Evaluation of Quantum Key Distribution for Secure Satellite-integrated IoT Networks

Andrew Edwards[1], Yee Wei Law[1], Ronald Mulinde[1], Jill Slay[1,2]
[1]UniSA STEM, University of South Australia, Mawson Lakes, Australia
[2]SmartSat Cooperative Research Centre, Adelaide, Australia

edwaj011@mymail.unisa.edu.au
yeewei.law@unisa.edu.au
ronald.mulinde@unisa.edu.au
jill.slay@unisa.edu.au

Abstract: There has been a dramatic increase in the number of Internet of Things (IoT) devices and their applications. Furthermore, there is a growing impetus to integrate IoT networks on a global scale, using satellites to expand the range of IoT connectivity into geographically remote areas. Ensuring the security of satellite backhaul for IoT networks is thus of paramount importance. The steady advance of quantum computing in recent years threatens to nullify classical cryptographic approaches based on assumptions of computational hardness, motivating the need for post-quantum cryptography. Quantum computing algorithms have been developed that, once a quantum computer of sufficient scale is realised, will be able to break classical cryptosystems efficiently (at polynomial-time complexity). A promising method of securing information against this threat at the physical layer has emerged in the form of quantum key distribution (QKD). QKD exploits the fundamental physical properties of light to guarantee information-theoretic security. Research into the application and standardisation of QKD to secure satellite backhaul, however, is still in its infancy. This paper presents a brief overview of the theoretical basis for QKD, whilst also providing a survey of contemporary QKD protocols. It evaluates the ability of these protocols to secure satellite backhaul in the context of a typical satellite-IoT network architecture. Furthermore, it highlights the vulnerabilities, as well as the technical challenges associated with this endeavour. Finally, it proposes directions for future research and development into protocols and standardisation for the satellite-integrated IoT domain. Several challenges must be overcome before QKD can evolve into a global-scale solution for securing satellite-IoT. Secret key generation rate remains very low in practical demonstrations of trusted-relay QKD satellite architectures. Further research is needed to overcome or mitigate the fundamental rate-distance trade-off before satellite QKD can be considered practicable in an IoT application. Alternatives that do not rely on trusted nodes are contingent on nascent technologies such as quantum repeaters and quantum memory. Whilst in theory QKD provides perfect information-theoretic security, it remains vulnerable to attacks that exploit imperfections in real-world equipment. Further effort is needed to develop QKD protocols that can safeguard against the aforementioned challenges.

Keywords: Internet of Things, satellite communications, quantum cryptography, quantum key distribution

1. Introduction

The Internet of Things (IoT) describes a family of technologies which enable physical "things" to sense and affect the world around them in an intelligent way, by communicating over the internet and processing information in the cloud. In this paper, we adopt the term *Machine-Type Device (MTD)* from Centenaro et al. (2021) to refer to a "thing" in the IoT network.

The number of MTDs connected to the Internet is rising rapidly. From 2016 to 2020, the total number of connected devices in the IoT rose from approximately 7 billion to more than 20 billion, and the number of connected devices per person increased from 0.8 to almost 3 over the same period (Cheng et al., 2017). This scale of networking presents a massive attack surface. There is a growing economic impetus to integrate IoT networks on a global scale using satellites to handle backhaul traffic (i.e., aggregated traffic between gateways in the IoT network) because the satellites can greatly expand the range of IoT services into remote or wide-spread areas, where wholly terrestrial networks are impracticable (Centenaro et al., 2021). Therefore, there is a strong motivation to find ways to guarantee the security of satellite-integrated IoT protocols well into the future.

Current techniques for securing IoT traffic rely on a public-key infrastructure and exploit the innate intractability of certain one-way (mathematical) functions, used in cryptography to ensure that unauthorised decryption is intractable to probabilistic polynomial-time adversaries (Diamanti et al., 2016). However, the rise of quantum computing threatens to undermine the efficacy of pre-quantum cryptographic schemes (i.e., cryptographic schemes designed without consideration of attacks using quantum computing). Shor's (1994) algorithm can provide superpolynomial speedup to classical algorithms for breaking (i) cryptosystems based on the RSA problem (e.g., RSA cryptosystems) and (ii) cryptosystems based on the discrete logarithm problem (e.g., elliptic-

curve cryptosystems, Diffie-Hellman key agreement); see (Bernstein and Lange, 2017). In particular, Gidney and Ekerå's (2021) implementation of Shor's algorithm can factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Grover's (1996) algorithm reduces the effective size of symmetric keys by half. The existence of these algorithms proves that the rise of quantum computing poses a serious threat to traditional secure communication protocols, including those used by satellite-integrated IoT networks.

There is a great deal of research currently underway to develop solutions that mitigate the emerging threat of quantum computing to traditional data security paradigms. The research can be divided into two main streams:

1. **Post-quantum cryptography (PQC)**: Also known as quantum-resistant cryptography (QRC), this refers to the design and development of computationally secure cryptographic schemes against which quantum-computing adversaries have no intrinsic advantage over classical adversaries. In 2016, NIST initiated a process to develop and standardise quantum-resistant public-key cryptographic algorithms to augment existing public-key cryptographic standards. In 2022, after three review rounds, four algorithms were selected to be standardised and four other algorithms were shortlisted for further reviews (Alagic et al., 2022). One of the shortlisted candidates, namely Supersingular Isogeny Key Encapsulation (SIKE), was recently broken (Castryck and Decru, 2022), serving as a reminder of the challenges of basing cryptographic algorithms on hard computational problems.
2. **Quantum cryptography**: Unlike cryptographic schemes that rely on computational intractability to deter attackers, quantum cryptography makes use of the fundamental physical properties of quantum mechanics to achieve information-theoretic or unconditional security.

The need to develop PQC is urgent, and in some areas, it may already be too late to protect the confidentiality of data. The fields of quantum computing and PQC are in a horse-race to see which will be ready first. The parameters of the race are illustrated in Figure 1, where the start line is an arbitrary point in time before quantum computing and PQC reach maturity. The distance to the finish line is determined by the developments needed to make PQC a practical reality. Confidence in the security of a PQC algorithm takes time to grow even after the algorithm has been standardised, because it is proportional to the time the algorithm stays undefeated. PQC cryptosystems need to be integrated with existing standards/protocols if feasible, or otherwise new standards/protocols will need to be designed and developed (Bernstein et al., 2022). Despite their resource constraints, IoT devices will need to implement both pre-quantum and post-quantum cryptographic schemes (Fernández-Caramés, 2020). If a large-scale quantum computing system becomes practicable before then, global data security is at risk on an unprecedented scale.

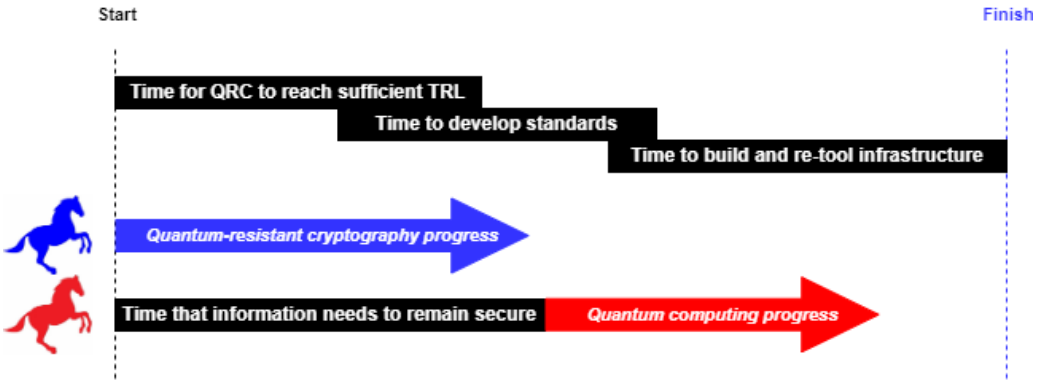

Figure 1: Illustration of the 'horse-race' metaphor between quantum computing and PQC progress.

The threat to global data security in fact more pressing than the preceding discussion would suggest, due to regulatory requirements on the length of time for which data needs to remain secure. Information that is transmitted over the IoT, even up to the day before PQC is fully in place, can still be harvested, stored and decrypted later once quantum computing reaches large-scale. For this analysis, "large-scale" refers to quantum computers of sufficient complexity to run Shor's algorithm. Quantum computing essentially has a head start equal to the maximum duration of time that electronic records need to remain secure. For example, for credit card information, this could be as little as one year, and for medical records it could be as much as 99 years (Commonwealth of Australia. *Archives Act 1983*).

The most widely studied and technologically mature sub-topic of quantum cryptography is quantum key distribution (QKD). QKD exploits the quantum mechanical properties of the Heisenberg uncertainty principle

and/or entanglement to encode a secret key using quantum states which are transmitted over a quantum channel that is theoretically immune to passive eavesdropping. These principles and their application to QKD will be described in Section 3.

QKD has been successfully applied to optical fibre networks for years, and QKD-enabled systems are offered as turn-key solutions for terrestrial networks. However, research into the application of QKD to wireless networks is still in its infancy, and application to satellite communications is lagging even further.

Nordholt et al.'s (2002) experiment first showed that QKD can be effectively utilised over a terrestrial free-space optical link. The experiment involved transmitting single photons with modulated polarisations from one place to another on the Los Alamos National Laboratory site. The researchers surmised that the technique could extend equally well to low-Earth orbit (LEO) distances.

More recently, there have been QKD experiments performed on actual space-ground optical downlinks from LEO, most notably using the satellite *Micius* under the auspices of the Chinese QUESS program (Liao et al., 2017) and *Tiangong-2 Space Lab* (Li et al., 2022). These experiments show that whilst their key generation rate is still too miniscule to be useful in an IoT backhaul application, the concept of satellite-based QKD is at least feasible and now needs only to be scaled up.

One of the main technical challenges limiting the deployment of QKD is the fundamental rate-distance trade-off. The path loss resulting from decoherence of entangled photons scales exponentially with distance, and hence the achievable secret key generation rate decreases exponentially with distance, even in free space (Takeoka et al., 2014). This limits the separation of two QKD-enabled communicating nodes to an order of hundreds of kilometres (Azuma et al., 2016). The use of a daisy chain of repeaters, in the traditional sense, to boost the range is untenable, due to the *no-cloning theorem*, a fundamental tenet of quantum mechanics which states that it is not possible to create a perfect copy of a quantum state (Wootters and Zurek, 1982). There is promising research into the development of a quantum version of the classical repeater, however such a repeater relies on the use of quantum memory for synchronisation purposes, which is still a nascent technology (Mastriani and Iyengar, 2020).

Only a handful of papers have considered the application of QKD to satellite-integrated IoT, and of those, most discuss it only in passing. Djordjevic (2020b) underscores the applicability of quantum methods to IoT, but does not specifically address the challenges of implementing quantum techniques to secure satellite-integrated IoT networks. It is apparent that whilst QKD is the most mature of the quantum cryptographic technologies under development, there is still a general lack of treatment in the literature on the viability and challenges in applying QKD specifically to the satellite-integrated IoT context. This paper seeks to provide a starting point for more focused research and development into this application area in the future.

2. Satellite IoT

There are two principal topologies for satellite-integrated IoT networks. In direct-to-satellite IoT, a satellite up-link is established directly from IoT device(s). In an indirect-access architecture, data from IoT devices is aggregated in the Network Layer using an LPWAN protocol such as LoRaWAN before being sent to a satellite for further routing (Fraire et al., 2019). At the destination, the data moves up the protocol stack to the Application and Business Layers (Zhou et al., 2021). Satellites are ideal for providing IoT connectivity in remote locations and/or over wide geographic areas where terrestrial communication technologies are impractical (Centenaro et al., 2021).

The four main security objectives for wireless networks (Zou et al., 2016) are equally applicable to satellite communications:

- **Confidentiality** - ensuring that unauthorised parties cannot decipher the communications between authorised parties involved in the communication session.
- **Integrity** - ensuring that all data transmitted by the sender is delivered intact, without modification, omission, or addition, to the recipient.
- **Authenticity** - ensuring that all parties involved in a communication session are who they claim to be.
- **Availability** - ensuring that a session can be set-up on demand and maintained for the required duration to enable communication to take place.

QKD can provide provable guarantees about the confidentiality and integrity of secret key exchange but does not address authenticity and availability requirements. However, there are choices that can be made in the architectural design of a QKD system to help ensure availability of the quantum channel, as we will discuss later.

3. Quantum Key Distribution

Quantum key distribution (QKD) is a method for generating and distributing symmetric cryptographic keys with information-theoretic security based on quantum information theory (ETSI, 2018). QKD typically uses a quantum channel in parallel with an authenticated classical channel to share a secret key between two parties (see **Error! Reference source not found.**). The secret key is encoded in the quantum states of photons transmitted over the quantum channel. The authenticated classical channel is used to exchange measurement metadata between authorised users to remove errors and recover a shared key from the randomised 'raw key' through a process known as 'sifting'.

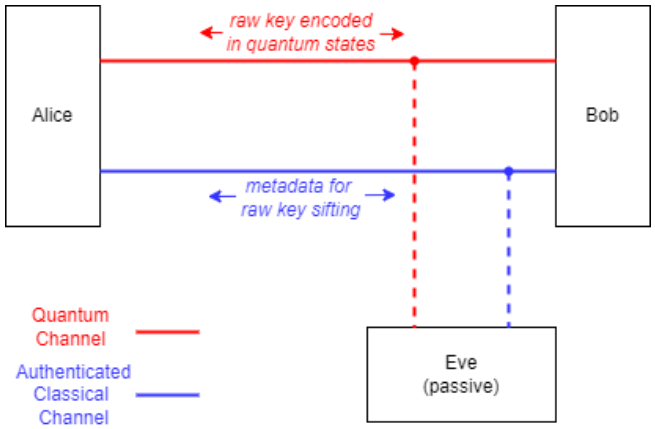

Figure 2: Block diagram showing a QKD system in a highly generalised form

QKD can be divided into the discrete-variable regime (DV-QKD) and the continuous-variable regime (CV-QKD); see (Hosseinidehaj et al., 2019) for a summary of the differences between the two regimes. In the discrete-variable regime, bits making up the raw key are encoded onto the discrete quantum states of a single photon, either by manipulating its polarisation or its phase. DV-QKD is typically realised using single photon sources and single photon detectors. By contrast, in the continuous-variable regime, the raw key is encoded in the quadratures of the optical field, which comprises many photons and can thus take on a continuous value in practical terms. CV-QKD is typically realised using either homodyne or heterodyne detectors at the receiver and promises a much higher potential key generation rate than DV-QKD, making it well-suited to handling the high volume of traffic through an IoT backhaul.

DV-QKD can be further divided into protocols that use a 'prepare-and-measure' approach and protocols that are based on quantum entanglement. In a 'prepare-and-measure' protocol – illustrated schematically in **Error! Reference source not found.** – Alice prepares a random sequence of quantum states. These are then transmitted over the quantum channel and Bob measures the quantum states to recover the raw key. In an entanglement-based protocol, a common source of entangled photon pairs distributes one photon each to Alice and Bob. The entanglement-based scheme obviates the need for random number generation in the coding and decoding process and allows Alice and Bob to use identical optical receiver architectures (Bedington et al., 2017).

Since the inception of the first QKD protocol in 1984, there has been a proliferation of protocols that aim to address the various weaknesses discovered in their predecessors, as the eternal cat-and-mouse game between attackers and defenders is played out in this new arena. Figure 2 depicts the evolution of some of the most significant QKD protocols since 1984 and categorises them according to whether they are continuous or discrete, and further whether they use a prepare-and-measure or entanglement principle. A summary of the major-milestone protocols follows.

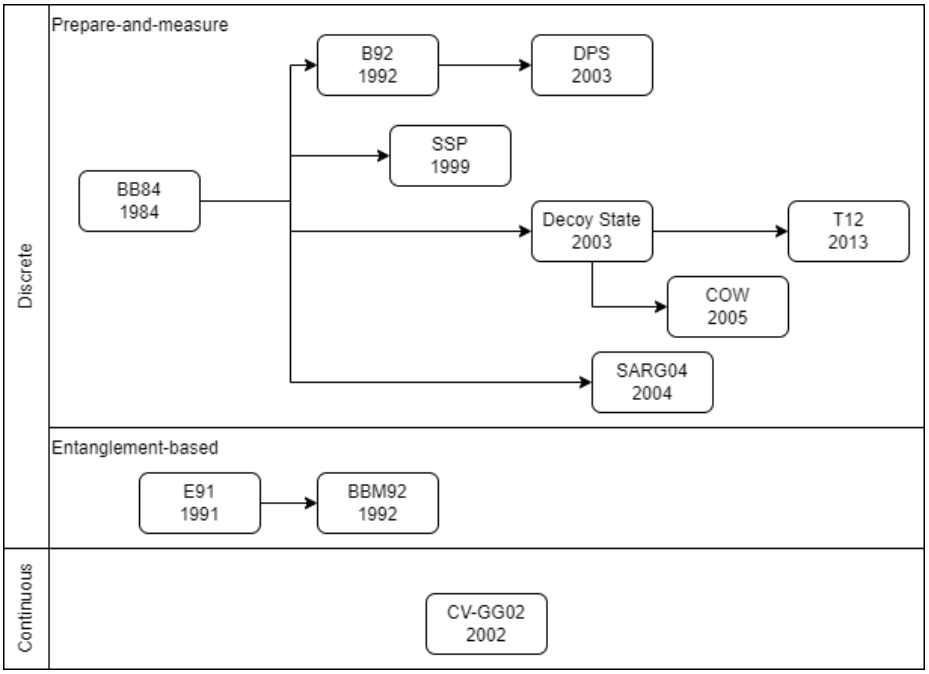

Figure 2: Classification and evolution of major-milestone QKD protocols.

The first QKD protocol to emerge was BB84, a prepare-and-measure type of DV-QKD, which encodes the raw key using the polarisation of single photons into one of four orthogonal states (Bennet and Brassard, 1984). E91 was the first protocol to use a common source of entangled photons, allowing Alice and Bob to use identical optical hardware (Ekert, 1991). The Decoy State protocol (Hwang, 2003) and SARG04 (Scarani et al., 2004) were developed in response to the vulnerability of BB84 to the photon-number splitting (PNS) attack. In a PNS attack, the attacker exploits the imperfections of real single photon sources. In general, single photon sources are imperfect, and sometimes emit more than one photon at a time. These clusters of photons share identical quantum states, and hence eavesdropper Eve can measure and recover information from one or more of the extraneous photons without violating the no-cloning theorem and without alerting Alice and Bob to her presence (Diamanti et al., 2016). This completes a non-exhaustive round-up of the watershed protocols in DV-QKD, but before moving on to the more esoteric subject of CV-QKD, it behoves us to provide a basic description of the mechanism by which DV-QKD achieves privacy against passive eavesdropping.

A single photon can exist in any one of a continuum of polarisation states, which can be thought of as the orientation of its electric field vector. When 'prepared'

- in a rectilinear basis, a photon becomes polarised either horizontally (encoding '0') or vertically (encoding '1');
- in a diagonal basis, a photon becomes polarised at either 45° (encoding '0') or 135° (encoding '1').

In the prepare-and-measure paradigm,

- Alice prepares a photon using a randomly selected polarisation basis, which is either rectilinear or diagonal, and transmits it to Bob.
- Bob then measures the photon using a randomly selected basis, which is either rectilinear or diagonal.

In the absence of Eve, if Bob happens to select the same basis as Alice's, then he can decode the photon's polarisation state into the right value (e.g., '0' for horizontal polarisation in the rectilinear basis); otherwise, Bob obtains the same value as Alice's at 0.5 probability. Now if Eve is interposed in the quantum channel and makes a measurement of the transmitted photon (see Figure 3), she may alter the photon's polarisation state such that Bob decodes it into a different value than Alice's even when he uses the same basis as Alice's.

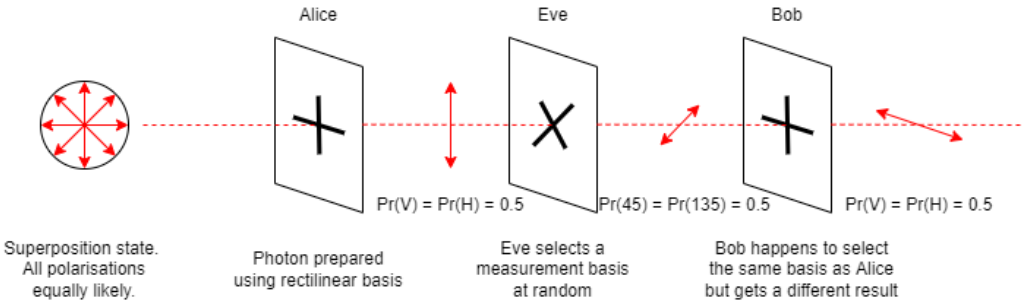

Figure 3: Passive eavesdropper detection in BB84.

Even when using the same basis, Alice and Bob obtain different values, which is an indication that the message may have been intercepted and hence altered by an eavesdropper.

Fundamentally, if a photon is first measured using the rectilinear basis, and then subsequently measured using the 'incompatible' diagonal basis, then the probability of finding the photon in any given state is 'reset'. Due to the Heisenberg uncertainty principle, the second, incompatible measurement disturbs the system in a way that creates maximum uncertainty of the measurement outcome (Wojcieszyn, 2022). This point is vital for understanding the security boon of QKD, because it means that an eavesdropper cannot intercept the raw key transmission without risking altering it in the process.

4. Application of QKD to Satellite IoT

Below, we assess each of the system parameters of QKD in turn in terms of potential performance and technical practicability.

Satellite access mode – direct vs indirect:
In a direct-access (a.k.a. direct-to-satellite) architecture, the satellite – typically in a LEO for the benefit of low latency – serves as the gateway, and the IoT devices communicate directly with the satellite. This provides the benefits of connecting geographically dispersed devices without the need for terrestrial infrastructure. This is particularly useful for ad hoc networks or geographically dispersed devices.

This requires the IoT device to have an onboard QKD module in addition to all the hardware necessary to establish and maintain an optical satellite connection, including (i) a telescope and (ii) a pointing, acquisition and tracking (PAT) system. The alternative, which is a far more plausible scenario for QKD, is an indirect-access scheme whereby IoT devices communicate with a terrestrial gateway, e.g., a cellular base station. The backhaul traffic from the base station is then carried via satellite.

See (Fraire et al., 2019) for a comparative analysis of the benefits and challenges associated with direct-to-satellite and indirect-to-satellite architectures for IoT networks.

QKD link direction – uplink vs downlink:
The raw key can be distributed via either an uplink or a downlink. A downlink is less lossy because beam wander occurs only over the last few km of the propagation path. Moreover, downlink QKD is less prone to denial-of-service attacks because the satellite only has a transmitter; an attacker aiming a high-intensity photon source at the satellite serves no purpose. It is also easier to build a large-aperture receiver (telescope) on a ground station than to deploy it in space. The principal advantage of the uplink scheme is that attackers have constrained physical access to tamper with an in-orbit receiver (Bedington et al., 2017).

Trusted Node relay:
Also known as a 'flying trusted node' architecture, the satellite establishes independent keys with Alice and Bob. Alice only knows the key she established with the satellite, and Bob only knows the key he established with the satellite. The general sequence is outlined as follows (Bedington et al., 2017):

1. Trusted relay establishes secure key with Alice, k_A.
2. Trusted relay establishes secure key with Alice, k_B.
3. Trusted relay combines the two keys: $k = k_A \oplus k_B$, where $\oplus$ denotes the exclusive-OR operation.

4. Parity announcement: the trusted relay distributes the combined key, k, to both Alice and Bob over the classical channel.
5. Alice recovers Bob's key from the combined key: $k_B = k_A \oplus k$.
6. Bob recovers Alice's key from the combined key: $k_A = k_B \oplus k$.
7. Alice can now use Bob's key to encrypt her plaintext for Bob, and vice versa.

Untrusted relays using quantum repeaters:
One of the fundamental problems with all forms of QKD, no matter the protocol used, is the rate-distance trade-off, which is well described in the literature. The key generation rate decays exponentially with distance, which indicates the need for a repeater chain to achieve global coverage (Takeoka et al., 2014). Whilst a conventional repeater in a communications network generally involves receiving, amplifying, and then re-transmitting a signal, the no-cloning theorem of quantum mechanics means that it is impossible for a repeater node to produce an exact copy of a quantum state for retransmission. One way around this problem is to establish a network of trusted node relays, which would decrypt the ciphertext and then establish a new key and re-transmit to the next node in the chain, but then these are no longer just repeaters, and it places additional security requirements on the space segment of the network. The ideal solution would be to use a network of untrusted repeaters, and recent developments in quantum physics research suggest that this may be feasible and even practicable in the near future (Mastriani and Iyengar, 2020). Quantum repeaters are based on the principle of *entanglement swapping* (see Definition 1), which currently is dependent on the development of quantum memory to overcome the problem of asynchronous photon arrival time, but this is a highly active area of research and progress is being made (Takeoka et al., 2014).

Definition 1: *Entanglement swapping* is a process whereby a pair of independently generated photons can be entangled so that they have correlated quantum states (Pan et al., 1998). This process can be repeated multiple times to effectively extend the range of a quantum transmission system, and is the key principle behind quantum repeater technology and for overcoming the rate-distance trade-off.

Untrusted relays using MDI-QKD:
In an alternative approach to realising an untrusted relay network architecture, namely a measurement-device-independent QKD (MDI-QKD) protocol, a third party (Charlie), who need not be trustworthy, is responsible for making all measurements on the quantum state of the encoded raw key (Hosseinidehaj and Malaney, 2017). Alice and Bob both prepare randomised quantum states using pre-agreed bases, and transmit them to Charlie, who measures the correlations between the signals from Alice and Bob, and then announces the correlations over an unsecure channel. If the correlation is high, Alice and Bob know that they have agreed on the same bit, but nobody else knows what that bit is; not even Charlie, who can only measure the superposition of Alice and Bob's signals but is unable to separate them.

Continuous-variable vs discrete-variable protocols:

All DV-QKD schemes suffer from the problem of losing photons over free-space transmission through the atmosphere. Dust and cloud cause loss of photons (Mastriani and Iyengar, 2020), severely limiting the key generation rate. DV-QKD protocols are better suited to terrestrial fibre transmission than long-distance free-space communications because loss of photons in the former is appreciably less. Moreover, when single-photon detectors are used, there is a certain amount of 'dead time', which can significantly hold back the maximum achievable baud rate (Djordjevic, 2020a). Thus, we propose that the satellite-integrated IoT infrastructure of the future will require the adoption of CV-QKD protocols to cope with backhaul demands.

Key Generation – synchronous vs stockpiled:
In the synchronous scheme, the connection is established on demand, and the secret key is generated in real time. This most closely resembles the format of present-day public-key infrastructure, where keys are generated on demand. However, this would work only if the secret key generation rates were sufficient to handle real-time IoT bandwidth requirements, and present demonstrations fall far short of this. Synchronicity also requires implementation of a globe-spanning constellation with either a relay of trusted nodes or untrusted repeaters.

The alternative is an asynchronous scheme, whereby a one-time pad is (i) accumulated whenever line-of-sight over a ground station is available and (ii) stockpiled for later user. This could in principle be realised using only a

single CubeSat in polar orbit to distribute a secure key using QKD to any two points on the globe (Sidhu et al., 2022). Keys are retrieved from storage and used for encryption/decryption as needed.

In Table 1, we synthesise two possible solutions for a globe-spanning QKD-secured satellite-integrated IoT network. The first is an ultimate solution (red dots ●) for implementing QKD security for satellite-integrated IoT backhaul – although this one might be many years off due to the nascent nature of certain technologies. And in the other (blue dots ●) we propose a solution that might be more attainable in the near-term and begin to satisfy the potentially urgent need for quantum-resistant cryptography.

Table 1: QKD architecture synthesis summary.

Parameter	Option 1	Option 2
Satellite access method	Direct-to-satellite	Indirect ● ●
Space segment security	Trusted relay ●	Untrusted ●
QKD link direction	Uplink	Downlink ● ●
Key generation	Synchronous ●	Stockpiled ●
Encoding basis	Discrete variable (DV) ●	Continuous variable (CV) ●

Several experiments have been carried out in recent years that lend credence to the concept of a satellite-based QKD network supporting an indirect-access architecture. All three of the examples listed below use the parameter set indicated by the blue dots (●) in Table 1.

In the first full-scale practical demonstration of satellite-based QKD, Liao et al. (2017) showed that a sat-to-ground data link can be established with a 1 kbps data rate over a range of 1200 km, during the testing of their satellite Micius in 2015. The window of effective key transfer was 273 seconds, and at a single fly-over per night, this resulted in a total key rate of 273 kb/night/satellite. Although this experiment was limited to only one node in the space segment, one can imagine extending this technology to a globe-spanning satellite constellation, where the inter-satellite links are secured using QKD.

Modelling performed by Mazzarella et al. (2020) as part of the QUARC project showed that a constellation of 15 CubeSats would be sufficient to provide a QKD-secured service to the UK with reasonable availability and key generation rate. They modelled a trusted relay network using Decoy State DV-QKD and managed to achieve a best-case key generation rate of 300 kb/night/satellite. This was based on a highly conservative assumption that interference prohibits transmission during the daytime or twilight hours.

Tiangong-2 Space Lab is a Chinese space station orbiting in a LEO at medium inclination. It has been used as a testbed for a trusted relay for a QKD experiment, achieving a sifted key generation rate of 1.33 Mb per day under best-case conditions (Li et al., 2022). This experiment showed that by combining satellites in sun synchronous orbit (SSO) and medium inclination orbit (MIO), a higher overall key rate per day can be achieved due to the multi-pass benefit of MIOs. A sun-synchronous orbit is a polar orbit (approximately 90° inclination) with a precession synchronised to the revolution of the earth around the sun, so that a satellite in SSO can be both exposed to the sun at all times for power generation, and have line-of-sight to the dark side of the Earth for clarity of optical communications at the same time.

Table 2 summarises the important performance figures achieved in the experiments discussed above.

Table 2: Summary of recent milestones in satellite-based QKD performance.

Experiment	Year	Location	Orbital Height (km) at zenith	Best Key Rate (kb/sat/night)	Reference
Micius (QUESS)	2017	Xinglong, China	500	300	Liao et al., 2017
QUARC	2020	Southeast England	574	300*	Mazzarella et al., 2020
Tiangong-2	2022	Nanshan, China	400	1330	Li et al., 2022

*The QUARC result is based on modelling and simulation rather than real-world experimental data.

5. Concluding remarks

We have established the need and urgency for PQC and provided a light introduction to QKD in its multitudinous forms. The security of current cryptosystems such as RSA is predicated on the absence of efficient solutions to some computational problems, but efficient solutions may become available with or without quantum computing. In contrast, QKD leverages quantum-mechanical properties to achieve information-theoretic

security. Having explained some of the variations in architectural design that are possible within QKD, we have provided some recent examples of practical demonstrations of the technology that lend credence to its viability for securing IoT backhaul over satellites in the future. We proposed two possible architectures for satellite-integrated IoT using QKD, one near-term and one longer-term. The ideal QKD architecture from a security perspective is one involving a relay of untrusted quantum repeaters establishing point-to-point secure keys between terrestrial IoT gateways over an optical (quantum) channel. Synergy among pre-quantum cryptography, PQC and QKD are required to achieve security against classical and quantum adversaries. Side-channel attacks are applicable to all cryptographic paradigms and hence comprehensive vulnerability assessments must accompany advances in QKD implementation (Sajeed et al., 2021).

References

Alagic, G., Apon, D., Cooper, D., et al. (2022) 'Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process', NISTIR 8413-upd1. DOI: 10.6028/NIST.IR.8413-upd1.

Azuma, K., Mizutani, A. and Lo, H.-K. (2016) 'Fundamental rate-loss trade-off for the quantum internet', *Nature Communications*, vol. 7, no. 1, p. 13523. DOI: 10.1038/ncomms13523.

Bedington, R., Arrazola, J. M. and Ling, A. (2017) 'Progress in satellite quantum key distribution', *npj Quantum Information*, vol. 3, no. 1, p. 30. DOI: 10.1038/s41534-017-0031-5.

Bennett, C. H. and Brassard, G. (1984) 'Quantum cryptography: Public key distribution and coin tossing', *Theoretical Computer Science*, vol. 560, pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

Bernstein, D. J., Hülsing, A., Lange, T. and Rekleitis, E. (2022) 'Post-quantum cryptography: integration study', European Union Agency for Cybersecurity. Available at https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study/@@download/fullReport.

Bernstein, D. J. and Lange, T. (2017) 'Post-quantum cryptography', *Nature*, vol. 549, no. 7671, pp. 188–194. DOI: 10.1038/nature23461.

Cao, Y., Zhao, Y., Wang, Q., et al. (2022) 'The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet', *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894. DOI: 10.1109/COMST.2022.3144219.

Castryck, W. and Decru, T. (2022) 'An efficient key recovery attack on SIDH (preliminary version)', Cryptology ePrint Archive, Paper 2022/975. Available at https://ia.cr/2022/975.

Centenaro, M., Costa, C. E., Granelli, F., et al. (2021) 'A Survey on Technologies, Standards and Open Challenges in Satellite IoT', *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1693–1720. DOI: 10.1109/COMST.2021.3078433.

Cheng, C., Lu, R., Petzoldt, A. and Takagi, T. (2017) 'Securing the Internet of Things in a Quantum World', *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116–120. DOI: 10.1109/MCOM.2017.1600522CM.

Commonwealth of Australia. *Archives Act 1983:* C2021C00366 (No. 79, 1983) Canberra, Office of Parliamentary Counsel.

Diamanti, E., Lo, H.-K., Qi, B. and Yuan, Z. (2016) 'Practical challenges in quantum key distribution', *npj Quantum Information*, vol. 2, no. 1, p. 16025. DOI: 10.1038/npjqi.2016.25.

Djordjevic, I. B. (2020a) 'Hybrid QKD Protocol Outperforming Both DV- and CV-QKD Protocols', *IEEE Photonics Journal*, vol. 12, no. 1, pp. 1–8. DOI: 10.1109/JPHOT.2019.2946910.

Djordjevic, I. B. (2020b) 'Secure, Global Quantum Communications Networks', *22nd International Conference on Transparent Optical Networks (ICTON)*, IEEE, pp. 1–5. DOI: 10.1109/ICTON51198.2020.9203116.

Ekert, A. K. (1991) 'Quantum cryptography based on Bell's theorem', *Phys. Rev. Lett.*, American Physical Society, vol. 67, no. 6, pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

ETSI (2018) 'Quantum Key Distribution (QKD); Vocabulary', Group Report reference DGR/QKD-0007_Ontology V1.1.1. https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_qkd007v010101p.pdf.

Fernández-Caramés, T. M. (2020) 'From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things', *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480. DOI: 10.1109/JIOT.2019.2958788.

Fraire, J. A., Céspedes, S. and Accettura, N. (2019) 'Direct-To-Satellite IoT - A Survey of the State of the Art and Future Research Perspectives: Backhauling the IoT Through LEO Satellites', in *Ad-Hoc, Mobile, and Wireless Networks*, Lecture Notes in Computer Science, Springer International Publishing, vol. 11803, pp. 241–258. DOI: 10.1007/978-3-030-31831-4_17.

Gidney, C. and Ekerå, M. (2021) 'How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits', *Quantum*, Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften, vol. 5, p. 433. DOI: 10.22331/q-2021-04-15-433.

Grover, L. K. (1996) 'A fast quantum mechanical algorithm for database search', *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, ACM Press, pp. 212–219. DOI: 10.1145/237814.237866.

Hosseinidehaj, N. and Malaney, R. (2017) 'CV-MDI Quantum Key Distribution via Satellite', *Quantum Info. Comput.*, vol. 17, no. 5–6, pp. 361–379. DOI: 10.26421/QIC17.5-6-1. Available at 10.48550/ARXIV.1605.05445.

Hosseinidehaj, N., Babar, Z., Malaney, R., et al. (2019) 'Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook', *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919. DOI: 10.1109/COMST.2018.2864557.

Hwang, W.-Y. (2003) 'Quantum Key Distribution with High Loss: Toward Global Secure Communication', *Physical Review Letters*, vol. 91, no. 5, p. 057901. DOI: 10.1103/PhysRevLett.91.057901.

Liao, S.-K., Yong, H.-L., Liu, C., et al. (2017) 'Long-distance free-space quantum key distribution in daylight towards inter-satellite communication', *Nature Photonics*, vol. 11, no. 8, pp. 509–513. DOI: 10.1038/nphoton.2017.116.

Li, Y., Liao, S.-K., Cao, Y., et al. (2022) 'Space–ground QKD network based on a compact payload and medium-inclination orbit', *Optica*, vol. 9, no. 8, p. 933. DOI: 10.1364/OPTICA.458330.

Mastriani, M. and Iyengar, S. S. (2020) 'Satellite quantum repeaters for a quantum Internet', *Quantum Engineering*, vol. 2, no. 4. DOI: 10.1002/que2.55.

Mazzarella, L., Lowe, C., Lowndes, D., et al. (2020) 'QUARC: Quantum research Cubesat—A constellation for quantum communication', Cryptography, vol. 4, no. 1. DOI: 10.3390/cryptography4010007.

Nordholt, J. E., Hughes, R. J., Morgan, G. L., et al. (2002) 'Present and future free-space quantum key distribution', Mecherle, G. S. (ed), San Jose, CA, pp. 116–126. DOI: 10.1117/12.464085.

Pan, J.-W., Bouwmeester, D., Weinfurter, H. and Zeilinger, A. (1998) 'Experimental Entanglement Swapping: Entangling Photons That Never Interacted', *Physical Review Letters*, vol. 80, no. 18, pp. 3891–3894. DOI: 10.1103/PhysRevLett.80.3891.

Sajeed, S., Chaiwongkhot, P., Huang, A., et al. (2021) 'An Approach for Security Evaluation and Certification of a Complete Quantum Communication System', *Scientific Reports*, vol. 11, no. 1, p. 5110. DOI: 10.1038/s41598-021-84139-3.

Scarani, V., Acín, A., Ribordy, G. and Gisin, N. (2004) 'Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations', *Physical Review Letters*, vol. 92, no. 5, p. 057901. DOI: 10.1103/PhysRevLett.92.057901.

Shor, P. W. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

Sidhu, J. S., Brougham, T., McArthur, D., et al. (2022) 'Finite key effects in satellite quantum key distribution', *npj Quantum Information*, vol. 8, no. 1, p. 18. DOI: 10.1038/s41534-022-00525-3.

Takeoka, M., Guha, S. and Wilde, M. M. (2014) 'Fundamental rate-loss tradeoff for optical quantum key distribution', *Nature Communications*, vol. 5, no. 1, p. 5235. DOI: 10.1038/ncomms6235.

Wojcieszyn, F. (2022) *Introduction to Quantum Computing with Q# and QDK*, Springer Nature. DOI: 10.1007/978-3-030-99379-5.

Wootters, W. K. and Zurek, W. H. (1982) 'A single quantum cannot be cloned', *Nature*, vol. 299, no. 5886, pp. 802–803. DOI: 10.1038/299802a0.

Zhou, I., Makhdoom, I., Shariati, N., et al. (2021) 'Internet of Things 2.0: Concepts, Applications, and Future Directions', *IEEE Access*, vol. 9, pp. 70961–71012. DOI: 10.1109/ACCESS.2021.3078549.

Zou, Y., Zhu, J., Wang, X. and Hanzo, L. (2016) 'A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends', *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765. DOI: 10.1109/JPROC.2016.2558521.