Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques

Olaf Grote[1], Andreas Ahrens[2] and César Benavente-Peces[3]
[1]*ETS de Ingeniería y Sistemas de Telecomunicación, University Politécnica de Madrid, Campus Sur, Ctra. Valencia, 28031 Madrid, Spain*
[2]*Hochschule Wismar, University of Applied Sciences - Technology, Business and Design, Philipp-Müller-Straße 14, 23966 Wismar, Germany*
[3]*ETS de Ingeniería y Sistemas de Telecomunicación, University Politécnica de Madrid, Campus Sur, Ctra. Valencia, 28031 Madrid, Spain*

Keywords: Post-quantum Cryptography, Crypto-agility, Quantum-safe, Quantum Algorithms, Quantum Computer Science.

Abstract: Current security protocols use cryptographic methods based on asymmetric and symmetric schemes. These are used for encrypted communication of information or for general data encryption. The security of these methods is based on well researched methods and known mathematical problems. These have been developed for common computing resources and with the certainty that they cannot be broken at a determinable runtime with finite resources. This excludes novel attack vectors such as those of a quantum computer using quantum algorithms. These cryptographic methods, especially the asymmetric schemes, are not prepared against quantum attacks and not considered quantum safe. Even the security of current quantum safe symmetric schemes is not based on proven security against quantum attacks. In order to effectively counter this threat, a new and effective strategy is necessary. One point of this strategy is the post-quantum cryptography to evaluate new quantum-safe cryptographic principles. The second point is to research security protocols which are quantum safe and resistible against quantum attacks. This paper describes the strategy of post-quantum cryptography and crypto-agility.

1 INTRODUCTION

Current cryptographic schemes must be evaluated to see how they are still effective against quantum attacks. This affects encrypted communication (data in transit) and encrypted data that is not continuously changed (data at rest). However, from the perspective of a quantum computer the symmetric scheme is considered quantum safe and the asymmetric as be broken. In order to make this scheme quantum safe, quantum computer resistant public key derivatives are sought because this method is currently needed. The novel contribution of this article is the review and presentation, which holistic concept is necessary to ward off possible attacks on established security mechanisms with quantum algorithms. The paper focusing is on the established cryptographic methods and how current security protocols can be adapted against quantum attacks. They are two variants to be resilient against quantum attacks. On the one hand, research and investigation of quantum computer-resistant cryptography primitives for post-quantum cryptography (PQC) is needed to find potential candidates. On the other hand is the cryptographic agility (crypto-agility) of security protocols to exchange, modify or parameterize public-key cryptography algorithms with new cryptographic primitives which from the perspective of quantum computing are resilient against quantum attacks. The remaining parts of this paper are structured as follows: Section 2 shows the state of the art established cryptography in context of the new approach. Section 3 introduce the need for use to define a concept and paradigm of post-quantum cryptography and crypto-agility. The main section 4 describes the paradigm. Thus section describes in the first part the new mathematical primitives and cryptographic schemes candidates and in the second part describes the crypto-agility how it is possible to integrate this schemes and the way to modify established security protocol quantum-safe. The results of this study are presented in section 5. Finally, section 6 provides some concluding remarks.

Grote, O., Ahrens, A. and Benavente-Peces, C.
Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques.
DOI: 10.5220/0008162800910098
In *Proceedings of the 9th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2019)*, pages 91-98
ISBN: 978-989-758-385-8

2 STATE OF THE ART

In general, the functionality of an algorithm is a unique, time dedicated, executable sequence of instructions with defined length. Such algorithms scale against the input value exponential. Computer-based programs deliver the quantified results of this algorithm. The estimated runtime and the efficiency of cryptographic algorithms are estimated relatively disadvantageously. Based on complexity theory, each algorithm is runtime efficient of class P, where P contains all decision problems when the input polynomial is determined and the result is computer-capable with a polynomial effort runtime. For example, the following algorithms belong to class P, which have a constant, logarithmic, linear and quadratic runtime. Nevertheless, all algorithms that are correctly recognized for the solution of a problem in polynomial time by means of a non-deterministic Turing machine, but require an exponential computing time in case of a wrong solution, are called runtime inefficient of the class NP, where NP define the non-deterministic polynomial time. Current cryptographic methods are based on these complexity-theoretical statements, since $P \neq NP$ is currently assumed to be mathematical, but has not yet been proven (Eckert, 2014). Thus, if the complexity class of a problem depends on the algorithm or is determined by the required resources such as computing power and memory, quantum algorithms can perform these tasks with optimized runtimes. In contrast to the algorithms that make all problems in complexity class P decidable to a polynomial runtime on a deterministic Turing machine, quantum algorithms include functions rather on questions like searching in a database, recognizing a global property of a function, e.g. period, mean value. Furthermore, quantum algorithms solve runtime-optimized problems on a non-deterministic Turing machine such as the number-theoretical problem or the calculation of the gradient in $n-$dimensions. Two quantum algorithms have received quite a bit of notice: Shor's algorithm for factoring integers in polynomial time on a quantum computer (Shor, 1994) and Grover's algorithm for searching a unsorted database of x elements with efficient runtime (Grover, 1996). The advantage and main reason of the high efficiency of quantum algorithms is the calculation of the periodicity of a function, which is available as a global property after the first operation in the quantum register of a quantum computer. With this method, which provides for a concrete parallelism, the periodic and recurring components within a bit sequence can be efficiently filtered and useful for a quantum attack.

3 QUANTUM ATTACK APPROACHES

Quantum mechanics describes in simplified terms the microscopic properties of a physical object where the specific state of this object temporal and physical space only be determined vaguely. This object (e.g. atoms, electrons, photons) particle has the same energetic order of magnitude as the object with which it is to be measured. This also means that the original particle is demonstrably changed after a measurement (Brands, 2011). Quantum computer follow the laws of quantum physics and performs operations with three states "0" or "1" or "0 and 1". This new computer capability solve mathematical problems of the complexity class NP in a polynomial time so that $P = NP$. Shor's algorithm (1) which performed on a quantum computer breaks in polynomial time cryptographic primitives and schemes that based on integer factorization and discrete logarithms (Shor, 1997). This algorithm delivers to one natural number N a nontrivial factor which are defined as:

$$O((\log N)^3) \tag{1}$$

All public-key cryptography that use those algebraic structure are affected like Rivest, Shamir, Adleman method (RSA), Elliptic Curve Cryptography (ECC) and Diffie-Hellman (DH). Grover's algorithm (2) is a runtime optimized quantum search algorithm to use brute-force attacking that checks all possible cipher key by determined time and resources (3) (Grover, 1999), where n is the number of bits that are searched (see Table 1):

$$O(\sqrt{n}) \tag{2}$$

$$O(\log n) \tag{3}$$

This enables the quantum computer to use the square-root factor and halved the exponent of time complexity in opposite to a linear search algorithm $O(n)$. The Table 1 shows the runtime and cost effort for each algorithm and for the symmetric cryptography Advanced Encryption Standard (AES).

Table 1: Runtime and cost efforts per algorithm.

n	$O(n)$	$O(\sqrt{n})$	$O(\sqrt[3]{n})$
128 bit	128 bit	64 bit	42,66
192 bit	192 bit	96 bit	64
256 bit	256 bit	128 bit	85,33

Furthermore, the Grover's algorithm is useful for attacking the established secure hash algorithm (SHA) to find preimages (Amy et al., 2017) and hash collisions by modifying the algorithm with a cube-root factor (Brassard et al., 1998). In general Grover algorithm is a probabilistic algorithm and tries to achieve a

good or approximately correct average result. To find the right key it makes sense to use this randomized algorithm again on the previous result.

4 PARADIGM OF POST-QUANTUM CRYPTOGRAPHY AND CRYPTO-AGILITY

In terms of special requirements, future-proof cryptography is characterized by the ability to adapt to new technologies and challenges. Today's cryptography achieves this ideal through post-quantum cryptography and crypto-agility. That includes research new cryptographic primitives and ensuring common mechanisms to stable current system environment and the idea to modify security protocols. This will be necessary because the development of quantum computers is an active field of research. Technical guidelines and recommendations for quantum computer resistant cryptographic methods are currently reaching a stage of development, but no standardization yet. According to the current state of research, one can classify symmetric encryption as a quantum computer resistant. The turn-based method (4), as well as the key length (5) of one of its key phrases $|K|$, allows this assumption:

$$|K| = 10/128, 12/192, 14/256 \quad (4)$$

$$|K| = 2^{128}, 2^{192}, 2^{256} \quad (5)$$

These properties make the symmetric scheme resistant to brute-force attacks by a quantum computer. A complete analysis of the keyspace is considered ineffective. An attacker could scan the ciphertext about 4 times faster and break it if he has little plaintext to the ciphertext than to perform an analysis of the keyspace (Bogdanov et al., 2011). Furthermore, the higher the key, the fewer steps are required for decryption. For example, a ciphertext created with AES-192 requires 2^{176} steps for decryption and only $2^{99,5}$ steps for AES-256 (Biryukov and Khovratovich, 2009). Nevertheless, in brute-force attacks of quantum computers on the key space of AES thanks to turn-based methodology and the key length as a quantum-safe. As an alternative to AES, the Camellia procedure recommended by the European ENISA can be used. Both methods are based on block encryption with the same block cipher. Camellia is slower in direct comparison to AES, but uses a block cipher directly of 128 bits for more laps $(18/128, 24/192, 24/256)$. For stream ciphers, the method Salsa20 (Snuffle 2005) with a 256 bit key length could be used. The standard version Salsa20/20 uses an encryption of 20 rounds. The algorithm is extremely efficient and resistant to possible side channel attacks. The Salsa20/12 and Salsa20/8 variants can be used for time-critical as well as jitter- and latency-relevant applications. In contrast to symmetric methods, the asymmetric method is considered non-quantum-safe. Nevertheless, this scheme still needs to be used for key exchange. With asynchronous encryption algorithms, it makes sense to use a RSA key length of ≥ 3000 bits to achieve a security level that can react to possible attacks from quantum computers. In order to attack a ≥ 3000 RSA key a quantum computer must have a few thousand logical Qubits for the mathematical operation. Furthermore, correction or cache Qubits are necessary, which hold intermediate results. To compare, state-of-the-art fully controlled quantum computer operates of 20 Qubits with entangled states (Friis et al., 2018). But it makes sense to search for other public-key alternatives to replace this asymmetric methods. The McEliece method can be used as an RSA alternative, since no quantum algorithm has yet been found that can effectively break this cryptographic method but use of the large matrices for this method is rarely used in practice. Quantum Key Distribution (QKD) is a possible solution for the key exchange. The QKD belongs to quantum cryptography and is a method for secure key exchange. The method guarantees its security with the physical fact of quantum mechanics. This method is not suitable as an encryption method for messages, but for the secure exchange of keys. A man in the middle attacker would have to actively measure the quantum particles. This generates high error rates and measurement inaccuracies on the quantum channel. Furthermore, the charge of the quantum particles would collapse. This gives you physical evidence of safety. With this method even very long symmetric keys can be transmitted in a relatively short time. An application of the Vernam's One Time Pad (OTP) method, which is considered quantum-safe, would be conceivable. ECC equivalents like Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) must be considered broken and not useful for the PQC. Nevertheless, one can provide security protocols with a hybrid procedure. The Supersingular Isogeny Diffie-Hellman (SIDH) is defined as quantum computer resistant and could be a candidate for hybride implementation of ECC with e.g. Montgomery and Twisted Edwards Curves (Boureanu et al., 2014). For digital signature procedures, new such hash-based eXtended Merkle Signature Scheme (XMSS) and SPHINCS can be used for PQC. This hash methods are high-security post-quantum state-

less hash-based signature schemes. The established secure hash algorithm SHA-2/-3 is currently believed secure and quantum computer resistant but not to be resilient and proved. However, the $\geq$ 384 hash value (bit) should already be used for long-term storage. Table 2 illustrates the recommended key length for the cryptographic scheme.

Table 2: Recommended key length and method.

Scheme	Recommendation
AES	256 bit
Camellia	192 bit
Salsa20	256 bit stream chiffre
RSA	$\geq$ 3000 bit
McEliece method	128 bit
SIDH	128 / 192 bit
SHA-2 /-3	256 / 384 Hash value (bit)
XMSS/ SPHINCS	SHA-256 / AES-128

4.1 Post-quantum Cryptography

Increase of the key space alone is not enough to be quantum-safe. For example, If the symmetrical encryption AES was attacked by the Grover quantum algorithm, the key strength would still be 50%. An attack via Shor quantum algorithm on asymmetric algorithms such as RSA or ECC could no longer nearly guarantee the same security that an asymmetric encryption would provide. Even increasing the size of the key space would not be an adequate measure and would also make the cryptographic process inefficient (Fumy, 2017). Table 3 shows the effectively capacity of the key size and key data and define the efficient properties of the established not quantum-safe public-key schemes.

Table 3: Key properties of no quantum-safe schemes.

Key-Length (bit)	Size (bytes)	Data (bytes)
RSA-2048	256	256
RSA-3072	384	384
RSA-4096	512	512
ECC-256	32	32
ECC-512	64	64

The Table 4 shows schemes which are believed quantum-safe and proofed secure level for public-key and key exchange method. This methods operates with a transmitted data capacity that is significant larger then established methods e.g. public-key signatures XMSS (Butin, 2017), SPHINCS (Bernstein et al., 2015) and HFE* (Petzoldt et al., 2015). The same situation with the public-key encryption e.g. the coding-based scheme McEliece (Bernstein et al., 2008) and grid-based scheme NTRU (IEEE, 2008), and the key exchange as well like NewHope (Alkim et al., 2015) and SIDH (Costello et al., 2016).

Table 4: Key properties of quantum-safe schemes.

Key-Length (bit)	Size (bytes)	Data (bytes)
HFE*/PMI*	$\geqq$ 500,000	30
NTRU	$\geqq$ 1,500	$\geqq$ 1,500
McEliece	$\geqq$ 800,000	$\geqq$ 180
SIDH	n/a	$\geqq$ 500
XMSS	64	$\geqq$ 2,000
SPHINCS	$\geqq$ 1,000	$\geqq$ 40,000

However, the challenge is to update the established security protocols and cryptographic methods in a manner that is useful and beware against possible quantum attacks. Here are five potential candidates of quantum-safe primitives.

4.1.1 Multivariate Cryptography

The multivariate cryptography is mathematically based on a quadratic polynomial equation. The functionality is based on the idea that figures on sets of n quadratic polynomials $p_1,...,p_n$ over finite elements K^n with more then n variables $\chi_1,...,\chi_n$ can be represented in different ways. For function P, this results in:

$$K^n \rightarrow \quad K^n \tag{6}$$

$$(\chi_1,...,\chi_n) \rightarrow \quad (p_1(\chi_1,...,\chi_n,...,p_n)(\chi_1,...,\chi_n)) \tag{7}$$

and $P(x)$ can therefore be calculated if $x \in K^n$ applies. The inverse way for a $y \in K^n$, thus a $x \in K^n$ with function $P(x) = y$ by means of a quadratic equation system. The difficulty of this variant and at the same time the safety of the procedure is to solve the equation system, as the following applies:

$$p_1(\chi_1,...,\chi_n) - y_1 \quad = 0 \tag{8}$$

$$p_n(\chi_1,...,\chi_n) - y_n \quad = 0 \tag{9}$$

For encryption the evaluation is performed by a polynomial. Decryption, on the other hand, is performed by the inverse polynomial mapping using knowledge of a mapping structure. The weakness of this procedure lies in the mathematical verifiability as to whether the function P is a one-way function, and to ensure that it is not effectively reversible. But security in cryptographic processes is based on this. Table 5 shows the properties of this method.

Table 5: Character of Multivariate cryptography.

Property	Specification
based on	quadratic equations
methods	HFE, HFEv, HFEv-, PMI+
benefits	efficient, ready for use
disadvantages	mathematically not proven

4.1.2 Grid-based Cryptography

The mathematical approach of grid-based cryptography is based on creating a grid as a discrete subset of a $n-$dimensional real vector space. It is thus divided in a $n-$dimensional space like a grid and divided into a defined number of cells. Each cell contains objects with statistical values such as number, average, deviations, min./max. values. The advantage results from the low complexity, since a runtime does not depend on the contained objects, but only on the cells to be considered. The values for these are saved as soon as the data has been loaded into the cells. Grid-based cryptographic methods are rather limited to solving mathematical problems in such grids e.g. shortest vector problem, close vector problem, Ring-Learning With Errors (Ring-LWE). Thus, for example, the sum of two grid points again results in a grid point in the grid where no other grid point exists. Furthermore, the runtime of the algorithm is exponentially, the more granular the more accurate the number of dimensions of the grid. This generally means that problems on standard grids will cause a strong safety proof but run slower. Problems in ideal grids are used for encryption and decryption at the expense of a low safety proof of runtime efficiency. Table 6 shows the general properties of the common grid-based method. The methods BLISS and Tesla are mentioned as grid-based methods but not presented.

Table 6: Character of Grid-based cryptography.

Property	Specification
based on	Grid calculation
methods	New Hope, Frodo, Kyber, NTRU
benefits	Runtime efficient
disadvantages	No experience by cryptanalysis

A possible compromise would be a procedure based on module grids. However, the proven speed over RSA encryption can be noticed. Furthermore, there are some implementation of security protocols with New Hope that based on grid-based cryptography (Alkim et al., 2015). The NTRU algorithm which is based on the principles of the Ring-LWE problem, requires a runtime of $O(N^2)$ for an encryption/decryption operation of a message of length N, while a conventional RSA method requires a runtime of $O(N^3)$ (Hoffstein et al., 1998). NTRU algorithm is thus depending on the three integer parameters N, p, q and four polynomials $p_1, ..., p_4$ with a degree of $N-1$ and an integer coefficient. The parameters p, q not necessarily need be prime numbers, where $gcd(p,q) = 1$ and $q > p$ apply. Thus, the ring R is calculated as follows if Z is the quantity of the total Numbers:

$$R = Z[X]/(X^N - 1) \tag{10}$$

4.1.3 Coding-based Cryptography

The coding-based cryptography is the oldest approach towards quantum computer resistant public-key methods and is based on the difficulty to decode general error correcting codes efficiently. The binary Goppa code is preferred for this, on which the methods McEliece and Niederreiter are based on. The property of error correction codes is that the decoding algorithm can correct a maximum of errors r, which is encoded and/or transmitted in a ciphertext c:

$$y = c + e \tag{11}$$

If thus e is regarded as error vector to r, one can conclude from y to c. An attacker could not determine c from y in an acceptable time. The basis for the security of the procedure is the secrecy of the decoding matrix. Only the coding matrix from which no conclusions about the decoding matrix can be derived may be published. The Goppa code forms such a large class of algebraic error correcting codes to ensure the security of this procedure. The Goppa code $\Gamma(L, g(z))$ is represented by the Goppa polynomial $g(z)$ having a degree t defined over a finite body having a finite number $GF(q^m)$ in conjunction with a generated matrix G and vector parameters. Based on the Goppa code, the McEliece and Niederreiter methods are used. Table 7 shows the character of this method.

Table 7: Character of Coding-based cryptography.

Property	Specification
based on	Efficient decoding
methods	McEliece, McBits, Niederreiter
benefits	McEliece method well studied
disadvantages	Large public-key, low power

4.1.4 Isogeny-based Cryptography

The isogeny-based cryptography based on the algebraic geometry and describes the state of two groups that produce a structure-preserving image when certain variety properties of a homogeneity are fulfilled. Restricted to cryptography, the elliptic curves form over an algebraically closed body. Thus a morphism of elliptic curves is considered to be isogenic if following is valid:

$$\Phi : E_1 \to E_2 \tag{12}$$

$$\Phi(O) = O \tag{13}$$

If such a Φ exists, then $E_1 \cap E_2$ is called isogenic. Thus, mathematical mappings between elliptical curves are generated, which can be used as a basis for the Diffie–Hellman key exchange (DH). The difficulty lies in finding this isogenies between the elliptic curves. Current implementations of DH are based on isogenies between supersingular elliptic curves such as the Montgomery curves. For example the Supersingular Isogeny Diffie Hellman key exchange (SIDH) is a possible method. Table 8 shows the character of this method.

Table 8: Character of Isogeny-based cryptography.

Property	Specification
based on	Elliptic curves principles
methods	SIDH
benefits	Elliptic curves well-researched
disadvantages	Less researched

4.1.5 Hash-based Cryptography

Cryptographic hash procedures or one-way hash functions are based on the difficulty of calculating hash collisions. Digital signatures are to be issued using collision-resistant hash algorithms such as XMSS (Buchmann et al., 2011) and SPHINCS (Bernstein et al., 2015). Since 2018, a first draft of the IETF standard has been available (Arrow et al., 2018). XMSS procedure is well developed and standardized and offers an efficient calculation runtime, since the signature length and the verification time are linear to the message length and independent of the number of signatures - in contrast to algorithms of signature chains, whose runtime is linear to the number of signatures on the signature length and verification time. The XMSS procedure is based on a stateful hash-based signature scheme, which is mapped on a single or multi tree (hash tree) and is based on the W-OTS+ variant. With the pure OTS procedure, only one message can be digitally signed with a key. With the extended W-OTS+ variant, a limited number of digital signatures can be generated for a XMSS public-key. Thus the secret key must be updated after each signing and the key pair is limited with regard to the signature process. The number of messages m to be signed and verified in a key pair is mathematically dependent on the height H of the hash tree. Thus, the number of 2^H messages applies if:

$$H \in N \tag{14}$$

$$H \geqq 2 \tag{15}$$

Furthermore, the limiting factor of 2^H can be the signature-generating device or a guideline. There is currently no quantum algorithm that allows finding a hash collision in polynomial time, so they are considered to be resistant to quantum computers.

4.2 Crypto-agility

Crypto-agility describes the ability to continue using existing cryptographic methods and security protocols with adapting for PQC. Non quantum resistant cryptographic algorithms will be replaced PQC proved algorithms. Furthermore, there is the need to achieve an affinity to modifying cryptographic systems by manufacturers. Proactive adapting and continuous improvement of the cryptographic methods and security protocols are the effectively countered against the quantum attacks. Three examples with X.509v3, Secure / Multipurpose Internet Mail Extensions (S/MIME) and Secure Shell (SSH) show a possible approach of crypto-agility.

4.2.1 Modifying X.509v3 Certificate

The X.509v3 certificate is a compilation of generally valid data formats and algorithms and not a native security protocol. The integral components of the X.509v3 certificate are Secure Socket Layer/Transport Layer Security (SSL/TLS), S/MIME and Extensible Markup Language (XML) Digital Signatures. Based on the format description and the data structure of the X.509v3 certificate a Public-Key-Infrastructure (PKI) specification can be defined to access digital certificates with quantum resistant algorithm. There is no need to adapt the RFC compliant standards. However, further adjustments must be made at the security protocol level, such as upgrading the TLS version to version 1.3 to ensure a hybrid approach. Furthermore, the very large key room for the public-key must be reckoned to realized the protection against quantum attack (Campagna et al., 2015).

4.2.2 Modifying S/MIME Protocol

The S/MIME protocol is used via the PKI procedure to ensure that digital signatures guarantee authentication, data integrity, binding nature and secure e-mail encryption. A similar scheme and protocol is Open Pretty Good Privacy (OpenPGP), which is based on Web of Trust (WOB). To generate and verify a key pair, a digital signature is required for S/MIME version 3.2, which requires an asymmetric key of at least 1024 bits. The asymmetric algorithms Digital Signature Algorithm (DSA), RSA and RSA Probabilistic Signature Scheme (RSA-PSS) with SHA-256 each are available. The content of the message is executed with the symmetric algorithm AES. Thus the content is secure against quantum algorithms with

AES encryption, but the key exchange is not quantum computer resistant. Note that the S/MIME protocol supports extended key sizes and encryption methods. Thus, the signature and key generation of the S/MIME protocol can be updated with quantum computer resistant algorithms. Therefore, the S/MIME protocol supports elliptic curve algorithms for Cryptographic Message Syntax (CMS), which is compatible with the Public Key Cryptography Standards#7 (PKCS#7) certificate regarding to data format. The implementation of CMS is possible for most applications. The strength of the security comes from the encapsulation. Furthermore, many security features are based on the parameters of CMS, which allow the modification and selection of algorithms. Some S/MIME versions prior to version 3.2 may only use RSA (Campagna et al., 2015).

4.2.3 Modifying SSH Protocol

The SSH architecture consists of TLS, a user authentication protocol and a connection protocol, each of which uses its own algorithm in different network layers. The TLS protocol ensures the protection goals of confidentiality, authentication and integrity and can be designed to be quantum-safe by a parameterized adaptation. In contrast, the user authentication and connection protocol with its cryptographic primitives such as RSA, Digital Signature Algorithm (DSA), ECDSA is not quantum secure. Fundamentally, however, the SSH protocol is cryptographically agile, since the SSH TLS protocol negotiates the first algorithm for key exchange between client and server when a connection is to be established. Thus, a quantum-safe algorithm can be used for key exchange, if the protocol flexible enough to cover the properties and requirements of PFS. Furthermore, the use of the non-quantum-safe signature algorithms DSA, ECDSA and RSA Probabilistic Signature Scheme (RSASSA-PSS) for the authentication of the host can be replaced by quantum-safe digital signatures. Thus, the standard as specified in RFC 4253 does not need to be fundamentally changed when making the appropriate modifications to the SSH protocol and its underlying layers (Campagna et al., 2015). The adapting already existing encryption methods is a common way to be quantum-safe.

5 RESULTS

It generally applies: Without any proof that a cryptographic algorithm via quantum algorithm is vulnerable or to broken by a quantum attack, a cryptographic method could be with sufficient research presumed to be quantum attack resistant. Furthermore, every cryptographic algorithm that based of mathematical complexities like factorization and discrete logarithms are believed as broken from the perspective of quantum computer. This applies also to all security protocols that use thus cryptographic algorithm. Typical asymmetric encryptions such as RSA, ECC, public key methods and their security protocols are not considered PQC ready. The asymmetric method can only react to potential quantum attacks by increasing the size of the key. Furthermore, the security of the method and the key length can be guaranteed until the next quantum attack and is dependent on the next higher quantum computer generation. However, a large RSA or ECC key affects the transfer of the key. Cryptosystems which based on symmetric encryption like AES are considered quantum resistant because the method is turn-based and the key size can be increased. The common security protocols, cryptosystems and applications use public-key method for the key exchange and symmetric key for the data payload. In order to be quantum-safe the public-key method must be adapted by PQC approved cryptographic algorithm and method. Furthermore, it must be ensure that all security protocols are easy to substituted and be cryptographic agility. The research for new cryptographic primitives compliment the strategy of crypto-agility and post-quantum cryptography.

6 CONCLUSIONS

At present, no quantum computers can break established encryption. Furthermore, the perception of the feasibility of a quantum computer is becoming more concrete and this is the reason why it is comprehensible that quantum computer has such an enormous impact on all areas of our society. The further development of quantum algorithms are no longer just a topic for universities or institutions of research and teaching. Especially larger IT companies such as Google, IBM, Microsoft, etc. are investing a great deal of time and effort in creating a powerful quantum computer. Just because we are currently still secure with our established encryption mechanisms does not mean that we do not have the cryptographic future to plan. It must rather be accompanied by the timely and parallel development of the quantum computer and the same procurement of resources.

REFERENCES

Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2015). Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092.

Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., and Schanck, J. (2017). Estimating the cost of generic quantum pre-image attacks on sha-2 and sha-3. In Avanzi, R. and Heys, H., editors, *Selected Areas in Cryptography – SAC 2016*, pages 317–337, Cham. Springer International Publishing.

Arrow, A., Butin, D., Gazdag, S., Rijneveld, J., and Mohaisen, A. (2018). Xmss: extended merkle signature scheme. Request for Comments rfc8391, Corporation of TU Darmstadt, Radboud University, University of Central Florida, genua GmbH.

Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., and Wilcox-O'Hearn, Z. (2015). Sphincs: Practical stateless hash-based signatures. In Oswald, E. and Fischlin, M., editors, *Advances in Cryptology – EUROCRYPT 2015*, pages 368–397, Berlin, Heidelberg. Springer Berlin Heidelberg.

Bernstein, D. J., Lange, T., and Peters, C. (2008). Attacking and defending the mceliece cryptosystem. In Buchmann, J. and Ding, J., editors, *Post-Quantum Cryptography*, pages 31–46, Berlin, Heidelberg. Springer Berlin Heidelberg.

Biryukov, A. and Khovratovich, D. (2009). Related-key cryptanalysis of the full aes-192 and aes-256. In *Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '09, pages 1–18, Berlin, Heidelberg, Germany. Springer-Verlag.

Bogdanov, A., Khovratovich, D., and Rechberger, C. (2011). Biclique cryptanalysis of the full aes. In *Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security*, ASIACRYPT'11, pages 344–371, Berlin, Heidelberg, Germany. Springer-Verlag.

Boureanu, I., Owesarski, P., and Vaudenay, S., editors (2014). *Applied Cryptography and Network Security - 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings*, volume 8479 of *Lecture Notes in Computer Science*, Berlin, Heidelberg, Germany. Springer.

Brands, G. (2011). Einführung in die quanteninformatik. In *Quantenkryptografie, Teleportation und Quantencomputing*, pages 17–18, Berlin, Heidelberg. Springer Berlin Heidelberg.

Brassard, G., HØyer, P., and Tapp, A. (1998). Quantum cryptanalysis of hash and claw-free functions. In Lucchesi, C. L. and Moura, A. V., editors, *LATIN'98: Theoretical Informatics*, pages 163–169, Berlin, Heidelberg. Springer Berlin Heidelberg.

Buchmann, J., Dahmen, E., and Hülsing, A. (2011). Xmss - a practical forward secure signature scheme based on minimal security assumptions. In Yang, B.-Y., editor, *Post-Quantum Cryptography*, pages 117–129, Berlin, Heidelberg. Springer Berlin Heidelberg.

Butin, D. (2017). Hash-based signatures: State of play. *IEEE Security Privacy*, 15(4):37–43.

Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J. K., Gisin, N., Hayford, D., Jennewein, T., Lütkenhaus, N., Mosca, M., Neill, B., Pecen, M., Perlner, R., Ribordy, G., Schanck, J. M., Stebila, D., Walenta, N., Whyte, W., and Zhang, Z. (2015). Quantum safe cryptography and security: An introduction, benefits, enablers and challengers. Technical report, ETSI (European Telecommunications Standards Institute).

Costello, C., Longa, P., and Naehrig, M. (2016). Efficient algorithms for supersingular isogeny diffie-hellman. In Robshaw, M. and Katz, J., editors, *Advances in Cryptology – CRYPTO 2016*, pages 572–601, Berlin, Heidelberg. Springer Berlin Heidelberg.

Eckert, C. (2014). *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. De Gruyter Oldenbourg, Munich, 9nd edition.

Friis, N., Marty, O., Maier, C., Hempel, C., Holzäpfel, M., Jurcevic, P., Plenio, M. B., Huber, M., Roos, C., Blatt, R., and Lanyon, B. (2018). Observation of entangled states of a fully controlled 20-qubit system. *Phys. Rev. X*, 8:021012.

Fumy, W. (2017). Quantencomputer und die zukunft der kryptographie. *Datenschutz und Datensicherheit*, 41(1):13–16.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA. ACM.

Grover, L. K. (1999). Quantum computing. *The Sciences*, 39(4):24–30.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). Ntru: A ring-based public key cryptosystem. In Buhler, J. P., editor, *Algorithmic Number Theory*, pages 267–288, Berlin, Heidelberg. Springer Berlin Heidelberg.

IEEE (2008). Ieee draft standard specification for public-key cryptographic techniques based on hard problems over lattices. *IEEE Unapproved Draft Std P1363.1/D12, Oct 2008*.

Petzoldt, A., Chen, M.-S., Yang, B.-Y., Tao, C., and Ding, J. (2015). Design principles for hfev- based multivariate signature schemes. In Iwata, T. and Cheon, J. H., editors, *Advances in Cryptology – ASIACRYPT 2015*, pages 311–334, Berlin, Heidelberg. Springer Berlin Heidelberg.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509.