UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UK QUANTUM TECHNOLOGY HUB

FOR QUANTUM COMMUNICATIONS TECHNOLOGIES

ANNUAL REPORT

2018 2019

Contents

This report was developed with Memetic Communications Ltd; we are grateful to all the Hub colleagues, partners and associates who contributed by providing their input

EXECUTIVE SUMMARY:

Why do we need quantum communications and how close are we to delivering it?

The modern world runs on the rapid and secure transfer of information. Private emails, financial transactions, classified information, and health care records all involve the storage and transfer of highly sensitive data. Data is often said to be the new oil.

To ensure data is kept safe from those who would abuse it, the sender, usually referred to as Alice, encrypts the data before she sends it to the recipient, whom we call Bob. Conventional encryption jumbles up the data so that it is impossible to read, and an algorithm is used to generate a key to decrypt it – a long string of random numbers which only Alice and Bob have access to.

Cracking the algorithms and calculating the key would take our best computers years, but they are not impossible to crack. If quantum computers are successful, they may be able to break many public-key cryptosystems, possibly in a matter of hours. This would seriously compromise the integrity of the world's digital communications.

Quantum Communications provides a solution. Quantum key distribution (QKD) techniques physically encode the key into a string of photons – single particles of light – so it is impossible to crack mathematically. It is also impossible to copy or steal the key since the rules of quantum mechanics dictate that any observation will change the quantum state. So, if Bob receives a changed key, he knows there has been interference and simply asks Alice to resend.

Some predict that within twenty years quantum computers will be able to break essentially all public key schemes currently in use. It took almost two decades to deploy our modern cryptography infrastructure. We must therefore begin now to prepare our information security systems to be able to defend against quantum computing.

This is not just about protecting future data. Information encrypted with today's algorithms could be cracked by future quantum computers. In fact, governments, and no doubt many shadowy organisations, collect encrypted information in the hope of being able to crack it later. Even if quantum computing takes longer than expected, other techniques may arise which can foil our best algorithms. We would like our health records to stay secure over our lifetime, and governments want to keep military secrets under wraps for decades.

Recognising the importance of future information security, the UK Government funded the Quantum Communications Hub in 2014, as part of its original £270 million investment into a UK National Quantum Technologies Programme.

During this time, major progress has been made in developing quantum secure communications, as this report discusses. We have set up dedicated optical fibre networks in and between major cities, allowing quantum technologies to be tested on real world communications infrastructure. We have developed chip -scale quantum communications, paving the way for QKD to be integrated into small devices. And we have made progress on free space QKD, allowing encoded photons to be transmitted from handheld devices. Alongside these major leaps forward, we have made improvements in transmitter and receiver technology and the software and hardware frameworks needed for QKD to operate in commercially viable ways. All in all, this brings together the necessary elements for practical QKD demonstrations using commercial technology. But there is still work to do. Current technology needs further improvements in size, weight and power to be commercially viable for most applications. We want to explore more efficient ways of encoding information into photons. And if QKD is to become truly a global technology, we will need to be able to share keys around the world via satellites. As the technology nears mainstream commercial readiness, we will need to develop further standards and frameworks to ensure it can be effectively integrated into existing, and evolving, infrastructure.

To this end, the Government has extended the programme for a further five years, allowing us to deliver our vision of integrated quantum secured communications at all distance scales.

As we embark on this next stage, we need to further increase industry engagement. We know the science and we are close with much of the technology. But we need those who will commercialise and deploy it to understand what we are doing, and help us understand how quantum communications technology can help their organisations. We already work closely with companies like BT and ADVA who work on optical fibre networks, and Toshiba and ID Quantique who are developing QKD technology, all of whom are at the forefront of this emerging industry. But we need to hear from many others to ensure the outcomes of our work reflect the full range of industry challenges and needs.

Commercial success will require investment, foresight, technical understanding and long-term commitment. But QKD – potentially in partnership with new forms of mathematical cryptography – could form the basis of all future secure communications. Those dealing in secure information need to get ahead of the game. Those developing security products have a big business opportunity there for the taking.

Facts, figures and achievements

Selected Highlights

- Launched the UK Quantum Network, the UK's first test bed for quantum technologies, encompassing metropolitan and intercity optical fibre networks, allowing new quantum communications innovations to be tested and demonstrated on real world communication infrastructure.

- Hub Partner, the University of Bristol, fabricated and demonstrated the world's first chip-to-chip QKD device, allowing information to be exchanged using single photons of light in a quantum state on a scale that could eventually be integrated into mobile devices.

- Demonstrated free-space QKD between a handheld device and a wall mounted terminal, paving the way for wireless QKD.

- Developed prototype quantum secured approaches for digital signatures – allowing recipients to 'sign' digital messages to confirm they are genuine – and advanced various other "next generation" technologies, beyond basic QKD.

- Led outreach activities to promote understanding of quantum technologies and signpost career pathways in schools and amongst the general public.

To date, Hub investigators and researchers have published extensively across the whole spectrum of quantum communications, with over 180 peer-reviewed publications produced. Hub researchers have presented their work all over the world, with over 350 presentations and lectures delivered at major international conferences and specialist workshops.

Hub partner institutions kick-started Hub R&D by providing 20 PhD studentships, and a further 17 dedicated EPSRC Doctoral Training PhD studentships that have started working on Hub projects during Phase 1. Hub academic researchers have also collaborated extensively with Hub industrial partners on a range of projects both developing and implementing quantum communications.

Further details on these papers, presentations and projects can be found in the four Hub Annual Reports available via the Hub website[1]. Details on the papers, presentations, and other achievements for the final year will be available on the Hub website at the end of this collaborative project.

[1] https://www.quantumcommshub.net/resources/hub-publications/

How does quantum key distribution work?

QKD takes advantage of a fundamental aspect of quantum mechanics - that observing a system changes its quantum state.

The key is encoded into the quantum states of pulses of light. If a third party – Eve – tries to intercept and then measure or copy the quantum state in transit, they cannot avoid introducing changes, which can be detected when the key is received. This is due to the fundamental properties of particles, and so will not be circumvented by any future technologies, quantum or otherwise. Once the stream of quantum light signals has been received unchanged, the two communicating parties, Bob and Alice, know that they - and only they - have the key. They can then begin sending encrypted messages with confidence.

In one example of QKD, Alice sends out a string of single photons encoded in different ways to represent a bit, either a '1' or a '0'. Not all will arrive with Bob. Some will be lost in the fibre. Some may be stolen. That doesn't matter, the key is just created from the photons that are received. Bob uses an open channel to tell Alice – I got the photons in position 1,5,7, etc. Those are used to create the key and encrypt the information, which is then sent down separate channels.

If Eve steals the photons, they won't arrive and so won't form part of the key, and so are useless to her. If she measures them, then tries to send a duplicate, quantum physics guarantees that she will sometimes change the state of the photons, making it clear that they have been tampered with. It is crucial that Alice uses different ways to encode either a '1' or a '0', so that Eve doesn't know what's coming and cannot make any sort of measurement that will resolve perfectly between these four possibilities, leading to her unavoidable introduction of errors. So, no matter how hard she tries, it is impossible for Eve to steal the key.

In this example, Alice's transmitter is a pulsed photon source (the highly-attenuated output from a laser) which modulates the properties of the photons, eg the phase, to create a 1 or 0 state. A random number generator selects the state to be encoded, and also the way in which the encoding is done, to keep Eve guessing.

At Bob's end are single-photon detectors. For example, if phase-encoding is used, an interference measurement is performed, with detectors at each output port of the interferometer. The phase is determined from knowing which detector detects the photon. When Alice and Bob have accumulated a long string of data, they need to communicate and perform "post-processing" on these data to produce the final key(s). It does not matter if Eve listens in on all the subsequent communications – she still doesn't get a share of the key!

About the UK National Quantum Technologies Programme

The UK National Quantum Technologies Programme is a significant government investment in the commercialisation of quantum technologies aiming to grow the UK economy and - in the case of quantum communications - make the UK more resilient against cyber attacks.

The Quantum Communications Hub, led by the University of York, is part of a national network of four hubs, the others being NQIT (Quantum Computing, led by Oxford), QuantIC (Quantum Imaging, Glasgow), and Quantum Sensors and Metrology (Birmingham).

The £120m initiative, part of a £270m government investment in quantum technologies, is being delivered by the Engineering and Physical Science Research Council (EPSRC) and Innovate UK. Evolved versions of all four hubs will move forward in a second phase of the UK National Programme, from 1st December 2019.

[2] http://uknqt.epsrc.ac.uk/

UK progress and achievements towards commercial QKD

Whilst the physics of quantum communications has long been understood, the real challenge is developing it into technology that is deployable into real life situations.

Modern encrypted communications travel between millions of devices. Generating algorithmic keys can be easily done in existing devices with a small amount of processing power. But quantum keys require a physical system to produce, transport, and detect the quantum states of photons. Suitable QKD technology must therefore be developed which can be integrated into existing communications infrastructure.

A fully functioning quantum communications network must bring together multiple moving parts. The key would be generated by a transmitter (Alice); these are currently bulky units, but smaller versions are in the pipeline, and long term we expect to do QKD on microchips. It would be transmitted, wirelessly if necessary, to a node of a high-speed fibre network. The photons would then be passed securely along the fibre and transferred to the receiver (Bob) – possibly with further short-range free space transmission. Initially, these receivers will likely be at secure institutions such as banks. But as technology improves, it will be possible to integrate them into consumer end points such as laptops.

These various parts have all undergone significant improvements over the course of Phase 1 of the Quantum Technologies Programme.

Quantum communication networks

For Alice and Bob units to share keys with each other in a practical way, they need to be able to send encoded photons through fibre networks – just as with all telecommunications. Existing optical fibre networks are capable of transporting encoded photons, but need precise setups to ensure the keys are reliably transferred.

Over the course of the Phase 1, the Hub established the **UK Quantum Network (UKQN)**, connected metro-scale and long-distance optical fibre links for quantum communications. This provides a testbed, comparable to national communications infrastructure, on which companies can test and validate new quantum communications devices such as transmitters and receivers. The Network is made up of three distinct parts developed during Phase 1. Each has setups capable of transmitting quantum keys through dedicated channels, whilst also transmitting the encrypted data through other channels.

A Metropolitan Network has been set up at Cambridge University between three University buildings and Toshiba Research Europe Ltd (TREL). This uses a high-speed fibre network owned by the University. The short distances mean high-performance key rates above 2Mb/s and low-key losses - researchers have successfully transmitted 500Gb/s of encrypted data secured by quantum keys. The network is well characterised and suffers from little outside interference, allowing optimisation of transmitters and receivers, robust key management, and reliable measurements of the effects of classical data in parallel channels. TREL has used this network to test its research grade QKD technology under controlled conditions and so better understand commercial requirements.

The Cambridge metropolitan network was then extended to BT Adastral Park near Ipswich (UKQNtel - launched March 2019), thanks to a separate EPSRC grant to Hub partners. This link runs over 120km of rented Openreach fibre via three trusted nodes, which have been fitted with QKD racks to receive and re-transmit keys. Work has been done to optimise this process and establish how transmitters and receivers should talk to each other via nodes.

This allows partners and collaborators to explore how QKD can be delivered using only commercial equipment, and to design rules for commercial deployment. The Hub has worked with partners to explore how photon transmission can be integrated into classical telecommunications equipment and to understand how classical encryption systems can be modified to use QKD keys.

The final strand comprises of **long-distance links between Cambridge and Bristol via London**. These networks have been linked via the EPSRC UK National Dark Fibre Facility (NDFF – formerly NDFIS), with validated QKD equipment in locations along the link. The Cambridge to London link is 129km of fibre, we believe this to be the longest deployed QKD field-trial in the world without intermediate trusted nodes. This allows research into optimising key transmission over long distances and thereby avoiding the need for nodes, which in some cases could represent a weak point if not properly secured. The link has demonstrated a secure transmission key rate of 2.7kb/s per second even at that distance. So, if we were using our quantum keys for 256-bit AES encryption, this would allow over ten keys to be transmitted per second.

A further Metro Network has been setup at Bristol with four nodes. In support of the network operation, University of Bristol colleagues have demonstrated experimentally a secure optical network architecture that combines Network Function Virtualisation (NFV) orchestration and Software Defined Networking (SDN) control with QKD technology. These approaches could allow network hardware operations to be run as software, reducing cost and time in network deployment and maintenance, and creating dynamic networks which scale easily and rapidly to meet changing demands.

Tests over 18 months have demonstrated the various parts of the network are fit for purpose, with multiple demonstrations successfully transmitting keys through one channel and encrypted data through others in the same fibre.

The establishment of the UKQN as a national capability provides the UK's first testbed for QKD technologies to be tested and demonstrated under real world conditions, typical of standard communications networks. It will also facilitate exploration of new theoretical approaches, applications, protocols, standards and services, and implementation of next generation quantum communications, beyond QKD.

Chip-scale QKD

It is possible to perform QKD using bulky and expensive devices. But for QKD to become a mass market technology, it will eventually need to operate in consumer devices such as phones and laptops. A significant challenge for widespread QKD adoption is developing chip-scale devices – which overcome size, weight and power (SWaP) limitations and which can be integrated into electronic products.

Leveraging the expertise at the University of Bristol, we successfully fabricated and demonstrated the world's first chip-to-chip QKD. The system allows information to be exchanged using single photons of light in a quantum state, at microchip scale. All the photonics required (bar the single photon detectors on the Bob unit) are integrated onto single chips a few millimetres in size.

The Alice unit is indium phosphide, with on-chip lasers, photodiodes and phase modulators to control production of single photons. Performance is comparable to current state-of-the-art bulky commercial devices. This creates devices with low SWaP requirements, which will be much cheaper to mass-manufacture using existing semiconductor fabrication infrastructure. They can be simply integrated into existing server facilities and other electronics, rather than operating as separate units.

The Bob unit is a silicon oxynitride receiver chip. Scaling this to a level where it can go into a phone will be more challenging, since materials sensitive enough to detect single photons are bulky or require cooling apparatus. However, detector size is less of an immediate problem since early QKD would likely involve a secure end-user – eg a bank or government department – that could accommodate a bulkier detector. But the long-term goal is smaller detectors integrated onto chips so that phones and laptops can communicate directly with each other.

Following our world first chip-to-chip QKD demonstration, we shifted focus to the development of more advanced QKD devices aimed at solving some practical limitations of QKD. We fabricated and successfully demonstrated a range of integrated devices including high performance QKD transmitters in the silicon-on-insulator platform; we also continued to explore the incorporation of compactness with high performance quantum random number generators.

Wireless QKD

Whilst much of the journey of digital communications happens in underground fibre, at the user end information must often make short journeys between the end of the network and the user's device. Fibre can be plugged directly into secure terminals in some businesses, but for consumer applications, this final journey is usually made wirelessly.

There is therefore a need to transmit quantum keys through free space (i.e. without the need for fibre). The Hub explored **short-range, free-space QKD systems,** which could allow secure key sharing between a mobile device and a terminal.

To demonstrate the possibility, we developed a prototype system which allows a cheap handheld Alice device (the size of a chip and pin authenticator such as Barclays' PINSentry), which docks into a larger fixed Bob terminal (which we hope to eventually produce for around £2,000), analogous to an ATM. Such a system could be adopted to establish keys between a user and an institution, such as a bank. The actual use of the keys isn't quantum so the user could establish many keys at a single ATM visit using quantum secured technology, then use these keys to protect subsequent communications between the user and their bank online.

We developed the prototype Quantum ATM containing optical and electronic hardware for detecting the input light from the Alice transmitter, and performing the required processing.

Our first design used a card slot-inspired system that aligns the handheld Alice transmitter to Bob's detectors. Working with the University of Oxford led NQIT Hub, we then added hand tracking functionality and correction mechanisms, which removed the requirement for physical contact between transmitter and receiver. For now, the transmitter still needs to be physically placed in a cradle to create a reliable connection, but we are working on improving the tracking to allow "contactless QKD", comparable to contactless payments.

The system allows users to share a few hundred kilobits in approximately four seconds, enough to exchange secure keys. If receiver terminals are placed on nodes of a fibre optic quantum network, users could establish secure keys via relatively cheap handheld devices and wall mounted terminals (eg an ATM or within a government facility), then exchange them with each other across the high-speed network. These technologies will enable many-to-one, short range, quantum secured communications.

The natural progression of this technology is to develop free-space, wireless transmitters integrated into mobile phones. These could communicate over LiFi (similar to WiFi, but using light instead of radio waves) to a fixed device (similar to a router), and so connect into fixed fibre networks. This would truly bring QKD to the consumer.

Next Generation Quantum Communications Technologies

The Hub also explored new approaches, applications, protocols and services which go beyond current QKD technologies. These will address some existing limitations and open new markets for quantum communications beyond key distribution alone.

A significant success has been developing **quantum digital signatures (QDS)**. Just as a hand-written signature on a document gives some confidence that the document is genuine, digital messages also need to be signed to guarantee that they haven't been forged.

Hub researchers developed an efficient way to sign messages using shared secret keys, generated using current QKD technology, although digital signatures use a slightly different protocol to QKD. Over the programme, they have taken quantum secured digital signatures from laboratory demonstrations to implementation in dark fibre in metropolitan networks up to 90km distances. The length of the key needed for signing messages scales only as the logarithm of the length of the message, making "quantum signatures" a very attractive application for quantum key distribution.

QDS currently have limitations - only recipients who are part of the QKD network can verify messages – so current QDS would only be viable in high security applications. But we are also developing methods for "quantum signatures" that don't rely on shared secret keys, but instead utilise secret polariser settings. These have potential for more flexible and widespread application.

Advances have also been made on the underpinning technology for sharing quantum keys.

Work during Phase 1 developed a **probabilistic quantum amplifier**, which can amplify certain quantum states up to 20 times, a first step towards increasing the distance for some forms of QKD. A practical deployment would be directly in front of a receiver station, where it can amplify weak incoming signals to improve the key rate. With further development it could potentially be used as a trusted node in a long distance network, to increase the distance quantum signals could travel.

Because it is probabilistic, it does not amplify every signal, but a 'feedforward' system has been developed whereby missed pulses can be passed through other circuits, improving amplification success rate.

Progress has also been made using **quantum dots as single photon emitters**. These are made from layers of 2D semiconductor materials which could be integrated into lightweight circuits. They are early stage and currently require very low temperatures but have potential to be developed as practical devices in the future.

Considerable work has also been done, in the Hub and through partners, on **quantum random number generators** (QRNGs). Random numbers have widespread application, in all forms of cryptography and cryptanalysis, for numerical simulations and modelling, and, crucially, in the generation of quantum keys. Quantum random numbers have the very appealing feature that two identically constructed QRNGs will never produce identical random data strings, so it is therefore very important to assure that a QRNG really is quantum. Hub work has focussed on establishing assurance criteria and measurements for QRNGs, as well as on development of new QRNG hardware.

PARTNERSHIP RESOURCE:

Flexible funding to advance the industry

A unique and innovative feature of the Quantum Technology Hubs has been the Partnership Resource – £4 million of flexible funding to spend on initiatives that advance each Hub's goals, bring in new partners, and initiate new activities that were not in the original Hub portfolio.

This novel approach was taken in recognition that quantum technologies were so new that no-one could predict how they would develop. The unique funding mechanism gave the hubs flexibility to respond to market changes in real time and direct investment where it would be most valuable.

The Quantum Communications Hub has invited submissions to overcome current limitations of quantum technologies, reach new markets, enable adoption, or otherwise support commercialisation. Throughout Phase 1 it has made investments in feasibility studies; proofs of concept; preliminary developments; demonstrators, and well as our education and outreach programmes (See Below).

Highlights of funded projects include:

- A feasibility study examining optical technologies and manufacturing processes to assess UK capability to develop new optical ground receivers for satellite QKD
- Accreditation of outputs of Quantum Random Number Generators, through theoretical and experimental understanding, to move towards Assurance and Certification approaches
- Development of quantum-enabled secure tokens allowing access authentication for use in financial transactions and other networks where time is critical

A major benefit of this funding has been a series of activities and workshops that have brought together the quantum and space industry, the results of which paved the way for a significant Phase 2 work package on satellite quantum communications.

GLOBAL CONTEXT

The UK's investment in the National Quantum Technologies Programme was the first of its kind, and has been an inspiration to the world. Since the investment began, other countries have launched their own programmes, many taking inspiration from the UK. Significant programmes now exist in many countries, including Germany, Canada, the US, Japan, South Korea and Australia.

In 2018, the EU established the Quantum Flagship, a large-scale research and innovation initiative with an investment of €1bn over 10 years. The goal is to consolidate European scientific leadership and kick-start a competitive European industry in Quantum Technologies, including QKD, and to make Europe a dynamic and attractive region for research, business and investments in quantum.

The biggest and most advanced investor in quantum communications is China, which hosts a state funded 3,000km quantum communications network using Chinese equipment. It was also the first country to launch a QKD satellite, Micius, in 2016. This has proven to the world that satellite QKD is possible, and has also demonstrated entangled satellite QKD, albeit at very low-key rates for the moment.

In recent years, partly thanks to the Chinese work, there has been growing global interest in satellite QKD and the Hub Phase 2 will include a big focus on this area. The UK is also currently involved in a £10 million initiative with Singapore to build and fly a satellite QKD test bed.

Although there is increasing collaboration in research, there is also a focus on developing national capabilities. QKD is likely to be important to a country's national security and many governments may not want to rely on international supply chains. So, for all the advances, there are significant drives around the world, including in the UK, to develop world leading QKD technologies at home.

STANDARDS

Quantum communications products are already available, but there are not yet agreed standards for testing device performance, limiting confidence from end-users and potential uptake.

The ETSI Industry Specification Group on QKD (ETSI ISG-QKD) – which includes Hub partners Toshiba Research Europe Ltd (TREL) and the National Physical Laboratory (NPL), is working to provide the first documented standards for quantum communications[3].

The group is working on standards for characterising components of QKD systems developing measurement approaches to confirm that the physics has been implemented correctly to create quantum randomness in the generation of photon states. If it is not truly random then it could be cracked with mathematical expertise.

Beyond this, standards will need to be developed for the engineered devices to ensure there are no design flaws which could be exploited by hackers. The theoretically secure QKD model is built on assumptions about the hardware performance, so any differences between the model and the physical system could introduce vulnerabilities, called side-channels; these can be exploited by an attacker, so it is essential to ensure the hardware operates as intended. Longer term, standards will also need to extend to interoperability, to make sure different parts of the QKD system are compatible and can talk to each other.

The goal of these standards is to create measurement protocols for each part of the system which ensure products are validated in same way, and so create end user confidence that they do what they say on the tin. Ultimately this will require a defined assurance process and a network of accredited testing facilities which can provide the test and validation against agreed standards.

Without standards there would be no global networks for fibre-optic and mobile communications, or low-cost consumer electronics, which are based on reliable and widely available components from multiple suppliers. New standards are therefore required to integrate quantum communications into networks and to stimulate their commercialisation. Work is underway but there is still much to be done here.

OUTREACH AND ENGAGEMENT

Throughout the programme, the Hub has worked to engage industry, government and the wider community with the aim of generating excitement around quantum communications technology.

- We established and funded the Quantum Ambassadors[4] scheme for all four hubs, a two-year programme of class-based activities for A-level students and educators at 157 schools, increasing awareness and understanding of quantum technologies and signposting career pathways. The programme received very positive feedback, and a lighter weight GCSE version is being developed.
- Along with the other hubs and other programme stakeholders, we launched Quantum City[5], an engagement initiative promoting public understanding of the benefits of quantum technologies. This includes a public facing website explaining quantum technologies in plain language and outreach activities at many science festivals since 2018.
- The MacroPhoton demonstrator developed at Heriot-Watt University is proving to be an excellent "hands-on" public engagement and teaching tool, which uses the concept of photons scaled to the macroscale to demonstrate how quantum secure communications work. Future plans include its rollout through an app for potential use in schools.
- Along with the other hubs and stakeholders, we took part in an EPSRC commissioned public dialogue exercise on quantum technologies, aiming to introduce members of the public to the potential of these emerging technologies, and understand any concerns, aspirations and priorities relating to their future development and eventual deployment[6].

[3] https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution
[4] https://www.stem.org.uk/quantum-technologies
[5] https://quantumcity.org.uk
[6] https://epsrc.ukri.org/newsevents/pubs/epsrc-quantum-technologies-public-dialogue-full-report

How industry is benefitting from quantum communications

The ultimate beneficiaries will be businesses that rely on secure communications such as banks, defence organisations, and health services. But the immediate adopters of QKD will be technology companies that develop and sell QKD equipment, and telecommunications companies that implement QKD into their networks. Here we look at three companies exploring the commercial potential of QKD.

BT

BT is an active investor in QKD and a partner of the Hub. It is making a big drive into QKD, which it sees as a potentially revolutionary technology and one that could transform network security.

BT is developing systems based on commercial fibre, with extra channels used for sending the QKD key. Through partnerships with technology providers, BT hopes to offer complete managed network solutions. Medium term, it sees opportunities to sell Openreach access solutions with integrated QKD to provide highly secure communications across and between sites, or bespoke links such as those between a bank and a datacentre. But ultimately QKD could be at the heart of ubiquitous Quantum-Safe Cryptography that underpins the world's secure communications, so BT wants to be ahead of the game.

Andrew Lord, Senior Manager of Optical Research at BT, says: "There is a genuine fear in industry that quantum computers will upend global security protocols. Already we are seeing information being captured with the intention of hacking it once quantum computers reach maturity, so we have customers right now who are considering ways to future-proof their existing communications."

"But longer term, we believe that QKD will be an essential part of communications in a post quantum world, and BT wants to be at the heart of providing trusted communications long into the future, which is why we are investing in QKD now."

Toshiba Research Europe Ltd (TREL)

TREL's prototype Quantum Key Distribution (QKD) system delivers digital keys for cryptographic applications on fibre optic networks.

TREL are already making inroads into markets where data needs to stay confidential beyond the advent of quantum computers.

For example, they are working in Japan to protect human genome data. The genome data is collected and analysed by a Toshiba company and shared with a data bank in another part of city over a quantum secured link. Andrew Shields, Assistant Managing Director at Toshiba Research Europe, says: "People would like their genome to remain private for at least their lifetime, if not that of their descendants' also. With quantum computers possibly only a decade away, such information should be encrypted with quantum safe techniques now. QKD is an attractive solution for this challenge."

"Through working with the Hub and other partners we have been able to develop various applications as well as standards for network integration," says Shields. The Hub has also benefitted from TREL's world leading QKD equipment, which has been demonstrated to deliver the world record for the highest secure key rate, at 13Mb/s. Faster key rates are important as it means more secure keys can be formed or refreshed, speeding the processing of encrypted information.

Right now, the price of QKD technology means that it is mainly used in corporate networks. However, TREL are working in another project funded by Innovate UK to dramatically lower the size and cost of the technology using photonic chips. This will open many new markets and may even be used in home consumer applications in the coming years.

KETS Quantum

KETS has developed QKD technology on a chip, and is now working on commercialising it. Their technology can distribute secure keys from a chip the size of a fingernail, which can be easily manufactured in standard semiconductor foundries, and easily integrated into modern electronics. This allows more flexible and scalable key distribution than bulky units, and could bring practical QKD to many applications.

The founders of KETS were behind the chip-to-chip QKD demonstration at Bristol. Having built the prototype as part of a Hub funded programme, they spun out the company to focus on commercialisation. Seed funding in 2017 allowed them to develop the technology further and embark on trials alongside companies such as BT and Airbus. Access to the UKQN via the Hub allows them to test and validate products and the Hub consortium helps them access partners and collaborators.

With partners, they are gradually developing secure communication use cases in finance, oil & gas, critical infrastructure and defence. One such project is working with Airbus and others to demonstrate quantum secured communication between Unmanned Aerial Vehicles and ground stations.

The size of their technology gives it significant advantages. It can be easily integrated into other technologies, such as the hardware security modules that currently handle cryptographic keys, allowing equipment manufacturers to build new quantum secured products using KETS chips.

The technology is still evolving. Within 2-3 years, KETS hopes to offer multiple key transmitters on a single chip. Long term it hopes to integrate chips into handheld devices, and ultimately phones and laptops, which can establish secure communication channels using QKD, for example to improve the security of password apps.

Chris Erven, CEO and Co-Founder of KETS, says "We are seeing growing interest in the commercial potential of quantum. When we were seeking seed funding, just two years ago, we had to look far and wide to find someone who saw the potential and was willing to invest in what was seen as a very new technology area. But we are now seeing genuine commercial interest in quantum communications technologies and, as a result, increasing recognition from businesses and investors."

Where next for Quantum Communications?

In July 2019, £24M of new government funding was announced for the Quantum Communications Hub to continue the work for another five years, which will run directly on from the end of Phase 1 in November 2019. This is part of a renewed £94M investment in the four hubs with additional funds committed to a National Quantum Computing Centre, fellowships and training and skills (all part of £235M committed to quantum technologies in the 2018 autumn budget) and yet further investment provided by the Industrial Strategy Challenge Fund or ISCF.

The £24M funding will allow the Hub to deliver its vision of integrated quantum secured communications for business and consumers. During the next five years, the Hub aims to deliver a wide range of technologies based on the concept of Quantum Key Distribution (QKD) for the secure distribution of secret keys.

Significant progress has been made advancing transmitters and receivers, fibre networks, and the associated software and hardware. But there is still work to be done in these areas, and others, before we can create commercially viable quantum secured communications. Here we discuss the next set of challenges that we are addressing in Phase 2.

Build on Phase 1 successes in chip, wireless and QKD networks

There continue to be technical challenges around integrating QKD transmitters and receivers onto chips to make them truly handheld. Current Alice chips provide workable devices for commercial QKD, but further photonics challenges remain. Bob units on a chip still need further research and development. Fundamental research in Phase 2 will look at materials choices, new and improved sources and detectors, integration and other areas which could improve chip and indeed other QKD.

It is also important that we build national expertise and capability in sources and detectors. Secure communications technologies are subject to import/export controls and there may be restrictions on using foreign made components in technology used to protect critical national infrastructure and other high security applications. Successful commercialisation will depend on being able to develop QKD technologies in the UK.

A major next step is to increase our industry collaboration. Now the UKQN testbed is up and running, we plan to start working with more commercial partners to test commercial applications. We also hope to develop networks further north to support quantum communications companies in the region.

Digital signatures and secure tokens will also be developed to new levels, along with their implementations using current technologies. Other new protocols, beyond QKD, will also be explored to broaden the solution space that can be addressed with quantum security.

Continuous variable QKD

Current QKD is close to the point where advances will be limited by the technology. Single photon sources are not the only way of encoding information into light, there is merit in exploring other approaches and their technology limits.

Continuous variable QKD (CV-QKD) encodes information into light pulses, utilising both their amplitude and phase. CV-QKD thus requires continuous modulation and measurement of electromagnetic field properties, in contrast to the discrete encoding of information into photons in conventional QKD. CV-QKD source and receiver technology also has significant overlap with conventional communications technologies, albeit at lower light levels. This offers potential to make future QKD integration easier.

The Hub is exploring the development of commercially viable CV-QKD propositions. Recent demonstrations have shown CV key distribution at transmission distances up to 100km, high key rates, and network field deployment. However, the current lower clock rate and data processing complexities affect commercial interest in CV-QKD systems. Demonstration at higher clock rates with enhanced secure key rates are thus important objectives to pursue.

Entangled state QKD

With single photon QKD based on the highly-attenuated output from a laser, there is a small possibility that both Eve and Bob can receive a photon. This potentially leaks information to Eve, so it has to be accounted for in the post-processing that generates the final key. With entangled photons there is a no way for a third party to be entangled, so if Alice and Bob have shared entanglement – which they can test – they can use these quantum states to distil the key and be sure no one else can be entangled.

The physics for entangled QKD is solid but for now further work is required on entangled photon sources to transmit keys at rates suitable for everyday communications. A further driver for this approach is quantum repeaters, to extend the operating distances of fibre QKD. Quantum repeater technology involves "stretching out" high quality quantum entanglement over very long distances, but the technology is a way off, as quantum processing and quantum memories are required. Nonetheless, an aim of Phase 2 is to achieve significant headway towards entanglement distribution and quantum repeater stations.

Long distance and satellite QKD

Fibre works for communications up to a few hundred kilometres, but beyond this it becomes redundant due to the attenuation loss as photons propagate over long distances. Performing QKD over 'lit' fibre which is also carrying classical signals reduces the range further, due to noise or light pollution in the quantum channel.

Trusted nodes can detect keys then re-encode quantum states, offering a short-term answer to increasing operating distances, but introducing potential points of failure, which have to be physically secured.

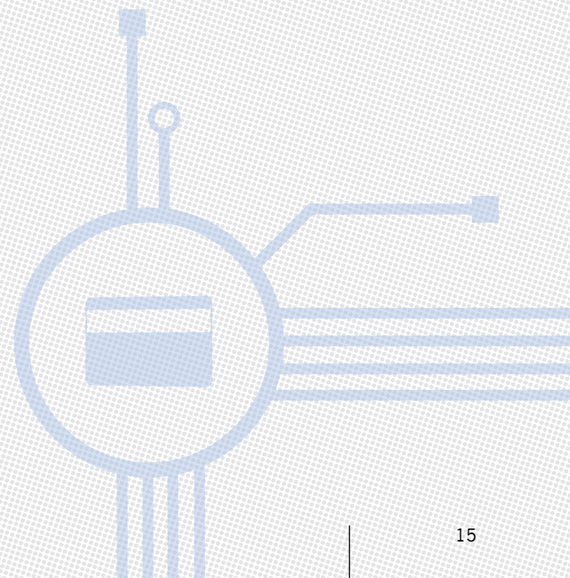
Regardless of advances in these technologies, we cannot install them every 100km across the Atlantic, and not everywhere has fibre. So global QKD will ultimately need to be achieved by distributing keys via satellites.

Satellite QKD is realistic as there is less photon loss and decoherence in the clear atmosphere and essentially none in space. A key Phase 2 project will put an Alice unit on a CubeSat – a small satellite suited for early investigations – with Bob connected to a receiver dish. The satellite will stay up for about a year to run the trial and gather data. In parallel with other satellite missions we will explore a number of options - including single photons based on weak laser pulses, continuous variables, and entangled photons. The objective is to determine the most applicable technologies for future commercial quantum communications in space.

Integration with Post-Quantum Cryptography

QKD is not the only word on secure encryption. A challenge is that it relies on the parties having an initial pre-shared private key which authenticates their first exchange. This works fine for static networks where Alice and Bob know each other and can be set up with pre-shared key – such as between a user and a bank. But it is a challenge for dynamic networks where Alice and Bob have never met, and such networks will still need a public key encryption mechanism.

Researchers are also working on post-quantum cryptography (PQC) – mathematical encryption and decryption algorithms that are immune to current quantum computer algorithms (e.g. Shor's algorithm) and conjectured to be immune to future developments. Overall future security will likely combine PQC and QKD. PQC could be used to share the initial key, which only needs to stay secure briefly in order to initiate QKD. Then QKD can do the rest, making the encrypted information permanently secure (PQC may evade current quantum computers but there is no guarantee that future innovations or mathematical insight will not crack it, whereas QKD keys will remain secure forever). Future research will bring together PQC and QKD communities to combine approaches and develop protocols to allow them to be interoperable.



Conclusion

The UK has always been good at the science and our research in quantum ranks with the best in the world. We are also now getting better at exploiting technology ideas and seeing them through to commercialisation.

The Quantum Communications Hub is a good example of this. We have supported the development ofthe fundamental science and helped demonstrate technological applications in the lab. But we have also engaged with industry throughout to direct research towards commercial needs, and created facilities for real world commercial testing of quantum communications technologies.

Our UKQN now provides a testbed for new quantum technologies, making the UK a great place to develop them. Having a place to test technologies will help their development, as well as proving their value to investors, service-providers and customers. We now aim for companies to use the UKQN for real world trials and fully formed QKD applications. Through such trials we would show we can adapt the network to a setup the customer needs, rather than simply proving what is technically possible.

We are also creating the support mechanisms for quantum to succeed, from supporting fundamental research, to developing standards that will put the industry on a clear footing, to nurturing the talent that will staff the quantum industry as it progresses. We have come a long way, and have a clear direction forward.

We are seeing the results of this play out as investment starts to grow in quantum technologies. A number of Hub partners and other major companies are investing in quantum technologies. The new Innovate UK Industrial Strategy Challenge Fund (ISCF) has seen considerable interest in quantum projects, with industry matching government funding. A number of investors are making long term investment in quantum technologies and the world's first quantum technologies focussed fund, Quantonation, was launched in 2018.

The next steps are further improvements to deliver commercially viable QKD, making the technology, smaller, faster, more robust and ensuring it integrates with existing infrastructure. More than ever, we now need engagement from industry and demonstrations of successful applications of QKD, using test facilities such as the UKQN to ensure end-user confidence. The ISCF provides a major strengthening of this exploitation pathway.

Early adopters are likely to be highly secure industries such as finance and defence, whose high value communications can be lucrative targets for sophisticated hackers, and who want information to stay secret over long time periods. But in the end, necessity may drive uptake of QKD. The advent of quantum computing will create the ability to quickly crack current algorithmic encryption codes. Post-quantum algorithms are being researched, but proof that these codes will always be 'uncrackable' is likely to be difficult. Future-proof secure systems will need to include QKD.

As long as momentum continues, the technology could be just a few years away. The tech push is there, we now need to create industry pull. We need to go out to industry, or for industry to come to us, to talk about their future security challenges and how to solve them so we can ensure our work on the remaining challenges of QKD is tailored to their eventual needs.

> We are hugely excited by the work of the Hub, and delighted that it has built a thriving community of outstanding researchers. The entrepreneurial outlook, the passion of students capturing the imagination of schoolchildren, and the innovation from algorithms, to chip based QKD, to the national quantum network, all show that the interplay between great science and great technology has so much to offer. Quite what futures quantum technologies will unlock is uncertain, but we can be very confident that this community will ensure that the UK will be at the forefront of both understanding and capitalising on the opportunities."
>
> *Martin Sadler OBE, Chair of the External Advisory Board*

The Partnership

ADVA Optical Networking
ArQit
Bristol City Council
BT
Cambridge Network
Craft Prospect
ETSI
Heriot-Watt University
IDQ — From Vision to Technology
KETS
National Cyber Security Centre — a part of GCHQ
NDFF — EPSRC National Dark Fibre Facility
NPL — National Physical Laboratory
NQIT — Networked Quantum Information Technologies
Oclaro
Quantic — The UK Quantum Technology Hub in Quantum Enhanced Imaging
RAL Space
Royal Holloway University of London
STEM Learning
Toshiba
TRL Technology — one step ahead
UK National Quantum Technology Hub — Sensors and Metrology
UK National Quantum Technologies Programme
UK Space Agency
University of Bristol
University of Cambridge
The University of Edinburgh
University of Glasgow
University of Leeds
University of Oxford
The University Of Sheffield.
University of Strathclyde Glasgow
University of York — Science Education Group
University of York

Schematic representation of the UKQN/UKQNtel


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


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


UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME
UK QUANTUM TECHNOLOGY HUB
FOR QUANTUM COMMUNICATIONS TECHNOLOGIES
ANNUAL REPORT
2016 2017


UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME
UK QUANTUM TECHNOLOGY HUB
FOR QUANTUM COMMUNICATIONS TECHNOLOGIES
ANNUAL REPORT
2017 2018

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

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

www.quantumcommshub.net

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