Building a secure, quantum internet for the future: will the UK's science policy keep up?

Alex Koehler-Sidki, Department of Engineering, University of Cambridge

The digital world is changing fast; the computing power of today's smartphones outpaces that of supercomputers from just twenty-five years ago. We can video-call people on the opposite side of the globe, and we trust that our data are transmitted securely from one device to another. But, given this breathless speed of advancement, can we maintain our security in the coming decades? The use of quantum mechanics could be the answer. Is the UK's science policy up to it?

Ensuring our digital security has never been a more pressing issue. The WannaCry virus wreaked havoc on the NHS last year, Russia has been the subject of numerous hacking allegations, and, more broadly, businesses suffer losses of billions of pounds annually as a result of hacking. Yet, on the horizon, a more benign threat is appearing in the form of quantum computers. These computers promise to solve problems that are currently intractable by modern supercomputers, particularly when it comes to factorising very large numbers – a technique that serves as the foundation for much of modern-day encryption. This would mean that current encryption methods, which would take thousands of years to crack with a conventional computer, could be broken in just seconds by a hacker using a quantum computer.

Much of contemporary internet security rests on a technique known as 'key encryption'. In general, key encryption provides security by encoding information that is shared between a receiver and transmitter using a key. The lynchpin of this security system stems from the mathematical complexity of determining the key. Keys are typically very large numbers, containing prime factors. Current computers struggle to extract these prime factors as they rely on a brute force approach that tests all possible combinations of factors, one after another. As these keys become larger and larger, the work required to crack them increases exponentially, quickly reaching the order of thousands of years.

The advent of quantum computers, a time that could be anywhere from ten to fifty years from now, would likely upend this entire encryption system. Quantum computers derive their computational power from quantum bits, or 'qubits'. While current computers use classical bits, which can only be in one of two states, a '0' or a '1', qubits can be in both states simultaneously due to something known as 'superposition'. This purely quantum phenomenon of existing in both states concurrently provides a huge advantage when it comes to factorisation: rather than trying thousands of combinations iteratively, quantum computer can try multiple combinations *simultaneously*.

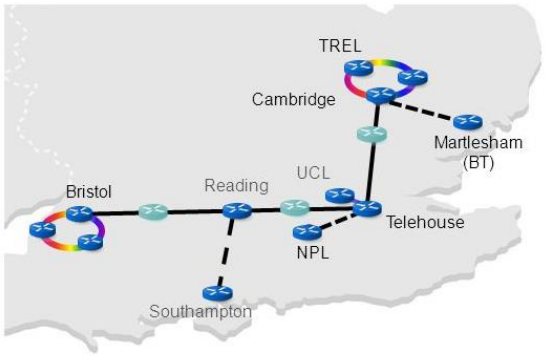
Although several decades may separate us from quantum computers, quantum cryptography, which exploits a different quantum phenomenon, Heisenberg's Uncertainty Principle, is already

commercially available in the form of a quantum key distribution (QKD). This cryptography technique encodes information on individual particles of light, known as photons. As an example, let us suppose that a sender, Alice, and a receiver, Bob, want to share a secure key. Alice prepares her photons and encodes information on them using their polarisation; she first chooses, at random, which basis, either horizontal-vertical (+) or diagonal (x). Then she chooses which bit, '1' or '0' to send, where horizontal (H) and anti-diagonal (A) correspond to '1' and vertical (V) and diagonal (D) correspond to '0'. She then sends these photons to Bob. Bob then chooses at random which basis to measure along. If he chooses correctly, he extracts the bit. If he chooses incorrectly, he has a 50/50 probability of getting either a '1' or '0'. After this, Bob announces publicly which basis he used for each measurement and Alice responds publicly whether he chose the correct basis. Bob then discards all the bits with incorrect measurements, after which Alice and Bob share a common string of '1s' and '0s'. They then publicly compare a small section of them to confirm that they do indeed have the same key. If an eavesdropper, Eve, would like to learn the key whilst going undetected, she can't for a number of reasons. Firstly, she doesn't know in advance which measurement to perform, so if she does an incorrect measurement, and then sends her own particle to Bob, this will introduce an error which can be detected by Alice and Bob when they compare their small selection of bits. Secondly, she cannot copy the photon, as this is physically impossible. In this way, Alice and Bob can share a key with perfect security. As such, since it is based on the laws of physics, quantum cryptography is theoretically unbreakable. Even an eavesdropper with an infinitely powerful computer, or even a quantum computer, could not break this means of communication. As other nations divert significant resources toward preparing for a quantum cryptography-era, one pressing question remains: has the UK kept up?

Well, actually, the answer is mostly 'yes'. In 2013, the UK invested in a £270 million Quantum Technology Hub [1], a nationwide initiative of universities and industrial partners who are dedicated to the development of quantum technology. Comprised of four hubs, the initiative has specialised teams responsible for sensing, metrology, computing and, most importantly, communication. Moreover, the Ministry of Defence (MoD) has committed £36m to the cause and the total investments from the public and private sector were estimated to exceed £350m this year. This hardly comes as a surprise since quantum technologies could be worth as much as the consumer electronics sector, which currently nets about £240bn a year globally [2].

The money invested so far has produced significant results. One ongoing project is the construction of a quantum communications network over fibre-optics. This would cover southern England, with nodes in, among others, Bristol, Reading, London, Martlesham in Suffolk (specifically at BT) and Cambridge, which also contains its own metropolitan network. However, the UK struggles with the commercial realisation of QKD. Currently, the Swiss firm IDQuantique have cornered the market, having sold their own systems for several years. American and Australian firms, such as MagiQ and Quintessence, claim to provide systems, but details are sparse at best. Toshiba look poised to announce their entrance into the market, having demonstrated numerous field trials over the years. The company also recently broke the record for the fastest transfer of secure keys over 50 km of fibre [3]. Although numerous British experts undoubtedly provide valuable services through consultancy, the only firm springing out of

this is the Bristol-based KETS. Comprised of several researchers, KETS recently secured access to more than £125 million of venture capital funding at a recent start-up competition hosted by Facebook and BT [4]. Taken together, it seems the strength of British firms lies more in the provision of the components for these systems rather than developing the entire product themselves.



The UK is developing a quantum network, with nodes in several major cities and at R&D centres such as Toshiba Research Europe Ltd (TREL) and National Physical Laboratory (NPL).

Despite significant achievements, the UK should be hesitant to rest on its laurels, particularly when drawing comparisons to the achievements of other countries. China has easily led the way in terms of translating funding and resources into real, tangible results; the launch of their quantum satellite, Micius, catalysed their success, which began with the demonstration of QKD between Micius and a ground station, easily surpassing any previous distance records [5]. They then went even further by performing a quantum-secured intercontinental video conference between Beijing and Vienna, a world first [6]. This, coupled with their announcement of a 2000 km long metropolitan network [7], a brand new quantum centre [8] and a pledge to create a global, quantum-secured network by 2030 has placed the Chinese at the top of the sector. Indeed, these results have caused quite a stir, resulting in a number of countries announcing their own satellite projects, including Canada and Japan [9], as well as other more collaborative approaches. Despite significant progress in CubeSats – compact and comparatively cheap satellites suitable for space-based QKD experiments – thus far, there is no indication that the UK plans to follow suit. Undoubtedly, the uncertainty surrounding Brexit makes it highly unlikely that the enormous investment required will be appropriated in the near future. Indeed, the UK's involvement in the €1 billion EU Horizon project has already come under question.

The official position of the UK government is against implementing QKD. The National Cyber Security Centre, a branch of GCHQ, currently advises against the adoption of QKD due to uncertainty surrounding its practical security and feasibility [10]. However, this is not set in stone, and a leading science policy advisor has even indicated that revisions to this position are underway. Furthermore, significant work has been carried out by the European Telecommunications Standards Institute (ETSI) toward standardisation of QKD in anticipation of its widespread implementation, and the UK's National Physical Laboratory (NPL) has played a key role in this. Such a collaboration suggests that QKD is gaining momentum, and the focus has now shifted away from proving theoretical security to demonstrating real-world, practical security. This shift suggests QKD may be moving outside of the lab and into something that could soon be part of everyday life.

So, what are the next steps for UK science policy? This will hinge upon the outcome of Brexit; significant research funding currently stems from the EU (e.g., in the form of the Marie Curie Fellowship), which

also sources many of the individuals currently involved in British QKD development. Next, as the initial funding phase for the four Quantum Hubs will end this year, policymakers must determine whether the funding will be extended or renewed. The Hubs have catalysed the development of several quantum technology clusters in York, Bristol and Cambridge, and, by continuing Hub funding, the UK government could not only grow the sector but also provide assurance to businesses that have yet to invest in quantum communication. Finally, Britain ranks within the top five in terms of spending, publications and patent applications in the area of quantum science [2], and continued collaborations between academia, business and government will ensure a strong global position for years to come. The age of quantum internet is imminent, and the UK must decide if it wants to continue as a leading player of the so-called 'quantum revolution,' or resign itself to a place on the sidelines.

Acknowledgements

Alex would like to thank the first editor of this article Maggie Westwater, and second editor Roxine Staats.

References

[1] EPSRC (2017) *UK National Quantum Technologies Programme.* [Online]. Available: https://bit.ly/2H8CbUk

[2] Government Office for Science (2016) *The Quantum Age: technological opportunities.* [Online]. Available: https://bit.ly/2w4JiZn

[3] Z. Yuan, et al., "10 Mb/s quantum key distribution," in *QCrpyt 2017*, Cambridge.

[4] BT (2017) *BT, Telecom Infra Project and Facebook announce start-up competition winners.* [Online]. Available: https://bit.ly/2gg365b

[5] S.-K. Liao, et al., "Satellite-to-ground quantum key distribution," *Nature,* vol. 549, pp. 43-47, Aug 2017.

[6] The Independent (2017) *Scientists hold world's first intercontinental video conference using quantum encryption.* [Online]. Available: https://ind.pn/2HnLM7C

[7] Financial Times (2017) *China trial paves way for 'unhackable' communications network.* [Online]. Available: https://on.ft.com/2u1cwGH

[8] Popular Science (2017) *China is opening a new quantum research supercenter.* [Online]. Available: https://bit.ly/2gtaV4s

[9] National Institute of Information and Communications Technology (2017) *World's First Demonstration of Space Quantum Communication Using a Microsatellite.* [Online]. Available: https://bit.ly/2HnM7ao

[10] National Cyber Security Centre (2016) *Quantum Key Distribution.* [Online]. Available: https://bit.ly/2HiX6BD

About the Author

Alex Koehler-Sidki is a 3rd PhD student with the Engineering Department at the University of Cambridge. His current research is focused on the security of single photon detectors in quantum cryptography which is based at Toshiba Research Europe, just north of the city. Prior to this, Alex completed an MSci at the University of Nottingham, including a year at the Ludwig-Maximilians-Universität in Munich, before spending half a year working at a leading photonics company.