CJSP Cambridge Journal of Science & Policy

Quantum Key Distribution: Advantages, Challenges and Policy

Communication | Editorial | Invited contribution | Perspective | Report | **Review**

Victor Lovic
Department of Physics
Imperial College London
v.lovic19@imperial.ac.uk

Abstract

The prospect of quantum computing threatens the security of modern encryption methods, putting our private communications at risk. With experts predicting the development of powerful quantum computers as early as the end of the decade, the urgency of transitioning to 'quantum-safe' communications is apparent. There are two classes of solutions available: post-quantum cryptography (PQC), which refers to communication algorithms designed to be safe against quantum computers, and quantum key distribution (QKD), a new technology with unique advantages and challenges. These solutions are not mutually exclusive, and this review argues that they are in fact complementary solutions to the threat of quantum computing. However, QKD has received criticism for being a less practical solution than PQC. This review makes the case for QKD and argues that it offers significant advantages which are not adequately recognised. I conclude that the development of QKD would benefit from increased government support and I provide policy recommendations for how to best support it.

Introduction

Quantum computing is a new technology which promises to perform certain computations much faster than any modern supercomputer. Accelerated drug discovery and better climate models are just two examples of applications which will benefit from the capabilities of quantum computers. On the flip side, quantum computers will also be able to break most methods of encryption used today, putting our private communications at risk.

Since the first theoretical developments in the 1980s, quantum computers have quickly become a reality. Major investments from government research budgets and private companies have led to the development of the first iteration of quantum computers, comparable perhaps to the first (classical) computers built nearly 70 years ago using vacuum tubes. This rapid progress is cause for alarm since when a sufficiently powerful quantum computer is developed, our standard encryption methods will become inadequate and our communications insecure. Moreover, not only are our future communications under threat, our cur-

CJSP Cambridge Journal of Science & Policy

rent communications are too: modern encryption methods rely on what is known as 'public-key' cryptography. The word 'public' points to the fact that information encrypted in this way can be recorded and stored by anyone. This opens the possibility for an eavesdropper to record our private, encrypted communications and wait for a sufficiently powerful quantum computer to become available and use it to decrypt them in the future. Since we require certain communications to remain private for long periods of time, we must make the transition to quantum-safe forms of communications well in advance of the development of quantum computers. This is especially true since transitioning to 'quantum-safe' forms of communications could take many years.

Fortunately, alongside the development of quantum computers, there has been ongoing research into alternative, quantum-safe communication methods. Broadly speaking, two distinct classes of solutions are available, known as post-quantum cryptography (PQC) and quantum key distribution (QKD). This review gives an overview of both technologies but will focus on the advantages and challenges presented by QKD. I argue that QKD, being a truly novel technology, is poorly understood and in need of a defence. It has significant advantages which are not adequately recognised and there has been tremendous progress in addressing the practical challenges of making it a useful and cost-effective solution. The review is structured as follows: Section 2 introduces public-key cryptography and why quantum computing poses a threat to private communications; Section 3 introduces PQC and QKD as potential solutions to this threat; Section 4 makes the case for QKD and finally Section 5 discusses the outlook of both technologies and provides policy recommendations.

Cryptography and Quantum Computers

Cryptography has been used for centuries. An early example is the so-called Caesar cipher used, as the name suggests, by the ancient Romans. The Caesar cipher works as follows: two people who want to communicate, conventionally called Alice and Bob, privately agree on a secret number, which we call the 'key'. To encrypt a message, Alice replaces each letter with another letter a fixed number of positions down the alphabet, determined by the value of the key. To decrypt the message, Bob simply reverses the process, replacing each letter by that found the same number of positions up the alphabet. While modern cryptography has advanced a great amount, it is still based on the same principle: two communicating parties agree on a secret number, or key, which they use to encrypt and decrypt their communications. This type of cryptography is known as 'symmetric-key' cryptography because the same key is used for encrypting and decrypting messages. The problem with symmetric-key cryptography is that Alice and Bob need to agree on a secret key before communicating. This requires them to either meet in person or use a trusted courier, neither of which are practical solutions for securing the vast amount of information that is nowadays sent over the internet. The solution to this problem, only developed in the 1970s, is known as 'public-key' cryptography. In public-key cryptography, the keys that are used to encrypt and decrypt the communications are different, but mathematically related. The key which is used to encrypt messages is made public, while the key used to decrypt messages is kept private. In this way Bob can send Alice his public key, which can be seen by anyone, for her to encrypt her messages with. She can then send her encrypted message to Bob and, crucially, only he will be able to decrypt it, since only he has the corresponding private key. Since the keys are mathematically related, it is important that no eavesdropper is able to figure out the private key given the public key. The mathematical problem for doing this needs to be 'intractable', that is, very difficult and time-consuming. For example, the mathematical problem that guarantees the security of the widely used public-key RSA protocol is factoring: the process of finding the prime factors of a large number. It would take modern computers thousands of years to factor the public keys used in RSA encryption, which is why the communications are considered secure. If an eavesdropper was able to quickly factor large numbers, then they would be able to break RSA encryption since they could extract the private key from the public one. Although there are good reasons to think that factoring

really is an intractable problem, there remains the possibility that a mathematical or technological breakthrough will allow us to quickly factor large numbers. Indeed, in 1994, the physicist Peter Shor showed that quantum computers will be able to quickly factor large numbers and decode other mathematical encryptions currently used in public-key cryptography. A white paper published by the European Telecommunications Standards Institute (ETSI) states that

> [m]ost of the public-key cryptography that is used on the Internet today is based on algorithms that are vulnerable to [attacks by a quantum computer]. These include public-key algorithms such as RSA, ECC, Diffie-Hellman and DSA [1].

This means that, in a future with sufficiently advanced quantum computers, currently used public-key cryptography is at risk. And not only are our future communications at risk: quantum computers threaten our current communications too. Public keys, by definition, can be recorded and stored by anyone, along with the encrypted messages. In this way an eavesdropper could record encrypted private communications and corresponding public keys and wait for a sufficiently powerful quantum computer to become available. They could then use the quantum computer to solve the mathematical encoding problem, obtain the private key, and decrypt the communications. This is known as 'retrospective decryption' and all public-key cryptography protocols are susceptible to this attack [2].

So how long will it take for sufficiently powerful quantum computers to become available? A leader in the quantum computing race, Google CEO Sundar Pichai, speaking at the 2020 World Economic Forum in Davos, claimed that

> In a five to ten year time frame, quantum computing will break encryption as we know it today [3].

This is arguably an overly optimistic outlook from a tech-company executive, but predictions coming from academia are also sobering. Michele Mosca, Physics professor at the Institute for Quantum Computing (IQC) at the University of Waterloo, predicts a 50% chance of quantum computers breaking RSA encryption by 2032 [4]. His colleague Matteo Mariantoni, also professor at IQC, believes that a quantum computer capable of breaking RSA encryption could be built by 2030 [5]. In many cases, private information needs to be kept secret for several years. For example, census data in the UK is required to remain undisclosed for 100 years [6] and it is easy to understand why health records, government communications, and other sensitive data have similar secrecy lifespans. If predictions about the development of quantum computers are correct, then these types of data are already at risk of being hacked by a future quantum computer. To make matters more urgent, transitioning to quantum-safe forms of communication could require several years, so it is apparent that we must start this transition now.

Two Solutions

Fortunately, scientific research has not focused solely on building quantum computers, but also on developing quantum-safe communications, such as PQC and QKD.

We saw that the security of public-key cryptography is based on the intractability of certain mathematical problems. For the most widely used public-key protocols, quantum computers could quickly solve these intractable problems, rendering the communications insecure. However, the possibility exists that other mathematical problems will remain intractable, even to quantum computers. This is what motivates research into PQC. PQC refers to cryptographic protocols which are thought to be secure even against quantum computers. In this way, the threat of quantum computing is averted by exchanging the cryptographic protocols we use with ones that are based on mathematical problems which are intractable even to quantum computers.

PQC is a very appealing solution since it is based on the same principles as the cryptographic methods we use today. Transitioning to quantum-safe communications using PQC could involve little more than a software update to our computers. And there are already many proposed PQC proto-

CJSP Cambridge Journal of Science & Policy

cols; currently there is active research into testing and validating these new protocols. The National Institute for Standards and Technology (NIST) in the USA is currently hosting a competition [7] to identify the most promising PQC protocols with the intention of establishing new standards for quantum-safe communications. After reducing the initial pool of 69 candidate protocols down to 26, they have now entered the second phase of this process, during which the remaining candidates will be further examined with the aim of drafting the final standards for PQC in 2022.

The downside is that public-key PQC protocols are still vulnerable to retrospective decryption and future advances in mathematics or technology that might render them insecure. The possibility remains that mathematical problems that we once thought intractable, even for quantum computers, turn out not to be.

Quantum key distribution (QKD) is a fundamentally different approach to quantum-safe communications, based on the principles of physics rather than on the use of intractable mathematical problems. QKD solves the same problem as public-key cryptography: it allows two parties (Alice and Bob) to establish a secret key between them. The key can then be used with symmetric-key cryptography to communicate securely. In QKD, Alice and Bob communicate using single particles of light, called photons. Photons obey the laws of quantum mechanics, which is the physical theory that describes the behaviour of very small objects, like single atoms, or photons. When we use single photons to carry information, we call that information quantum information, which has different properties to classical information. Quantum information has two unique properties that make QKD secure:

1. It is impossible to make exact copies of quantum information.
2. It is impossible to measure or observe quantum information without introducing a disturbance and changing it in some detectable way.

In this way, if Alice sends Bob a secret key using quantum information carried by photons, she can be sure that: 1. no eavesdropper is able to copy and store that information and 2. if an eavesdropper tried to measure or observe the secret key, they would inevitably introduce a disturbance in the key, which Alice and Bob could detect. Crucially, quantum mechanics and these two properties of quantum information are fundamental theories in physics. This makes QKD resilient to any future advances in mathematics or technology since, unlike public-key cryptography, it does not make any assumptions about the intractability of certain mathematical problems, or about the technology available to potential eavesdroppers. In practice, QKD consists of using hardware like lasers and specialised electronics to send single photons through optical fibres between Alice and Bob. Making the transition from our current encryption methods to QKD would therefore require much more than a software update.

Clearly there are pros and cons to each solution. PQC offers quantum-safe communications based on the same cryptographic principles used today. QKD provides unique advantages at the cost of requiring large changes in infrastructure and hardware.

The Advantages and Challenges of QKD

The National Cyber Security Centre (NCSC) in the UK released a white paper on QKD in 2016 '[making] the case for research into developing post-quantum cryptography as a more practical and cost-effective step [than QKD] towards defending real-world communication systems from the threat of a future quantum computer' [8]. They followed this up with a report in 2020 reiterating that they '[do] not endorse the use of QKD for any government or military applications' citing the 'specialised hardware requirements of QKD' as a reason [9]. In light of this criticism, and the fact that QKD is a truly novel technology, I argue that the advantages of QKD are poorly understood and the practical challenges are overstated. In what follows, I will outline the unique advantages offered by QKD, as compared to PQC, and then address the main issues regarding the practicality of this technology.

First, QKD offers *future-proof* communications. This does not mean that a QKD system will never be hacked, but rather that communications secured via QKD cannot be hacked after the com-

munication has happened: either the hacking happens in real-time or it does not happen at all. With QKD, cryptographic keys are never made public and, as described in the previous section, QKD keys are impossible to copy and store. This is an important advantage over our current, and any future, public-key cryptography methods, including those based on PQC. With public-key cryptography there is always the possibility that encrypted messages and public keys are stored by an eavesdropper and decrypted at a future date when, through advances in technology or mathematics, the communication protocols become insecure. QKD is the only known solution to this retrospective decryption. QKD is therefore particularly suited to securing communications with long secrecy lifespans that must remain undisclosed for many years. Promising use cases for QKD include the storage of financial and customer data by large institutions, the handling of private health records, including human genome data, and the protection of government and military communications [10].

Second, theoretical QKD protocols have been proven to be perfectly secure, while no such proof is available for PQC. PQC relies on assumptions about the intractability of certain mathematical problems. But we have seen how developments in technology like quantum computing can undermine these assumptions. With QKD we do not need to rely on such assumptions, and we say that QKD is 'unconditionally secure'. This is not to say that QKD systems are perfectly secure, just that the underlying theory is. It is then still important to make sure that the physical systems that implement the theoretical QKD protocols do not inadvertently introduce any vulnerabilities, which might be exploited by an eavesdropper[1]. The study of these 'implementation security' vulnerabilities is an active area of research that is bringing QKD systems closer to achieve an ideal of perfect security.

Lastly, I argue that investing into the development of QKD promises benefits that go well beyond just securing our private communications. In the long run, we can envision a 'quantum internet', which is a network of quantum computers connected via QKD links. While the details are outside the scope of this review, the quantum internet has applications not just for secure communications but also for 'secure access to remote quantum computers, more accurate clock synchronisation and scientific applications such as combining light from distant telescopes to improve observations.' [11]. A QKD infrastructure will serve as the foundation for such a quantum internet.

The main arguments against QKD revolve around practicality. QKD is based on hardware, like lasers used to send photons through optical fibres, while PQC is based on software, algorithms much like the ones we currently use, which could run on our computers without modification. Obviously, as suggested by NCSC, PQC is the more 'practical and cost-effective solution'. However, there has been tremendous progress in the past 20 years towards addressing the practical challenges that come with implementing QKD in the real world. Here, I will address potential concerns and give a sense for how far the technology has come.

A central challenge in implementing QKD over long distances and at high communications rates is the 'transmission loss' in optical fibres: approximately nine out of ten photons are lost for every 50km of fibre they travel. In conventional communications this problem is easily solved: optical signals can be amplified at regular distance intervals using 'repeaters', allowing us, for example, to send signals from Europe to the American continent through underwater optical fibres. However, the process of amplifying an optical signal can be thought of as making extra copies of the photons to counteract the transmission losses. We saw that quantum information cannot be copied, which makes it challenging to develop repeaters for quantum information. Although it is an active area of research, currently QKD cannot rely on quantum repeaters to send quantum information over long distances. This means that the range of QKD is limited and that there is a trade-off between distance and the communication rate: the longer the distance between Alice and Bob, the fewer photons sent by Alice will reach Bob, slowing the communication rate.

Much of the research in QKD has been devoted to increasing the distance and communication

[1] It should be pointed out that practical implementations of PQC can also introduce security vulnerabilities in the communication system.

CJSP Cambridge Journal of Science & Policy

rate. Over the past two decades, there has been great progress on this front: record distances for QKD have increased roughly tenfold from around 50km to current state-of-the-art demonstrations reaching distances over 500km [12]. These improvements are due to advances in the QKD hardware as well as to the development of newer and more efficient theoretical protocols. For longer distances QKD needs to rely on repeaters. We saw that quantum repeaters are not yet available, but by linking several QKD systems one after the other we can achieve a similar result. The drawback is that at every link, or node, the secret key is revealed. Therefore, we need to ensure that no eavesdropping can occur at these nodes. Until quantum repeaters become available, trusted nodes will be the main solution for long distance QKD.

Communication rate is another parameter where QKD falls short compared to classical communications. Current classical optical communications deliver speeds on the order of 100Gbit/s, whereas QKD communications achieve rates in the range of Mbit/s (100,000 times less). QKD is only used to distribute the secret keys used for encryption and not the private communications themselves, so the communication rate requirements for QKD are lower. However, increasing the communication rate of QKD is 'arguably the most pressing task in order to widen the applicable areas of QKD technology' [13].

QKD secured communications require specialised hardware and will undoubtedly cost more to develop than the PQC alternative. As QKD moves out of the lab and towards commercialisation and real-world use, cost-effectiveness is becoming an increasing focus of QKD research efforts. Two results are particularly promising: first, it has been demonstrated that QKD can be performed on the same optical fibres and at the same time as high-traffic classical communications [14]. QKD signals are so faint that there is no negative consequence for other users of these fibres. In this way QKD can make use of existing optical fibre networks, removing much of the need for expensive new optical fibre connections. Second, QKD components are being integrated onto semiconductor chips similar to the ones used in computers and mobile phones. By leveraging advances in semiconductor device manufacturing, QKD chips can be mass-produced at low cost and with extremely small footprints. Chip-based QKD will lower costs and allow for easier integration with conventional computers and communication systems.

A testament to how far QKD has come are the many field-deployments of QKD networks around the world. Most impressive is the 2000km long QKD link (using trusted nodes) between Shanghai and Beijing in China [15]. This project included the first demonstration of QKD performed via a satellite, connecting cities in China and Austria. Other countries including the UK [16], Switzerland [17], Austria [18] and Japan [19] have also established prototype QKD networks. Most recently the 'OpenQKD' project, a collaboration between 38 partner universities and companies, was launched in September 2019. With EU funding, the collaboration aims to 'raise awareness of the maturity of QKD' as a technology and 'lay the foundation for a pan-European quantum network' [20].

The challenges point nonetheless to the fact that QKD will at first find applications in sectors dealing with especially sensitive information, which needs to be kept secret for many years. Less sensitive communications can benefit from the high speeds and low cost of PQC that we have come to expect from our current communication methods. QKD and PQC can be seen as complimentary solutions for building quantum-safe communication systems, together covering the whole range from low cost and high speed, to long-term high-security applications. Indeed the NCSC [9], the Blackett review [10], industry, and academia [2] agree that QKD and PQC should continue to be researched in parallel.

Outlook and Policy Recommendations

ETSI cites a 'perception of non-urgency' as a barrier to the adoption of quantum-safe communications [1]. This perception means that currently there are no strong financial incentives for developing quantum-safe communications, in stark contrast to quantum computing. For this reason, investments into quantum technologies, the so-called 'quantum gold rush', have been mostly

directed to the latter [21]. Large technology companies like Google, Microsoft and IBM are investing in their own research efforts. Companies, not countries, are leading the race in quantum computing. In this context, government support for the development of quantum-safe communications is crucial. I argue that PQC is well supported, while QKD could benefit from increased support and investment.

There are already many proposed PQC protocols, mostly coming from academia. What is needed now is to test and validate these protocols. This work has been taken up by standards bodies. As mentioned earlier NIST is planning to conclude its effort in this direction in 2022. In 2015 ETSI established the Quantum Safe Cryptography Working Group to assess and recommend PQC protocols. They recently held their seventh 'Quantum Safe Cryptography Workshop', bringing together academic and industry partners. Additionally, companies like Google [22], Microsoft [23] and Amazon [24] are already working towards integrating PQC protocols into their services. This all contributes to a positive outlook for PQC.

The perception of non-urgency, the practical challenges inherent to QKD, and a lack of awareness of its unique advantages make commercialising QKD challenging. Government support for this technology is crucial, not least since government and military applications are cited among the first use cases for QKD. I propose the following policy recommendations to support the development of QKD, with a UK focus:

- **Raise awareness of the threat of quantum computing to private communications and the available solutions.** This is especially important for industries and sectors with long-term security needs, which are particularly vulnerable to retrospective decryption, like government, military, and healthcare. The NCSC provides practical cyber security guidance through its Cyber Assessment Framework. This framework should be updated to account for the threat of quantum computers, especially to communications with long secrecy lifespans. Awareness of the available solutions is equally important. A survey of Information Technology and Security professionals by the Cloud Security Alliance found that 'most respondents do not believe there is an existing solution to the quantum computing threat' [25].
- **Clarify the unique advantages offered by QKD as compared to PQC.** QKD is particularly suited to securing communications with long security lifespans and it is complementary to PQC. In response to the recent NCSC white paper, a commentary by the QKD industry and academic community states that 'wherever possible QKD should be used in tandem with [PQC]' and that 'an approach suggesting a need to choose between QKD and [PQC] is based on a false dichotomy' [2].
- **Involve the NCSC in key programmes for the development and standardisation of QKD.** The QKD community commentary explicitly welcomes direct involvement from the NCSC in the development of new standards for QKD [2]. The ETSI QKD Industry Specification Group [26] works to ensure the future interoperability of diverse QKD systems and that these systems are implemented in a safe manner. Involvement by the NCSC would ensure these standards meet the requirements of the Cyber Assessment Framework.
- **Engage in early trials of QKD for government and military applications.** Government and military have long-term security needs that QKD is well suited to address. Direct involvement in early trials will support the development of QKD and ensure QKD systems meet the needs of this specialist sector.
- **Continue funding research addressing the practical challenges of QKD.** This funding can be seen as an investment, eventually paid off by the reduction in cost and by the increase in performance of real-world QKD systems. Progress in QKD research shows no signs of stopping, with novel theoretical protocols designed on a regular

CJSP Cambridge Journal of Science & Policy

basis and proof-of-principle experiments moving to real-world demonstrations [27]. With continued investments we can expect the great progress of the past two decades to continue.

- **Invest in a backbone QKD network.** QKD is limited in range, therefore establishing long distance connections between cities, and eventually countries, will require a large financial effort. An established backbone QKD network will make it easier for companies and individuals to connect, widening the market and demand for QKD. A backbone QKD network will serve as the foundation for a future quantum internet, with applications that go beyond just secure communications, increasing its value.

Conclusion

There is an urgent need to transition the world's communication systems to quantum-safe methods. This review made the case for quantum key distribution as a solution. QKD is:

- future-proof: communications secured by QKD cannot be retroactively hacked;
- based on provably secure theoretical protocols;
- a building block towards a future quantum internet.

The past 20 years of research and development in the field of QKD have helped to address the practical challenges of implementing QKD systems in the real-world. Proof of this are the many demonstrations of quantum networks around the world. Together, PQC and QKD can be used to secure our communications even in the presence of quantum computers. Government support for QKD in particular is crucial while the technology moves from research and development to commercialisation. Sectors with long-term security needs, including government and military, stand to benefit from the unique advantages of QKD. The policy recommendations provided will support the development of this technology and ensure that the long-term security needs of government, military and other sectors are met.

References

[1] European Telecommunications Standards Institute, "Quantum safe cryptography and security: An introduction, benefits, enablers and challenges," *ETSI White Paper No. 8*, June 2015. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[2] Quantum Communications Hub, "Community Response to the NCSC 2020 Quantum Security Technologies White Paper," *Issue 1.1*, May 2020. [Online]. Available: http://bit.ly/NCSC2020Response

[3] H. Boland, "Quantum computing could end encryption within five years, says Google boss," *The Telegraph*, Jan 2020. [Online]. Available: https://www.telegraph.co.uk/technology/2020/01/22/googles-sundar-pichai-quantum-computing-could-end-encryption/

[4] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[5] NIST, "Report on Post-Quantum Cryptography," April 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[6] UK Office for National Statistics, "About the census," September 2018. [Online]. Available: https://www.ons.gov.uk/census/censustransformationprogramme/aboutthecensus

[7] NIST, "Post-Quantum Cryptography," January 2017. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[8] NCSC, "Quantum Key Distribution," November 2016. [Online]. Avail-

able: https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution

[9] ——, "Quantum Security Technologies," March 2020. [Online]. Available: https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf

[10] UK Government Office for Science, "The quantum age: technological opportunities," November 2016. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf

[11] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[12] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km," *Physical review letters*, vol. 124, no. 7, p. 070501, 2020.

[13] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, pp. 1–12, 2016.

[14] K. Patel, J. Dynes, I. Choi, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Physical Review X*, vol. 2, no. 4, p. 041010, 2012.

[15] J. Qiu *et al.*, "Quantum communications leap out of the lab." *Nat.*, vol. 508, no. 7497, pp. 441–442, 2014.

[16] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho *et al.*, "Cambridge quantum network," *npj Quantum Information*, vol. 5, no. 1, pp. 1–8, 2019.

[17] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[18] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[19] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Optics express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[20] "OpenQKD," September 2019. [Online]. Available: https://openqkd.eu/

[21] E. Gibney, "The quantum gold rush," *Nature*, vol. 574, no. 7776, pp. 22–24, 2019.

[22] K. Kwiatkowski, "Towards Post-Quantum Cryptography in TLS," *The Cloudfare Blog*, June 2019. [Online]. Available: https://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/

[23] Microsoft, "Post-Quantum TLS." [Online]. Available: https://www.microsoft.com/en-us/research/project/post-quantum-tls/

[24] A. Hopkins, "Post-quantum TLS now supported in AWS KMS," *Amazon Web Services Security Blog*. [Online]. Available: https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms

[25] Cloud Security Alliance, "Quantum-Safe Security Awareness Survey," January 2018. [Online]. Available: https://cloudsecurityalliance.org/artifacts/quantum-safe-security-awareness-survey/

[26] ETSI, "Quantum Key Distribution." [Online]. Available: https://www.etsi.org/technologies/quantum-key-distribution

[27] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography [preprint]," *arXiv*, 2019.

CJSP Cambridge Journal of Science & Policy

About the Author

Victor is a PhD student in the Department of Physics at Imperial College London. His research is in the field of quantum cryptography, investigating the security of quantum key distribution and quantum random number generation. He is interested in the potential of emerging technologies to change the world, in good or bad ways, and thinks that good policymaking is key to ensuring good outcomes and mitigating any risks. Previously, Victor studied Physics at the University of Glasgow.

Conflict of interest The Author declares no conflict of interest.