Quantum Communications Technologies

NB - this is text version of a paper written by invitation of the RSI journal. For the fully formatted version, please view this document.

Background on quantum technologies

Quantum mechanics was developed and refined during the first half of the last century, as the branch of physics required to understand matter at the atomic, nuclear and fundamental particle levels, and to understand light at the level of single quanta, or photons. It has since proved to be an invaluable tool in understanding the building blocks of all the information technologies (IT) we use in the modern world, such as: electronic circuits that underpin computers and all the other devices we rely on every day; lasers and optoelectronic components that underpin communications technologies and numerous home, consumer and personal devices. Indeed, quantum mechanics has aided the repeated improvements of all these technologies to the state-of-the-art from which we benefit today.

The fundamental features of quantum physics, which determine how atoms and photons behave, run counter to our intuition and everyday experience. Quantum systems can be in multiple states at the same time – this is termed *superposition* (of states). Furthermore, quantum systems, even when separated by large distances, can be correlated more strongly than any correlations familiar to us – such systems are termed *entangled*. Finally, when any of us try to measure or interact with a quantum system to learn about what it is doing, we inevitably and irreversibly disturb it. This relationship between *disturbance and information gained* is fundamental. It is not something that we will overcome by building better measurement devices and probes in the future – it is built into Nature.

These fundamental features of quantum mechanics were appreciated in the early stages of its development. However, study of these features was viewed as a somewhat academic pursuit – undertaken only to understand the basis of this part of physics. They didn't affect our macroscopic and "classical" (meaning non-quantum) lives. Fifty years ago there was no inkling at all that these quantum behaviours would ever contribute to our daily lives. Even today, the electronic, optical and other components that comprise our conventional IT do not exhibit these counter-intuitive behaviours. However, things are now changing. Over the last few decades – initially just theoretically or abstractly, but increasingly now as actual prototype devices – it has been realised that these fundamental features of quantum physics can play centre stage in completely new technologies. These new "quantum technologies" have the potential to outperform our conventional IT, or even achieve some tasks impossible with our usual stuff. The benefits could arise across IT: in computing and processing, in sensing and imaging, and in communications.

When evaluating something with a conventional computer, in general it is fed with one of a very large number of possible inputs[1]. A quantum computer, that exhibits *superposition behaviour*, could be fed with all these inputs at the same time. So if the desired result is some property of all the possible outputs, there is the potential to compute this property with essentially just one run of the computer, rather than a very (exponentially) large number of runs. This vast speed-up could give advantage in a range of applications: cryptanalysis and solution to other mathematical problems; annealing and optimisation; simulations – from quantum chemistry through to financial modelling.

[1] More technically, if the input register comprises n bits there are 2^n possible inputs. This range of possible inputs grows rapidly in size – exponentially – as a function of n.

When imaging or measuring something with conventional light, or using lithography to define an electronic circuit for manufacture, there is a limit of resolution set by the light. If *entangled*, *or other forms of quantum light* are used, this resolution can be improved[2]. Indeed, in principle it can then be pushed all the way to that permitted by the *fundamental disturbance introduced by information gain*. This is the best that Nature permits – in effect imaging at the limit of Heisenberg's famous uncertainty principle. Analogous to the use of light for high-resolution imaging, technologies utilising the quantum behaviour of atoms can be used for high resolution sensing, for example to detect hidden objects, buried infrastructure, or sinkholes before they appear. Quantum light or atoms have widespread potential for applications across the imaging and sensing sectors.

Everyone – in government, business, health, education, and society as a whole – uses electronic information every day. We are all increasingly reliant on the security of our communications and other forms of digital transactions. This security can be effected by using keys for encryption and decryption, so the security is then determined by how securely the keys have been distributed. This is where quantum physics steps in. If the process of distributing keys is implemented with quantum light signals, anyone sneakily *attempting to gain information about the keys will necessarily disturb the light signals* as they do so. Thus Nature ensures that eavesdroppers cannot avoid being detected – in fact even if they try to use other quantum technologies to examine the light signals.

The UK National Quantum Technologies Programme

The UK has a very long and strong tradition in fundamental science. However, particularly in the second half of the last century, we also had something of a reputation for failing to exploit the science, with technologies and new businesses instead emerging elsewhere in the world. Over the last couple of decades, successive UK Governments have listened, appreciated these missed opportunities, and acted to prevent continued ball-dropping. This has covered many technology and business sectors, with new quantum technologies being one of the showcase examples.

In 2013, the UK Government provided £270M to support development of quantum technologies, building on the very solid base of UK excellence in quantum science. Thus the UK National Quantum Technologies Programme (UKNQTP) came into being, with an initial five-year Phase 1 of the Programme starting 1 December 2014. This broad Programme supports technology development through: four large collaborative Hubs (funded via the Engineering and Physical Sciences Research Council), focused on sensing, imaging, computing and communications; additional capital investment projects; a scheme of industry-led targeted projects (funded via Innovate UK); a new Quantum Metrology Institute at the National Physical Laboratory. The UKNQTP also supports skills and training development – another vital step if new industry is to emerge and flourish in the UK – through Centres for Doctoral Training along with focused Skills and Training Hubs. Given it is a technology rather than a science programme, industry plays a crucial role in the UKNQTP. In addition to leading Innovate UK projects, many UK companies are partners in and provide support to the Hubs. Adding to this, stakeholders such as DSTL contributing, through studentship and other schemes, results in a leveraged total investment for Phase 1 of the UKNQTP well above the £270M Government stake.

Earlier this year, a Phase 2 of the UKNQTP was established, through funding awards to four Hubs – with evolved portfolios but still covering the full spectrum of quantum technologies: sensing, imaging, computing and communications. Added to these is a new National Quantum Computing

[2] A very topical example in fundamental science is the use of (squeezed) quantum light to further enhance the resolution of the LIGO gravitational wave detector.

Centre, which will be a physical centre in a new building designed to bring together and exploit the UK's expertise in this sector. This is in contrast to the Hubs, each of which is a distributed collaboration that exploits the UK's relevant expertise where it is already established: in universities, national laboratories and companies all across the UK. The role of industry in Phase 2 of the UKNQTP is significantly expanded and enhanced. This is exactly what is required, as technologies progress from breadboard models, through prototypes, towards actual commercialisation, with applications and services based on these technologies developing in parallel. There is now a major quantum technology theme within the UK Industrial Strategy Challenge Fund (ISCF). Via Innovate UK, this is supporting major industry-led projects aimed at the commercialisation of quantum technologies and services. The integrated investment in Phase 2 of the UKNQTP is comparable to that in Phase 1, but with the crucial shift towards commercialisation and future wealth-creation.

Quantum Communications Technologies

To present a specific sector example, this article focuses on quantum communications[3]. As has already been noted, everyone worldwide is becoming increasingly reliant on the security of information and communications, in all aspects of our daily lives. The trouble is that current methods used for security are becoming ever more vulnerable. We know that encryption techniques[4] widely used today can be broken by a large and powerful quantum computer, when this gets built in the future. For information that is only required to be secure for a short time now, this threat is clearly just looming. However, for sensitive information that requires a long security "shelf-life", the threat is already here. Encrypted communications can be stored now and broken in the future, when the tools exist. Clearly new approaches to security are required.

Encryption and decryption methods are needed that are not vulnerable to quantum computer attack. One approach is to utilise shared keys – for encryption and decryption – and cryptographic techniques immune to such attack. Then the security is determined by the security of the key distribution mechanism. This is where the quantum technology comes in – it provides a secure method of quantum key distribution (QKD). To share a key, the basic idea is that the transmitter – usually called Alice – sends a long sequence of quantum light pulses to the receiver – usually called Bob. These may be sent down an optical fibre or through free space, whichever technology provides the best solution, but either way any adversary – usually called Eve – can only gain information on the transmitted light signals by measuring them in some way. Quantum physics dictates that Eve cannot avoid introducing disturbance to some of these signals through her measurements, so she cannot avoid exposing her eavesdropping[5]. Clearly Bob also has to measure the quantum light signals that he receives in order to establish a key shared with Alice. Nevertheless, the really clever thing with QKD is that Alice and Bob can afterwards identify a subset of shared data to keep. Without exposing the actual data values, they can identify the specific light signals that Bob should not have disturbed by his measurements. They can locate and correct errors in the data that they keep, and then mathematically compress it down to a final shared secret key. What's more, all these subsequent communications do not have to be encrypted (although they could be) – the security of the final key is not compromised even if Eve overhears all this discussion.

---

[3] Information on the UKNQTP and all the technology sectors and Hubs can be found in "Further Reading and Information".

[4] Public key cryptography, such as RSA or that based on elliptic curve algorithms.

[5] If instead of eavesdropping, Eve adopts a different kind of attack and simply blocks all the signals, this constitutes "denial of service", which clearly also exposes Eve being at work. In this scenario Alice and Bob would need a more involved network, instead of a single fibre or free space link, to progress.

Once Alice and Bob have secret shared key data, they can use this in a range of approaches. For secure communications the ultimate (information theoretically secure) would be one-time-pad encryption. A much more economical (with key) approach would be to use quantum keys to drive a system using the Advanced Encryption Standard (AES) – this approach is compatible with current high-speed telecommunications infrastructure. Other quantum key applications include single-use PINs, or passwords, or entry codes. Two important things to note are: (i) that almost certainly the key use will be once only to maintain security (and so afterwards used keys should be irreversibly deleted); (ii) the use of the keys is conventional, requiring no quantum technology. It is the distribution, or replenishment, of the keys that is quantum.

In parallel to the development of quantum communications, R&D is also being pursued with other forms of "quantum-safe" communications – secure against eavesdroppers or adversaries armed with arbitrarily powerful quantum computers or sensors working at the absolute quantum limit. One such direction is with new mathematical approaches, called post-quantum cryptography (PQC), which are known to be immune to current quantum computer algorithms and thought to be immune to any that might be developed in the future. It may well be that the most flexible and secure security in the future will incorporate both QKD and PQC. One example would be with authentication, in a dynamic and changing network scenario. For example, if a particular Alice wishes to correspond with a Bob she's never met before, they will have no previously shared key to support a QKD session. So PQC could provide this, with the security "shelf-life" of the PQC exchange only being needed until new key from QKD is generated.

The UK Quantum Communications Hub

Over the last five years the vision of the Quantum Communications Hub has been 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. To achieve this, our main effort has been to take proven and working concepts in QKD and to advance these towards commercialisation.

We have built a short-range, free-space QKD prototype, with the vision of Alice being in a phone and Bob being in a terminal. This would bring QKD security to consumers and individuals, for linking to their Bank, or employer, or NHS, or government. We have advanced putting both Alice and Bob on chips, to reduce size, weight and power demands, and support future mass-manufacture, to make the technology much more widely deployable. Hub partner the University of Bristol has spawned a start-up company KETS, to pursue such chip-scale quantum technologies. We have also built the UK's first fibre quantum network – the UKQN. This comprises metropolitan scale networks around the cities of Bristol and Cambridge, and links these using parts of the UK's National Dark Fibre Facility (NDFF). An extension has already been added – UKQNtel – between Cambridge and BT Research at Adastral Park near Ipswich, utilising additional UKNQTP capital funding and BT fibre. These quantum networks utilise standard telecoms fibre and provide testbeds for technologies and application development, whilst also acting as demonstrators for user engagement and generation of market pull for QKD. Key to the establishment of these networks has been strong collaboration with the technology companies ADVA, ID Quantique and Toshiba, and with the service-provider BT.

In addition to all the work on QKD, the Hub has also advanced other quantum communications technologies, beyond QKD and addressing other aspects of the "security space". We have taken the quantum analogues of digital signatures out of the laboratory to operation under real world conditions. We have advanced "next generation" QKD systems, which have fewer constraints on their hardware. The Hub is also progressing the assurance of quantum random number generators

(QRNGs). Random numbers are an essential consumable in many forms of cryptography, cryptanalysis, modelling and simulation, and genuine QRNGs have major appeal from their (quantum) guarantee of irreproducibility of random sequences. Hence the importance of assuring the "quantumness" of a QRNG.

International Perspective

The establishment of the UK National Quantum Technologies Programme in 2014 certainly generated attention worldwide. It was not just the very substantial investment from the UK Government, but equally the vision and coherence built into the programme: the focus on technology; the leverage of existing science and expertise; the collaboration between academia, industry, national laboratories and stakeholders; and the complementary skills and training activities. There were long-running R&D programmes linked to quantum technologies in various other countries, but the UKNQTP did stimulate some re-evaluation of investment and, perhaps more so, coordination. Today there are flourishing quantum technology programmes in many countries worldwide, for example China, Canada, the US, Germany, Japan, South Korea and Australia. There is no doubt that the UKNQTP also helped stimulate and shape the current Quantum Flagship, which is a €1bn investment over 10 years by the EU to advance quantum technologies across Europe.

The biggest current investor worldwide is China, with a fibre network connecting Beijing and Shanghai. China also launched the Micius satellite in 2016, which has demonstrated the future feasibility of QKD in space through various breakthrough experiments. Given the limitations of fibre for intercontinental distances, quantum communications in space will be needed for truly global reach.

The Future

Earlier in 2019 a Phase 2 of the UKNQTP was set in motion for the next five years. Within the Quantum Communications Hub we will be continuing our work on consumer QKD and chip-based technologies. We will be expanding and leveraging the UKQN to stimulate wider adoption of QKD. Crucial to widespread adoption are technology standards, so Hub partners will be continuing their vital metrology, calibration and standardisation work into Phase 2.

In addition to these evolutionary activities, the Hub is expanding its portfolio in a number of new directions. We will be advancing UK capability in the required quantum light emitter and detectors, to underpin all our technologies. We will be investigating new approaches to QKD and networking, based on entangled and other novel quantum states of light. We will also be advancing the very longest distance technologies, through a satellite-to-ground QKD demonstrator.

We will also be developing new quantum protocols, to broaden the scope of quantum communications beyond key distribution and its close cousins. In addition, we will be integrating QKD with PQC to exploit the best of both. Customers want solutions, not technologies they have to integrate. So for market pull we need to produce solutions.

Further Reading and Information

1. The UK National Quantum Technologies Programme: http://uknqt.epsrc.ac.uk/ ; Peter Knight and Ian Walmsley, Quantum Sci. Technol. **4** (2019) 040502, https://doi.org/10.1088/2058-9565/ab4346
2. The UK Government Blackett Review of Quantum Technologies: https://www.gov.uk/government/publications/quantum-technologies-blackett-review

3. The four Quantum Technology Hubs: http://www.quantumsensors.org/ ; https://quantic.ac.uk/ ; https://nqit.ox.ac.uk/ ; https://www.quantumcommshub.net/ .
4. The ETSI White Paper on the Implementation Security of Quantum Cryptography: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf .