frontiers | Frontiers in Quantum Science and Technology

TYPE Perspective
PUBLISHED 14 April 2023
DOI 10.3389/frqst.2023.1164428

OPEN ACCESS

EDITED BY
Laszlo Gyongyosi,
Budapest University of Technology and Economics, Hungary

REVIEWED BY
Michele Amoretti,
University of Parma, Italy
Yuan Cao,
Nanjing University of Posts and Telecommunications, China

*CORRESPONDENCE
Aleksey K. Fedorov,
akf@rqc.ru

SPECIALTY SECTION
This article was submitted to Quantum Communication, a section of the journal Frontiers in Quantum Science and Technology

RECEIVED 12 February 2023
ACCEPTED 23 March 2023
PUBLISHED 14 April 2023

CITATION
Fedorov AK (2023), Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. *Front. Quantum Sci. Technol.* 2:1164428. doi: 10.3389/frqst.2023.1164428

Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together

Aleksey K. Fedorov[1,2]*

[1]Russian Quantum Center, Skolkovo, Moscow, Russia, [2]National University of Science and Technology "MISIS", Moscow, Russia

Most currently used cryptographic tools for protecting data are based on certain computational assumptions, which makes them vulnerable with respect to technological and algorithmic developments, such as quantum computing. One existing option to counter this potential threat is quantum key distribution, whose security is based on the laws of quantum physics. Quantum key distribution is secure against unforeseen technological developments. A second approach is post-quantum cryptography, which is a set of cryptographic primitives that are believed to be secure even against attacks with both classical and quantum computing technologies. From this perspective, this study reviews recent progress in the deployment of the quantum-secured infrastructure based on quantum key distribution, post-quantum cryptography, and their combinations. Various directions in the further development of the full-stack quantum-secured infrastructure are also indicated. Distributed applications, such as blockchains and distributed ledgers, are also discussed.

KEYWORDS

quantum key distribution, post-quantum cryptography, quantum blockchain, quantum algorithm, quantum computing, quantum communication

1 Introduction

The amount of data that human society creates, collects, copies, transmits, and stores has increased rapidly (STATISTA, 2020). Such digitalization increases demand efficient methods for (long-term) data protection. Moreover, the portion of data requiring protection is also expected to grow annually (Anant et al., 2020).

Among existing ways to protect data in the current digital era, *cryptography* plays a central role in ensuring the security and privacy of information, with applications ranging from personal data to critical infrastructure. The basic premise of cryptography is to realize *encryption*, i.e., a transformation of data to a form that maintains[1] its accessibility for legitimate communication (commonly referred to as Alice and Bob) but not for a third unauthorized party (Eve). This allows the prevention of unauthorized extraction of information that is transmitted over an insecure channel (Schneier, 1996). The idea

1 V.A. Kotel'nikov, Classified Report (1941).

behind this premise is that a certain parameter, known as a *cryptographic key*, determines the choice of a specific transformation of the information (among possible transformations) when performing encryption.

As shown by Shannon (1948) and, independently, by Kotelnikov, there is a cryptographic algorithm; namely, the one-time pad, also known as the Vernam Cipher, which is perfectly secure (Vernam, 1926). Perfect or information-theoretic security here means that the scheme remains secure even if one assumes that the eavesdropper has unlimited computational resources (its abilities are limited only by the laws of physics). In this scheme, a legitimate side of communication, Alice, encrypts her message, a string of bits denoted by the binary number m with the use of a randomly generated key k as $d = m \oplus k$, where $\oplus$ denotes modulo-2 summation. The message is then sent to Bob, who decrypts the message as $d \oplus k = m \oplus k \oplus k = m$. However, the cost for this level of security is the fact that cryptographic key k should be 1) random, 2) used only once, and 3) has a length in bits that is not less than the length of the message to be encrypted. The class of cryptosystems that uses the same key for encrypting and decrypting data, as in the Vernam Cipher, is known as *symmetric* cryptography (or private-key cryptography).

Cryptographic keys are a valuable resource; as emphasized by Schneier, (1996): "Keys are as valuable as all the messages they encrypt, since knowledge of the key gives knowledge of all the messages. For encryption systems that span the world, the key distribution problem can be a daunting task." Thus, key distribution is crucial for cryptography. One possible solution is to use trusted couriers, which physically, by non-digital means, transfer cryptographic keys between places. Although this approach may seem rudimentary, it is still used for specific applications (Mulholland et al., 2017). However, in the era of digital communications, it is impossible to use trusted couriers to supply cryptographic keys to all users of global, distributed communication networks. Moreover, the human factor may impose additional threats: if the courier knows the key, then any data that are protected by this key are accessible unless the key is changed; moreover, it is almost impossible to identify an attack; thus, this vulnerability can be used for a long time. One can think of more frequent key changes; however, this increases the cost of the trusted-courier-based key distribution. As noted in the seminal paper by Diffie and Hellman (1976), the cost and delay imposed by a "physical" key distribution method is "a major barrier." Existing symmetric cryptographic tools, such as AES (the Advanced Encryption Standard), address common private keys of lengths that are less than the sizes of the messages. In this sense, the problem of their security belongs to the matter of practical (computational) security.

An alternative is to use so-called *public-key* or *asymmetric* encryption systems, which are based on the idea of reducing the problem of unauthorized access to information to solving a computational problem that is believed to be hard (Diffie and Hellman, 1976). For example, multiplying two large prime numbers, P and Q, is easy (at it is then easy to verify that the multiplication of two prime numbers gives the correct integer number), but finding the prime factors of a given product N is a hard computational problem. Under the assumption that existing computers cannot solve such mathematical tasks in a reasonable time, modern public-key cryptography techniques, such as the Rivest–Shamir–Adleman (RSA) scheme (Rivest et al., 1978), seem to be secure. However, this is an assumption and has not been proven. Moreover, quantum computing devices (Brassard et al., 1998; Ladd et al., 2010) are believed to be powerful in solving certain classically difficult tasks, including prime factorization, as proposed by Shor (1994). Therefore, the paradigm of information protection in the era of quantum computing ("post-quantum era") should be reconsidered as an adversary can potentially use quantum computing devices to attack cryptographic tools. This attack can be delayed in time but is still important for understanding the principles of information security in the post-quantum era.

The consequences of the appearance of a large-scale quantum computer that can attack, for instance, the RSA algorithm for realistic key sizes can be seen as a catastrophe [here I refer the reader to the paper entitled "The Day the Cryptography Dies" (Mulholland et al., 2017)]. Fortunately, not all tools are vulnerable to quantum cryptanalysis. One existing option to counter this potential threat is quantum key distribution (QKD) (Bennett and Brassard, 1984; Ekert, 1991; Gisin et al., 2002). The idea behind QKD protocols is to use quantum objects instead of physical couriers for cryptographic keys. The security proof of QKD (Gisin et al., 2002; Scarani et al., 2009; Walenta et al., 2014; Kiktenko et al., 2016; Portmann and Renner, 2022) is based on the laws of quantum physics, and, thus, it is guaranteed to be secure against any unforeseen technological developments, including, for example, even more powerful quantum computers. A class of attacks on QKD systems may be split between two major issues: the first is to prove that the protocol is secure and the second is to illuminate the technological drawbacks in implementing QKD devices. The second approach is to switch to post-quantum cryptography (Bernstein and Lange, 2017), which is based on cryptographic primitives that are believed to be secure even against attacks with quantum technologies. Mathematical tools for post-quantum cryptography include hash-based, lattice-based, code-based, and other approaches with advantages and disadvantages [reviewed by Bernstein and Lange (2017)]. Both QKD and post-quantum cryptography have prospects and limitations, which must be considered when deploying them.

In this context, I review recent progress in the deployment of the quantum-secured infrastructure based on quantum key distribution, post-quantum cryptography, and their combinations. I also indicate various directions in the further development of the full-stack quantum-secured infrastructure and argue that the hybrid approach, which combines quantum key distribution and post-quantum cryptography, can be beneficial for various applications. I specifically focus on distributed applications such as blockchains and distributed ledgers.

This perspective is organized as follows: Section 2 reviews quantum-secured cryptography tools, highlighting their advantages and limitations. Section 3 discusses hybrid approaches, in which quantum key distribution works jointly with post-quantum primitives. Section 4 concludes this article.

2 Quantum-secured cryptography

2.1 Quantum cryptoanalysis

New approaches for designing computational devices may lead to the need to modify assumptions regarding the security of certain cryptographic primitives. A celebrated example is Shor's algorithm (Shor, 1994; Shor, 1999) for solving prime factorization and discrete logarithm problems in polynomial time. Proof-of-concept experimental factoring of 15, 21, and 35 have been demonstrated on superconducting (Lucero et al., 2012), trapped ion (Monz et al., 2016), and photonic (Lanyon et al., 2007; Lu et al., 2007; Martín-López et al., 2012) quantum computers. Generally, a variant of Shor's algorithm by Beauregard (2003) requires $\mathcal{O}(n^3 \log n)$ operations under $2n + 3$ logical (ideal) qubits if $N = p \times q$ fits into n bits (Bernstein and Lange, 2017). Considering the need for quantum error correction, Shor's algorithm for practically relevant key sizes (for example, 2048 bit) would require 8 h using 20 million physical qubits (Gidney and Ekerå, 2021), which greatly exceeds the capabilities of today's quantum computing devices. Another recent proposal (Gouzien and Sangouard, 2021) demonstrated a way to factor 2048 RSA integers in 177 days with 13,436 physical qubits and a multimode memory. A forecast review (Sevilla and Riedel, 2020) estimated the likelihood for quantum devices capable of factoring RSA-2048 to exist before 2039 as less than 5%.

Quantum computing also affects symmetric cryptography, such as AES encryption. Grover's algorithm (Grover, 1996) enables quadratic speedup in brute force search, which means that the key length should be doubled to provide the same level of protection (Kim et al., 2018). The same scaling applies to cryptographic hash functions, for which the primary attack method is also brute-force search (Kim et al., 2018). In certain cases, this could be offset by increasing the length of the symmetric key.

Although the problem of breaking certain cryptographic tools may seem abstract and far from end users, several arguments exist to support this concern. The first argument is related to the so-called "store now—decrypt later" attack (Mulholland et al., 2017). The idea is that the adversary is harvesting information in the encrypted form, in the hope that new computational devices, for example, quantum computing, will help them to uncover valuable information in the future. That is why for some applications dealing with long-term sensitive information (such as medical records or genetic data), one should consider the priority replacement of cryptographic primitives. This fact is expressed in Mosca's theorem (Mulholland et al., 2017; Mosca, 2018): we should consider the impact of quantum computers when the amount of time that we wish our data to be secure for (X) added to the time it will take for our computer systems to transition from classical to secured against quantum attacks (Y) is greater than the time it will take for quantum computers to start breaking existing quantum-susceptible encryption protocols (Z).

The second argument indicates that the security problems impact not only encryption but also digital signatures, which are widely deployed across governmental services and business applications: the whole system of digital signatures must be replaced to use them in the quantum computing era. Therefore, each information system requires a transition plan and security recommendations for public-key infrastructures in the post-quantum era (see Yunakovsky et al. (2021) as an example for the case of recommendations for production environments).

Finally, it is extremely hard to predict the time of appearance of a large-scale quantum computing device as a hardware or algorithmic breakthrough in quantum computing may quickly change the situation and actualize this problem. No fundamental obstacles preventing the further scaling of quantum computers have yet been identified. However, there is an increasing interest in alternative schemes for solving the prime factorization problem using quantum tools, such as variational quantum factoring (Anschuetz et al., 2019; Karamlou et al., 2021). A very recent proposal demonstrated the possibility of accelerating factoring using quantum computers with sublinear scaling in the number of qubits (Yan et al., 2022) (however, this proposal is not yet fully verified). To summarize, we are in a race against time to deploy quantum-safe cryptographic tools, which are protected both from attacks with classical and quantum computers, before powerful enough quantum computing devices appear.

2.2 Quantum key distribution

The basic problem of symmetric cryptographic primitives is to ensure the proper organization of key distribution processes. As discussed previously, the cost of the key distribution process is extremely high, especially in the case of one-time pad encryption.

A beautiful idea is to replace vulnerable cryptographic primitives with one-time-pad encryption with QKD (Bennett and Brassard, 1984; Ekert, 1991), which is a technology that uses individual quantum objects to establish cryptographic keys. Historically, one of the first BB84 QKD protocols (Bennett and Brassard, 1984) developed the idea of conjugate coding (Wiesner, 1983) without using the feature of quantum entanglement, whereas the protocol proposed independently by Ekert (1991) uses so-called entangled quantum states. The information carriers in QKD systems are photons, as they are perfectly suited for this task in both classical and quantum domains (QKD can use fiber-based and free-space communication channels). The fundamental advantage of this approach is that QKD security relies not on any computational assumptions but rather on the laws of quantum physics (Shor and Preskill, 2000; Mayers, 2001; Gisin et al., 2002; Koashi, 2009; Scarani et al., 2009; Tomamichel et al., 2012; Portmann and Renner, 2022). I focus on the BB84 QKD protocol in the following paragraphs.

The concept of QKD is that two legitimate users (Alice and Bob) have a *pre-shared authentication key* (this aspect is discussed in the following paragraphs) and a communication channel. They use a certain protocol to prepare quantum states and encode information on the Alice side, and measure the states on the Bob side. Here and in following sections, I follow Trushechkin et al. (2021) in explaining the basics of QKD. Alice and Bob use four qubit states, which form two orthogonal bases $z = \{|0\rangle_z, |1\rangle_z\}$ and $x = \{|0\rangle_x, |1\rangle_x\}$ in the two-dimensional Hilbert space. The values 0 or 1 indicate which classic bit is encoded by the corresponding basis vector. The elements of the bases are expressed in terms of elements of another basis according to the relations

$$|0\rangle_x = \frac{|0\rangle_z + |1\rangle_z}{\sqrt{2}}, \qquad |1\rangle_x = \frac{|0\rangle_z - |1\rangle_z}{\sqrt{2}}. \tag{1}$$

If the information is encoded into photon polarization, then the vectors $|0\rangle_z$ and $|1\rangle_z$ can correspond, for example, to horizontal and vertical polarizations. In this case, $|0\rangle_x$ and $|1\rangle_x$ correspond to two diagonal polarizations that are rotated by 45° and 135° degrees, respectively, relative to the horizontal direction. The polarization coding is used to illustrate the idea but there is no restriction on the method of information encoding: Formally, $|0\rangle_z$, $|1\rangle_z$, $|0\rangle_x$, and $|1\rangle_x$ are vectors in the Hilbert space and one can use any encoding which fulfills relation given by Eq. 1. The equivalence of two popular ways of encoding—polarization and phase encodings—is explained in detail in Trushechkin et al. (2021).

Importantly, as seen from Eq. 1, when measuring a qubit in a basis different from the preparation basis, the result is a random value. In contrast, if the bases of preparation and measurement coincide, the result perfectly correlates with the prepared state of the qubit (in the absence of errors in the channel, measuring devices, and so on).

The BB84 protocol works as follows (Bennett and Brassard, 1984; Gisin et al., 2002; Trushechkin et al., 2021):

1. Alice randomly chooses a basis from the set $\{z, x\}$ and the value of the transmitted bit of information (1 or 0). Bits are selected with equal probabilities of 1/2.
2. Then, the photons prepared in the corresponding states are transmitted through the communication channel.
3. Bob randomly chooses a measurement basis, z or x, for each qubit and measures the state of the qubit in the selected basis. If the preparation and measurement bases coincide, the received bit value coincides (ideally) with the sent one. If the bases do not coincide, the bits of Alice and Bob do not correlate (that is, they may or may not coincide with equal probabilities) because the bases are mutually unbiased 1). Usually, the communication channel contains large losses; therefore, not all positions are registered by the receiver.
4. The aforementioned steps are repeated many times, i.e., many quantum states are transmitted. As a result, legitimate parties receive two sequences of bits k_A^{raw} and k_B^{raw} called *raw quantum-generated keys*.

Since a perfect copy of a quantum state cannot be created (Dieks, 1982; Wootters and Zurek, 1982) and the adversary does not know the basis in which the bit is encoded in a given position, the adversary must employ imperfect copying techniques that induce errors. So-called continuous-variables QKD protocols are also possible, which I do not cover in this paper (see Gyongyosi (2020); Pirandola et al. (2020)).

In the second stage, Alice and Bob use the classical post-processing of raw quantum-generated keys, k_A^{raw} and k_B^{raw}, with the use of communications over a public authenticated channel (Gisin et al., 2002; Fung et al., 2010; Walenta et al., 2014; Kiktenko et al., 2016):

2.2.1 Announcements

Bob announces the position numbers, in which the signal has been registered. Alice and Bob then discuss the bases used in all positions. When using the decoy-state method (see Section 2.2.2), Alice also announces the type of each pulse (signal or decoy) at this state. Alice and Bob can also announce bits in positions that do not participate in the formation of the secret key, in positions in which the parties used the x basis and in the decoy pulses.

2.2.2 Key sifting

Positions in which the decoy state intensity has been used, registration did not occur, or at least one of the legitimate parties used the x basis are sifted out. The resulting keys, k_A^{sift} and k_B^{sift}, are called *sifted keys*. Ideally, they should match, but because of natural noise in the channel or adversary actions, they do not match. Moreover, the adversary (Eve) may have partial information about them.

2.2.3 Error correction

One of the sifted keys (for example, belonging to Alice) is considered a reference. Differences between it and the sifted key of the other side are considered to be caused by errors. One can use error correction codes or interactive error correction procedures to correct errors. Low-density parity-check (LDPC) codes are commonly used for this purpose. Often, this procedure ends with *verification*: the identity of the sifted keys is checked using hash functions (see Fedorov et al. (2018a)). As a result of this stage, the legitimate parties receive identical *verified keys* $k_A^{\mathrm{ver}} = k_B^{\mathrm{ver}}$ with a high probability. An efficient method for error correction in the BB84 protocol error correction based on LDPC codes is described in Kiktenko et al. (2017); see also Sagingalieva and Kronberg, (2021) for progress in LDPC codes and Kiktenko et al., (2020) for polar codes.

2.2.4 Estimation of the level of eavesdropping

Estimation of the level of eavesdropping and deciding to create or renounce (aborting the protocol) a key are based on the observed data. QKD protocols are based on the fact that information encoded in non-orthogonal quantum states cannot be read by a third party (which does not know the basis in which the key bit in a given position was encoded) without "spoiling" these states. Therefore, any interception by Eve would lead to increased numbers of errors (i.e., mismatched positions in sifted keys) between legitimate parties. In this version of the protocol, where only the bits encoded in the z basis are involved in key formation, only the fraction of errors in the x basis is needed to assess the level of eavesdropping. If the error rate exceeds a certain critical threshold, the protocol is aborted with a warning message. Otherwise, the parties proceed to the last step. The basic idea behind the implementation of QKD protocols is to create conditions in which eavesdropping is impossible without being detected.

2.2.5 Privacy amplification

Alice randomly chooses a so-called hash function from a family of two-universal hash functions and sends it to Bob over a public channel. Then, they compute the hash value of their (identical) sifted keys. As a result, Alice and Bob obtain a common shorter key (*final key*) $k_A^{\mathrm{fin}} = k_B^{\mathrm{fin}}$, but the information of the adversary about which is now negligible. With an infinitely large length of the sifted key, it can be made arbitrarily small. The more information the adversary has about the sifted key (because of eavesdropping and as a result of disclosure by legitimate users of some of the information during error correction), the more the compression of the key in the privacy amplification procedure is required; i.e., the shorter the final key, the lower the key rate.

The final key is split into two parts: the first is used for authentication for the next QKD rounds [when this portion must be minimized, the problem of optimizing resources for QKD authentication appears, see Kiktenko et al. (2020)] and the rest can be used for external applications. The seminal BB84 protocol for QKD (Bennett and Brassard, 1984; Gisin et al., 2002; Trushechkin et al., 2021), which is typically accomplished using the decoy-state method (Trushechkin et al., 2021) [to avoid the photon-number splitting attack, which appears because Alice uses weak laser pulses instead of a true single photon source (Brassard et al., 2000)], is considered a candidate for the standard[2].

As a result of the QKD session, Alice and Bob have a key for external applications, such as one-time pad encryption or AES block ciphers, which are used to frequently refresh keys (Gisin et al., 2002). Such quantum-generated keys are information-theoretically secure against arbitrary attacks, including quantum attacks. Recent progress in the development and commercialization of QKD systems is a significant step toward improving information secrecy. However, several challenges hinder the wider adoption of QKD technology.

2.2.6 Practical aspects

The first aspect is the problem of QKD protocol security. Although it is largely accepted that the decoy-state BB84 protocol has verified security proofs (one of the latest developments here is related to the security of quantum key distribution with detection-efficiency mismatch in single-photon (Bochkov and Trushechkin, 2019) and multiphoton (Zhang et al., 2021; Trushechkin, 2022) cases), various alternatives to this protocol have been proposed (Pirandola et al., 2020). While these alternatives may seem interesting for achieving higher key generation rates or simpler practical implementation, their security proofs require further analysis to achieve a level at least as high as that for the decoy-state BB84 protocol (Pirandola et al., 2020; Trushechkin et al., 2021). That is why currently available QKD implementations are mostly based on the decoy-state BB84 protocol. Thus, alternative protocols should be investigated in detail before being used in industrial QKD systems.

The second question is related to the efficiency of the post-processing procedure. Remarkable progress has been made regarding all steps of the procedure in the last decade. However, there remains room for improvement. One specific direction is the optimization of post-processing with respect to the network topology. For example, Borisov et al. (2022) proposed a method for asymmetric error correction that could be used in practical QKD systems with limited computational resources on the sides. Also, new types of error correction codes, such as polar codes, can be considered (Kiktenko et al., 2020).

The third aspect is the distance issue. The efficient performance of QKD devices over long distances (≥500 km) remains a serious challenge due to optical losses over the entire communication distance (Muralidharan et al., 2016) [we note several remarkable experiments on long-distance QKD with the twin-field protocol (Wang et al., 2022)]. The range of commercial QKD systems is typically 100 km over optical fibers. Despite tremendous work on creating new protocols (Wang et al., 2022) and quantum repeaters (Muralidharan et al., 2016; Bhaskar et al., 2020), as well as the use of satellites for global-scale QKD (Dai et al., 2017) [for a review, see Bedington et al. (2017); Lu et al. (2022)], QKD technology still faces several challenges (Lo et al., 2014; Diamanti et al., 2016), which makes it best suitable for some domain-specific applications such as the protection of highly loaded communications links at a distance, which does not require the use of intermediate nodes. Long-range QKD without trusted nodes is not possible with current technology (Huttner et al., 2022). Therefore, an important challenge is optimizing the performance of large-scale backbone QKD networks. One approach is to use switch-based QKD backbone networks with trusted repeaters. Tayduganov et al. (2021) estimated that for a network link 670 km in length consisting of eight nodes, the switch-based architecture achieves significant resource savings of up to 28%, with only 8% reduction in throughput.

The fourth question relates to the practical security of QKD devices; i.e., a class of attacks that appear because real QKD devices do not exactly follow the underlying theoretical models (in particular, because of various engineering issues). I acknowledge intensive research on various practical imperfections in QKD systems [for example, see Gerhardt et al., (2011)]. This "quantum white-hat hacking" activity is important for the further development of QKD devices.

Finally, quantum-secured cryptographic primitives are required for various problems beyond the key distribution problem (Broadbent and Schaffner, 2016). For example, we need digital signatures, which in principle can be realized using QKD (Gottesman and Chuang, 2001; Arrazola et al., 2016; Kiktenko et al., 2022); however, deployment of the corresponding infrastructure is practically challenging.

2.3 Post-quantum cryptography

Fortunately, several tools can provide security even under the assumption that the eavesdropper has a large-scale quantum computer (Bernstein and Lange, 2017). One idea is to use another class of computational problems that are not vulnerable to attacks by quantum computers (see Table 1). As mentioned previously, quantum computing also affects symmetric cryptography since the quantum Grover's algorithm provides a quadratic speed-up in the brute force search. However, the quadratic speed-up may not be dramatic since doubling the key size helps to eliminate this effect. Moreover, if the key is distributed by utilizing non-quantum-secured tools, the system would not guarantee security in the post-quantum era. Finding ways to ensure quantum-secured key generation is crucial for various applications, in particular, transport layer security (TLS), which is the security protocol behind hypertext transfer protocol secure (HTTPS). Therefore, how to design quantum-secured for key distribution and digital signatures remains a question to be answered. Several cryptosystems for these purposes, which aim to

2 K. Chen, J. Ma, and H. Shi, Talk, ISO/IEC JTC1 SC27 WG3 SP Proposal, Security Requirements, Test and Evaluation Methods for the Decoy State BB84 Quantum Key Distribution (QKD), Berlin, Germany, 10/31/2017; ISO/IEC JTC 1/SC 27/WG 3 N 1537, 30th ISO/IEC JTC1/SC27 Working Group Meeting, H. Shi, J. Ma, and G. Pradel Wuhan, China, April 2018 30th Security Requirements, Test and Evaluation Methods for Quantum Key Distribution.

TABLE 1 Security of cryptographic algorithms in the post-quantum era (see Fedorov et al. (2022); Bernstein and Lange (2017)).

Cryptographic algorithm	Type	Purpose	Quantum security
AES	Symmetric	Encryption	Larger key sizes needed
SHA-2 and SHA-3	–	Hash functions	Larger output needed
RSA	Public key	Signature and key distribution	No longer secure
ECDSA and ECDH	Public key	Signature and key distribution	No longer secure
DSA	Public key	Signature and key distribution	No longer secure

remain secure under the assumption that the attacker has a large-scale quantum computer, have been proposed. Such an approach is known as *post-quantum cryptography*. Its main advantage is the ability to relatively cheaply and quickly switch to new post-quantum algorithms (Y is minimized in terms of Mosca's theorem).

Post-quantum protocols are based on different mathematical approaches, such as 1) the shortest vector problem in a lattice (Micciancio and Goldwasser, 2002; Hanrot et al., 2007; Regev, 2009), 2) learning with errors (Schnorr and Euchner, 1994; Regev, 2010; Arora et al., 2011; Chen et al., 2011; Albrecht et al., 2015; Kirchner et al., 2015), 3) solving systems of multivariate quadratic equations over finite fields (Patarin and Maurer, 1996; Faugère et al., 2003; Beullens et al., 2017), 4) finding isogenies between elliptic curves (Galbraith, 1999; Zhang and Wang, 2005; Tani et al., 2007; Jao et al., 2011; Costello et al., 2016; Delfs and Galbraith, 2016; Costello et al., 2017; Koziel et al., 2017), 5) decoding problems in an error-correcting code (Berlekamp et al., 1978; Alekhnovich, 2003; Bernstein and Sendrier, 2010; Becker et al., 2012; May et al., 2015), 6) security properties of cryptographic hash-functions (Buchmann et al., 2011; Hülsing et al., 2016; Bernstein and Hülsing, 2019), and other primitives (Bernstein and Lange, 2017) (see also the NIST website[3] for existing submissions and refs. (Bernstein and Lange, 2017; Yunakovsky et al., 2021)). The present work does not provide a detailed description of these primitives, which can be found in Bernstein and Lange (2017) and Yunakovsky et al., 2021).

2.3.1 Practical aspects

Developing reliable security analysis for post-quantum algorithms is challenging. Several post-quantum cryptographic systems based on post-quantum methods have been considered as candidates by the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization and by the European Telecommunications Standards Institute (ETSI). Standardization processes are crucial for reducing cryptographic risks. Known examples exist of finding possible classical attacks to a post-quantum algorithm even at the mature stage of the standardization procedure. New details in the security proofs also appear [for example, Hülsing et al. (2022) as a reply to Kudinov et al. (2021)]. Recently, an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman (SIDH) protocol has been proposed (Castryck and Decru, 2022). Moreover, one should keep in mind, again, that the assumptions about post-quantum algorithms can be reduced to statements based on computational assumptions. In a sense, the status of post-quantum cryptography is equivalent to the status of currently deployed public-key algorithms under the assumption of the absence of quantum computers.

An interesting aspect is that certain primitives, if used in specific protocols, may be able to detect their hacking, as has been shown in the case of hash-based digital signatures (Kiktenko et al., 2021). Kiktenko et al. (2021) demonstrated that with properly adjusted parameters, Lamport and Winternitz's one-time signature schemes could detect forgery property. This property is important in the framework of the crypto-agility paradigm since forgery detection warns that the cryptographic hash function is insecure and the corresponding scheme must be replaced.

We also note that the mitigation to post-quantum cryptography infrastructure for realistic cases requires a deep analysis of related aspects such as universal security requirements for the used software and SDKs, especially in terms of the update policy. Yunakovsky et al. (2021)providea detailed description of the security recommendations for public key infrastructures (PKIs), which are used as a part of security systems for protecting production environments. Finally, post-quantum algorithms can be more resource-demanding compared to existing tools. Time and memory consumption of post-quantum digital signature schemes is also discussed by Yunakovsky et al. (2021).

3 Inherently hybrid approach

A closer look at the QKD systems shows that such systems are inherently hybrid in the sense that quantum tools are essentially *combined* with classical cryptography (Kabanov et al., 2018). Quantumness plays an important role at the stage of solving the key distribution problem, but not typically at the level of data protection.

3.1 A peer-to-peer topology

3.1.1 Authentication

The initial state of realizing QKD protocols requires authentication between users (Gisin et al., 2002; Fung et al., 2010; Walenta et al., 2014; Kiktenko et al., 2016). Typically, the classical approach of pre-shared cryptographic keys jointly with the Wegman–Carter scheme (Wegman and Carter, 1981), which provides information-theoretic security. From this perspective,

3 https://csrc.nist.gov/pro jects/post-quantum-cryptography.

the QKD workflow appears to be *a key growing process* since the parties already require a short pair of pre-distributed keys before launching the first QKD round. For authentication in the second and subsequent rounds, the parts of quantum-generated secret keys from the previous round can be used (Kiktenko et al., 2020).

One possible approach to solve the authentication problem for large-scale QKD systems is to use post-quantum security. As noted by Stebila et al. (2010): "If authentication is unbroken during the first round of QKD, even if it is only computationally secure, then subsequent rounds of QKD will be information-theoretically secure" [for a review, see also Alléaume et al. (2014)]. Specifically, post-quantum digital signatures can be used for authentication in QKD devices (Wang et al., 2021; Yang et al., 2021). One needs to assume only the short-term security of post-quantum cryptography algorithms to achieve long-term security of the distributed keys, since in the next rounds, one can also use quantum-generated keys or their mixture for authentication purposes. This system is also of interest for QKD networks (see Section 3.1.2) since for a QKD network of n nodes in the case of using pre-sharing symmetric keys, $n(n-1)/2$ pairs of symmetric keys are required to realize pairwise interconnection.

3.1.2 Hybrid QKD protocols

An original version of the BB84 QKD protocol assumes the choice of bases $\{z, x\}$ with equal probabilities of 1/2. An improved variant of this protocol has been proposed, in which one of the bases (for example, the z basis) is chosen more frequently than the other (Lo et al., 2005) to reduce the number of basis mismatches and, therefore, the portion of sifted positions; i.e., it increases the quantum-generated key rate.

This idea can be extended to a QKD protocol, in which the bases are chosen pseudo-randomly using a pre-distributed random sequence (likely a portion of the authentication key). Such a modification of the BB84 protocol is considered in Trushechkin et al., (2018). For single-photon sources, this protocol gives better secret key rates than the BB84 and asymmetric BB84 protocols. However, the protocol requires single-photon sources.

3.1.3 Hybrid encryption

Quantum-generated keys are then used for encryption, which is again purely based on the principles of classical cryptography. The combination of QKD with one-time pad encryption enables an information-theoretic secure cryptographic scheme (Gisin et al., 2002).

However, most industrially-available encryptors use standardized symmetric protocols, such as AES, which is post-quantum under the assumption that the key was generated *via* a quantum-secured approach (Bonnetain et al., 2019). To maintain the security level in the era of quantum computing, doubling the key size is also necessary due to the quadratic speed-up in the brute-force search provided by Grover's algorithm. In this context, one of the scenarios related to the practical use of QKD in cryptographic infrastructures is to employ QKD as a key renewal technique for a symmetric cipher, such as AES, over a point-to-point link (Alléaume et al., 2014). Symmetric quantum-generated keys also can be efficiently combined with asymmetric post-quantum keys in various security models (for example, see Bogomolec et al. (2019) for a hybrid encryption scheme with session and public keys).

3.2 Network applications for multiple users

A natural application of QKD for multiple users is to consider a network containing many users, which offers an any-to-any key establishment service (Alléaume et al., 2014). Such a scheme is easy to realize for networks with all-to-all topology but is practically challenging. Long-range QKD without trusted nodes is not practically realizable with the current level of technology (Huttner et al., 2022). A hybrid quantum-secured infrastructure may use QKD to protect highly loaded communications links at a distance, which do not require the use of intermediate nodes, whereas end-users without direction connections can be protected by post-quantum cryptography. Other schemes with hybrid (QKD with post-quantum) security can be also considered.

3.2.1 Post-quantum protection of trusted nodes

One issue with implementing QKD protocols is the limitation related to the distance. As mentioned previously, long-range QKD without trusted nodes is not possible with current technology (Huttner et al., 2022). Thus, it seems to be reasonable to have additional post-quantum authentication of the trusted nodes. This can be especially important for QKD networks without fully connected topology.

3.2.2 Quantum-secured blockchains and blind computing

An area of particular concern in the context of quantum security is blockchains and cryptocurrencies (Aggarwal et al., 2018; Fedorov et al., 2018b; Kiktenko et al., 2018). Typical blockchain and cryptocurrency protocols use several cryptographic tools. First, blockchains use digital signatures to confirm the authorship of transactions. Second, hash functions are used to achieve a consensus (proof-of-work) between users in the absence of trust.

The digital signatures typically used in blockchains are based on primitives that are vulnerable to attacks by quantum computers. For example, Bitcoin uses the elliptic curve signature scheme. As predicted by Aggarwal et al. (2018), by the most optimistic estimates, such schemes could be completely broken by a quantum computer as early as 2027. One potential application of quantum computers on the bright side of cryptoanalysis is finding the lost private keys of legitimate users of cryptocurrencies. The quantum vulnerability of hash functions is similar to that of AES since the attack is based on brute-force search (Kim et al., 2018), which can be enhanced by the Grover algorithm in the quantum domain. Again, as discussed by Aggarwal et al. (2018), blockchains using proof-of-work consensus mechanisms, such as Bitcoin, are relatively resistant in the near term. However, various blockchain platforms, such as Ethereum, mitigate proof-of-stake consensus[4], which can make them more resistant to the aforementioned types of attacks.

Attacks by quantum computers have become the subject of many studies, which have proposed solutions for quantum-resistant blockchains (Fedorov et al., 2018b; Kiktenko et al., 2018), including

4 https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

blockchains that use quantum key distribution (Gisin et al., 2002) or post-quantum digital signatures and consensus schemes. A quantum-secured blockchain protocol was experimentally demonstrated in 2018 (Kiktenko et al., 2018). Several proposals have described the realization of quantum-secured blockchains using entangled states (Farouk et al., 2017; Krishnaswamy, 2020; Nimbe et al., 2022), which generally follow the initial idea of a quantum solution to the Byzantine agreement problem (Fitzi et al., 2001). Several options exist to combine QKD with post-quantum security in blockchain networks (Fedorov et al., 2018b). This is important since the primary requirement of the original quantum-secured blockchain protocol is an all-to-all connected QKD network to implement the broadcast protocol.

In addition to blockchains, another relevant application of both QKD and post-quantum cryptography is secure remote/blind computing, which is especially applicable in the quantum domain (Broadbent et al., 2009). The idea is to ensure that a remote user can delegate a computational problem with a desire to keep the computation perfectly secret from untrusted servers implementing quantum computation. Various cryptographic protocols for blind quantum computing have been proposed and tested (Aharonov et al., 2008; Dunjko et al., 2012; Morimae and Fujii, 2012; Barz et al., 2013; Mantri et al., 2013; Morimae and Fujii, 2013; Reichardt et al., 2013; Fisher et al., 2014; Morimae, 2014; Gheorghiu et al., 2015; Hayashi and Morimae, 2015; Greganti et al., 2016; Marshall et al., 2016; Fitzsimons and Kashefi, 2017; Gheorghiu et al., 2017; Ma et al., 2022) [reviewed by Fitzsimons, (2017)]. A proof-of-principle realization of blind quantum computing for completely classical clients was recently presented (Huang et al., 2017). Further developments in this domain are required since both classical communication channels and computational algorithms themselves should be protected considering the pending threat posed by quantum computers.

4 Discussion and outlook

The expected breakthrough in quantum computing, which poses a significant threat to the currently widely deployed techniques for encrypting and protecting data, will actualize the problem of protecting data. This is because most cryptographic tools, which are difficult or impossible to break using conventional computing, are easy to destroy using large-scale quantum computing devices.

The effect of quantum computing on information security can be mitigated by upgrading information security protocols with the use of QKD networks or post-quantum technologies. Thus, we are in a race against time to deploy quantum-safe cryptography that is protected both from attacks with classical and quantum computers, before powerful enough quantum computers arrive (Mulholland et al., 2017; Kiktenko et al., 2018; Wallden and Kashefi, 2019). For example, a present-day hacker might intercept and store encrypted messages with the hope of later decrypting them with a quantum computer. If the information is long-term sensitive (medical records, genetic data, strategic plans, etc.), this attack may result in damage. In this domain, we see various opportunities for combining QKD security with its physics-laws-based security level and post-quantum cryptography that can substantially enhance the security level of information exchange protocols. I would also like to note that at the current technology level, QKD cannot cover all the required cryptographic primitives (Broadbent and Schaffner, 2016); thus, many opportunities exist in which quantum and post-quantum approaches can efficiently work together.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

The author confirms being the sole contributor to this work and has approved its publication.

Funding

The analysis of quantum information processing aspects was supported by the Russian Science Foundation (Grant No. 19-71-10091). This work was supported by the Priority 2030 program at the National University of Science and Technology “MISIS” (project K1-2022-027 (analysis of quantum networks)).

Acknowledgments

The author thanks E. Kiktenko for the useful comments and A. Mastiukova for inspiring discussions as well as helping to prepare the manuscript. The author also thanks the reviewers for useful comments, especially for pointing out secure remote computing as a potential application for quantum-secured tools.

Conflict of interest

The author is a shareholder of QRate, a company working in the field of quantum communications. Owing to the employment and consulting activities, the author has financial interests in the commercial applications of quantum computing and quantum cryptography.

Publisher’s note

References

Aggarwal, D., Brennen, G., Lee, T., Santha, M., and Tomamichel, M. (2018). Quantum attacks on Bitcoin, and how to protect against them. *Ledger* 3. doi:10.5195/ledger.2018.127

Aharonov, D., Ben-Or, M., and Eban, E. (2008). *Interactive proofs for quantum computations*. Ithaca, NY: Cornell University. arXiv:0810.5375 [quant-ph].

Albrecht, M. R., Player, R., and Scott, S. (2015). *J. Math. Cryptol.* 9, 169.

Alekhnovich, M. (2003). "More on average case vs approximation complexity," in 44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings, Cambridge, MA, USA, 11-14 October 2003, 298.

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., et al. (2014). Using quantum key distribution for cryptographic purposes: A survey. *Theor. Comput. Sci.* 560, 62–81. doi:10.1016/j.tcs.2014.09.018

Anant, V., Donchak, L., Kaplan, J., and Soller, H. (2020). *The consumer-data opportunity and the privacy imperative*. New York, United States: McKinsey and Company.

Anschuetz, E., Olson, J., Aspuru-Guzik, A., and Cao, Y. (2019). in *Quantum technology and optimization problems*. Editors S. Feld and C. Linnhoff-Popien (Cham: Springer International Publishing), 74–85.

Arora, S., and Ge, R. (2011). in *Automata, languages and programming*. Editors L. Aceto, M. Henzinger, and J. Sgall (Berlin, Heidelberg: Springer Berlin Heidelberg), 403–415.

Arrazola, J. M., Wallden, P., and Andersson, E. (2016). Multiparty quantum signature schemes. *Comput.* 16, 435–464. doi:10.26421/qic16.5-6-3

Barz, S., Fitzsimons, J. F., Kashefi, E., and Walther, P. (2013). Experimental verification of quantum computation. *Nat. Phys.* 9, 727–731. doi:10.1038/nphys2763

Beauregard, S. (2003). Circuit for Shor's algorithm using 2n+3 qubits. *Comput.* 3, 175–185. doi:10.26421/qic3.2-8

Becker, A., Joux, A., May, A., and Meurer, A. (2012). in *Advances in cryptology – eurocrypt 2012*. Editors D. Pointcheval and T. Johansson (Berlin, Heidelberg: Springer Berlin Heidelberg), 520–536.

Bedington, R., Arrazola, J. M., and Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Inf.* 3, 30. doi:10.1038/s41534-017-0031-5

Bennett, C. H., and Brassard, G. (1984). "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 December 1984, 175–179.

Berlekamp, E., McEliece, R., and van Tilborg, H. (1978). On the inherent intractability of certain coding problems (Corresp.) *IEEE Trans. Inf. Theory* 24, 384–386. doi:10.1109/tit.1978.1055873

Bernstein, D. J. (2010). in *Post-quantum cryptography*. Editor N. Sendrier (Berlin, Heidelberg: Springer Berlin Heidelberg), 73–80.

Bernstein, D. J., and Hülsing, A. (2019). "Advances in cryptology–ASIACRYPT 2019," *Proceedings, Part III 25* in 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, 33–62.

Bernstein, D. J., and Lange, T. (2017). Post-quantum cryptography. *Nature* 549, 188–194. doi:10.1038/nature23461

Beullens, W., and Preneel, B. (2017). in *Progress in cryptology – indocrypt 2017*. Editors A. Patra and N. P. Smart (Cham: Springer International Publishing), 227–246.

Bhaskar, M. K., Riedinger, R., Machielse, B., Levonian, D. S., Nguyen, C. T., Knall, E. N., et al. (2020). Experimental demonstration of memory-enhanced quantum communication. *Nature* 580, 60–64. doi:10.1038/s41586-020-2103-5

Bochkov, M. K., and Trushechkin, A. S. (2019). Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds. *Phys. Rev. A* 99, 032308. doi:10.1103/physreva.99.032308

Bogomolec, X., Underhill, J. G., and Kovac, S. A. (2019). *Towards post-quantum secure symmetric cryptography: A mathematical perspective*. Cryptology ePrint Archive. Paper 2019/1208.

Bonnetain, X., Naya-Plasencia, M., and Schrottenloher, A. (2019). Quantum security analysis of AES. *IACR Trans. Symmetric Cryptol.* 2019 (2), 55–93. doi:10.13154/tosc.v2019.i2.55-93

Borisov, N., Petrov, I., and Tayduganov, A. (2022). Asymmetric adaptive LDPC-based information reconciliation for industrial quantum key distribution. *Entropy* 25, 31. doi:10.3390/e25010031

Brassard, G., Chuang, I., Lloyd, S., and Monroe, C. (1998). Quantum computing. *Proc. Natl. Acad. Sci.* 95, 11032–11033. doi:10.1073/pnas.95.19.11032

Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Phys. Rev. Lett.* 85, 1330–1333. doi:10.1103/physrevlett.85.1330

Broadbent, A., Fitzsimons, J., and Kashefi, E. (2009). "Annual IEEE symposium on foundations of computer science," in 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Atlanta, GA, USA, 25-27 Oct. 2009, 517–526.

Broadbent, A., and Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* 78, 351–382. doi:10.1007/s10623-015-0157-4

Buchmann, J., Dahmen, E., and Hülsing, A. (2011). in *Post-quantum cryptography*. Editor B.-Y. Yang (Berlin, Heidelberg: Springer Berlin Heidelberg), 117–129.

Castryck, W., and Decru, T. (2022). *An efficient key recovery attack on sidh*. Cryptology ePrint Archive. Paper 2022/975.

Chen, Y., and Nguyen, P. Q. (2011). in *Advances in cryptology – asiacrypt 2011*. Editors D. H. Lee and X. Wang (Berlin, Heidelberg: Springer Berlin Heidelberg), 1–20.

Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., and Urbanik, D. (2017). in *Advances in cryptology – eurocrypt 2017*. Editors J.-S. Coron and J. B. Nielsen (Cham: Springer International Publishing), 679–706.

Costello, C., Longa, P., and Naehrig, M. (2016). in *Advances in cryptology – crypto 2016*. Editors M. Robshaw and J. Katz (Berlin, Heidelberg: Springer Berlin Heidelberg), 572–601.

Dai, H.-N., Yang, B., Reingruber, A., Sun, H., Xu, X.-F., Chen, Y.-A., et al. (2017). Four-body ring-exchange interactions and anyonic statistics within a minimal toric-code Hamiltonian. *Nat. Phys.* 13, 1195–1200. doi:10.1038/nphys4243

Delfs, C., and Galbraith, S. D. (2016). Computing isogenies between supersingular elliptic curves over $${\mathbb {F}}_p$$ F p. *Des. Codes Cryptogr.* 78, 425–440. doi:10.1007/s10623-014-0010-1

Diamanti, E., Lo, H.-K., Qi, B., and Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Inf.* 2, 16025. doi:10.1038/npjqi.2016.25

Dieks, D. (1982). Communication by EPR devices. *Phys. Lett. A* 92, 271–272. doi:10.1016/0375-9601(82)90084-6

Diffie, W., and Hellman, M. E. (1976). New directions in cryptography. *IEEE Trans. Inf. Theory* 22, 644–654. doi:10.1109/tit.1976.1055638

Dunjko, V., Kashefi, E., and Leverrier, A. (2012). Blind quantum computing with weak coherent pulses. *Phys. Rev. Lett.* 108, 200502. doi:10.1103/physrevlett.108.200502

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* 67, 661–663. doi:10.1103/physrevlett.67.661

Farouk, A., Batle, J., Elhoseny, M., Naseri, M., Lone, M., Fedorov, A., et al. (2017). Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states. *Front. Phys.* 13, 130306. doi:10.1007/s11467-017-0717-3

Faugère, J.-C., and Joux, A. (2003). in *Advances in cryptology - crypto 2003*. Editor D. Boneh (Berlin, Heidelberg: Springer Berlin Heidelberg), 44–60.

Fedorov, A. K., Gisin, N., Beloussov, S. M., and Lvovsky, A. I. (2022). *Quantum computing at the quantum advantage threshold: A down-to-business review*. Ithaca, NY: Cornell University.

Fedorov, A. K., Kiktenko, E. O., and Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. *Nature* 563, 465–467. doi:10.1038/d41586-018-07449-z

Fedorov, A. K., Kiktenko, E. O., and Trushechkin, A. S. (2018). Symmetric blind information reconciliation and hash-function-based verification for quantum key distribution. *Lobachevskii J. Math.* 39, 992–996. doi:10.1134/s1995080218070107

Fisher, K. A. G., Broadbent, A., Shalm, L. K., Yan, Z., Lavoie, J., Prevedel, R., et al. (2014). Quantum computing on encrypted data. *Nat. Commun.* 5, 3074. doi:10.1038/ncomms4074

Fitzi, M., Gisin, N., and Maurer, U. (2001). Quantum solution to the byzantine agreement problem. *Phys. Rev. Lett.* 87, 217901. doi:10.1103/physrevlett.87.217901

Fitzsimons, J. F., and Kashefi, E. (2017). Unconditionally verifiable blind quantum computation. *Phys. Rev. A* 96, 012303. doi:10.1103/physreva.96.012303

Fitzsimons, J. F. (2017). Private quantum computation: An introduction to blind quantum computing and related protocols. *npj Quantum Inf.* 3, 23. doi:10.1038/s41534-017-0025-3

Fung, C.-H. F., Ma, X., and Chau, H. F. (2010). Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* 81, 012318. doi:10.1103/physreva.81.012318

Galbraith, S. D. (1999). Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math.* 2, 118–138. doi:10.1112/s1461157000000097

Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., and Makarov, V. (2011). Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* 2, 349. doi:10.1038/ncomms1348

Gheorghiu, A., Kashefi, E., and Wallden, P. (2015). Robustness and device independence of verifiable blind quantum computing. *New J. Phys.* 17, 083040. doi:10.1088/1367-2630/17/8/083040

Gheorghiu, A., Wallden, P., and Kashefi, E. (2017). Rigidity of quantum steering and one-sided device-independent verifiable quantum computation. *New J. Phys.* 19, 023043. doi:10.1088/1367-2630/aa5cff

Gidney, C., and Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* 5, 433. doi:10.22331/q-2021-04-15-433

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys.* 74, 145–195. doi:10.1103/revmodphys.74.145

Gottesman, D., and Chuang, I. (2001). *Quantum digital signatures*. Ithaca, NY: Cornell University.

Gouzien, E., and Sangouard, N. (2021). Factoring 2048-bit RSA integers in 177 Days with 13 436 qubits and a multimode memory. *Phys. Rev. Lett.* 127, 140503. doi:10.1103/physrevlett.127.140503

Greganti, C., Roehsner, M.-C., Barz, S., Morimae, T., and Walther, P. (2016). Demonstration of measurement-only blind quantum computing. *New J. Phys.* 18, 013020. doi:10.1088/1367-2630/18/1/013020

Grover, L. K. (1996). "Stoc 96," in *Proceedings of the twenty-eighth annual ACM symposium on theory of computing* (New York, NY, USA: Association for Computing Machinery), 212–219.

Gyongyosi, L. (2020). Multicarrier continuous-variable quantum key distribution. *Theor. Comput. Sci.* 816, 67–95. doi:10.1016/j.tcs.2019.11.026

Hanrot, G., and Stehlé, D. (2007). in *Advances in cryptology - crypto 2007*. Editor A. Menezes (Berlin, Heidelberg: Springer Berlin Heidelberg), 170–186.

Hayashi, M., and Morimae, T. (2015). Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett.* 115, 220502. doi:10.1103/physrevlett.115.220502

Huang, H.-L., Zhao, Q., Ma, X., Liu, C., Su, Z.-E., Wang, X.-L., et al. (2017). Experimental blind quantum computing for a classical client. *Phys. Rev. Lett.* 119, 050503. doi:10.1103/physrevlett.119.050503

Hülsing, A., and Kudinov, M. (2022). in *Advances in cryptology – asiacrypt 2022*. Editors S. Agrawal and D. Lin (Cham: Springer Nature Switzerland), 3–33.

Hülsing, A., Rijneveld, J., and Song, F. (2016). in *Public-key cryptography – PKC 2016*. Editors C.-M. Cheng, K.-M. Chung, G. Persiano, and B.-Y. Yang (Berlin, Heidelberg: Springer Berlin Heidelberg), 387–416.

Huttner, B., Alléaume, R., Diamanti, E., Fröwis, F., Grangier, P., Hübel, H., et al. (2022). Long-range QKD without trusted nodes is not possible with current technology. *npj Quantum Inf.* 8, 108. doi:10.1038/s41534-022-00613-4

Jao, D., and De Feo, L. (2011). in *Post-quantum cryptography*. Editor B.-Y. Yang (Berlin, Heidelberg: Springer Berlin Heidelberg), 19–34.

Kabanov, I. S., Yunusov, R. R., Kurochkin, Y. V., and Fedorov, A. K. (2018). Practical cryptographic strategies in the post-quantum era. *AIP Conf. Proc.* 1936, 020021. doi:10.1063/1.5025459

Karamlou, A. H., Simon, W. A., Katabarwa, A., Scholten, T. L., Peropadre, B., and Cao, Y. (2021). Analyzing the performance of variational quantum factoring on a superconducting quantum processor. *Npj Quantum Inf.* 7, 156. doi:10.1038/s41534-021-00478-z

Kiktenko, E., Kudinov, M., Bulychev, A., and Fedorov, A. (2021). *Proceedings of the 18th international conference on security and cryptography-SECRYPT*. Setúbal, Portugal: SciTePress, 333–342.

Kiktenko, E. O., Malyshev, A. O., Gavreev, M. A., Bozhedarov, A. A., Pozhar, N. O., Anufriev, M. N., et al. (2020). Lightweight authentication for quantum key distribution. *IEEE Trans. Inf. Theory* 66, 6354–6368. doi:10.1109/tit.2020.2989459

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., et al. (2018). Quantum-secured blockchain. *Quantum Sci. Technol.* 3, 035004. doi:10.1088/2058-9565/aabc6b

Kiktenko, E. O., Trushechkin, A. S., Lim, C. C. W., Kurochkin, Y. V., and Fedorov, A. K. (2017). Symmetric blind information reconciliation for quantum key distribution. *Phys. Rev. Appl.* 8, 044017. doi:10.1103/physrevapplied.8.044017

Kiktenko, E. O., Zelenetsky, A. S., and Fedorov, A. K. (2022). Practical quantum multiparty signatures using quantum-key-distribution networks. *Phys. Rev. A* 105, 012408. doi:10.1103/physreva.105.012408

Kiktenko, E., Trushechkin, A., Kurochkin, Y., and Fedorov, A. (2016). Post-processing procedure for industrial quantum key distribution systems. *J. Phys. Conf. Ser.* 741, 012081. doi:10.1088/1742-6596/741/1/012081

Kim, P., Han, D., and Jeong, K. C. (2018). Time–space complexity of quantum search algorithms in symmetric cryptanalysis: Applying to AES and SHA-2. *Quantum Inf. Process.* 17, 339. doi:10.1007/s11128-018-2107-3

Kirchner, P., and Fouque, P.-A. (2015). in *Advances in cryptology – crypto 2015*. Editors R. Gennaro and M. Robshaw (Berlin, Heidelberg: Springer Berlin Heidelberg), 43–62.

Koashi, M. (2009). Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* 11, 045018. doi:10.1088/1367-2630/11/4/045018

Koziel, B., Azarderakhsh, R., Mozaffari Kermani, M., and Jao, D. (2017). Post-quantum cryptography on FPGA based on isogenies on elliptic curves. *IEEE Trans. Circuits Syst. I Regul. Pap.* 64, 86–99. doi:10.1109/tcsi.2016.2611561

Krishnaswamy, D. (2020). *Proceedings of the twenty-first international symposium on theory, algorithmic foundations, and protocol design for mobile networks and mobile computing, mobihoc '20*. New York, NY, USA: Association for Computing Machinery, 327–332.

Kudinov, M. A., Kiktenko, E. O., and Fedorov, A. K. (2021). *Matematicheskie Voprosy Kriptografii Math. Aspects Cryptogr.* 12, 129–145. doi:10.4213/mvk362

Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., and O'Brien, J. L. (2010). Quantum computers. *Nature* 464, 45–53. doi:10.1038/nature08812

Lanyon, B. P., Weinhold, T. J., Langford, N. K., Barbieri, M., James, D. F. V., Gilchrist, A., et al. (2007). Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Phys. Rev. Lett.* 99, 250505. doi:10.1103/physrevlett.99.250505

Lo, H.-K., Chau, H. F., and Ardehali, M. (2005). Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* 18, 133–165. doi:10.1007/s00145-004-0142-y

Lo, H.-K., Curty, M., and Tamaki, K. (2014). Secure quantum key distribution. *Nat. Photonics* 8, 595–604. doi:10.1038/nphoton.2014.149

Lu, C.-Y., Browne, D. E., Yang, T., and Pan, J.-W. (2007). Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.* 99, 250504. doi:10.1103/physrevlett.99.250504

Lu, C.-Y., Cao, Y., Peng, C.-Z., and Pan, J.-W. (2022). Micius quantum experiments in space. *Rev. Mod. Phys.* 94, 035001. doi:10.1103/revmodphys.94.035001

Lucero, E., Barends, R., Chen, Y., Kelly, J., Mariantoni, M., Megrant, A., et al. (2012). Computing prime factors with a Josephson phase qubit quantum processor. *Nat. Phys.* 8, 719–723. doi:10.1038/nphys2385

Ma, Y., Kashefi, E., Arapinis, M., Chakraborty, K., and Kaplan, M. (2022). QEnclave - a practical solution for secure quantum cloud computing. *npj Quantum Inf.* 8, 128. doi:10.1038/s41534-022-00612-5

Mantri, A., Pérez-Delgado, C. A., and Fitzsimons, J. F. (2013). Optimal blind quantum computation. *Phys. Rev. Lett.* 111, 230502. doi:10.1103/physrevlett.111.230502

Marshall, K., Jacobsen, C. S., Schäfermeier, C., Gehring, T., Weedbrook, C., and Andersen, U. L. (2016). Continuous-variable quantum computing on encrypted data. *Nat. Commun.* 7, 13795. doi:10.1038/ncomms13795

Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., and O'Brien, J. L. (2012). Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics* 6, 773–776. doi:10.1038/nphoton.2012.259

May, A., and Ozerov, I. (2015). in *Advances in cryptology – eurocrypt 2015*. Editors E. Oswald and M. Fischlin (Berlin, Heidelberg: Springer Berlin Heidelberg), 203–228.

Mayers, D. (2001). Unconditional security in quantum cryptography. *J. ACM* 48, 351–406. doi:10.1145/382780.382781

Micciancio, D., and Goldwasser, S. (2002). "Complexity of lattice problems: A cryptographic perspective," in *The kluwer international series in engineering and computer science* (Boston, Massachusetts: Kluwer Academic Publishers). Vol. 671.

Monz, T., Nigg, D., Martinez, E. A., Brandl, M. F., Schindler, P., Rines, R., et al. (2016). Realization of a scalable Shor algorithm. *Science* 351, 1068–1070. doi:10.1126/science.aad9480

Morimae, T., and Fujii, K. (2013). Blind quantum computation protocol in which Alice only makes measurements. *Phys. Rev. A* 87, 050301. doi:10.1103/physreva.87.050301

Morimae, T., and Fujii, K. (2012). Blind topological measurement-based quantum computation. *Nat. Commun.* 3, 1036. doi:10.1038/ncomms2043

Morimae, T. (2014). Verification for measurement-only blind quantum computing. *Phys. Rev. A* 89, 060302. doi:10.1103/physreva.89.060302

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we Be ready? *IEEE Secur. Priv.* 16, 38–41. doi:10.1109/msp.2018.3761723

Mulholland, J., Mosca, M., and Braun, J. (2017). The day the cryptography Dies. *IEEE Secur. Priv.* 15, 14–21. doi:10.1109/msp.2017.3151325

Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M. D., and Jiang, L. (2016). Optimal architectures for long distance quantum communication. *Sci. Rep.* 6, 20463. doi:10.1038/srep20463

Nimbe, P., Weyori, B., Mensah, J., Amponsah, A., Adekoya, A., and Adjei Domfeh, E. (2022). *Quantum blockchain: A systematic review*. Pennsylvania, United States: IGI Global.

Patarin, J. (1996). in *Advances in cryptology — eurocrypt '96*. Editor U. Maurer (Berlin, Heidelberg: Springer Berlin Heidelberg), 33–48.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., et al. (2020). Advances in quantum cryptography. *Adv. Opt. Phot.* 12, 1012. doi:10.1364/aop.361502

Portmann, C., and Renner, R. (2022). Security in quantum cryptography. *Rev. Mod. Phys.* 94, 025008. doi:10.1103/revmodphys.94.025008

Regev, O. (2010). "No strong parallel repetition with entangled and non-signaling provers," in 2010 IEEE 25th Annual Conference on Computational Complexity, Cambridge, MA, USA, 09-12 June 2010, 191–204.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* 56, 1–40. doi:10.1145/1568318.1568324

Reichardt, B. W., Unger, F., and Vazirani, U. (2013). Classical command of quantum systems. *Nature* 496, 456–460. doi:10.1038/nature12035

Rivest, R. L., Shamir, A., and Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 120–126. doi:10.1145/359340.359342

Sagingalieva, A. B., and Kronberg, D. A. (2021). Adaptive algorithms of error correction and error estimation in quantum cryptography. *AIP Conf. Proc.* 2362, 050002. doi:10.1063/5.0055360

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Rev. Mod. Phys.* 81, 1301–1350. doi:10.1103/revmodphys.81.1301

Schneier, B. (1996). *Applied cryptography*. 2nd ed. New York, United States: Wiley.

Schnorr, C. P., and Euchner, M. (1994). Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.* 66, 181–199. doi:10.1007/bf01581144

Sevilla, J., and Riedel, C. J. (2020). *Forecasting timelines of quantum computing*. Ithaca, NY: Cornell University. arXiv:2009.05045 [quant-ph].

Shannon, C. E. (1948). A mathematical theory of communication. *Bell Syst. Tech. J.* 27, 379–423. doi:10.1002/j.1538-7305.1948.tb01338.x

Shor, P. (1994). "SFCS '94," in Proceedings 35th Annual Symposium on Foundations of Computer Science, Washington, DC, November 20 - 22, 1994, 124–134.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* 41, 303–332. doi:10.1137/s0036144598347011

Shor, P. W., and Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* 85, 441–444. doi:10.1103/physrevlett.85.441

STATISTA (2020). *The total amount of data created, captured, copied, and consumed globally is forecast to increase rapidly, reaching 64.2 zettabytes*. Hamburg: STATISTA.

Stebila, D., Mosca, M., and Lütkenhaus, N. (2010). in *Quantum communication and quantum networking*. Editors A. Sergienko, S. Pascazio, and P. Villoresi (Berlin, Heidelberg: Springer Berlin Heidelberg), 283–296.

Tani, S. (2007). in *Mathematical foundations of computer science*. Editors L. Kučera and A. Kučera (Berlin, Heidelberg: Springer Berlin Heidelberg), 536–547.

Tayduganov, A., Rodimin, V., Kiktenko, E. O., Kurochkin, V., Krivoshein, E., Khanenkov, S., et al. (2021). Optimizing the deployment of quantum key distribution switch-based networks. *Opt. Express* 29, 24884. doi:10.1364/oe.427804

Tomamichel, M., Lim, C. C. W., Gisin, N., and Renner, R. (2012). Tight finite-key analysis for quantum cryptography. *Nat. Commun.* 3, 634. doi:10.1038/ncomms1631

Trushechkin, A. (2022). Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case. *Quantum* 6, 771. doi:10.22331/q-2022-07-22-771

Trushechkin, A. S., Kiktenko, E. O., Kronberg, D. A., and Fedorov, A. K. (2021). Security of the decoy state method for quantum key distribution. *Physics-Uspekhi* 64, 88–102. doi:10.3367/ufne.2020.11.038882

Trushechkin, A. S., Tregubov, P. A., Kiktenko, E. O., Kurochkin, Y. V., and Fedorov, A. K. (2018). Quantum-key-distribution protocol with pseudorandom bases. *Phys. Rev. A* 97, 012311. doi:10.1103/physreva.97.012311

Vernam, G. S. (1926). Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *J. AIEE* 45, 109–115. doi:10.1109/jaiee.1926.6534724

Walenta, N., Burg, A., Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O., et al. (2014). A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.* 16, 013047. doi:10.1088/1367-2630/16/1/013047

Wallden, P., and Kashefi, E. (2019). Cyber security in the quantum era. *Commun. ACM* 62, 120. doi:10.1145/3241037

Wang, L.-J., Zhang, K.-Y., Wang, J.-Y., Cheng, J., Yang, Y.-H., Tang, S.-B., et al. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. *npj Quantum Inf.* 7, 67. doi:10.1038/s41534-021-00400-7

Wang, S., Yin, Z.-Q., He, D.-Y., Chen, W., Wang, R.-Q., Ye, P., et al. (2022). Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* 16, 154–161. doi:10.1038/s41566-021-00928-2

Wegman, M. N., and Carter, J. (1981). New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* 22, 265–279. doi:10.1016/0022-0000(81)90033-7

Wiesner, S. (1983). Conjugate coding. *SIGACT News* 15, 78–88. doi:10.1145/1008908.1008920

Wootters, W. K., and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature* 299, 802–803. doi:10.1038/299802a0

Yan, B., Tan, Z., Wei, S., Jiang, H., Wang, W., Wang, H., et al. (2022). *Factoring integers with sublinear resources on a superconducting quantum processor*. Ithaca, NY: Cornell University.

Yang, Y.-H., Li, P.-Y., Ma, S.-Z., Qian, X.-C., Zhang, K.-Y., Wang, L.-J., et al. (2021). All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Opt. Express* 29, 25859. doi:10.1364/oe.432944

Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., et al. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technol.* 8, 14. doi:10.1140/epjqt/s40507-021-00104-z

Zhang, S. (2005). in *Computing and combinatorics*. Editor L. Wang (Berlin, Heidelberg: Springer Berlin Heidelberg), 430–439.

Zhang, Y., Coles, P. J., Winick, A., Lin, J., and Lütkenhaus, N. (2021). Security proof of practical quantum key distribution with detection-efficiency mismatch. *Phys. Rev. Res.* 3, 013076. doi:10.1103/physrevresearch.3.013076