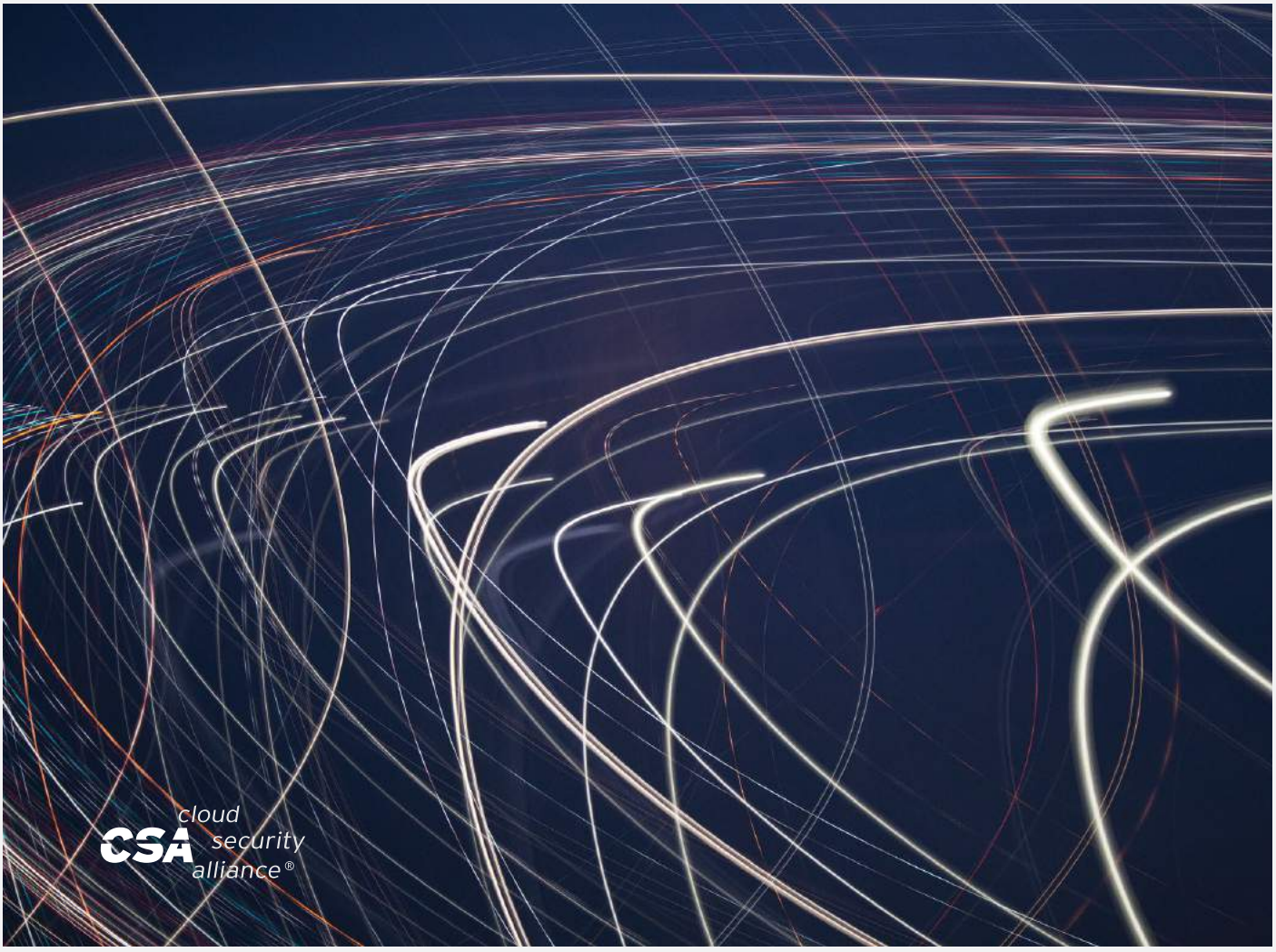
Applied Quantum-Safe Security

Quantum-Resistant Algorithms and Quantum Key Distribution



The permanent and official location for *Cloud Security Alliance Quantum-Safe Security Working group* is **https://cloudsecurityalliance.org/group/quantum-safe-security/**.

Acknowledgements

Cloud Security Alliance

Frank Guanco
Ryan Bergsma
Victor Chin
Stephen Lumpe

Quantum-Safe Security Working Group

Bruno Huttner, Co-Chair
Jane Melia, Co-Chair
Ludovic Perret
Lee Wilson

Special Thanks

Sauvik Bhattacharya
Tom Brennan
Roberta Faux
Dan Hiestand
Jens Jensen
Xu Lei
Xinhua Ling
Larry Ramos
Rino Sanchez
The members of the Quantum-Safe Security Working Group

1. Introduction: the Quantum-Safe Security Working group

The Quantum-Safe Security Working Group (QSS-WG) is an industry forum, organized by the Cloud Security Alliance. Its goal is to promote the understanding and implementation of *quantum-safe security*[1]: digital and physical data security that is enhanced by protection against attacks by a *quantum computer*, to which modern security cryptosystems are vulnerable.

The QSS-WG is a unique forum that brings together communities with different approaches to the common goal of quantum-safe security, a union that enables real, meaningful dialogue. It is comprised of participating members, or followers, from various parts of the security industry. The most active members come from commercial organizations and academic institutions that are developing *quantum-resistant algorithmic* solutions, as well as individuals working on physics-based, *quantum technology*-reliant alternatives.

The aim of this white paper is to provide individuals in the security industry and related fields with applicable knowledge regarding the quantum computer and its influence on cyber security. Cloud Security Alliance hopes this information will help these interested parties find the most suitable solutions for their specific issues and challenges as we all prepare for the quantum era.

[1] The terms in italics are defined in the Glossary of Terms in Section 11.

2. The need for quantum-safe security

Over the last year or so, the perceived threat of the *quantum computer* to modern cryptographic standards in widespread use has increased dramatically. Government security agencies, such as the United States Government National Security Agency (NSA) and the Communications-Electronics Security Group (CESG), a group within the UK Government Communications Headquarters (GCHQ), have called for a move to *quantum-safe* cryptographic schemes. Standardization bodies such as the European Telecommunications Standards Institute (ETSI), the U.S. National Institute for Standards and Technology (NIST), and the International Organization for Standardization (ISO), have started investigating the need for new, global standards [CJLMPPS16]. These entities have arrived at the same conclusion and the consensus is clear: the cryptographic foundation that underlies today's cybersecurity solutions needs to be retooled sooner rather than later, and the transition to *quantum-safe* security must begin now.

Although the arrival date for a practical quantum computer is still in debate, experts believe we will see a quantum computer capable of breaking current public key cryptosystems within five to 15 years. This may seem to allow for considerable preparation time, but two factors shorten the perceived runway.

- First, the transition to quantum-safe security means significantly changing our security ecosystems, which cannot be done overnight. The consensus is that five to 10 years may be required to adapt those systems to use new security algorithms and protocols.
- Second, most encrypted data has a long lifetime, often requiring secrecy ranging from a few years to a decade or longer. With current progress in data storage technology, a nearly unlimited amount of data in motion can be intercepted now and stored for future decryption. This is commonly known as the 'download now, decrypt later' or 'harvesting' type of attack. As expressed in the ETSI white paper, **Quantum Safe Cryptography and Security**, [CCDDFGZ15] "Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure." A quantum computer will—in principle—be able to decrypt all the confidential information which was previously encrypted using unsafe methods. Therefore, to prevent disruption in the confidentiality of our cybersecurity systems, the time for action is now. Finding new solutions that protect against quantum attacks should be a hot topic for everyone in the cybersecurity industry.

3. An exercise in risk management

Security is not an absolute. There is no universal solution which would provide perfect security against all possible threats. Providing security is always an exercise that aims to assure a certain level of protection—at a given cost—and for an appropriate duration. However, one size does not fit all. Let us provide a few examples.

- If you are a software company providing applications online, your most pressing concern is guaranteeing the authentication and integrity of your solutions. Your customers must be convinced they are downloading and installing the correct application on their device.
- If you are a police force in operations, your first concern is availability, followed by confidentiality, over your communications.
- If you are a hospital transmitting patient medical records to a distant location, long-term privacy is a major requirement.
- If you operate a large data center that requires daily backups of terabytes of data from different companies between two locations, your security requirements are not the same as Mr. Smith, surfing the Internet to buy a new appliance.
- If you are a government needing "perfect" security, you could use a one-time pad (OTP), which has been proven to be secure. However, security rests completely on the randomness of the key and the security of the key distribution, which must be addressed.

The conclusion: cryptographic tools must be adapted to fit specific types of data. Any new tools developed to answer the threat of the quantum computer must be tailored for specific applications.

4. Digital and physical security

Since the discovery of public key cryptography about 40 years ago, the public's understanding of computer security has focused primarily on digital security methods, such as algorithms that provide authentication and encryption for online communications. Security of a cryptographic scheme is based on mathematics and resilience against large computing power. In this framework, cryptographic keys are seen as an abstract series of bits, ones and zeroes. To ensure the security of the scheme, this string has to be truly random (and of course kept secret).

However, the physical security of data is also critical. For example, security breaches affecting governments and large organizations are often linked to insiders, capable of physical access not afforded the outside world. This, despite the fact that digital avenues may have been closed and intensive security protocols employed. Cryptographic keys are not only abstract random strings, but also real physical objects which should be stored in secured physical appliances. Serious certificate authorities use hardware security modules (HSMs) certified to Federal Information Processing Standards (FIPS) 140-2 level 3 or 4, as well as proactive and retrospective measures to protect the root keys for most certificates used on the Internet. This comprehensive approach leads to a physical security levels on par with Fort Knox.

Interestingly enough, while the understanding of keys as physical objects is well-accepted for storage applications, the same does not yet apply to key distribution, which is still mostly seen on the digital abstract level. In reality, one can also understand key distribution on the physical level. This is typically the case for *quantum key distribution* (QKD), which will be addressed in section 8. Quantum key distribution is an example of a physical system that can be used as an element of a complete security solution in much the same manner as an HSM (which stores the physical keys in another element of the security solution). The quantum computer itself is proof that data is not only a series of bits, but may take other guises, and with unexpected outcomes.

New tools should include all physical and mathematical security systems, each with its own practical application domain.

5. The impact of cloud computing on quantum-safe security strategies

The ongoing move toward the cloud for all our information technology (IT) needs greatly increases the reliance on data networks. Data is stored in huge data centers, and transferred between them at ever-increasing rates. The cloud model—with its associated storage and network requirements—enables a stronger and more reliable IT infrastructure. This heavily networked model also opens some serious new post-quantum threat vectors. One of the most serious threat vectors is a "data-vaulting" or harvesting attack where an attacker—in the here and now—stores communications between the client and the cloud so that data can be decrypted in the future when general purpose quantum computers are available. In the pre-cloud past, much of this data would have moved over private intranets not accessible by attackers. Today, it is physically transmitted over public telecommunication networks. Confidentiality and trust is restored by the use of virtual private networks (VPNs), which are based on cryptographic methods.

Current news reports inform us that organizations are orchestrating data vaulting attacks of public network communications traffic on a regular basis. Simultaneously, governments, financial institutions, healthcare organizations and many other entities are expected to keep their records confidential for decades to come. Alarmingly, information compiled during a successful data vault attack and transmitted *today* may already be compromised by future quantum computers (if the data is being monitored and stored). In reality, general purpose quantum computers may be here *long before this data becomes non-confidential*. Additionally, if networks are not re-tooled to be *quantum-safe*, the network infrastructure itself will be at serious risk to many post-quantum attack vectors. In the post-quantum era, denial of service attacks will be possible—perhaps even common—for networks that have not been re-tooled to be *quantum-safe*. Data "at rest" in enormous cloud data centers will also be at risk since quantum computers will effectively reduce the keys protecting that data to half of their original strength. Additionally, post-quantum attack vectors will compromise the key management systems that generate, distribute and protect the keys needed to secure that data.

Why do we expect attackers to go to such great lengths to attack cloud computing, both now and in the future? This can be explained with an analogy: a famous American bank robber of the 1930s, Willie Sutton, was asked by a reporter why he robbed banks. Sutton allegedly answered: "Because that's where the money is." In our connected world, data is the new asset. Hackers will concentrate their efforts on the largest data collections, the modern-day equivalent of the banks during the last century. In fact, most money in circulation today is not printed on paper or stamped into coins. It's data—1s and 0s—securely transmitted over data networks, with the largest concentrations of information in cloud data centers. Any connections and links between these large data centers must have the highest levels of protection possible. The need for *quantum-safe* cybersecurity is greatly compounded in a cloud-based IT environment.

6. Current cryptographic tools

6.1 The Tools

Our most crucial communication protocols and key management systems rely principally on three core cryptographic functions:

- Digital signatures
- Data encryption
- Key exchange

In order to fulfill these functions, we have several families of tools at our disposal, namely:

- Hash functions
- Symmetric cryptography
- Asymmetric cryptography
- Quantum key distribution (QKD)

The relationship between the tools and the functions they fulfill is presented in Table 1 (following page).

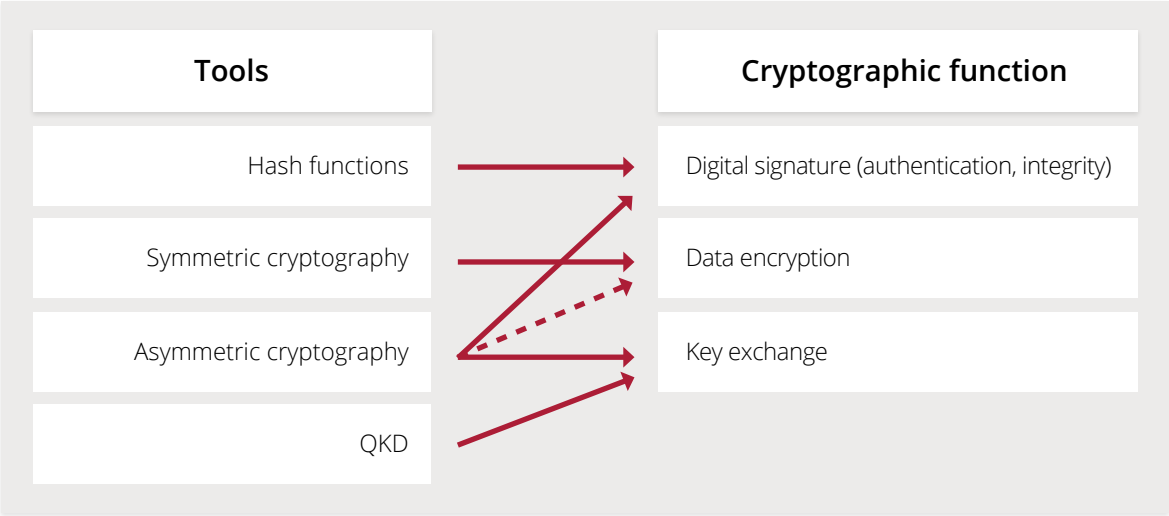


Table 1: Relationships between tools and cryptographic functions

The main applications for each of the tools are linked with a full red line; the secondary application has a dotted red line (see text for details).

As is apparent from Table 1, asymmetric cryptographic algorithms can be used for all functions[2]. However, they are not often applied to data encryption because of the low encryption speed. Because of their speed, especially with specific hardware implementations, symmetric algorithms (like advanced encryption standard (AES)) are the tool of choice for this purpose.

[2] Note, however, that not all asymmetric algorithms can be used for all functions.

6. 2 The need for randomness

It is important to note that all the functions above require randomness for their implementation. A recent white paper from the QSS-WG [MHMW15] explains this need, and suggests using quantum random number generators (QRNGs) to obtain them. Good, reliable random number generation is a requisite for all cryptographic applications.

6.3 Quantum-safe status

The standard asymmetric cryptographic algorithms currently in use are Diffie-Hellman (DH) key exchange, RSA and elliptic curve cryptography (ECC). These algorithms base their security on one of the following hard mathematical problems: the integer factorization problem; the discrete logarithm problem; and the elliptic curve discrete logarithm problem. All of these problems are solved easily with Shor's algorithm [Shor97] running on a general purpose quantum computer with a sufficient number of qubits. For example, a quantum computer with about 4,000 qubits would break 2048 bit RSA and DH, while a quantum computer with only 2,300 qubits would already break 384 bit ECC. Therefore, none of the aforementioned algorithms will withstand the arrival of the quantum computer. The key to quantum-safe cryptographic algorithms is to base them on difficult mathematical problems which neither classical computers nor quantum computers can break.

Symmetric cryptography (AES, 3 Data Encryption Standard (DES), etc.) and hash functions (Secure Hash Algorithm (SHA)-2 and above, etc.) do not succumb as easily to quantum computers. A quantum computer algorithm called "Grover's search algorithm" can be used to attack these [Grover96]. It provides, at most, quadratic speedup in comparison with search algorithms on classical computers. In addition, it has been shown that an exponential speed-up for search algorithms is impossible, suggesting that symmetric algorithms and hash functions should be usable in a quantum era. To offset the effect of Grover's algorithm on symmetric cryptographic algorithms, a simple approach would be to double the symmetric key sizes and hash function sizes.

A recent NIST document [CJLMPPS16] provides a table which summarizes the current situation and forecast for hashes, symmetric cryptography and asymmetric cryptography in the post-quantum era. The conclusions

drawn from the table and the report are twofold. The following quotes are from the report itself:

1. "Symmetric algorithms and hash functions should be usable in a quantum era…"
2. "The search for algorithms believed to be resistant to attacks from both classical and quantum computer attacks has focused on public key algorithms…"

NIST also makes a clear distinction between the quantum-resistant status of hash functions and symmetric cryptography (which are considered safe), and the new asymmetric cryptographic algorithms (detailed below), which are good candidates but require further scrutiny.

In terms of resistance to quantum computer attacks, QKD is in a different class because it is not based on hard mathematical problems and the quantum computer has no impact on its security.

7. Candidates for quantum-resistant algorithms

7.1 Definitions

The terminology for the algorithms that should be used in the post-quantum era is still uncertain. Currently, two (mostly) equivalent terms are being used by the security industry. Some refer to post-quantum algorithms (PQAs), while others prefer the term quantum-resistant algorithms (QRAs). Here, we will use the latter, which conveys the fact that the new algorithms should withstand the power of the quantum computer. As explained in the NIST report [CJLMPPS16], there exist good candidates for QRAs for all our cryptographic applications, which we review below. The QSS-WG has published a short white paper on this topic [CHH15], and ETSI has also produced an extensive document [CHH15].

7.2 Symmetric cryptography

It is widely believed that basic symmetric cryptosystems such as block ciphers (typically, AES) or hash functions (e.g., SHA2 or SHA3) are QRAs. Indeed, the best-known quantum attack against such cryptosystems is Grover's algorithm [Grover96]. Thus, the advent of the quantum computer will require an increase in the key size (and a doubling of the bit number). The current recommended key size of 256 bits is considered as safe, even against Grover's algorithm.

Symmetric encryption is used for data encryption. It relies on the existence of a secret key, shared between users. The most widespread algorithm, AES, is widely believed to be a QRA. Due to Grover's algorithm, it is also known that the advent of the quantum computer will require an increase in the key size (a doubling of the bit number). The current recommended key size of 256 bits is considered as safe, even against Grover's algorithm.

7.3 Asymmetric key exchange and signature

In the process to establish a secure channel, public-key cryptography is mostly used for authentication and for exchanging the secret keys, which will then be applied in a symmetric scheme as in Section 7.2. We describe below some of the most promising schemes; however, this area is still changing quickly. The NIST competition launched in February 2016 [M2016] will certainly help advance these issues.

7.3.1 Code-based cryptography

The McEliece cryptosystem [McE78] has been around since 1978 and has not been broken. This is the oldest quantum-resistant algorithm. Other systems based on error-correcting codes have been proposed. Code-based cryptosystems usually have very fast encryption and decryption algorithms. These code-based algorithms have large key sizes. Recently, in an attempt to decrease key sizes, some new code-based cryptographic algorithms—which have added more structure to the code—have been introduced [MB09, MTSB13]. The added structure has tended to lead to successful attacks against those proposals (e.g., [FOPT10], [FOPPT15] and [JSG16]). Code-based cryptography can be used in encryption as well as in signature [CFS01].

7.3.2 Lattice-based cryptography

Lattice cryptography has been around for about 20 years, providing asymmetric cryptography and signing.

Of the original proposed lattice cryptographic schemes, one scheme—NTRU [HPS98]—has undergone scrutiny the duration of this period. As a result, NTRU has been enhanced and ultimately standardized [9]. Recently, additional lattice-based algorithms such as "learning with errors" (LWE) [Reg05] and "ring learning with errors" (R-LWE) [RLWE13] have been proposed and are receiving scrutiny. Very recently, Google announced it will test an R-LWE algorithm in a test version of Chrome [G16]. The algorithm, dubbed "New Hope," will be implemented in combination with Google's standard encryption (see Section 9.3.1 for the description of hybrid systems). In April 2016, an NIST Report [CJLMPPS16] summarized the state of lattice cryptography, as follows:

> *"Most lattice-based key establishment algorithms are relatively simple, efficient, and highly parallelizable. Also, the security of some lattice-based systems are provably secure under a worst-case hardness assumption, rather than on the average case. On the other hand, it has proven difficult to give precise estimates of the security of lattice schemes against even known cryptanalysis techniques."*

Lattice cryptography is also expanding into other important areas of cryptography beyond the basic functions of signing and public/private key encryption, such as homomorphic encryption [G09] and code obfuscation [K14].

7.3.3 Multivariate cryptography

Multivariate cryptography is based on the difficulty of solving systems of multivariate polynomials over finite fields. It is a classical candidate in quantum-safe cryptography—dating from the late 1980s—and has been well-identified by ETSI [CCDDFGZ15] and NIST [CJLMPPS16]. The first multivariate scheme, known as C*, was proposed by Matsumoto and Imai [MI88]. Although C* has been broken, the general principle of the Matsumoto and Imai scheme inspired a whole generation of researchers that proposed improved variants based on that original blueprint (see: [HFE96], [ETSI16]). Multivariate cryptography has been very productive in terms of design and cryptanalysis (see: [ETSI16], [DFSS], [FJ03], [BFP13]). Overall, the situation is now more stable and the strongest schemes have withstood the test of time. Multivariate cryptography turned out to be successful as an approach to signatures primarily because multivariate schemes provide the shortest signature among quantum-resistant algorithms.

7.3.4 Hash-Based cryptography

Hash-based signatures are digital signatures constructed using hash functions. Their security against both classical and quantum attacks is well understood. However, all existing hash-based signature schemes have very large signature sizes compared to asymmetric key solutions. In general, with hash-based signatures, a private key is actually made up of a series of subkeys. Each signature is carried out with a different subkey. If the same subkey is ever used twice, the security of the entire public key is compromised. Therefore, a secure signature requires that one of two actions occur: either the signer must maintain a record of every subkey that has been used (a stateful signature); or the key must have so many subkeys—and such a large private key—that there is no chance the same key will be chosen at random twice (a stateless signature). XMSS [XMSS] is a stateful hash-based signature scheme with a large signature size that is currently undergoing standardization [6]. SPHINX [SPHINCS15] is a stateless hash-based signature scheme with a large key size and a very large signature size. Finally, the Leighton-Micali signature scheme (LMSS) instantiates Merkle's tree-based approach with a one-time signature scheme of Lamport-Diffie-Winternitz-Merkle. The Internet Engineering Task Force (IETF) is reviewing a draft of this authored by David McGrew. Note that the harvest attack, whereby the eavesdropper stores the data for later use (as described in Sections 2 and 5), does not apply to signatures schemes. Signatures are verified immediately after the transmission.

8. Current status of quantum key distribution

8.1 Principle

Quantum key distribution (QKD) [GRTZ02], provides a way to share a secret key between two users. It is based on the transmission of physical particles, typically photons, over a transparent channel. The basic idea is that any attempt at eavesdropping on the transmission channel, which represents a measurement of the particles, modifies their states. This change will be discovered by legitimate users, who can then discard the exchange. A brief introduction to QKD is presented in a previous white paper from the QSS-WG [MHHWK15]. Secrecy is not based on any mathematical assumption or result, but has been theoretically proven from the tenets of quantum mechanics. This key can later be used for any cryptographic purpose. So far, the main application is for encryption, especially in conjunction with symmetric key encryption. Information theoretically secure encryption can also be achieved with QKD and a one-time pad. As QKD is not based on computations, it is intrinsically quantum safe: the quantum computer has no influence on its security.

8.2 Need for a physical link

As explained above, QKD requires transmission of physical particles over a so-called quantum channel. Due to unavoidable loss in the channel, this brings up a limitation in the length of a QKD link. Commercial implementations of QKD utilizes the widely available optical fiber infrastructure used in telecommunication. The typical length of a QKD channel is tens of kilometers (with a maximum of approximately 100 kilometers). However, up to 300 kilometers has been achieved in an academic proof of principle. Free space implementations, which may lower the cost of a solution and/or increase the maximum length, are in research stages. The length of a QKD network can be increased by means of a trusted node infrastructure, where several QKD links are connected through safe locations (such as telecom exchanges). For example, a QKD backbone linking Beijing to Shanghai is under construction. A worldwide QKD network can be envisaged with improved technology (see Section 8.6)

8.3 Real-time eavesdropping

The fact QKD requires a physical link is rightly seen as a hindrance. However, in some aspects, it is also an advantage. A stark difference between algorithmic-based key distribution and QKD is that, for the later, an eavesdropper can only attempt to discover the key during a transmission. At the conclusion of a transmission, legitimate users know if their key is safe or not. When QKD is utilized, this basic equation will not change: The eavesdropper must intercept the key during those moments, or remain ignorant.

All things considered, one advantage of QKD is that it has to fight only against existing technology. If you cannot intercept the key with existing technology, you will not be able to use superior technology in the future to gain further knowledge. In contrast, algorithmic systems have the much more difficult task of having to plan for both current and future threats. Indeed, descriptions of harvesting attacks outlined in Sections 2 and 5 can be used for data, but also for keys. It's anyone's guess which technological and mathematical advances will be available in 20 or 30 years. However, one example may be useful to consider as a cautionary tale: In 1977, when the RSA algorithm was first introduced, an article in *Scientific American* estimated it would take 40 quadrillion years to decrypt a message encrypted with the then-current key size. In fact, that key was cracked less than 20 years later.

8.4 Authentication and signature

QKD only addresses one specific issue in the wide spectrum of security tasks: namely, the key distribution. In order to provide a complete solution, it requires the addition of conventional cryptographic tools. In particular, quantum secure authentication and signature—as well as quantum secure encryption—are needed. Fortunately, the QRAs described in Section 7.3.3 can provide the required tools.

8.5 Quantum hacking and certification

A significant advantage of QKD is that it has been proven to be theoretically secure. Any eavesdropper attempt to extract information from the exchange will be discovered. However, this does not preclude possible flaws in its implementation. The security proofs apply to an eavesdropper who only has access to the transmission channel. More advanced strategies, where the eavesdropper gains access to users through a so-called

"side-channel attack," have been successfully designed [BP12]. This is the domain of quantum hacking.

Side-channel attacks are not restricted to QKD, or to physically-based cryptography. At the end of the day, any cryptographic implementation is based on some physical system, such as a computer churning out numbers. Indeed, acoustic cryptanalysis—a side-channel attack based on the noise emitted by the computer performing cryptographic operations—was shown to be able to break RSA encryption. Other attacks are based on electromagnetic emissions. Once the attack is known, it is relatively simple to implement a counter measure. However, these types of attacks bring to light the fact that any proof of security relies on a given set of assumptions that a clever eavesdropper will always try to find her way around. In order to attain confidence in a cryptographic scheme, implementations of the scheme have to be thoroughly scrutinized and subjected to various types of attacks. Implementation guidelines can then be written by the proper certification bodies.

Quantum hacking is in no way different from the side-channel attacks on conventional cryptography. The quantum world only adds a new facet to the ongoing struggle between cryptographers and hackers. As for existing implementations of conventional cryptography, proper certification ensures that various attacks have been taken into consideration, and that the implementation follows a set of rules. Developing a proper certification structure is a must in order to provide trust in a QKD infrastructure.

8.6 A future worldwide QKD network

The most significant restraint to widespread use of QKD is the distance limitation for a QKD link. However, this is not a fundamental restriction. This same technology, which should usher in the arrival of the quantum computer in the next 10 to 15 years, should also generate solutions for QKD shortcomings. A worldwide QKD network is definitely a possibility. This system could utilize satellites as trusted nodes, which would safely exchange secret keys with the ground, securely store the secret keys, and finally carry the keys to another location. In fact, the first QKD satellite was recently launched by the Chinese Academy of Science [X16]. The Academy's aim is to provide a proof-of-principle for QKD in space. The trusted nodes can later be replaced by untrusted ones through the use of quantum repeaters, which will remove the distance limitation on a quantum link. With quantum memories—where qubits (the quantum counterpart of the usual bit) can be stored and later used in computations—the keys will not be distilled at all, but kept in a quantum state until they are used.

These new components—which will be built for the quantum computer—can be used to design a complete QKD infrastructure, capable of distributing secret keys everywhere. This QKD network might be expensive, and may not be used for low-level encryption. However, it would allow for truly long-term confidentiality and privacy, independent of future progress (or lack thereof) in computation (classical or quantum) that may be required for other types of data.

If we look a bit deeper in our crystal ball, we can also envisage a full quantum Internet. Once we can distribute, store and manipulate qubits, we can also build an extra layer at the quantum level. This quantum layer will then be integrated into the structure and become transparent. This scenario exactly describes the optical layer we have today. Internet does rely on the transmission of physical objects, specifically optical pulses, between different points. However, the optical layer is entirely integrated, and people using it do not even realize what lies below.

9. Re-tooling to quantum safety

One of the aims of the QSS-WG is to provide the industry with practical suggestions for achieving *quantum-safe* security. The threats posed by the development of the quantum computer—which is both credible enough to warrant action and far enough away from reality to give us time to react—might be a good opportunity to open our cryptographic toolbox and find new ways to protect information. Reflecting on the three major cryptographic functions defined in Section 6.1, Section 9 will present methods to ensure current and future quantum safety for each function that could be implemented immediately.

9.1 Quantum-safe signatures and authentication

Quantum-resistant signature and authentication schemes were introduced in Section 7.3. Among them are schemes which are practical and already well-accepted in the cryptographic community. While a great deal of new work is expected in these areas, effective quantum-resistant signature algorithms already exist today which will allow us to start the journey to post-quantum signing and authentication. Note that signature and authentication are absolutely fundamental to information security. The Internet may survive as a commercial tool with lower privacy, but it cannot survive against the quantum computing threat if its authentication and integrity are compromised.

9.2 Quantum-safe data encryption

Data encryption is, comparatively, the "easy" part because it mainly relies on symmetric cryptography, which is not threatened dramatically by the quantum computer. AES with 256 bit keys is considered as safe against both classical and *quantum attacks*. If new threats occur, key length may be increased in the future.

9.3 Quantum-safe key exchange

9.3.1 Hybrid systems

Currently, there are several quantum-resistant public key algorithms for key exchange and asymmetric encryption available. Some have been extensively vetted, and one has undergone standardization. In addition to standardization, many implementers prefer to—or are required to—use cryptographic algorithms which are approved by governments (e.g., NIST SP800-131a, NSA Suite B, ISO standards, etc.). However, governments have not yet updated their approved algorithms lists to include quantum-resistant algorithms. Fortunately, we do not have to wait to start making today's communications *quantum-safe*. There is a solution, and it's called the "Quantum-Safe Hybrid Technique" (QSH), which mixes a standard, approved method and a quantum-resistant algorithm. QSH can even be implemented to be FIPS 140-2 compliant, and is not specific to any particular quantum-resistant cryptographic algorithm. It has been published as an Internet Engineering Task Force (IETF) draft [SWZ02], and is currently in the process of being advanced to an IETF request for comments (RFC) document.

As a practical example of a hybrid system, examine how QSH permits TLS (transport layer security) to use any of its current cryptographic algorithms together with a quantum-resistant algorithm, an interaction that occurs during the negotiation of the TLS symmetric session key. The TLS session key is a shared symmetric key which is negotiated using asymmetric cryptographic algorithms. The additional post-quantum algorithm is used to transport a *quantum-safe* component between the two parties negotiating the communications session. Below are some of the highlights of QSH.

- Implementers are allowed to continue using approved algorithms in their TLS session key negotiation with the added benefit of making them *quantum-safe*. If the original implementation is FIPS 140-2 compliant, the FIPS 140-2 compliance can be preserved when implementing the addition of the *quantum-safe* component.
- The additional necessary quantum-safe component is added to the TLS key generation function. Each party in the TLS communication session uses their key derivation function (KDF) to generate the shared symmetric session key needed for private communications.
- Today, using only current cryptographic algorithms for the negotiation of the TLS session key, a quantum computer would be able to expose the session's symmetric key as clear text. The addition of the quantum-resistant cryptographic algorithm and the *quantum-safe* component stops the exposure of the TLS session key by a quantum computer. The confidentiality of today's data against harvesting attacks (see Sections 2 and 5) can be maintained going forward into the post-quantum era.

The following figure provides a detailed flow of how QSH works:

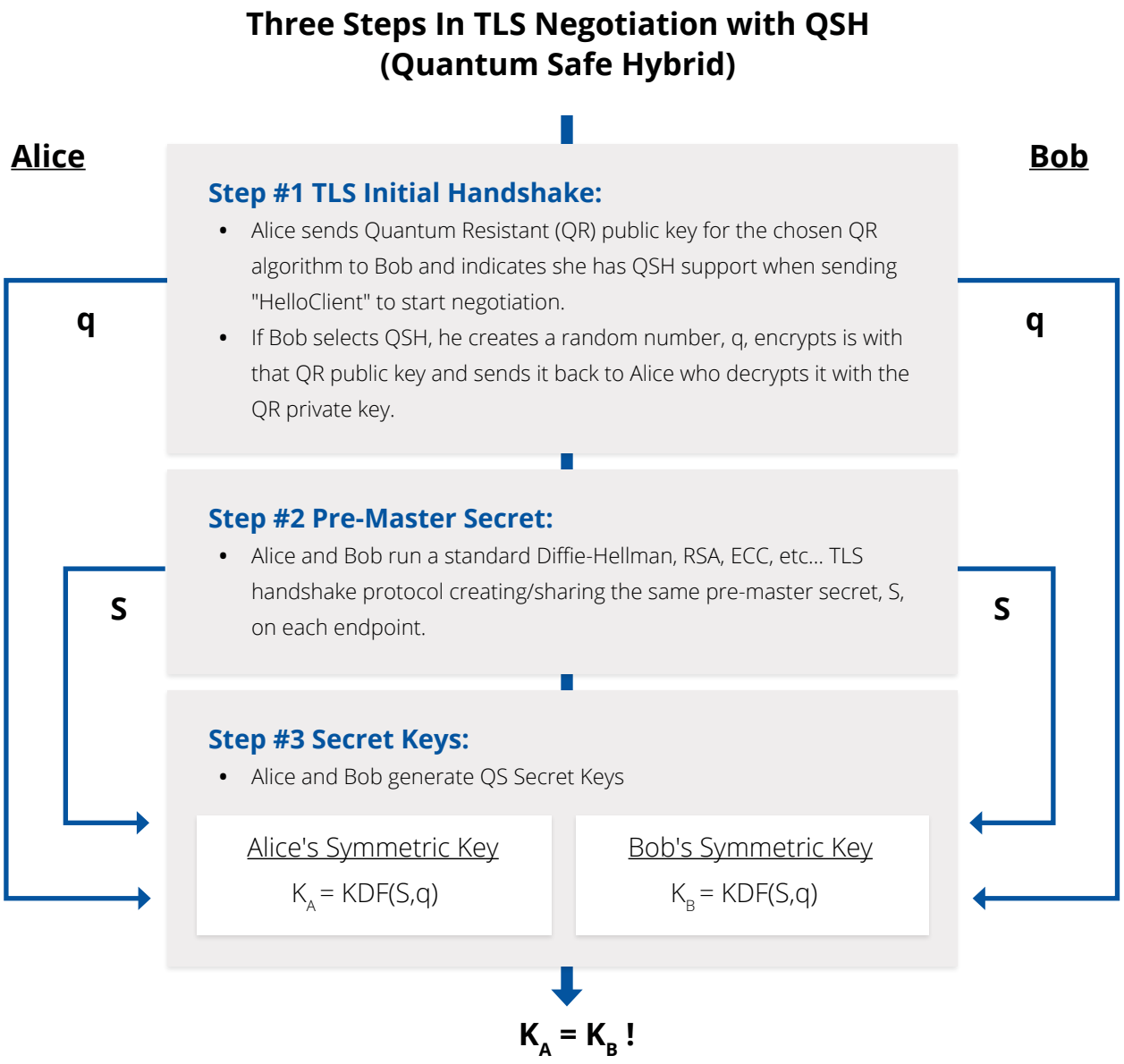


Figure 1: Flow of QSH negotiation for TLS protocol

(KDF stands for Key Derivation Function)

The QSH technique can be extended beyond TLS for a variety of key establishment/key exchange environments.

9.3.2 QKD as an add-on for high-value links

As discussed in section 8.3, a fundamental advantage of QKD is the fact that the only attack which can be attempted by an eavesdropper must be in real-time. If eavesdroppers do not attempt to steal information about the key during its transmission, downloading and storing the whole transaction between legitimate users will not achieve anything. Furthermore, because of the very nature of QKD, any such attempt will be discovered by legitimate users. At the end of the transmission, users know if the key is secure, or if it should be discarded. Therefore, for high-value links, adding QKD provides an extra layer of safety (which is known to be *quantum-safe*). A new type of hybrid system—specifically one that can use any asymmetric cryptographic system (including the above QSH) while adding the QKD layer—will ensure the highest security level, especially for links requiring long-term security. It should be used in conjunction with *quantum-safe* signature and authentication protocols described in Section 7 . This system will not be threatened by new technological advances such as the quantum computer, or by new mathematical progress. However, due to its current length limitations and higher cost, it cannot be applied everywhere. It should be used for specific links (for example between data centers), and for all links where long-term privacy is a requirement.

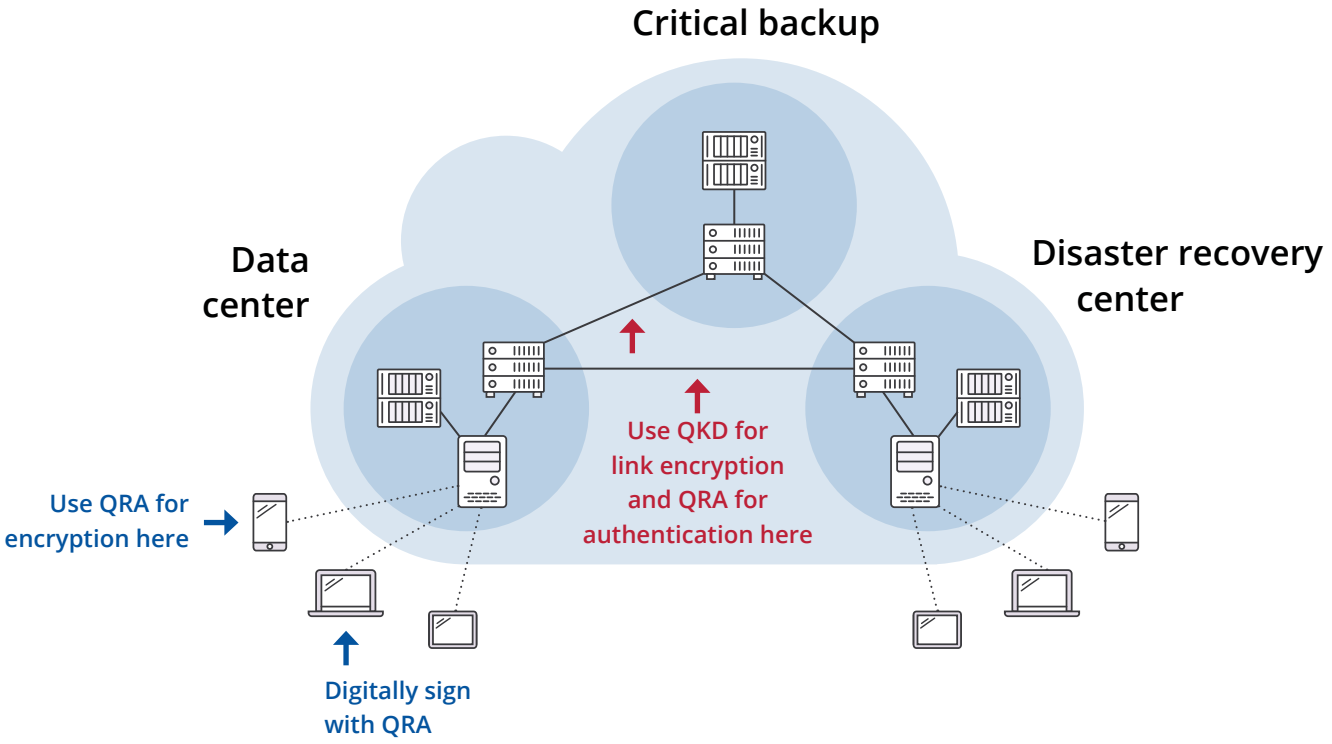


Figure 2: Use case of QRA and QKD

The links between the data center and the users are protected by QRA for encryption and signature. The more crucial links between the data center and the backup or recovery center are protected by QKD. This is exemplified in Figure 2, which shows a use case for a QKD and QRA application. High-value links require long-term protection, which is obtained with QKD. Foreseeable developments in quantum technologies should lift the distance limitation and enable a worldwide QKD network.

10. Conclusion

> *"Prediction is very difficult, especially if it is about the future."*
>
> **—Niels Bohr**

That famous quote from Niels Bohr seems to apply well to the current situation regarding cyber security. It is very difficult to predict the direction of cyber security in the long-term. However, what does seem certain is that our current toolkit must be completely modified to answer the potential threat of the quantum computer. Until about one year ago, the feasibility of a quantum computer was still a largely unresolved issue, but recent statements by the NSA and NIST have changed this equation. Most in the cyber security community now believe that having a cryptographically relevant quantum computer is only a question of time and investment. The positive news is that we have meaningful information which can help us set timeframes for addressing the post-quantum threat. In Section 2, we laid out the timeline for the arrival of general purpose quantum computers that can do crypto breaking. The probability of its development increases rapidly starting at the beginning of the next decade. For industries with very high security requirements (such the healthcare and financial sectors), preparation must occur before quantum computing becomes a real threat. Being prepared means they must be completely re-tooled for quantum-safety, which is a noteworthy undertaking. If they gamble and quantum computers arrive before they predict, the result could be catastrophic. Confidential data being transmitted today over the Internet may already be compromised since much of it is required to remain confidential after the quantum computing threat has arrived.

Today, a significant portion of the security community is not familiar with quantum-safe cryptography and QKD. It is important that the IT industry begins to develop "quantum risk-management plans" (a term from the Institute for Quantum Computing) for an orderly transition to a fully quantum-resistant security infrastructure. We all need to start understanding and employing quantum-safe cybersecurity measures and technologies. The truth is, a great deal of work is yet to be done with governments and standards organizations in regard to certain important aspects of the post-quantum threat. However, there are numerous areas where we can begin to plan for quantum-safe cybersecurity and, in some cases, take action now.

ANNEXES

11. Glossary of Terms

- **quantum technology:** Technology that relies on specific aspects of quantum mechanics, namely coherent superposition and entanglement. QKD and quantum computers are two examples of these technologies, which are relevant to the field of cyber security.
- **post-quantum cryptography:** A broad term typically used to refer to cryptographic schemes which offer resistance to computers capable of running quantum algorithms. This includes physics-based cryptosystems that rely on quantum technology, such as QKD, as well as algorithmic cryptosystems (potentially, lattice-based, multivariate quadratic-based, hash-based, and isogeny-based cryptosystems, etc.).
- **quantum-safe:** This term is used interchangeably with post-quantum to describe cryptographic schemes and security protocols, which should withstand the arrival of the quantum computer and the implementation of quantum algorithms. It has been used by ETSI and the CSA Quantum-Safe working group.
- **quantum-resistant algorithms:** Refers to algorithm-based cryptosystems which achieve quantum-safe security in conventional computer ecosystems. This is the terminology used consistently by the NSA in their announcement regarding their, "preliminary plans for transitioning to quantum-resistant algorithms." Quantum resistant may be used to describe a cryptographic algorithm that is not susceptible to attack by a quantum computer, or to describe a security solution that implements security protocols that use quantum-resistant algorithms.
- **quantum attack:** An attack on a security system, which rely on quantum algorithms running on a quantum computer, to break security.
- **quantum key distribution (QKD):** A cryptographic primitive, which relies on quantum technology to provide quantum-safe security.
- **cryptographic primitives:** Low-level cryptographic algorithms and systems that can be used to build security protocols and cryptosystems.
- **practical quantum computer:** A computer capable of running one or more of Shor's or Grover's algorithms to break conventional public-key cryptography; also called a cryptographically relevant or universal quantum computer.

References

[BFP13] Bettale, L., Faugère, J.-C.,& Perret, L. (2013). Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Designs, Codes and Cryptography*, 69 (1), pp. 1–52

[SPHINCS15] Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., & Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical Stateless Hash-Based Signatures. In: Oswald, E. & Fischlin, M. (Eds.) *Advances in Cryptology—EUROCRYPT 2015* (pp. 368-397). Lecture Notes in Computer Science, Vol. 9056. Springer Berlin Heidelberg

[BP12] Braunstein, S. L., & Pirandola, S. (2012). Side-Channel-Free Quantum Key Distribution. *Physical Review Letters* 108 (13).

[BDH11, XMSS] Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS: A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In: Yang, B.-Y. (Ed.) *Post-Quantum Cryptography* (pp. 117-129) Lecture Notes in Computer Science, Vol. 7071. Springer Berlin Heidelberg

[CCDDFGZ15] Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J.K., Gisin, N., ... Zhang, Z. (2015). Quantum Safe Cryptography and Security. [White Paper]. No. 8, June 2015. European Telecommunications Standards Institute. Retrieved January 17, 2017, http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[CHH15] Carter, G., Hayford, D. & Huttner, B. (2015). What is Post-Quantum Cryptography? [White Paper]. Cloud Security Alliance.

[CJLMPPS16] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). NISTIR 8105 DRAFT: Report on Post-Quantum Cryptography. N*ational Institute of Standards and Technology Internal Report 8105* (February 2016). Gaithersburg, MD: U.S. Department of Commerce. Retrieved January 17, 2017, from http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf

[CFS01] Courtois, N.T., Finiasz, M., & Sendrier, N. (2001). How to Achieve a McEliece-Based Digital Signature Scheme. In: Boyd, C. (Ed.), *Advances in Cryptology—ASIACRYPT 2001* (pp. 157-174). Lecture Notes in Computer Science, Vol. 2248. Springer Berlin Heidelberg

[DFSS] Dubois, V., Fouque, P-A., Shamir, A., & Stern, J. (2007). Practical Cryptanalysis of SFLASH. In: Menezes, A. (Ed.), *Advances in Cryptology—CRYPTO 2007* (pp. 1-12). Lecture Notes in Computer Science, Vol. 4622. Springer Berlin Heidelberg

[ETSI16] ETSI Industry Specification Group (ISG) Quantum-Safe Cryptography (QSC). (July 2016) Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. [Group Report]. Retrieved from ETSI http://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf

[FJ03] Faugère, J-C., & Joux, A. (2003). Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In: Boneh, D. (Ed.), *Advances in Cryptology*—CRYPTO 2003 (pp. 44-60). Lecture Notes in Computer Science, Vol. 2729. Springer Berlin Heidelberg

[FOPT10] Faugère, J-C., Otmani, A., Perret, L. & Tillich, J-P. (2010). Algebraic Cryptanalysis of McEliece Variants with Compact Keys. In: Gilbert, H. (Ed.), Advances in Cryptology—*EUROCRYPT 2010* (pp. 279-298). Lecture Notes in Computer Science, Vol. 6110. Springer Berlin Heidelberg

[FOPPT15] Faugère, J.-C., Otmani, A., Perret, L., Portzamparc, F., & Tillich, J-P. (2016). Structural cryptanalysis of McEliece schemes with compact keys. *Designs, Codes and Cryptography*, 79 (1), pp. 87-112

[G09] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *STOC '09 Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178). New York, NY: ACM Publications.

[GRTZ02] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002) Quantum Cryptraphy. *Reviews of Modern Physics*, 74 (1), pp. 145-195. Retrieved January 17, 2017, from https://d22izw7byeupn1.cloudfront.net/files/RevModPhys.74.145.pdf

[Grover96] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *STOC '96 Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp 212-219). New York, NY: ACM Publications.

[G16] Greenberg, A. (2016, July 7) Google Tests New Crypto in Chrome to Fend Off Quantum Attacks. *Wired*. Retrieved January 17, 2017, from https://www.wired.com/2016/07/google-tests-new-crypto-chrome-fend-off-quantum-attacks

[JSG16] Guo, Q., Johansson, T., & Stankovski, P. (2016). A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors. In: Cheon, J.H. & Takagi, T. (Eds.), *Advances in Cryptology—ASIACRYPT 2016* (pp. 789-815). Lecture Notes in Computer Science, Vol. 10031. Springer Berlin Heidelberg

[HPS98] Hoffstein, J., Pipher, J., & Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (Ed.), *Algorithmic Number Theory* (pp. 267-288). Lecture Notes in Computer Science, Vol. 1423. Springer Berlin Heidelberg

[K14] Klarreich, E. (2014, February 3) Cryptography Breakthrough Could Make Software Unhackable. *Quanta Magazine*. Retrieved January 17, 2017, from https://www.wired.com/2014/02/cryptography-breakthrough

[KPG99] Kipnis, A., Patarin, J., & Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (Ed.), *Advances in Cryptology—EUROCRYPT '99* (pp. 206-222). Lecture Notes in Computer Science, Vol. 1592. Springer Berlin Heidelberg

[RLWE13] Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On Ideal Lattices and Learning with Errors over Rings. *Journal of the ACM (JACM)*, 60 (6), Article No. 43

[MHHWK15] Melia, J., Huttner, B., Hayford, D., Walenta, N., & Kerling, F. (2015). What is Quantum Key Distribution? [White Paper]. Cloud Security Alliance.

[MHMW15] Melia, J., Huttner, B., Moulds, R., Walenta, N., & Fuller, A. (2016). Quantum-Safe Security Working Group: Quantum Random Number Generators. [White Paper]. Cloud Security Alliance.

[MB09] Misoczki, R., & Barreto, P.S.L.M. (2009). Compact McEliece Keys from Goppa Codes. In: Jacobson, M. J., Riimen, V., & Safavi-Naini, R. (Eds.), *Selected Areas in Cryptology* (pp. 376-392). Lecture Notes in Computer Science, Vol. 5867. Springer Berlin Heidelberg

[MTSB13] Misoczki, R., Tillich, J.-P., Sendrier, N., & Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. *2013 IEEE International Symposium on Information Theory* (pp 2069-2073). Istanbul, Turkey: IEEE

[McE78] R.-J. McEliece (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory. T*he Deep Space Network Progress Report* (No. 42-44, pp 114-116). Pasadena, CA: National Aeronautics and Space Administration.

[NTRU09] NTRU Cryptosystems, Inc. (2009, February 18) *NTRU Announces That IEEE Has Approved the Standardization of NTRUEncrypt* [Press Release]. Acton, Mass.: BusinessWire.

[NTRU11] NTRU Cryptosystems, Inc. (2011, April 11) Security Innovation's NTRUEncrypt Adopted as X9 Standard for Data Protection [Press Release]. Wilmington, Mass.: BusinessWire.

[Reg05] Regev, O. (2005). On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *STOC '05 Proceedings of the thirty-seventh annual ACM symposium on Theory of computing* (pp 84-93). New York, NY: ACM Publications.

[MI88] Matsumoto, T. & Imai, H. (1998). Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Barstow, D., Brauer, W., Hansen, P.B., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N, & Günther, C.G.(Eds.), *Advances in Cryptology—EUROCRYPT '88* (pp. 419-453). Lecture Notes in Computer Science, Vol. 330. Springer Berlin Heidelberg

[M2016] Moody, D. (2016, February). Post-Quantum Cryptography: NIST's Plan for the Future. Presented at The Seventh International Conference on Post-Quantum Cryptography, Fukuoka, Japan. Retrieved January 17, 2017, from http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf

[HFE96] Patarin, J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. (Ed.), *Advances in Cryptology—EUROCRYPT '96* (pp. 33-48). Lecture Notes in Computer Science, Vol. 1070. Springer Berlin Heidelberg

[Shor97] Shor, P.W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*., 26 (5), pp. 1484–1509

[SWZ02] Schanck, J.M., Whyte, W., Zhang, Z. (2015). *Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.3.(Internet Engineering Task Force Draft)*. Retrieved January 17, 2017, from https://datatracker.ietf.org/doc/draft-whyte-qsh-tls13/.https://datatracker.ietf.org/doc/draft-whyte-qsh-tls13/

[X16] Xinhua (2016, August 16) China Launches First-Ever Quantum Communication Satellite. *Xinhua*. Retrieved January 17, 2017, from http://news.xinhuanet.com/english/2016-08/16/c_135601026.htm