Quantum Safe Cryptography V1.0.0 (2014-10)

Quantum Safe Cryptography and Security;
An introduction, benefits, enablers and challenges

ISBN 979-10-92620-03-0

Disclaimer

This document reflects the views of the authors.
It does not necessarily represent the views of the entire ETSI membership.

Reference

Quantum Key Distribution, Quantum Safe Cryptography

Keywords

Quantum Key Distribution, Quantum Safe Cryptography, Forward Security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Figures

Executive summary

Recent research in the field of quantum computing and quantum information theory has brought about a credible threat to the current state-of-the-art for information protection. The current data protection mechanisms that typically comprise cryptographic systems rely on computational hardness as a means to protect sensitive data. This is to say that there are cryptographic problems that are difficult or impossible to solve using conventional computing.

Because of recent advances in quantum computing and quantum information theory, the quantum computer presents a serious challenge to widely used current cryptographic techniques. This is because some of the same cryptographic problems, which are difficult or impossible to solve using conventional computing, become fairly trivial for the quantum computer.

In the practical case, even encrypted information sitting in a database for 25 years, for instance, will be subject to discovery by those having access to quantum computing platforms. The discovery of the content of such data may lead to serious consequences. These include the possible misuse of bank account numbers, identity information, items relating to military security and other sensitive information.

The current state-of-the-art cryptographic principles use well-studied methods that have been relied upon for more than 20 years. Amongst cryptographic experts, well-studied, proven and mature techniques are the most preferred for security reasons. However, such techniques were not designed to resist quantum attacks, because at the time of their invention, research into quantum computation was obscure and unknown to most cryptographic practitioners.

New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed “quantum safe” and consist of both techniques based on quantum properties of light that prevent interception of messages, as well as classic computational techniques, all of which were designed to resist quantum attacks emerging from the rapidly accelerating research field of quantum computation.

Cryptographic techniques are commonly found in many industries and fielded systems, usually as a component of broader network security products. These commonly available security products need to be upgraded with quantum safe cryptographic techniques, and this paper explores some of the most pervasive security systems while giving practical recommendations for upgrading to a quantum safe state. This is not a trivial undertaking, and requires the interest and support of security product vendors, industry customers, academic researchers and standards groups.

An important consideration is the cost of transitioning to quantum safe technologies. New products and trends tend to follow a standard cycle of innovation starting with early adopters who pay high premiums, and ending with commoditized product offerings with abundant competition. Quantum safe features will reset the innovation cycle for many common commoditized security products, but the real costs of concern are related to switching to new quantum safe technologies.

Quantum safe communication techniques are not compatible with techniques incumbent in products vulnerable to quantum attacks. In a well-ordered and cost efficient technology transition, there is a period of time where the new products are gradually phased in and legacy products are phased out. Currently, quantum safe and quantum vulnerable products can co-exist in a network; in some cases, there is time for a well-ordered transition. However, the window of opportunity for orderly transition is shrinking and with the growing maturity of quantum computation research, for data that needs to be kept secret for decades into the future, the window for transitioning may already be closed.

This paper is designed to be a practical introduction and reference for those in the Information and Communication Technology (ICT) community. The primary objective is to help raise awareness of the potential impacts of quantum computing on information security globally. This includes a 1) survey of current cryptographic principles, 2) the possible impact of quantum computing on their effectiveness and 3) what can be done to mitigate the risks in an economically and technically practical manner. We further include discussion of the enablers of quantum safe cryptographic techniques along with the realistic economic and technical challenges to its deployment in existing systems and the impact of global standards. We also present a section defining acronyms and related terminology, which is designed to be a reference for those operating in the ICT space in fields other than information security and cryptography.

1 Scope and purpose

Until fairly recently, the Information and Communication Technology (ICT) industry has considered information interchange transactions across electronic networks to be secure when encrypted using what are considered to be an unbroken conventional cryptographic system. Recent research in the field of quantum computing has produced a credible and serious threat to this assumption. Some problems that are considered difficult or impossible to solve using conventional computation platforms become fairly trivial for a quantum computer. Any information that has been encrypted, or will be encrypted using many of the industry's state-of-the-art cryptosystems based on computational-hardness is now under threat of both eavesdropping and attack by future adversaries who have access to quantum computation.

This means that even encrypted information sitting in a database for 25 years for example, will be subject to discovery by those with access to quantum computing platforms. The discovery of the content of such data could lead to very serious consequences. These include the misuse of bank account numbers, identity information, items relating to military security and other sensitive information. **Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure.**

This paper is designed to be a practical introduction and reference for those in the Information and Communication Technology (ICT) community. The primary objective is to help raise awareness of the potential impacts of quantum computing on information security globally. This includes a 1) survey of current cryptographic principles, 2) the possible impact of quantum computing on their effectiveness and 3) what can be done to mitigate the risks in an economically and technically practical manner. We further include discussion of the enablers of quantum safe cryptographic techniques along with the realistic economic and technical challenges to its deployment in existing systems and the impact of global standards.

2 Overview

2.1 What is cryptography and how is it used?

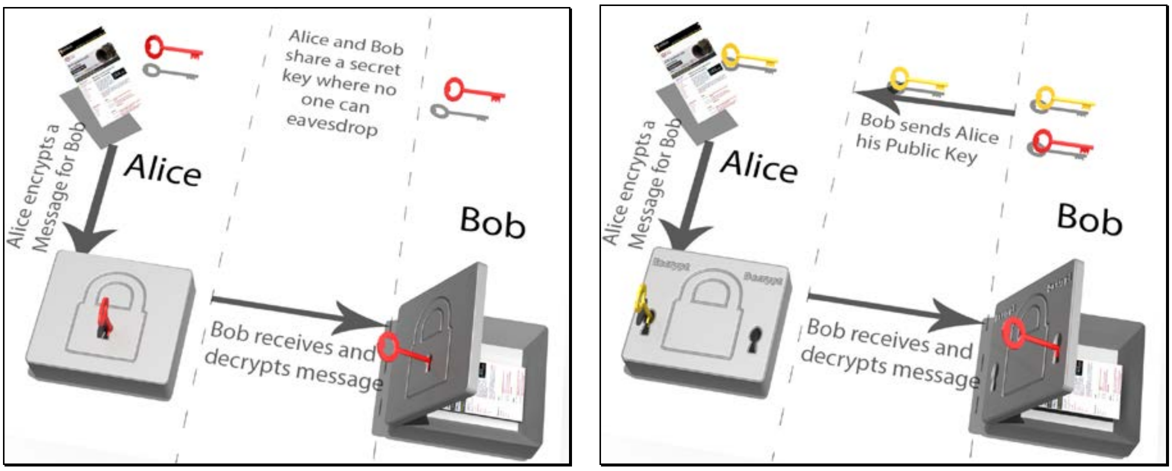
Cryptography is literally the art of “secret writing”. It is used to secure communication by protecting the confidentiality and integrity of messages and sensitive data. Without it, anyone could read a message or forge a private conversation. Messages are made secret by transforming them from “plaintext” into “ciphertext” using a cipher and performing the process of encryption. Decryption turns scrambled and unreadable ciphertext back into plaintext.

When cryptographers talk about a “key”, they are referring to a shared secret that controls the ability to hide and un-hide information. There are two types of cryptography that are often referred to as “symmetric key” and “public key” cryptography:

1. In symmetric key cryptography, the same key is used for both encryption and decryption, and that key needs to be kept a secret by everyone who is sending and receiving private messages. The major difficulty of symmetric key cryptography is to provide the secret keys to legitimate parties without divulging the keys to eavesdroppers.

2. Public key cryptography[1] is more involved and complex. There are two keys, one for encrypting and another key for decrypting. The two keys are mathematically related, and only one key is intended to be kept a secret. Public key cryptography allows anyone to send an encrypted message, but only one person, with the private key, can decrypt the message. Public key cryptography can also be used for digital signatures where someone with a private key can sign a message that anyone can verify with the public key.

Figure 1 - Cryptography Basics - Encryption and Decryption


Alice and Bob share a secret key where no one can eavesdrop
Alice encrypts a Message for Bob
Alice
Bob
Bob receives and decrypts message
Bob sends Alice his Public Key
Alice encrypts a Message for Bob
Alice
Bob
Bob receives and decrypts message

A - Symmetric Key Cryptography **B - Public Key Cryptography**

Cryptography is necessary but not sufficient for secure transmission of information. In practice, information is secured using cryptography within the context of security protocols which handle message formatting, key management and a plethora of other considerations that are used to broaden the primitive concept of secret message passing to the more practical art of modern secure communications.

While cryptography is not the entirety of security, it is an essential part. If the cryptography fails, all of the secret messages that are sent over public channels become readable to anyone who can passively observe.

Cryptography is important because without it, everyone could read anything they intercept, regardless of whether it was intended for them. Cryptography keeps sensitive data a secret (confidentiality), it is used to protect against changes to data over an unreliable public channel (data integrity), and it can ensure that communicating parties are indeed who they claim to be (authentication).

[1] Also sometimes referred to as “asymmetric key cryptography”

2.2 What is quantum computing?

Today's computers are governed by the laws of classical physics and Moore's law[2] which states that, historically speaking, computers double their speed and capacity every 18 months because chip makers are able to squeeze twice as many transistors onto a computer chip. In order for these computing improvements to continue, placing more transistors on a computer chip means that transistors need to get smaller. But physics presents a natural barrier in that once technology has shrunk a transistor to the size of a single atom there are no more improvements to be made to transistor size. But what if the transistor could be replaced with a better technology, a technology that allows for a new paradigm of computing?

The laws of physics that can be seen, observed, and understood through experiences in everyday life are referred to as classical physics, and these laws govern the workings and computational capabilities of computers as they are known today. However, everything that is described by classical physics at a macroscopic level can be described by quantum physics at a nanoscopic level, and these different physical laws are known as quantum mechanics. In the past few decades, researchers have realized that the ways in which the laws of physics allow different things to happen to very small objects can be harnessed to make computers out of novel materials, with hardware that looks and behaves very differently from the typical classical computers that people use in their homes and offices today. Quantum computers, obeying the laws of quantum mechanics, can calculate things in ways that are unimaginable from the perspective of people's regular day-to-day experiences.

In classical computing, information is stored in fundamental units called bits, where a bit can hold a binary digit with the value of 0 or 1. In quantum computing, the fundamental unit can hold both a 0 and a 1 value at the same time; this is known as a superposition of two states. These quantum bits are known as qubits and measuring the state of a qubit causes it to select or "collapse into", being a 0 or a 1. Interestingly, if you prepare a string of qubits of the same length in the same way, the resulting bit string will not always be the same. This gives quantum computers an advantage over classical computers in that they can perform very rapid parallel computations.

Quantum mechanics has some novel properties that researchers have realized can be harnessed to make quantum computers that behave very differently than the classical computers commonly used today. Using these novel quantum properties, a quantum computer is able to solve certain problems like searching and factoring much faster than the time it would take a classical computer, with the best known algorithms, to solve the same problem.

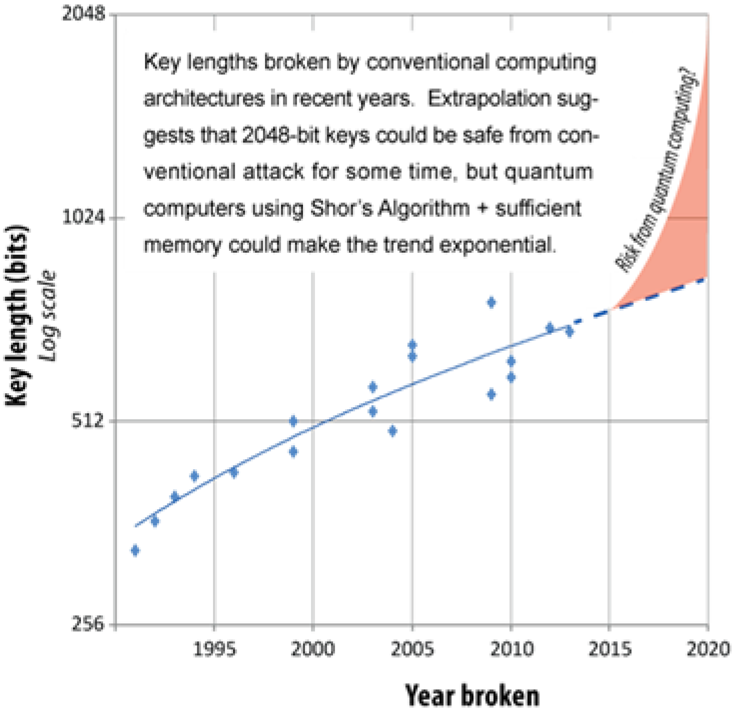


Figure 2 - Breaks of the RSA cryptosystem in recent years using conventional computation.

[2] Moore's law is not an actual law of physics, but instead a general observation and prediction made by a co-founder of Intel that describes the speed in which computing has matured.

For certain classes of problems, including integer factorization and discrete logarithms, quantum computers are able to perform computational tasks with efficiencies that are not known to be possible with classical computers. The development and analysis of patterns of computation carried out by quantum computers is a field known as quantum algorithms, and the most well-known quantum algorithms – Shor’s algorithm and Grover's algorithm – are used to quickly factor numbers and speed up searches, respectively. These algorithms consequently threaten many widely used cryptosystems that base their security on the premises that certain computational problems are difficult to solve. Quantum computers, employing quantum algorithms, can solve these classes of problems quickly enough to jeopardize the security of the information that is encrypted. Current public-key cryptography relies on the assumption that some problems take an extremely long time to solve - and consequently, that it would take a very long time for their messages to be decrypted - but the speed with which quantum algorithms can solve some of these problems severely challenges that assumption.

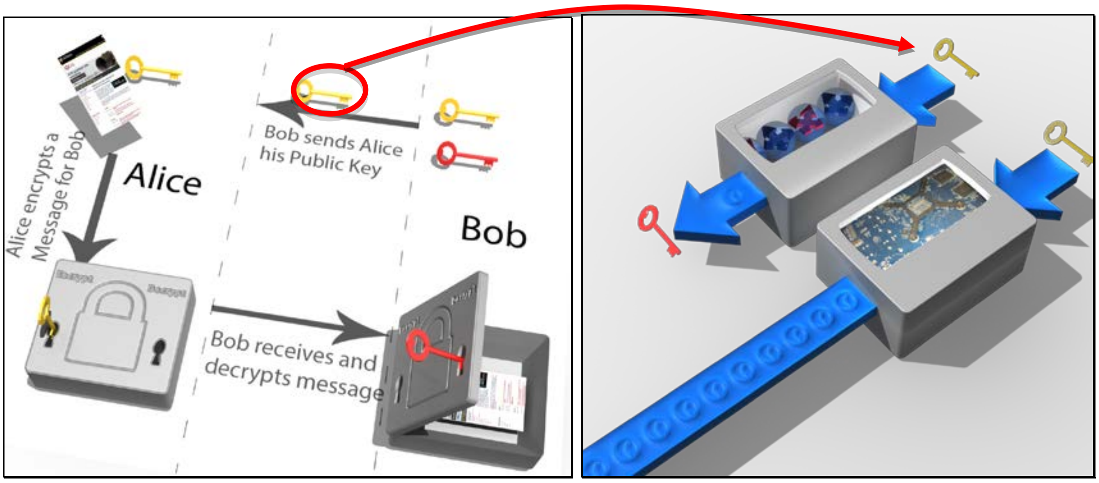
In practice, there are a number of physical systems that realize different implementations of quantum computers. Some common systems are nuclear spins, superconducting qubits, ion traps, and optical cavity quantum electrodynamics. Each research direction is at a different level of maturity, with some being stronger contenders than others for large-scale quantum computing.

2.3 How does quantum computing impact cryptography and security?

Cryptography plays a very important role in most secure electronic communication systems today because it ensures that only authentic parties can read each other’s exchanged messages. Quantum computing threatens the basic goal of secure, authentic communication because in being able to do certain kinds of computations that conventional computers can not, cryptographic keys can be broken quickly by a quantum computer and this allows an eavesdropper to listen into private communications and pretend to be someone whom they are not. Quantum computers accomplish this by quickly reverse calculating or guessing secret cryptographic keys, a task that is considered very hard and improbable for a conventional computer.

A quantum computer cannot break all types of cryptographic keys and some cryptographic algorithms in use today are also safe to use in a world of widespread quantum computing. The following sections will describe which types of cryptography are safe from quantum attacks and which ciphers, protocols and security systems are most vulnerable.

Figure 3 - Cryptography Basics - Effect of a quantum attack.


Alice encrypts a Message for Bob
Alice
Bob sends Alice his Public Key
Bob
Bob receives and decrypts message

A – Eavesdropper obtains public key from public channel

B – Quantum computer can break security by reverse computing private key faster than a conventional computer

2.4 Why is quantum safety an important issue?

Information in many ways equates to geopolitical, social, and economic power. The economic, social, and political well-being of developed countries depends on integrity, confidentiality, and authenticity of sensitive data sent over networks. Corporations and governments have legal responsibilities to their investors, constituents, and customers to preserve the confidentiality of sensitive information. Whether this information consists of military communications, secret government documents, industrial trade secrets, or financial and medical records, interception of information allows adversaries to not only learn about the contents of these communications, but also to discover metadata in patterns within a network of communicators, to extract general patterns using machine learning, and even to insert false or misleading information or malware into a data stream.

Previously, communications and transactions were considered secure when encrypted using an unbroken cryptosystem as part of an otherwise rigorous information security framework. Quantum computing challenges this assumption, because it offers a new and powerful set of tools under which many of these cryptosystems may collapse. Many ciphersuites have already been demonstrated to be insecure in the presence of a quantum computer, including some of our most pervasive cryptosystems such as RSA and Elliptic Curve Cryptography. Any data that has been encrypted using many cryptosystems whose security was based on the computational intractability of the so-called “hard problems” of discrete log and integer factorization is under threat of both eavesdropping and attack by future adversaries in possession of quantum computers. Without quantum-safe encryption, everything transmitted over an observable network is vulnerable to such an adversary. These issues do not only impact data that may be encrypted in this manner in the future, but apply to the information that is currently stored in this manner, or has been transmitted over an observable channel in the past. Choosing to ignore quantum-safe cryptography and security before quantum computers are able to perform these functions leaves almost all of present and future data vulnerable to adversarial attack.

It is essential for industries with interest in keeping secret information safe from adversaries to be forward thinking in their approach to information security. This involves considering more than merely how soon a quantum computer may be built. It also means thinking about how long information needs to stay secure, and how long it will take to update the existing IT infrastructure to be quantum-safe. Specifically, it is necessary to consider:

x: "how many years we need our encryption to be secure"

y: "how many years it will take us to make our IT infrastructure quantum-safe"

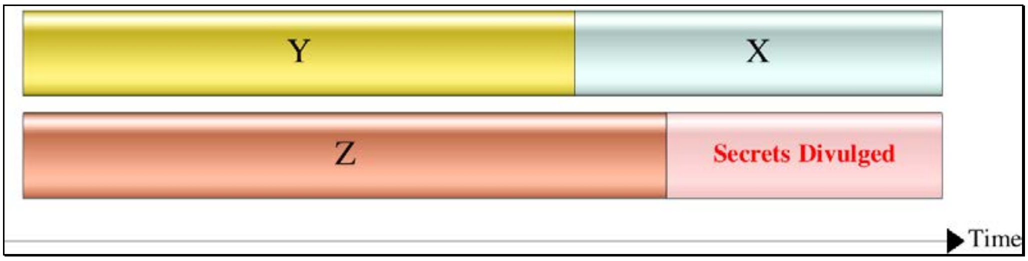
z: "how many years before a large-scale quantum computer will be built"

If a large-scale quantum computer (z) is built before the infrastructure has been re-tooled to be quantum-safe and the required duration of information-security has passed (x+y), then the encrypted information will not be secure, leaving it vulnerable to adversarial attack.

In real-world application, the value of *x* must be carefully considered, specifically: what are the practical consequences of a certain category of information becoming public knowledge after *x* number of years? For example, would it be a problem if your credit card numbers of today are made available to everyone in the world after *x = 5* years? Probably not, because it is very likely that you would have a new credit card issued, having a new expiry date and security code.

On the other hand, if personal identity information is made public after *x = 5* years, you may be exposed to identity theft and any resulting consequences. Indeed, one would also need to be cautious about defining the value of *x* in the case of certain other information categories such as top-secret military information, e.g. the orbits of secret military satellites, location of military bases and their resources and capabilities. Therefore, defining the value of *x* is a non-trivial matter, and requires a fair amount of thought, risk analysis and modeling. [Mosca13]

Figure 4 - Lead time required for quantum safety



2.5 What does quantum-safe mean?

Not all security protocols and cryptographic algorithms are vulnerable to quantum attacks; some are believed to be safe from quantum attacks, while some are known to be vulnerable. A security control that is believed to be quantum-safe today might - over time and with sufficient research - be shown to be vulnerable tomorrow. Without proof that an algorithm is vulnerable to a quantum attack, a cryptographic primitive and the protocols that use it are presumed to be quantum-safe if they are well studied and resists attacks using all known quantum algorithms.

Security controls that are known to be highly vulnerable to quantum attack, and can be easily broken by a quantum computer, include:

1) Any **cryptosystem** that is built on top of the mathematical complexities of Integer Factoring and Discrete Logarithms. This includes RSA, DSA, DH, ECDH, ECDSA and other variants of these ciphers. It is important to point out that almost all public key cryptography in fielded security products and protocols today use these types of ciphers.

2) Any **security protocols** that derive security from the above public key ciphers.

3) Any **products or security systems** that derive security from the above protocols.

Controls that are known to be somewhat vulnerable to quantum attack, but can be easily repaired include symmetric key algorithms like AES that can be broken faster by a quantum computer running Grover's algorithm than by a classical computer. However, a quantum computer can be made to work just as hard as a conventional computer by doubling the cipher's key length. This is to say that AES-128 is as difficult for a classical computer to break as AES-256 would be for a quantum computer.

AES is considered quantum-safe because the cipher can adapt to a quantum attack by increasing its key size to rectify a vulnerability introduced by quantum computing.

Ciphers like RSA and ECC are not quantum safe because they are not able to adapt by increasing their key sizes to outpace the rate of development of quantum computing. In order to attack a 3072-bit RSA key, for instance, a quantum computer must have a few thousand logical qubits. In general, the number of logical qubits needed scales in a linear fashion with the bit length of the RSA key. When such a quantum computer becomes available, moving to a larger RSA key size would thwart a quantum attack until a larger quantum computer is invented. However, doubling the size of an RSA or ECC key increases the running time of the cipher on a conventional computer by a factor of 8. That means that if the size of keys that a quantum computer can attack doubles every two years, then the running time of keys on a conventional computer increases by a factor of 8 every two years, outstripping Moore's Law and rapidly becoming impractical both in terms of speed and in terms of channel size, i.e. the required bandwidth to transmit the key information over an electronic medium.

Symmetric key ciphers like AES are believed to be quantum-safe, whereas many public key ciphers like RSA are known not to be. A protocol that relies exclusively on ciphers like RSA is vulnerable to quantum attack, but a protocol that can adapt to use quantum-safe ciphers is itself considered quantum-safe. In protocols and applications where public key cryptography is preferred over symmetric-key cryptography (usually, to overcome the difficulty of key distribution and key management problems), quantum safe cryptographic ciphers must be substituted in place of RSA or ECC in order to resist quantum attack.

Table 1 - Comparison of conventional and quantum security levels of some popular ciphers.

Algorithm	**Key Length**	**Effective Key Strength / Security Level**	
		Conventional Computing	**Quantum Computing**
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Note : Effective key strength for conventional computing derived from NIST SP 800-57 "Recommendation for Key Management"

3 Technology survey – current state of the art

Some of the most important people responsible for the ongoing strength of our security tools are the people who try to break them. At the network level this includes approaches such as penetration testing, or sometimes security research, and at the cryptography level it is called cryptanalysis. The researchers that perform this level of testing are exceptionally creative when it comes to circumventing security systems or compromising ciphers and it is directly because of their research and efforts that state-of-the-art tools and ciphers are constantly improved.

When the security of a software system, network implementation or end-user device needs to be fixed it is not uncommon to receive a software security update. This may come in the form of a software patch, a special system configuration, or an added security control. In the case of a broken cipher, there may be a standard parameter adjustment or a change to the algorithm implementation that is pushed out to products and buried deep in the software update.

Security research and cryptanalysis is a long practiced art form. The designers of security products are so accustomed to people trying to break their security systems that they build in redundant controls and layer these controls so that, over time, if a particular safeguard fails then the security of the system may still be recovered. With regards to cryptography, security architects will also design in recoverable security features, for instance, if a cipher is broken or discovered to be weak then the system can accommodate with a change in key size, parameter, or possibly even a new cipher or ciphersuite combination.

Many generic security protocols have some form of cryptographic agility, but in most cases, the only public key cryptography options designed into these protocols are variants of RSA or ECC, as well as Diffie-Hellman for key exchange, which from the perspective of quantum computing are not resilient against quantum attacks. Even if the protocols support other algorithms, RSA and ECC are the most widely deployed in practice. RSA and ECC are the most popular and pervasive public key cryptographic algorithms in use today due to their historical precedent as well as their efficiencies. RSA was the first practical public-key cryptosystem discovered and was built into early versions of the Secure Sockets Layer (SSL) protocol; ECC was the first algorithm discovered after RSA to offer considerably smaller keys and comparable-speed operations. Unfortunately, due to Shor's algorithms and the progressing maturity of quantum computing, ECC and RSA will become increasingly vulnerable to quantum attacks over time.

Changing from classical algorithms to quantum safe algorithms is not a simple task. It takes a long time for a particular algorithm to be accepted by security practitioners, researchers and standards bodies. Classical algorithms like ECC and RSA are widely studied and well accepted by the security community. Quantum safe algorithms have been around for a long time, but have not benefited from nearly as much public scrutiny and cryptanalysis, so they are less prevalent in standards and a difficult feature to find in security products.

3.1 Pervasiveness of RSA and ECC in security products

Classical public key algorithms like RSA and ECC are used pervasively in security protocols and applications to provide some of the following general security services:

Public Key Infrastructure typically this takes the form of a Certificate Authority (CA) where an entity that everyone implicitly trusts will attest that a particular cryptographic key belongs to a particular person or entity. Communication between two parties is assumed authentic because the trusted third party has previously confirmed each identity and issued each a certificate. For example, this is accomplished on the Internet where a WebTrust(c) accredited CA sends their self-signed root certificate to web browser makers to be embedded in the web browser software that is distributed to PC and mobile phone users. Companies that want to be trusted will purchase an SSL Certificate from a registrar that resolves to the root CA embedded in the browsers so that PC or mobile phone users who visit the company's website can be sure that they are not talking to an impostor. A secure lock icon is displayed to the web browser user, and the user may examine the details of the SSL certificate. As of 2014, almost all certificates issued by commercial CAs use RSA public keys of at least 2048 bits.

Secure Software Distribution is often achieved using public key based Digital Signatures where important information is digitally signed and the resulting signature is appended, transmitted and stored beside the original information and later used to authenticate. For example, software updates to a mobile handset's operating system will usually include a digital signature and before the mobile handset will install the software update, it will first verify that the update is authentic and was issued by the phone manufacturer and not an impostor. This ensures that the mobile handset may only run operating system software designed by the manufacturer that has not been tampered with prior to or during transmission. For example, Apple and Microsoft issue developers with code signing certificates containing RSA public keys.

Federated Authorization is a method of "single sign on" that allows a user of a website to enter their login credentials once, and be granted access to a number of other websites without divulging logon credentials to the other websites.

Key Exchange over a Public Channel is a common way to establish a secure connection where two individuals can use their public keys to exchange messages in public that allow them to agree on a private shared secret. Anyone who eavesdrops on the public messages cannot derive the shared secret, which is subsequently used to encrypt confidential messages. Key exchange, and key agreement protocols are used extensively in some of the most pervasive network security protocols like SSL/TLS, SSH and IKE/IPsec that protect private communications on the Internet. These protocols almost exclusively rely on key exchange using RSA, Diffie-Hellman, or elliptic curve cryptography.

Secure Email (i.e. S/MIME) is popular within government entities and regulated enterprises for exchanging confidential and authentic emails and is often a required feature by these high security organizations. Most S/MIME certificates contain RSA public keys.

Virtual Private Networks (i.e. IPsec) are used by enterprises to provide company network access, and work related application access, to its mobile workforce. VPNs are also commonly used by expats living in foreign countries with Internet restrictions, where the expat uses a VPN to create a network "tunnel" back to their native country, avoiding the visiting country's network filtering technologies. RSA and ECC are commonly used to setup the secure network tunnel using a key establishment protocol called IKE or mobileIKE.

Secure Web Browsing (SSL/TLS) is most commonly associated with the secure "lock" icon displayed on a web browser when visiting an SSL enabled website. Typically websites that accept credit card payments or deal with a user's private information will SSL enable their webpages due to regulatory requirements (i.e. Payment Card Industry compliance), or because their user base has been trained to only use websites that display the lock icon when asked to disclose their private information. . Almost all SSL/TLS certificates contain RSA keys for authentication. As of 2014, use of elliptic curve cryptography for key exchange is increasing but still not widespread.

3.2 Cryptographic primitives that are quantum safe

Most of the public key cryptography that is used on the Internet today is based on algorithms that are vulnerable to quantum attacks. These include public key algorithms such as RSA, ECC, Diffie-Hellman and DSA. All of these examples are easily broken by Shor's algorithms [Sho97] and are deemed to be insecure as quantum computing matures.

The reason Shor's algorithms break these public key cryptosystems is that they are based on two specific computational problems - namely, Integer factorization and discrete logarithm. These problems are believed to be hard for a classical computer to solve, but are known to be easily solved by a quantum computer. In order to sustain the security of the Internet and other technologies reliant on cryptography it is necessary to identify new mathematical techniques upon which cryptography can be built that are resilient against quantum attacks.

The main classes of computational problems that are currently believed to resist quantum algorithm attacks stem from the fields of lattice theory, coding theory and the study of multivariate quadratic polynomials. Each of these classes of computational problems offers new possible frameworks within which to build public key cryptography. The quantum safe ciphers that are built on these methods do admittedly present some challenges. Typically, they suffer from large key sizes and signature sizes when compared to popular, current public key algorithms that are not quantum safe. However, in terms of performance, some quantum-safe algorithms are competitive with – or even faster than – widely used public key algorithms such as RSA or ECC.

Some forms of symmetric-key cryptography are guaranteed to be quantum-safe. These primitives make no computational assumptions and are thus information-theoretically secure. An example of this is Vernam's One Time Pad, which has been proven to have perfect unconditional security against arbitrarily powerful eavesdroppers [SHA49]. Wegman-Carter Authentication [CW79] is also known to be resistant against quantum attacks [PER09].

There are also other types of symmetric key cryptography that are believed (but not proven) to be resilient against quantum attacks. For example, generic quantum search only provides a quadratic speedup over classical search [BEN97], indicating that quantum computers could not perform a brute force search to find symmetric keys much faster than could classical computers. Thus, unless the symmetric key algorithm happens to have a particular structure that can be exploited by a quantum computer, the bit security of a symmetric cipher can be retained in the presence of a quantum adversary by simply doubling the key length. Since quantum search does not provide exponential speedups, symmetric key encryption like AES is believed to be quantum-safe. Similarly, good hash functions are also believed to be resistant to quantum adversaries.

From these examples, it is clear that some forms of symmetric key cryptography are guaranteed to be an important example of secure cryptography in a post-quantum world. However, the need for establishing shared secret symmetric keys between communicating parties invites the challenge of how to securely distribute these keys. For key establishment, quantum-safe options include both computational and physics-based methods. These physics-based methods are collectively known as Quantum Key Distribution.

3.2.1 Quantum Key Distribution

While there are several symmetric key cryptographic tools that are either believed or known to be quantum-safe, establishing shared secret symmetric keys through an untrusted medium is traditionally accomplished with public key methods that are known to be vulnerable to quantum attacks, which is the main vulnerability of symmetric key schemes in the presence of a quantum computer. This opens up the question of how to securely distribute symmetric keys between distant parties, without relying on insecure legacy public key algorithms. One of the proposed solutions to the key distribution problem is known as Quantum Key Distribution (QKD).

There do exist alternative key distribution algorithms using public key schemes that are not RSA or ECC. However, in contrast to these public key schemes, QKD as a cryptographic primitive offers security that is guaranteed by the laws of physics. QKD as a method for secure key establishment [GIS02] is proven to be information theoretically secure against arbitrary attacks, including quantum attacks. This means that even assuming an adversary to have unlimited computational resources, including unlimited classical and quantum computing resources, QKD is secure now and always will be. By enabling provable security based on fundamental laws of quantum physics, QKD remains resilient even to future advances in cryptanalysis or in quantum computing.

Consequently, quantum key distribution provides the means to securely distribute secret keys that can be used with quantum safe symmetric key algorithms like Advanced Encryption Standard (AES), or one-time pad encryption.

Conceptually, the security of QKD is achieved by encoding information in quantum states of light. Using quantum states allows security to be based on fundamental laws in quantum physics and quantum information theory. There are three deeply related notions from quantum physics that illustrate the source of the unique security properties of QKD:

1. The Heisenberg uncertainty principle implies that by measuring an unknown quantum-mechanical state, it is physically changed. In the context of QKD, this means that an eavesdropper observing the data stream will physically change the values of some of the bits in a detectable way.

2. The no cloning theorem states that it is physically impossible to make a perfect copy of an unknown quantum state. This means that it is impossible for an adversary to make a copy of a bit in the data stream to only measure one of the copies in hopes of hiding their eavesdropping. (See ‘Prepare-and-measure QKD’ in section 3.2.1.3)

3. There exist properties of quantum entanglement that set fundamental limits on the information leaked to unauthorized third parties. (See ‘Entanglement-based QKD’ in section 3.2.1.3).

Importantly, these are not technological limitations that can be overcome by clever advances in engineering, but rather are fundamental and irrefutable laws of quantum physics.

Interestingly, due to the laws of quantum mechanics, it is physically impossible for an adversary to invisibly eavesdrop on quantum key distribution. Looking at the information encoded in quantum states actually changes the information in ways that can be detected by the legitimate parties. The mere act of her observing the data in transmission will physically change the bits of information in the data stream and introduce errors in ways that the sender and recipient can readily detect and quantify. The percentage of errors which an eavesdropper necessarily introduces allow the sender and recipient to calculate not only whether an eavesdropper was present, but also precisely how much of the information about the key the adversary could have gained in the worst possible case with the most powerful algorithms and hardware. This allows them to use well-studied post-processing methods to remove any information an eavesdropper could have gained about the shared key.

An important characteristic of quantum key distribution is that any attack (e.g. any attempt to exploit a flaw in an implementation of transmitters or receivers) must be carried out in real time. Contrary to classical cryptographic schemes, in QKD there is no way to save the information for later decryption by more powerful technologies. This greatly reduces the window of opportunity for performing an attack against QKD; the window is much wider for conventional cryptography.

The security of QKD has been proven in a number of frameworks including the universal composability [BHL05, Sca09], the abstract cryptography framework [MAU11], or the authenticated key exchange framework [MSU13]. The composability of QKD as a cryptographic primitive allows safely combining the distributed keys with other provably secure schemes such as Wegman-Carter authentication or onetime pad encryption while maintaining quantifiable long-term security.

3.2.1.1 How quantum key distribution works

Quantum key distribution is a process that uses an authenticated communication channel together with a quantum communication channel in order to establish a secret key. There are several different protocols for implementing quantum key distribution, all of which require both a quantum channel (to send quantum states of light), and an authenticated classical channel (for the sender, Alice, and the recipient, Bob, to compare certain measurements related to these quantum states and perform certain post-processing steps to distil a correct and secret key). The quantum channel uses optical fibres or free space/ satellite links to send photons (quantum states of light) between Alice and Bob, whereas the classical channel could be a simple (authenticated) telephone line that Alice and Bob use to talk to each other. Interestingly, both of these can be public. It is described in section 3.2.1 that the quantum channel necessarily shows Alice and Bob when an eavesdropper has been listening in, and it is a fact of the QKD protocols that the classical channel could be broadcast publicly without compromising security.

Quantum Key Distribution begins by Alice deciding to distribute some cryptographic key to Bob. Both Alice and Bob have the specialized optical equipment necessary for establishing the quantum channel, as well as access to a classical channel where they can communicate with one another. Alice uses a light source to send a stream of photons (quantum states) one-at-a-time. Each photon can be thought of as one bit of information. As each photon is sent, she randomly chooses to prepare it in one of two ‘’bases’’. Basis can be described as a perspective from which a photon is measured.

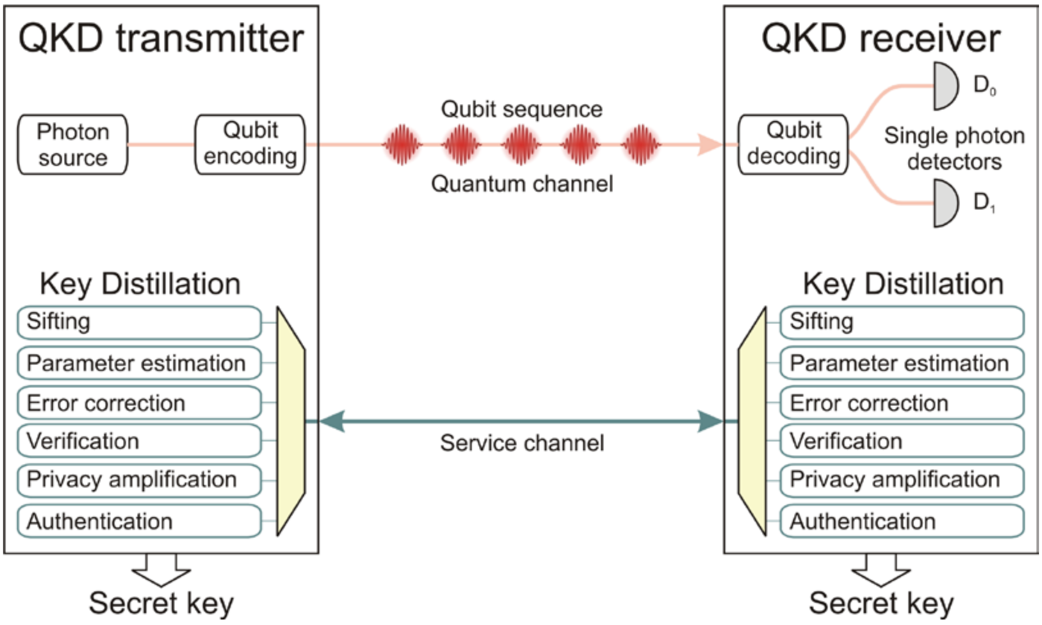


Figure 5 - Illustration of a typical prepare-and-measurement QKD setup.

As the recipient, Bob needs to record values for each photon he receives via the quantum channel. To do this, he must, like Alice, make a measurement of each one, and he therefore also chooses one of the two possible ‘’bases’’ and records which one he measured in. These choices are random and do not require any information about the bases that Alice chose when she was sending each bit. Afterward, Alice and Bob then communicate over the classical channel to compare which basis each bit was measured in at each end of the quantum channel. Sometimes Alice and Bob will randomly choose the same basis, and these are the bits for which they will get the same value for the photon (which is useful, so they will keep this bit as part of the key). When Alice and Bob measure the photon using different bases, they throw this bit away and do not use it in the final key.

After each bit has been sent and received, Alice and Bob can speak publicly about which basis they used to measure each photon, and this can provide enough information for each of them to generate key from the received quantum states, but not enough information for an adversary to reconstruct the key. Thus, an eavesdropper will not be able to discover the transmitted key for two important reasons. Firstly, the adversary cannot directly observe the photon without changing them, therefore being detected and having these bits discarded by Alice and Bob. Secondly, the adversary cannot indirectly observe the photon through observing the measurements of Alice and Bob, either, since Alice and Bob do not disclose the final measurement result for each quantum state. Rather, they only disclose which basis they used to measure it. By this time, it is too late for the adversary to measure the photon, because it has already been received by Bob, so knowing the basis that Alice used is not useful. It is well-established using information theoretic proofs that the measurement information is inadequate for an adversary to use to reconstruct the generated key.

3.2.1.2 Authenticating the QKD channel

An important methodological consideration in quantum key distribution is how to authenticate the classical communication channel to ensure that the two people communicating are actually Alice and Bob. The authenticated classical communication channel may be realized a few different ways.

The most secure method for authentication does not require any computational assumptions and uses a small amount of random secret data that is initially shared between Alice and Bob. Combining this form of authentication with QKD may be viewed as an expansion of the initial secret data without sacrificing randomness or secrecy. Subsequent communication using QKD normally uses part of the generated key material for authenticating subsequent QKD sessions, and part of the keying material for encryption.

If initially Alice and Bob do not share an authentication key, a natural alternative is to use public key signatures to authenticate their initial QKD session. Provided the public key signature is not broken during the QKD session, the resulting key is information theoretically secure and thus cannot be broken by future algorithmic advances, even if the public key signature is later broken [PPS07, IM11, MSU13]. Subsequent QKD sessions between Alice and Bob may be authenticated using a portion of previous QKD keys, so that they only need to rely on the short-term security of the public key signature once.

3.2.1.3 QKD protocols and their implementations

Several QKD protocols have been successfully implemented in academic and commercial research labs, transmitting keys over long distances through either optical fibres or free space. These protocols fall into two categories, and while theoretically identical in their analysis, are differentiated experimentally in part by how eavesdropping is detected:

1. **Prepare-and-measure QKD** allows legitimate parties to detect eavesdroppers by comparing the amount of error they might expect in their communications to the actual error of their measurements. This technique relies upon the fact that an adversary intercepting a quantum state must measure it, and in this adversary attempting to guess the original state to forward it to the recipient, they will introduce a percentage of identifiable error.

2. **Entanglement-based QKD** allows legitimate parties to detect eavesdroppers by virtue of the fact that if the sender and recipient each have a photon the two of which are related by quantum-mechanical entanglement - interception or measurement by an adversary will change the two-photon system in a way that the legitimate parties can readily detect.

One example of a QKD protocol is the BB84 protocol [BB84], which was the first protocol proposed for quantum key distribution and remains one of the most widely implemented protocols inside of commercial products and used within research labs. QKD based on the BB84 protocol has been demonstrated over distances over 100 km in length in both optical fibre and free space, reaching transmission speeds on the order of one megabit per second over shorter distances ([SMA07, LUC13]). Optical fibre based QKD products have already been commercially deployed and are in use today to distribute quantum safe keys in real networks.

The SARG protocol [SARG04] is similar to BB84 and has been used over a period of 21 months of continuous operation on the international SwissQuantum network [STU11].

More recent protocols which aim to have convenient implementations while still enabling long-distance and high transmission rate QKD are the Differential-Phase-Shift protocol [WAN12] and the Coherent OneWay protocol [STU09], which both have exceeded 250 km transmission distance in optical fibre.

There is also Continuous Variable QKD protocol that is the only QKD protocol that does not require single-photon detectors. This protocol relies upon homodyne detection and continuous encoding of quantum states [GRO02, QLI].

In addition to the above commonly used protocols, there is on-going research into protocols that aim to reduce the security assumptions of the actual implementation of the QKD devices. For example, the measurement device independent (MDI) QKD protocol allows for the complete removal of the single photon detectors and measurement devices from the security consideration [BHM96, Ina02, LCQ12]. That means that users of the QKD system do not need to trust the distributors of their measurement devices. Another possibility exists in the Ekert protocol [EKE91], which proposes the use of quantum entanglement to implement QKD with complete device-independent security. Once implemented, this would ultimately mean that trust assumptions of the QKD system implementation by a manufacturer could be reduced to a minimum.

Quantum key distribution penetration testing and security research (‘quantum hacking’) is an active area of academic and commercial work, and has identified some implementation specific vulnerabilities in QKD systems, leading to improved system designs.

3.2.1.4 QKD in networks

Quantum Key Distribution is intrinsically a point-to-point technology, but has been demonstrated in a routed network topology over multiuser optical fibre networks [SEC09, CHE10, STU11, SAS11] to secure data transmissions such as encrypted telephone communication and videoconferences throughout all nodes in a network. Therefore, the point-to-point nature of QKD can be implemented in such a way as to secure communications throughout a multiuser network. These networks are currently being explored through industrial and academic research into optical fibre networks. Additionally, current work on free space QKD links are also progressing toward the ultimate goal of using a satellite as a trusted node to enable free space quantum key distribution around the globe.

Optical fibre quantum key distribution can be implemented on existing optical infrastructures, but the quantum channel cannot pass through optical amplifiers. The maximum distance over which QKD photons can travel is limited because of the absorption of the signal that occurs over long distance transmission in optical fibre. Classical signals in the optical infrastructure use repeater nodes throughout the network to amplify and propagate the signal. However, due to the no cloning theorem of quantum information, there are challenges in developing a repeater system for a QKD network. The present solution to this problem is to concatenate multiple QKD systems to let keys propagate via intermediate nodes, which requires that the intermediate nodes must all be trusted to some extent.

While routing QKD using trusted nodes is one solution to the distance limitations and point-to-point nature of quantum key distribution, current research is exploring quantum repeater architectures that exploit something known as quantum entanglement in order to extend the range of QKD links beyond 400 km.

Another way of overcoming distance related challenges to implementing QKD is to send the signals through free space rather than optical fibre, as signals are diffracted less rapidly through the medium of air than they are through the medium of optical fibre. There is a trade-off with this approach; it is a more difficult engineering problem to protect against noise from atmospheric fluctuations. Several international research teams are currently working to develop satellites for use in quantum key distribution. These systems would have the benefit of not only being able to receive point-to-point signals over distances of a few hundred kilometres from the ground to low earth orbit [ELS12], but furthermore, a network of these satellites could act as trusted intermediary nodes capable of transmitting free space links all around the world. While this is an area of active research, satellite based quantum key distribution has yet to be demonstrated.

Current limitations of quantum key distribution, in general, are its higher costs for dedicated hardware, its transmission distance of a few hundred kilometres, and its key generation rate which decreases with increasing distance between sender and receiver. However, for specific applications for which strong security conditions must be met, QKD will likely become an increasingly attractive option in the upcoming years as research extends the distances over which quantum key distribution can be performed.

3.2.2 Code-based cryptosystems

Error correcting codes have played a prominent role in communication technology for a long time. They provide added redundancy to digital communications so that the receiver in real time can correct errors, which inevitably occur during transmission. An example of efficient error correcting codes are Goppa codes which can be turned into a secure coding scheme by keeping the encoding and decoding functions a secret, and to only publicly communicate a disguised encoding function that allows the mapping of a plaintext message to a scrambled set of code words. Only in possession of the secret decoding function can the secret mapping be removed in order to recover the plaintext. This technique is computational hard to reverse using either a conventional or quantum computer, it is based on a mathematical problem called syndrome decoding which is known to be an NP-complete problem if the number of errors is unbounded.

The notion of code-based cryptography was first introduced by an encryption scheme published by McEliece in 1978. The McEliece cryptosystem [McE78] builds on (binary) Goppa codes and its security is based on the syndrome decoding problem. It is known to be extremely fast in encryption and reasonably fast in decryption. The biggest drawback of this cryptosystem that prevents its practical adoption is the extremely large key sizes that are required.

In 2001, Courtois, Finiasz, and Sendrier [CFS01] proposed the first code-based signature scheme called CFS. CFS signatures are very short in length and are very fast to verify. However, CFS signatures suffer from the same extremely large key size drawback as the McEliece cryptosystem. In addition, the generation of signatures is highly inefficient. The security of the CFS signature is also based on the syndrome decoding problem. The fastest implementation of CFS can be found in [BCS13] and, on average, is roughly 100 times slower than signing with the RSA signature scheme.

A popular way to obtain signature schemes is by applying the Fiat-Shamir transformation on identification protocols. In this vein, the scheme by Stern [Stern94] and Cayrel et al [CVE10] can be transformed to a signature scheme outperforming CFS (see more details in [A+13]). Still, code-based signature schemes perform weakest among the quantum safe alternative primitives.

3.2.3 Lattice-based cryptosystems

Among all computational problems believed to be quantum safe, lattice-based problems have received the most attention during the past decade. Like code-based and multivariate-based algorithms, lattice-based algorithms are very fast and are considered quantum safe.

Lattice problems also benefit from something called worst-case to average-case reduction, which means that all keys are as hard to break in the easiest case as in the worst case when setting up any of the parameters of a lattice based cryptosystem. In a crypto system like RSA, generating keys involves picking two very large random numbers, that should be prime and should yield a hard instance of the factorization problem, but there is a certain degree of probability of choosing wrong and resulting in a weak security level. In lattice-based cryptography, all possible key selections are strong and hard to solve.

The core problem among all lattice problems, named Shortest Vector Problem (SVP), is to find the shortest non-zero vector within the lattice. This problem is NP-hard. And unlike the factorization problem nor the discrete log problem, there is no known quantum algorithm to solve SVP with the help of a quantum computer. In practice, cryptosystems are based on the assumption that the relaxed variants of this problem are still hard to solve. Among all the candidates, the following two deliver best performance and security:

1. NTRU: The NTRU cryptosystem was proposed by Hoffstein et al. [HPS98] as the first practical lattice-based cryptosystem. It is based on the assumptions that lattice problems are hard to solve within a specific family of lattices – the NTRU lattices. In 2011, Stehle and Steinfeld [SS11] proposed a variant of the NTRU encryption scheme, SS-NTRU, which had a reduction to problems over ideal lattices – a specific subgroup of lattices that includes NTRU lattices, though at the cost of reduced performance. The NTRU encryption scheme beats classical cryptography in performance but comes with larger pubic key sizes than RSA.

2. LWE: The Learning With Error (LWE) problem enables cryptosystems whose security can be reduced to lattice problems over general lattices. In [LP11], Lindner and Peikert have created a lattice-based cryptosystem called LP-LWE that is proven to be secure as long as worst-case instances of lattice problems are hard. In practice, usually the Ring Learning With Error (R-LWE) variant is used to boost efficiency. The R-LWE and SS-NTRU are reducible to a same lattice problem.

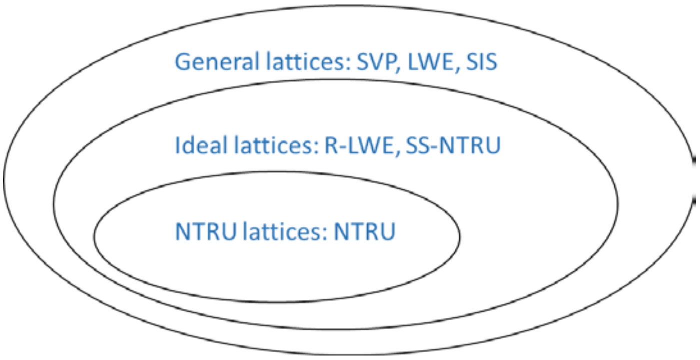

General lattices: SVP, LWE, SIS
Ideal lattices: R-LWE, SS-NTRU
NTRU lattices: NTRU

Figure 6 - Relationship of Lattice-based problems

In a series of work, Lyubashevsky et al. proposed lattice-based signature schemes based on short integer solution (SIS). The latest outcome is, called BLISS (Bimodal Lattice Signature Scheme) [DDLL13], is the currently most efficient signature scheme having approximately 0.6 KB public-key size and 0.25 KB private key size comparable in strength to AES-128. When compared to RSA-2048, BLISS is roughly 3-10 times faster at signing, and BLISS has similar speed improvements over RSA for verification. BLISS is basically a translation of discrete-logarithm-based Schnorr signatures [Sch91] to lattices with several optimizations with respect to distributions and efficient sampling from those. A very recent result improves BLISS further to enable an implementation of BLISS on embedded devices [PDG14].

As opposed to code-based and multivariate-based cryptography, there exists a couple of practical key exchange protocols based on lattice problems. A current matter of research is to implement those key exchange protocol into the TLS framework [BCNS14] and derive variants with additional entity authentication.

3.2.4 Hash based cryptosystems

Hash-based cryptography offers one-time signature schemes based on hash functions such as Lamport-Diffie or Winternitz signatures. The security of such one-time signature schemes relies solely on the collision-resistance of the chosen cryptographic hash function.

Since Winternitz and Lamport-Diffie signatures cannot be used more than once securely, they are combined with structures like binary trees so that instead of using a signing key for a single one-time use signature, a key may be used for a number of signatures limited and bounded by the size of the binary tree. The main concept behind using a binary tree with hash signature schemes is that each position on the tree is calculated to be the hash of the concatenation of their children nodes. Nodes are thus computed successively, with the root of the tree being the public key of the global signature scheme. The leaves of the tree are built from one-time signature verification keys.

This idea was introduced by Merkle in 1979 **[**Merkle79] and suffered a number of efficiency drawbacks such as large keys, large signature sizes and slow signature generation.

XMSS is a more current scheme and is in the process of becoming standardized[3]. It builds on Merkle Trees with the following improvements:

- More efficiency of the tree traversal, i.e. the computation of the path of nodes relating a given one-time signature to the root of the tree and the overall public key.
- Reduced private key sizes and forward secrecy through the use of a pseudo-random number generator for the creation of the one-time signature keys.

A significant strength of hash-based signature schemes is their flexibility as they can be used with any secure hashing function, and so if a flaw is discovered in a secure hashing function, a hash-based signature scheme just needs to switch to a new and secure hash function to remain effective.

An important drawback of Merkle-related schemes is their statefullness in that the signer must keep track of which one-time signature keys have already been used. This can be tricky in large-scale environments. Stateless variants are a matter of current research[4].

In terms of efficiency, successive iterations have greatly improved hash-based signature schemes, yet some drawbacks remain. For a comparable level of bit security, XMSS instantiated with AES-128 produces signatures over ten times larger than RSA-2048. Timings for signature and verification are comparable and additional improvements are expected in the future.

3.2.5 Multivariate cryptosystems

The most promising multivariate encryption scheme is currently the Simple Matrix (or ABC) encryption scheme [DPW14]. In this scheme, all computations are done over one finite field and the decryption process consists only of the solution of linear systems, which makes the scheme very efficient.

There are a number of other multivariate encryption schemes including PMI [Ding04] and ipHFE [DS05], however, these encryption systems tend to be inefficient because the decryption process includes some guessing, which is a required part of the algorithm that ensures its security.

Multivariate cryptosystems are public key based systems and can be used for digital signatures. The most promising signature schemes include UOV [Patarin96] and Rainbow [DS05, DYCCC05].

[3] http://gepris.dfg.de/gepris/projekt/251300380?language=en

[4] https://huelsing.files.wordpress.com/2013/04/20140710_sphincs_darmstadt.pdf

UOV and Rainbow are SingleField schemes, which means that all computations are performed over a single finite field. UOV has a large ratio between the number of variables and equations on the order of 3:1, which means that signatures are three times longer than hash values and the public key sizes are also large. Rainbow is more efficient; it is secure using smaller ratios, which has the impact of reducing digital signature and key sizes. Signature and key sizes can be further reduced for UOV and Rainbow [PBB10, SSH11] at the expense of increasing the time it takes to generate a key pair.

There also exist BigField schemes such as HFE (Hidden Field Equations) and pFLASH. A recent variant known as HFEv- is able to obtain secure signatures that are comparable in size to schemes like RSA and ECC. Another candidate BigField scheme is known as pFLASH [DDYCC08] which is a modified version of the C* scheme of Matsumoto and Imai.

3.3 Comparison: classical and quantum safe

The following tables compare the practical factors between public key cryptography schemes that are popular, but vulnerable to quantum attack, and quantum safe public key schemes that were introduced in prior sections above. The important factors being compared include key generation time, signing time, verification time, encryption time, and decryption time. The data represented in the tables is not benchmark data, but instead are values that are relative to an RSA signing operation where 1 unit of time is equivalent to producing an RSA signature using a 3072 bit private key.

Each quantum resistant cryptographic scheme may have multiple versions. Instead of using the specific acronyms, a more general name is used in the tables for each scheme and a reference is given that identifies the exact scheme.

The quantum safe encryption schemes used in the table comparisons include:

1. NTRU encryption scheme [HHHW09]
2. McEliece encryption scheme [NMBB12]
3. A variant of McEliece encryption scheme from Moderate Density Parity-Check (MDPC) codes and another from quasi-cyclic MDPC codes [MTSB12].

The time values are extrapolated from EBACS [EBACS] and the referred papers specifying the selected schemes. In addition to comparing the time taken to perform cryptographic operations, the key sizes of the public key and private key, and the size of the resulting the cipher text are shown. These comparisons all assume an equivalent effective symmetric key strength of 128 bits and are represented by the value k (i.e. k = a key that is as strong as a 128 bits of symmetric key). The time scaling and key scaling columns describe the rate at which operation time increases and the size of keys increase in order to increase the security level.

The following table comparisons are not exact and are intended for illustration only. Comparisons were composed from multiple referenced external sources and are not the result of tests conducted in the same controlled environment.

Table 2 - Comparison on encryption schemes (RSA decryption = 1, size in bits, k security strength)

Algorithm	*KeyGen (time compared to RSA decrypt)*	*Decryption (time compared to RSA decrypt)*	*Encryption (time compared to RSA decrypt)*	*PubKey (key size in bits to achieve 128 bits of security)*	*PrivateKey (key size in bits to achieve 128 bits of security*	*Cipher text (size of resulting cipher text)*	*Time Scaling*	*Key Scaling*
NTRU	*5*	*0.05*	*0.05*	*4939*	*1398*	*4939*	k^2	*k*
McEliece	*2*	*0.5*	*0.01*	*1537536*	*64861*	*2860*	k^2	k^2
Quasi-Cyclic MDPC McEliece	*5*	*0.5*	*0.1*	*9857*	*19714*	*19714*	k^2	*k*
RSA	*50*	*1*	*0.01*	*3072*	*24,576*	*3072*	k^6	k^3
DH	*0.2*	*0.2*	*0.2*	*3072*	*3238*	*3072*	k^4	k^3
ECDH	*0.05*	*0.05*	*0.05*	*256*	*256*	*512*	k^2	*k*

Note: in key scaling, the factor log k is omitted.

The quantum safe digital signature schemes used in the following table comparisons include:

1. Hash tree based signature from [BDH11];
2. BLISS -Lattice based signature [DDLL13];
3. Rainbow signature (Multivariate) [PBB10].

Hash tree based signatures are unique in that their keys can only be used to produce a limited number of signatures. The maximum number of signatures for a hash tree scheme needs to be chosen at the time of key generation. For the purpose of comparisons below, hash tree scheme keys are set at a fixed 2^{20} signatures.

Table 3 - Comparison on signatures (RSA signing = 1, size in bits, k security strength)

Algorithm	Num of sign	Key Gen (time compared to RSA sign)	Signing (time compared to RSA sign)	Verifying (time compared to RSA sign)	PubKey (size in bits to achieve 128 bits of security)	PrivateKey (size in bits to achieve 128 bits of security	Signature (size in bits of resulting digital signature)	Time Scaling	Key Scaling
XMSS signatures (hash based)	2^{20}	100000	2	0.2	7296	152	19608	k^2	k^2
BLISS (lattice-based)		0.005	0.02	0.01	7000	2000	5600	k^2	k
Rainbow signature (multivariate)		20	0.02	0.02	842400	561352	264	k^3	k^3
RSA		50	1	0.01	3072	24,576	3072	k^6	k^3
DSA		0.2	0.2	0.2	3072	3328	3072	k^4	k^3
ECDSA		0.05	0.05	0.05	512	768	512	k^2	k

Note: in key scaling, the factor log k is omitted.

Currently, the actual implementation benchmarks for these quantum safe schemes are not generally available. The data on performance provided in Table 1 and Table 2 is based on estimations to obtain approximate scaling about the performance. In other words, the performance data should not be considered as a precise comparison. It is worth noting that QKD is a quantum-safe key agreement primitive, but it has not been included in the table, because the relevant parameters and performance figures are different from those of mathematics based cryptographic primitives.

Based on Table 1, the key pair generation of the selected quantum safe schemes are far better than RSA. But they are not as good as DH and ECDH. Therefore, using a one time key pair to achieve perfect forward secrecy is possible during a key establishment scheme, however, it will be slower than an ephemeral Diffie-Hellman key agreement.

For the selected digital signature schemes, XMSS has the asymmetry property of RSA, i.e. verifying is faster than signing. Likewise, for the selected encryption schemes, the McEliece variants also share the asymmetry property of RSA, i.e. encryption is faster than decryption.

The selected quantum safe schemes generally have performance comparable to or better than pre-quantum schemes of the same security level. However, key, message, and signature sizes are generally larger. In the cases of McEliece and Rainbow, key sizes are a lot larger. Also, quantum safe schemes have not been studied as thoroughly as the listed pre-quantum schemes.

4 Security protocols: potential for upgrade

Security protocols are designed with the most effective cryptographic tools available at the time, and if successfully adopted by the security community, these protocols tend to be long lived in products and networks. Designers of security protocols tend to anticipate that the security level of cryptography used in their protocols will degrade over time, and they will allow for corrections in the future by supporting changes to key sizes and cryptographic parameters. Protecting against quantum attacks may require more drastic changes than designers have historically anticipated. Cryptographic primitives may need to be replaced entirely, and protocol-level changes may be necessary to accommodate the new primitives. It can be a great challenge to insulate an established standard against quantum attacks because non-security issues such as adoption rates, backwards compatibility and performance characteristics must also be considered. Changing cryptographic systems in a standard can be done, however, the pace is slow and requires strong demand from the market.

The following sections explore the cryptographic agility that is currently built into some of today's most widely used security protocols. Each protocol's tolerance for accommodating quantum-safe controls is evaluated and recommendations are made outlining a migration path to a quantum safe security posture. In some cases this can be achieved using existing cryptographic agility features that are already built into the protocol, but unfortunately some protocols are too rigid and require fundamental messaging and data structure changes to safeguard them from quantum threats.

4.1 X.509 certificates

Many applications involving public key cryptography rely on certificates – these are cryptographically signed documents, often issued by a trusted third party or certificate authority (CA), who attests to the ownership of a particular public key by a particular entity. A certificate includes information identifying its owner, a public key for the owner, a validity period, and a signature binding this information together and certifying its authenticity. Certificates are often chained together, enabling one CA to certify all of the certificates of another CA.

The X.509 standard specifies a common format for public key certificates, mechanisms for managing and revoking certificates, a set of valid attributes of certificates, and an algorithm for validating the certificates. X.509 is not a protocol but rather a suite of data formats and algorithms that collectively constitute a public key infrastructure (PKI).

X.509 certificates play a central role in the use of SSL/TLS on the Internet, as servers are authenticated to clients using X.509v3 certificates. Every web server supporting TLS must have a certificate, the vast majority of which are issued by one of the several hundred commercial CAs that are recognized by major web browsers. X.509v3 certificates are also used in other contexts, including secure email (S/MIME), web services (XML Digital Signatures), and code signing.

4.1.1 Analysis of current algorithms

The X.509v3 standard allows for algorithm agility in that an ASN.1 Object Identifier (OID) defines the formats of public keys. The OID scheme is highly extensible and any organization holding an OID can issue further OIDs within their hierarchy and so new ciphers can be defined by any organization that participates in the OID hierarchy.

Adding a new cipher OID is the first step needed to extend X.509, but what is also needed is for software that reads X.509 certificates to be able to comprehend the new OID and be able to process the X.509 signatures according to the new cipher definition.

The vast majority of certificates issued by commercial CAs contain RSA public keys, and a small number of CAs are starting to issue certificates containing elliptic curve public keys. Similarly most certificates on the internet today are signed with an RSA key. There are currently no CAs issuing certificates for quantum-safe public keys, and no CAs signing their certificates with a quantum-safe signature algorithm.

Regardless, the X.509 certificate structure is extensible and can be made to support quantum-safe algorithms with relative ease.

4.1.2 Recommendations for quantum-safe X.509 certificates

Using quantum-safe algorithms and public keys in X.509 certificates does not require a change to the standard; it simply requires OIDs to be created for quantum-safe algorithms, something that can easily be done by any organization already holding an OID. However, X.509 is a standard that is used in many other standards that would require an update to support the newly defined quantum-safe algorithm identifiers. For example, TLS would require new ciphersuites to be introduced.

The importance of using quantum-safe X.509 certificates now depends on the application in which they are used.

- Some X.509 certificates are relatively short-lived. For example, the certificates used to authenticate websites using TLS typically have validity periods between 1 and 5 years and will expire before quantum computers are available. Using a quantum computer to break authentication after the validity period would have no impact on current TLS sessions.

- Some X.509 certificates are longer-lived. For example, certificates that are used for signing legal documents may need to have validity for decades. As a result, applications requiring long-term security from X.509 certificates should place higher priority on migrating to quantum-safe algorithms in X.509 certificates due to higher likelihood of exposure to quantum threats in the future.

In practice, adoption of new algorithms in X.509 certificates is constrained by choices of major software developers as well as commercial CAs. Deployment of new algorithms is generally slow.

4.1.3 Technical concerns

The X.509 data format allows for very long public keys and signatures, so post-quantum schemes with large public keys should not be problematic for X.509 certificates directly. However, some applications may put size limits on X.509 fields, not anticipating future cipher changes.

4.1.4 QKD and X.509 certificates

QKD when used in combination with a quantum safe public key algorithm could make use of X.509 certificates to authenticate the service channel that is required by a QKD system during the key distillation phase of the QKD protocol.

4.2 Internet key exchange version 2 (IKEv2)

Internet Key Exchange (IKEv2) is a protocol used to establish keys and security associations (SAs) for the purpose of setting up a secure Virtual Private Network (VPN) connection that protects network packets from being read or intercepted over a public Internet connection. This allows a remote computer on a public network to access resources and benefit from the security of a private closed network without compromising security.

The IKE protocol standard is rigid and does not permit VPN designers to choose beyond a small set of cryptographic algorithms. At present, none of the permitted algorithms are completely quantum safe.

4.2.1 Analysis

In a typical IKE protocol three exchanges are used to setup a Security Association. In the first exchange, a common key is derived using the Diffie-Hellman key agreement algorithm. This common key is authenticated in a second exchange using either certified digital signatures, or a pre-shared authentication key. In the third exchange, Diffie-Hellman key agreement is conducted again to generate new ephemeral keys for encrypting or authenticating IP packets, these keys makeup a Security Association.

There is no alternative to Diffie-Hellman for key agreement specified in the standard. Since Diffie-Hellman is not a quantum safe algorithm, it would need to be replaced in order for IKE to be secure against quantum attacks. Of the authentication methods given, only the pre-shared key option may be considered quantum-safe.

As currently deployed, IKE session establishment data and the subsequent VPN traffic is vulnerable to being captured, stored in an encrypted state, and later decrypted when quantum computing is available.

4.2.2 Important security aspects of IKE

IKE offers very useful security properties that would need to be maintained if cryptographic agility were introduced to the standard. IKE security associations are built on the concept of Perfect Forward Secrecy (PFS); in conventional security terms this means that ephemeral, one-time-use, keys are created for every new secure connection. This ensures that the compromise of a long-term key does not affect the confidentially of sessions established prior to the compromise. Furthermore, the compromise of an ephemeral key does not affect the confidentially of sessions in which that key was not used.

IKE also provides authenticated connections, using RSA, DSS or MAC with a pre-shared secret. While the MAC option with proper key and MAC tag length justification is quantum safe, RSA and DSS algorithms are not. Simply specifying the use of a MAC with pre-shared secret is not an adequate substitute for a public key based algorithms because a large network with individual pre shared secrets for every connection does not scale well and quickly becomes a key management problem as the network grows. Pre-shared keys are also problematic in a large network because, if a global key is being used it is very hard to keep such a global key a secret, representing a vulnerability with a single point of failure.

4.2.3 Recommendations for quantum safe IKE

Any option to make IKE quantum safe would require a change to the standard. Specifically, these changes would include:

- A replacement algorithm for the first and third exchanges, for instance, a quantum-safe alternative to Diffie-Hellman key agreement that maintains PFS. Note that there is not a well studied alternative, however, university level research is occurring and has resulted in some proposals from the academic community. These proposals should be reviewed and evaluated by standards bodies as potential avenues to create a quantum safe IKE that maintains desirable PFS security features.

- A replacement algorithm for the second exchange, public key based, authentication schemes for setting up a security association. Currently these are based on RSA and DSS, a quantum safe algorithm should also be specified as an option giving an alternative to the logistics problems associated with MAC using pre-shared secrets.

4.2.4 On the use of QKD in IKE

QKD may be used as a replacement for Diffie-Hellman key agreement to establish the shared secret for an IKE SA with perfect forward security. Together with a quantum-resistant authentication algorithm this would enable IKE to negotiate quantum safe symmetric keys. The shared secrets provided by QKD may either be used with conventional encryption ciphers, or for one-time pad encryption in high security applications.

QKD may also be used for the second pass to solve the key management problem of distributing shared secret keys for message authentication. Instead of calculating shared secrets and computing secret keys, QKD keys could be used to protect integrity.

4.3 Transport layer security (TLS) version 1.2

The Transport Layer Security (TLS) protocol, earlier versions of which were called the Secure Sockets Layer (SSL) protocol, establishes a protected tunnel between a client and server for transmission of application data. The handshake sub-protocol is used to perform server-to-client and optional client-to-server authentication, and to establish shared secret keys. Shared secrets are subsequently used in the record layer sub-protocol to encrypt and authenticate application data.

TLS is used to secure a variety of applications, including web traffic (the HTTP protocol), file transfer (FTP), and mail transport (SMTP). The design of TLS is largely independent of cryptographic algorithms, and allows for parties to negotiate ciphersuites (combinations of cryptographic algorithms to use). As of TLSv1.2, all cryptographic components (public key authentication, key exchange, hash functions, bulk encryption) can be negotiated, although generally all must be negotiated at once in a single ciphersuite rather than independently.

Certain ciphersuite selections like Ephemeral Diffie-Hellman allow for perfect forward secrecy.

4.3.1 Analysis of current TLS ciphersuites

The handshake sub-protocol is used to perform authentication and establish shared secret keys. In almost all cases, these operations involve public key operations.

Currently, the majority of servers are authenticated using X.509 certificates containing RSA public keys, and thus cannot be considered quantum safe.

Public key operations are also used to establish shared secret keys, which are then used for encryption in the record layer sub-protocol. There are two main types of key exchange used in the TLS handshake sub-protocol:

1. RSA key transport: The client picks a random secret key, encrypts it using the server's RSA public key, and sends the ciphertext to the server, who decrypts the secret key. Notably, this scheme does not offer perfect

forward secrecy, meaning compromise of the server's long-term key leads to the immediate compromise of all sessions, past and future, established with that key.

2. Ephemeral Diffie–Hellman key agreement: The client and server generate ephemeral Diffie–Hellman public keys, which they exchange and use to generate a shared secret key. Their ephemeral Diffie–Hellman public keys are authenticated using digital signatures based on certificates. This scheme does offer perfect forward secrecy, meaning compromise of the server's long-term key does not help in computing the shared secret session keys. TLS includes ciphersuites utilizing both traditional Diffie-Hellman and Elliptic Curve Diffie-Hellman. Neither variant is quantum-safe.

The remaining operations in the TLS protocol involve symmetric primitives, such as hash functions, message authentication codes, and block or stream ciphers. In general, quantum computers have less of an effect on such primitives: Shor's algorithm does not apply, so exponential speedups are not expected. Grover's search algorithm would allow quantum computers a quadratic speedup in brute force search, which means that the primitives need to double the key length to maintain the same level of security against a quantum computer.

4.3.2 Recommendations for quantum-safe TLS

Any option to make TLS quantum-safe would require a change to the standards. New ciphersuites can be proposed and standardized by a Request for Comments (RFC).

The following two-stage approach can be used to introduce quantum-safe cryptography into TLS:

1. A quantum-safe key exchange mechanism with perfect forward secrecy replaces existing key exchange mechanisms. To ease adoption, non-quantum-safe digital signatures, such as RSA, can continue to be used to provide authentication. Quantum-safe ciphersuites should match the security estimates of their symmetric primitives to the security estimates of their public key primitives. As an example, a ciphersuite utilizing a quantum-safe public key algorithm at the 128-bit security level should use symmetric primitives at the 256-bit level to account for the impact of quantum search attacks.

2. Quantum-safe digital signatures are deployed in certificates and used for authentication of the purely quantum-safe key exchange mechanism introduced in stage 1.

The use of a quantum-safe key exchange mechanism with non-quantum-safe digital signatures is suitable in the short term: future quantum computers will still not be able to decrypt the messages encrypted using the key from the quantum-safe key exchange mechanism.

In the short term, it may also be appropriate to consider a “hybrid” key exchange mechanism, which employs both quantum-safe key exchange and non-quantum-safe exchange (such as elliptic curve Diffie–Hellman). A hybrid approach, securely implemented, allows early adopters to have the potential of quantum-safe cryptography without abandoning the security offered by existing mechanisms at present, while maintaining with existing regulations such as FIPS.

These replacements are currently at the stage of "university-level" research. Various academic groups have proposed a variety of key exchange protocols based on quantum-safe primitives [FSXY13,SecInn13,Pei14], and early implementation results indicate that performance of quantum-safe key exchange in TLS can be competitive with elliptic curve ciphersuites [SecInn13,BCNS14].

4.3.3 Technical concerns

Quantum-safe algorithms with large public keys or signatures may require additional changes to the standard. At present, TLS record layer fragments can be at most 2^{14} B = 16 KB long, though messages can be split across multiple fragments, certificates can be at most 2^{24} B = 16 MB; these sizes could be increased in a future version of TLS.

4.3.4 On the use of QKD in TLS

TLS currently supports ciphersuites where the parties use a pre-shared key (PSK) for encryption, and perform key confirmation for authentication [RFC4279, RFC5487]. Some of these PSK ciphersuites use solely symmetric key operations such as AES-256 for encryption and HMAC-SHA384 for message integrity and authentication. This seems a suitable mechanism for incorporating key material established from a quantum key distribution channel into TLS, as it would allow parties to achieve a high level of computational security from a relatively short QKD key. An alternative mechanism would have to be developed to incorporate QKD keys directly into the TLS standard if information-theoretic security were desired. It would be possible, for instance, to define ciphersuites which make use of a long QKD key for one-time pad for encryption and a short pre-shared key for Wegman-Carter MAC based authentication.

4.4 S/MIME

Secure/Multipurpose Internet Mail Extension [RFC2311, RFC2312, RFC2632, RFC2633, RFC2634, RFC5751] is a standard for digital signatures and public-key encryption used to securely send email messages. It offers origin authentication non-repudiation, data integrity, and confidentiality through use of digital signatures and message encryption. This standard is widely adopted throughout government and enterprise. S/MIME, and a similar scheme called OpenPGP, allow email to remain encrypted during the entire path from sender to recipient, meaning that at the email servers of both the sender and receiver, as well as the links between sender, sender's email server, recipient's email server, and receiver, the plaintext cannot be read or modified by an adversary. This contrasts with other protocols like SMTP-over TLS and IMAP/POP3-over-TLS which are used to secure the individual links between intermediate mail servers, but do not preserve end-to-end confidentiality and data integrity.

By far the strongest alternative to S/MIME for preserving end-to-end security is OpenPGP. They are very similar at a protocol level, but OpenPGP relies on a Web of Trust, while S/MIME uses Certificate Authorities and Public Key Infrastructure (PKI) to overcome key distribution issues that seriously hinder the usability of OpenPGP. For usability reasons, S/MIME continues to be a preferred choice within large enterprise email environments. S/MIME requires recipients to publish a public key signed by a certificate authority. As is usual within a PKI, this allows users with a signed public key to be authenticated and enables secure emails from the first instance of communication.

4.4.1 Analysis of current algorithms in S/MIME version 3.2

In the S/MIME protocol, digital signatures are used for authentication, data integrity guarantees, and non-repudiation of origin. Within version 3.2, a digital signature or certificate is required. Digital signatures within version 3.2 require the use of asymmetric keys of at least 1024 bits for the generation and verification of key pairs, using one of the following algorithms: DSA (with SHA-256), RSA (with SHA-256), or RSA-PSS (with SHA-256). While the hash algorithms selected are quantum-safe, the use of DSA or RSA(-PSS) provides inadequate security in the presence of a quantum computer, and therefore requires replacement in all implementations of S/MIME. Similarly, the allowed public key encryption primitives are based on either RSA, or Diffie-Hellman. Neither of these primitives are quantum-safe.

Content encryption itself in S/MIME relies upon symmetric ciphers like AES that are believed to be quantum-safe. Unfortunately, the aforementioned key establishment algorithms for these symmetric keys – in addition to the algorithms used for digital signatures – are insecure in a post-quantum environment. It is important to note, however, that S/MIME supports extended key size and encryption methods of the sender's choice, offering the potential for security engineers to upgrade signature and key-establishment algorithms, to ensure respectively, data/origin authentication and integrity, as well as message security.

4.4.2 Recommendations for quantum-safe S/MIME

S/MIME relies on uses of MIME (Multipurpose Internet Mail Extension) wrapped around content produced in Cryptographic Message Syntax (CMS), which is data-protection encapsulation syntax [RFC5652]. Consequently, many of its security properties rely on the parameters of CMS. Fortunately, CMS offers a variety of customizable parameters, including algorithm selection. This means that the protocol has the potential to transition to quantum-safe cryptography. The SMIME Capabilities attribute (which includes algorithms for signatures, content encryption, and key encryption) was designed to be flexible and extensible so that other capabilities added later would not break earlier clients. However some very early versions of S/MIME may present backward-compatibility issues. Requirements and recommendations are in the CMS Request for Comments to ensure a basic level of interoperability between S/MIME implementations. Since some clashes between versions seem unavoidable, it is highly recommended that users be warned of instances when the use of S/MIME relies only upon weak cryptography. There currently exists a parameter within S/MIME where an agent can state whether or not to allow the use of weak encryption (currently defined as use of 40 bit keys), which overrides all specific algorithm preferences of that user. It would be valuable to update this parameter to define 'weak' as any cryptographic primitive that is not quantum-safe at any point in the protocol.

4.4.3 Technical concerns

The primary technical challenge of this implementation will be the backward compatibility with clients of versions 3.1 or earlier that may use cryptographic primitives that are not quantum safe. For example, some implementations of S/MIME from earlier versions may only include RSA. This may instead present difficulty to one party trying to communicate securely with another party, who might then be forced to communicate using weak encryption. Furthermore, some implementations based on S/MIME version 3.1 or earlier may lack cryptographic agility due to reduced available key sizes, and therefore security architects must be mindful of backwards compatibility with respect to key length when selecting quantum-safe cryptographic primitives to substitute into existing frameworks.

4.5 Secure shell (SSH) version 2

SSH (Secure Shell) version 2 [RFC4250, RFC4251, RFC4252, RFC4253, RFC4254] is a cryptographic network protocol used to encrypt information sent over an insecure network such as the Internet. In essence, it relies on a client-server model to allow a user on one computer to remotely log-in, send commands, and transfer files on another computer, without compromise of data integrity or confidentiality. It has a wide range of uses, with some implementations of SSH (namely OpenSSH) enabling users to create fully encrypted Virtual Private Networks (VPNs). This allows users to treat a public network such as the Internet as if it were a more secure, private network.

Secure Shell (SSH) is a secure remote-login protocol. It has pervasive and diverse applications, and can be used for a variety of purposes, including the construction of cost-effective secure Wide Local Area Networks (WLAN), secure connectivity for cloud-based services, and essentially any other enterprise process that requires secure access to a server from a remote client.

4.5.1 Analysis of current algorithms

The SSH protocol involves three major sub-protocols [RFC4251]: the Transport Layer Protocol, the User Authentication Protocol, and the Connection Protocol. Each uses its own set of algorithms to perform specific functions at different network layers.

The Transport Layer Protocol [RFC4253] creates the secure channel used for server (host) authentication, and ensures the confidentiality and integrity of data sent over an insecure network. It runs over top of TCP/IP. The generation of a unique session ID occurs within this protocol. Within this protocol, several parameters are negotiated between server and client, including symmetric encryption algorithms, message authentication algorithms, and hash algorithms – all of which are quantum-safe. However, much like S/MIME, the methods of key exchange and public key authentication rely upon algorithms that are insecure in the presence of quantum adversaries. Specifically, the current standardized key exchange algorithms each rely on some form of the Diffie-Hellman protocol, and the standardized authentication algorithms are all based on RSA, DSA, or ECDSA. None of these primitives are quantum-safe.

The User Authentication Protocol [RFC4252] authenticates the client to the server, using the Transport Layer Protocol's session ID. Its security/integrity properties are dependent upon those defined within the initial algorithm negotiation of the Transport Layer Protocol.

Similarly, the Connection Protocol [RFC4254] takes the encrypted tunnel generated by the Transport Layer protocol and multiplexes it into several channels for actions such as shell/login access, proxy forwarding of external protocols and TCP/IP or X11 connections through the secure tunnel, and accessing the server host's secure subsystems. It runs on top of both the Transport Layer Protocol and the User Authentication Protocol. Its security/integrity properties are dependent upon those defined within the initial algorithm negotiation of the Transport Layer Protocol.

4.5.2 Recommendations for quantum-safe SSH

The SSH protocol was specified with a high level of cryptographic agility and allows servers and clients to negotiate the algorithms used for encryption, data integrity, authentication and key exchange. The addition of quantum-safe controls will not require significant changes to the base SSH protocol. It is integral that all versions of SSH include quantum-safe algorithms for all parameters in the Transport Layer Protocol, since the SSH Transport Layer Protocol looks for the first algorithm that both server and client will support for key exchange. Should one of these parties fail to have a quantum-safe algorithm available, the tunnel becomes insecure for both parties – not only at the Transport level, but also for the dependent User Authentication and Connection layers. The following recommendations are suggested at the level of the Transport Layer Protocol:

- Use of the Diffie-Hellman (DH) key exchange must be replaced by use of a quantum-safe algorithm that offers fast key-pair generation and perfect forward secrecy.

- Use of the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the RSA Signature Algorithm (RSA-SSA) for host authentication must be replaced by use of quantum-safe authentication mechanisms such as quantum-safe digital signatures or message authentication codes based on pre-shared symmetric keys.

- It may be in the best interest of users for standards organizations to solicit and distribute an updated specification for SSH that adds quantum-safe algorithms to the list “required” algorithms within each of the protocol-specification documents for SSH.

4.5.3 Technical concerns for SSH

There also exists a possibility, even with a quantum-safe suite of algorithms in the SSH protocol, that via SSH proxy forwarding of other protocols (SMTP, HTTP, etc) may compromise machines when versions of these external protocols that are not quantum-safe are used. The security properties of SSH are not transitive to the security properties of proxied protocols, which illustrate the importance of comprehensive and cohesive adoption of quantum-safe cryptography. Not only can weak cryptography compromise an otherwise secure network security protocol, but additionally, compromised protocols themselves can further jeopardize machines within the network when integrated with other protocols that are quantum-resistant.

4.5.4 On the use of QKD in the context of SSH

Quantum Key Distribution appears to be a viable method for secret key generation within the SSH protocol. The use of QKD would bypass issues related to the presently unsafe methods of secret key exchange, and could potentially replace the current key-establishment methods for symmetric (AES) keys.

The major concern is the rate of key generation for QKD, which depends largely on the distance travelled – regardless of whether the implementation occurs through optical fiber or free space. Since current SSH security parameters suggest that keys should be changed after every gigabyte of transmitted data [RFC4253], the specific key rate of a specific implementation of QKD will likely determine whether key material can be generated sufficiently quickly for real-time use.

5 Fields of Application and Use Cases

The impending realization of scalable quantum computing will have damaging and pervasive effects for governments, enterprises, and individuals, who are caught relying on products and protocols that are not using quantum-safe cryptography. The following section describes some fields that may be particularly vulnerable to quantum attacks.

Broadly speaking, there are two states of data under which it is vulnerable: in transmission, and at rest.

Each of these presents its own needs and challenges for encryption. For instance, encrypting data while it is in transit over the Internet, point-to-point leased lines, or even an internal network has a different set of considerations than encrypting data at rest, which may include protecting large cloud databases, PCs, smartphones and other end-user devices.

The following section broadly highlights some use cases where technological infrastructures appear particularly vulnerable to an adversary with a quantum computer. Subsequently, some major industries are highlighted where these use cases are likely to arise.

5.1 Use Cases

5.1.1 Encryption and authentication of endpoint devices

Endpoint devices include any piece of hardware that a user utilizes to interact with a distributed computing system or network. This can include canonical examples such as personal computers and mobile phones, as well as kiosks/terminals in banks, stores, and airports, as well as any kind of embedded technology connected to a broader network. Encryption of endpoint devices refers to the practice of making the contents of the device unreadable to unauthorized parties through the use of cryptography and security protocols. This is an important practice to prevent unauthorized data transfer and access, to ensure that only approved devices are allowed access to the system, and to deal appropriately with rogue or compromised devices that threaten system security through intrusions such as malware, key loggers, or viruses.

Quantum computing presents several potential threats to the security of endpoint devices. Even if an endpoint device's contents are completely encrypted through the use of full-disk encryption, they may still be vulnerable to decryption by an adversary employing quantum algorithms, depending on the algorithms used for the initial encryption of the device. Software implementations of disk encryption rely on symmetric key cryptography, which is generally considered quantum safe. However, the vulnerability in this design is that key generation relies on existing asymmetric key signature and key establishment protocols such as DSA (for AES), RSA (for Triple-DES) or ECDSA, none of which are quantum-safe. This means that it is conceivable that even fully encrypted endpoint devices are vulnerable to adversarial decryption. This results in a number of potential vulnerabilities:

- If an adversary were able to hijack an authenticated endpoint device, they will have access to the same ports, devices, networks, and classes of information as the intended enterprise user. This could conceivably enable certificate hijacking and the installation or execution of unauthorized rootkits or other malware.
- An adversary on a compromised device may make use of vulnerabilities in secure remote access protocols (such as implementations of SSH relying upon quantum-unsafe algorithms) to use these devices to additionally forge undesirable tunnels between devices to create further nodes of damage within an enterprise network.
- Adversaries with illicit access to a central server or network node (through a malicious SSH tunnel or comparable access point) may be able to compromise an entire network, including:
    - Taking control of read/write/copy/file-transfer access and the types of files, devices, and removable media allowed to access the network by specific users or endpoint devices.
    - Undoing control parameters (such as location, user, or device authentication) used to previously prevent endpoint devices from "bridging" from an enterprise Local Area Network (LAN) to Wi-Fi, enabling easier extraction of sensitive content from the enterprise network.
- False indications of compliance with network access control parameters, whereby an adversarial-controlled endpoint device may fraudulently indicate that it has the required anti-virus and patches, and then intentionally or unintentionally bring malware onto the enterprise network.

In addition to the threats to information security, compromised endpoint devices may also result in legal penalty in jurisdictions in which occurrences of breached personal information due to inadequate encryption must be disclosed by law.

5.1.2 Network infrastructure encryption

In addition to endpoint devices and storage servers, data must be secured throughout its' entire transfer through a network from one location to another. Network infrastructure encryption refers to the idea that as data moves throughout a network, the reliant network infrastructure must use cryptography in a way that is impervious to an adversary's attempt to undermine data integrity, confidentiality, or authenticity. Areas of concern include the Internet backbone over which much of the principal internet traffic travels between the Internet's many networks, as well as the encryption between linked enterprise data centers, and the encryption used to secure wide-area networks (WAN).

Fiber optic cables can easily be tapped and data can be copied as a form of physical attack on the network infrastructure. These cables can either be part of the Internet backbone itself, or else used internally for enterprise network objectives such as communications between a company's cloud servers or their data centres [EFF14]. Consequently, it is clear that even without the present threat of a quantum computer, unencrypted data (at the very least) is vulnerable to adversarial observation and manipulation. At present, not all data transmitted over the Internet is encrypted, which leaves it open to attack. However, the deployment of quantum algorithms means that encrypted information may also be compromised, depending on the method of encryption.

One of the most common methods used to encrypt web browser data traffic over networks is the Hypertext Transfer Protocol Secure (HTTPS), which layers regular HTTP traffic on top of TLS/SSL. This offers authentication of client and server in addition to encryption. Unfortunately, present implementations of TLS/SSL rely upon RSA public keys for server authentication and Diffie-Hellman for key agreement, both of which are susceptible to attack by Shor's algorithm. Consequently, a quantum computer could decrypt all traffic sent between the server and client side web browser.

Organizations protect their network by encryption communication either at OSI Layer 2 (Ethernet) or OSI Layer 3 (IP) implemented in dedicated encryption hardware or networking gear such as a switch or router. There are currently no widely used standardized protocols for layer 2 encryption and each vendor develops its own cryptographic implementation. Most vendors rely on RSA or Diffie-Hellman for key agreement, making the solution vulnerable to an adversary equipped with a quantum computer. However, there are quantum safe layer 2 encryption solutions, commercially available today, consisting of a quantum key distribution system providing keys to layer 2 encryption devices. As for layer 3 encryption, it is typically based on IPsec that relies on the IKE protocol for key establishment. IKE is not considered quantum-safe, implying that communication exchanged over these networks can be decrypted using a quantum computer.

In general, should network infrastructure be encrypted using algorithms that are not quantum-safe, all data that is transmitted over that network is vulnerable to immediate or later decryption by an adversary in possession of a quantum computer. Importantly, it should be noted that an adversary could store this encrypted information for years into the future, when a quantum computer that would enable them to read it.

5.1.3 Cloud Storage and computing

Cloud storage is a high-level term describing computing as a service, rather than a product. This allows users to utilize centralized, shared resources (both hardware and software) over a network. Cloud services have become ubiquitous due to the rise of high-capacity networks, the decreased cost of computers and data storage devices, and trends toward hardware virtualization as well as infrastructure-, platform-, and software-as-a-service models. Cloud computing has numerous benefits, including accessibility from multiple devices/locations, a reduction in a business' need for in-house IT solutions, and an optimized use of computing power distributed across many users and businesses. However, a major issue with the use of cloud computing is that since these services are shared by many users and often not offered over a private network – but rather to large organizations on an opt-in basis, encryption is essential.

Options for quantum-safe cloud computing are subsumed by quantum-safe server, endpoint, and network infrastructure security. Key exchange parameters for protocols such as HTTPS should no longer make use of RSA, DSA, or ECDSA. Fortunately, cloud computing offers the distinct advantage of having a centralized IT security management system across many applications and businesses, reducing security overhead for individual enterprises and consequently offering easier transition to quantum-safe protocols. This transition is essential in particular due to both the fact that cloud storage is – by definition – remotely accessed, requiring data to traverse a public network between the user and the cloud. The need for strong encryption is further amplified by the multitude of distinct and untrusted users sharing the infrastructure.

5.1.4 Big data, data mining and machine learning

Big Data describes any practice of collecting, searching, analyzing and sharing any data set so large that these efforts are beyond the scope of traditional data management tools. Increasingly powerful computer hardware and efficient software have enabled the use of these large data sets to find important patterns in fields as diverse as physics, genomics, environmental science, life sciences research, criminology, and business informatics. Applying the techniques of data mining, it is possible to extract valuable information from these data sets and to build networks of association. This offers enterprises and governments power to discover important patterns despite the once-obscuring scope and level of detail of these databases. There even exist techniques that enable researchers to see these patterns without revealing to themselves identifying information about the individual data points [VBF04]. It is important to encrypt and secure these systems because should they be left exposed, the same power offered to these organizations to identify individual users can also be obtained by hostile adversaries.

The vulnerabilities to big data (and security architecture recommendations) in the presence of a quantum computer are generally those associated with big data's supporting technologies – particularly, data/cloud storage and data transmission through a network.

Quantum-safe solutions for securing big data are essential because large data sets offer unprecedented insights into the details of their subjects – so intricate and detailed that they cannot even be analyzed by conventional means. Consequently, all of this knowledge leads to a great deal of power in the hands of an adversary. Organizations must ensure their storage/disk and communication encryption systems comply with quantum safe cryptographic primitives.

5.1.5 SCADA (Supervisory Control and Data Acquisition) systems

SCADA systems are a type of industrial control system used for remote monitoring and control of industrial processes. These can be anything from resource extraction and distribution (oil, natural gas, mining), to national utilities/infrastructures (electric grids, railway and traffic systems control, water treatment and distribution systems), to manufacturing, to facility processes (HVAC, energy consumption, etc.). Failure to encrypt and secure SCADA systems offers an adversary the opportunity of the remote take-over of factories, oil pipes, electrical grids, airports, mining operations, and the power supply. The potential for destruction in these cases is self-evident and beyond quantification.

Historically, the security of SCADA systems has been poorly researched, due in part to the initially proprietary nature of these systems. However, in the light of newer, networked methods of industrial control, the “security by obscurity” approach no longer will suffice. In the years following the damage by the Stuxnet worm, penetration testing has revealed an overall bleak picture of the security of these systems. While some elements of some systems in the post-Stuxnet era are encrypted using Advanced Encryption System (AES) – which is quantum-safe – it is important to remember that any weak link in the security model of these systems is vulnerable to attack by an adversary with a quantum computer. Further work must be done to identify vulnerable links in the information flow through SCADA systems, and to bring the majority of systems – which have poor encryption or even none at all – up to date through the use of AES as recommended in numerous standards [IEEEP1711]. These symmetric keys must be established using a quantum-safe key exchange algorithm.

The projected future trend of use of satellites for large distributed control systems and the internet of things for intelligent remote monitoring emphasizes a particular need for designers and administrators of SCADA systems to migrate toward quantum-safe security, in an increasingly connected and vulnerable world.

5.2 Fields of application

5.2.1 Medicine and health

Medicine and health services in industrialized countries share core values of patient confidentiality, which is increasingly important giving the rising ubiquity of regional and national public health information networks, as well as multi-clinic information systems for centralized patient records. Many countries impose legal liability for clinics whose patient data is compromised due to inadequate security measures.

Particular vulnerabilities for health-care providers resulting from quantum computers include, but are not limited to:

- Data breaches of patient information through poorly encrypted staff endpoint devices, or due to poorly encrypted data links between health care centres within a regional network.
- Unauthorized access to individual patient data points in a research environment through use of data mining practices that are not privacy preserving in a post-quantum world.

- Fraudulent acquisition of patient files through improperly authenticated channels.
- The releasing of vulnerable scientific information that may be stored on clinic computers (such as certain genetic patterns) that would also undermine biometric security identifiers.

Protecting information related to medicine and healthcare using quantum-safe solutions is particularly important, as this type of information typically requires long-term confidentiality, at least equal to the life expectancy of the patient and possibly extending even beyond in the case of genetic data. These requirements are often integrated in legislation. German law for example stipulates that medical data must remain confidential even after the death of a patient.

5.2.2 Financial Services

Banks and financial services rely heavily on information technology in their operations, and as a consequence are extensive users of cryptography to guarantee authenticity, integrity and confidentiality of the information they process. Cryptography within this industry is used in the following examples:

- Intra-organizational communications sent within the corporate network or between data centers for information transfer, backup, and disaster recovery need to be protected. Typically, these systems are implemented as hardware or software AES encryption, and are vulnerable in the respect that they use a public key system of key distribution.
- Interbank financial messaging across the SWIFT network is used to transfer payment orders, allowing for standardized, encrypted transactions between different banks around the world. SWIFT operates a Public Key Infrastructure to digitally sign and encrypt messages sent over SWIFTNet. Crucially, these messages require a migration to quantum-safe forms of digital signatures and encryption in order to remain secure.
- Credit card information is protected according to the Payment Card Industry Data Security Standard (PCIDSS). Cardholder data is typically encrypted for transmission for example at a point of sale prior to transmission to the bank. This encryption utilizes symmetric key cryptography, however, the keys are exchanged using public key cryptosystems that require a quantum-safe alternative.
- Stored data such as tapes and hard disks are encrypted by organizations for secure offsite archiving. These solutions are typically based on hardware AES encryption.
- Online banking relies upon the TLS protocol to secure web traffic, and consequently is vulnerable to post-quantum issues with server authentication using X.509 certificates and RSA public keys, as well as session key establishment.

Quantum computing creates numerous, high impact challenges for organizations in this sector. They are indeed faced both with the challenge of long-term security for certain types of information (e.g. customer data) and of extremely high value electronic transactions (e.g. SWIFT messaging). Moreover, in the event of a threat arising from quantum computing, the sector will have a high chance of being targeted first because of the financial benefits that can be directly derived from cryptographic vulnerabilities.

The implementation details for the financial services industry, in particular, require consideration of problem specific requirements for timing and information payload. Due to criticality of the speed at which many of these transactions must be completed, solutions providers are advised to carefully evaluate quantum safe schemes for key generation, encryption, and decryption speeds.

5.2.3 Mobile Applications

Mobile applications may or may not be owned and controlled by a Mobile Network Operator (MNO), the availability of these applications and services are often a deciding factor for users as to which handset they will purchase and to which mobile network they will subscribe.

- **Ecosystem Identification,** a single sign on feature for a brand-name company that offers an umbrella of services, often their brand id is attached to account information that includes the user’s credit card and can be used for digital purchases at the brand’s on line store. Digital purchases can include movies, games or apps and transactions will be protected by some end-to-end security mechanism such as TLS and employing a userid and password.
- **Near Field Communication (NFC),** used for mobile contactless payment, mobile ticketing and other applications involving a Secure Element that is embedded in the handset using a discrete chip, a special uSIM or uSD card, or a handset that supports Trustzone/Trusted Execution Environment (TEE). The secure element

is like a digital locker for cryptographic keys, where an MNO or 3rd party may setup their own Security Domain in order to host an application such as a mobile payment based credit card, access control or ticketing.

- **Digital Rights Management (DRM),** used to protect movies and television shows which allow content producers to sell or rent premium video content to end users through an online store. Content is protected by Microsoft PlayReady, Google Widevine or Adobe Access. These technologies separately encrypt the content with a title key, and the title key is distributed to users via license file that is purchased from an online store.

- **Enterprise Mobility Management,** software solutions used by enterprises to manage and secure corporate data on employees' mobile devices. These types of solutions will either install a work container on a mobile device, or assume complete control of the mobile device so that it can be remotely managed, located or wiped of its data. Software applications can also be remotely installed; typically these are digitally signed to prevent tampering.

- **Cloud Applications/Services,** are popular with companies who subscribe to an application for all of their employees with a 3rd party provider who then makes the application broadly available via a web browser and mobile device applications. A very common cloud based application for corporations is a Customer Relationship Management (CRM) service used for sales employees. Depending on cost, and sensitivity of the data, companies are moving many traditional on-premise corporate software services into the cloud by transitioning from in house built and supported applications, to a 3rd party cloud based application provider. Confidentiality of corporate data is a large component of these types of software sales; often data is protected in transit using TLS/SSL.

5.2.4 Mobile Network Operator Wholesale

- **Internet of Things - M2M**, sensors are used everywhere to remotely monitor assets and communicate back to their owners. Electrical meters, vending machines, shipping containers, medical monitoring equipment are some of the examples of embedded devices that require remote connectivity that either uses a proprietary dedicated wireless network or purchases wireless cellular bandwidth from an MNO as a wholesale application. Many commercial applications have regulated security requirements, often with unique and constrained cryptographic key management needs.

- **Connected Vehicles**, telematics and emerging vehicle-to-vehicle communications used for fleet logistics and public safety applications. Many of these applications rely on confidential and authentic communications.

6 Economics of quantum safe security

6.1 Benefits of quantum safe security

Cryptography has a very rich and entertaining history that weaves stories of clandestine communication and cat-and-mouse detective work. For the past century alone, some of the historical tales include: The Black Chamber, a forerunner to the American National Security Agency which decoded foreign diplomatic codes; the work performed by British GCHQ to solve World War II era ciphers, leading to breakthroughs in computation and machine computing; the advent of wide scale commercial use of cryptography starting in the 1970's with the invention of DES through research performed at IBM. Popular documentaries are broadcast on television that glamorize encryption systems that have come and gone over past decades, and when these cryptographic systems fade, they are always replaced with stronger, faster algorithms and technologies because the global research community is forever redefining the state of the art.

If history can be used to accurately predict events yet to come, then breaking a cryptographic cipher can have catastrophic repercussions for anyone using a cipher who is ignorant of its compromise. And great advantages are bestowed upon anyone who takes advantage of their adversary's ignorance.

In most cases, when a cipher is secretly broken by an adversary it is unfair for the historical record to criticize past choices to continue using the cipher, because history has the benefit of hindsight. After all, what indications were visible at the time to suggest to a reasonable person that a cipher had been broken and that an adversary was profitably taking advantage? But in the case of today's state of communications, security practitioners are giving early warning of the wide scale security collapse of communications infrastructure due to heavy reliance on Diffie-Hellman, RSA and ECC. These cryptographic systems are increasingly vulnerable to quantum attacks as quantum computing matures and the state of the art in computation and algorithm design is redefined.

Quantum Safe Security is a concept that is less about moving from an old technology to something that is a new. It is more about promoting the idea that communication standards are inflexible and often make a naive assumption that current ciphers will remain good enough until replaced by something superior. This assumption is true sometimes, however, cryptography as a field of research is strange and unique in that old ciphers get weaker simply because new researchers get smarter.

Introducing Quantum safe security schemes and cryptographic agility into protocols promotes rigour and quality amongst the security engineering profession. It is hard to design a technology that assumes its underlying security mechanisms will erode over time. But introducing quantum safety into systems provides an exit strategy from RSA and ECC.

Regardless of the critics of quantum computing, history can be used to predict the future of a cryptographic algorithm, and RSA and ECC will eventually be broken by either quantum attacks or new mathematical techniques. And with the benefit of hindsight, future critics will certainly conclude, "they had adequate warning, how could they possibly have let history repeat itself?"

6.2 Challenges for quantum safe security

Many of the challenges for the adoption of quantum safe security are rooted in common best practices within the security industry. Very early in their careers security practitioners are taught to avoid new cryptographic algorithms that have not received years of public scrutiny, to not design their own security protocols, and rely only on well established security standards. These security tenants are still sound and very relevant in a world with quantum computing but the industry needs to recognize the amount of lead-time required to make systemic changes to existing security products and infrastructure because of the pragmatic security mind-set. These best security practices that routinely block and protect against bad or questionable security schemes also slow the adoption of changes meant to protect against never-before-seen attacks. Some of the main barriers in security culture that need to be recognized and addressed before quantum safety will be widely adopted:

- **Confidence in Algorithms**. There are many well-studied public key based cryptographic algorithm options that could be used as a substitute for RSA or ECC, however, many of these substitutes do not have the benefit of wide spread practical use.

- **Rigidity of Security Protocols**. Quantum safe ciphers may not fit into an established protocol because of historical protocol design assumptions, key size choices and tolerance for message expansion. Earlier sections in this whitepaper give examples of common security protocols that demonstrate the varying degree to which quantum safe cryptography can be used effectively. Many protocols were not designed with cryptographic agility in mind, and may not easily accommodate a change of cipher.

- **Perception of non-urgency.** An exact date for the arrival of general purpose quantum computing cannot be given, however, global interest is growing and steady progress is being made. As quantum computing matures, computer security weakens. Some businesses require their security to have medium longevity in the sense that confidential information that is worth protecting now, will also remain sensitive and should be kept private a year or two in the future. Other businesses require their security to have greater longevity, keeping information private for decades. Quantum safety is “not urgent” only for those with short term security needs but any business that requires its secrets to remain secret will need to consider their quantum safe transition strategy now. A quantum attack is just as effective at divulging all past communications, i.e. encrypted military information residing on physical storage medium.

6.3 Risk management: cryptography or insurance premiums

While cryptography is the art of writing secret messages, security is an art form as well, with a primary focus of managing risk. What things are worth protecting? If something were to happen to these things, what are the likely consequences and how can the potential damage be limited?

Security uses cryptography as a fundamental building block. Consider transferring money from one bank account to another, the account holder may write a cheque and sign it with their personal signature, or they may initiate an electronic money transfer where two banks electronically communicate using cryptography and digital signatures. In both cases, the bank relies on some type of a signature to authorize the money transfer, either an ink signature or a digital one. But signatures alone are not the only safeguard at work protecting the financial system, the risk of banking fraud is managed carefully with many more checks and balances, above and beyond that of simply requiring an authorizing signature. After these checks and balances are in place, any residual risk is then either accepted as a cost of doing business or it is transferred to someone else using insurance.

This banking example is not an attempt to marginalize the importance of cryptography; instead it is critical to point out that the use of cryptography in day-to-day life is deceivingly innocuous and tremendously pervasive. How important is a digital signature really? Cryptography is a tool and a foundational building block that is used by security practitioners everywhere to protect anything that relies on electronic communication. It looks like a small thing to have to worry about, but in its absence, larger sweeping consequences emerge.

What would happen if cryptography stopped working? One side effect would be a dramatic rise in banking fees and insurance premiums. There may even be a rise in the creation of economic substitutes for the banking system itself. This has occurred in recent times in countries where the population lost trust in banks and preferred to convert funds into precious metals stored outside of the banking system.

Risk is managed in a multitude of ways. Preventative steps can be taken that reduce risk, for instance, in the case of a digital signature on a money transfer, safeguards are put in place to reduce the chance of bank fraud. If these automatic and invisible safeguards were not in place, banks would still operate and money would still change hands, but it would be a more costly proposition because of higher rates of bank fraud, the cost of which would be passed onto the consumer in the form of higher transaction fees.

Another example can be found in the business of comprehensive auto insurance. Insurance premium rates are quoted based on a number of factors; including rates of theft based on make and model years. Engine ignition inhibitors use cryptography by embedding special electronics in the ignition key to reduce rates of theft. This in turn keeps insurance premiums low because the particular car model is less likely to be stolen. Were these technologies suddenly to stop working, automobiles would still be driven, but they would be easier to steal and insurance premiums would inevitable rise to compensate.

The world will not come to an end without cryptography; it will just be a lot more expensive to live in it.

Quantum computing threatens modern cryptographic tools and renders them ineffective. It does not negate all of the cryptography tools at society’s disposal, just the tremendously popular ones. The gains that are promised by mature quantum computing are exciting with a great potential for capitalization, however, the unintended costs to our existing communications infrastructure will be extremely expensive, starting on the very day that quantum computers graduate from the lab to commercially available. Fraud and insurance premium hikes will be noticed first, followed by expensive infrastructure upgrades and wasteful disorganized repairs.

Quantum computing is itself a risk to businesses, the likelihood is growing that quantum computing will become commercially available at a reasonable cost and the impact is a many fold increase in the severity and occurrences of

Cybersecurity events throughout a business. The way to prevent this risk is to migrate systems away from cryptography that is vulnerable to quantum attack, while keeping in mind the potential costs of making such a transition. Handled in an organized fashion, and with enough lead-time, technology switching costs are manageable because efforts can focus on hardening today's existing security safeguards so that they remain effective as quantum computing matures and becomes ubiquitous.

6.4 Technology switching costs: gradual vs. immediate

It can take years for a standards body to significantly alter a well-established and popular standard. This is because it is usually much simpler to create a new standard than it is to retrofit an old one with sweeping new features. Nevertheless, without technology standards, the market will still find a solution to its problems, often resulting in a number of expensive proprietary methods vying for market dominance until an oligopoly of winners emerge who will sacrifice interoperability for market share and price premiums. Historically, widespread adoption of any technology is simply not economically feasible in the absence of standardisation.

But what should be standardized? In most cases, the elements that interface with the components and systems are the only ones that require standardisation. The internal workings of a system can often remain not standardised, and be treated as an economic differentiator by its respective manufacturer.

Most commercial communication and security products are built on top of standards based cryptography and protocols because designing and building a secure system is tricky in the sense that a security system appears to be working, until sometime after it has been successfully exploited. Seemingly innocuous errors in design and implementation are routinely demonstrated as the cause of security vulnerabilities with seemingly disproportionate and vastly negative commercial ramifications. As a result, security practitioners have been trained that, to prevent these problems from occurring, it is important to layer security controls on top of each other and to use standards based cryptography and protocols to limit the impact of system flaws and oversights. This approach to layering suggests that in some cases, it may indeed be a better choice to build a new standard than to retrofit an existing one with very many new features that may increase the risk of breaking the existing standard.

If standards are updated or new quantum safe variants of standards emerge then security products can be more transparently upgraded over a gradual period of time, e.g. adding a new layer of quantum-safety to an existing system. Gradual and transparent upgrades are much less costly than requiring an immediate or urgent transition, in theory. While it sounds like a rational argument that careful planning is superior to having to perform urgent patchwork, in practice, a gradual process of standard evolution can also lead to high technology switching costs if left unchecked and without the benefit of real world commercial experimentation. A balance must be struck between the choices made by standards bodies to close exposures to quantum attacks, and the choices of commercial IT organizations with an eye towards justifying solution, deployment and ongoing operation costs given a number of secure alternatives. Simply asking standards researchers to change their cryptography, in the absence of commercial viability testing, is a sure way to land in the high technology switching cost trap.

6.4.1 Avoiding technology switching costs

Technology switching costs occur anytime a change is made in a basic technological system such as a data center, core network, wireless sub-system, etc. These costs can often be avoided by reasonable planning before the switch from one technology to another must be made. For many categories of secure information, there may be no need to introduce quantum-safe techniques into systems for some time. For other such categories, action may be required within a relatively short time period.

The time to start planning is nevertheless now. Standards groups and product vendors need to see a demand to justify time and effort investments. Demonstrating demand does not necessarily translate to paying price premiums often characterized by technology early adopters, but instead, leveraging well established and commoditized security products and influencing their respective product roadmaps in parallel to the associated standard's evolution. This can be done with some straightforward and low business impact changes to existing standard IT practices present in most organizations.

- **Review proprietary in house IT systems**, for areas where simple cryptographic primitives are used without the need of more elaborate security protocols. For instance, log files and backups are often digitally signed for integrity and authentic audit trail purposes and signatures are stored in a database. Extending the database tables to include a second quantum safe signature is low impact to existing systems and has desirable side effects. IT staff gain initial experience and exposure to quantum safe technologies, and trusted vendors who provide product support witness steps being taken towards quantum safety and report to their own internal sales and product teams.

- **Evaluate vendor products with quantum safe features** using non-production and staging IT environments, IT equipment and software is often evaluated and compared to other solutions prior to making purchasing decisions. Ensuring that solutions under review contain a mix of vendors, some of which offer quantum safe features, will naturally drive competitive positioning and competitive evaluation by each vendor's sales and product teams. Demonstrating a buying preference for products with quantum-safe features will ultimately drive quantum safety into products, however, simply evaluating products with quantum features can also drive adoption, regardless of purchasing decisions, because forward thinking vendors will pay close attention to the features being offered by their competitors and whether or not those competitive features are being taken seriously by their customers.

- **Ask vendors for quantum safe features in procurement templates.** Larger organizations use procurement teams for IT capital expenditures and use standard templates for Request for Information (RFI) or Request for Proposal (RFP) documents that are sent to vendors. These documents will have a checklist of feature related questions ranging from hard requirements to optional nice-to-have features that vendors are asked to answer in an effort to help buyers evaluate and compare competitive offerings from multiple vendors. A procurement team will typically have a list of standard security questions that are included in RFPs that are sent to IT product vendors, and this security template is a good place to add questions about quantum safe features because it will broadcast a customer's interest within the sales and marketing teams of the product vendors for quantum safety. Initially, responses from vendors will be "not supported", but overtime, savvy vendors will respond "roadmap feature" if enough of their customers and prospects demonstrate an interest in quantum safe features.

- **Lobby government organizations to include quantum-safety in legislation and recommendations.** Security investments are usually a zero-sum game, where a fixed sum of money is allocated to different solutions. While this allocation should theoretically be based on risk and impact, larger organizations tend to prioritize based on compliance with legislation and government regulations. This implies that risk with dramatic impact but small probability (at least in the foreseeable future) is typically not well covered. Government organizations such as NIST in the US or ENISA in the European Union can have a strong impact in ensuring that quantum-safe alternatives become available and are seriously considered by users.

7 Conclusions and opportunities for further work

Quantum computing indeed poses a credible threat to conventional information security systems. The ICT community nevertheless has the ability to analyse and better understand this threat and its consequences for the various categories of information that requires protection. Following are several recommendations and opportunities for further work:

Recommendations for enterprises:

- It is advisable for ICT organisations to consider how long the information they handle in each category needs to be secure, and to analyse the consequences of having their various categories of secure information made available to the public via future quantum computing attacks. Generally speaking, if the organization has a need to archive certain information or protect the privacy of online transactions for more than 10 years, and currently uses encryption techniques, then these security methods should be upgraded to known quantum safe algorithms and techniques in order to protect long-term privacy.

- Investigate quantum safe products that are currently on the market and prototype within a network-staging environment in order to evaluate the production readiness of available commercial solutions and to develop an internal knowledge base amongst IT staff.

- Examine cost saving strategies to reduce technology switching costs, outlined in section 6.4.1 above as part of a broad CIO strategy to address and mitigate potentially high switching costs that may be involved when switching to a quantum-safe networking and security environment.

- Enterprises with advanced research teams should document quantum safe use cases for their industry and publish within standards groups such as ETSI who maintain a standards leadership role in quantum safe technologies.

- Further work within the global standards community should include an effort to identify what quantum-safe techniques and/or portions of quantum-safe systems require standardisation and which ones do not.

Recommendations for security product vendors:

- Perform product and market research to determine if there is a justified opportunity to add quantum safe features to product roadmaps.

- Market test quantum safe features and products with existing customer base to determine if there is a business case for offering new quantum safe products or upgrades to an existing install base.

Opportunities for further research:

- Security researchers should examine security protocols and standards for opportunities to upgrade with quantum safe cryptography. Section 4: Security protocols and potential for upgrade, examines a small number of prevalent security protocols and identifies areas that could be improved to accommodate quantum safe techniques. This work should be extended further to examine other security protocols to determine if there is potential for upgrade.

- Cryptographers should submit performance benchmark data to EBACS for algorithms and techniques that are considered quantum safe.

- Cryptographic researchers should study quantum safe primitives and attempt to break their security. The security research community will trust only ciphers and techniques that have been studied and scrutinized by the cryptographic and security research community.

- Researchers should interview and discuss quantum safe use cases with security specialists working in particular industries to better describe various niche applications and fields of use for quantum safe security controls.

- Quantum Computing Researchers should track the latest progress of quantum computing research and develop a model for the purpose of forecasting the availability of general purpose quantum computing that can break or impact popular cryptographic algorithms and key sizes used within today’s information security infrastructure.

8 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

[A+13] Alaoui, S. M. E. Y., Cayrel, P. L., El Bansarkhani, R., & Hoffmann, G. (2013). Code-based identification and signature schemes in software. In Security Engineering and Intelligence Informatics (pp. 122-136). Springer Berlin Heidelberg.

[BB84] C. H. Bennett, G. Brassard. *Quantum cryptography: Public key distribution and coin tossing*. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175-179 (1984).

[BCNS14] J.W. Bos, C. Costello, M. Naehrig, and D. Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. Cryptology ePrint Archive, report 2014/599. http://eprint.iacr.org/2014/599

[BDH11] Buchmann, Dahmen, and Hülsing, "XMSS - A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions" https://eprint.iacr.org/2011/484.pdf

[BEN97] C. Bennett, E. Bernstein, G. Brassard, U. Vazirani. *Strengths and weaknesses of quantum computation*. SIAM Journal on Computing **26** (5), 1510 (1997).

[BHL05] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, J. Oppenheim. *The universal composable security of quantum key distribution*. In Theory of Cryptography, Proceedings of TCC 2005, **3378,** 386-406, (2005).

[BHM96] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. Physical Review A, 54(4):2651–2658, 1996.

[CHA09] T. E. Chapuran et al. Optical networking for quantum key distribution and quantum communications. New Journal of Physics **11,** 105001 (2009).

[CHE10] T.-Y. Chen et al. Metropolitan all-pass and intercity quantum communication network. Optics Express **18**(26), :27217 (2010).

[CVE10] Cayrel, P.-L., Véron, P., El Yousfi Alaoui, S.M.: A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 171–186. Springer, Heidelberg (2011)

[CW79] J. L. Carter, M. N. Wegman. Universal classes of hash functions. Journal of Computer and System Sciences, **18** (2), pp. 143-154 (1979).

[DDLL13] Lucas et al. , "Lattice Signatures and Bimodal Gaussians". https://eprint.iacr.org/2013/383.pdf

[Ding04] J. Ding: A new Variant of the Matsumoto-Imai Cryptosystem through Perturbation. PKC 04, LNCS vol. 2947, p.305-318. Springer (2004)

[DS05] J.Ding, D. Schmidt: Cryptanalysis of HFEv and Internal Perturbation of HFE. PKC 05, LNCS vol. 3386, p. 288-301. Springer (2005)

[DPW14] J.Ding, A. Petzoldt, L.-C. Wang: The cubic Simple Matrix Encryption Scheme. PQCrypto 2014, LNCS vol. 8772, pp. 76-87. Springer (2014)

[DDYCC08] J.Ding, V. Dubois, B.Y. Yang, C.-H. O. Chen, C.-M. Cheng: Could SFlash be repaired? Automata, Languages and Programming (ICALP 2008), LNCS vol. 5126, pp. 691 – 701. Springer (2008)

[DYCCC05] Ding, J., Yang, B.-Y., Chen, C.-H. O., Chen, M.-S, and Cheng, C.M.: New Differential-Algebraic Attacks and Reparameterization of Rainbow. In: LNCS 5037, pp.242-257, Springer, Heidelberg (2005)

[EBACS] EBACS web site http://bench.cr.yp.to/ebasc.html

[EFF14] Electronic Frontier Foundation “Encrypt the Web” Report. https://www.eff.org/encrypt-the-web-report

[EKE91] A. K. Ekert. *Quantum cryptography based on Bell's theorem*. Physical Review Letters, **67**, 661-663, (1991). doi:10.1103/PhysRevLett.67.661.

[ELS12] D. Elser et al. *Network architectures for space-optical quantum cryptography services*. ICSOS 2012 International Conference on Space Optical Systems and Applications, (2012).

[ERE10] P. Eraerds et al. Quantum key distribution and 1 Gbps data encryption over a single fibre. New Journal of Physics **12** 063027 (2010).

[FSXY13] A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism. In Proc. ASIACCS 13, pages 83–94. ACM, May 2013.

[GIS02] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. *Quantum cryptography*. Review of Modern Physics **74**, 145–95 (2002).

[GRO02] F. Grosshans, P. Grangier. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88:057902 (2002).

[Gro96] Lou Grover. A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 212, 1996.

[HHHW09] P. Hirschhorn, et al. “Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches” Applied Cryptography and Network Security, Springer, LNCS 5536, 2009. https://www.securityinnovation.com/uploads/Crypto/params.pdf

[HWA03] W. Y. Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys. Rev. Lett. **91**, 057901 (2003).

[IDQ] ID Quantique SA. www.idquantique.com

[IM11] Lawrence M. Ioannou and Michele Mosca. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In BoYin Yang, editor, Proc. 4th International Workshop on PostQuantum Cryptography (PQCrypto) 2011, LNCS, volume 7071, pp. 255–274. Springer, 2011.

[Ina02] Hitoshi Inamori. Security of practical timereversed EPR quantum key distribution. Algorithmica, 34(4):340–365, 2002.

[LCQ12] H.-K. Lo, M. Curty, B. Qi. Measurement-device-independent quantum key distribution. Phys. Rev. Lett., **108**, 130503 (2012).

[LAN13] Thomas Länger. *Information Security and the Enforcement of Secrecy: The Practical Security of Quantum Key Distribution*. Ph.D. Thesis University of Lausanne (2013)

[LIM13] C. W. Lim et al. Device-Independent Quantum Key Distribution with Local Bell Test. Phys. Rev. X **3**, 031006 (2013).

[LUC13] M. Lucamarini et al. Efficient decoy-state quantum key distribution with quantified security. Optics Express **21**(21), 24550 (2013).

[MAU11] U. Maurer, R. Renner. *Abstract cryptography.* In Proceedings of Innovations in Computer Science, ICS 2010, 1-21, (2011).

[Merkle79] Ralph C. Merkle, Method of providing digital signatures, US Patent 4309569-A, Filed September 5, 1979.

[Mosca13] M. Mosca, “Setting the Scene for the ETSI Quantum-safe Cryptography Workshop”, e-proceedings of “1st Quantum-Safe-Crypto Workshop”, Sophia Antipolis, Sep 26-27, 2013. http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf

[MSU13] M. Mosca, D. Stebila, B. Ustaoglu, "Quantum Key Distribution in the Classical Authenticated Key Exchange Framework", In Proceedings of the 5th International Conference on PostQuantum Cryptography (PQCrypto 2013), Lecture Notes in Computer Science, Vol. 7932, pp. 136154, Springer (2013).

[MTSB12] R. Misoczki, et al. “MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes” Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on Information Theory. https://eprint.iacr.org/2012/409.pdf

[NMBB12] R. Niebuhr, et al. “Selecting Parameters for Secure McEliece-based Cryptosystems” Informational Journal of Information Security, June 2012, Volume 11, Issue 3, pp 137-147. https://eprint.iacr.org/2010/271.pdf

[PAT14] K. A. Patel et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. Applied Physics Letters **104** (5), 051123 (2014).

[Patarin96] Patarin, J.: Hidden Field equations (HFE) and Isomorphisms of Polynomials (IP). In: Proceedings of EUROCRYPT’96, pp. 38-48, Springer, Heidelberg (1996)

[PBB10] Petzoldt , Bulygin, and Buchmann “Selecting Parameters for the Rainbow Signature Scheme” https://eprint.iacr.org/2010/437.pdf

[PBB11] A. Petzoldt, S. Bulygin, J. Buchmann: Linear Recurring Sequences for the UOV Key Generation. PKC 2011, LNCS vol. 6571, p. 335-350, Springer, 2011.

[PDG14] Pöppelmann, Thomas, Léo Ducas, and Tim Güneysu. "Enhanced Lattice-Based Signatures on Reconfigurable Hardware." to appear inCHES 2014.

[Pei14] C. Peikert. Lattice cryptography for the Internet. In Proc. 6th International Conference on Post-Quantum Cryptography (PQCrypto) 2014, LNCS. Springer, 2014. To appear. Full version available at http://eprint.iacr.org/2014/070.

[PER09] R. Perlner, D. Cooper. *Quantum Resistant Public Key Cryptography: A Survey*. Proc. of IDtrust 2009, pp. 85 (2009).

[PET09] N. A. Peters et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments. New J. Phys. **11**, 045012 (2009).

[PPS07] Kenneth G. Paterson, Fred Piper, and R¨udiger Schack. Quantum cryptography: A practical information security perspective. In Marek Zukowski, Sergei Kilin, and Janusz Kowalik, editors, Proc. NATO Advanced Research Workshop on Quantum Communication and Security, NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security, volume 11. IOS Press, 2007.

[QBC13] T. Lunghi et al. Experimental Bit Commitment Based on Quantum Communication and Special Relativity, Phys. Rev. Lett. **111**, 180504 (2013).

[QLI] QuintessenceLabs Inc. www.quintessencelabs.com

[QPQ11] Markus Jakobi et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**, 022301 (2011).

[SARG04] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**(5), 057901 (2004).

[SAS11] M. Sasaki et al. Field test of quantum key distribution in the Tokyo QKD Network. Optics Express, **19**, (11), 10387-10409 (2011). doi: 10.1364/OE.19.010387.

[SEC09] M. Peev et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics **11** 075001 (2009).

[SecInn13] Security Innovation, Inc. ntru-crypto: Open Source NTRU Public Key Cryptography Algorithm and Reference Code. Github. https://github.com/NTRUOpenSourceProject/ntru-crypto

[SHA49] C. Shannon. *Communication Theory of Secrecy Systems*. Bell System Technical Journal **28** (4), 656 (1949).

[SMA07] T. Schmitt-Manderbach et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys. Rev. Lett. **98**, 010504 (2007).

[SSH11] K. Sakumoto, T. Shirai and H. Hiwatari: Public-Key Identification Schemes based on Multivariate Quadratic Polynomials. CRYPTO 2011, LNCS vol. 6841, pp. 706 – 723, Springer 2011.

[Stern94] Stern, J.: A New Identification Scheme Based on Syndrome Decoding. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg (1994)

[STU09] D. Stucki et al. High rate, long-distance quantum key distribution over 250 km of ultra-low loss fibres. New Journal of Physics **11**, 075003 (2009).

[STU11] D. Stucki et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics **13**, 123001 (2011).

[VBF04] V. Verykios et al. State-of-the-art in privacy-preserving data mining. ACM SIGMOD Record, 33 (1), 2004

[WAL14] N. Walenta et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New Journal of Physics **16**, 013047 (2014).

[WAN12] Shuang Wang et al. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. Optics Letters, **37** (6), 1008 (2012).

[ZZDS14] Jiang Zhang and Zhenfeng Zhang and Jintai Ding and Michael Snook, Authenticated Key Exchange from Ideal Lattices, http://eprint.iacr.org/2014/589 (2014)

9 Definitions, symbols and abbreviations

9.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Adversary: In information security, a malicious opponent who wants to prevent authorized users in the security system from achieving their goals. These goals may include confidentiality, data integrity, or correct authentication.

ASN.1: An ITU specification for a self defining data type structure. Digital Certificates follow the ITU X.509 standard that defines a certificate structure using ASN.1 data types.

Authentication: A means of corroborating the source of data, where "source" could refer to a person, place, or specific machine.

Block Cipher: A symmetric key cryptography algorithm that operates on fixed sized units of plaintext to produce fixed sized units of cipher text. Block ciphers can be configured to operate in different modes, most commonly: ECB, CBC, OFB, CFB, CTR.

Certificate Authority: An entity that is trusted by all participants within a PKI system that signs and publishes Digital Certificates.

Certificate Chain: X.509 Digital Certificates contain an issuer field that points to the issuer’s certificate. This allows certificates to form a linked list of related certificates where the first certificate in a chain is “self signed”, this is the Certificate Authority. Validating a certificate chain means checking the signature of every certificate in the chain for authenticity.

Cipher: Short form name meaning an “encryption algorithm” or “encipherment algorithm”.

Ciphersuite: Used in the context of the SSL/TLS protocol it is a combination of algorithms that perform public key based authentication, key agreement, encryption, and MAC.

Confidentiality: A measure of how secret data has been kept from all but those authorized to see it.

Cryptographic Agility: Describes whether or not a security protocol was designed with the capacity to change underlying cryptographic ciphers.

Data Integrity: A term describing the degree to which data has been lost or altered by unauthorized means. Maintaining data integrity implies that the data is consistent, and accurate to the authorized representation of it, across its' lifecycle.

Diffie-Hellman: A prevalent key agreement protocol based on public key cryptography.

Digital Certificate: Main purpose is to cryptographically bind a public key with identifying information of the owner. A Certificate Authority issues a Digital Certificate. See also X.509.

Digital Signature: Used to authenticate a message, it is a code that can only be generated, using a private key known only to the signer, and can be verified by anyone with an associated public key. The public and private keys make a key pair and are mathematically related.

Discrete Log Problem: A mathematical problem that is considered hard for a conventional computer to solve, but is easily solved by a quantum computer. The problem requires an understanding of the concept of an algebraic group. Solve for k, where b^k=g and b and g are elements in the same algebraic group.

Endpoint Device: A device utilized by a user to interact with a distributed computing system. Common examples include PCs and smartphones.

Entanglement: A quantum mechanical phenomenon, where separate photons cannot be described and treated independently, such that measurements of their physical properties obey non-local correlation which cannot be observed in classical mechanics.

Ephemeral Key: A short-lived cryptographic key used for a discrete communication session and then thrown away and never used again. Central to implementing a system that features Perfect Forward Secrecy (PFS).

Free-space QKD: An implementation of quantum key distribution that involves sending polarized light photons through the air, often to a satellite as a trusted intermediary node. This is in contrast to Optical Fibre QKD, which utilizes optical fibres for photon transmission. Free-space QKD is a superior candidate for QKD over several hundred kilometers, because it introduces less noise than within current implementations of Optical Fibre QKD.

Grover's algorithm: A probabilistic quantum algorithm that provides a quadratic speedup over search algorithms implemented on classical computers. Specifically, average-case sorting of an unsorted database takes N/2 steps on a classical computer, and only O(√n) steps using Grover's algorithm on a quantum computer.

Hash Tree: See Merkle Tree.

Information Theoretic Secure: A cipher that cannot be broken, even when analyzed with unlimited computing power.

Integer Factorization Problem: A mathematical problem that is considered hard for a conventional computer to solve, but is easily solved by a quantum computer. The problem starts with the fact that any number is a “product of prime numbers”, and is described as: given an arbitrary number, find the prime numbers that when multiplied together produce the given arbitrary number.

Internet Backbone: The physical infrastructure of which the Internet is built; the principal data routes between the major networks that make up the Internet.

IPSec: Internet Protocol Security is a layer 2 networking security protocol used to setup a Virtual Private Network (VPN).

Key Agreement: A type of algorithm, based on public key cryptography, that allows two remote parties to each exchange some information publicly, that can be intercepted by anyone, and then privately compute the same secret key. The secret key can only be computed by the two participants, anyone else who intercepted the information sent publicly cannot derive the same secret value. Most prevalent key agreement algorithm is Diffie-Hellman.

Key Pair: Used in the context of public key cryptography, refers to 2 values that are calculated and mathematically related to each other. One value remains secret and is called private key. One value is made public and is called the public key.

Key Size: The number of bits of the key used in a cryptographic primitive. Key sizes (or "lengths") are related to the security of a given algorithm because the length directly affects how quickly an encrypted message can be attacked by brute force by simply testing all potential keys of that length.

Message Authentication Code: A short code that is computed on some information using a key. The code can be used to check the integrity and authenticity of the information.

Merkle Tree: A quantum safe public key cryptography system based on a tree of message digests where each child leaf is computed using a cryptographic hash function that is keyed with a key derived from it’s parent.

M2M: Abbreviation for Machine-to-Machine, describing a networked communication system in which an autonomous device communicates with another autonomous device without the participation of a human.

Near Field Communication: A standards based method for two devices to communication when placed in very close proximity, often touching or tapping together.

Network Infrastructure: The software and hardware that makes up a network, allowing multi-user communication, and distributed processes, applications and services.

No-Cloning Theorem: An important idea in quantum mechanics that forbids the copying of an unknown quantum state. This means that if you do not know the exact value of a quantum state, you cannot make a copy that will be guaranteed to have the same value. The no-cloning theorem is the basis for information-theoretic security in QKD, as well as what necessitates quantum repeaters for quantum key distribution over distances exceeding 200 kilometers.

NTRU: A type of lattice based cryptographic public key cipher.

One-time pad: An unconditionally secure encryption method, where a plaintext is encrypted with a random secret key (or pad) of same length as the message. The secret key needs to be known by the sender and receiver and must be used only once.

Public Key Infrastructure: A set of defacto standards and protocols used to distribute and manage cryptographic keys using certificates.

Perfect Forward Secrecy: An attribute of a security protocol that means that temporary/ephemeral cryptographic keys are used in the protocol so that if an adversary breaks the keys and can listen to traffic in the session, they can only listen for the current session, and need to break the keys again in any future secure session.

Polynomial Time: A term used by computer scientists to describe the amount of computing time that is required to solve a mathematical problem as the problem scales upwards in size. A polynomial time algorithm, in short, means that the algorithm solves a problem very fast. In contrast, a sub exponential time algorithm or an exponential time algorithm runs very slow as the size of the problem grows. Encryption that can be solved, without knowing the key, in polynomial time is considered broken and not suitable for providing security.

Private Key: Used in the context of public key cryptography to describe one of 2 values in a key pair that remains secret and is used for either decipherment, key agreement, or creating a digital signature.

Public Key Cryptography: A type of encryption, key agreement or digital signature algorithm, sometimes called asymmetric cryptography, is characterized by methods using 2 cryptographic keys, one key is public and one key is private. The public key is used to either encrypt or verify a message. The private key is used to either decrypt or sign a message.

Public Key: Used in the context of public key cryptography to describe one of 2 values in a key pair that is publicly available to anyone and is used for either encipherment, key agreement, or verifying a digital signature.

Quantum Algorithm: A step-by-step procedure that could be run on a working quantum computer.

Quantum Computing: A computing device based on Qubits that can run quantum algorithms.

Quantum Key Distribution: A communication device that sends and receives single photons in order to communicate cryptographic keys in a way that is impossible for a third party to intercept or eavesdrop without the receiver discovering.

Quantum Repeater: The quantum analogue to the amplifiers seen in classical optical-fibre communication networks. Quantum repeaters are devices that extend the distance that a sender can communicate to a receiver before quantum de-coherence degrades the signal to have too much error to be usable. These repeaters use different technology than classical repeaters because of the no-cloning theorem of quantum mechanics.

Secret Key: Used in the context of symmetric key cryptography, is a value that is used to either perform encryption, decryption or MAC on a message.

Security Association (SA): An instance of an encipherment key that is used to temporarily protect network communications in an IPSec based VPN. An SA is setup using the IKE protocol.

Shor's Algorithm: a method intended to run on a quantum computer that solves an instance of the Integer Factorization Problem and Discrete Log Problem in polynomial time.

Symmetric Key Cryptography: A type of encryption or MAC algorithm characterized by a single shared key that all communicators must know in order to encrypt and decrypt messages.

Trusted Third Party: Typically refers to a Certificate Authority, is an entity that two communicators trust, and who will endorse the authenticity of each communicating party to the other.

Wegman–Carter authentication: An unconditionally secure message authentication scheme. It is based on (almost strongly) universal-2 families of hash functions and requires short shared secret keys.

X.509: The defacto standard format for a digital certificate.

9.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard is a standard NIST symmetric key based encryption algorithm.
CA	Certificate Authority, see definition.
CBC	Cipher Block Chaining, a particular mode of operation for a block cipher.
CTR	Counter mode, a particular mode of operation for a block cipher.

CFB	Cipher Feedback mode, a particular mode of operation for a block cipher.
COTS	Commercial Off The Shelf
DRM	Digital Rights Management, a class of technology used primarily for protecting movies and music from piracy.
DSA	Digital Signature Algorithm is a NIST standard that is based on the ElGamal signature scheme that is a type of public key based digital signature dependent of the complexity of the Discrete Log Problem. DSA is easily solved by Shor’s Algorithm using a quantum computer.
EBACS	ECRYPT Benchmarking of Cryptographic Systems (http://bench.cr.yp.to/)
ECB	Electronic Code Book, a particular mode of operation for a block cipher, where each block of plaintext is encrypted independently of other blocks in the same message.
ECC	Elliptic Curve Cryptography is a type of public key cryptography, this acronym does not refer to a specific cipher, but instead, a family of ciphers including ECDH, ECDSA and others, that base their security on the discrete logarithm problem over an elliptic curve cyclic group.
ECDH	Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman algorithm that derives it’s security from an Elliptic Curve algebraic group, the ECDH algorithm is characterized by smaller key sizes and faster performance than Diffie-Hellman. ECDH is easily solved by Shor’s Algorithm using a quantum computer.
ECDSA	Elliptic Curve Digital Signature Algorithm. A variant the DSA algorithm, derives its security from an Elliptic Curve algebraic group, the ECDSA algorithm is characterized by smaller key sizes and faster performance than DSA. ECDSA is easily solved by Shor’s Algorithm using a quantum computer.
GCHQ	Government Communications Headquarters, a British intelligence and security agency.
IKE	Internet Key Exchange algorithm used to exchange keys and establish Security Associations, primarily used to protect IPSec based VPNs.
ITU	International Telecommunication Union is the United Nations specialized agency for information and communication technologies.
IV	Initialization Vector, a specified block of data that is used when enciphering the first block of plaintext using a block cipher operating in a mode other than ECB.
MAC	Message Authentication Code, see definition.
NFC	Near Field Communication, see definition.
OID	Object Identifier, is a series of numbers that represents a node within an OID registry that is organized in the form of a tree.
OFB	Output Feedback mode, a particular mode of operation for a block cipher.
PKI	Public Key Infrastructure, see definition.
PFS	Perfect Forward Secrecy, see definition.
QKD	Quantum Key Distribution, see section 3.2.1
RFC	Request For Comment which is a type of standard that is published by the Internet Engineering Task Force
RSA	Cryptosystem named after authors, Ron Rivest, Adi Shimer, and Leonard Adleman. The most prevalent public key cryptography algorithm used on the internet, RSA derives its security from the Integer Factorization problem that is known to be broken by Shor’s Algorithm in the presence of a Quantum Computer.
SSL	Secure Sockets Layer is an internet RFC that is a predecessor of TLS.

TLS	Transport Layer Security is an Internet RFC that specifies a security protocol that is used to encrypt and authenticate network communications for software applications. TLS v1.0 is the subsequent version of SSL v3.

Annex A

Authors & contributors

The following people have contributed to this whitepaper:

Authors and contributors:

Matthew Campagna, Ph.D., IQC Affiliate.

Lidong Chen, Ph.D, Mathematician, National Institute of Standards and Technology

Dr Özgür Dagdelen, TU Darmstadt

Jintai Ding, Ph.D. Department of Mathematical Sciences, University of Cincinnati

Jennifer K. Fernick, B.Sc, Institute for Quantum Computing, University of Waterloo

Nicolas Gisin, Department of Applied Physics, University of Geneva, Switzerland

Donald Hayford, National Security Division, Battelle

Thomas Jennewein, PhD, Institute for Quantum Computing, University of Waterloo

Norbert Lütkenhaus, PhD, Institute for Quantum Computing, University of Waterloo

Michele Mosca, D.Phil., Institute for Quantum Computing, University of Waterloo

Brian Neill, CISSP, CSSLP, Institute for Quantum Computing, University of Waterloo

Mark Pecen, Approach Infinity, Inc.

Ray Perlner, Computer Scientist, National Institute of Standards and Technology

Grégoire Ribordy, PhD, Chief Executive Officer, ID Quantique

John M. Schanck, Institute for Quantum Computing, University of Waterloo

Dr Douglas Stebila, Queensland University of Technology

Nino Walenta, Ph.D., National Security Division, Battelle

William Whyte, D. Phil., Chief Scientist, Security Innovation

Dr Zhenfei Zhang, Security Innovation Inc.

Other contributors:

Sarah Kaiser, B.Sc, Institute for Quantum Computing, University of Waterloo

Albrecht Petzold, Technical University of Darmstadt

Daniel Smith-Tone, Mathematician, National Institute of Standards and Technology
Assistant Professor, University of Louisville

Rapporteur:

Mark Pecen, Approach Infinity, Inc.

History

Document history		
1.0.0	October 1, 2014	First Release.