Chapter 20
Post-quantum Cryptography in 6G

This is author's version. Original to appear in Wu Y., Singh S., Taleb T., Roy A., Dhillon H. S., Kanagarathinam M. R., De A. (ed.), *6G Mobile Wireless Networks*, Springer.

Juha Partala

Abstract The quantum computing paradigm is fundamentally different from the classical one. There are computational problems we are not able to solve on a contemporary computer, but which we can efficiently solve on a quantum one. One of these problems is the discrete logarithm problem (DLP) which is the basis of modern asymmetric cryptography. Once large-scale quantum computing becomes a reality, these cryptographic primitives need to be replaced with quantum-secure ones. While we are still in the early stages of quantum computing, steps have been taken to prepare for the shift to cryptography that is secure in the post-quantum world. According to the current knowledge, contemporary symmetric cryptography remains secure for the most part even after the advent of quantum computing. Asymmetric primitives based on integer factorization and the DLP need to be replaced. In this chapter, we take a look at the post-quantum secure alternatives for key establishment, public-key encryption and digital signatures. We also discuss their properties and the effect on the performance of the future 6G networks.

Keywords: cryptography, quantum computing, public-key cryptography, post-quantum security

1 Introduction

Quantum computing has drawn a lot of interested in the last years. Development has been rapid and commercial devices have been predicted to be available already in the near future [7]. Quantum computing will have a dramatic effect on modern cryptographic algorithms. The security of these algorithms is based on the hardness

Juha Partala
Center for Machine Vision and Signal Analysis
University of Oulu, Finland
e-mail: firstname.lastname@oulu.fi

of specific computational problems. However, it seems that certain problem types are much easier to solve on a quantum computer than on a contemporary one. While we are still in the early stages of quantum computing and large-scale quantum computing can be expected to take a decade or more, steps have been taken to prepare for the shift to cryptography that is secure when quantum computing is a reality.

The sixth generation of communication networks are envisioned to provide nearly unlimited wireless connectivity, ultra-high reliability and ultra-low latency, as well as to be dependable even for critical applications such as eHealth [10]. Computations will be performed on the edges of the network to reduce latency requiring complex trust mechanisms. These properties will place complicated requirements for the network security architecture. In order that the envisioned properties of 6G are realizable in practice, several research questions relating to network security need to be solved [16]. It is evident that the complex security mechanisms of 6G will be based on both symmetric and asymmetric cryptography and quantum computing will affect those mechanisms. Even though security can be achieved against quantum computing, there will be a penalty to efficiency. It will not be straight-forward to satisfy currently envisioned requirements of 6G with quantum secure algorithms.

In this chapter, we take a look at the current status in quantum secure cryptography. We briefly introduce basic concepts of cryptography, such as symmetric and asymmetric primitives and the computational problems underlying contemporary asymmetric cryptography. We also take a look at the recent successes in quantum computing and its predicted development in the future. In the United States, the National Institute of Standards and Technology (NIST) is currently hosting a selection process called NIST PQC for a post-quantum cryptography standard. These primitives will provide post-quantum secure key exchange, public-key encryption and digital signatures in a standardized way. We describe the cryptographic primitives in the current stage of the competition and discuss their properties and efficiency in regard to 6G.

The chapter is organized as follows. First, we introduce the basic concepts of cryptography and quantum computing in Sect. 2. Section 3 is devoted to recent developments in quantum computer engineering. The development in the application of cryptography towards 6G is laid out in Sect. 4. Section 5 describes the state-of-the-art alternatives for post-quantum secure key establishment, public-key encryption and digital signatures. Finally, Sections 6 and 7 provide the discussion and conclusion.

2 Cryptography and Quantum Computing

2.1 Cryptography

Cryptography studies techniques for securing transactions, information and computations. It encompasses fundamental techniques for modern communications such as confidentiality, message integrity, key exchange and digital signatures. The security of cryptographic schemes is based on the assumed infeasibility of specific compu-

tational problems. First, a rigorous and precise definition of security is formulated. Based on the security definition, a cryptographic algorithm is proven to satisfy it by reducing an infeasible problem to the problem of breaking the algorithm. That is, if an adversary is able to violate the security of that algorithm, he/she is able to also solve the hard computational problem. Therefore, a cryptographic algorithm can be at most as secure as the underlying problem and a lot of research is devoted into the study of those problems.

Cryptography can be roughly divided into two classes:

1. Symmetric cryptography, where communication participants share a secret key. This class contains classical cryptographic primitives such as stream and block ciphers, cryptographic hash functions and message authentication codes. Symmetric cryptography always requires a trusted channel to establish the shared secret key.
2. Asymmetric cryptography, also called public-key cryptography, does not require a shared secret key. Instead, a private and public key pair is used. This class contains, for example, key exchange schemes to establish shared keys for symmetric primitives, public key encryption and digital signatures. Of the key pair, only the private key is kept secret. The public key can be used, for example, to encrypt a message intended to the owner of that key or to verify digital signatures. The private key is needed, for example, to decrypt or to generate signatures.

Asymmetric cryptography is more susceptible to quantum computing and we will mostly concentrate on it. Regarding the solvability of computational problems, polynomial time computation is typically viewed as feasible computation. If an algorithm finishes in polynomial time with respect to the length of its input, then it can be also executed in practice. A problem that cannot be solved in polynomial time is generally considered to be infeasible.

Every non-prime integer n can be factored into a product of smaller integers. The problem of factoring arbitrary integers has proved out to be hard and no polynomial-time classical algorithm is known. Integer factorization is the underlying computational problem of several asymmetric cryptographic schemes. These schemes include, most notably, the RSA public-key encryption scheme [14]. Another well-known computational problem is the discrete logarithm problem (DLP) in finite cyclic groups. The DLP asks to find an integer x given g^x, where g is a generator of the group. It underlies another widely used class of asymmetric schemes: those based on the Diffie-Hellman key exchange scheme [3]. The original scheme applies modular arithmetic and no polynomial-time classical algorithm is known for the DLP on such groups. ElGamal public-key encryption and the Digital Signature Algorithm (DSA) also apply the DLP. The problem seems to be even harder on cyclic groups based on elliptic curves and the so called elliptic curve DLP (ECDLP). Currently, the elliptic curve based Diffie-Hellman scheme is the most efficient key exchange scheme available when considering both key length and performance.

2.2 Quantum Computing

Quantum computing is based on quantum bits, *qubits*. Unlike ordinary bits that can be either in state 0 or 1, qubits can be in a superposition (a linear combination with complex coefficients) of these two states. Furthermore, multiple qubits can be entangled meaning that the quantum state of a single qubit cannot be described independently of the others. Similarly to ordinary computers, operations can be carried out on the qubits. In the quantum circuit model, reversible transformations are applied to construct quantum logic gates. Such gates can then be connected into a circuit performing an arbitrary computation thus implementing a quantum computer. Other equivalent models of computing, such as adiabatic or measurement based quantum computing, also exist. However, our discussion will be based on the quantum circuit model.

Computational problems that are solvable on a contemporary computer can be also solved on a quantum one. The converse is also true. Any problem solvable on a quantum computer is also solvable on an ordinary one. However, the superposition of entangled qubits facilitates an exponential speedup on solving specific problem types compared to the classical model of computation. This means that while any computation can be performed on both types of computers, in practice certain problems seem to be much easier in the quantum computing model. However, the number of entangled qubits is the enabling factor of such algorithms. The algorithm can be executed and finished fast if and only if enough qubits are available. Therefore, the number of qubits that we can entangle and keep coherent determines whether we can consider a specific problem feasible in practice.

Quantum computing affects both classes of cryptography but not in equal measure. Symmetric cryptography survives for the most part. However, asymmetric primitives in wide use need to be updated. There are two important quantum algorithms that affect cryptography: Grover's algorithm and Shor's algorithm. The former affects both symmetric and asymmetric schemes, while the latter targets asymmetric schemes.

2.2.1 Grover's Algorithm

Let f be an injective function with N different inputs and suppose that we are only able observe the input and output behavior of f. That is, f is viewed as a black box. In order to find a secret input to f, we need to make $O(N)$ queries into the black box in the worst case, since our last try could be the right value. In the quantum computing paradigm, the secret value can be found faster. Grover's algorithm finds the secret value on a quantum computer in time $O(\sqrt{N})$ [6], which also seems to be optimal [1]. This may seem only a quadratic improvement, but it is significant in practice.

Grover's algorithm affects both symmetric and asymmetric schemes. For example, due to the quadratic speedup, symmetric 128-bit encryption can be broken in approximately 2^{64} steps and 256-bit encryption in 2^{128} steps. In general, this means that the key length of any cryptographic scheme needs to be at least doubled to

maintain the current level of security in the quantum computing model. The lowest security options, such as AES-128, will be rendered obsolete in the post-quantum era. However, the higher security versions, such as AES-196 and AES-256 will remain secure with a lower security level. The same is true for any other symmetric primitive applying a secret key such as message authentication schemes.

Regarding cryptographic hash functions, the Grover's algorithm applies to the problem of finding preimages. In the quantum model, preimage resistance is halved. However, due to the birthday attack and its effect on the collision-resistance of hash functions, the digest length is already on an adequate level. The birthday attack is a classical algorithm that finds a collision (m_1, m_2) such that $H(m_1) = H(m_2)$, where H is a cryptographic hash function, in $O(\sqrt{N})$ steps. Due to the birthday attack, message digests computed using cryptographic hash functions need to have a length that is at least double of the security parameter. That is, to have a security level of 128 bits against collisions, the digest has to be 256 bits. In the quantum computing model, the birthday attack can be theoretically mounted in $O(\sqrt[3]{N})$ steps [2]. However, such an attack would also require $O(\sqrt[3]{N})$ qubits making it infeasible in practice. Quantum algorithms for collision-finding targeting specific hash function constructions also exist [9]. However, to the best of current knowledge, hash function security remains largely unaffected in the quantum computing model.

2.3 Shor's Algorithm

Shor's algorithm is a quantum algorithm for factoring integers in polynomial time [15]. On a classical computer, the fastest algorithm for integer factorization is sub-exponential time. Therefore, integer factorization represents a practical separation of the traditional and quantum computing models. Due to the polynomial time solvability of factoring, RSA is not secure in the quantum circuit model. The DLP can be also solved in polynomial time using Shor's algorithm for both the original modular aritmetic based groups and the elliptic curve groups.

The practical solvability of the factoring problem and the DLP on a quantum computer depends on the security parameter. For example, when solving the DLP on the group of multiplication modulo a prime p, $\mathbb{Z}_p^*$, where p is an n-bit prime, Shor's algorithm needs at least $2n + 3$ qubits. The same is true for factorization. For the ECDLP, there exists an algorithm using at most $5n+8\sqrt{n}+4\lceil\log_2 n\rceil+10$ qubits [13]. Therefore, the deciding factor in the future security of the DLP and factoring-based schemes is the development of the number of qubits. NIST recommendations for the binary length of the composite n for factoring based schemes or for the prime p for the DLP and ECDLP based schemes together with the minimum number of required qubits have been collected into Table 1 and Table 2. Note that factoring and modular multiplication based cryptography is more secure than elliptic curve cryptography with these parameter choices in the quantum computing model.

Table 1 The required bit length of the composite integer n for factoring based schemes and that of the prime modulus p for DLP based schemes using a specific security level. On the right, the minimum number of qubits required to solve the corresponding instance in polynomial time on a quantum computer

Security Parameter [bits]	Factoring and DLP [bits]	Number of Qubits
80	1,024	2,051
112	2,048	4,099
128	3,072	6,147
196	7,680	15,363
256	15,360	30,723

Table 2 The required bit length of the prime p of the underlying finite field for the elliptic curve DLP. On the right, the minimum number of qubits required to solve the corresponding ECDLP in polynomial time on a quantum computer

Security Parameter [bits]	ECDLP [bits]	Number of Qubits
80	160	944
112	224	1,282
128	256	1,450
196	384	2,124
256	512	2,788

3 Development of Quantum Computing

In order to build a physical quantum computer using the quantum circuit model, five requirements need to be met [4]:

1. We need a scalable physical system, where the qubits are instantiated.
2. We have to be able to initialize and reinitialize the system into an initial state, where the qubits are entangled with each other.
3. The entangled qubits need to stay in coherence long enough in order to perform meaningful computations. Coherence means that the qubits remain entangled with each other and do not get interfered or entangled with, for example, the environment thus ruining the computation.
4. There has to be a universal set of quantum gates that can be implemented in practice to be able to carry out arbitrary computations.
5. We have to be able to measure the qubits to read out the result of the computation.

Solving these engineering problems is not easy in practice. For example, decoherence of the qubits is easily caused by interaction with the outside environment. In fact, decoherence and noise are the limiting factors of contemporary quantum computation. Novel methods and development in quantum error correction among other things are needed before large-scale quantum computing is possible.

Despite the numerous engineering challenges, quantum computing has progressed rapidly during the last decade and the development in the number of qubits has been

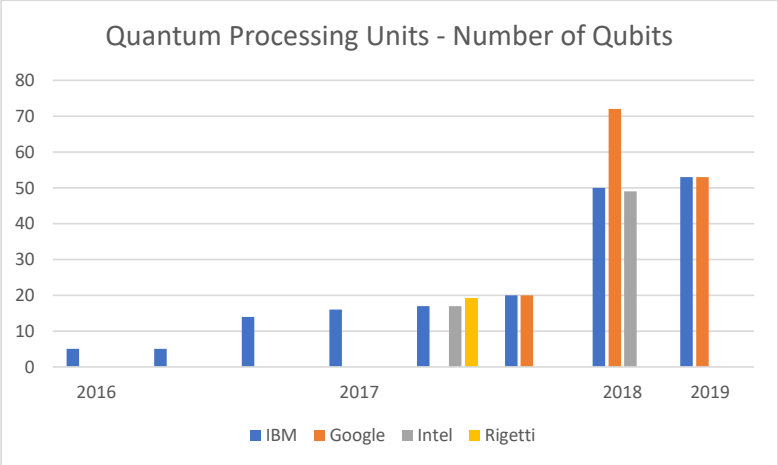

Fig. 1 Development in the number of qubits in published quantum processing units. However, it should be noted that development in coherence and other factors influencing computability are not reflected in this chart

especially rapid in the last five years. In 2020, state-of-the-art quantum computing processors can practically operate on 53 qubits. Such processors have been published by IBM and Google. In 2019 Google announced that it has achieved "quantum supremacy": solving a problem that would be infeasible on a classical computer. Notable published quantum processing units from IBM, Google, Intel and Rigetti Computing and their respective qubit lengths have been depicted in Fig. 1. However, it should be noted that the number of logical qubits might be lower than that of physical ones due to errors and error correction. In addition, the coherence times are not the same for all of these computers. These issues are not reflected in the chart. In fact, the number of qubits does not give the full picture. IBM measures the development using a "quantum volume" metric. It is based on the width and depth of a circuit that a quantum computer can successfully compute. In addition to the number of qubits, quantum volume attempts to capture progress in all the five requirements by incorporating, for example, the fidelity of the quantum gates.

Precise predictions on the development of the quantum volume or the number of qubits are obviously impossible to make. However, there are predictions that are based on the rate of development observed during the last decade. At IBM, the current hope is that quantum volume will double annually. There are also other optimistic estimates. The "Neven's Law", which can be considered a quantum analogue of Moore's Law, predicts that quantum computing power experiences a double ex-

ponential growth relatively to classical computing. Naturally, it is impossible to be certain whether these predictions will hold or whether a more modest development will realize. However, based on the recent developments in quantum computing, it makes sense to prepare for the possibility that large-scale quantum computing is a reality in the lifetime of the future 6G networks.

4 Cryptography and the Development Towards 6G

Up to the 4th generation, as well as in the currently implemented 5G, authentication is based on symmetric cryptography. A shared key is stored in a Subscriber Identity Module (SIM) card. Functionality of the authentication and key agreement (AKA) protocol in 4G is based on symmetric primitives and authentication is performed only between the user equipment (UE) and the mobility management entity. In 5G, service providers and other third parties need to be also authenticated requiring a more flexible authentication mechanism [5]. In addition, the SIM card methodology does not work well with Internet-of-Things (IoT) devices and therefore alternative methods have been devised. The 5G specification currently includes three authentication protocols: 5G AKA, EAP-AKA and EAP-TLS. The first two are based on symmetric cryptography. However, the third one is based on asymmetric cryptography and has been included, especially, to support IoT environments. The Extensible Authentication Protocol (EAP) supports multiple authentication mechanisms directly on the data link layer. Transport Layer Security (TLS) is a set of cryptographic protocols designed to provide authentication, confidentiality and message integrity and is widely used on the internet.

The current 5G standard does not address the issue of quantum computing. As of August 2020, the standard specifies three ciphers for symmetric encryption and integrity: SNOW 3G, the Advanced Encryption Standard (AES) and ZUC. SNOW 3G and ZUC are stream ciphers, while AES is a block cipher that is used in the counter mode for encryption. Message integrity is provided using the same three algorithms with AES applied in the CMAC mode. The standard defines the key lengths to be 128 bits for each of these algorithms for both encryption and message integrity. However, as we have observed before such a length is not sufficient in the quantum computing model. Authentication in TLS is based on certificates and a public-key infrastucture (PKI). The inclusion of EAP-TLS into 5G makes the internet and its PKI an integral part of the wireless communication architecture and will be inherited into 6G. In fact, the core network of 5G will be implemented as a set of microservices communicating over the internet. The development towards internet technologies is expected to continue in 6G and future generations.

It is envisioned that 6G will constitute the main boundary that connects the digital world to the physical world. Critical applications, such as remote health monitoring, are envisioned to be built based on the connectivity of the 6G network. The development towards cloud and edge native infrastructures that started in 5G is expected to continue in 6G. Virtualization and software-defined functionality

will increase. Computations will be performed both in the cloud and on the edge of the network to reduce latency. The importance of the robustness of the trust mechanisms will increase as cyber attacks could even endanger the physical safety of the individuals. The number of Internet-of-Things (IoT) devices will drastically increase. The security of the core network of 6G will also depend heavily on the security of the internet and its security mechanisms such at TLS.

TLS and the PKI have been built using asymmetric cryptography that does not satisfy post-quantum security. However, there are efforts towards standardized post-quantum secure cryptography. These efforts are heavily influenced by the importance of TLS. In fact, the suitability of a particular scheme as a replacement for elliptic curve primitives in TLS will be one of the most important deciding factor which post-quantum secure scheme will eventually be standardized. We shall take a look at the post-quantum alternatives and their characteristics in the next section.

5 Post-quantum Secure Asymmetric Cryptography for 6G

There are public-key primitives that are generally considered to be quantum-safe. These include classic methods such as the McEliece cryptosystem [11] and NTRU [8]. These schemes have survived decades of attacks both in the classical and quantum models and can thus be considered post-quantum secure. However, compared to ECDLP based schemes, efficiency may be poor or the key sizes big. In the recent years, a lot of research has been devoted into the design of efficient post-quantum secure cryptography and standardization efforts are ongoing. The NIST PQC competition for a post-quantum cryptography standard is expected to provide post-quantum secure key exchange and public-key encryption, as well as to augment the Digital Signature Standard (DSS).

In 2020, the competition is in its third round and is expected to yield a standardized set of quantum-secure public-key primitives at the latest after the fourth and final round in 2024. Currently, there are four key exchange schemes and three digital signature schemes considered as finalists in round three and will be considered for standardization already after the third round is over. In addition, eight algorithms have been chosen as alternatives and may be included into the standard after the fourth round. Although there are other standardization efforts, the attention of the cryptographic community is currently fixed on the NIST competition. Therefore, current state-of-the-art results are reflected in its outcomes. It can be argued that the schemes chosen to advance into the third round will offer the best security-performance trade-off and thus will be the main contenders for post-quantum secure 6G. In the following, we briefly describe and analyze these schemes regarding their security assurance, efficiency in key generation, encryption/signing and decryption/verification performance. In addition, we take a look at the private and public key lengths, as well as at the length of the ciphertexts. These parameters will affect the performance of the security protocols and 6G communications.

5.1 Key Establishment and Public-key Encryption

Post-quantum secure key establishment methods (KEMs) and public key encryption algorithms attempt to replace the Diffie-Hellman key exchange scheme and the RSA cryptosystem. In the general case, public-key encryption schemes are required to satisfy a well-established security definition of indistinguishability under an adaptive chosen message attack (IND-CCA2). For the ephemeral use cases, indistinguishability under the chosen plaintext attack (IND-CPA) is sufficient. In the following, we describe the NIST PQC third round finalists and the alternative schemes for KEMs and public key encryption. The security assurance, as well as the key and ciphertext lengths have been collected into Table 3. Here, the security is evaluated as the relative assurance on the security of the underlying problem, as well as on the supplied security proofs. It should be noted that some problems have been under attack for decades, while others are more recent suggestions. The performance of the reference implementations on Intel architecture can be found in Table 4. The numbers in these tables have been collected from the official webpages and documents of the NIST submissions.

5.1.1 Classic McEliece

The McEliece scheme is based on the original McEliece cryptosystem from 1978 [11]. Its security is based on the NP-hardness of decoding a random linear code. A private key includes the generator matrix of a Goppa error-correcting code and a public-key is derived by scrambling the generator matrix. Due to its long history, the McEliece cryptosystem and its underlying problem has been extensively studied and can thus be considered a conservative, secure choice for post-quantum security. The private and public keys are very large; in several millions of bits for secure parameters in the quantum setting. The ciphertext size is very small and encryption and decryption are efficient, making McEliece a good choice for scenarios where public keys do not need to be generated and exchanged often.

5.1.2 CRYSTALS-Kyber

CRYSTALS is a cryptographic suite that contains the key-encapsulation mechanism Kyber, as well as the digital signature scheme Dilithium. CRYSTALS is based on module lattices and the Module Learning With Errors (MLWE) problem thought to be hard even on a quantum computer. The Learning With Errors (LWE) is a well-studied problem and can be considered secure. The MLWE problem is younger and not as well-studied. However, no algorithms attacking the MLWE that would not apply to the LWE have been found.

Kyber has a simple specification and enables relatively easy adjustment of the security parameter even for optimized implementations. In the current specification, key lengths for 128-bit security (Kyber-768) are 2,400 bytes for the private key,

1,184 bytes for the public-key and 1,088 bytes for the ciphertext. According to NIST, performance is good for most applications. CRYSTALS-Kyber is one of the structured lattice schemes in the third round of the competition and at most one of those is planned to be selected for the standard.

5.1.3 NTRU

NTRU is another structured lattice scheme originally suggested already in the 1990s [8]. Its security is based on the problem of factoring polynomials and depends on the shortest vector problem (SVP) in a lattice. Contrary to the other structured lattice schemes remaining in the competition, NTRU is not based on the LWE problem. Although previously patented, NTRU is currently in the public domain. Due to its age, NTRU is a well-established scheme and has been already standardized by IEEE (IEEE P1363.1), as well as the American National Standards Institute (ANSI) for financial services (X9.98). It has been studied for over 20 years and, therefore, its security can be considered to be on a stronger foundation compared to the other lattice schemes. For the lowest parameter set `ntruhps2048509` designed to offer 128 bits of security, the private key is 935 bytes and the public key and the ciphertext are both 699 bytes. Encryption and decryption are fast. However, performance is not on the level of Kyber or Saber. Key generation is costly compared to the other lattice schemes.

5.1.4 Saber

Saber is a structured lattice scheme based on the the Module Learning With Rounding (MLWR) problem. It is a variant of the MLWE problem, where errors have been replaced by rounding. The algorithm has been designed to be simple, flexible and efficient. Only power-of-two integer moduli are used making secure software and hardware implementation easier. The MLWR problem is relatively new and the security of Saber cannot be currently reduced to the MLWE problem, which NIST sees as a mild concern. For the lowest security level, private keys are 992 bytes, public keys are 672 bytes and the ciphertext length is 736 bytes. Saber offers the best performance among the lattice-based finalists of round three.

5.1.5 Alternate candidates

In addition to the three finalists, five schemes were chosen to advance to the third round as alternatives. The schemes may be standardized later. The alternative schemes are the following.

1. **BIKE** is a code-based scheme similar to McEliece. Specially structured codes are applied to offer a more balanced performance that approaches that of the lattice-

Scheme	Security	Private key [bytes]	Public-key [bytes]	Ciphertext [bytes]
Classic McEliece	+++++	6,452	261,120	128
CRYSTALS-Kyber	+++	1,632	800	736
NTRU	++++	935	699	699
SABER	+	992	672	736

Table 3 Security and the private and public key lengths, as well as the ciphertext length of the third round finalists of the NIST PQC for post-quantum key establishment and public-key encryption (lowest security level)

Scheme	Key Generation [cycles]	Encryption [cycles]	Decryption [cycles]
Classic McEliece	93,309,536	44,576	132,452
CRYSTALS-Kyber	118,044	161,440	190,206
NTRU	12,506,668	761,236	1,940,870
Saber	98,000	139,000	151,000

Table 4 Performance of the third round finalists of the NIST PQC for post-quantum key establishment and public-key encryption (lowest security level, Intel Haswell architecture)

based schemes. However, due to the added structure, the security assurance is lower than for McEliece.

2. **FrodoKEM** is a lattice based scheme that applies the original LWE problem. The LWE problem is the most-studied computational primitive regarding lattice cryptography. Therefore, FrodoKEM can be considered to offer better security guarantees than the structured lattice schemes. However, performance is worse compared to the structured schemes.
3. **HQC** is a code-based scheme with security based on the quasi-cyclic syndrome decoding with parity problem. It has a good security assurance, but the public key and ciphertext lengths are bigger than those of BIKE.
4. **NTRU Prime** consists of two lattice-based schemes. One of these is based on the assumptions of the original NTRU, while the other is inspired by the RLWE problem.
5. **SIKE** follows a completely different approach than the previous schemes. Its security is based on the hardness of computing isogenies of elliptic curves, the supersingular isogeny Diffie-Hellman (SIDH) problem. It has the smallest public keys and ciphertexts of the described schemes. However, the performance is worse than most of the other schemes and the SIDH problem is still less-studied than the other problems.

5.2 Digital Signatures

Post-quantum digital signature schemes are designed to replace or augment the Digital Signature Standard (DSS). Methods in the competition are required to satisfy existential unforgeability under an adaptive chosen message attack (EUF-CMA). In the following, we describe the three third round finalists for post-quantum digital

Scheme	Security	Public-key [bytes]	Signature [bytes]
CRYSTALS-Dilithium	+++	1,184	2,044
Falcon	+++	897	657.38
Rainbow	+	148,500	64

Table 5 Security assurance and public key and signature lengths of the third round finalists for post-quantum digital signatures (lowest security level)

Scheme	Key generation [cycles]	Signing [cycles]	Verification [cycles]
CRYSTALS-Dilithium[1]	242,532	1,058,483	272,800
Falcon[2]	26,136,000	814,464	158,040
Rainbow[3]	1,302,000	601 000	350,000

Table 6 Performance of the third round finalists for post-quantum digital signatures (lowest security level, Intel architecture)

signatures in the NIST PQC competition, as well as the alternative schemes that were also advanced to the third round. The security assurance, as well as the public key and signature lengths have been collected into Table 5. As with the key esblishment schemes, the security is evaluated as the relative assurance on the security of the underlying problem, as well as on the supplied security proofs. The performance of the reference implementations can be found in Table 6. The numbers in these tables have been collected based on the documents of the submissions to the NIST PQC.

5.2.1 CRYSTALS-Dilithium

Dilithium is a lattice based digital signature scheme based on the same cryptographic suite CRYSTALS underlying the Kyber key establishment scheme. The security is based on the MLWE problem. The scheme has been designed to be easy to implement securely and efficiently by applying the same parameter set for all security levels. For the same reason, contrary to many other lattice based digital signatures, randomness is generated solely using the uniform distribution which is easy to implement regardless of the platform. Dilithium has good performance regarding key generation, signing and verification and performs well in real world situations. The key and signature lengths are also relative small for a post-quantum scheme; for the lowest security level, the public key is 1,184 bytes and a signature 2,044 bytes.

It should be noted that only one of the lattice based digital signature schemes will be included into the standard.

[1] Haswell architecture

[2] Skylake architecture using the native floating point hardware (SSE2)

[3] Skylake architecture

5.2.2 Falcon

Falcon is another lattice based digital signature scheme and therefore a contender with Dilithium to be standardized. The security of Falcon is based on the Short Integer Solution (SIS) problem over the same lattice structure to NTRU. Compared to Dilithium, Falcon is more complex to implement securely due to floating point operations and Gaussian sampling. Due to the application of NTRU lattices, signatures are shorter than for other lattice schemes. For the lowest security level, public keys are 897 bytes and the signatures 657.38 bytes. Signing and verification are also efficient and scale well when security is increased. However, similar to NTRU, key generation is less efficient. Table 6 lists the performance of the Falcon reference implementation on the Intel Skylake architecture with the hardware floating point operations provided by the SSE2 instruction set [12].

5.2.3 Rainbow

Rainbow follows a different approach compared to the other third round finalists. It is a digital signature scheme based on multivariate polynomials. The underlying construction is a so called multi-layered unbalanced Oil-and-Vinegar scheme. The construction is not as well-studied as the underlying problems of the lattice schemes. Rainbow signatures are small, down to 64 bytes (512 bits) for the lowest security level. However, public keys are large with 148,500 bytes for the same level. Table 6 lists the performance of the Rainbow reference implementation on the Intel Skylake architecture without special instructions. However, if the AVX2 vector instructions are available, performance can be increased by over 80% resulting in very fast signing and verification. However, key generation is costly and does not scale well with the security parameter. Due to the large keys, NIST does not see Rainbow suitable as a general purpose digital signature scheme such as those standardized in FIPS 186-4. Rainbow is suitable for scenarios, where vector instructions are available, keys do not have to be generated and exchanged often and small signatures are required.

5.3 Alternate candidates

1. **GeMSS** follows the multivariate polynomial approach similar to Rainbow, but is based on a different computational assumption that is better-studied. It has even bigger public keys and slower signing than Rainbow. However, signatures are even shorter.
2. **Picnic** is a signature scheme based on a non-interactive zero-knowledge proof of knowledge. It is designed to be highly modular. Its building blocks can be easily exchanged for alternative ones. The public keys are small, but signatures are large and both signing and verification are slow.

3. **SPHINCS+** is constructed entirely of a cryptographic hash function. Therefore, its post-quantum security guarantees can be considered among the strongest of the submissions. Public keys are very small. However, signing is very slow and the signatures are large meaning that the performance would be poor if contemporary digital signatures were replaced with SPHINCS+.

6 Discussion

Quantum computer engineering has progressed rapidly during the last five years. According to the predictions of IBM, quantum volume will double annually in the near future. Provided that such a development is realized, contemporary cryptographic schemes would come under quantum attacks during the lifetime of 6G networks. At the same time, 6G is envisioned to provide connectivity for applications such as remote health monitoring. Steps need to be taken to secure wireless connectivity against quantum attacks in order to provide reliability for these critical applications.

In the 5G specification, symmetric algorithms such as SNOW 3G, AES and ZUC are applied with 128-bit keys for both encryption and message integrity. These key lengths are not sufficient in the post-quantum world. Due to the Grover's algorithm, the key lengths of symmetric primitives need to be doubled. In the future 6G networks, symmetric cryptography has to be implemented with at least 256-bit keys in order to maintain the current security level against quantum attacks. Fortunately, block ciphers such as AES remain secure and applicable. The same is true for contemporary cryptographic hash functions such as SHA-2 and SHA-3. According to the current knowledge, quantum computing does not pose significant challenges to the protocols implemented solely using symmetric primitives provided that the key lengths are adjusted. However, these key lengths need to be maintained also if the communication shifts from 6G to older generation networks. That is, changes need to made to pre-6G network standards and equipment to assure post-quantum security. It should be also noted that the increase to 256 bits in key length will incur a penalty to performance.

In 5G, the core network functionality has become dependent on the internet. Such a development will continue even further in 6G. It will be impossible to separate the security of 6G from the security of the internet. However, the current lack of security on the internet and the amount of security and privacy threats will pose significant challenges to the envisioned dependability of the 6G networks especially regarding critical applications such as remote health monitoring. The security architecture will become highly complex and hard to implement securely. The security mechanisms will be based on those developed for the internet such as TLS, IPSec and DNSSEC and their cryptographic primitives. However, these protocols have been designed for typical internet applications and may not be optimal for the envisioned applications and latency requirements of the 6G networks.

Currently, internet security protocols such as TLS are not secure against quantum attacks due to factoring and DLP based public key cryptography. Fortunately,

standardization for post-quantum secure replacements are ongoing. Finalists of the third round in the NIST PQC offer adequate performance and key sizes for typical applications of TLS. However, the applicability of those schemes regarding 6G may differ from their applicability regarding the standard use of TLS on the internet. For example, the strict latency requirements envisioned for 6G place strict requirements on the size of cryptographic keys and the efficiency of the algorithms.

Regarding key establishment and public key encryption, its use cases in 6G need to be carefully evaluated and specified. If public keys do not need to be generated often or exchanged, then Classic McEliece will offer the most succinct ciphertexts with efficient encryption and decryption. However, its public keys are very large and key generation is very slow. If new keys are frequently generated and exchanged, which is the case when ephemeral keys are applied, then Kyber and Saber offer the best performance. NTRU offers faster key generation than McEliece and key lengths similar to Kyber and Saber, but its encryption and decryption are considerably slower.

Digital signatures will be heavily applied through the PKI and the EAP-TLS protocol and its successors in 6G. Falcon offers the smallest public-keys of the three NIST PQC third round finalists. Its signatures are also smaller than those of Dilithium and it offers reasonable signing and verification performance. However, key generation is very slow and its secure implementation is harder than for Dilithium. For a use case, where new keys are needed, Dilithium offers significantly faster key generation than the other two candidates. It also has the benefit of sharing the same design base with Kyber if both key establishment and digital signatures are needed. Rainbow is an interesting candidate. Its signatures are significantly smaller than those of the other schemes. Its performance is also good on hardware that supports vector instructions. However, such hardware might be rare for resource constrained IoT devices. In addition, the public keys are very large making the scheme unsuitable for scenarios where the public keys are not pre-stored on the device.

There are no post-quantum secure cryptographic algorithms that simultaneously offer very small keys and ciphertexts/signatures and have efficient key generation, encryption and decryption or signing and verification. Trade-offs need to made when contemporary asymmetric primitives are replaced with post-quantum secure ones. Such a replacement necessarily incurs costs either in the communication or operational efficiency of the network. Research is needed to identify the correct application of post-quantum secure cryptography in order to satisfy the envisioned performance and functionality of the 6G architecture.

7 Conclusion

Practical quantum computing is expected to be a reality during the lifetime of 6G networks. Therefore, the security architecture of the future 6G needs to provide security against quantum attacks. While symmetric cryptography will remain secure by updating the key length, contemporary public-key cryptography will not. We note that symmetric primitives will need key lengths of at least 256 bits for current

level of security. Due to the development towards internet and cloud based architecture, 6G will be dependent on the public key infrastructure of the internet and its security mechanisms. We review the state-of-the-art post-quantum secure public-key primitives for key establishment, encryption and digital signatures selected into the third round of the NIST PQC competition for post-quantum secure cryptography standardization. These schemes have significant differences in their operational characteristics such as key or signature lengths and algorithmic performance. Careful consideration is needed for their optimal application in the 6G security architecture.

Acknowledgements

This work is supported by the TrustedMaaS project by the Infotech institute of the University of Oulu, and the Academy of Finland 6Genesis Flagship (grant318927).

References

1. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.: Strengths and weaknesses of quantum computing. SIAM Journal on Computing **26**(5), 1510–1523 (1997). DOI 10.1137/S0097539796300933. URL https://doi.org/10.1137/S0097539796300933
2. Brassard, G., HØyer, P., Tapp, A.: Quantum cryptanalysis of hash and claw-free functions. In: C.L. Lucchesi, A.V. Moura (eds.) LATIN'98: Theoretical Informatics, pp. 163–169. Springer Berlin Heidelberg, Berlin, Heidelberg (1998)
3. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory **22**(6), 644–654 (1976)
4. DiVincenzo, D.P.: The physical implementation of quantum computation. Fortschritte der Physik **48**(9-11), 771–783 (2000). DOI 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E
5. Fang, D., Qian, Y., Hu, R.Q.: Security for 5G mobile wireless networks. IEEE Access **6**, 4850–4874 (2018)
6. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, p. 212–219. Association for Computing Machinery, New York, NY, USA (1996). DOI 10.1145/237814.237866. URL https://doi.org/10.1145/237814.237866
7. Gyongyosi, L., Imre, S.: A survey on quantum computing technology. Computer Science Review **31**, 51 – 71 (2019). DOI https://doi.org/10.1016/j.cosrev.2018.11.002. URL http://www.sciencedirect.com/science/article/pii/S1574013718301709
8. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: J.P. Buhler (ed.) Algorithmic Number Theory, pp. 267–288. Springer Berlin Heidelberg, Berlin, Heidelberg (1998)
9. Hosoyamada, A., Sasaki, Y.: Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In: A. Canteaut, Y. Ishai (eds.) Advances in Cryptology – EUROCRYPT 2020, pp. 249–279. Springer International Publishing, Cham (2020)
10. Latva-Aho, M., Leppänen, K.: Key drivers and research challenges for 6G ubiquitous wireless intelligence. Tech. rep., 6G Flagship, University of Oulu, Finland (2019). http://urn.fi/urn:isbn:9789526223544

11. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. DSN Progress Report **44**, 114–116 (1978)
12. Pornin, T.: New efficient, constant-time implementations of Falcon (2020). URL https://falcon-sign.info/falcon-impl-20190918.pdf. Accessed 14 Aug 2020
13. Proos, J., Zalka, C.: Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Info. Comput. **3**(4), 317–344 (2003)
14. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978). DOI 10.1145/359340.359342. URL https://doi.org/10.1145/359340.359342
15. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994)
16. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., Hewa, T., Liyanage, M., Ijaz, A., Partala, J., Abbas, R., Hecker, A., Jayousi, S., Martinelli, A., Caputo, S., Bechtold, J., Morales, I., Stoica, A., Abreu, G., Shahabuddin, S., Panayirci, E., Haas, H., Kumar, T., Ozparlak, B.O., Röning, J.: 6G white paper: Research challenges for trust, security and privacy. Tech. rep., arXiv eprint 2004.11665 (2020). https://arxiv.org/abs/2004.11665