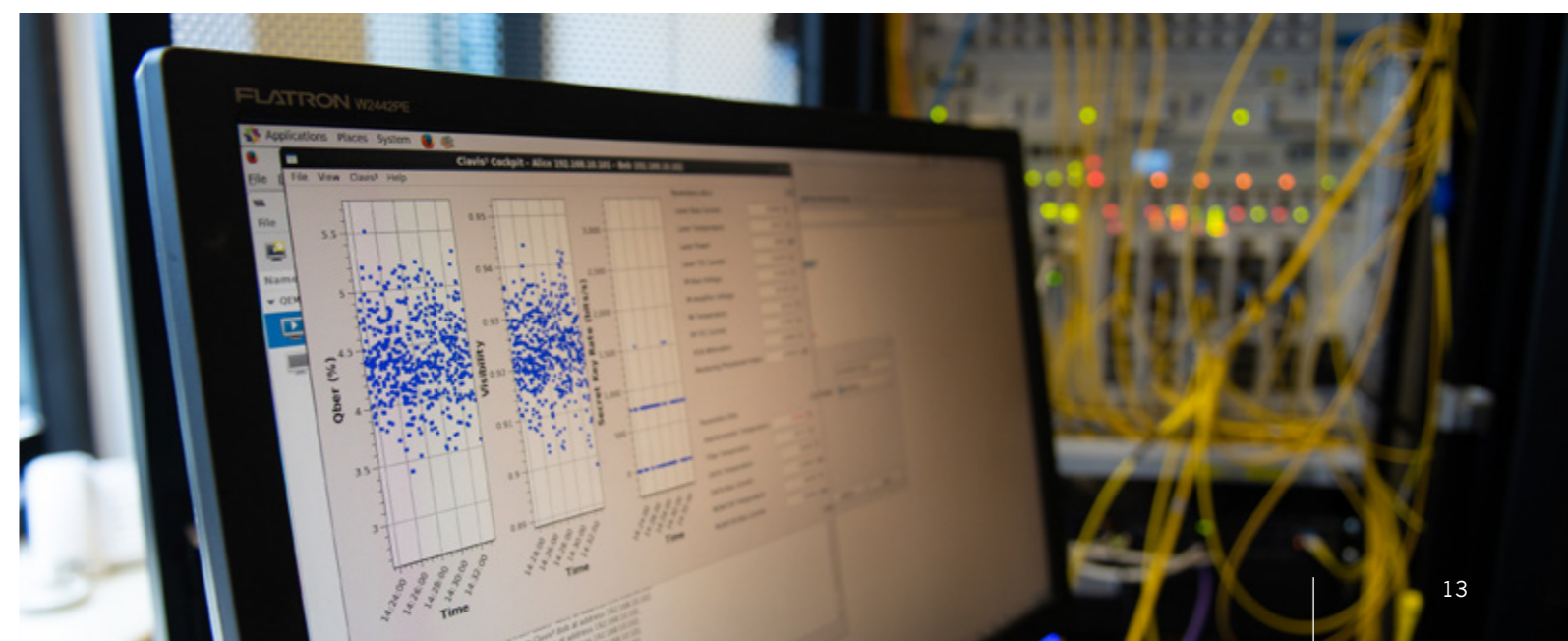
(1) 18 months' operation of the quantum layer: Long-term operation of the quantum layer in the CQN has been realised. Three installed links distilled on average 120 Tbits of secure key material over 1.6 years. Recorded long-term secure bit rates, on average 2.5 Mbps including stoppages, were attained in order to achieve this remarkable result.

(2) Key relay in the CQN: A key relay has been successfully demonstrated in CQN for global keys supplied to a 100G encrypted link operating over the same fibre link as QKD. By forcing this link to stop delivering keys, the network reacted favourably and re-routed the keys via a third site (ENG) using the other two QKD links. No service interruption was observed on the application side, indicating the key rerouting had been executed successfully. In the future, we hope to demonstrate key relay for more complex network scenarios involving more than three QKD links.

Both the above results were presented at the SPIE Photonics Europe Quantum Technologies conference in April 2018.

Metro-core network – Bristol Quantum Network (BQN): During this year, our key management system became operational with a software defined network (SDN)-controlled Network Manager used for receiving requests from the site agents, located in two physical locations (HPN and NSQI laboratories) in Bristol. Based on these requests, the network manager communicates with the quantum path algorithm to establish the most suitable path in the network. Then, the network manager configures the suitable cross-connections in the optical switch for the transmission of the quantum signal. The system was demonstrated live in front of an audience on multiple occasions to advertise its potential and stability. During the demonstrations, the system was taken from cold start to functional web streaming using the exchanged keys.

In Bristol, additional work was also undertaken optimising the co-existence of quantum communication channels with classical channels. To this extent, an artificial intelligence approach was implemented to enable the sharing of the spectrum in between one quantum channel and several classical channels. This approach alleviates the



impact of unpredictable non-linearities appearing when several classical channels are sharing the spectrum in a single optical fibre. This work on "Machine Learning-Assisted QKD Networking with SDN" was presented in September at the European Conference on Optical Communications (ECOC 2018), in Rome, Italy, as a prestigious invited paper. This work also shows the Bristol City field-trial co-existence of quantum and classical channels with SDN as an enabler for secure and optimum channel and path allocation, which reflects the use of such approach in actual installed optical network infrastructures.

Work was also demonstrated in the Internet of Things sector, where the chip-based quantum devices of theme 2 are particularly relevant. The use of quantum keys from a QKD system was probed to decrease the power consumption, moving the key generation from the devices to the quantum supplier. This work was also presented in the ECOC 2018 conference. In addition, the extension of the work presented on the mitigation of Denial of Service (DOS) over QKD networks with SDN has been thoroughly investigated and will be published soon.

Backbone network - UK long distance Quantum Network: Last time we reported the development of four QKD systems designed for the long distance links spanning Cambridge-London-Bristol, which form part of the National Dark Fibre Infrastructure Service (NDFIS). This year we have used these systems to build and test a laboratory replica of the Cambridge-London-Bristol network. We emulated the fibre distances and real losses using laboratory fibre spools and attenuators. The total fibre distance was > 400km with a combined loss of around 90dB. All four QKD links showed secure bit rates > 1.5kbps indicating we could refresh a 256-bit AES key once every 250ms across the entire network.

An important part of the long distance systems is CE certification. This is to enable the systems to be placed into the nodes of the long distance network, which contain safety critical infrastructure. CE certification was successfully completed towards the end of 2018. This certification now paves the way for the network to be deployed. We are currently awaiting a slot on the NDFIS to become available so we can realise the Cambridge-London QKD link during 2019, and then extend to Bristol.

## 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 subthemes 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 feeds into themes 1-3, to accelerate progress from the laboratory to the UK Quantum Network and eventual commercialisation.*

In theme 4, we have continued to investigate new approaches, applications, protocols and services, as well as more advanced component areas for existing QKD systems. At present, the areas being investigated include: quantum digital signatures; quantum oblivious transfer, quantum state elimination, quantum relays, repeaters and amplifiers; quantum state comparison amplifier, single photon emitters; and device-independent technologies.

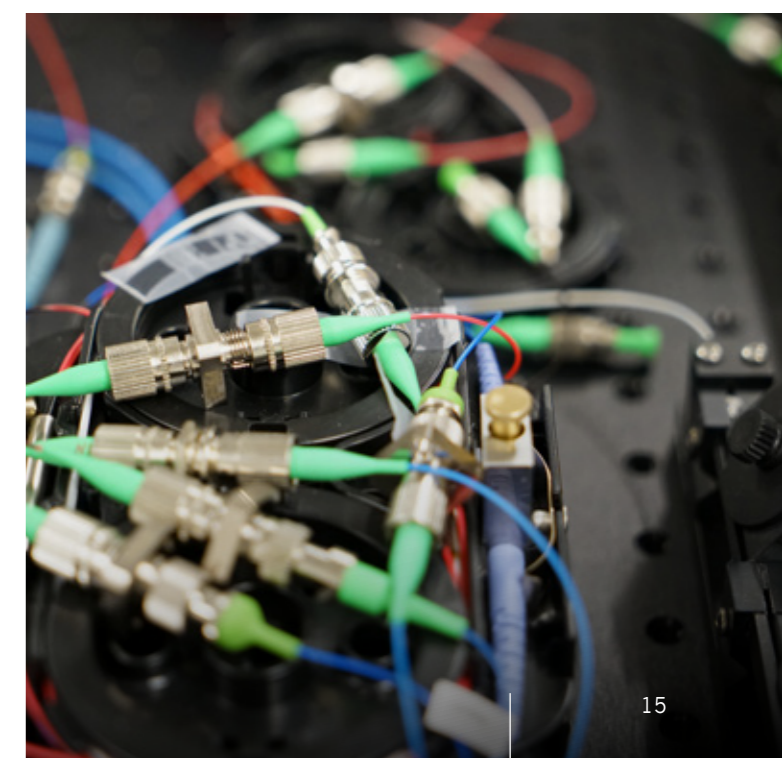
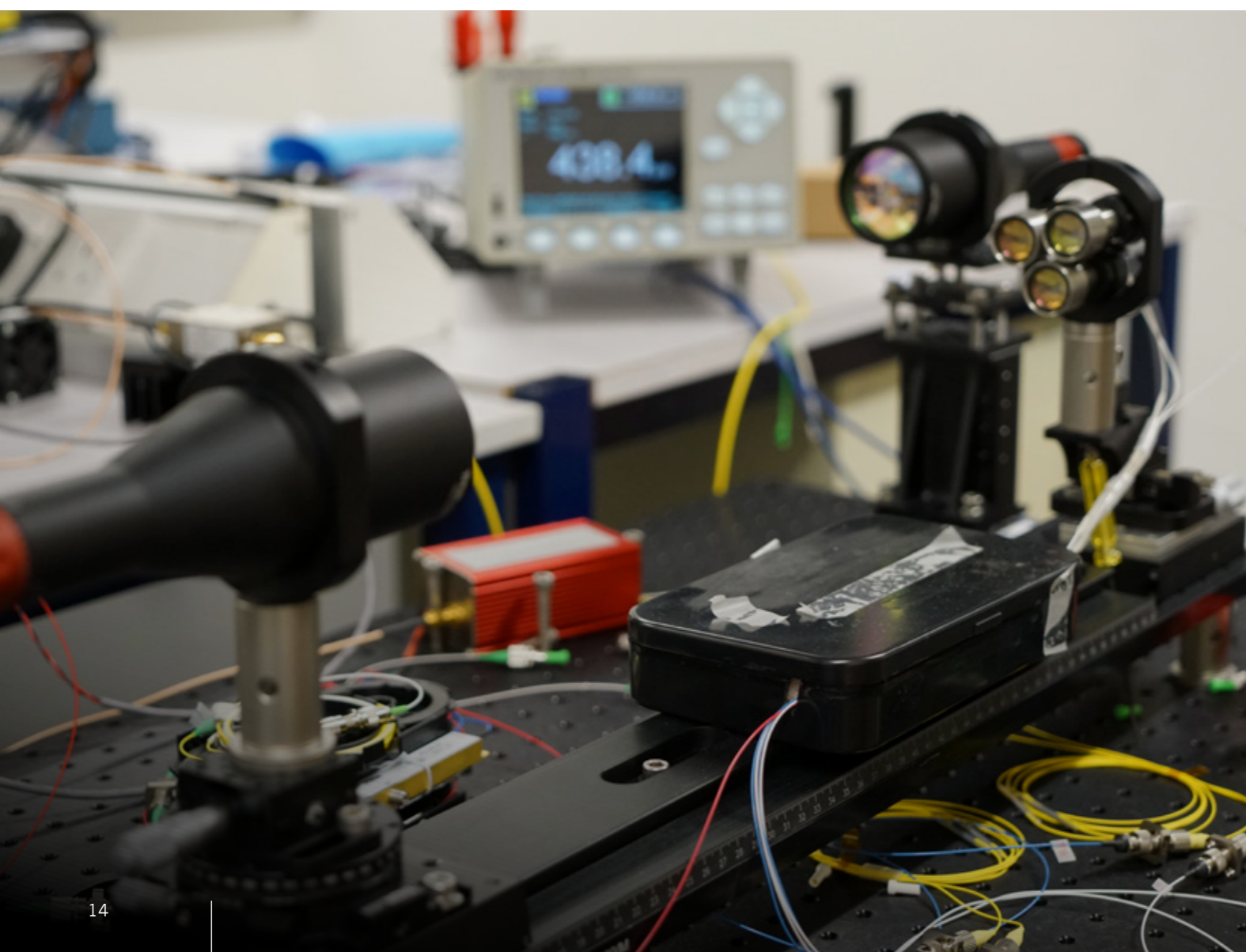
During the Hub, the application of quantum digital signatures (QDS) has developed from laboratory demonstrations over several metres of optical fibre to implementation in dark fibre in metropolitan networks over 100km distances. In parallel, the Hub has conducted the first experimental demonstration of measurement-device-independent (MDI) QDS. The existing security analysis for signatures generally (whether classical or quantum) is for stand-alone use, but in real applications composable security is desirable where overall security must be guaranteed. Hub researchers are actively examining the composable security of signature schemes. Our Hub researchers are also investigating practical approaches to quantum oblivious transfer using coherent quantum states of light.

With regard to amplifiers and repeaters, we continue to work on the state comparison amplifier (SCAMP) which has led to a practical feedforward approach with a significantly enhanced success rate over previous implementations. A miniaturised SCAMP has also been prototyped using ultrafast laser inscription techniques in fused silica to form the low-loss optical waveguides and beam splitters. A close collaboration between theoretical and experimental groups has resulted in the establishment of a detailed theoretical model, which has been used to predict the performance of future amplifier designs.

A quantum relay has been implemented by TREL and University of Cambridge using a Quantum Dot (QD)

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

Building on our recent realisation of ultra-bright and scalable single-photon sources in two-dimensional (2D) layered semiconductor material, we have designed heterostructure devices that enable loading electrons or holes one-by-one (via Coulomb blockade). This enables a spin-photon interface, where future applications may be in quantum repeaters. Also, we have combined a 2D semiconductor photon source and CMOS compatible photonic chips to create hybrid quantum photonic chips in lithium niobate. Initial work includes integration of a single-photon emitter coupled to a waveguide with a beam splitter to perform on-chip Hanbury Brown and Twiss interferometry. Finally, we have developed a new way to create 2D quantum dots – the so-called Moiré super lattices created by stacking two sheets of atoms (MoSe<sub>2</sub> and WSe<sub>2</sub> in our case) together with a relative angle. The electrons / holes are trapped in separate layers and spatially at the locations of the Moiré pattern. Quantum properties are determined solely by the band structure rather than a defect or external perturbation.



## Highlight: Strategic Development of Satellite Quantum Communications Initiative

Hub interest in quantum secure communications in space can be traced back as early as 2016, when we organised a specialist workshop ("QKD in Space") at the Harwell science campus. By 2018, a number of developments relating to: the advancement of the second phase of the National Quantum Technologies Programme; the idea of quantum technology Innovation Centres; the UK's new Industrial and Prosperity from Space Strategies, further investment in the emerging technologies through the Industrial Strategy Challenge Fund; and the proposed Space Sector Deal – all made a reappraisal of the UK landscape and a discussion about potential next steps both timely and necessary. The new National Satellite Testing Facility at Harwell and a commitment to a Quantum Space Lab at Harwell were also important developments influencing the need for a long-term strategy.

The Quantum Communications Hub took the initiative to explore the potential value of a UK coordination framework for space focused activities between the Space sector and the National Quantum Technologies Programme under an aligned vision, ambition, strategy and delivery. To that end, two key stakeholder meetings were organised for July and November 2018 with representation from EPSRC and Innovate UK, STFC/ RAL Space and UK Space Agency, the National Physical Laboratory, and of course the Hub. The group explored the UK environment and its strengths in research and innovation, the new landscape as shaped by important developments in satellite QKD missions (e.g. the bilateral UK/Singapore in-orbit QKD satellite and ESA-/UKSA-backed commercial satellite QKD service demonstrators), the international context with specific reference where strong links and complementarity of interests could be identified (e.g. Canada) and – importantly – any significant gaps in sovereign capability preventing the UK from playing an important role in the wider environment.

The main conclusion from the initial meetings was that although in the UK growth of the Space sector itself is a national strategic priority, and satellite communications one of the central application areas within it, there has been little attention to satellite quantum communications. We therefore have significant and distinctive but entirely discrete national strategic objectives, programmes and investment in three related areas: (1) satellite communications; (2) Space; (3) quantum technologies.



Satellite quantum communications is not included in any of these but if it were to be judged a national priority, then measures would be required to ensure that the UK does not continue to fall further behind in a research-led market that is inherently global.

A national coordinated initiative would put the UK at the forefront of research-led but industry-focused development and commercialisation. Such an initiative would be composite, bringing together distinct elements: R&D, design and engineering, experiment and testing; space qualification; launch/delivery machinery; operation and management. Funding would also need to be composite, with private/public investment. The latter would be driven by the strategic value of both research and research-led innovation and commercialisation. Private investment would be driven by early commercial return facilitated by publically research and innovation. Coordination would also balance the need for ongoing research at one end to feed the innovation engine, and the pull of commercialisation to exploit it at the other.

Moving forwards, the Hub will be expanding its work portfolio into satellite quantum communications in the context of a possible second phase of the national programme, and remains committed to pursuing the establishment of a national initiative in this area, bringing together stakeholders in satellite communications, space and quantum technologies.

## Highlight: A high-gain and high-fidelity coherent state comparison amplifier

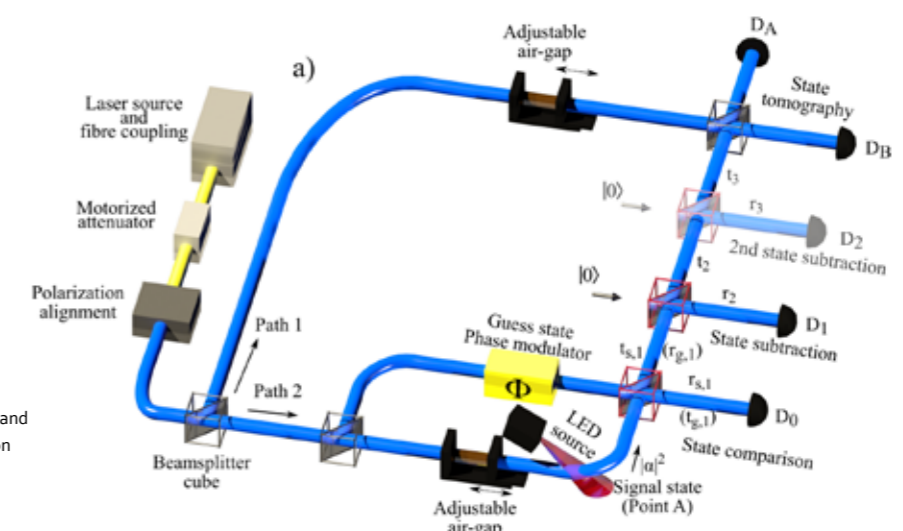
The internet is an essential tool in today's society for sharing and accessing vast amounts of information, streaming of high-resolution videos, as well as many other applications. The internet is linked over intercontinental distances thanks to the implementation of optical fibre cables and optical amplification technology, which allows optical signals to propagate further and at a higher bandwidth. So what is stopping us from sharing quantum information over an equivalent scale to create a global quantum internet? Can we not use the same amplifier technology for our quantum optical signals? Due to the unique features of quantum mechanics, it turns out the answer is, unfortunately, no. Using conventional optical amplifier technology on quantum optical signals will introduce too much noise in the output signal, which will lead to the original quantum information being swamped. However, there are alternative methods for amplifying quantum optical signals, which limit the amount of noise added to the quantum signals; these work probabilistically rather than 100% of the time.

The Quantum Communications Hub enabled the Heriot Watt Single Photon Group to perform experimental implementations of the state comparison amplifier (SCAMP), which is a method for amplifying quantum optical coherent states that are typically used in quantum communication protocols as they can be generated by a laser source. The SCAMP is a relatively simple quantum optical amplifier that only requires "off-the-shelf" components, such as attenuated laser sources, single-photon avalanche diode detectors, and linear optical components. In the first experimental implementation

of the SCAMP, we demonstrated significantly higher success probability and rates than previously demonstrated with other quantum optical amplifier methods.

In our highlighted paper, which was published in Nature's Communications Physics journal, we performed three experiments investigating the broader operation of the SCAMP. Our first demonstration highlighted that the SCAMP's characteristic gain can be tailored to the particular application by simply changing the beam splitter ratios in the experimental set-up. In a real operational scenario, there will be sources of photon noise not under the users' control, and in our second demonstration we showed that the SCAMP output was robust to external noise for realistic real-world levels of signal-to-noise ratios. Our final demonstration showed that we could improve the quality of the amplification output, at a small cost to the gain, by introducing an additional modular stage.

The highlighted paper's results prompted the development of significant enhancements to the system, firstly leading to our implementation of SCAMP on a chip to reduce the volume of the optical system and move towards a more real-world integrated device. We have also demonstrated a SCAMP 2.0 system that approaches the ultimate physical limits of amplification more closely by introducing a feed-forward mechanism to correct for incorrect amplifications. Such a feed-forward system could be used to operate as a quantum trusted node repeater in quantum communications systems.



Ross J. Donaldson, et al., "A high-gain and high-fidelity coherent state comparison amplifier", Communications Physics volume 1, Article number: 54 (2018)

Highlight:

## The Second Phase of the National Quantum Technologies Programme

The identification of quantum technologies as one of fourteen 'core industrial challenges' for its new Industrial Strategy Challenge Fund at a time when the first phase of the national programme was nearing completion and was thus ripe for evaluation, led the UK Government to launch an inquiry in early 2018 into these emerging technologies. The Inquiry was run by the Government's Science and Technology Select Committee, chaired by the Rt. Hon. Norman Lamb MP. Its remit was to collect and evaluate evidence on the opportunities and challenges for quantum technologies, including: progress on the recommendations of the 2016 Blackett report; the support needed from government, researchers and businesses to succeed in creating a quantum economy; the current state of the UK quantum industry; the oversight and regulation structures required; potential barriers and how these might be overcome; research priorities; the role of international collaboration within the context of Brexit; and any potential societal implications.

A number of Hub partners submitted written evidence during the first phase of the inquiry, followed by an invitation to the Director, Professor Spiller, to attend an oral evidence hearing in front of the Committee at the University of Glasgow in late June 2018. That hearing was also attended by representatives from the other Hubs, centres for doctoral training and industry leaders, while a subsequent session heard evidence from the then Science Minister, Sam Gyimah MP and the UKRI Chief Executive, Professor Sir Mark Walport. The evidence collected was crucial in highlighting the progress achieved during the first phase of the national programme, and the need for the work to progress, especially in the context of similar investment globally. The Select Committee's report was highly complimentary of the technical achievements in the first four years of the programme, while also recognising the strong case for continuity. The result was a set of recommendations, the most pressing of which was for the programme to continue for a further five years without the danger of any disruption caused by a "cliff edge". The UK Government took the Committee's findings on board and in September 2018 announced further funding towards a Network of four Hubs to continue work in the areas of quantum communications, computing, imaging and sensors and metrology. Additional investment was committed in the months to follow for capital equipment and towards a National Centre for Quantum Computing.

At the same time, and in anticipation of this investment into a second phase of the national quantum technologies programme, the Engineering and Physical Sciences Research Council initiated a scoping exercise in consultation with academic, industry, and government representatives to determine a) the strategic scope of the new Hubs; b) existing expertise relevant to the new scope, and c) any capability gaps. A number of consortia-building workshops took place, which then fed into an expression of interests call over the summer 2018, and eventually to an invitation to respond to an outline call for new Quantum Technology Research Hubs in the four main areas outlined above. In response to the new scope, our Hub significantly expanded the existing consortium by bringing in new partners with world-leading satellite (RAL Space), hardware security (Queen's Belfast), and quantum (incl. post-) cryptography (University of Kent) expertise, while also submitting an ambitious proposal for quantum secure communications at all distance scales, pursuing integration between these technologies and with conventional communications infrastructure - access, through metropolitan, up to inter-city scale quantum communications based on fibre and integrated with conventional systems; and even longer distance secure communications, across seas and country-to-country, requiring ground-to-satellite quantum links. Major new proposed activities include - in addition to the satellite work - entanglement-based networking, components (detectors and sources) to underpin the whole range of quantum communications technologies, as well as new work on the UK Quantum Network (including CV-QKD), hand-held QKD and chip-based systems. We plan to also include a dedicated activity for new protocols, beyond key distribution. The final theme of our proposed future work is security of devices, systems and end-to-end. This work cuts across all our technology approaches and will comprise three activities: metrology and calibration, contributing further to relevant standards; exploration of a range of cryptographic and quantum primitives and the integration of quantum and post-quantum technologies; and, finally, security analysis, vulnerability analysis and testing, and the development of countermeasures - all from the perspective of providing practical and secure applications and services.

A full proposal submission will take place in 2019, when a funding decision will also be made.

Highlight:

## 3QN - Towards A New UK Industry for Novel Quantum Receivers in Nascent Satellite QKD Global Markets

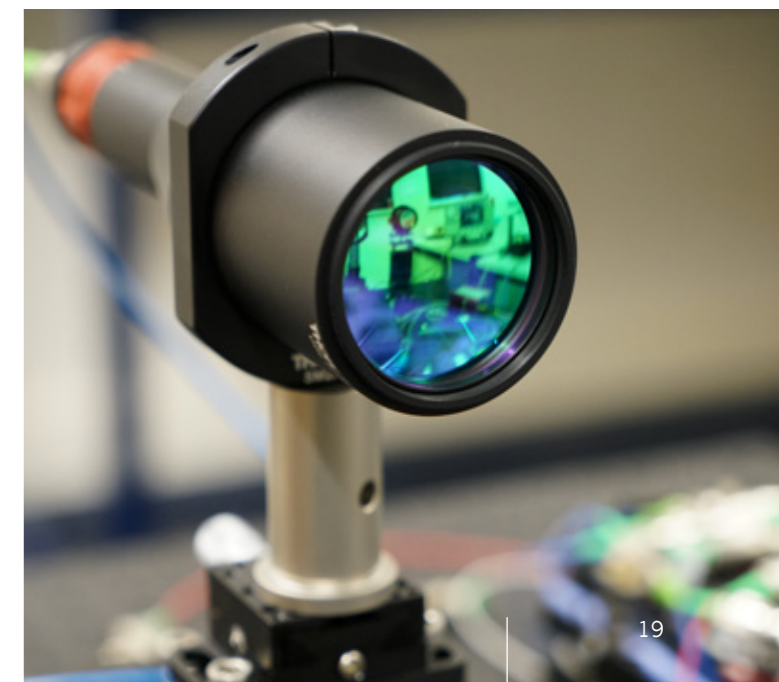
The UK Government's Industrial Strategy Challenge Fund (ISCF) brings together leading research and business to tackle the big societal and industrial challenges today. 2018 saw the investment of a further £20m, part of the overall ISCF quantum technology allocation, towards projects designed as industry-led collaborations with academics and further pursuing research and development geared towards the commercialisation of quantum technologies. This was the so-called Quantum Technologies Pioneer Fund, administered by Innovate UK, which following a highly competitive process in late spring of that year, selected four suitable projects: two in the area of quantum sensors and gravity, and - crucially - two in the area of quantum secure communications. The two successful projects were firstly AQuaSec (Agile Quantum Safe Communications; £5.8m), led by Hub industrial partner Toshiba Research Europe Ltd, and including numerous other partners from across the Hub (the Universities of Cambridge, Glasgow, Heriot Watt, Royal Holloway London, Sheffield, BT, KETS Quantum Security and NPL). AQuaSec aims to develop new quantum-resistant algorithms while also implementing new ultra-compact QKD prototypes based on photonic integrated circuit (PIC) technology.

The second awarded project in the area of quantum secure communications is 3QN (Towards A New UK Industry for Novel Quantum Receivers in Nascent Satellite QKD Global Markets; £3.25m) led by industrial partner ArQit and again incorporating many Hub partners (the Universities of Cambridge, Heriot Watt, York, BT, NPL). Our Hub had significant input in both proposals but especially so in this latter 3QN project, as it aligns with our vision of expanding our work into free-space quantum communications at extra-terrestrial scales using satellites, and it is based on technology borne through Hub research and development.

3QN seeks to address the well-known distance limitations of QKD - the abundance of noise inside optical fibre in transmissions greater than a distance of about 150km makes QKD use impractical over large terrestrial scales. QKD through free space, on the other hand, can be less sensitive to distance. Satellites therefore provide the means for distributing keys across very large distances between end users spread across countries or continents, and facilitating global QKD networks. Following the

launch of the world's first Quantum Communications satellite by China in 2016, a number of international missions (Canada, Japan, Switzerland, many European countries including the UK) are planning their own missions, all directed at delivering commercial satellite QKD services. Crucial in all of these will be networks of Optical Ground Receivers (OGRs) required to receive and detect the photons carrying the key information.

The 3QN project is focused on designing and building such affordable prototype modular optical QKD receivers that can be used to receive quantum keys from satellites using different QKD transmitters. Such devices would therefore not be limited to servicing any particular satellite but have a "plug and play" functionality instead, thus widening options for adoption and impact in the commercial world. The strategic aim of the Pioneer Fund call was to pave the way for scaled-up production of commercial prototypes, for UK manufacture and assembly to address global markets, and, in the process, opening up the existing small, niche markets, which only cater for scientific research instruments. The project will draw on the UK's (and the Hub's) expertise in advanced optical and photonic technologies, as well as the wider UK opto-electronics ecosystem for visible and telecoms wavelength detectors and emitters. Early adopters and beneficiaries of any resulting commercial products will be the telecommunications, finance and energy sectors, which all have global footprints and requirements for global services.



## Highlight: International Engagement – Canada



In spring 2018, Hub Director, Professor Tim Spiller, took part in a Global Expert Mission into Quantum Technologies to Canada, an initiative led by Innovate UK (IUK). Delivered by the Knowledge Transfer Network (KTN) with support from the Catapult Centres, Expert missions help further IUK's global strategy by providing the evidence base for investment, and the opportunities for UK businesses to build partnerships and collaborations with key economies. Canada has invested over \$1B in quantum-related R&D over the past decade and is currently a global leader in this emerging field.

The mission came a year after the UK and Canadian governments signed a Memorandum of Understanding (MOU) related to science, technology and innovation. The MOU represents a commitment to enhance bilateral co-operation on complementary areas of research, technology, entrepreneurship and innovation, with the aim of accelerating the commercialisation of emerging technologies, and thus promoting the growth of jobs and businesses. Quantum technologies was stated as being one of four initial priority areas on which to focus.

The Canada Quantum Technologies Expert Mission visited Ottawa, Waterloo and Vancouver during the week of 19-23 March 2018. The UK and Canada have a history of world-class research and substantial investment in quantum science and quantum technology. There are two distinct industrial markets: specialist technology to support the ~1,500 laboratories world-wide engaged in quantum research, and end-user products

incorporating quantum technology. This particular mission's focus was mainly on Canadian work on QKD in space (a key Quantum Communications Hub priority for any potential second phase of the national programme), and future mission and exploitation plans, as well as Canadian work on quantum computing.

The mission was led by Sir Peter Knight, member of the national programme's strategic advisory board and Chair of the Quantum Metrology Institute, and included senior programme stakeholders from all four UK Quantum Technology Hubs, the National Physical Laboratory as well as leading industry representatives. It sought to: develop a deeper understanding of the quantum technologies landscape in Canada; explore prospective areas for future collaboration on quantum technologies between the UK and Canada; identify synergies between the activities of the two countries; and gain a greater understanding of Canadian priorities in R&D and industrial, supply-chain, end-user and technology exploitation.

A summary report has been published by IUK/KTN summarising the information and insight gathered in Canada. The mission found a "genuine appetite for long-term and meaningful collaboration, from foundational science through technologies in space, security and defence, to standards, training and entrepreneurship". Communications in particular was singled out as the most promising area for technical collaboration.

## Highlight: Launch of the Cambridge Metro Quantum Network

The UK's first quantum network, a major Hub deliverable, was launched in Cambridge in early summer 2018, enabling 'unhackable' communications, made secure by the laws of physics, between three sites around the city.

The metropolitan network provides secure quantum communications between the Electronic Engineering Division at West Cambridge, the Department of Engineering in the city centre and Toshiba Research Europe Ltd (TREL) on the Cambridge Science Park.

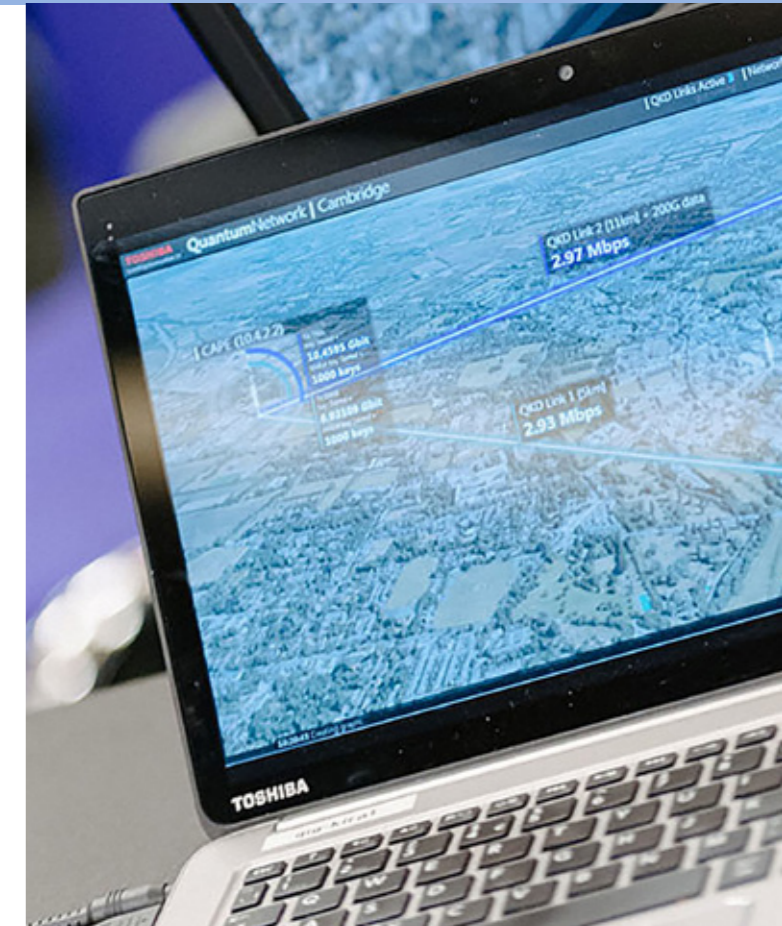
Quantum links are so secure because they rely on particles of light, or photons, to transmit encryption keys through the optical fibre. Should an attacker attempt to intercept the communication, the key itself changes through the laws of quantum mechanics, thus alerting the communicating parties to the presence of an eavesdropper.

Researchers have been testing the ultra-secure network for the last year, providing stable generation of quantum keys at rates between two and three megabits per second. These keys are used to securely encrypt data, both in transit and in storage. Performance has exceeded expectations, with the highest recorded sustained generation of keys in field trials that include encryption of data in multiple 100 gigabit channels.

The Cambridge network was built by partners in the Quantum Communications Hub. The local infrastructure was provided by Toshiba Research Europe Ltd (TREL), who supplied the quantum key distribution (QKD) systems; ADVA, who supplied the optical transmission equipment; and the University's Granta Backbone Network, which provided the optical fibre.

"Through this network we can further improve quantum communications technologies and interoperability, explore and develop applications and services, and also demonstrate these to potential end users and future customers," said Professor Timothy Spiller of the University of York, and Director of the Quantum Communications Hub.

"The development of the UK Quantum Network has already led to a much greater understanding of the potential of this technology in secure applications in a



range of fields, in addition to bringing new insights into the operation of the systems in practice," said Professor Ian White from Cambridge's Department of Engineering. "I have no doubt that the network will bring much benefit in the future to researchers, developers and users."

"Working with the Quantum Communications Hub, Cambridge and ADVA has allowed us to develop an interface for delivering quantum keys to applications," said Dr Andrew Shields, Assistant Director of Toshiba Research Europe Ltd. "In the coming years the network will be an important resource for developing new applications and use cases."

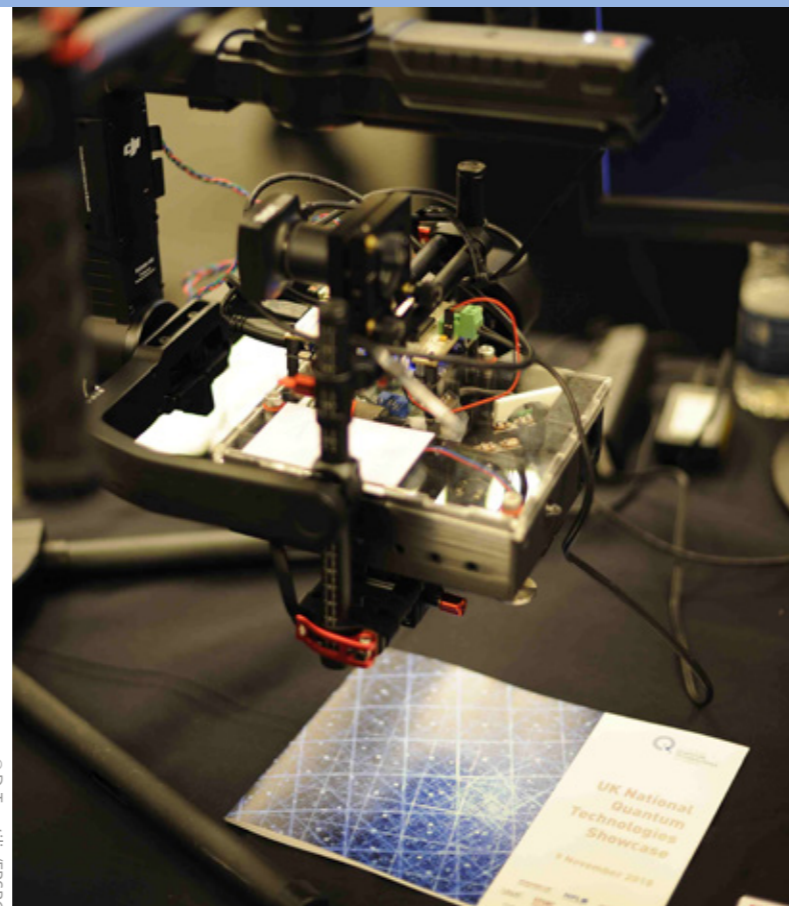
"Development of the network has brought together in the Quantum Communications Hub partnership many world-class researchers and facilities from both UK universities and industry," said Dr Liam Blackwell, Head of Quantum Technologies at EPSRC. "This is a reflection of EPSRC's commitment to investing in UK leadership in advanced research and innovation in quantum technologies."

## Highlight: The 2018 National Quantum Technologies Showcase

The quantum community gathered once again in late autumn 2018 in central London to mark what has become a fixture in the industry calendar – the annual national quantum technologies showcase. With over 80 exhibits and more than 700 delegates, the event was the biggest yet and representative of the many advances achieved towards the commercialisation of prototype quantum technology in the context of the national programme. The mood was celebratory following the preceding Treasury Budget announcement of a further £235m investment in a second phase of the UK national quantum technologies programme (UKNQTP) to fund a National Quantum Computing Centre, a quantum funding round within the context of the Industrial Strategy Challenge Fund (ISCF) and more money for skills and training, e.g. through centres for doctoral training. The investment followed on from an earlier – September – announcement of an additional £80m available towards the continuation of the work of the UK National Quantum Technology Hubs committed to developing commercial-ready technologies in the specific sectors of quantum sensing, imaging, computing and secure communications.

David Delpy CBE, Chair of the UKNQTP Strategic Advisory Board, delivered the welcoming address, followed by Nick Chism, Director General, Enterprise at the Department for Business, Energy and Industrial Strategy (BEIS), and finally Roger McKinlay, Challenge Director for Quantum Technologies at UK Research and Innovation. During the opening addresses the winners of the most recent £20m ISCF quantum technologies Pioneer Fund competition were announced, which included the AQuaSec and 3QN projects, led by TREL and Arqit respectively and involving a number of Hub partners.

Our Quantum Communications Hub participated in the showcase with eight technical demonstrations: a quantum cryptography system with classical communication elements (CV QKD) offering high noise resistance using off-the-shelf components and benefitting from low cost, less complex and high through-put options for network operators; a chip-scaled fibre-based QKD with verification system, offering reduction in cost and size for this emerging technology; a handheld QKD system offering low size, weight and power requirements and specifically suited for financial applications as a quantum secure



© D. Tsantilis/EP5RC

replacement for chip authentication devices; miniaturised quantum communications nanosatellite systems enabling space-based QKD services via cheap, effective and mass-producible nanosatellites; a demonstration of software defined network QKD setup with practical applications in adaptive networks for encryption using disposable symmetric keys fitting within a standard framework; a quantum alarm demonstration for physical layer security centred around a low-cost classical communications system with embedded quantum signals that can detect eavesdropping offering a significantly reduced requirement for data post-processing; a demonstration of operability and setup of the UK's first quantum network; and a demonstrator of optical receiver technology for satellite quantum communications, highlighting the potential for truly global quantum network capabilities and opening up a range of end user applications.

This year's event was organised by the Engineering and Physical Sciences Research Council with input from all other major stakeholders of the UKNQTP.

## Highlight : The MacroPhoton

Conceived in early 2018 by Heriot Watt researcher Dr Robert Collins, the MacroPhoton is a demonstrator using the concept of photons scaled to the macroscale to demonstrate how quantum secure communications work. It is an interactive, easily transportable teaching aid using the duality of photons (light particles) and light polarisation to highlight the potential of quantum mechanics for uncompromisingly secure, encrypted communications. It introduces people to the concept of the polarisation of light by demonstrating the Bennett-Brassard 1984 quantum key distribution protocol, or put another way, it shows how single photons can be used to encode, process and transmit information securely.

The MacroPhoton consists of a sender unit ("Alice") in the form of a small, portable suitcase with big bright buttons in primary colours and flashing lights, representing a laser

(photon source). Alongside Alice, there are eight equally portable, glossy plastic receiver units, each approximately the size of a fizzy drink can, representing the photons that Alice is sending but scaled up – literally macro-photons. Communication scenarios are enacted involving two (or more) people performing the role of sender and receiver. The person handling the Alice unit is asked to make a series of eight random choices by choosing a light polarisation state (linear or diagonal) and a bit state (0 or 1) each time and pressing the encoding button in the middle of the unit to wirelessly send part of the secret key as encoded information to the receiver. A second person, representing the receiver ("Bob") is then being handed the MacroPhoton units, one by one, and is asked to make an equally random choice regarding the polarisation, i.e. how to measure the encoded information that is being received. At the end of the experiment, Alice is asked to reveal to Bob the eight polarisation states used each time and results between the two parties are compared. Due to quantum effects such as the uncertainty principles and superposition, the two parties will have randomly chosen the same option only some of the times (e.g. both chose linear). By comparing the screens of Alice and the "correctly encoded" macro-photons, Alice and Bob can see that they have correctly transmitted parts of the secret key as 0s and 1s in the case where they made the same choice of polarisation state. The rest of the macro-photons, where different polarisations states were used, are then discarded.

Since its inception, the MacroPhoton has been used in a number of outreach events involving thousands of participants across all age ranges and education backgrounds. It has been met with enthusiastic response and hugely positive feedback throughout and in early 2019, it won the Heriot Watt University Principal's Public Engagement Prize in the Public Engagement Partnership category.

The MacroPhoton was developed as a joint investment by the Quantum Communications Hub and the School of Engineering and Physical Sciences, Heriot Watt University. Future plans include extending the functionality of the MacroPhoton by expanding the software to demonstrate the Ekert 1991 protocol, and to add on an eavesdropping unit.

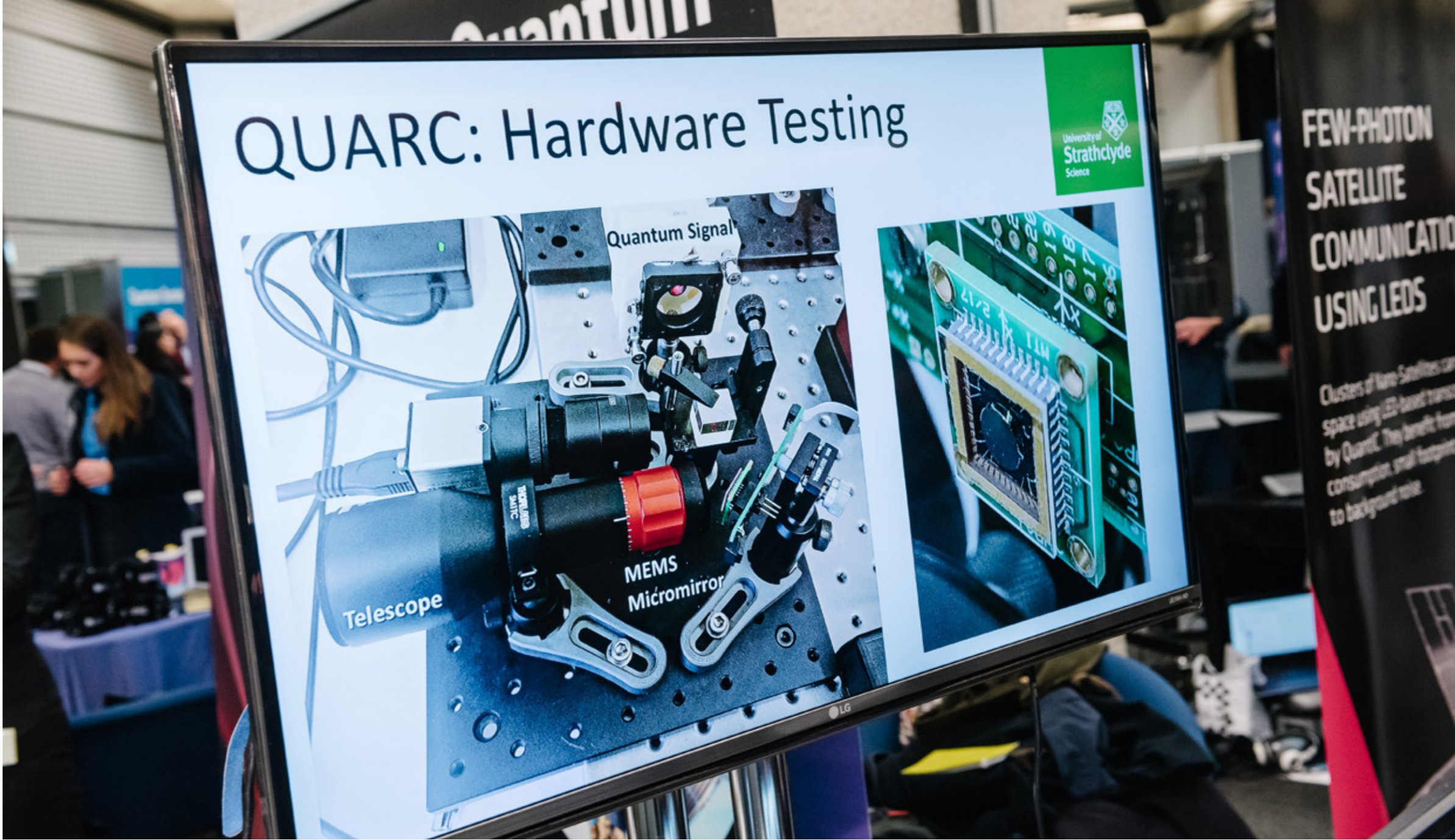


# Partnership Resource Investment

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

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

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



## Autonomous System for Measurement Device Independent QKD (Toshiba Research Europe Limited, the University of York)

MDI-QKD is a recently developed protocol that is secure from attacks on the photon detectors, which are often deemed to be the most vulnerable components in a QKD system. Although attractive from a security viewpoint, the technology for MDI-QKD is much less mature than for conventional QKD. This project seeks to realise a MDI-QKD prototype that can operate continuously and with spatial separation of the two communicating parties, tackling challenges such as realisation of high-speed, real-time modulation of indistinguishable pulses from remote locations, and synchronisation of those remote locations.

## CubeSat QKD and Groundstations (Craft Prospect, the Universities of Bristol and Strathclyde)

The project will realise a satellite QKD with cube satellites, through exploitation of their lower development, launch costs and rapid development, and culminating in a terrestrial demonstration and engineering model of a CubeSat QKD system and optical ground station ready for full mission capability and in-orbit-demonstration. It will involve detailed engineering and testing of the various sub-systems (Optical Ground Station: telescope, receiver unit. CubeSat: development of optics, ATP, sources, relevant software and firmware), thus preparing the ground for further development work on full mission capability and in-orbit-demonstration (IOD).

## Realistic Threat Models for Satellite Quantum Key Distribution (ID Quantique, the Universities of Leeds and York)

Key challenges for a secure satellite-based QKD system include loss and noise levels in the link. Current experimental demonstrations suggest that a typical LEO satellite-ground link would suffer around 40 dB of loss for a modest-size receiver telescope, and with night operation only in order to minimise the noise. Some of these limitations are partly based on assumptions in our security analysis. This project will provide an in-depth security study of satellite QKD, examining various assumptions about the physical channel between satellites and ground stations and aiming to add new capabilities through maximising the user exploitability of current and future quantum satellite missions.



### Satellite Visibility Simulator for Quantum Optical Services and Experiments (RAL Space, the University of Edinburgh)

Quantum Communications systems needing line of sight, and low-noise optical communications between space and ground-stations require elements of both simulation methods in order to develop feasible usage scenarios. Developing commercial services and applications based on quantum communications will be highly dependent on modelling the communication throughput against a statistically correct Earth model that takes into account clouds, aerosols and other scattering mechanisms. The project will develop an atmospheric visibility model, based on high temporal and spatial resolution data used to determine realistic optical transmission statistics derived from short (90 minutes) to medium (1 year) timescale data, and of value to missions currently in planning.

### QCHAPS – Quantum Communications & HAPS: A Feasibility Study (BT, the Universities of Heriot Watt and York)

Interest in the use of aerial platforms for communications has steadily grown, as has the number and types of platform available. These range from tethered hybrid helium-filled kite-like systems at relatively low altitudes, to aircraft or airships at high altitudes. These higher altitude systems (typically 17-22km) are often referred to generically as HAPS / HAPs (High Altitude Platform Stations / High Altitude Pseudo Satellites, or High Altitude Platforms). The usefulness of specific platforms for any application is determined by multiple variables and constraints, including altitude and stability of the platform, as well as payload size / weight, power requirements etc. This project is a feasibility study intended to provide the basis for future experimental work / technical demonstration by bringing together the relevant expertise across HAPS, HAPS-based communications, QKD in free space, and satellite QKD receivers / ground-stations, with input from industry perspectives.



# Public Engagement and Outreach

Hub public engagement and outreach activities in 2018 increased considerably both as a result of renewed resource investment and diversification of approach. The Hub provided generous sponsorships to a number of Quantum Summer Schools (Bristol, Glasgow, York), to colleagues at Heriot Watt in support of a Royal Society summer science exhibition demonstration, and to a collective initiative (the “Quantum City”) along with fellow national programme stakeholders, which in turn resulted to appearances in numerous high-profile science festivals.

Quantum City was launched in late 2018 as the public engagement arm of the National Quantum Technologies Programme. It is a joint initiative involving the Network of Quantum Technology Hubs, the National Physical Laboratory and the Quantum CDTs at Bristol, Imperial and UCL, aiming to promote public understanding of the benefits of quantum technologies and the work that is taking place within the remit of the national programme. Through a joint communications and impact evaluation plan, a series of science festival demonstrations, strong online presence and a coordinated social media strategy, participating partners hope to instil an understanding of the applications of quantum technologies, showcase the UK’s expertise in this area, and inspire young audiences to become the next generation of quantum technologists. Under the Quantum City branding, the Hub took part in numerous major science festivals in 2018 – Cheltenham and the York Festival of Ideas in June, New Scientist Live in London in September, the Festival of Physics in Edinburgh in October – engaging with thousands of visitors who reported overwhelmingly positive feedback.

At the same time, the partners launched the Quantum City website ([www.quantumcity.org.uk](http://www.quantumcity.org.uk)) featuring content in non-technical, engaging language, with the aim of promoting awareness, creating interest and addressing any questions about the impact the new technologies will have across all aspects of everyday life: healthcare, environment, transport, finance, manufacturing, communications, and many more. With a design that is modern, colourful and

easy to navigate, the website aims to appeal to a wide range of audiences: from interested audiences with no technical background to science enthusiasts, and from teachers to young students, who want to find out more about quantum related career pathways. The site has been conceived as an ever-evolving depository of content to eventually include: pieces explaining basic concepts in quantum technologies, how these translate onto practical applications and how they compare to existing solutions; videos and animations, including of fun technical demonstrations; educational materials and teaching resources; news items highlighting exciting developments; blogs written by researchers and partners relating their experiences of working in the field; events listings; and much more.

At the same time Hub colleagues at Heriot Watt, led by Professor Brian Gerardot, were selected to take part in the prestigious Royal Society Summer Science Exhibition which celebrates the cutting edge of UK science. Over the space of a week the Atomic Architects team created an interactive exhibit to explain how new nanoscale devices can be made possible. Visitors could isolate single sheets of atoms from a crystalline sample using sticky tape, and re-stack them to create brand new crystal structures with unique properties. To help visitors appreciate how many atomic layers they had exfoliated and why they were so colourful, a thin film interference demonstration was made using bubbles – a particularly popular feature for younger visitors. An eye-catching part of the exhibit was the large interactive Moiré wheel which, when activated by the push button and motor, would spin a top sheet of, and atomic crystal relative to, the bottom layer to produce a mesmerizing display of Moiré patterns. This model, along with some hand-held paper Moiré images, helped explain how atomic spacing and patterns affect the electronic and optical properties of materials and how atomic layers can be fine-tuned to make entirely new materials. An accompanying video game (Atomic Architects – available on Android Play and Apple App Store as well as at the team’s website) showed the challenges an electron faces in crystals to produce light. The Hub supported the creation of the exhibit by covering a large part of the manufacturing costs.

Finally, the Hub contributed generously through both support with running costs and human resource (lectures and demos) to three quantum summer schools in the summer of 2018: Quantum in the Summer (organised by the University of Bristol, 6-10 August); Quantum Technology School (organised by the University of Glasgow, 4-5 September); and the Quantum Information, Computing,



and Control (QuICC) Summer School (organised by Imperial College and hosted at the University of York, 13-17 August). The first two of those focused on A-level students with an interest in science and, in the case of Glasgow, also their science teachers; everyone got an introduction in some of the ideas behind quantum communications, through tutorial, talks and hands-on workshops. The QuICC school involved lectures for some 50 early stage researchers and students who were introduced to a number of topics varying from quantum foundations to quantum biology. Overall feedback was very positive.

Our project Twitter feed (@QCommHub) continues to be our main communicating channel between our team and fellow research, industrial, business, STEM, education, media and general public communities, and a constant source of up-to-date Hub news.

## APPENDICES

### Peer reviewed publications and conference proceedings

Amiri R, Abidin A, Wallden P & Andersson E. Efficient unconditionally secure signatures using universal hashing. In: International Conference on Applied Cryptography and Network Security, 143-163 (2018)

Bahrani S, Elmabrok O, Currás Lorenzo G & Razavi M. Finite-Key Effects in Quantum Access Networks with Wireless links. In: GLOBECOM 2018 - 2018 IEEE Global Communications Conference. IEEE Global Communications Conference (GLOBECOM), 09-13 Dec 2018, Abu Dhabi, UAE. IEEE (In Press)

Brotons-Gisbert M, Branny A, Kumar S, Picard R, Proux R & Gerardot BD. "Charge-tunable quantum dots in monolayer WSe<sub>2</sub>," in Frontiers in Optics / Laser Science, OSA Technical Digest (Optical Society of America, 2018), paper FW6C.2 DOI: 10.1364/FIO.2018.FW6C.2

Collins RJ, Donaldson RJ & Buller GS. Progress in experimental quantum digital signatures. Proceedings SPIE Volume 10771, Quantum Communications and Quantum Imaging XVI; 107710F (2018) DOI: 10.1117/12.2319015

Cope TPW, Goodenough K & Pirandola S. Converse bounds for quantum and private communication over Holevo-Werner channels. J. Phys. A: Math. Theor. 2018; 51:494001 DOI: 10.1088/1751-8121/aae964

Derbez P, Fouque PA, Lambin B & Minaud B. On Recovering Affine Encodings in White-Box Implementations. IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925, Vol. 2018, No. 3, pp. 121-149, DOI:10.13154/tches.v2018.i3.121-149

Donaldson RJ, Mazzarella L, Collins RJ, Jeffers J & Buller GS. A high-gain and high-fidelity coherent state comparison amplifier. Communications Physics 2018; 1: 54 DOI: 10.1038/s42005-018-0054-z

Ellis DJP, Bennett AJ, Dangel C, Lee JP, Griffiths JP, Mitchell TA, Paraiso TK, Spencer P, Ritchie DA & Shields AJ. Independent indistinguishable quantum light sources on a reconfigurable photonic integrated circuit. Appl. Phys. Lett. 2018;112:211104 DOI:10.1063/1.5028339

Huang A, Barz S, Andersson E & Makarov V. Implementation vulnerabilities in general quantum cryptography. New J. Phys. 2018; 20:103016 DOI: 10.1088/1367-2630/aade06

Kent A. Unconstrained summoning for relativistic quantum information processing. Phys. Rev. A 2018; 98: 062332 DOI: 10.1103/PhysRevA.98.062332

Kotzias P, Razaghpanah A, Amann J, Paterson KG, Vallina-Rodriguez N & Caballero J (2018). Coming of Age: A Longitudinal Study of TLS Deployment. In Proceedings of the Internet Measurement Conference 2018 (IMC '18). ACM, New York, NY, USA, 415-428. DOI: <https://doi.org/10.1145/3278532.3278568>

Lupo C, Ottaviani C, Papanastasiou P & Pirandola S. Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution. Phys. Rev. Lett. 2018; 120: 220505 DOI: 10.1103/PhysRevLett.120.220505

Lupo C, Ottaviani C, Papanastasiou P & Pirandola S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. Phys. Rev. A 2018; 97: 052327 DOI: 10.1103/PhysRevA.97.052327

Martinez A, Fröhlich B, Dynes JF, Sharpe AW, Tam W, Plews A, Lucamarini M, Yuan Z & Shields AJ. Quantum key distribution using in-line highly birefringent interferometers. Appl. Phys. Lett. 2018; 113, 031107, DOI: 10.1063/1.5036827

Mavromatis A, Ntavou F, Hugues Salas E, Kanellos G, Nejabati R & Simeonidou D. Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient Software-Defined Internet of Things. In Proceedings of 44th European Conference on Optical Communication-ECOC 2018, Rome, Italy, 23-27 Sept. 2018 DOI: 10.1109/ECOC.2018.8535267

Mazzarella L, R. J. Donaldson, R. J. Collins, U. Zanforlin, G. Tatsi, G. S. Buller, J. Jeffers. Quantum state comparison amplifier with feedforward state correction. Proc. SPIE 10674, Quantum Technologies 2018, 106741D (21 May 2018) DOI: 10.1117/12.2307818; <https://doi.org/10.1117/12.2307818>

Mukherjee S, Chandrasekharan HK, Öhberg P, Goldman N & Thomson RR. State-recycling and time-resolved imaging in topological photonic lattices. Nature Communications 2018; 9: 4209. DOI: 10.17861/490f2eff-e1a8-45d0-846d-3444b42af3f1

Mukherjee S, Di Liberto M, Öhberg P, Thomson RR & Goldman N. Experimental Observation of Aharonov-Bohm Cages in Photonic Lattices. Phys. Rev. Lett. 2018; 121:075502 DOI: 10.1103/PhysRevLett.121.075502

Papanastasiou P, Lupo C, Weedbrook C & Pirandola S. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels. Phys. Rev. A 2018; 98: 012340 DOI: 10.1103/PhysRevA.98.012340

Papanastasiou P, Ottaviani C & Pirandola S. Gaussian one-way thermal quantum cryptography with finite-size effects. Phys. Rev. A 2018; 98, 032314 DOI: 10.1103/PhysRevA.98.032314

Pereira J, Pirandola S. Hacking Alice's box in continuous-variable quantum key distribution. Phys. Rev. A 2018; 98, 062319 DOI: 10.1103/PhysRevA.98.062319

Pirandola S, Bardhan BR, Gehring T, Weedbrook C & Lloyd S. Advances in photonic quantum sensing. Nature Photonics 2018; 12:724–733 DOI: 10.1038/s41566-018-0301-6

Pirandola S, Braunstein SL, Laurenza R, Ottaviani C, Cope TPW, Spedalieri G & Banchi L. Theory of channel simulation and bounds for private communication. Quantum Science and Technology 2018; 3: 3 DOI: 10.1088/2058-9565/aac394

Qin H, Kumar R, Makarov V & Alléaume R. Homodyne detector blinding attack in continuous-variable quantum key distribution. Phys. Rev. A 2018; 98: 012312 DOI: 10.1103/PhysRevA.98.012312

Raffaelli F, Sibson P, Kennard JE, Mahler DH, Thompson MG & Matthews JCF. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip. Opt. Express 2018; 26: 19730-19741. DOI: 10.1364/OE.26.019730

Scerri D, Malein RNE, Gerardot BD & Gauger EM. Frequency-encoded linear cluster states with coherent Raman photons. Physical Review A 2018; 98 DOI: 10.1103/PhysRevA.98.022318

Spedalieri G, Pirandola S & Braunstein SL. Discrimination of discord in separable Gaussian states. Proc. SPIE 10771, Quantum Communications and Quantum Imaging XVI, 1077119 (18 September 2018) DOI: 10.1117/12.2320311

Tang X, Wonfor A, Kumar R, Penty RV & White IH. Quantum-Safe Metro Network With Low-Latency Reconfigurable Quantum Key Distribution. Journal of Lightwave Technology 2018; 36:22, pp. 5230-5236. DOI: 10.1109/JLT.2018.2870823

Vaquero-Stainer A, Kirkwood RA, Burenkov V, Chunnilall CJ, Sinclair AG, Hart A, Semenenko H, Sibson P, Erven C, Thompson MG. Measurements towards providing security assurance for a chip-scale QKD system. Proc. SPIE 10674, Quantum Technologies 2018, 106741A (21 May 2018) DOI: 10.1117/12.2307409

Wonfor A, Qin H, Kumar R, Tang X, Dynes JF, Shields AJ, Penty RV & White IH. Field trial of a QKD and high-speed classical data hybrid metropolitan network. Proc. SPIE 10559, Broadband Access Communication Technologies XII, 1055907 (20 March 2018) DOI: 10.1117/12.2290544

Zhou H, Zeng P, Razavi M & Ma X. Randomness quantification of coherent detection. Phys. Rev. A 2018; 98: 042321 DOI: 10.1103/PhysRevA.98.042321

Papers submitted for peer review

Albrecht MR, Massimo J, Paterson KG & Somorovsky J. Prime and Prejudice: Primality Testing Under Adversarial Conditions. Cryptology ePrint Archive: ia.cr/2018/749

Ashur T, Eichlseder M, Lauridsen MM, Leurent G, Minaud B,

Rotella Y, Sasaki Y & Viguier B. Cryptanalysis of MORUS\*. Cryptology ePrint Archive: ia.cr/2018/464

Bahrani S, Elmabrok O, Lorenzo GC & Razavi M. Wavelength Assignment in Quantum Access Networks with Hybrid Wireless-Fiber Links. arXiv:1810.01693

Brotons-Gisbert M, Branny A, Kumar S, Picard R, Proux R, Gray M, Burch KS, Watanabe K, Taniguchi T, Gerardot BD. Coulomb blockade in an atomically thin quantum dot strongly coupled to a tunable Fermi reservoir. arXiv:1810.02855

Brown PJ, Ragy S & Colbeck R. An adaptive framework for quantum-secure device-independent randomness expansion. arXiv:1810.13346

Cope TPW, Colbeck R. New Bell Inequalities From No-Signalling Distributions. arXiv:1812.10017

Gehring T, Lupo C, Kordts A, Solar Nikolic D, Jain N, Pedersen TB, Pirandola S & Andersen UL. 8 GBit/s real-time quantum random number generator with non-iid sample. arXiv:1812.05377

Ghalaii M, Ottaviani C, Kumar R, Pirandola S & Razavi M. Long-distance continuous-variable quantum key distribution with quantum scissors. arXiv:1808.01617

Huang Z, Macchiavello C, Maccone L & Kok P. Loss-tolerant and ancilla-assisted Gaussian state quantum metrology. arXiv:1811.10554

Kent A. Summonable Supermoney: virtual tokens for a relativistic economy. arXiv:1806.05884

Kent A. Summoning, No-Signaling and Relativistic Bit Commitments. arXiv:1804.05246

Kent A. Unconstrained Summoning. arXiv:1806.01736

Laurenza R, Tserkis S, Braunstein SL, Ralph TC & Pirandola S. Tight finite-resource bounds for private communication over Gaussian channels. arXiv:1808.00608

Ottaviani C, Woolley MJ, Erementchouk M, Federici JF, Mazumder P, Pirandola S & Weedbrook C. Terahertz quantum cryptography. arXiv:1805.03514

Pirandola S, Bardhan BR, Gehring T, Weedbrook C, Lloyd S. Advances in Photonic Quantum Sensing. arXiv:1811.01969

Pirandola S, Laurenza R & Banchi L. Conditional channel simulation. arXiv:1807.00784

Potoček V, Reynolds AP, Fedrizzi A & Corne DW. Multi-objective evolutionary algorithms for quantum circuit discovery. arXiv:1812.04458

Sassermann M, Vörös Z, Razavi M, Langbein W, Weihs G. Quantum statistics of polariton parametric interactions. arXiv:1808.01127

Vinay SE, Kok P. Statistical analysis of quantum entangled network generation. arXiv:1808.09774

Xiang ZH, Huwer J, Stevenson RM, Skiba-Szymanska J, Ward MB, Farrer I, Ritchie DA, Shields AJ. Long-term transmission of entangled photons from single quantum dot over deployed fiber. arXiv:1807.10690

Scientific presentations at conferences and workshops

Alsina D & Razavi M. “Quantum repeaters with optimal encoding from absolutely maximally entangled states”. Poster presentation at QCrypt 2018, Shanghai, China, Aug 2018

Bahrani S, Elmabrok O, Currás Lorenzo G & Razavi M. “Integrating quantum and classical networks at core and access levels”. Keynote speech at International Symposium on Telecommunication Technologies 2018, Tehran, Iran, 17-19 December 2018

Bahrani S, Elmabrok O, Curras Lorenzo G & Razavi M. “Finite-Key Effects in Quantum Access Networks with Wireless Links”. Contributed talk at IEEE GLOBECOM, workshop on Quantum Communications and Information Technology, Abu Dhabi, 9-13 December 2018

Brown P, Ragy S & Colbeck R. “An adaptive framework for quantum-secure device-independent randomness expansion”. Poster presentation at QCrypt 2018, Shanghai, China, 27-31 August 2018

Brown P. “Feasibility of device-independent randomness expansion”. Contributed talk, Quantum Roundabout, Nottingham, 11th - 13th July 2018

Brown P. “Feasibiligy of device-independent randomness expansion”. Contributed talk, Q-Turn : changing paradigms in quantum science, 26th - 30th November 2018, Florianópolis, Brazil

Chun H, Lowndes D & Choi I. “Miniaturised Hand-held Quantum Key Distribution System with Tracking Capability”. Poster presentation at QCrypt 2018, Shanghai, China, 27- 31 August 2018

Chunnilall CJ, Hart A, Kirkwood R, Semenenko H, Sibson P. Measurements towards providing security assurance for a chipscale QKD transmitter. Contributed talk at SPIE Photonics Europe, Strasbourg, France, 22-26 April 2018

Collins RJ, Donaldson RJ & Buller GS. Progress in experimental quantum digital signatures. Invited presentation at SPIE Optical Engineering + Applications 2018 - San Diego, United States, 19-23 August 2018

Curras Lorenzo G, Razavi M. “Finite-key analysis for memory-assisted decoy-state quantum key distribution”. Poster presentation at QCrypt 2018, Shanghai, China, 27-31 August 2018

Donaldson R. Wide-angle receiver for long-distance free-space quantum key distribution. Contributed talk at Photon 18, 3-6 September 2018, Birmingham

Donaldson R. Wide-angle receiver for long-distance free-space quantum key distribution. Contributed talk at Quantum Photonic Technologies for Space, 8-10th October, Bern Switzerland

Donaldson R, Mazzarella L, Collins R, Zanforlin U, Jeffers J & Buller G. Quantum optical state comparison amplification of coherent states. Contributed talk at SPIE Photonics Europe, Strasbourg, France, 22-26 April 2018

Duan X, Edwards T, Kumar R, Griesser H, Straw A, Wonfor A, White C, Lord A & Spiller T. “Hybrid Manager for QKD Network”. Poster presentation at QCrypt 2018, Shanghai, China, 27–31 August 2018

Dynes JF, Tam WWS, Sharpe AW, Lucamarini M, Plews A, Yuan ZL, Takahashi R, Cho JY, Dixon AR, Tanizawa Y, Wonfor A, Penty RV & Shields AJ. “High speed quantum key distribution in a metropolitan network”, Contributed talk at Photonics Europe, Strasbourg, France, 22 - 26 April 2018

Elmabrok O, Bahrani S, Curras Lorenzo G & Razavi M. “Finite-Key Analysis for Quantum-Classical Access Networks with Hybrid Links”. Poster presentation at QCrypt 2018, Shanghai, China, 27-31 August 2018

Erven, C. IEEE IPC 2018, Reston, Virginia https://ieee-ipc.org/ Oct 2018. “Integrated Quantum Cryptography: A new tool in the encryption tool chest” (invited talk)

Gerardot BD. Coulomb blockade in an atomically thin quantum dot strongly coupled to a Fermi sea. Invited talk at International Conference on Nonlinear Optics and Excitation Kinetics in Semiconductors (NOEKS 14), 23 - 27 September 2018, Berlin, Germany

Gerardot BD. Charge-tunable quantum dots in monolayer WSe2. Invited talk at Frontiers in Optics, Washington DC, 16-20 September 2018

Gerardot BD. Coulomb blockade in atomically thin quantum dots. Invited talk at 6th Engineering of Quantum Emitter Properties, Rome, Italy, 5-7 December 2018

Gerardot BD. Atomically thin quantum dots in charge-tunable devices. Invited talk at Smart NanoMaterials, Paris, France, 10-13 December 2018

Ghesquiere A, Varcoe B. “Generating secrecy from the act of secrecy”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018.

Gong Y, Kumar R, Wonfor A, Penty R & White I. “Quantum alarm: a novel approach to monitor the physical security of optical transport networks”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Hart A, Semenenko H, Frick S, Erven C, Lowndes D, Sibson P, Thompson M & Rarity J. “Small Form Factor, Low Cost Electronics for Chip Scale and Handheld Quantum Key Distribution Systems”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Huang Z. Noise-dependent optimal strategies for quantum metrology. Contributed talk at Photon 2018, Birmingham, 3-6 September 2018

Koong ZX. Poster presentation at 6th International Workshop on Engineering of Quantum Emitter Properties, Rome, 5-7 December 2018

Kumar R, Wonfor A, Penty R & White I. “Experimental Demonstration of Simultaneous Quantum and Classical Coherent Communication using a Single Wavelength Channel”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Lowndes D. Quantum key distribution for nanosatellite-to ground application. Contributed talk at Photon 2018, Birmingham, 3-6 September 2018

Mavromatis A, Ntavou F, Hugues Salas E, Kanellos GT, Nejabati R & Simeonidou D. Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient Software-Defined Internet of Things. 2018 European Conference on Optical Communication (ECOC), Rome, 2018, pp. 1-3. DOI: 10.1109/ECOC.2018.8535267

Mazzarella L, Donaldson R, Collins R, Zanforlin U, Tatsi G, Buller G & Jeffers J. “Hall Rhin Quantum state comparison amplifier with feedforward state correction”. Poster presentation at SPIE Photonics Europe, Strasbourg, France, 22-26 April 2018

Mazzarella L, Donaldson R, Collins R, Zanforlin U, Tatsi G, Buller G & Jeffers J. “Quantum state comparison amplifier with feedforward state correction”. Poster presentation at SPIE Photonics Europe, Strasbourg, France, 22-26 April 2018

Mazzarella L, Jeffers J. “A Learning Scheme with Coherent State Amplification”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Mazzarella L, Donaldson RJ, Collins RJ, Zanforlin U, Canning DW, Tatsi G, Buller G & Jeffers J. A learning scheme with coherent state amplification. Contributed talk at SPIE Conference: Defence and Security Sensing, Data and Signal Analysis, Quantum Science and Optical Technologies for Advanced Security and Defence Systems, Berlin, Germany, 10-13 September 2018

Oi. D. “Space Quantum Communications”. Invited talk at Gravity in the Lab Workshop, Benasque, Spain, 29 July – 10 August 2018

Oi D. “Quantum Research CubeSat”. Invited talk at From Quantum to KOSMOS - Optical Quantum Technologies for Small Satellites workshop, Berlin, Germany, 12 – 14 September 2018

Ou Y, Hugues-Salas E, Ntavou F, Wang R, Bi Y, Yan SY, Kanellos G, Nejabati R & Simeonidou D. Field-Trial of Machine Learning-Assisted Quantum Key Distribution (QKD) Networking with SDN. Invited talk at ECOC 2018, 44th European Conference on Optical Communication, Rome, Italy, 23-27 September 2018

Penty R. “Quantum Communications”. Contributed talk at Cambridge-Tsinghua Engineering Forum, Cambridge, 2 Oct 2018

Pirandola S. Converse bounds for private communication over bosonic Gaussian channels. Invited presentation at SPIE Optical Engineering + Applications, San Diego, United States, 19-23 August 2018

Price A, Rarity J & Erven C. “Implementing Hybrid Quantum-Postquantum Security in a Prototype Network”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Ragy S, Brown P & Colbeck R. “Feasibility of device-independent randomness expansion”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Rambach M. Poster presentation at 6th International Workshop on Engineering of Quantum Emitter Properties, Rome, 5-7 December 2018

Rarity J. Quantum Communications Technologies. Invited talk at Health of Photonics IOP Workshop, London, 16 May 2018

Razavi M. “Quantum communications at local and global scales”. Keynote speech at IEEE Globecom, workshop on Quantum Communications and Information Technology, Abu Dhabi, United Arab Emirates, 9-13 December 2018

Razavi M. “Quantum Networks: Opportunities and Challenges”. Invited tutorial at International Symposium on Telecommunication Technologies 2018, Tehran, Iran, 17-19 December 2018

Ren S, Kumar R, Wonfor A, Tang X, Penty R & White I. Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise. Journal of the Optical Society of America B 2018; Doc. ID 347079

Semenenko H, Sibson P, Erven C & Thompson M. “Integrated Photonic Devices for Measurement-Device-Independent Quantum Key Distribution”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Spiller T. Quantum (Communications) Technologies. Invited talk at the Department of International Trade, UK Government, London, 8 October 2018

Spiller T. Quantum Technologies and Their Implication for Cyber Security. Invited keynote address, Cyber Security and Quantum Computing Symposium, Malvern Festival of Innovation, Great Malvern, 11 October 2018

Spiller T. Quantum Technologies and their implications for Security. Invited talk at Network Rail meeting (Future Communications & Positioning Systems Advisory Group), London, 6 November 2018

Spiller T. Quantum Communications Technologies. Invited talk at special Quantum Communications session ahead of evening reception at Canada House organised by Innovate UK to celebrate the arrival of Canadian quantum delegation in the UK, London, 8 November 2018

Spiller T. Participation in round table discussion as part of CSaP Policy Workshop: Future threats and challenges of quantum technologies, Centre for Science and Policy, Cambridge, 4 December 2018

Tadza N, Kumar R, Wonfor A, Penty R & White I. “Adaptive Forward Error Correcting Design for Faster PostProcessing in Practical CV-QKD systems”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018.

Tadza N, Kumar R, Wonfor A, Penty R & White I. “Equalization Technique of Multiple Input Multiple Output (MIMO) Methods in Quantum Coherent Communications”. Poster presentation at QCrypt 2018, Shanghai, China, 27 – 31 August 2018

Tang X, Kumar R, Cunningham D, Wonfor A, Penty R & White I. “Inter-Symbol-Interference Reduction in Continuous Variable QKD Using Equalization”. Contributed talk at 2018 IEEE Globecom, Workshop on Quantum Communications and Information Technology, Abu Dhabi, United Arab Emirates, 9-13 December 2018

White C. Quantum Key Distribution in Real Networks. Contributed talk at Photon 2018, Birmingham, 3-6 September 2018

### Selected Media Coverage

“Quantum Outlook 2019”, by David Shaw, posted on 17 December 2018 on factbasedinsight.com website (incl. references to the Hub’s UK Quantum Network): <https://www.factbasedinsight.com/quantum-outlook-2019/>

“What to expect from the budding quantum industries”, by Rhys Lewis, posted on 12 December 2018 on The Engineer website (incl. reference to the work of the Hub on quantum secure

communications): <https://www.theengineer.co.uk/budding-quantum-industries/>

“The quantum Y2K moment”, by Margaret Harris, posted on 3 December 2018 on the Physics World website <https://physicsworld.com/a/the-quantum-y2k-moment/#>

“Quantum Technology for a Global Britain?”, by David Shaw, posted on 21 November 2018 on the factbasedinsight.com website (incl. references to Hub exhibits and work on the UKQN): <https://www.factbasedinsight.com/quantum-technology-for-a-global-britain/> (accessed 14/02/19)

“BT Is Harnessing The Power Of Quantum Mechanics To Root Out Fiber-Optic Hacks” by Parmy Olson, posted on 12 November 2018 on the Forbes website (incl. reference to the UKQN): <https://www.forbes.com/sites/parmyolson/2018/11/12/bt-is-harnessing-the-power-of-quantum-mechanics-to-root-out-fiber-optic-hacks/> (accessed 14/02/19)

“Quantum cryptography and the future of security”, posted on 8 October 2018 on Wired website: <https://www.wired.co.uk/preview/article/quantum-cryptography-and-the-future-of-security> (accessed 14/02/19)

“Academics in drive to make code from space unbreakable” by Ken Macdonald, posted on 19 September 2018 on the BBC news website: <https://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-45567496>

“Heriot-Watt University sets sights on communications technology breakthrough”, by Ken Symon, posted on 19 September 2018 on the Insider website: <https://www.insider.co.uk/news/heriot-watt-quantum-satellites-space-13266848>

“£80m funding to boost UK quantum technology programs”, by Matthew Peach, posted on 13 September 2018 on optics.org website: <http://optics.org/news/9/9/20>

“£80 million funding boost will help Scottish universities and businesses develop ‘quantum’ technology that could help save lives”, posted on 6 September 2018 on the gov.uk website: <https://www.gov.uk/government/news/80-million-funding-boost-will-help-scottish-universities-and-businesses-develop-quantum-technology-that-could-help-save-lives>

“Quantum-secured network ‘virtually un-hackable’”, by Patrick Nelson, posted on 12 July 2018 on the network world website: <https://www.networkworld.com/article/3289626/lan-wan/quantum-secured-network-virtually-un-hackable.html>

“Quantum encryption combats threat posed by quantum computing hacks” by Stephen Hardy, posted on 2 July 2018 on the Lightwave Online website: <https://www.lightwaveonline.com/articles/2018/07/quantum-encryption-combats-threat-posed-by-quantum-computing-hacks.html>

"A new quantum network has been launched in the UK and quantum initiatives are underway at telecom players SK Telecom, BT, Telefónica and Huawei – the world is starting to prepare in earnest for the advent of large scale quantum computers" by David Shaw, posted on 27 June 2018 on the Fact Based Insight website (incl. extensive references to the UKQN/Cambridge network launch): <https://www.factbasedinsight.com/the-world-is-waking-up-to-the-need-for-quantum-safe-cryptography/>

"Quantum-Based Technique for Protecting Secure Information from Hacks", posted on the AZOquantum website on 21 June 2018: <https://www.azoquantum.com/News.aspx?newsID=6093> (see also phys.org website: <https://phys.org/news/2018-06-quantum-hackers.html>)

"Networks carry quantum-encrypted data in UK and Spain", posted on optics.org website on 18 June 2018: <http://optics.org/news/9/6/26>

"Launching the first quantum network in the UK", posted on SciTech Europa website on 18 June 2018: <https://www.scitecheuropa.eu/launching-quantum-network-uk/87424/>

"Cambridge University has invented an unhackable computer network" by Abigail Rabbett, posted on 13 June 2018 on Cambridge News website: <https://www.cambridge-news.co.uk/news/cambridge-news/unhackable-computer-quantum-network-physics-14781007>

"Cambridge launches UK's first quantum network", posted on 14 June 2018 on Cambridge Network website: <https://www.cambridgenetwork.co.uk/news/cambridge-launches-uks-first-quantum-network/>

"ADVA FSP 3000 Powers UK's First Quantum Network", press release on the Cambridge quantum network launch, posted on 13 June 2018 on Newswire Today website: <https://www.newswiretoday.com/news/167216/ADVA-FSP-3000-Powers-UKs-First-Quantum-Network/>

"UK's first quantum network launched", press release on the Cambridge quantum network launch, posted on 13 June 2018 on the University of York website: <https://www.york.ac.uk/news-and-events/news/2018/research/uk-first-quantum-network-launched/>

"Cambridge launches UK's first quantum network", press release on the Cambridge quantum network launch posted on 13 June 2018 on the University of Cambridge website: [https://www.cam.ac.uk/research/news/cambridge-launches-uks-first-quantum-network?utm\\_source=Twitter&utm\\_campaign=YC&utm\\_medium=social](https://www.cam.ac.uk/research/news/cambridge-launches-uks-first-quantum-network?utm_source=Twitter&utm_campaign=YC&utm_medium=social)

"BT and partners take quantum leap towards 'ultra-secure' future networks", posted on Webwire website on 13 June 2018: <https://www.webwire.com/ViewPressRel.asp?ald=225212>

"BT announces 'unhackable' quantum-secured network", by Warwick Ashford, posted on 12 June 2018 on the Computer Weekly website: <https://www.computerweekly.com/news/252442910/BT-announces-unhackable-quantum-secured-network>

"UK scientists build 'unhackable' fibre network", posted on 12 June 2018 on telecompaper website: <https://www.telecompaper.com/news/uk-scientists-build-unhackable-fibre-network--1248128>

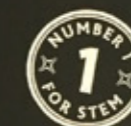
"BT and partners take quantum leap towards 'ultra-secure' future networks", press release on the Cambridge to AP link posted on 12 June 2018 on BT website: [https://www.btplc.com/News/?utm\\_source=BTBetterFuture#/pressreleases/bt-and-partners-take-quantum-leap-towards-ultra-secure-future-networks-2538664](https://www.btplc.com/News/?utm_source=BTBetterFuture#/pressreleases/bt-and-partners-take-quantum-leap-towards-ultra-secure-future-networks-2538664)

"Britain's first 'unhackable' internet network may solve quantum computing threat" by Margi Murphy posted on 12 June 2018 on The Telegraph website: <https://www.telegraph.co.uk/technology/2018/06/11/britains-first-unhackable-internet-network-may-solve-quantum/>

THE UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME  
[www.quantumcity.org.uk](http://www.quantumcity.org.uk)

# QUANTUM CITY

The next generation of quantum technologies is here. Learn about quantum science with partners from the UK National Quantum Technologies Programme and see what living in a "Quantum City" might be like.



Quantum  
technologies  
Exploring the future





**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](mailto:enquiries@quantumcommshub.net)

[www.quantumcommshub.net](http://www.quantumcommshub.net)

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