The EPSRC Quantum Communications Hub

Timothy P. Spiller*
Department of Physics, Information Centre, Market Square, University of York, York YO10 5DD, United Kingdom.

ABSTRACT

The Quantum Communications Hub is one of four Hubs comprising the research and development end of the UK National Quantum Technologies Programme. This programme is now in its second phase (2019-2024), following a successful first phase that ran 2014-2019. This Hub provides the UK focus for the quantum communications sector. This report provides a brief overview of the Hub's phase 1 developments, which mainly concentrated on progressing quantum key distribution (QKD) towards wider application. The grand vision of the phase 2 Hub is integrated secure quantum communications at all distance scales. For practicality and flexibility, this involves free-space communications at the shortest distance scales, fibre-based communications at the metropolitan and inter-city distance scales covered by current fibre networking, and free-space communications to support the very longest distances required for global reach. This report also outlines the ongoing Hub activities on short-range consumer QKD, fibre networking and long distance satellite-to-ground QKD. Brief discussion of the Hub work on new protocols, hybrid secure communications, standards and components is also given.

Keywords: quantum communications, quantum key distribution, security, quantum technologies

1. THE UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Quantum technologies are new information technologies (IT) in which one or more of the fundamental features of quantum physics – superposition, entanglement and the irreversible disturbance introduced by quantum measurement – play centre stage in their operation. Such technologies thus communicate, store and process information according to quantum laws, in contrast to the conventional (classical) laws that underpin the manipulation of information in conventional IT. Consequently, quantum technologies have the potential to provide advantage over their conventional counterparts, either by pushing performance to new limits, or enabling tasks that cannot be achieved at all with conventional IT. These new technologies are emerging across the whole IT spectrum, in communications, sensing, imaging, processing and computing. The theoretical ideas and potential for new quantum technologies began to emerge over forty years ago. The last couple of decades have seen massive advances in the control and manipulation of quantum light, matter and fabricated devices, in laboratories all over the world. These have led to demonstrations, prototypes and now quantum technologies starting to transition out of laboratories and into the real world. A hundred years of quantum science research is beginning to have direct technological impact.

In late 2013, the UK Government provisioned £270M of funding to establish a new UK National Quantum Technologies Programme[1] (UKNQTP). This funding was not additional funding for further basic research into quantum science, which is (still) supported through the Engineering and Physical Sciences Research Council (EPSRC) and other UK funding bodies and stakeholders. Rather, this new funding was for technology development – to turn the basic quantum science outputs into working technologies, turning the theoretical ideas and potential into reality. Formation of the UKNQTP took about a year and it began in late 2014, for an initial five-year phase. The technology foci of the UKNQTP are four Hubs[1], which between them cover the whole IT spectrum, of communications, sensing, imaging, processing and computing. Each Hub constitutes a very substantial and distributed collaborative activity, comprising about ten university partners, national laboratories and other stakeholders, and numerous companies. In addition to the four Hubs, the initial UKNQTP included a separate capital equipment programme, investment in the National Physical Laboratory (NPL), Centres for Doctoral Training, additional Training and Skills Hubs, and funding through Innovate UK to support industry-led projects towards commercialisation. Other UK stakeholders, such as the Defence Science and Technology Laboratory (DSTL) made parallel investments, to further augment the UKNQTP. The establishment of this new UK programme had significant impact worldwide, because of the magnitude of the initial investment but also because of the

*timothy.spiller@york.ac.uk

coordination and coherence across the multiple activities within. Programmes that have emerged elsewhere in the world since 2013 have clearly adopted aspects of the UK approach.

The initial fraction of the UKNQTP investment set aside for industry-led projects, supported through Innovate UK, was relatively modest. As these projects provide one of the "tech transfer" and commercialisation pathways for Hub outputs, there was clearly not a massive demand for such new disruptive technology projects on day one. Nevertheless, this initial Innovate UK scheme was very successful, demonstrated significant industry appetite and pull, and stimulated a much more substantial quantum technologies investment being made during phase 1 of the UKNQTP, through the Industrial Strategy Challenge Fund (ISCF). With the renewal of the UKNQTP for a second phase and taking into account all the parallel stakeholder investments and the very substantial industry investments into both ISCF projects and the Hubs, the total value of the UKNQTP over the ten-year period 2014-2024 has been estimated at around £1bn.

This report now focuses on the activities of one of four UK Quantum Technology Hubs, the Quantum Communications Hub[2], led by the University of York. The next section provides a brief overview of secure communications and the role played by quantum communications. The following two sections then outline the activities of the Hub during the first five-year phase of the UKNQTP and the planned activities for the second five-year phase.

2. QUANTUM-SAFE COMMUNICATIONS

Digital communications support every aspect of society today. Many of these need to be secure, because of the information they contain, or the transaction they are supporting, or the application they are facilitating. This current security is built on conventional cryptography. However, it is now widely appreciated that ongoing major advances in quantum computing provides a threat to these current cryptographic techniques. Quantum computers of sufficient size for such hacking do not yet exist; however, retrospective decryption is a very real threat and so critical data requiring long-term security should be protected now. Information which is encrypted with current cryptographic techniques can be intercepted, stored and then decrypted once large quantum computers become available. There is thus a clear and urgent need to make current cyber security "quantum-safe" – that is safe in a future world where all forms of quantum technology exist, including large quantum computers.

In simple terms, there are two forms of conventional cryptography: symmetric and asymmetric. The latter provides the current public-key infrastructure (PKI), widely used across the internet. Both cryptographic approaches utilise digital keys, at the transmitter ("Alice") and receiver ("Bob") ends of the communication. Also used is a known mathematical algorithm, for Alice to encrypt the data with her key and Bob to decrypt it with his key. In symmetric cryptography, Alice and Bob use the same key, which has to be kept secret from everyone else if their information is to remain secure, so they also need a mechanism to securely share this key. Asymmetric cryptography uses pairs of keys: Alice uses a public key ("public" because it is not a secret and available to everybody) to encrypt the data, whereas Bob uses a private key (secret, and known only to him) to decrypt. Current real-world internet and other communications often rely upon a combination of the two approaches: asymmetric PKI first, to establish shared secret keys that are then used symmetrically to secure the communications or transaction. This two-stage approach is clearly essential if Alice and Bob have never corresponded before. The threat is that current asymmetric PKI will be vulnerable to attack from a large quantum computer. This PKI has been built on so-called "one-way" mathematical functions, where it is easy to work out a public key from the corresponding private key, but essentially impossible (with existing technology) to work out the private key given only the corresponding public key. This is why PKI is so widely deployed today. However, it is known that a sizeable quantum computer running a quantum algorithm devised by Peter Shor[3] will be able to efficiently determine a private key from the corresponding public key. So the days are numbered for current PKI, deployed worldwide. Clearly the principle of this threat has been known since 1994; however, it is now being taken far more seriously because of quantum technological advances.

Two major approaches are being developed to counter this threat and to progress cyber security to being quantum-safe.

Quantum key distribution (QKD) systems enable Alice and Bob to generate shared symmetric keys, with the security of these keys underpinned physically because they were established using the communication of quantum light signals. The irreversible disturbance introduced by quantum measurement means that any potential eavesdropper is unable to gain information about the key without revealing their attempt to pry. Alice and Bob follow a predetermined protocol with their quantum communications and subsequent conventional communications (the latter of which can be assumed to be public and thus overheard by any eavesdropper) and can distil a final shared secret key, known only to them. The earliest protocol (BB84) was put forward by Charles Bennett and Gilles Brassard[4] in 1984, which illustrates the era when

concepts for quantum technologies were beginning to emerge. Variants of BB84 are used extensively today in QKD technologies. To avoid a person-in-the-middle attack, QKD does need Alice and Bob to have some initial shared secret (or "seed" key material), to provide authentication. However, two very important features of QKD are that: as long as they have a suitable seed, Alice and Bob can grow as much new key material as they want; and this new key material is (quantum) random and so cannot be deduced from the seed by anyone else. It is also important to stress that with QKD, the quantum aspect is in the key distribution (and any subsequent "top-ups" that Alice and Bob choose to make). Once distributed, the secret keys can be used for any application. Their use is not quantum, and requires no quantum technology.

Quantum-resistant, or post-quantum cryptography (PQC), comprises new mathematical encryption techniques that are immune to attack by Shor's algorithm and are thought to be resistant to other quantum algorithms that may be developed in the future. The National Institute of Standards and Technology (NIST) in the US is currently overseeing a worldwide process[5] for the establishment of a suite of new PQC techniques, which will be made available for widespread use.

Clearly, in order to address the vulnerability of current PKI and to do so in a flexible manner appropriate for the internet and mobile networks, it is essential to provide a quantum-safe solution for Alice and Bob who have never met, and to future proof this solution. A combination of PQC and QKD provides a very appealing solution. If Alice and Bob seed a QKD session with new, asymmetric PQC, the quantum keys they establish will remain secure even if the PQC were to be subsequently broken, by the emergence of a new quantum algorithm. So any secure transactions or communications reliant on these symmetric quantum keys will remain secure. With communications, the ultimate information-theoretic security can be achieved by using quantum keys in a one-time-pad arrangement. For more economical use of the key material, Alice and Bob can use their quantum keys to drive a symmetric conventional encryption system such as the Advanced Encryption Standard (AES). Such symmetric encryption is more resistant to quantum computer attack than current PKI.

3. PHASE 1 OF THE QUANTUM COMMUNICATIONS HUB

The vision of the Hub during phase 1 (2014-2019) was focused firmly on technology development, rather than basic research: "To develop new quantum communications technologies that will reach new markets, enabling widespread use and adoption in many scenarios – from government and commercial transactions through to consumers and the home." Given that QKD represented (and still does today) the most advanced of the various quantum communications technologies, delivery against the Hub vision was largely via three parallel activities designed to progress QKD towards much wider application and commercialisation. In addition, a fourth activity pursued next generation – beyond QKD – applications.

In order to bring QKD technology and applications towards the consumer market and hand-held devices, the Hub developed a very compact Alice transmitter, capable of eventual integration into future mobile phones and other portable devices, alongside a bulkier Bob receiver, which would deploy as a fixed unit. The scenario is that Bob would sit on the secure network of a bank, or employer, or the government, etc, enabling individuals and consumers to share secure keys with a whole range of institutions and service providers. Clearly in this model there are very many Alices, so this unit has to be very cheap, and rather fewer Bobs. During phase 1, the Hub delivered a consumer QKD prototype based on a card-slot-inspired system, in order to demonstrate suitable quantum transmission and operation. The system is now being further advanced in phase 2.

In order to address size, weight and power (SWaP) constraints for both Alice and Bob, and to push towards integration with conventional IT at the component and device level, there is clearly huge appeal to move quantum communications technologies on-chip. This will clearly also facilitate mass manufacture capability and thus progress these technologies towards much wider deployment and commercialisation. During phase 1, the Hub developed various chip-based quantum communications technologies and indeed Hub partner the University of Bristol underpinned demonstration of the world's first chip-to-chip QKD system. This activity continues to expand and evolve. A start-up company, KETS, has formed out of Bristol to exploit a range of chip-based quantum technologies and some of this work has also now progressed into a major ISCF project, taking further steps towards commercialisation.

In order to explore integration with conventional fibre communications, highlight possibilities for quantum secure applications over networks, and facilitate end-user engagement, the Hub established and now operates the UK's first quantum network, the UKQN. This is an R&D-focused network, comprising multi-(trusted)-node metropolitan scale quantum networks in the cities of Bristol and Cambridge, and utilising the National Dark Fibre Facility (NDFF) to

connect these. The UKQN inter-city connection has a length of 410km, over four links, with three intermediate trusted nodes and comprises four spans of 129, 112, 51 and 118 km, with the furthest distance between trusted nodes being 129 km. Launched in June 2018, Cambridge's metropolitan network includes four trusted nodes: the Electronic Engineering Division at West Cambridge, the Department of Engineering and the University's central network facility in the city centre, and Toshiba Research Europe Ltd (TREL) on the Cambridge Science Park. This network has demonstrated long term, stable performance. The metropolitan network in Bristol, launched in September 2019, has the capacity to provide QKD over the 5GUK test network using specially developed Open Source software. It has demonstrated the world's first quantum (QKD) secured Network Function Virtualisation (NFV) orchestration with Software Defined Networking (SDN) control.

The UKQN is augmented with the UKQNtel network, operational since March 2019. This utilises previously installed standard commercial grade optical fibre, thus providing a real-world environment for field trials of new quantum secure communications technologies and systems. The network extends over 125km, operates with commercial QKD equipment, contains three trusted nodes in BT Exchanges and, very importantly, demonstrates that quantum key signals can be sent in the same fibre as the high-rate data encrypted with quantum keys. Linking the large industrial complex at BT's Adastral Park to research facilities at Cambridge's Science Park, a node of the UKQN, the UKQNtel facilitates demonstrations of new quantum secure communication technologies and applications for direct user engagement.

Other developments by the Hub during phase 1 included: taking quantum signatures out of the laboratory and into real world demonstration, with a new protocol utilising standard QKD systems; and significantly increasing the key rate delivered by measurement-device-independent (MDI) QKD technology. A novel feature of all the UK Quantum Technology Hubs is a Partnership Resource (PR) element of the funding, unassigned at the start of the Hub and thus available for new projects during the Hub lifetime. During phase 1, the Quantum Communications Hub made strategic use of PR to bring in new partners and nurture a range of new projects. These included preliminary investigations and developments with: transferable quantum tokens; assurance of quantum random number generators (QRNGs); continuous variable (CV) QKD; quantum communications in space; Quantum Ambassadors. The latter is an educational project, on behalf of the whole UKNQTP and in partnership with the UK National STEM Learning Centre, to develop quantum technology educational material for schools, along with the "Ambassadors" to deliver the material. The success of the Hub PR programme during phase 1 is evidenced by the facts that numerous PR projects have led to either major new activities for the phase 2 Hub, or new ISCF projects (or both), alongside the Quantum Ambassadors project continuing into phase 2.

4. PHASE 2 OF THE QUANTUM COMMUNICATIONS HUB

Starting in December 2019, the grand vision of the Quantum Communications Hub[2] in phase 2 of the UKNQTP is: "Integrated secure quantum communications at all distance scales." Very short (a few metres) range communications for consumers and individuals, in both open spaces and rooms, require the convenience and flexibility of free-space transmission. Network access, through metropolitan scale and up to inter-city distance quantum communications clearly need to leverage off and integrate with conventional fibre network communications. The longest distance secure communications, across seas and country-to-country, require free-space ground-to-satellite or stratospheric (high altitude platform, HAP) quantum links. To pursue this vision, the Hub is leveraging strongly from phase 1 developments and has brought on board new expertise and partners[6], both academic and industrial. Given the broader set of objectives, the Hub is now pursuing eight parallel, interacting activities, with an additional three cross-cutting activities that address key matters relevant to a wide spectrum of technologies and services.

The UKQN, augmented with UKQNtel, is clearly an existing asset on which to build. Expansion of this network, to facilitate both new R&D and user engagement, is being undertaken in four different senses: physical – with new fibre links and interfacing to free-space at both the short and very long ranges; multi-party – beyond simple point-to-point; capability – beyond QKD to bring in other protocols and PQC; application – offering a wider range of use models and demonstration services. Clearly all this links to and will provide demonstration and exploitation capability for other Hub activities.

CV-QKD uses continuous quantum light signals, as opposed to single photons (or weak pulse approximations thereto), to distribute quantum keys. The phase and amplitude modulation used, along with detection techniques that generally utilise a local oscillator, mean that CV-QKD systems have overlap with conventional optical communications

technologies (albeit at much lower light levels), thus offering new scope for integration. The Hub is undertaking theoretical and experimental work to improve CV-QKD systems and demonstrate these in real world environments.

Entanglement distribution is a key enabler for various quantum communications. It can facilitate QKD (overcoming some limitations of non-entangled QKD systems), enable new multi-party protocols and provides an important step towards the ultimate goal of a future quantum internet. Hub partners are working to advance the capabilities of entanglement distribution, and have already demonstrated quantum conference key agreement and bipartite entanglement sharing for multiple users over networks.

Leveraging the phase 1 work, Hub researchers are now advancing the consumer QKD technology towards practical hand-held operation. This involves engineering of pointing and tracking capabilities, for the automatic establishment of short range free-space links. This will support practical hand-held consumer devices or in-room quantum "li-fi", with onward interfacing to fibre networks. Given the many-Alice, fewer-Bob nature of this technology sector, it provides a prime example for combining QKD with PQC. The Hub is therefore pursuing (computationally) "lightweight" PQC and its hardware implementation, suitable for integration into this hybrid solution.

A major addition to the Hub portfolio for phase 2 is the development of free-space quantum communications at the very longest distance scales. There is still much to investigate and optimise in terms of approaches, technologies and protocols, en route to practical and commercial communications. The Hub work involves three stages of delivery. First, the development of space-capable quantum payload sources, compatible quantum receiver technologies and protocols. Second, the testing, validation and engineering for space-qualification of these technologies, including modelling and detailed analysis. Finally, an in-orbit demonstration (IOD) – of satellite-to-ground QKD from a Hub CubeSat to a Hub ground station. All this work will provide essential input for future commercial pursuits and open up potential for both international collaboration with other missions and integration to terrestrial fibre networks.

Clearly the incentives of low SWaP and conventional IT integration provide a permanent driver towards putting quantum technologies on-chip. The Hub has already demonstrated successes and now has multiple "tech transfer" exploitation pathways (companies, ISCF or other commercially-focused projects) undertaking high technology readiness level (TRL) work. This enables Hub partners to now concentrate on key low TRL developments, such as on-chip implementations of MDI QKD and protocols beyond QKD, and new devices such as integrated ultra-low loss switches for quantum light level operation.

It is widely appreciated that, whilst extremely useful, key distribution doesn't cover the whole security solution space. Thus there is clearly demand for quantum protocols and their implementations beyond basic QKD. Hub researchers are pursuing a range of new protocols, including secure transferable tokens, position-based cryptography, signatures and multi-party interactions. These have the potential to feed into other Hub activities when practical implementations are designed. In addition, Hub work on QRNG assurance and certification is continuing, including new approaches based on device-independence.

In a rapidly changing political and economic landscape worldwide it is clearly important that new technology supply chains are robust. Particularly for secure communications systems, where import and export regulations can also impact. It is therefore desirable for the Hub to develop key component technologies – quantum sources for Alice and quantum detectors for Bob. Use of genuine single photons can remove some potential side-channel limitations, compared to quantum communications based on weak pulse approximations. The Hub is developing compact entangled sources to support space and other applications, and cavity-integrated quantum dot photon sources at telecom wavelengths for fibre applications. To support receiver technologies, the Hub is developing superconducting nanowire detectors for high efficiency and mid-infrared applications, alongside Ge-on-Si single-photon avalanche diode (SPAD) detectors for more flexible application and semiconductor integration.

The three cross-cutting Hub activities all relate to security – of devices, systems and end-to-end – which is clearly essential for delivery of the Hub vision. Led by NPL, the Hub is continuing to undertake metrology and calibration of technologies, contributing further to relevant standards through ETSI and other bodies. The Hub is also investigating a range of cryptographic and quantum primitives, and the integration of quantum and PQC technologies into practical solutions. The third activity comprises security analysis, vulnerability analysis and testing, plus the development of countermeasures – all from the perspective of providing practical and secure applications and services.

As was the case during phase 1, Hub delivery against all these objectives that contribute to the grand vision is relying crucially on strong collaboration between academic and industrial partners and UK national laboratories.

ACKNOWLEDGEMENTS

The phase 1 Quantum Communications Hub was supported by EPSRC grant EP/M013472/1 and the phase 2 Hub is supported by EPSRC grant EP/T001011/1.

REFERENCES

[1] http://uknqt.epsrc.ac.uk/
[2] https://www.quantumcommshub.net/
[3] Shor, P. W., "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press: 124–134 (1994). https://ieeexplore.ieee.org/document/365700
[4] Bennett, C. H. and Brassard, G. "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179 (1984). https://doi.org/10.1016/j.tcs.2014.05.025
[5] https://csrc.nist.gov/projects/post-quantum-cryptography
[6] https://www.quantumcommshub.net/partners/