A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography

Nick Aquina[1,3†], Bruno Cimoli[1,3†], Soumya Das[2,3†], Kathrin Hövelmanns[2,3†], Fiona Johanna Weber[2,3†], Chigo Okonkwo[1,3], Simon Rommel[1,3], Boris Škorić[2,3], Idelfonso Tafur Monroy[1,3], Sebastian Verschoor[4]

[1]Department of Electrical Engineering, Eindhoven University of Technology, Flux Building, Eindhoven, 5612 AZ, The Netherlands.
[2]Department of Mathematics and Computer Science, Eindhoven University of Technology, MetaForum Building, Eindhoven, 5612 AZ, The Netherlands.
[3]Eindhoven Quantum Hub, Eindhoven University of Technology, Qubit Building, Eindhoven, 5612 AZ, The Netherlands.
[4]Informatics Institute, University of Amsterdam, Science Park 904, 1098 XH Amsterdam, The Netherlands.

Contributing authors: n.aquina@tue.nl; b.cimoli@tue.nl; s.das2@tue.nl; kathrin@hoevelmanns.net; crypto@fionajw.de;
†These authors contributed equally to this work.

Abstract

Quantum Key Distribution (QKD) is currently being discussed as a technology to safeguard communication in a future where quantum computers compromise traditional public-key cryptosystems. In this paper, we conduct a comprehensive security evaluation of QKD-based solutions, focusing on real-world use cases sourced from academic literature and industry reports. We analyze these use cases, assess their security and identify the possible advantages of deploying QKD-based solutions. We further compare QKD-based solutions with Post-Quantum Cryptography (PQC), the alternative approach to achieving security when quantum computers compromise traditional public-key cryptosystems, evaluating their respective suitability for each scenario. Based on this comparative analysis, we critically discuss and comment on which use cases QKD is suited for, considering factors such as implementation complexity, scalability, and long-term security. Our findings contribute to a better understanding of the role QKD could play in future cryptographic infrastructures and offer guidance to decision-makers considering the deployment of QKD.

Keywords: Quantum Key Distribution, Quantum communications, Quantum cryptography, Quantum Network, Use-cases, Post-Quantum Cryptography, Harvest-Now-Decrypt-Later attack

1 Introduction

Heavy corporate and public investments are accelerating the development of large-scale quantum computers [1, 2]. This development threatens the confidentiality of current data transmissions because sufficiently powerful quantum computers could break certain cryptographic algorithms [3] that currently are widely used. Importantly, this is not only a threat to future data, but also to data encrypted today: in a so-called HNDL (Harvest-Now-Decrypt-Later) attack, attackers record data

on transit and decrypt the data once a quantum computer becomes available, thereby breaching confidentiality retroactively [4]. While such attacks compromise confidentiality, they do not enable retroactive breaches of authentication (e.g., impersonation), as authentication relies on real-time verification during the interaction. To protect confidential communication against quantum attacks, it is necessary to overhaul current cryptographic solutions. Currently, the main overhaul strategies in discussion are a), replacing the broken algorithms with still-classical algorithms that are secure against quantum attacks (so-called PQC (Post-Quantum Cryptography)), b), utilize QKD (Quantum Key Distribution), and additionally, using mixes of both [5, 6].

PQC essentially allows to maintain already established security infrastructures (with some caveats concerning compatibility), and the first PQC solutions have recently been standardized [7]. At the same time, PQC is not unconditionally secure and future algorithmic breakthroughs could occur, one thus cannot unconditionally rule out HNDL attacks [8], even ones run on classical computers. While QKD-based solutions theoretically overcome this limitation of PQC, they will introduce significant changes to security infrastructures and are not yet fully standardized [9, 10], though several solutions have been demonstrated at different locations around the world. QKD currently exhibits practical limitations that public-key cryptography does not have – first, QKD is limited in distance and until quantum repeaters [11] are developed, QKD cannot provide end-to-end security over long distances, and, second, wireless QKD technologies currently only exist with free space optics, where photons are sent over the air [12], making it incompatible with the currently predominant radio networks. These limitations restrict the use cases in which QKD can be applied and prevent QKD from serving as a general-purpose replacement for public-key cryptography. Additionally, information cannot be protected with QKD alone – to ensure confidentiality and authenticity, it has to be used in conjunction with quantum-secure authentication and quantum-secure symmetric encryption. To assess which level of security can be guaranteed for a concrete use case, it is necessary to account for *all* involved cryptographic algorithms and *all* underlying assumptions. Assessments that account for this fuller picture help clarify the comparison between QKD-based solutions and solutions that do not involve QKD. This also paves the way towards a comparison between QKD-based solutions and solutions stemming from PQC, on a case-by-case basis.

Most governmental bodies that have commented on the choice between QKD and post-quantum asymmetric cryptography currently prefer the latter: The US National Security Agency (NSA) considers post-quantum cryptography to be 'more cost-effective and easily maintained' and 'does not support the use of QKD to protect communications in national security systems' [13]. Their criticism about QKD are addressed in detail in [14]. In a joint position document, the French Cybersecurity Agency (ANSSI), the German Federal Information Security Office (BSI), the Netherlands National Communications Security Agency (NLNCSA) and the Swedish National Communications Security Authority declare 'the clear priority should [...] be the migration to post-quantum cryptography' and state that QKD can 'due to current and inherent limitations [...] currently only be used in practice in some niche use cases' [8]. However, they also state that 'research on this topic should be continued in order to investigate if there are ways to overcome some of the limitations of the current technology'. The British National Cyber Security Centre (NCSC) published a statement stating that 'the NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical networks' and instead advises 'that the best mitigation against the threat of quantum computers is quantum-safe cryptography'. NCSC also recommends any other organizations considering the use of QKD as a key agreement mechanism ensure that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them.' [15].

Considering the recommendations from various governmental bodies, significant global investments are being directed toward research aimed at overcoming the current limitations of QKD [16] along with other quantum technologies. The US with their National Quantum Initiative [17], emphasizing secure communications and related technologies. In Europe, EuroQCI [18], a part of the EU Quantum Flagship [19] focuses on building secure quantum communication infrastructure spanning the whole EU. The UK with its National Quantum Technologies Program [20], built a Quantum communication hub [21] to accelerate the development and commercialization of quantum secure communications technologies and services at all distance scales. Germany, the Netherlands [22], China, Japan, South Korea, India [23], Singapore and other countries [16] are also heavily investing which gives a competitive global push toward secure and scalable quantum communication systems. Not only does this result in a lot of ongoing research, but there are also numerous private companies and start-ups offering QKD-based solutions such as ID Quantique [24], Toshiba [25], etc [26, 27].

According to Business Insights reports, the global Quantum Communication market size was USD 1.1 billion in 2023 and the market is projected to touch USD 8.6 billion by 2032 [28].

As QKD has emerged as a promising technology for secure communication, supported by investments from various governmental bodies, private organizations, and commercial enterprises, identifying the appropriate use cases is crucial to maximize its potential, ensure widespread adoption, and guide further research and development. Numerous surveys, white papers, and listings on commercial companies' websites provide valuable insights into potential and realized use cases. In earlier works, such as the one by [29], the authors enumerated several use cases for QKD, including off-site backup/business continuity, enterprise metropolitan area networks (MANs), critical infrastructure control and data acquisition, backbone protection, high-security access networks, and long-haul services. These use cases are discussed in detail in [29], with sections outlining the goal, concept of operation, involved actors, actor-specific challenges and benefits, and operational implications. A more recent survey by [30] highlights additional use cases in new and emerging domains, such as metropolitan areas for securing communication networks in urban environments, healthcare for securing sensitive medical data and genome sequencing information, and other domains like smart cities and industrial automation, often integrating PQC for added robustness. Several companies have showcased their QKD products in real-world applications, providing concrete examples of the technology's impact. Toshiba, in [31], highlighted the deployment of their QKD products in areas such as genome data security, back-office data protection, and secure data transfer solutions. Similarly, ID Quantique has implemented QKD in various sectors, including banking, finance, data centers, government and defense, critical infrastructure, telecommunications, healthcare, and automotive industries [32]. QNu Labs identified QKD use cases ranging from secure communication in enterprise networks to critical infrastructure protection [33], while QuantumCTek listed use cases such as securing governmental communications and critical infrastructure within urban and national frameworks [34]. Quantum Xchange, as noted in [35], described use cases of their QKD solutions, focusing on high-level applications. The ongoing exploration and implementation of QKD use cases demonstrate the technology's adaptability across sectors.

Motivation. While numerous QKD use cases exist, the currently available literature (including manufacturers' resources and project reports) do not provide a comprehensive practical security analysis. Specifically, sources in the literature often fail to critically examine (or even frequently omit) key aspects we view as crucial. This encompasses aspects such as security requirements, the concrete usage of the generated keys, which kind of data they aim to protect (and for how long), the protocol with which the proposed solution operates, network topology, and the concrete targeted security guarantees. Further relevant aspects that are missing in such documents are whether the proposed solution involves additional cryptographic components (and the impact of potential failures of these components), and a discussion of/comparison with potential alternative approaches (such as pre-shared keys and PQC).

Our contribution. This paper addresses this gap by conducting a comprehensive, detailed and practical security analysis of available QKD-based use cases to evaluate their feasibility and effectiveness. We evaluated use cases deployed in optical fiber networks, focusing on those with sufficient publicly available information to enable detailed evaluation. We systematically selected use cases from the literature, sorting them chronologically from older to more recent examples. We critically analyze each use case based on parameters such as target sector, QKD system employed (including technical details provided by QKD providers and underlying technology), security goals, and type of data to be protected. We excluded use cases that lack adequate information for the analysis but listed them in the appendix for reference. Our analysis identifies strengths and gaps in the reviewed use cases, thus contributing to a general assessment of their practicality and effectiveness. Furthermore, we provide recommendations on how to improve the solutions discussed per use case and explore whether similar outcomes could be achieved using classical cryptographic systems, thus offering a comprehensive perspective on the applicability of QKD solutions.

Organization of this paper. We begin by providing necessary background in section 2 and details on the use cases to be analyzed in section 3. We then describe our approach to use case analysis in section 4. In section 5, we apply this method to analyze use cases, critically comment on the use cases and offer recommendations for improvement. Finally, in section 6, we conclude the paper.

Acronyms

AES Advanced Encryption Standard.
AKE Authenticated Key Exchange.
AONT All-or-nothing transform.

Ciemat Research Centre for Energy, Environment and Technology.
COW Coherent One Way.
CRQC Cryptographically Relevant Quantum Computer.
CSIC Spanish National Research Council.
CV-QKD Continuos Variable QKD.
CWDM Coarse Wavelength Division Multiplexing.

DHKX Diffie-Hellman Key Exchange.
DM Discrete Modulation.
DPS-QKD Differential Phase Shifted QKD.
DRC Disaster Recovery Center.
DV-QKD Discrete Variable QKD.

GM Guassian Modulation.
GMAC Galois Message Authentication Code.

HMAC Hash-based Message Authentication Code.
HNDL Harvest-Now-Decrypt-Later.
HSM Hardware Security Module.

IPsec Internet Protocol Security.
ITS Information-theoretic security.

KM Key Management.
KMS Key Management System.

MAC Message Authentication Code.
MACsec Media Access Control security.
MAN Metropolitan Area Network.
MDI-QKD Measurement-Device-Independent QKD.

NEC Nippon Electric Company.
NICT National Institute of Information and Communications Technology.

OTP One-Time Pad.

P2P Point-to-point.
PCS Post-Compromise Security.
PKI Public Key Infrastructure.
PQ Post-Quantum.
PQC Post-Quantum Cryptography.

Q-ITS Quantum Information-theoretic security.
QAM Quadrature Amplitude Modulation.
QKD Quantum Key Distribution.
QPSK Quadrature Phase Shift Keying.
QRNG Quantum Random Number Generator.

RSA Rivest–Shamir–Adleman.
Rx receiver.

SCADA Supervisory Control and Data Acquisition.
SHA Secure Hash Algorithm.
SIG Services Industriels de Genève.
SKR Secret Key Rate.

SNR Signal to Noise Ratio.
SSS Shamir's Secret Sharing.

TB terabyte.
ToMMo Tohoku Medical Megabank Organization.
Tx transmitter.

UPM Universidad Politécnica de Madrid.

VPN Virtual Private Network.

WAN Wide Area Network.
WDM Wavelength Division Multiplexing.

XOR Exclusive OR.

2 Background

QKD is a comparatively new technology, that allows two parties to establish a shared key. In this section, we will give an explanation of the terms used and a brief overview of QKD including trade-offs, alternatives such as PQC and pre-shared keys, assumptions, and related schemes.

2.1 Security properties

A cryptographic solution can provide different security properties. Our main focus in this work is on confidentiality and authenticity as the most commonly required ones, but we note that other properties such as anonymity may be as, or even more important, depending on the use case.

2.1.1 Confidentiality

Confidentiality intuitively means that the content of an interaction remains hidden from everyone but the involved parties. As far as encryption of large plaintexts is concerned, this means that no outside party should be able to learn any information about it, except for its length. In case of QKD and key-exchange protocols, an equivalent but usually preferred definition is that the key is indistinguishable from a random key sampled from the same distribution. This property is inherently vulnerable to HNDL attacks, and security parameters are generally chosen to make decryption infeasible, even for extended periods.

Some protocols achieve confidentiality by encrypting messages to keys that are in use for a long time. If such a key is corrupted at some point, this allows the decryption of all future and past communication. To deal with this threat, protocols will often implement stronger versions of general confidentiality, that require graceful treatment of this scenario: Forward Secrecy and PCS (Post-Compromise Security).

Forward Secrecy, also occasionally known as Pre-Compromise Secrecy or, misleadingly, as Perfect Forward Secrecy (there is nothing perfect about it) is the property that a protocol prevents the decryption of old messages, even if a key is corrupted at some point. To achieve forward secrecy, a protocol can update its session key at regular intervals and remove old ones, for example with a new key exchange such as QKD or with a symmetric ratchet.

PCS (Post-Compromise Security), also known as Backward Secrecy, on the other hand is the property that a protocol can recover from a corruption and get back to a point of full confidentiality, even if a party's state gets corrupted at some point [36]. To achieve Post-Compromise Security, a protocol can update its session key with fresh randomness at regular intervals with a new key exchange, for example with QKD or an AKE (Authenticated Key Exchange).

2.1.2 Authenticity

Authenticity intuitively means that the parties participating in an interaction are indeed the parties that they claim to be and that their messages contain the content that they actually transmitted. Sometimes the latter part is treated as the distinct property 'integrity', though we will use the term authenticity to also cover integrity.

2.2 Computational and information-theoretical security

Cryptographic security notions can offer resistance against different classes of attackers. The most powerful notion in this respect is *perfect* security, which is defined as unconditional security against computationally unbounded adversaries in all cases. A slightly weaker version of this is *statistical* security, which allows an adversary to break security in a very small and random number of cases, but without any influence on whether he *gets lucky*. Both of these can be summarized as information-theoretical security, since they can be proven directly from information theory. However, information-theoretical security is sometimes also used to refer to perfect security only.

The more common alternative is computational security, in which computationally bounded adversaries should only have a negligible chance of breaking a scheme. This class can be further subdivided based on whether the adversary has access to a quantum computer or not: In the former case we call the adversary a *quantum adversary* and in the latter a *classical adversary*.

In the context of QKD, we gain one further class: Schemes whose security can be proven with quantum information theory, which adds quantum mechanical assumptions to information theory. We call notions that fall into this category *quantum-information-theoretically* secure.

2.3 One-Time Pads and Message Authentication Codes

OTPs (One-Time Pads) are a method in which a plaintext is XORed with a random key of equal length. The key is used only once before being discarded. OTPs at times are not even viewed as an encryption scheme in the stricter sense due to the inability to reuse keys, and since the length requirement on the key poses severe limitations. On the other hand, OTPs are the only way to achieve unconditional confidentiality that requires no further conditions or assumptions. A scheme with this level of security could be called *perfectly* confidential.

On their own, however, OTPs offer no authenticity – it is trivial to manipulate ciphertexts with (partially) known plaintexts in a way such that they decrypt to other messages. To prevent this, we require an authenticity mechanism, which is usually achieved via message authentication. The strongest possible way to achieve this is with MACs (Message Authentication Codes) based on universal hash families, originally introduced by Carter and Wegman [37]. MACs based on universal hashing still can be attacked with a very small chance – the very small chance is that an attacker correctly guesses the authentication tag due to sheer luck, but there exist no successful attack strategies beyond guessing. While such schemes thus aren't perfectly secure, they offer *statistical* authenticity.

2.4 Quantum Key Distribution

QKD is a mechanism that uses a quantum channel, a channel that allows the transmission of quantum states (generally speaking qubits), to establish a shared secret between the endpoints. On its own, this mechanism would be inherently vulnerable to man-in-the-middle (MitM) attacks. It is thus necessary to perform the procedure in an authenticated way, by means of an authenticated channel (which may be classical). Usually, 'QKD' refers to the combined mechanism and encompasses the authenticated channel. The resulting shared secret is said to offer confidentiality based on the postulates of quantum mechanics, assuming that the authenticated channel is indeed information-theoretically secure and that executions of the protocol do not deviate from its abstract design. This is often claimed to offer ITS (Information-theoretic security), though we would argue that this can be confusing – security is based on the additional assumptions that underlie QKD, such as the postulates of quantum mechanics. We expand on the assumptions underlying QKD in section 2.4.1. To make a clear distinction between information-theoretic security and its extension with quantum physics postulates, we will use the term **Q-ITS (Quantum Information-theoretic security)**.

The keys established by QKD can be used with a OTP and a statistical authentication mechanism to achieve quantum-information-theoretic confidentiality and authenticity, but this requires a large amount of key material. Many real-world QKD schemes will thus instead use classical, computationally secure symmetric encryption mechanisms, resulting in computational security with additional quantum assumptions.

2.4.1 Assumptions about QKD

Although QKD-based solutions are often advertised as solutions that dispense with the computational assumptions underlying public-key cryptography, it is important to note that they come with

their own assumptions and limitations. Most of these assumptions are protocol-dependent, but below are some fundamental ones independent of this choice of the QKD protocol [38].

1. **Quantum theory is correct:** We assume that quantum theory accurately predicts measurement outcomes, as numerous experiments have confirmed. However, while this assumption is sufficient for quantum cryptography's security, it may be stronger than necessary. The security relies only on key elements of quantum theory such as state space structure, operations on it, and the prohibition of superluminal communication. These principles show that quantum states cannot be cloned, and entanglement is monogamous. Other aspects, like the Schrödinger equation, are not essential. Even if quantum theory is adjusted, as it likely will be to incorporate gravity, as long as these core principles remain approximately valid, quantum cryptography remains secure.
2. **Quantum theory is complete:** Completeness means there is no extended theory that can make better predictions used for the security analysis of QKD. It has been shown that the completeness of quantum theory follows from its correctness and the existence of free randomness [39]. In QKD, security is guaranteed against any attack within quantum theory's framework. *Completeness ensures that an adversary cannot gain more information about the key than what quantum theory predicts.*
3. **Free randomness exists:** It is assumed that basis choices, for example for the construction or measurement of a quantum state, can be made randomly and independently of the sending and measurement device.
4. **Devices do not leak any relevant/useful/secret information:** It is assumed that devices like single photon detectors, the QRNGs, and the classical computer only leak information as specified in the protocol. For instance, the raw key stored on the classical computer must not be leaked externally. To ensure this, the hardware is typically required to be properly shielded. Whether this is fundamentally possible, remains an open question [40, 41].
5. **Existence of Authenticated Classical Channel:** Any quantum key distribution protocol relies on the existence of an authenticated classical channel [42]. A common solution is the use of cryptographic signatures that have the advantage of a much smaller attack window than encryption, as store-now, decrypt-later attacks don't work, but still fundamentally tie the authenticity of the protocol to a scheme that offers computational, but not quantum-theoretic security. Alternative options include the use of statistically secure authentication mechanisms, which first requires a shared secret, and methods to extend the authenticity of an initially authentic protocol, that would limit the use of signatures to an initial setup [43].
6. **The protocol is implemented correctly:** In addition to fundamental assumptions about the underlying physical theory, various assumptions can be made about the protocol's implementation. The more assumptions we make, the easier the security proof becomes, as each assumption limits the range of possible attacks by an eavesdropper. For example, assuming all detectors have the same detection efficiency simplifies the security proof by excluding that threat. However, the proof is only valid if the assumptions hold—any deviation in implementation can compromise the protocol's security.
7. **Use of Quantum repeater or Trusted nodes for long-distance communication:** From the implementation point of view, QKD faces limitations in long-distance communication as quantum signals attenuate significantly over long distances, and increasing this range without compromising security is challenging. However, QKD works effectively over short distances because the attenuation and noise levels are manageable, ensuring high security and low error rates. For long-distance communication, either quantum repeaters or trusted nodes are necessary. Quantum repeaters use principles like entanglement swapping and quantum memory to extend the communication range, but they are not yet fully developed for large-scale practical use. Trusted nodes are more practical with current technology but introduce vulnerabilities if the nodes are compromised. Thus this assumption is not inherent but rather a technological assumption.

2.5 Encryption with pre-shared keys

Considering the significant cost of setting up quantum channels between two parties, it is worthwhile to investigate whether the cost of doing this exceeds the cost of simply exchanging the necessary key material directly (in person) between the endpoints. Although such an approach does not scale to universal use on the Internet, it can be viable with a small number of well-known endpoints and predetermined connectivity. Some of the use cases that we analyzed fall into that category, even when envisioned as fully deployed.

We distinguish two scenarios, depending on the encryption method. First, the OTP can be combined with a statistically secure MAC to achieve ITS. Since OTP requires a key that is at least as long as the data that is being transmitted, this requires an initial trusted offline distribution of a large number of pre-shared key bits, each of which has to be discarded after use. For example, this distribution could be done by a trusted courier. Moreover if more data needs to be transmitted, then additional trusted offline key distributions are required. The key material for an OTP must be deleted after use, both to prevent accidental reuse, but also to reduce the attack surface by preventing the decryption of past ciphertexts as a consequence of a later compromise of the keys ('forward secrecy'). Once this is done on both ends, this method guarantees everlasting confidentiality. A second option is to use computationally secure symmetric cryptography, for example AES with GMAC, so that only a small number of pre-shared key bits are required. Only an initial offline distribution is required: as estimated below, one could simply distribute enough key bits initially to last for the effective lifetime of the system. Alternatively, a single small key can be distributed initially, which is stretched via a symmetric ratchet (the ratchet even be based on AES to minimize the computational assumptions in the system). This ratchet would also provide forward secrecy in case of key leakage via (for example) a device compromise.

Modern mass storage has become incredibly cheap, to the point where micro SD cards with a capacity of 1 TB are commercially available for under 100€. At the rate of consuming one 256-bit key per minute for AES, this would be enough capacity to store key-material for almost 60.000 years[1] at the cost of exchanging a physical item once, requiring no assumptions besides the availability of a good source of randomness and the correct identification of the peer when handing over the key-material. We compare the usage of pre-shared keys with QKD in table 1.

The downside of pre-shared keys compared to QKD and AKE is that this method does not provide PCS. PCS is not achieved because key-material cannot easily be generated on the fly. This is problematic after a breach that may have corrupted key-material intended for later use, because this could result in the unavailability of key-material until new key-material is exchanged. We remark though that even QKD and AKE could run into issues in that scenario, as this kind of breach could also affect key-material for authentication. Whether the cost of the new individual exchange is cheap or expensive heavily depends on the use case in question.

2.6 Asymmetric Cryptography, PQC

Traditionally, the problem of establishing a shared secret key between two parties is solved using asymmetric cryptography. Initially, this came mainly in the form of asymmetric encryption based on the RSA (Rivest–Shamir–Adleman) algorithm, a public-key cryptosystem that relies on the computational difficulty of factoring large composite numbers [44]. At this point, we also see a large number of protocols based on versions of the DHKX (Diffie-Hellman Key Exchange) [45]. We compare the usage of an authenticated key exchange using asymmetric cryptography with QKD in table 1. These techniques scale exceptionally well and by now protect most of the communications infrastructure upon which the World Wide Web operates. Additionally, they also protects much of the Internet and most digital communication. On the other hand, like all asymmetric cryptography, RSA and DHKX rely on computational assumptions. Shor's algorithm additionally renders them vulnerable to quantum attacks.

PQC is a name for classical algorithms that are expected to withstand quantum attacks. The first PQC solutions have recently been standardized, encompassing ML-KEM [46] (based on Kyber [47]) for key establishment as well as several digital signing algorithms, called ML-DSA [48] (based on Dilithium [49]), SLH-DSA [50] (based on SPHINCS+ [51]), and FALCON ([52], FIPS to appear).

The fact that these algorithms can still be run on classical machines has one advantage: at least in some use cases, the infrastructures that so far used RSA/DHKX can accommodate them with reasonable little work (e.g., without switching to a quantum channel, and without adapting the bigger protocols surrounding the algorithm in a major way). For example, ML-KEM/Kyber have already been deployed in Chrome and Firefox to establish TLS connections [53], by Amazon for its AWS Key Management Service [54], and by iMessage [55] and Signal [56] (whose key agreement mechanism PQXDH is also used by WhatsApp).

Additionally, asymmetric cryptography is able to provide one-sided authenticity, which is, for example, the typical need in the World Wide Web and similarly desirable for sending anonymous

[1] 1 TB SD cards can store enough 256 bit keys for $10^{12} \cdot 8/256/(60 \cdot 24 \cdot 365.25) = 59415$ years, when one key is used every hour.

messages. This property is much harder to achieve with QKD (without relying on asymmetric cryptography).

A caveat with regards to integrating post-quantum algorithms into protocols is that the algorithms tend to have a larger data footprint and/or are slower to compute than pre-quantum ones, thus potentially requiring some protocol adjustments.

2.6.1 Assumptions of PQC

With PQC having been standardized and the first algorithms having been deployed, we note that the main caveat of asymmetric cryptography (including PQC) is that all computationally secure primitives have to rely on computational hardness assumptions (which could turn out to be wrong). The difference between PQC algorithms and their predecessors lies in the concrete computational assumptions on which the algorithms rely. Most of the assumptions that are used by the aforementioned standards are assumptions about certain lattice problems – ML-KEM and ML-DSA use an assumption called Module-LWE [57], and Falcon uses an assumption called NTRU [58].(The only 'non-lattice' exception is SLH-DSA, with a conservative design that uses hash assumptions.) These lattice assumptions are comparably 'young' – while the scientific community has been conducting dedicated cryptanalysis for several years, the assumptions have not encountered cryptanalytical attention for the same period of time as the ones underlying RSA and DHKX. It should also be noted that the PQC assumptions involve mathematical principles that are more complex.

Table 1 Comparison of Communication Protocols.

Scheme	Security	Key Management	Complexity	Scalability
Preshared Keys + OTP + ITS MAC	Perfect confidentiality, statistical authenticity. No PCS.	Biggest challenge is securely sharing, re-sharing (if more keys are required), and storing a key as long as the messages.	High complexity in key management. High due to the need for large keys and secure storage.	Very Poor, due to need for quadratic number of in person interactions.
Preshared Keys + Symmetric Encryption	Computational confidentiality and authenticity. No PCS.	Secure key distribution is required. Key size is much smaller than in OTP, making it more practical.	Moderate to high in key management. Slightly easier than with OTP due to smaller key sizes.	Very Poor, due to need for quadratic number of in person interactions.
Preshared Authentication Keys + ITS MAC + QKD + OTP	Q-ITS confidentiality, statistical authenticity. PCS.	Secure key distribution is required. QKD allows on-demand generation of OTP-keys.	Moderate to high in key management, but overall high due to need for QKD infrastructure.	Extremely poor, due to quadratic number of in person interactions combined with the need for quantum channels.
QKD + OTP + Signatures	Q-ITS confidentiality, computational authenticity. PCS.	QKD allows on-demand creation of OTP-key, signature verification key needs to be securely shared.	High complexity due to need for QKD infrastructure. Low complexity for key management.	Poor, due to need for quantum channels; star-networks can take some of the edge of, but inherently require trust into operator.
QKD + Symmetric Encryption + Signatures	Computational confidentiality with additional need of quantum-assumptions, computational authenticity. PCS.	QKD allows on-demand creation of encryption-key, signature verification key needs to be securely shared.	High complexity due to need for QKD infrastructure. Low complexity for key management.	Poor, due to need for quantum channels; star-networks can take some of the edge of, but inherently require trust into operator.
Authenticated Key Exchange + Symmetric Encryption	Computational confidentiality and authenticity. PCS.	AKE allows on-demand creation of encryption-key, authenticity-key needs to be securely shared and stored.	Low complexity for key management.	Excellent, if PKI (Public Key Infrastructure) is available.

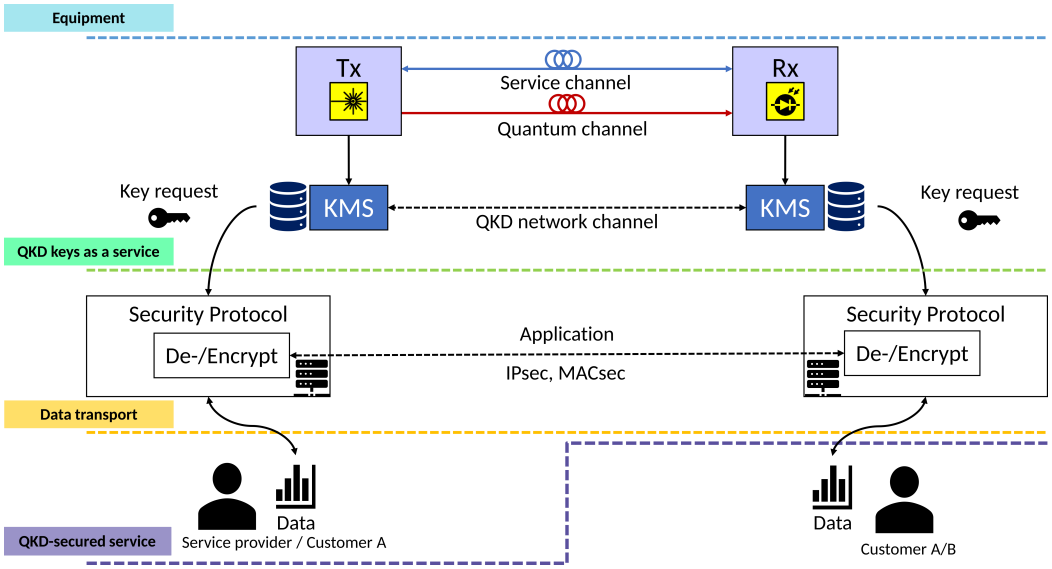

Figure 1 Overview of systems involved in the encryption of data using QKD keys. Different types of service provide different functionality and determines which systems the user is required to operate.

2.7 Types of QKD service

There are multiple ways in which a user can use QKD. Fig. 1 shows which ones we encountered in our use case analysis and shows what is operated by the end-user and what is operated by the service provider. All components above the respective line are operated by the service provider, while the components below the respective line are operated by the end-user. Vertical communication lines are within a node and are assumed to be physically secured, while horizontal communication lines can be accessed by an attacker.

- Equipment. An end-user can operate all the necessary equipment himself, including the QKD Tx (transmitter) and Rx (receiver).
- QKD keys as a service. In QKD keys as a service, the QKD equipment is operated by a network operator and the QKD equipment can be shared with multiple customers. The customer might pay a subscription fee or pay per QKD key. The provider operates the KMS (Key Management System) and allows the customer to connect to the KMS to retrieve his keys.
- Data transport. The customer does not use the QKD key himself but the key is used by the provider to securely transport the data of the customer. The provider is responsible for the encryption and decryption of the user data. The provider might for example offer encrypted transport based on MACsec or IPsec with QKD keys as a service.
- QKD-secured service. The provider provides a service to the customer in which QKD is used and in which one endpoint of the QKD system is used by the service provider and the other endpoint by the customer.

2.8 QKD network topology

The purpose of a key exchange is that only two parties share the key material, which perfectly fits the basic P2P (Point-to-point) connections. However, when dealing with more complex network topologies, a device-based technology such as QKD requires a more complex architecture (see Fig. 2) [59]. Because deploying fibers is an expensive and time-consuming operation, any fiber operator would prefer sharing their pre-existing fiber infrastructure over deploying an entire new one only for QKD. A typical architecture of shared infrastructure includes two parallel optical networks [60, 61]: the classical network, which is based on the OSI model of 7 layers, and the QKD network, which includes two subnetworks referred as KM (Key Management) and quantum layers. The connection between the two classical and QKD networks is provided by an application layer that manages keys requests, which are managed by the QKD network. As the name suggests, the KM layer connects the KMSs assigned to each node. The KM and application layers can easily share the infrastructure with standard WDM (Wavelength Division Multiplexing). However, this is not the case for the quantum layer, which connects QKD Tx and Rx, because of the quantum channel. The sharing of

fibers in classical networks presents numerous technical challenges, such as crosstalk, scattering, and additional filters so that quantum channels can bypass optical amplifiers [62].

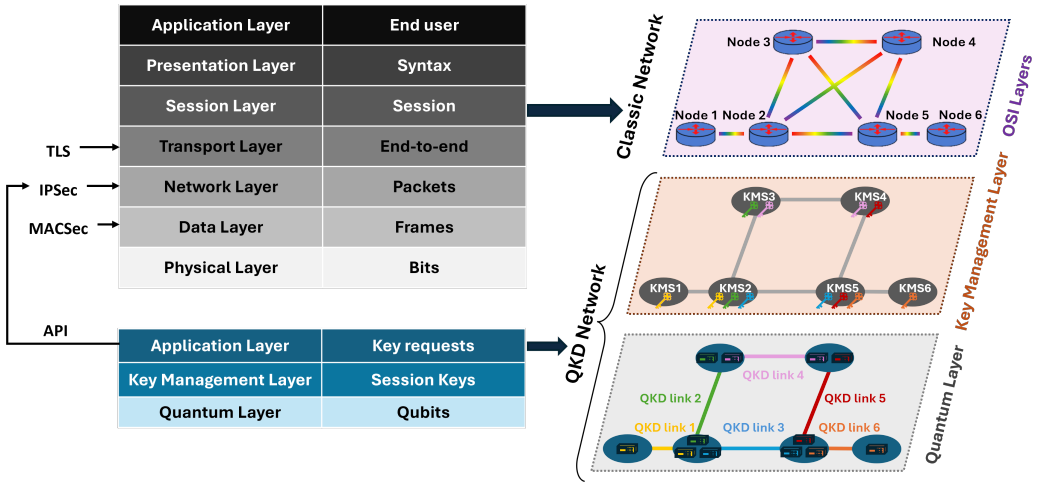

Figure 2 General architecture of an optical network supporting QKD. Protocol stacks of classic optical network (top-left) and QKD network (bottom-left).

QKD protocols are executed in the quantum layer. Typically, service channels must be synchronized with quantum ones, thus sharing the same or parallel fibers is preferred. However, no standardization has been proposed yet on the QKD protocol to adopt, making it difficult for fiber operators to integrate QKD into their infrastructure [63]. There are two main families of QKD protocols: DV-QKD (Discrete Variable QKD) and CV-QKD (Continuos Variable QKD). Table 2 reports some of the QKD protocols that are closest to being deployed on real networks.

Table 2 List of most common QKD Protocols.

Protocol	Quantum state	Cost	Distance [km]	SKR [Mb/s]	Maturity level
BB84 (DV) [64]	Single photon	medium	150	0.3	Variants of BB84 available as commercial products.
COW (DV) [65]	Coherent pulses	medium	90	0.05	Available as commerical product.
MDI (DV) [66]	Pair of photons (entanglement)	high	511	$3.37\ 10^{-9}$	Deployed on real networks.
Gaussian (CV) [67, 68]	Coherent state	low	20	0.03	Field demonstrations.
QAM (CV) [69]	Coherent state	low	16	35	Field demonstration.
QPSK (CV) [70]	Coherent state	low	20	10	Deployable system under development.

We can observe that all proposed protocols are limited in SKR (Secret Key Rate) when compared to typical data rates on fiber communications, which are on the order of hundreds of gigabits. This limitation prevents the use in real time of QKD for ITS symmetric encryption schemes that require keys comparable in size to the data, such as OTP. SKRs are still sufficient for symmetric encryption algorithms with smaller keys such as AES, although this comes with a cost in terms of the overall security of the system. The low SKR is one of the main motivations for the a virtual division between classical and quantum networks even if they share the same fiber infrastructure. The other clear

limitation is the distance that, combined with the absence of quantum repeaters, makes the presence of chains of trusted nodes necessary [71].
DV-QKD protocols were the first to be formulated and demonstrated, thus they are currently the most mature technologically and are already available as commercial products. However, DV-QKD protocols have significant technological limitations and challenges that limit their deployment in realistic scenarios. The first limitation is the cost, mainly due to the single-photon detectors, which are expensive and are not standard telecom devices. The second limitation is the high sensitivity to crosstalk due to the extremely low power of the quantum channel compared to classic ones. A promising family of protocols are MDI-QKD (Measurement-Device-Independent QKD) protocols, which rely on an intermediate node for measuring two different streams of qubits. The main advantage of MDI-QKD is the increment of the maximum distance between two nodes in distance without relying on trusted intermediate nodes, although the key rates are significantly lower [66].
CV-QKD protocols have the advantage of using coherent receivers with detectors more similar to those use for classical optical communications. This advantage enables not only the reduction of costs, but also the compatibility with equipment from telecom operators and WDM systems [72]. CV-QKD protocols can be based on GM (Guassian Modulation) or DM (Discrete Modulation) such as QAM (Quadrature Amplitude Modulation) and QPSK (Quadrature Phase Shift Keying) [70]. DM based protocols show some advantages compared to GM: higher reconciliation efficiency of practical error correction schemes, simpler implementation, and higher capacity in the very low SNR (Signal to Noise Ratio) regime, which is a very common regime for CV-QKD schemes [73]. These properties make DM CV-QKD protocols optimal and scalable options for deployment into classical optical networks. However, the signal-to-noise ratio in CV-QKD protocols rapidly decreases with channel losses, thus limiting the use to shorter distances, as shown in Table 2. In terms of maturity, CV-QKD relies on standard photonic components for telecommunications, which make it easier to demonstrate and deploy [74]. However, significant effort is required in terms of signal post-processing and calibration. GM and QAM-DM CV-QKD system have been demonstrated in a field demonstrations [67, 69] over deployed fiber links below 20 km. DM CV-QKD systems have been shown to achieve key rates beyond 1 Mbps in short distances, although significant effort is still needed for deployment in a real optical network [75–77]. Compared to DV-QKD a significant limitation of CV-QKD protocols is their security that is based the assumption of perfect states separation, which cannot be guaranteed in a practical CV-QKD system [78].

3 Current use cases

This section briefly introduces the use cases being analyzed in the subsequent sections. Analyzing all the available use cases in the literature, in commercial QKD company documents [79–81], in the OpenQKD project [82, 83] and in other sources is not possible due to the limited details provided on some use cases. Use cases with sufficient technical information are analyzed here. The order is based on the year of occurrence. We summarize the use cases in table 3.

3.1 Authenticity of election results (2007)

The State of Geneva, Switzerland, used QKD during its 2007 election process to secure transmission of the election count totals from the counting center to the location where the votes were stored [84–86]. The QKD keys were used in conjunction with AES-256 for confidentiality and HMAC-SHA-256 for authenticity [87, 88]. ID Quantique provided the QKD devices. The locations were directly connected using 4 km long fibers [89].

3.2 Backup for disaster recovery (2017)

A private asset and wealth management company in Switzerland needed to secure its communication network between its headquarters and a DRC (Disaster Recovery Center) [90, 91]. To protect sensitive data long-term, they used Thales' network encryptors and Cerberis QKD devices to combine layer 2 Ethernet encryption using AES-256 with keys from QKD. The success of this implementation led to the expansion of the encryption platform to other areas of the company for MAN and WAN applications.

3.3 Financial data (2019)

In 2019, Toshiba and Quantum Xchange reported on a collaboration that augmented the encrypted connection between Wall Street's financial markets and a data center in New Jersey, using the QXC Phio QKD network [92, 93]. The connection between Wall Street and the data center is usually used to transmit sensitive financial data like trading algorithms and customer settlement accounts. As a demonstration, the QKD-augmented connection was used to transmit an uncompressed live video stream. The fiber connection multiplexes the QKD channels, including the quantum one, and the commercial data over a single dark fiber. The multiplexing scheme was based on CWDM (Coarse Wavelength Division Multiplexing) with the quantum channel in the O-band and the rest of the channels in the C-band. Deploying new optical fibers is one of the most expensive operations for a network provider. Therefore, the capability of Toshiba's system of avoiding a dedicated dark fiber for the quantum channel only is a significant improvement for the solution proposed in this use case.

3.4 Distributed information sharing and backups

We encountered several use cases in which actors wanted to store sensitive information, which we describe below. All use cases followed the principle of protecting that information against server breaks via a cryptographic protocol known as 'Secret Sharing', i.e., by splitting them into N many components ('shares') that cannot be used to reconstruct the original information without obtaining at least n many shares out of these N. The rationale is that by distributing the separate shares to spatially separated secure locations, it is ensured that an attacker cannot access the information without breaking into at least n many (secured) servers.

3.4.1 Facial recognition (2019)

The NICT (National Institute of Information and Communications Technology) of Japan, NEC (Nippon Electric Company), and the National Olympic Committee of Japan have partnered to use facial recognition to access a server room [94]. QKD is used to secure the necessary data for facial recognition. A facial recognition server decides if a person gets access to a server room that stores medical and athlete data records. The video recordings of athletes are used for analysis to improve their performance. A camera is connected to the central server and over this connection facial recognition data is sent which is secured using QKD. The central server is also connected to three servers using a QKD-secured connection. The biometric data of people who should be given access to the server room is stored on the facial recognition server and a backup is stored on three servers using secret sharing.

3.4.2 Key storage and key backup (2020)

Mt. Pelerin, a Swiss company specializing in cryptocurrency, partnered with ID Quantique to involve QKD in their asset management to secure digital assets [95, 96][97, Use Case 03]. These assets include blockchain private keys with which transactions can be signed and were split into five shares using SSS (Shamir's Secret Sharing) [98]. To recover the assets, access is necessary to three of five storage nodes [99]. The procedure for backing up assets to storage nodes involves OTP encryption of each share, for which the application uses keys distributed by ID Quantique's QKD devices.

3.4.3 Medical image sharing (2020)

The Diagnostic and Research Center for Molecular BioMedicine of Medical University Graz, Austria, exchanged images with the pathological institute of the LKH Graz West II, so that the images could be analyzed at both sites [100, 101]. The images were split in three shares using fragmentiX secret sharing which is based on SSS [102]. Two shares were encrypted using AES with QKD keys and transferred to two different datacenters in the same city. The third share was transferred using TLS to a storage at the Medical University Graz. In case one storage location encounters data loss, all data can be restored using the other two storage locations.

3.4.4 Medical record backup (2020)

NICT, NEC and ZenmuTech partnered to backup medical records [103, 104]. Dummy medical records were sent from the medical institution to a server using QKD. This server split the medical records

into three shares using the AONT (All-or-nothing transform) [105]. The three shares were then transmitted to three different data centers in different cities while being secured by QKD.

3.5 Connecting data centers (2020)

SIG (Services Industriels de Genève), a Swiss public utility company managing a fiber optical network, partnered with ID Quantique (IDQ) to secure a connection between two data centers using QKD and AES [97, Sec. 3.4]. SIG runs an encrypted connection between their two main data centers to secure sensitive data processed in their cloud applications [106]. They used QKD keys to augment the standard encryption key. Functionality in the case of unavailable QKD keys is maintained by falling back to the non-augmented encryption keys.

3.6 Genome data (2020)

By 2020, Toshiba Corporation and Tohoku Medical Megabank Organization (ToMMo) finished a five-year trial in which they used Toshiba's QKD system to encrypt sensitive large-scale genome sequence data [107–109]. Over two years, genome data produced with the Japonica Array tool was encrypted and transmitted from the Toshiba Life Science Analysis Center to the Tohoku Medical Megabank Organization over a distance of 7 km. Toshiba reported to have achieved stable communication with speeds exceeding 10 Mbps.

Toshiba furthermore reported that the sequencing of 24 genome data sets took over 117 hours to generate. During the generation of this data, the data was transmitted after being encrypted with OTP using keys from QKD. The transmission of this data finished in less than 4 minutes after the sequencing finished.

In 2020, the QKD network was extended with a connection between Tokohu University Hospital and ToMMo, which are a few hundred meters away from each other. The QKD keys were used to encrypt video conferences and exome sequence data using OTP. The exome sequence data was encrypted and transmitted while the sequencing was ongoing. One exome sequence produces approximately 344GB of data.

3.7 Metrics of an overbraider machine (2020)

Toshiba, BT, the Centre for Modelling and Simulation (CFMS), and the National Composites Centre (NCC) recently partnered to send production data between NCC and CFMS, encrypting this data using QKD-generated keys [110–112]. The data, which was sent over a 7km long fiber, included quality and performance metrics of an overbraider machine.

3.8 Self-driving cars (2021)

In collaboration with QRate, researchers from Innopolis University, Russia, integrated QKD hardware into a self-driving car in 2021 [113], to facilitate the exchange of key material with QKD-enabled gas/charging stations over an optical fiber. The gained key material was to be used to launch an encrypted OpenVPN connection (4G LTE) with the vendor's data center, in order to facilitate remote software updates and the transmission of telemetry data.

3.9 Grid network (2022)

IDQ additionally partnered with SIG to connect two of SIG's power stations to the OpenQKD testbed, as a demonstrator for an envisioned Smart Grid network connecting all of SIG's power stations in Geneva with each other and the operations center by a peer-to-peer (p2p) architecture [97, Sec. 3.1]. According to the OpenQKD report [97, Sec. 3.1], the use case was motivated by the goal to 'secure data transmission and detect intrusions such as hackers taking control of the electricity distribution network'.

3.10 Authentication of smart grid communications (2022)

In this use case, QKD was deployed over a distance of 3.4 kilometers between a power distribution center and an electrical substation in Tennessee, United States [114]. The keys from the Qubitekk QKD system were used to authenticate SCADA (Supervisory Control and Data Acquisition) traffic which was send using MQTT (Message Queuing Telemetry Transport). The SCADA traffic contains

non-confidential control data and measurement data such as voltage, current, frequency and phase. The traffic was authenticated using the GMAC (Galois Message Authentication Code) with AES.

3.11 Genome distance sharing (2022)

In the QuGenome project, the UPM (Universidad Politécnica de Madrid), the CSIC (Spanish National Research Council) and the Ciemat (Research Centre for Energy, Environment and Technology) had one or more genome sequences of which they would like to know how they are related to the genome sequences at the other institutions [115]. Using quantum oblivious transfer, secure multiparty computation and a distance-based method, the evolutionary distances between every pair of sequences were calculated without revealing the genome sequences at one institution to the other institutions [116]. The evolutionary distances were encrypted using OTP with QKD keys and shared with the other institutions to calculate the phylogenetic tree of the genome sequences. This tree can be used to visualize how family members or different variants of a virus are related.

Table 3: A summary of use cases

Use Case	Target Sector, Country	Description	QKD System and network	Intended impact	Security Goals	QKD service
3.1: Authenticity of election results	Government, CH	Used QKD to guarantee authenticity of election results during transmission between the counting center and storage location.	ID Quantique Cerberis QKD system directly connected using a 4 km long fiber.	Ensured authenticity of election results.	Transmission reliability, successful integration of QKD with existing cryptographic methods.	Equipment.
3.2: Backup for disaster recovery	Banking, CH	Used QKD with AES to secure connections between a bank's headquarters and a disaster recovery center.	QKD via ID Quantique's Cerberis QKD server. Direct connection, approx. 100 km apart.	Enhanced security for disaster recovery operations.	Forward secrecy, high performance, secure communication.	Equipment.
3.3: Financial data	Financial, US	Used QKD to secure a video stream transmission over a 32km dark fiber between financial offices.	Toshiba's QKD system. Data transmission over 32 km dark fiber between New York and New Jersey.	Enhanced security for financial data transmission.	Increased network capacity, secure long-distance communication.	QKD keys as a service.
3.4.1: Facial recognition	Biometrics, JP	Used QKD to secure the transfer of data for facial recognition in a server room.	NEC's QKD devices in Tokyo QKD Network. One trusted node between the camera server and the facial recognition server.	Secure storage and transfer of biometric data.	Reliability of QKD-secured video storage, successful facial recognition data transfer.	Data transport.
3.4.2: Key storage and key backup	Cryptocurrency, CH	Used QKD with OTP to transfer key shares in a cryptocurrency exchange's key storage system.	QKD with ID Quantique's QRNG. Direct connection.	Secure storage and backup of keys	Robustness of key recovery, resilience against attacks	QKD keys as a service [99].
3.4.3: Medical image sharing	Medical research, AT	Exchanged medical images using QKD and secret sharing between different datacenters.	QKD devices from ID Quantique, Toshiba, and ADVA. Direct connection with intermediate nodes at Citycom Graz data centers.	Secure storage and sharing of medical data.	Data recovery capabilities, redundancy of data storage.	Equipment.
3.4.4: Medical record backup	Healthcare, JP	Backed up medical records using QKD to split and transmit data to different datacenters.	The Tokyo QKD Network was used, which connected three locations using equipment from NEC, Toshiba, NTT-NICT and Gakushuin University.	Secure backup of electronic medical records.	Data redundancy, secure multi-location storage.	Data transport.

3.5: Connecting data centers	Public utility, CH	Secured connection between two data centers using QKD and AES-256 on layer 1 to protect cloud applications.	ID Quantique's Cerberis3 system. Direct connection using ADVA FSP 3000 for optical transport.	Increased data security for cloud applications.	Secure data transmission, fallback mechanisms.	Equipment.
3.6: Genome data	Medical research, JP	Secured transfer of genome data and video conferences using QKD and OTP encryption.	Toshiba's QKD system. Data transmission over 2 connections between 3 medical institutions, of which one connection 7 km long.	Secure high-speed transmission of genome data and video conferences.	Stable communication, real-time transmission capabilities.	QKD-secured service.
3.7: Metrics of an overbraider machine	Industrial manufacturing, UK	Sent quality and performance metrics of an overbraider machine between two facilities using QKD.	Toshiba's QKD system. Data transmission over 7 km connection.	Secure transmission of industrial data.	Secure and reliable data exchange, optimized industrial process monitoring.	Equipment.
3.8: Self-driving cars	Automotive, RU	Integrated QKD hardware into a self-driving car to securely transfer data and software updates over 4G LTE.	QRate QKD hardware. Quantum key distribution during refueling/charging via optical channel. VPN over 4G LTE.	Secure transfer of software updates and telemetry data.	Cache and retrieve QKD keys, secure data transfer over mobile network.	Equipment.
3.9: Grid network	Energy, CH	Secured data transmission between power stations using QKD to prevent intrusions.	QKD, Peer-to-peer architecture.	Enhanced security for Smart Grid communications.	Latency impact, link stability, service continuity during QKD-related issues.	Equipment.
3.10: Authentication of smart grid communications	Energy, US	Authentication of SCADA traffic (i.e. measurement and control data) between a power distribution center and an electrical substation.	Qubitekk QKD System. Direct connection, 3.4 km.	Ensured authenticity of SCADA traffic.	Information-theoretic authentication in smart grid communications.	Equipment.
3.11: Genome distance sharing	Medical research, ES and PT	Used QKD with OTP to secure information sharing on how genome sequences (for example from family members) are related.	ID Quantique and Huawei QKD systems were used to secure 2 connections of 7 km and 24 km between 3 institutions.	Secure sharing of genome distances.	Securely calculating and sharing of genome distances without revealing the genome sequences.	Equipment.

4 Method of analysis

While the use cases listed in section 3 differ in terms of target sector and concrete technological means, they share similarities in their technological approaches and/or their security goals. To structure our discussion in section 5, we will analyze the use cases using the following questions:

- How is the key used?
- What does the network topology look like?
- What security guarantees does the system provide?

4.1 How is the key used?

While all use cases involve the use of keys provided by QKD, these keys are used in different protocols. The respective protocol determines

- which data is encrypted. For example, MACsec encrypts the source and destination IP address, while TLS does not.
- and possibly, the symmetric cipher used to encrypt the data.

Different symmetric ciphers have different security guarantees. While AES provides computational security, OTP provides secrecy independent of the computational resources of the attacker, assuming the secrecy of the key does not depend on this as well and assuming the key is only used once. This has implications for the security guarantees that are provided by the system. To analyze the use cases in section 5, it is therefore important to keep the following questions in mind:

- What is the key used for? What kind of data will the key protect?
- By which protocol is the key used? Does it involve any additional cryptography? If yes, what are the implications if that additional cryptography breaks?
- How long does the data need to be protected?

4.2 What does the network topology look like?

Understanding network topology is crucial because it directly impacts the security, scalability, and feasibility of QKD deployment. The choice of QKD protocols, devices, and the configuration of trusted nodes influences overall security guarantees and determines the practicality of implementing QKD in real-world scenarios. By examining these aspects, we can assess how well the system aligns with the intended use case and its security requirements. Therefore, we look for the following points:

- What does the network topology look like?
- What QKD protocols and devices are used?

4.3 What security guarantees does the system provide?

The two primary properties that we discuss in this work are confidentiality and authenticity. Additionally we require correctness (the property that the scheme 'works' in the absence of an attacker) and availability, the property that a scheme can be used when needed. For the most part, the latter two are however less of an issue and none of the use cases that we analyzed seemed to encounter major issues with them.

5 Use case assessment and recommendations

To address the specific questions raised in section 4 for each use case, we now examine to what end the established QKD keys are used, which protocols and devices are involved, and the obtained security guarantees. To enable a comparison with traditional cryptographic methods and PQC, we additionally discuss if and how traditional cryptography and PQC could enable each use case, and if this would lead to different security guarantees. We also critically comment on the discussed use cases and offer recommendations for improvement. We summarize the analysis in table 4.

Comment on backups in general

We encountered several use cases that use QKD to protect the transmission of data with the goal to backup this data. QKD is primarily a replacement for key exchange mechanisms aiming for transport protection.

However, transported data should ideally also be protected at rest, i.e., while being stored as backups. Generally, this is not an ideal use case for dynamically created (or 'non-static') keys since such keys have to be stored along with the backup for eventual data recovery. For backup use cases, it may be desirable to use a pre-existing key to encrypt the to-be-transmitted data already before transmission since the storage facility then does not have to store the key material, making it harder for attackers to recover the encrypted data even if they gain digital or physical access to the storage facility. If the encryption scheme used for this long-term encryption is asymmetric, the generator of the data does not even need to maintain knowledge about the used secret key – it could be stored in a separate secure location, independent of the mass-data backup.

One way to then further strengthen such storage-encryption is to secret-share the key in a way that requires multiple parties to work together to decrypt the back-ups. Depending on the use-case this could for example involved all members of a company's board of directors receiving a share.

5.1 Authenticity of Election Results (3.1)

Aim

- Secure the link between the central ballot-counting station in downtown Geneva and government data centers in the suburbs over fiber-optic channels.
- The QKD key ensures the authenticity of election results during transmission.

Used technology

- *Protocol and devices:* ID Quantique Cerberis QKD using SARG04 and ID Quantique Vectis link encryptor using AES-256.
- *Connection:* Direct end-to-end connection using 4 km long fibers.
- *Additional Crypto:* AES-256 for confidentiality of election results, HMAC-SHA-256 for authenticity of election results.

Analysis and recommendation

In this use case, the QKD key was used to protect count totals of a public election. This data can be made public as soon as the voting stations close. If the data is transferred after closing the voting station, it does not have to be confidential anymore. The data only has to be authenticated to make sure the count totals are not modified. Therefore, it is not clear that this use case requires any form of confidentiality whatsoever; it seems that it only requires authenticity. Any QKD protocol requires an authenticated channel, which would suffice to solve the use case in a more natural way (by directly authenticating the transmitted local results once the election concluded). Therefore, we assess that QKD does not add value to this use case.

One could envision a variant of this use case in which votes are transmitted as they are being cast, instead of being transmitted only as an aggregate that needs no confidentiality. This would change the setting to a setting that requires confidentiality, which could be provided by QKD or AKEs. This variant, however, would inherently introduce additional attack vectors – e.g., parties with access to the receiving system could collaborate with a party that collects information about when a given voter voted, thereby breaking the secrecy of the election.

5.2 Backup for Disaster Recovery (3.2)

Aim

- Protect highly sensitive business and customer data, including financial records, credit card information, personal details, and any other critical data relevant to the company's operations and customer trust.
- The established QKD key is used to maintain security in case the pre-shared key is compromised. The QKD key is combined with the AES-256 pre-shared encryption key used by the 10 Gigabit Ethernet encryptors to ensure forward secrecy and protect against eavesdropping and future decryption attempts. The combined key is used for data transmitted between the company's headquarters and the DRC.

Used technology

- *Protocol and devices:* ID Quantique's Cerberis QKD system using SARG04 and Thales' encryptor using AES-256.
- *Connection:* The setup includes a direct end-to-end connection between the headquarters and the DRC, approximately 100 kilometers apart. The connection uses four 10 Gigabit Ethernet encryptors that facilitate the encrypted data transmission.
- *Additional Crypto:* AES-256 to protect business and customer data.

Analysis and recommendation

QKD is used here to provide transport security, which is it's primary strength. However, the backup data is only secured in transit and not secured at rest. The recommendation to secure the data at rest from section 5 applies.

5.3 Financial Data (3.3)

Aim

Secure the transmission of sensitive and high-value data between a datacenter on Wall Street and a datacenter in New Jersey. This data includes trading algorithms, customer settlement accounts, real-time trading and transactional data, core banking applications and video conferencing data.

Used technology

- *Protocol and devices:* Toshiba's QKD system using BB84/T12 and Senetas encryptor using AES.
- *Connection:* Toshiba's Multiplexed Single Fiber QKD system operating in the O-Band is used. This system allows combined commercial data and QKD traffic over a single fiber. The data transmission occurs over a 32 km dark fiber between New York and New Jersey.
- *Additional Crypto:* AES-256 to protect financial data.

Analysis and recommendation

QKD is used here to provide transport security, which is it's primary strength. We only note that the institutions in question are physically close enough and pre-determined enough, that exchanging AES-keys physically, as discussed in section 2.5, would be a viable and even more secure, but more labor-intensive alternative here.

5.4 Distributed information sharing and backups

5.4.1 Facial Recognition (3.4.1)

Aim

Secure the transmission of biometric authentication data, specifically feature data in a face recognition system, between the central server and the face recognition server. Additionally, secret sharing is used to secure the storage of reference data for authentication across distributed servers.

Used technology

- *Protocol and devices:* NEC's QKD devices, using BB84 and DPS-QKD, integrated into the Tokyo QKD Network.
- *Connection:* There is one trusted node between the camera server in the NOC (Network Operation Center) in Tokyo and the facial recognition server at NICT headquarters.
- *Additional Crypto:* SSS to split biometric data and an unknown symmetric cipher to encrypt the split biometric data.

Analysis and recommendation

As biometric authentication cannot be changed like a password, this data has to be protected for a long time. QKD is indeed a possible way to provide some transport security, though AKEs would be able to do the same and the comment on backups in section 5 also applies to this use case.

5.4.2 Key storage and key backup (3.4.2)

Aim

- Protect the split private keys that correspond to digital assets such as cryptocurrencies. These private keys are critical as they are the proof of ownership of the digital assets.
- The established QKD key is used for encrypting the private keys that have been split using SSS (Shamir's Secret Sharing). Specifically, each component is encrypted with a OTP, and the keys necessary for this OTP encryption are distributed via QKD.

Used technology

- *Protocol and Devices:* ID Quantique's QRNGs are used to generate the blockchain private keys on a HSM (Hardware Security Module). The private keys are then secured in transit using QKD keys from ID Quantique's DV-QKD devices.
- *Connection:* Management node connected with five storage nodes using QKD.
- *Additional Crypto:* To sign transaction on a blockchain, a public-private key pair is generated. OTP is used to encrypt the secret shares which were split using SSS.

Analysis and recommendation

The private keys protected by the system need to be protected for the entire duration that the digital assets are in custody, which could potentially be indefinite or until the assets are moved or redeemed. However, assuming these private keys are used to control cryptocurrencies such as Bitcoin or Ethereum, the private keys can be calculated from the public key by a CRQC and the usage of QKD in this use case will not protect the private key from being recovered by a CRQC.

The use case aims to protect asymmetric secrets, i.e., secrets that are used by asymmetric cryptosystems. The use case thus assumes that the respective cryptosystems are secure – otherwise, protection of these secrets would not be worthwhile. Considering the significant overhead of QKD in comparison with classical cryptosystems, this calls the use case into question in general.

5.4.3 Medical image sharing (3.4.3)

Aim

- Protect sensitive medical data, including digital histological slides (up to 10 GB per image), clinical and genetic data, and other medical records and images exchanged between Medical University Graz and Hospital Graz II.
- The established QKD key is used for encrypting split data fragments during transmission between the hospitals (Medical University Graz and Hospital Graz II) and external S3 storage locations. The data was split using fragmentiX secret sharing.

Used technology

- *Protocol and Devices:* ID Quantique DV-QKD system and Toshiba BB84/T12 QKD system. The data was encrypted using AES with an encryptor provided by ADVA.
- *Connection:* The two hospitals were directly connected to the two datacenters operated by Citycom Graz. The datacenters function as an intermediate node for the connection between the hospitals.
- *Additional Crypto:* Additional cryptographic measures include fragmentiX Secret Sharing (which is based on SSS) and traditional TLS protection for one of the data fragments.

Analysis and recommendation

This use case uses QKD to provide transport security, which is its primary strength. Given the nature of medical records, protection may be required for many years or even decades. Even if the TLS connection used to transport shares of the medical images is broken by an attacker, the attacker would still need access to a second share to restore the original image. Besides the caveats regarding the use of QKD in general, we note that the institutions in question are physically close enough (and pre-determined enough) that exchanging AES keys physically, as discussed in section 2.5, would be an alternative that is viable and does not have to rely on quantum assumptions.

5.4.4 Medical Record Backup (3.4.4)

Aim

Secure the transmission of medical records that were split using secret sharing. Medical records contain detailed patient information, diagnostic results, treatment plans, and other confidential health-related data.

Used technology

- *Protocol and Devices:* The system utilizes QKD equipment from the Tokyo QKD Network, which uses equipment from NEC (BB84), Toshiba (BB84/T12), NTT-NICT (DPS-QKD) and Gakushuin University (CV-QKD).
- *Connection:* A medical institution is connected using QKD to a secret sharing server. This secret sharing server is connected using three QKD connections to three servers.
- *Additional Crypto:* AONT, which uses AES [117], to split medical records and an unknown symmetric cipher to encrypt the split medical records.

Analysis and recommendation

The confidentiality of the medical data needs to be protected for as long as the data is sensitive, which generally means many years. The data is sent to a server that secret-shares them and distributes the shares towards storage servers. As a consequence, the connections between the sender and the various servers have to be secured. Considering that the medical data is secret shared by a trusted server and not the original producer raises significant questions about why this is done this way, as it introduces the need for an otherwise unnecessary third party. Getting rid of this component and encrypting the data directly under secret-shared keys could improve the overall security and would still allow to use QKD to protect transport-encryption as a defense-in-depth measure. At that point the analysis given in Section 5.4.3 would apply.

5.5 Connecting data centers (3.5)

Aim

Secure the connection between SIG's two main data centers to protect utility operations data, customer information, and other confidential business data.

Used technology

- *Protocol and Devices:* ID Quantique's Cerberis3 using the COW protocol and ADVA's FSP3000 encryptor using AES-256-GCM.
- *Connection:* There is a direct end-to-end connection between the two main data centers using ADVA's FSP 3000 product for optical transport. The setup does not mention intermediate nodes explicitly, suggesting a direct link.
- *Additional Crypto:* AES-256-GCM to protect confidential business data. The QKD key is XORed with the standard session key to generate a super session key, which is then used by the ADVA FSP 3000 encryption equipment for Layer 1 encryption of data in transit over the optical network [99]

Analysis and recommendation

QKD is used to provide transport security, its primary strength. We note, however, that this use case is highly vulnerable to downgrade-attacks – attackers can completely eradicate the QKD component from this solution by simply interrupting the quantum channel. When the quantum channel stops working, no QKD keys will be used and only the standard session key is used to encrypt data. This behaviour prevents the unavailability of the connection. We recommend to change this behaviour. We also note that XORing keys is not without issues if it cannot be fully guaranteed that the keys are independent and non-maliciously generated; a dual-PRF could be more appropriate here [118].

We were unable to find information about the distance between the data centers. In case they are physically close, the alternative mentioned in 5.4.3 (physical exchanges of key material) would also apply here.

5.6 Genome Data (3.6)

Aim

Secure the transmission of video conferences, exome data and genome data, which can legally be considered personally identifiable information.

Used technology

- *Protocol and Devices:* Toshiba's QKD system using BB84/T12.
- *Connection:* Data transmission occurs over 2 connections. One connection with a distance of 7 km between Toshiba Life Science Analysis Center and ToMMo (Tohoku Medical Megabank Organization), and one connection between ToMMo and Tokohu University Hospital which are a few hundred meters away from each other. ToMMo can function as a trusted node.
- *Additional Crypto:* One-time pad encryption to encrypt exome and genome data.

Analysis and recommendation

QKD is used to its primary strength, providing transport security. This transport security is used to protect genome and exome sequence data, which is sensitive personal information that should be protected for a long time. Different from most other use cases, the one-time pad is used instead of AES. This prevents the need to rely on computational hardness assumptions. Considering the short distance between the endpoints, the comment about physical exchanges of key material (see 5.4.3) also applies here. Amongst the use cases we analyzed, we view this one and 5.11 as the two more reasonable ones due to the lack of obvious and/or fundamental problems (in comparison with the other use cases) and because of the use of one-time pad encryption instead of AES encryption.

5.7 Metrics of an overbraider machine (3.7)

Aim

- Secure the transmission of manufacturing production data between the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS).
- Secure data from the NCC's Overbraider machine, which weaves carbon fiber to create precision hollow composite components, such as aircraft engine blades. This data is critical for the manufacturing processes and may include detailed production parameters, measurements, and assessments necessary for remote monitoring and control of manufacturing operations.

Used technology

- *Protocol and Devices:* Toshiba's QKD system using BB84/T12.
- *Connection:* The system uses BT Openreach's standard fiber optic infrastructure and includes QKD enabled encryption tunnels between two Edge firewalls. The data transmission occurs over a dedicated 7 km long point-to-connection between the NCC and CFMS sites.
- *Additional Crypto:* Unknown symmetric cipher to protect the transmission of manufacturing production data.

Analysis and recommendation

We arrive at similar conclusions as in section 5.4.3, in that we don't see anything fundamentally wrong about the way that QKD is used here.

5.8 Self-driving cars (3.8)

Aim

- Secure an OpenVPN connection, securing software updates and telemetry data of an autonomous control system of a driverless car.
- Secure the real-time transmission of telemetry data on the status of all its subsystems to the laboratory monitoring system.
- Secure software updates upon the release of new versions, preventing unauthorized access or alteration of the software update.

Used technology

- *Protocol and Devices:* QRate QKD system using BB84 [119].
- *Connection:* QKD between the driverless car and the data center during refueling or charging for an electric vehicle which occurs via an optical channel.
- *Additional Crypto:* OpenVPN over 4G LTE to protect software updates and telemetry data.

Analysis and recommendation

In the case of rental cars, we note that the owning company will be in regular physical contact with them for maintenance. In this scenario, installing pre-shared keys appears to be an alternative that uses much simpler and cheaper technology, while at the same time being significantly more secure since it does not have to rely on trusted nodes (recall section 2.4.1).

In the case of privately owned cars, we first note that transmitting significant amounts of real-time telemetry data to the manufacturer could pose a significant infraction of privacy, which would make transmission undesirable in any case. Even when setting these ethical concerns aside, it is still not clear why this would make a convincing use case: it would still be viable and more practical to rely on pre-installed key material that gets updated (replaced) during the necessary regular maintenance in a car workshop.

For the protection of software updates, we note that QKD is used purely to ensure authenticity. Like in the voting use case (5.1), this begs the question from where the QKD protocol derives its authenticated channel and why that authentication mechanism couldn't be used directly for the software updates instead.

5.9 Grid network (3.9)

Aim

- Secure Geneva's smart grid network (800+ power stations).
- Test and assess QKD technology in a real operational environment.
- Prevent hacking and ensure secure data transmission between power stations.

Used technology

- *Protocol and devices:* ID Quantique's DV-QKD system for QKD and Cisco's IOS-XE equipment to encrypt data in transit.
- *Connection:* Direct connection using a dedicated 3.4 km long dark fiber for QKD and classical channels.
- *Additional Crypto:* SKIP protocol and unknown symmetric cipher to encrypt data in transit.

Analysis and recommendation

The security goals of this use case seem underspecified – for example, the level of protection did not become fully clear: it neither became clear what kind of data it aims to protect, nor for how long, nor against which kinds of attacks. The stated security goals furthermore include phrasing that suggests that they are independent of the used cryptography, such as 'hackers taking control of the electricity distribution network' [97, Sec. 3.1] (which would go far beyond dealing with cryptography). For network takeovers, the main attack surfaces (code execution and privilege escalation) cannot be fixed on the level of cryptographic protocols. Our primary recommendation for this use case thus is to first create a clear threat model, to analyze which attacks follow from that threat model, and then to analyze which technologies can prevent these attacks. In case the involved data needs long-term confidentiality (e.g. private information on energy usage), then QKD could be an (albeit more expensive) alternative to PQC to accomplish that.

5.10 Authentication of smart grid communications (3.10)

Aim

- Achieve information-theoretic authentication in smart grid communications.
- Authenticate SCADA traffic which contains non-confidential control and measurement data.

Used technology

- *Protocol and devices:* Qubitekk's QKD system using an entanglement-based QKD protocol.
- *Connection:* Dedicated dark fiber for QKD and classical channels.
- *Additional Crypto:* GMAC with AES to authenticate SCADA traffic.

Analysis and recommendation

Although the presentation in [114] suggests that the solution achieves information-theoretic authentication, this is not the case. The solution uses GMAC with AES which is not information-theoretic secure. (GMAC with OTP would achieve statistical authenticity, but this drops to computational security when used with AES.)

This use case only requires authentication. With the same reasoning as for the other use cases that only require authenticity, voting (5.1) and software updates of self-driving cars (5.8), we assess QKD as not adding any value to this use case.

5.11 Genome distance sharing (3.11)

Aim

Secure the transmission of genome distance data.

Used technology

- *Protocol and devices:* ID Quantique's DV-QKD system and Huawei's CV-QKD system.
- *Connection:* Data transmission was achieved over 7 km long fibers between UPM and Ciemat and 24 km long fibers between Ciemat and CSIC. Ciemat functioned as a trusted node for the connection between CSIC and UPM.
- *Additional Crypto:* Secure multiparty computation, which used quantum oblivious transfer, to compare genome data. One-time pad encryption to secure the transmission of genome distance data.

Analysis and recommendation

We come to the same conclusions as for the genome distance sharing use case (5.6) with two additional remarks:

- As noted by the authors of the implementation, the current implementation is missing authentication for the one-time pad encryption [120].
- Pre-shared keys could be used as an alternative. In the case that 3 institutions all have 10 SARS-CoV-2 genome sequence and would like to calculate the phylogenetic tree as given by the example in [116], $18.6 * 10^3$ bits of key material would be necessary to share the distances between genome sequences. Although QKD might already be available in case quantum oblivious transfer is used, instead of using QKD for the sharing of genome distances, the institutions could share SD cards with 1 TB of key material with each other. This would be enough key material to calculate a phylogenetic tree more than 2 million times every day for a year[2] and could thus be used as an alternative to QKD in this use case.

[2] A 1 TB SD card can provide enough keys to calculate a phylogenetic tree $(10^{12} \cdot 8)/((18.6 \cdot 10^3)/2)/365.25 = 2\,355\,140$ times, every day.

Table 4: Security analysis of QKD Use Cases

Use case	Aim	Used technology	Security Requirements	Alternatives
5.1 Authenticity of election results	Ensures authenticity of election results during transmission. Secures the link between central ballot-counting stations and government data centers.	SARG04, AES-256, HMAC-SHA-256	Authenticity	PQ Signatures
5.2 Backup for disaster recovery	Additional security layer for encryption between headquarters and DRC. Protects sensitive business and customer data.	SARG04, AES-256	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.3 Financial data	Secures transmission of sensitive data between financial centers. Protects trading algorithms, customer accounts, etc.	BB84/T12, AES-256	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.4.1 Facial recognition	Secures transmission of biometric authentication data. Protects feature data in a face recognition system.	BB84 and DPS-QKD, Secret sharing, symmetric cipher used unknown	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.4.2 Key storage and backup	Encrypts digital asset components split using secret sharing. Protects private keys for digital assets such as cryptocurrencies. The to-be-protected assets are secrets for computationally secure cryptography	DV-QKD, OTP, Secret sharing	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.4.3 Medical image sharing	Encrypts data fragments during transmission between hospitals and external storage. Protects highly sensitive medical data.	DV-QKD and BB84/T12, AES, Secret sharing, TLS	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.4.4 Medical record backup	Secures transmission of medical records. Protects extremely sensitive personal data.	BB84, BB84/T12, DPS-QKD, CV-QKD, Secret sharing	Confidentiality, Authenticity	Pre-shared keys PQ key exchange

5.5 Connecting data centers	Secures symmetric key exchange between data centers. Protects utility operations and customer data.	COW, AES-256	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.6 Genome data	Secures transmission of genome data and video conferences. Protects highly sensitive genome data and video conferences.	BB84/T12, OTP	Confidentiality, Authenticity	Pre-shared keys PQ key exchange (losing everlasting confidentiality)
5.7 Metrics of an overbraider machine	Secures transmission of manufacturing data. Protects production parameters of composite components.	BB84/T12, symmetric cipher used unknown	Confidentiality, Authenticity	Pre-shared keys PQ key exchange
5.8 Self-driving Cars	Secures software updates and telemetry data. Quantum-protected software updates for the autonomous control system.	BB84, OpenVPN	Authenticity for Software Updates, Confidentiality and Authenticity for Telemetry.	Pre-shared keys PQ key exchange Signatures (auth only)
5.9: Grid network	Secure Communication between power stations, prevent hacking	DV-QKD, Peer-to-peer architecture, symmetric cipher used unknown	Authenticity, Maybe Confidentiality (unclear) (Secure implementations; not really a crypto-problem in the first place)	Pre-shared keys PQ key exchange
5.10: Authentication of smart grid communications	Ensure authenticity of measurement and control data	Entanglement-based QKD, GMAC with AES	Authenticity	Pre-shared keys
5.11: Genome distance sharing	Secures transmission of genome hamming distances	CV-QKD, OTP, quantum oblivious transfer, secure multiparty computation	Confidentiality, Authenticity	Pre-shared keys

6 Conclusion

As quantum computing continues to develop, there is increasing attention on the risks that surround traditional cryptography in the presence of quantum attackers. To mitigate these risks, it is necessary to consider alternative approaches such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). In this paper, we conducted an in-depth security evaluation of QKD-based approaches across various real-world use cases. Our analysis highlights both the theoretical strength of QKD (not having to rely on computational assumptions), as well as its theoretical and practical limitations, such as the need to rely on physical assumptions, high implementation costs in currently available systems, poor scaling behaviour, and limitations in applicability.

We compared QKD with other cryptographic alternatives, particularly with PQC, which offers a more direct transitioning path for existing systems and infrastructures. While PQC addresses the potential threats from quantum computers, QKD in conjunction with One-Time-Pads (OTPs) might be able to offer everlasting confidentiality. We analyzed sufficiently documented use cases and saw that in most, QKD provides very limited or no advantage over other methods for key establishment such as PQC or pre-shared keys. The analyzed examples included using QKD for authentication, using QKD with AES to secure data between just two specific locations over a short distance, and using QKD to secure digital signing keys. The only use cases where we saw that QKD might be able to provide an advantage are use cases that use QKD with OTP (instead of AES) to secure a short-distance connection, as this might be able to secure data against an attacker with unlimited computational resources. These use cases include sharing genome data using OTP. One other potential advantage of QKD is that it can provide PCS without relying on computational assumptions, although none of the analyzed use cases even mention this as a security requirement.

Decision-makers must weigh the trade-offs between QKD and PQC to select the most appropriate solution for securing their systems in the post-quantum era.

Appendix

A Not considered use cases

Here, we additionally list use cases that we encountered, but did not analyze due to lack of technical information.

A.1 Madrid QCI use cases

Besides not finding enough information for the use cases demonstrated by the Madrid QCI [121], we sometimes had other reasons for exclusion. We briefly discuss the use cases below:

- **Network security and attestation** The proof of transit protocol in this use case was proven to be insecure [122].
- **Critical Infrastructure Protection** While not enough information was available to analyze this use case, it seems comparable to 3.10.
- **QKD as a Cloud Service** Providing QKD as a cloud service is not a use case on itself, but rather a way to provide QKD.
- **e-Health services** Not enough information available to analyze the use case.
- **Quantum Cryptography for B2B and 5G** Not enough information available to analyze the use case.
- **Self-healed network management** Not enough information available to analyze the use case.
- **Quantum Cryptography with minimal amount of QKD devices allowing independent protection of users in collocated computing centers** Describes a feature of a QKD system, but not a use case.
- **Security independence of a network provider from QKD device manufacturers** Describes a feature, not a use case.
- **Open Call KaaS: Key as a Service** Providing QKD as a service is not a use case on itself, but rather a way to provide QKD.
- **OpenCall QGeKO** Satellite use cases are out of scope for this paper.

A.2 Quantum CTek use cases

The use cases listed on the website of Quantum CTek [34] did not include enough technical information for analysis and we therefore have been unable to verify the claims made by the original project. However, we still summarize the use cases including the unverified claims below.

1. **Hefei Metro Area Quantum Communication Demonstration Network** The Hefei Metro Area Quantum Communication Demonstration Network is the world's first large-scale quantum network, developed and constructed by QuantumCTek. Utilizing commercial optical fiber from radio and television operators, the network covers the main urban area of Hefei city. It serves a wide range of customers, including government departments, financial institutions, military enterprises, and research institutes. The network provides quantum-secure real-time voice and text communication, file transfer, and other functions. Its topology mirrors that of the operators, featuring a three-tier structure: core, convergence, and access layers. It boasts scalability, routing capabilities, attack alarms, and a monitoring and management system that allows administrators to remotely monitor network status, observe equipment operations, and perform timely diagnostics.
2. **Financial Information Quantum Communication Verification Network of Xinhua News Agency** This network connects the head office building of Xinhua News Agency with its Financial Information Exchange using commercial optical fiber. It provides highly confidential video and voice communication, real-time text interaction, and high-speed data transmission. The network has successfully verified a trading system based on quantum cryptography, achieving simulated equity and bond transactions.
3. **Communication Support System for a Major Event** Designed for a significant event, this system includes a quantum telephone network and a high-speed data transmission line with quantum-safe encryption. It uses QOS-AT networking products to distribute keys without intermediate nodes. Hot backup technology ensures uninterrupted data transmission even in the event of a line fault.
4. **Quantum Secure Communication Project for Public Security** This project establishes a standard quantum network with a cycled backbone centered around a centralized control station. Quantum gateways at each end-user node enable network expansion. As the quantum secure communication system scales, terminal nodes can be upgraded to centralized control stations, facilitating the transition to a larger quantum network.
5. **Jinan Quantum Communication Demonstration Network** Building on the Hefei metro area's technological achievements, the Jinan network promises a secure, reliable, and integrated QKD system. At its inception, it featured the world's largest number of quantum nodes, users, business categories, and distributed keys for a metro area quantum communication network. The network supports various sectors, including government, finance, scientific research, and education, providing high-quality user experiences.
6. **Banking Regulatory Information Acquisition Demonstration** Under the guidance of the China Banking Regulatory Commission, this network facilitates data acquisition among a supervisory unit headquarters, a local supervisory unit, and a commercial bank using a quantum secure communication network. It supports practical information submission and management, allowing banks to securely transmit data to supervisory units.
7. **Quantum Secure Communication 'Beijing-Shanghai Backbone' Project** This project aims to build a quantum secure communication backbone connecting Beijing and Shanghai via Jinan and Hefei, spanning over 2,000 kilometers. It links metro area access networks across various cities, creating a wide-area optical fiber quantum communication network. The project serves as a platform for large-scale quantum communication technology verification, research, and application demonstrations.
8. **Electronic Record Application Database Synchronization for a Large State-owned Bank** Guided by the China Banking Regulatory Commission, a large state-owned bank uses quantum communication technology to regularly synchronize archived data from its main database to a standby database across the city. This ensures data synchronization for remote databases.
9. **Alibaba Quantum Secure Domain** By establishing multiple quantum secure domains within the Alibaba Cloud network, Alibaba achieves inter-city data center interconnection via Quantum Portal. This setup provides customers with secure data transmission services, including key distribution, confidentiality, and networking, verified through actual business testing.
10. **ICBC Offsite Data Quantum Encryption Transmission** Using QuantumCTek's platform, the Industrial and Commercial Bank of China (ICBC) has successfully implemented quantum

communication technology for the Beijing-Shanghai offsite wide area network under the 'two cities and three centers' framework. This marks the first application of quantum communication technology over a thousand kilometers in the banking industry, enabling secure online banking data transmission.

11. **Mybank Cloud Quantum Encryption Communication** Mybank utilizes QuantumCTek's quantum communication technology for long-distance cloud quantum encryption communication of credit business data on dedicated cloud channels between metro areas.
12. **Bank of Communications Enterprise Online Banking Use Case** In February 2017, the Bank of Communications implemented a use case for enterprise online banking based on QuantumCTek's platform. This marked the first application of quantum secure communication technology in real-time trading for financial enterprise online banking users.
13. **Quantum Technology in Metro Ring Network of Beijing Rural Commercial Bank** The Beijing Rural Commercial Bank applied quantum encryption technology to its metro area ring network. This enabled secure transmission of office, production, and disaster recovery data among various locations, marking the first use of quantum communication technology in a metro area optical fiber ring network within the financial industry.
14. **World's First Commercial Ultra-long Distance Co-propagation of QKD and Terabit Classical Optical Data Channels** The China Telecom Beijing Institute, with QuantumCTek, Fiber Home, and ZTE Anhui Wan Tong, released the test results for the world's first commercial ultra-long distance co-propagation of QKD and large-capacity classical optical data channels. This test utilized a commercial QKD system and an 8Tbps large capacity dense wavelength division multiplexing (DWDM) system, achieving QKD transmission over 100 kilometers without the use of trusted nodes.

Declarations

Availability of data and materials

Data sharing does not apply to this article as no datasets were generated or analysed during the current study. The analysis of use case was performed entirely on the information and data available in the references listed.

Competing interests

The authors declare that they have no competing interests.

Funding

This work was in part funded by the Dutch Ministry of Economic Affairs and Climate Policy (EZK) as part of the Quantum Delta NL National Growthfunds on Quantum Technology and by the NWO NWA project FIQCS (NWA.1436.20.005)

Authors' contributions

NA, BC and SD conducted the literature search for relevant use cases. NA, BC, SD, KH, FJW and SV contributed to the background and discussion of QKD and PQC. NA, BC, SD, KH, FJW and SV devised the analysis method. NA, SD, KH, FJW conducted the use case analysis. NA, BC, SD, KH and FJW wrote the manuscript. CO, SR, BS, ITM and SV reviewed the manuscript text. All authors contributed to final revision of the manuscript. All authors read and approved the final version of the manuscript.

Acknowledgements

Not applicable.

References

[1] Tsubasa Ichikawa et al. "Current numbers of qubits and their uses". In: *Nature Reviews Physics* 6.6 (May 2024), pp. 345–347. ISSN: 2522-5820. DOI: 10.1038/s42254-024-00725-0.

[2] Travis L. Scholten et al. *Assessing the Benefits and Risks of Quantum Computers*. 2024. eprint: arXiv:2401.16317.
[3] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.
[4] General Intelligence and Security Service. *Prepare for the threat of quantum computers*. Feb. 17, 2022. URL: https://english.aivd.nl/binaries/aivd-en/documenten/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers/Prepare+for+the+threat+of+quantumcomputers.pdf.
[5] Lydia Garms et al. "Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem". In: *Advanced Quantum Technologies* 7.4 (Apr. 2024), p. 2300304. ISSN: 2511-9044, 2511-9044. DOI: 10.1002/qute.202300304.
[6] Pei Zeng et al. *Practical hybrid PQC-QKD protocols with enhanced security and performance*. Version Number: 3. 2024. DOI: 10.48550/ARXIV.2411.01086.
[7] National Institute of Standards and Technology. *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*. ID Quantique. Aug. 13, 2024. URL: https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved (visited on 11/20/2024).
[8] French Cybersecurity Agency (ANSSI) et al. *Position Paper on Quantum Key Distribution*. Jan. 26, 2024. URL: https://open.overheid.nl/documenten/797c7e8e-9c70-4a98-bfb4-11cb5f19515f/file.
[9] CEN-CENELEC FGQT. *Standardization Roadmap on Quantum Technologies*. Jan. 3, 2023. URL: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf.
[10] Telecommunications Standards Development Society India (TSDSI). "Standardization Opportunities for Quantum Communication Technologies, Standardization Gaps and demands, Challenges and Opportunities to arise in the future". In: *White paper* (Dec. 2024). URL: https://tsdsi.in/wp-content/uploads/2025/01/Quantum-WP-Final_Webfile-20250101.doc.pdf.
[11] Koji Azuma et al. "Quantum repeaters: From quantum networks to the quantum internet". In: *Rev. Mod. Phys.* 95 (4 Dec. 2023), p. 045006. DOI: 10.1103/RevModPhys.95.045006.
[12] Andrej Kržič et al. "Towards metropolitan free-space quantum networks". In: *npj Quantum Information* 9.1 (Sept. 2023). ISSN: 2056-6387. DOI: 10.1038/s41534-023-00754-0.
[13] National Security Agency (NSA). *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. URL: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (visited on 09/11/2024).
[14] Renato Renner and Ramona Wolf. *The debate over QKD: A rebuttal to the NSA's objections*. 2023. eprint: arXiv:2307.15116.
[15] National Cyber Security Center. *Quantum security technologies*. Mar. 24, 2020. URL: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.
[16] Isabelle Desouches. *Quantum Initiatives Worldwide 2024 - Qureca — qureca.com*. https://www.qureca.com/quantum-initiatives-worldwide/.
[17] https://www.quantum.gov/.
[18] *The European Quantum Communication Infrastructure (EuroQCI) Initiative — digital-strategy.ec.europa.eu*. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.
[19] *The future is Quantum — qt.eu*. https://qt.eu/.
[20] *UK National Quantum Technologies Programme — uknqt.ukri.org*. https://uknqt.ukri.org/.
[21] *Quantum Communications Hub — quantumcommshub.net*. https://www.quantumcommshub.net/.
[22] *Quantum Networks — quantumdelta.nl*. https://quantumdelta.nl/catalyst-programs/quantum-network.
[23] *Cabinet approves National Quantum Mission to scale-up scientific & industrial R&D for quantum technologies | Department Of Science & Technology — dst.gov.in*. https://dst.gov.in/cabinet-approves-national-quantum-mission-scale-scientific-industrial-rd-quantum-technologies.

[24] *Products — idquantique.com*. https://www.idquantique.com/quantum-safe-security/products/. (Visited on 12/04/2024).
[25] *Toshiba Quantum: QKD & Quantum Security Solutions — toshiba.eu*. https://www.toshiba.eu/quantum/.
[26] James Dargan. *Top 25 Quantum Cryptography & Encryption Companies [2024] — thequantuminsider.com*. https://thequantuminsider.com/2021/01/11/25-companies-building-the-quantum-cryptography-communications-markets/.
[27] *Top Quantum Key Distribution companies | VentureRadar — ventureradar.com*. https://www.ventureradar.com/keyword/Quantum%20Key%20Distribution.
[28] Business Research Insights. *Quantum Communication Market Size, Share, Growth, and Industry Analysis, (Hardware, Software and Services), By Application (Government, Military And Defense, Telecommunication, BFSI, Enterprise And Industrial), Regional Insights, and Forecast To 2032*. Base Year: 2023, Historical Data: 2019-2022. Nov. 2024, p. 82. URL: https://www.businessresearchinsights.com/market-reports/quantum-communication-market-113933.
[29] QK Distribution. "GS QKD 002-V1. 1.1-Quantum Key Distribution; Use Cases". In: *Innovation* 1 (2010), pp. 1–32. URL: https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf.
[30] Marco Gramegna, Paolo Traina, et al. "FGQT Q05 Quantum Technologies Use Cases [written by the CEN-CENELEC Focus Group on Quantum Technologies (FGQT)]". In: (2023). URL: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q05_quantumtechnologiesusecases_release1.pdf.
[31] *Use Cases | Quantum Key Distribution | TOSHIBA DIGITAL SOLUTIONS CORPORATION — global.toshiba*. https://www.global.toshiba/ww/products-solutions/security-ict/qkd/cases.html. [Accessed 28-01-2025].
[32] *Applications — idquantique.com*. https://www.idquantique.com/quantum-safe-security/applications/. [Accessed 28-01-2025].
[33] *Quantum Cryptography Case Studies | QNu Labs - Real-World Security Solutions — qnulabs.com*. https://www.qnulabs.com/case-studies. [Accessed 28-01-2025].
[34] *Typical Cases_QuantumCTek 2013; Quantum Secures Every Bit — quantum-info.com*. http://www.quantum-info.com/English/case/. (Visited on 06/28/2024).
[35] *Quantum Communications in Real World Applications | Quantum Xchange — quantumxc.com*. https://quantumxc.com/blog/quantum-communications-real-world-applications/. [Accessed 28-01-2025].
[36] Katriel Cohn-Gordon, Cas Cremers, and Luke Garratt. "On Post-compromise Security". In: *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*. 2016 IEEE 29th Computer Security Foundations Symposium (CSF). Lisbon: IEEE, June 2016, pp. 164–178. DOI: 10.1109/csf.2016.19.
[37] J. Lawrence Carter and Mark N. Wegman. "Universal classes of hash functions (Extended Abstract)". In: *Proceedings of the ninth annual ACM symposium on Theory of computing - STOC '77*. the ninth annual ACM symposium. Boulder, Colorado, United States: ACM Press, 1977, pp. 106–112. DOI: 10.1145/800105.803400.
[38] Renato Renner and Ramona Wolf. "Quantum Advantage in Cryptography". In: (2022). Publisher: arXiv Version Number: 2. DOI: 10.48550/ARXIV.2206.04078.
[39] Roger Colbeck and Renato Renner. "No extension of quantum theory can have improved predictive power". In: (2010). Publisher: arXiv Version Number: 3. DOI: 10.48550/ARXIV.1005.5173.
[40] Daniel J. Bernstein. *Is the security of quantum cryptography guaranteed by the laws of physics?* 2018. arXiv: 1803.04520 [quant-ph]. URL: https://arxiv.org/abs/1803.04520.
[41] Joseph M. Renes and Renato Renner. *Are quantum cryptographic security claims vacuous?* Version Number: 1. 2020. DOI: 10.48550/ARXIV.2010.11961.
[42] Kenneth G. Paterson, Fred Piper, and Ruediger Schack. "Quantum cryptography: a practical information security perspective". In: (2004). Publisher: arXiv Version Number: 2. DOI: 10.48550/ARXIV.QUANT-PH/0406147.
[43] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. "The Case for Quantum Key Distribution". In: *Quantum Communication and Quantum Networking*. Ed. by Alexander Sergienko, Saverio Pascazio, and Paolo Villoresi. Vol. 36. Series Title: Lecture Notes of the

Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 283–296. ISBN: 978-3-642-11730-5. DOI: 10.1007/978-3-642-11731-2_35.

[44] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/359340.359342.

[45] W. Diffie and M. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (Nov. 1976), pp. 644–654. ISSN: 0018-9448, 1557-9654. DOI: 10.1109/TIT.1976.1055638.

[46] Federal Information Processing Standards Publication. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. DOI: 10.6028/NIST.FIPS.203.

[47] Joppe Bos et al. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM". In: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2018, pp. 353–367. DOI: 10.1109/EuroSP.2018.00032.

[48] Federal Information Processing Standards Publication. *Module-Lattice-Based Digital Signature Standard*. DOI: 10.6028/NIST.FIPS.204.

[49] Leo Ducas et al. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018.1 (Feb. 2018), pp. 238–268. DOI: 10.13154/tches.v2018.i1.238-268.

[50] Federal Information Processing Standards Publication. *Stateless Hash-Based Digital Signature Standard*. DOI: 10.6028/NIST.FIPS.205.

[51] Daniel J. Bernstein et al. "The SPHINCS+ Signature Framework". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. London, United Kingdom: Association for Computing Machinery, 2019, pp. 2129–2146. ISBN: 9781450367479. DOI: 10.1145/3319535.3363229.

[52] Pierre-Alain Fouque et al. *Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU, Specification v1.2*. https://falcon-sign.info/falcon.pdf.

[53] David Adrian et al. *A new path for Kyber on the web*. https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html.

[54] *Using hybrid post-quantum TLS with AWS KMS*. https://docs.aws.amazon.com/kms/latest/developerguide/pqtls.html.

[55] *iMessage with PQ3: The new state of the art in quantum-secure messaging at scale*. https://security.apple.com/blog/imessage-pq3/.

[56] Ehren Kret and Rolfe Schmidt. *The PQXDH Key Agreement Protocol*. https://signal.org/docs/specifications/pqxdh/.

[57] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. ACM* 56.6 (Sept. 8, 2009), 34:1–34:40. ISSN: 0004-5411. DOI: 10.1145/1568318.1568324.

[58] Jeffrey Hoffstein et al. "NTRUSign: Digital Signatures Using the NTRU Lattice". In: *Topics in Cryptology — CT-RSA 2003*. Ed. by Marc Joye. Red. by Gerhard Goos, Juris Hartmanis, and Jan Van Leeuwen. Vol. 2612. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 122–140. ISBN: 978-3-540-00847-7. DOI: 10.1007/3-540-36563-X_9.

[59] ITU-T. *Quantum key distribution network interworking -Framework - Recommendation ITU-T Y.3810*. Standard. Geneva, CH: Telecommunication Standardization Sector of ITU, Sept. 2022.

[60] M. Sasaki et al. "Tokyo QKD Network and the evolution to Secure Photonic Network". In: *CLEO: 2011 - Laser Science to Photonic Applications*. 2011. DOI: 10.1364/CLEO_AT.2011.JTuC1.

[61] Carlos Rubio García et al. "Secure and Agile 6G Networking – Quantum and AI Enabling Technologies". In: *2023 23rd International Conference on Transparent Optical Networks (ICTON)*. 2023, pp. 1–4. DOI: 10.1109/ICTON59386.2023.10207418.

[62] Pouya Mehdizadeh et al. "Quantum-Classical Coexistence in Multi-Band Optical Networks: A Noise Analysis of QKD". In: *IEEE Communications Letters* 28.3 (2024), pp. 488–492. DOI: 10.1109/LCOMM.2024.3356165.

[63] Juan Morales Sáez et al. "Current Status, Gaps, and Future Directions in Quantum Key Distribution Standards: Implications for Industry". In: *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. 2024, pp. 341–345. DOI: 10.1109/QCNC62729.2024.00059.

[64] Toshiba. *Long-Distance QKD System LD*. QKD Systems. Mar. 22, 2023. URL: https://www.toshiba.eu/quantum/products/quantum-key-distribution/long-distance-qkd-system-ld/ (visited on 01/30/2025).
[65] IDQ. *Quantum-Safe Security Products*. ID Quantique. Jan. 30, 2025. URL: https://www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution (visited on 01/30/2025).
[66] Jiu-Peng. Chen et al. "Twin-field quantum key distribution over a 511km optical fibre linking two distant metropolitan areas". In: *Nature Photonics* 15 (2021), pp. 570–575. DOI: 10.1038/s41566-021-00828-5.
[67] Duan Huang et al. "Field demonstration of a continuous-variable quantum key distribution network". In: *Opt. Lett.* 41.15 (Aug. 2016), pp. 3511–3514. DOI: 10.1364/OL.41.003511.
[68] Brian P. Williams et al. "Field test of continuous-variable quantum key distribution with a true local oscillator". In: *Phys. Rev. Applied* 21.1 (2024), p. 014056. DOI: 10.1103/PhysRevApplied.21.014056. arXiv: 2309.03959 [quant-ph].
[69] Xin Wang et al. "Field Trial of 7 × 89λ × 256 Gb/s C-Band Classical / CVQKD Co-Existence Transmission over 7-Core Fiber". In: *2023 Asia Communications and Photonics Conference/2023 International Photonics and Optoelectronics Meetings (ACP/POEM)*. 2023, pp. 1–4. DOI: 10.1109/ACP/POEM59049.2023.10369872.
[70] Qin Liao et al. "Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source". In: *Phys. Rev. A* 102 (3 Sept. 2020), p. 032604. DOI: 10.1103/PhysRevA.102.032604.
[71] Cuong Le Quoc and Patrick Bellot. "A New Proposal for QKD Relaying Models". In: *2008 Proceedings of 17th International Conference on Computer Communications and Networks*. 2008, pp. 1–6. DOI: 10.1109/ICCCN.2008.ECP.92.
[72] Cédric Ware et al. "Potential Impact of CV-QKD Integration on Classical WDM Network Capacity". In: *IEEE Photonics Technology Letters* 34.18 (2022), pp. 957–960. DOI: 10.1109/LPT.2022.3195433.
[73] Ivan B. Djordjevic. "Optimized-Eight-State CV-QKD Protocol Outperforming Gaussian Modulation Based Protocols". In: *IEEE Photonics Journal* 11.4 (2019), pp. 1–10. DOI: 10.1109/JPHOT.2019.2921521.
[74] Fotini Karinou et al. "Toward the Integration of CV Quantum Key Distribution in Deployed Optical Networks". In: *IEEE Photonics Technology Letters* 30.7 (2018), pp. 650–653. DOI: 10.1109/LPT.2018.2810334.
[75] Yichen Zhang et al. "Continuous-variable quantum key distribution system: Past, present, and future". In: *Applied Physics Reviews* 11.1 (Mar. 2024), p. 011318. ISSN: 1931-9401. DOI: 10.1063/5.0179566. eprint: https://pubs.aip.org/aip/apr/article-pdf/doi/10.1063/5.0179566/19855574/011318_1_5.0179566.pdf.
[76] François Roumestan et al. "High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM". In: *2021 European Conference on Optical Communication (ECOC)*. 2021, pp. 1–4. DOI: 10.1109/ECOC52684.2021.9606013.
[77] João Frazão et al. "Experimental Demonstration of Real-time Bob Continuous-Variable Quantum Key Distribution over 25.7-km fiber". English. In: 24th Asian Quantum Information Science Conference, AQIS 2024, AQIS 2024 ; Conference date: 26-08-2024 Through 30-08-2024. Aug. 2024.
[78] Sara Ahmed et al. "Security Analysis of Gaussian and Discrete Modulations in FSO/CV-QKD Systems Employing LLO Under Phase and Amplitude Attacks". In: *IEEE Access* 10 (2022), pp. 100041–100053. DOI: 10.1109/ACCESS.2022.3208132.
[79] *QKD Technology — idquantique.com*. https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/.
[80] *Tosiba QKD Use Cases*. https://www.global.toshiba/ww/products-solutions/security-ict/qkd/cases.html.
[81] *QKD — thinkquantum.com*. https://www.thinkquantum.com/quky/.
[82] *openqkd.eu*. https://openqkd.eu/.
[83] *OPENQKD - Open European Quantum Key Distribution Testbed — qt.eu*. https://qt.eu/projects/archive/communication/openqkd.
[84] ID Quantique. *IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation*. ID Quantique. Nov. 23, 2017. URL: https://www.idquantique.

com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/ (visited on 03/13/2024).

[85] ID Quantique. *Use Case: Government*. Aug. 31, 2023. URL: https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-/-/-/-/Geneva%20Govt_%20DCI%20QKD%20Use%20Case.pdf (visited on 03/13/2024).

[86] Lester Houston III. *Secure Ballots Using Quantum Cryptography*. Dec. 2, 2007. URL: https://www.cse.wustl.edu/%7Ejain/cse571-07/ftp/ballots/index.html (visited on 06/19/2024).

[87] ID Quantique. *Specsheet Cerberis V1*. Apr. 5, 2007. URL: https://web.archive.org/web/20070728200426/http://www.idquantique.com/products/files/Cerberis-specs.pdf (visited on 03/13/2024).

[88] ID Quantique. *Spec Vectis V2*. Apr. 14, 2005. URL: https://web.archive.org/web/20071015070059/http://idquantique.com/products/files/vectis-specs.pdf (visited on 03/13/2024).

[89] Nicolas Gisin. Oct. 31, 2007. URL: https://www.schneier.com/blog/archives/2007/10/switzerland_pro.html/#comment-73567 (visited on 01/30/2025).

[90] ID Quantique. *Use Case: Financial Services*. Aug. 31, 2023. URL: https://marketing.idquantique.com/acton/attachment/11868/f-0211/1/-/-/-/-/Financial%20Services_DRC%20QKD%20Use%20Case.pdf.

[91] ID Quantique. *Cerberis Specs*. Jan. 20, 2012. URL: https://web.archive.org/web/20170129080704/http://www.idquantique.com/wordpress/wp-content/uploads/Cerberis-Datasheet.pdf.

[92] Toshiba. *Securing the critical link between front office and back office operations of major financial institutions*. URL: https://www.global.toshiba/ww/products-solutions/security-ict/qkd/cases/case2.html (visited on 06/04/2024).

[93] Quantum Xchange. *Quantum Xchange Tests Toshiba's Quantum Key Distribution System / Quantum Xchange*. Apr. 25, 2019. URL: https://quantumxc.com/press-release/testing-toshibas-quantum-key-distribution-system/ (visited on 06/18/2024).

[94] 生体認証データの高秘匿・高可用性な伝送・保管を量子暗号を用いて実現. NEC. Oct. 29, 2019. URL: https://jpn.nec.com/press/201910/20191029_02.html (visited on 06/03/2024).

[95] ID Quantique. *Use Case: Finance - Digital Assets Storage*. Aug. 31, 2023. URL: https://marketing.idquantique.com/acton/attachment/11868/f-b2d8657c-6132-434c-8f38-09ee1ed5d9bd/1/-/-/-/-/IDQ-Mt%20Pelerin_Quantum%20Vault%20Use%20Case.pdf.

[96] ID Quantique. *ID Quantique and Mt Pelerin start testing their quantum-safe digital asset custody solution in Geneva*. ID Quantique. Mar. 26, 2020. URL: https://www.idquantique.com/id-quantique-and-mt-pelerin-start-testing-their-quantum-safe-digital-asset-custody-solution-in-geneva/ (visited on 01/31/2025).

[97] Jean-Sébastien Pegon. *Second and Final Report on Field Trial Execution*. Mar. 1, 2023. URL: https://openqkd.eu/wp-content/uploads/2024/05/D8-7.pdf.

[98] Adi Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (Nov. 1, 1979), pp. 612–613. ISSN: 0001-0782. DOI: 10.1145/359168.359176.

[99] Bruno Huttner. "The Quantum Vault". Quantum Safe Security Live use cases in Geneva - with Equinix, Mt Pelerin and ID Quantique. Mar. 26, 2020. URL: https://www.youtube.com/watch?v=CtMrCcTFMDk.

[100] Bernhard Zatoukal et al. "OpenQKD Use-case for Securing Sensitive Medical Data at rest and in transit". In: *2021 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)*. 2021 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC). June 2021, pp. 1–1. DOI: 10.1109/CLEO/Europe-EQEC52157.2021.9542590.

[101] fragmentiX Storage Solutions GmbH. *Medical Data successfully protected by quantum-cryptography in Graz*. Oct. 12, 2020. URL: https://marketing.idquantique.com/acton/attachment/11868/f-2b39fb7a-37d5-436a-9b20-49f95100585a/1/-/-/-/-/IDQ-fragmentiX_pressrelease_OpenQKD_2020-12-10_EN.pdf.

[102] Werner Strasser. "fragmentiX Secret Sharing". Nov. 11, 2020. URL: https://www.unibw.de/code/events/code2020_content/code2020_ws2_fragmentix.pdf.

[103] NEC. *NEC, NICT and ZenmuTech use quantum cryptography to encrypt, transmit and backup electronic medical records*. NEC. Oct. 22, 2020. URL: https://www.nec.com/en/press/202010/global_20201022_01.html (visited on 06/03/2024).

[104] Masahide Sasaki. "QKD applications in Japan: Healthcare and IoT". Sept. 14, 2017. URL: https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/NICT_SASAKI.pdf (visited on 11/27/2024).

[105] Ronald L. Rivest. "All-or-nothing encryption and the package transform". In: *Fast Software Encryption*. Ed. by Eli Biham. Vol. 1267. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 210–218. ISBN: 978-3-540-63247-4. DOI: 10.1007/BFb0052348.

[106] ID Quantique. *Future-proof datacenter interconnection*. Aug. 31, 2023. URL: https://marketing.idquantique.com/acton/attachment/11868/f-deeaa59c-bec2-489a-afa7-5e5eefdd5b8a/1/-/-/-/-/IDQ-ADVA-SIG_Future-Proof%20Datacenter%20Interconnection%20Use%20Case.pdf.

[107] Toshiba. *Securing the high speed transfer of large scale sensitive genome data between two remote sites*. URL: https://www.global.toshiba/ww/products-solutions/security-ict/qkd/cases/case1.html (visited on 06/03/2024).

[108] *First real-time quantum system for genomic medicine*. URL: https://www.toshiba.eu/quantum/news/worlds-first-development-and-demonstration-of-a-quantum-cryptographic-communication-technology-applied-system-for-genomic-medicine/ (visited on 10/08/2024).

[109] *World-first Demonstration of Real-time Transmission of Whole-genome Sequence Data Using Quantum Cryptography:Quantum encryption technology capable of large-capacity data transmission allows practical applications to genomic research and genomic medicine | Corporate Research & Development Center | Toshiba*. Toshiba. Jan. 14, 2020. URL: https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/20/2001-01.html (visited on 11/06/2024).

[110] CFMS. *First Quantum Key Distribution Trial for Manufacturing Passes Test*. CFMS. URL: https://cfms.org.uk/article/first-quantum-key-distribution-trial-for-manufacturing-passes-test/ (visited on 06/04/2024).

[111] CFMS. *QKD for secure Inter-Site Connectivity*. CFMS. URL: https://cfms.org.uk/article/qkd-for-secure-inter-site-connectivity/ (visited on 06/04/2024).

[112] DETI and cfms. *Quantum Key Distribution (QKD) for Secure Inter-Site Connectivity Successful Trial of Remote Monitoring for Manufacturing*. Apr. 19, 2021. URL: https://cfms.org.uk/wp-content/uploads/2024/07/Quantum-Key-Distribution-QKD-for-Secure-Inter-Site-Connectivity-Successful-Trial.pdf.

[113] Center for Technologies in Robotics and Mechatronics Components. Университет Иннополис внедрил в беспилотники систему квантового распределения ключей для защиты их от взлома — Центр технологий компонентов робототехники и мехатроники. 14 мая 2021. URL: https://robotics.innopolis.university/news/universitet-innopolis-vnedril-v-bespilotniki-sistemu-kvantovogo-raspredeleniya-klyuchej-dlya-zashhity-ih-ot-vzloma/ (дата обр. 21.05.2024).

[114] Muneer Alshowkan et al. "Authentication of smart grid communications using quantum key distribution". In: *Scientific Reports* 12.1 (July 26, 2022), p. 12731. ISSN: 2045-2322. DOI: 10.1038/s41598-022-16090-w.

[115] Lina Moscoso. *Quantum Enabled Private Recognition of Composite Signals in Genome*. Apr. 2021. URL: https://qugenome.av.it.pt/Outputs.html (visited on 10/21/2024).

[116] Manuel B. Santos et al. "Private Computation of Phylogenetic Trees Based on Quantum Technologies". In: *IEEE Access* 10 (2022), pp. 38065–38088. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3158416.

[117] ZenmuTech. *About our core technology: secret sharing | ZenmuTech, Inc.* ZenmuTech, Inc. Oct. 10, 2024. URL: https://en.zenmutech.com/sss/ (visited on 01/30/2025).

[118] Federico Giacon, Felix Heuer, and Bertram Poettering. *KEM Combiners*. 2018. URL: https://eprint.iacr.org/2018/024 (visited on 03/20/2024).

[119] QRate: Квантовое шифрование. Безопасность, гарантированная законами физики — goqrate.com. https://goqrate.com/.

[120] Manuel Santos. *private-phylogenetic-analysis/smc_engine/src/qHamParties.cpp at 4c8348c857bca0cfc74493067f3af7d15e8cd0b6 · manel1874/private-phylogenetic-analysis*. Nov. 23, 2022. URL: https://github.com/manel1874/private-phylogenetic-analysis/blob/4c8348c857bca0cfc74493067f3af7d15e8cd0b6/smc_engine/src/qHamParties.cpp#L810 (visited on 11/22/2024).

[121] V Martin et al. “MadQCI: a heterogeneous and scalable SDN QKD network deployed in production facilities”. In: *arXiv preprint arXiv:2311.12791* (2023).

[122] Christian Huitema. *[secdir] Secdir last call review of draft-ietf-sfc-proof-of-transit-08*. IETF Mail List Archives. Sept. 20, 2021. URL: https://mailarchive.ietf.org/arch/msg/secdir/oatRrqmn1SSSqpwxBmTtu9DDYqc/ (visited on 10/08/2024).