SCTE CABLE-TEC EXPO® FAST FORWARD 2021
VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall
Technical Forum
SCTE® • NCTA • CABLELABS®

Hitchhiker’s Guide to Quantum Key Distribution

A Technical Paper prepared for SCTE by

Vaibhav Garg
Sr. Director Cybersecurity Research & Public Policy
Comcast Cable
Blacksburg VA
Vaibhav_garg@comcast.com

Walter Krawec
Assistant Professor
University of Connecticut
Storrs, CT
Walter.krawec@uconn.edu

Pete Quesada
Sr. Principal Engineer
Comcast Innovation Labs
Denver, CO
pete_quesada@cable.comcast.com

Tony Tauber
Distinguished Engineer
Comcast Cable
Boston, MA
Tony_Tauber@cable.comcast.com

Aman Satija
Research Engineer
Purdue University
West Lafayette
asatija@purdue.edu

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Abstract

Quantum Key Distribution or QKD offers a quantum safe mechanism to establish an encrypted and authenticated communications channel. QKD is theoretically secure against a computationally unbounded adversary; this contrasts with classical key distribution systems where security is contingent on the assumptions made about the computational capacity of the adversary. These systems are being deployed in operational test environments across the globe. Most commercial systems require expensive proprietary technology, where the marginal cost of deployment is proportional to the capital investment. This means that the cost of adding an additional user is proportional to the cost of the original system. Thus, some experts have argued that the security assurance of QKD systems is not adequate to justify a transition from current approaches, other than for niche or otherwise narrow use cases. This paper provides an overview of current QKD systems, provides insight into the economics of deployment, and discusses the potential for commercial applications.

2. Introduction

The promised advent of quantum computers has focused on the negative impact of quantum technologies for security. Large quantum computers can void the security of current public key cryptosystems, necessitating a transition to Post Quantum Cryptography (PQC), i.e. cryptography that would be secure against know quantum cryptoanalysis. Less attention has been paid to security enabling solutions such as Quantum Key Distribution (QKD) [1]. These solutions, unlike quantum computers, are currently being tested in operational settings across the world. South Korea Telecom, which announced the first 5G smartphone enabled with Quantum Random Number Generator (QRNG), is now testing ID Quantique's QKD system in its 5G network [2]. British Telecom partnered with Toshiba Labs and is now testing a QKD-enabled link between two research sites in Bristol, United Kingdom [3]. Stateside, Verizon is piloting a QKD network in the Washington D.C. area [4].

The key security advantage of QKD systems is that they are theoretically secure against a computationally unbounded adversary [1]. Thus, unlike RSA or Elliptic Curve cryptography, the security of these systems is not based on the hardness of solving a mathematical problem. Simultaneously, unlike AES and post-quantum cryptography, their security is not based on the computational limits of the adversary. Instead, the security of QKD is based on the laws of quantum physics. This means that any communications secured using QKD can be recorded by an adversary and the communicating parties can be assured that, regardless of any future technological advances, the messages will be secure in perpetuity [5]. Critics, however, will point out that adversaries typically do not rely on cryptoanalysis or breaking the math. The easier solution is to find a vulnerability in the software [6].

In the United States, the NSA has supported the critics' view by stating that national security systems should not be secured with the use of quantum cryptography, including quantum key distribution [7]. Yet, the Bureau of Industry and Security continues to restrict the dissemination of QKD technology as part of export controls [8]. Internationally, ETSI [9], ITU [10], as well as ISO/IEC [11] have continued their standards efforts for QKD, advancing the view of supporters of QKD.

If you are new to QKD and all this confuses things, DON'T PANIC. This paper is an effort to provide a representative overview of QKD, the arguments for and against this technology, and the possible future implications. We begin with an introduction to QKD in Section 3. Section 4 provides an overview of the commercial landscape and deployment architectures. In Section 5, we discuss the benefits and limitations of various solutions as well as potential use cases. Section 6 concludes with a summary of key points.

3. An Introduction to QKD

QKD is a subset of quantum cryptography technologies [12]. These solutions are based in large part on the quantum physical property of *no cloning*, i.e. it is impossible to measure a quantum state without changing its properties [13]. This property has led to many quantum cryptography solutions, such as quantum coin tossing [14], quantum oblivious transfer [15], quantum zero knowledge proofs [16], quantum bit commitment [17], quantum secret sharing [18], and QRNGs [19]. While many of these solutions have been of theoretical interest to cryptographers, some, like QRNGs and QKD, have gotten significant commercial traction [1].

The first and perhaps the most well-known QKD protocol is BB84, which was designed by Charles Bennett and Giles Brassard in 1984 [20]. Every subsequent protocol is to a degree an adaptation for BB84 for a specific technical design under distinct constraints. BB84 has two main stages. In stage 1 Alice sends a series of quantum states to Bob over a quantum channel. These states are randomly constructed in either the X or Z basis by Alice and similarly arbitrarily measured in either basis by Bob. If the states are measured in the same basis as the one in which they are constructed, the outcome is deterministic, otherwise it is random and destructive.

In stage 2 Alice reveals her basis to Bob through a classical channel and Alice and Bob keep the states in which Bob chose the correct basis. The channel for classical communication is public but authenticated, i.e. Eve can eavesdrop on this channel, but not tamper with any message sent on it. Due to the no cloning theorem of quantum mechanics, Eve must actively attack the quantum signal (she cannot store the quantum data to attack at some future time). Finally, since Eve does not know the basis choice that Alice used, she cannot deterministically extract any information with certainty. In fact, any attempt by Eve to extract information from the quantum data will cause the quantum state to become disturbed, which may be detected by Alice and Bob.

The BB84 protocol was designed to be used with single photon emitters. However, these can be difficult to build and operate and thus add expense to the system. Researchers have addressed this by proposing decoy state BB84, which can be implemented using weak coherent lasers [21]. Others have proposed measurement device independent or MDI QKD protocols, which protect against side channel attacks [22]. Finally, a recent addition has been semi-quantum QKD protocols [23]. In these protocols, some of the participants need to be able to prepare or measure quantum states, whereas others can simply reflect them.

The cost of QKD systems is driven by the photon detectors, i.e. Single Photon Avalanche photoDiodes (SPADs). These may require special cooling equipment, resulting in higher capital costs, increased operational costs, greater operational complexity, as well as more cumbersome form factors. A good SPAD should always click when a photon hits it (quantum efficiency), should not click when a photon is not present (dark count), have a low reset time (dead time), should not result in multiple clicks for a single photon (afterpulsing), and be accurately able to ascertain when a photon was detected (timing jitter).

The physics of single-photon detection leads to fundamental trade-offs between the various desired characteristics. For example, an increase in quantum efficiency is achievable with a larger detector area. However, that leads to a greater uncertainty in the incident location of the photon which translates an increase in timing jitter. Similarly, it is desirable to lower detector temperature to reduce dark noise however that increase the probability of after-pulsing (as well as the cost).

QKD systems can operate over fiber or in free space. Systems that operate over fiber are typically limited to a range of 50-100kms. This is a fundamental difference between classical and quantum communication. One cannot use a traditional fiber amplifier on single-photons due to the *no cloning* theorem [13]. Thus, QKD systems use trusted nodes to extend their range. This inherently limits the security guarantees offered by QKD, i.e. the overall security of the system becomes dependent on the trustworthiness of the trusted nodes. Another limitation is the hold-off period of SPADs applied to prevent after-pulsing after an avalanche breakdown, i.e. the detector needs a time gap between detecting two distinct photons. Without this gap, or hold-off period, the detector may click multiple times even though there is only one photon in the fiber. The hold-off period of Indium Gallium Arsenic or InGaAs SPADs, for example, is 1-10 µs. This limits communication speed to 100 kbps-1 Mbps.

Free space solutions, i.e. earth to space or space to space, may overcome the distance constraints of fiber-based systems. They are instead constrained by line of sight. Furthermore, their efficiency may be impaired by atmospheric conditions such as rain. In fact, QKD systems have a range of variations in implementations, each with distinct advantages and disadvantages. For example, QKD systems that form the base of quantum communication use entangled photons. Some QKD systems use discrete variable implementations, while others use continuous variable alternatives. An exhaustive discussion is beyond the scope of this paper and is covered elsewhere [1].

4. Systems in the Wild

QKD systems are increasingly being tested in a variety of operational setting for various use cases. Some of these are being deployed by the industry alone, others in collaboration with academia and government. There are a range of commercial solutions being offered by traditional technology companies as well as startups of varying levels of maturity. In this section we aim to provide a representative overview of these systems.

4.1. ID Quantique

ID Quantique's flagship product is the Cerberis XG QKD system [24]. The system is designed to be operated over 50km with a secret key rate of 1.4 kbps. The quantum channel can operate over dark fiber or via channel multiplexing with the quantum channel around 1310nm (O-band). The system can be integrated in a diversity of network topologies, including point-to-point, relay, and ring, as well as hub-and-spoke. The system complies with the Advanced Telecommunications Computing Architecture (ACTA) to allow for easy plug and play into existing physical infrastructure.

4.2. Toshiba

Toshiba systems use both proprietary detector, self-differencing single photon detectors, as well as a proprietary protocol, T12 [25, 26, 27]. This allows Toshiba to offer 1 Mbps key rates over 50km deployments, with the equipment operating at room temperature. Toshiba offers two commercial solutions. The first uses multiplexing to allow data and QKD on the fiber. The second operates on dark fiber for long-distance applications. Toshiba has been awarded the contract to deploy and manage the QKD infrastructure of the National Institute of Information and Communications Technology in Japan. The company has partnered with British Telecom to lead the first industry deployment of QKD in UK. In the U.S., it is partnered with Verizon and Quantum Xchange to pursue QKD demonstrations in operational environments.

4.3. Quantum Xchange

At the time of writing, Quantum Xchange does not produce its own QKD systems. Instead, it has partnered with other QKD vendors to provide a key management solution that works with and without QKD. Additionally, Quantum Xchange also has a proprietary trusted node technology developed in collaboration with Battelle [28]. This is being used to build a QKD network from Boston to Washington, D.C., over which it plans to offer QKD as a service. Its systems operate over dark fiber to allow for better key rates and longer-range deployments [29]. The flagship product, known as Phio QK, is available standalone or as a managed service to allow for an easier transition. At the time of writing (summer 2021), the company's primary focus is the financial sector, although, as noted, it is conducting pilots with Verizon.

4.4. Qubitekk

Qubitekk's solution uses entanglement-based QKD rather than prepare and measure systems [30]. Its systems are specifically designed for industrial control systems, and run over standard optical fibers with an offering of 100kbps over 20 kms. Qubitekk's focus is on the energy sector, as a participant in the Department of Energy's Quantum Grid initiative. In one instance, it demonstrated trusted relay based QKD in collaboration with the Electric Power Board in Chattanooga, TN. The demonstration used three distinct QKD systems: 1) a COTS system with BBM92, 2) a research system with BB84, and 3) COTS systems with SARG04. The overall key generation rate was slower than the slowest QKD system [31].

4.5. Quintessence Labs

Quintessence systems are based on Continuous Variable QKD (CV-QKD) vs. Discrete Variable QKD (DV-QKD) [32]. The company's flagship product is qOptica$^{\text{TM}}$ 100. Quintessence is focusing on free-space QKD, where CV-QKD may offer additional advantages. The latter does not use SPADs, which are sensitive to atmospheric conditions. Instead, CV-QKD relies on homodyne detectors that may operate unimpeded under daylight conditions, without the need for spatial filters or spectral filters.

4.6. VeriQloud

VeriQloud's flagship product, QLine, takes a different approach to QKD architecture [33]. It does not require each client to both prepare and measure the state of a qubit. The product QLine then requires only one photon source and detector for a set of clients on a single linear fiber. These clients have neither the ability to measure nor prepare qubits. However, they can transform the state of the photon using optical modulators. Its architecture may be used with either DV-QKD or CV-QKD. At the time of writing (summer 2021), no commercial product is available.

5. The Case for QKD

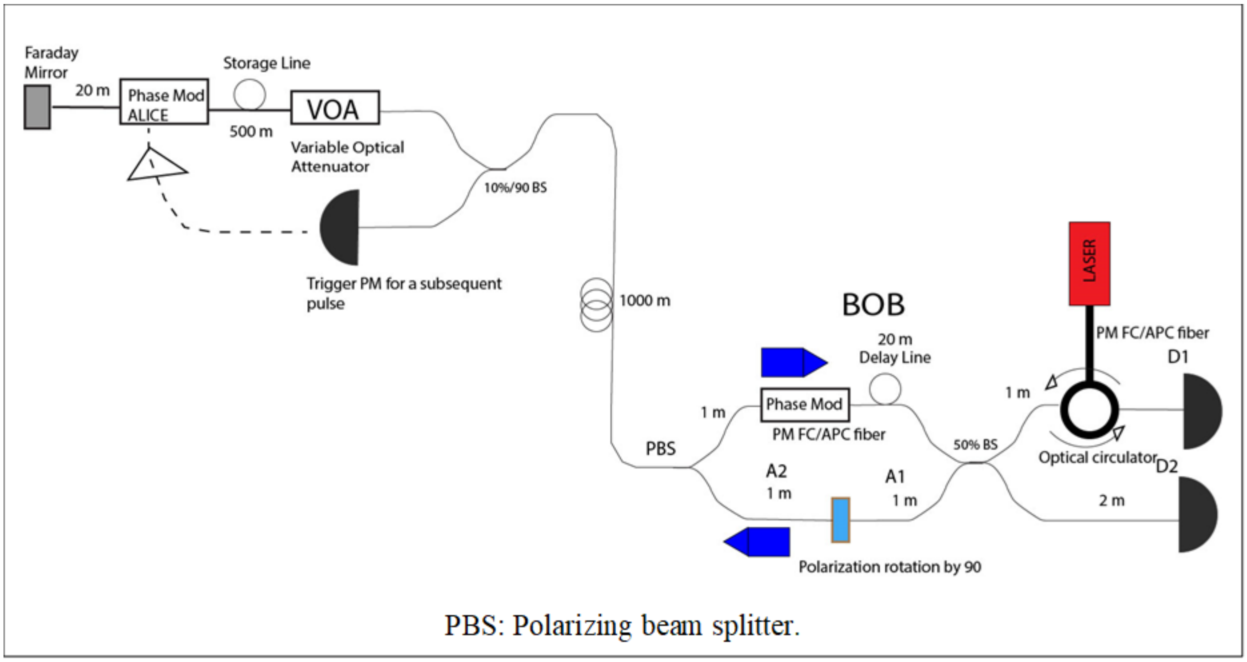
The unconditional security of QKD comes at a cost, which impacts the availability of potential use cases. In this section we will discuss how the economics of QKD may change with technological evolution and thus open the technology to additional use cases.

5.1. Economics of Deployment

QKD systems often use specialized hardware, have more usable keys rates over dark fiber, and may also require special cooling equipment. Given these requirements, a QKD system connecting two nodes may cost on the order of ~$100,000. Simultaneously, as these systems are designed to operate point to point. Thus, the marginal cost of adding another node is the same as that of the initial capital investment. This does not account for the cost of adding a trusted relay, which can further impinge costs for deployments over longer distances. Fortunately, there are both academic as well as commercial solutions emerging that may redefine the economics of deployment.

Many commercial solutions are now ACTA-compliant to allow the use of existing chassis. Commercial products, such as IDQuantique's Gen 4 Cerberis, work in a variety of network topologies, e.g. star, spoke and hub, etc. New experiments from Toshiba have extended the range of fiber-based QKD from 50-100km to 600km [34]. This reduces the cost of long-range deployments by a factor of six (or perhaps even 12). The distance limitations of fiber-based QKD can also be compensated by satellite-based QKD. In Canada, Loft, in partnership with QEYSSat and the Canadian Space Agency, is looking to build small, inexpensive satellites for QKD [35]. Singapore-based startup Speqtral has already demonstrated entanglement in space with ira nano satellite SpooQy-1 CubeSat [36].

Another promising solution is the potential for auto-compensated QKD systems that use Faraday Mirrors in combination with semi-quantum protocols. These essentially act as mirrors for optical signals and simply reflect them back down the fiber. As early as 2002, IDQuantique conducted a demonstration of one such solution over 67km with a bit rate of 50bps at 1550nm [37]. This was followed up with another auto-compensated system as part of the SECOQC initiative where key rates were closer to 1Kbps [38]. VeriQloud's QLine requires but one set of sender and receiver for a set of clients. With these solutions the capital cost of deployment may be high, but the marginal cost of adding another client will likely be orders of magnitude lower. For example, Faraday Mirrors (FM) used in auto-compensated QKD are on the order of $100 (vs. a single detector which runs on the order of $25,000). The corresponding end point systems may be on the order of ~$1000 for Faraday Mirrors vs. ~$100,000 for detectors.



PBS: Polarizing beam splitter.

Figure 1 - Example Auto-Compensated DV-QKD System

At its core QKD is simply a mechanism for securely distributing keys. These keys can then be used in any of the various contexts that currently use PKI for key distribution. For example, as far back as 2010, ETSI published a white paper noting that the keys generated from QKD can be integrated in any part of the network stack from Data Link Layer to Application Layer [39]. On the Data Link Layer, QKD keys can be used be used to support the encryption component of Point-to-Point Protocol (PPP). They can be combined with a link encryptor to support a Virtual Private Network (VPN) [40]. Fortinet, for example, in partnership with IDQuantique ,will begin to offer a QKD-based VPN platform [41].

It has been argued that any protocol that requires a pre-shared secret can use QKD keying material instead [42]. Thus, the use of QKD keys can be extended to Network Layer protocols such as IPSec [43], Transport Layer Protocols such as TLS [44], and application layer protocols such as Kerberos [45] or Single Sign On [46]. For example, IPSec uses Internet Key Exchange (IKE) protocol for key management. A QKD key may be used in place of the Diffie-Hellman shared secret used by IKE. This can be done in conjunction with an agreed upon cipher suite, or alternatively, the QKD key may be used as an One Time Pad (OTP). The second option will ensure security in perpetuity, whereas the security of the first option will be contingent on the security of the cipher suites.

Thus, QKD keys can be integrated in any part of the infrastructure. The specific use cases will depend on the cost of the QKD end-points vs. the benefit of the security offered. There are many sectors, such as defense and health, where data may need to be protected for 100 years, and perhaps more, in the case of genetic data. However, at $100,000 per QKD-end point, the solution may be cost prohibitive. Over fiber, QKD requires trusted nodes over long distance, which impacts its security assurance.

One solution is to focus fiber use cases for smaller distances [33]. Smart buildings, smart campuses, data centers etc. all require key distribution over short distances. Furthermore, many current approaches assume that both the sender and the receiver need to be able to prepare and measure quantum states. Another alternative is to use auto-compensated systems, which require only the sender to have this capability [37]. The receiver need only manipulate the phase of the photon. The receiver then needs to have a phase modulator along with a Faraday Mirror.

The sender, Bob, can be treated as a central key distribution authority interacting with multiple Alices using polarization division multiplexing [47] (or wavelength division multiplexing [48]). Assuming a distance limit of 50km based on current commercial systems, this system on average can provide coverage for 7850 sq kms. (=3.14 x 50^2). An average U.S. city is 338 sq kms, whereas the average county is 2911.4 sq kms. Thus, many city-wide and metropolitan networks may also satisfy the distance constraints of current QKD systems without trusted repeaters [49].

This can be used to connect local government offices, to secure electronic voting, or even to offer highly secure VPN for remote workers. Advances in the use of QKD with drones may allow for secure key distribution in hard-to-reach areas, disaster zones, etc [50]. With an auto-compensated system using a Faraday Mirror + Phase Modulator, the receiver will offer a more usable form factor both in terms of size and weight for drones.

6. Conclusion

In the past two decades, QKD systems have gone from an academic pursuit to being commercially viable. Implemented correctly, their security is based on the laws of physics rather than the computation ability of the attacker. This guarantee comes at a cost that is partly driven by the need for specialized hardware. However, crypto has often required specialized hardware -- from Hardware Roots of Trust to Hardware Security Modules. Furthermore, there are certain classes of data, such as health data, that may need to be secured for long time, e.g. 100 years. There are no current crypto solutions, including PQC, which can guarantee this. The only solution for these classes of data is QKD, as it does not make assumptions about the computation capability of the attacker, which may evolve with time [51]. (Although it does require QKD key rates that allow for OTPs.)

Perhaps unsurprisingly, market analysts sized the QKD market in 2019 at $2472.4M, with expected growth to $8562.7M by 2026 [52]. Currently, the cost of deployment has limited use cases to high-risk environments such as defense. However, as technological evolution reduces the cost of deployment, it is likely that new use cases will emerge to further increase the size of the market. This potential revenue stream is driving investments in both startups across the globe, and operational proofs of concepts (PoCs) in a range of sectors, from energy to communications.

Finally, entanglement-based QKD is critical to securing a Quantum Internet. QKD, then, is a technology that will increasingly become mainstream. While it will never be the answer to life, the universe, and everything cybersecurity, it will certainly have its use cases. This is reflected in the efforts to standardize architectures and interfaces to ensure interoperability [10,11]. QKD itself comes in many different flavors, i.e. CV-QKD vs. DV-QKD; entanglement vs. prepare and measure; fiber vs. free-space, etc. As with any emerging technology, it is unclear which solution will become the default option. It is possible that different versions may be applicable for distinct uses cases. Thus, this paper was intended to provide a representative overview of relevant technical, operational, and economic considerations, with an eye toward practical QKD.

Abbreviations

ACTA	Advanced Telecommunications Computing Architecture
AES	Advanced Encryption System
BB84	(Charles) Brassard + (Giles) Brassard (19)84
COTS	Commercial Off the Shelf
CV-QKD	Continuous Variable Quantum Key Distribution
DV-QKD	Discrete Variable Quantum Key Distribution
ETSI	European Telecommunications Standards Institute
FM	Faraday Mirror
ISO/IEC	International Standards Organization / International Electrotechnical Commission
IKE	Internet Key Exchange
MFA	Multi-Factor Authentication
NSA	National Security Agency
OTP	One Time Pad
PoC	Proof of Concept
PPP	Point-to-Point Protocol
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adleman
SECOQC	SEcure Communication based On Quantum Computing
SPAD	Single Photon Avalanche (photo)Diode
TLS	Transport Layer Security
UK	United Kingdom and Northern Ireland
USA	United States of America
VPN	Virtual Private Network

Bibliography & References

1. Amer, O., Garg, V. and Krawec, W.O., 2021. An Introduction to Practical Quantum Key Distribution. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), pp.30-55.
2. Press Release, 2020. ID Quantique and SK Broadband selected for the construction of the first nation-wide QKD network in Korea. [weblink]
3. Dunn, J., 2020. BT Is Using Quantum Technology to Secure Gigabytes of Sensitive Data Sent Between Two Industrial Sites In The UK. Forbes. [weblink]
4. Ashraf, C., 2020. Verizon achieves milestone in future-proofing data from hackers. [weblink]
5. Stebila, D., Mosca, M. and Lütkenhaus, N., 2009, October. The case for quantum key distribution. In *International Conference on Quantum Communication and Quantum Networking* (pp. 283-296). Springer, Berlin, Heidelberg.
6. Paterson, K.G., Piper, F. and Schack, R., 2007. Quantum cryptography: a practical information security perspective. *Nato Security Through Science Series D-Information and Communication Security*, *11*, p.175.
7. NSA, 2019. Quantum Key Distribution and Quantum Cryptography. [weblink]
8. Bureau of Industry and Security, 2017. Encryption and Export Administration Regulations. [weblink]
9. Alléaume, R., 2018. Implementation Security of Quantum Cryptography: Introduction, challenges, solutions. *ETSI White Paper*, *27*, p.28.
10. Technical Report, 2020. Security Considerations for Quantum Key Distribution Networks. Telecommunication Standardization Sector of ITU. [weblink]
11. ISO/IEC CD 23837-1. Security requirements, test, and evaluation methods for quantum key distribution. [weblink]
12. Wiesner, S., 1983. Conjugate coding. *ACM Sigact News*, *15*(1), pp.78-88.
13. Wootters, W.K. and Zurek, W.H., 1982. A single quantum cannot be cloned. *Nature*, *299*(5886), pp.802-803.
14. Döscher, C. and Keyl, M., 2002. An introduction to quantum coin tossing. *Fluctuation and Noise Letters*, *2*(04), pp.R125-R137.
15. Bennett, C.H., Brassard, G., Crépeau, C. and Skubiszewska, M.H., 1991, August. Practical quantum oblivious transfer. In *Annual international cryptology conference* (pp. 351-366). Springer, Berlin, Heidelberg.
16. Kobayashi, H., 2008, March. General properties of quantum zero-knowledge proofs. In *Theory of Cryptography Conference*(pp. 107-124). Springer, Berlin, Heidelberg.
17. Hillery, M., Bužek, V. and Berthiaume, A., 1999. Quantum secret sharing. *Physical Review A*, *59*(3), p.1829.
18. Song, Y. and Yang, L., 2020. Semi-counterfactual Quantum Bit commitment protocol. *Scientific reports*, *10*(1), pp.1-12.
19. Herrero-Collantes, M. and Garcia-Escartin, J.C., 2017. Quantum random number generators. *Reviews of Modern Physics*, *89*(1), p.015004.
20. Bennett, C.H. and Brassard, G., 1984, August. An update on quantum cryptography. In *Workshop on the theory and application of cryptographic techniques* (pp. 475-480). Springer, Berlin, Heidelberg.
21. Lo, H.K., Ma, X. and Chen, K., 2005. Decoy state quantum key distribution. *Physical review letters*, *94*(23), p.230504.
22. Xu, F., Curty, M., Qi, B. and Lo, H.K., 2014. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, *21*(3), pp.148-158.
23. Krawec, W.O., 2015. Mediated semiquantum key distribution. *Physical Review A*, *91*(3), p.032323.
24. IDQuantique. Cerberis QKD System. [weblink].

25. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Optics Express*, 21(21):24550, October 2013.
26. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields. High speed single photon detection in the near infrared. *Applied Physics Letters*, 91(4):041114, July 2007.
27. L. C. Comandar, B. Fro ̈hlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields. Room temperature single-photon detectors for high bit rate quantum key distribution. *Applied Physics Letters*, 104(2), January 2014.
28. Hadley, T, 2018. Quantum Xchange Launches the First Quantum Network in the United States to Provide Quantum-Safe Encryption Over Unlimited Distances. BusinessWire. [weblink]
29. Quantum Xchange, 2018. Quantum Xchange Selects Zayo Group for Dark Fiber to Deploy First Quantum Network in the United States. [weblink]
30. Mink, A., Frankel, S. and Perlner, R., 2010. Quantum key distribution (QKD) and commodity security protocols: Introduction and integration. *arXiv preprint arXiv:1004.0605*.
31. Alshowkan, M., Evans, P., Peters, N., Earl, D., Grice, W., Mulkay, D., Jones, K., Morgan, T., Morrison, S., Newell, R. and Peterson, G., 2021. Field Demonstration of a Multiple Trusted Node Quantum Key Distribution on an Electric Utility Fiber Network. *Bulletin of the American Physical Society*.
32. Lance, A., Leiseboer, J., and Symul, T., 2020. Quantum Key Distribution Systems Compared. White Paper – ID 3676. Quintessence Labs. [weblink]
33. Kaplan, M., 2020. Building Small-Scale Quantum Communication Networks. VeriQloud. [weblink]
34. Pittaluga, M., Minder, M., Lucamarini, M., Sanzaro, M., Woodward, R.I., Li, M.J., Yuan, Z. and Shields, A.J., 2020. 600 km repeater-like quantum communications with dual-band stabilisation. *arXiv preprint arXiv:2012.15099*.
35. Winder, D., 2020. Meet the Scrappy Space Startup Taking Quantum Security Into Space. Forbes. [weblink]
36. Villar, A., Lohrmann, A., Bai, X., Vergoossen, T., Bedington, R., Perumangatt, C., Lim, H.Y., Islam, T., Reezwana, A., Tang, Z. and Chandrasekara, R., 2020. Entanglement demonstration on board a nano-satellite. *Optica*, *7*(7), pp.734-737.
37. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. and Zbinden, H., 2002. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, *4*(1), p.41.
38. Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J.F. and Fasel, S., 2009. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, *11*(7), p.075001.
39. Quantum Key Distribution: Use Cases. ETSI GS QKD 002 v1.1.1. 2010. [weblink]
40. Aguado, A., López, V., Martinez-Mateo, J., Peev, M., López, D. and Martín, V., 2018, March. VPN service provisioning via virtual router deployment and quantum key distribution. In *2018 Optical Fiber Communications Conference and Exposition (OFC)* (pp. 1-3). IEEE.
41. ID Quantique, 2020. Partner Fortinet Commercializes a Quantum-Safe VPN Solution. [weblink]
42. Piotr K Tysowski, Xinhua Ling, Norbert Lütkenhaus, and Michele Mosca. The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD). *Quantum Science and Technology*, 3(2):024001, 2018.
43. Mink, A., Frankel, S. and Perlner, R., 2010. Quantum key distribution (QKD) and commodity security protocols: Introduction and integration. *arXiv preprint arXiv:1004.0605*.
44. Mohamed Elboukhari, Mostafa Azizi, and Abdelmalek Azizi. Improving TLS security by quantum cryptography. *International Journal of Network Security & Its Applications (IJNSA)*, 2(3):87–100, 2010.
45. Fatima, S. and Ahmad, S., 2021. Quantum Key Distribution Approach for Secure Authentication of Cloud Servers. *International Journal of Cloud Applications and Computing (IJCAC)*, *11*(3), pp.19-32.
46. Dai, G. and Wang, Y., 2014. A Non-entanglement Quantum Single Sign-On Solution. *International Journal of Theoretical Physics*, *53*(4), pp.1143-1149.

47. Park, B.K., Woo, M.K., Kim, Y.S., Cho, Y.W., Moon, S. and Han, S.W., 2020. User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1× N quantum key distribution network system. *Photonics Research*, *8*(3), pp.296-302.
48. Woo, M.K., Park, B.K., Kim, Y.S., Cho, Y.W., Jung, H., Lim, H.T., Kim, S., Moon, S. and Han, S.W., 2020. One to Many QKD Network System Using Polarization-Wavelength Division Multiplexing. *IEEE Access*, *8*, pp.194007-194014.
49. Wonfor, A., Dynes, J.F., Kumar, R., Qin, H., Tam, W.W.S., Plews, A., Sharpe, A.W., Lucamarini, M., Yuan, Z.L., Penty, R.V. and White, I.H., 2017. High performance field trials of QKD over a metropolitan network. *Quantum Cryptography (Qcrypt)*, p. 467.
50. Conrad, A., Isaac, S., Cochran, R., Sanchez-Rosales, D., Wilens, B., Gutha, A., Rezaei, T., Gauthier, D.J. and Kwiat, P., 2021, March. Drone-based quantum key distribution: QKD. In *Free-Space Laser Communications XXXIII* (Vol. 11678, p. 116780X). International Society for Optics and Photonics.
51. Lovic, V. Quantum Key Distribution: Advantages, Challenges and Policy. *Cambridge Journal of Science and Policy, 1* (2. e8410270193)https://doi.org/10.17863/CAM.58622
52. Market Watch, 2021. Quantum Key Distribution (QKD) Market 2021: Analysis of Key Trends, Industry Dynamics and Future Growth 2026 with Top Countries Data. [weblink]