International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 13, Issue 12 [December. 2024] PP: 153-160

Impact of Quantum Computing in Modern Cryptography

Jollanda Shara
Dept.of Mathematics & Computer Science, Faculty of Natural Sciences, University of Gjirokastra, ALBANIA

ABSTRACT: *Cryptography has been used from ancient time for preserving the confidentiality of data. Thus, cryptography research has also been evolving from the classical Caesar cipher to the modern cryptosystems based on quantum computing. The development of quantum computing brings down a major threat on the modern cryptosystems based on modular arithmetic. Quantum computers can reach a level of optimization that would break many of today's encryption keys in less time than it takes to generate them using conventional digital computers. The traditional cryptography algorithms are completely vulnerable to quantum computers. This threat leaded to post-quantum cryptography research for designing and developing post-quantum algorithms that can be resistant to quantum computing attacks. In this paper we try to explain the important role that the quantum computing plays in current cryptography with its benefits and perils, as well.*

Date of Submission: 14-12-2024 Date of acceptance: 28-12-2024

I. INTRODUCTION

The current advancements in technology and particularly in electronic communications have become one of the main technological pillars of the modern age. But, the data transmission and data storage need confidentiality, integrity, authenticity and non-repudiation. These have made the science of cryptography one of the most important disciplines in information technology. Cryptography, etymologically derived from the Greek words hidden and writing. [2]

Soldiers in ancient Greece would send secret dispatches by wrapping a strip of parchment around a staff and writing across it. Their messages could be deciphered only by someone with a staff of the same thickness. It is one of the earliest examples of cryptography. As it is pointed out in the literature… "Cryptography is about communicating in the presence of an adversary". Cryptography is an art of providing technique and science for securing the information. This information can be interpreted only by the sender and intended recipient. Most of the modern cryptography algorithms are based on complex mathematical functions. These mathematical functions are a kind of one-way function which is easy to solve in one direction but very hard to solve in the reverse direction. The security of these cryptography algorithms is based on the fact that with the existing computing possibilities hundreds of years are needed to break them. Quantum computers, however, can easily break most of the modern cryptography algorithms in suitable time complexity. Quantum computing is a technology based on the principles of quantum theory and it is much faster than classical computing techniques. [25] Richard Feynman introduced for the first time the quantum computing theory as a concept in 1982. From then on, this theory has been researched considerably. It is considered as the destructor of the present modern asymmetric cryptography. In addition, it is a fact that symmetric cryptography can also be affected by specific quantum algorithms; however, its security can be increased with the use of larger key spaces. [2] With the rapid progress of computer technology, e.g., progress in quantum computing, as we mention above, and the increasing amount of data exchanged and transferred on internet, the security of classical cryptography based on computational complexity is facing great challenges. Quantum cryptography based on the principles of quantum mechanics has received considerable attention over the past years. [33] The term "Quantum Cryptography" was coined in a paper which was presented by Brassard and Bennett at Crypto '82, an annual conference that had started one year earlier. The emerged field of Quantum Cryptography (QC) "lies at the intersection of quantum mechanics and information theory and that, moreover, the tension between quantum mechanics and relativity-the famous Einstein-Rosen-Podolsky (EPR) paradox (Einstein *et al.,* 1935)-is closely connected to the security of QC" [52,53]. QC has provided cryptographical protocols with provable unconditional security independent on future technological advancements. (see [51]) Quantum cryptography is the only approach to privacy ever proposed that allows two parties (who do not share a long secret key ahead of time) to communicate with provably perfect secrecy under the nose of an eavesdropper endowed with unlimited computational power and whose technology is limited by nothing but the fundamental laws of nature. [34] Quantum random number generation (QRNG) and quantum key distribution (QKD), compared with classical cryptosystems, can solve the problems of truly random keys and information theoretic secure distribution of keys. But, because of the short transmission distance, restriction to point-to-point links, high manufacturing and maintenance cost, and lack of scalability, it is a challenge to deploy QKD systems in real networks. Post--quantum cryptography (PQC), on the other hand, is similar to classical

cryptography that is algorithm-based, but as it is believed, it enables holding out against attacks from powerful quantum computers. PQC builds cryptosystems on mathematical operations for which quantum algorithms offer little advantages. However, PQC algorithms have problems to replace classical ones that are already mature and widely used. Deploying a new cryptosystem incurs potentially high cost, with the time and energy consumed by cryptographic computations. [33] Certain candidate families of post-quantum schemes have been realized including code-based [28], hash-based [29], multivariate [30], lattice-based [31,32] and isogeny-based [26] solutions. The maturity in post-quantum research has led to the formulation of various post-quantum cryptosystems, standardization of post-quantum algorithms by various standardization bodies world-wide, industry adoption of post-quantum technology and the development of open source post-quantum libraries. ([27])

II. QUANTUM COMPUTING

Quantum computing is an application of a quantum mechanism that uses a quantum phenomenon to perform computation. A Quantum computer is a device that performs quantum computing. It manipulates the states of qubits in a controlled way to perform algorithms. A qubit (or quantum bit) is the quantum-mechanical analogue of a classical bit. In classical computers information is encoded in a bit, where each bit can be either zero or one. In quantum computing, the information is encoded in qubits. The state of the qubits is written as $|0\rangle$ and $|1\rangle$. The qubits can be simultaneously both at 0 and 1. Quantum computers are built using the following features of quantum states:

Superposition: Quantum systems can exist in two states at once. A qubit can be in 0 and 1 at the same time. When the measurement is performed, the qubit collapses to either zero or one.

Entanglement: It's a quantum mechanical phenomenon where the state of entangled particles can be described with reference to each other. Measurement performed on one entangled particle will immediately influence the other entangled particle irrespective of the distance among the entangled particle.

Interference: The fundamental idea in quantum computing is to control the probability of qubits collapsing into a particular measurement state. Quantum interference, a by-product of superposition, allows controlling the measurement of a qubit toward a desired state or set of states. [25]

Increasing the number of qubits plays an important role in calculation because it gives rise to an exponential processing speed. Two traditional binary bits are needed to match the power of a single qubit; four bits are required to match two qubits; eight bits are needed to match three qubits; and so on. It would take about 18 quadrillion bits of traditional memory to model a quantum computer with just 54 qubits. A 100 qubit quantum computer would require more bits than there are atoms on our planet. And a 280 qubit computer would require more bits than there are atoms in the known universe. William Phillips, who is a Nobel Prize–winning physicist, has compared the jump from today's technology to quantum with that from the abacus to the digital computer itself. In 2019 Google used a quantum computer to perform a specific computation task in just 200 seconds. The same task would have taken 10,000 years with the most powerful digital supercomputer at that time. [56] The work was initiated by several mathematicians and physicists such as Paul Benioff (1980) [17], Yuri Manin (1980) [18], Richard Feynman (1982) [19], and David Deutsch (1985) [20]. Quantum computing constitutes a new computing paradigm, which is expected to solve complex problems that require far more computational power than what is possible with the current generation of computer technologies. Advance research in materials science, molecular modelling, and deep learning are a few examples of complex problems that quantum computing can solve. Quantum computers could also help us understand climate change. (see [3])

SOME HISTORICAL NOTES

It took some time, but gradually the influence of Feynman's ideas grew. In 1985, David Deutsch formalized the notion of a quantum computer [44]. It was an important advance which raised the question whether quantum computers might have an advantage over classical computer for solving problems that are not at all related with quantum physics. In 1993, Umesh Vazirani and his student Ethan Bernstein formulated a contrived problem that a quantum computer could solve with a superpolynomial speedup over a classical computer [45]. Soon after, Daniel Simon showed that a quantum computer could achieve an exponential speedup in solving an idealized version of the problem of finding the period of function [46]. Though Simon's problem had no obvious applications, it inspired Peter Shor [47], who worked out a very effective way of performing a Fourier transform using a quantum computer. Then he applied it to formulate an efficient quantum algorithm for computing discrete logarithms. Only a few days later, Shor used similar ideas to find an efficient quantum algorithm for factoring large numbers. Shor's discovery, and its obvious implications for cryptanalysis, grew the interest in quantum computing. But very good physicists like Rolf Landauer [48], Bill Unruh [49], and Serge Haroche [50] voiced strong skepticism about the effective work of the quantum computers. Those physicists viewed quantum computing as "… the computer scientist's dream [but] the experimenter's nightmare." And, it was again Shor who led the next crucial advances: the discovery of quantum error-correcting codes [41, 42] and of fault-tolerant

methods for executing a quantum computation reliably using noisy hardware [43]. By the end of 1996, it was understood, at least in principle, that quantum computing could be scaled up to large devices that solve very hard problems, assuming that errors bothering the hardware are not too common or too strongly correlated [36 - 40]. This "accuracy threshold theorem" for quantum computing was already in place 2.5 years after the discovery of Shor's algorithm. (see [35])

We give below a short summary of more important historical events in the Quantum Computing progress road.

1980 Paul Benioff suggests quantum mechanics could be used for computation.
1981 Term "Quantum Computer" coined by Nobel-winning physicist Richard Feynman.
1985 David Deutsch formulated a blueprint of quantum computers called Quantum Turing Machine.
1992 Deutsch-Jozsa algorithm, was proposed one of the first examples of quantum algorithm exponentially faster that any possible deterministic classic algorithm.
1994 Shor's algorithm, was proposed. It can break widely used encryption forms.
1996 Grover's algorithm, a quantum search algorithm, offers a quadratic speedup over classical computers.
2007 D-Wave announces a quantum computing chip that it claims can solve Sudoku puzzles.
2009 Yale created first solid-state quantum processor, a 2-bit superconducting chip.
2011 The first commercially available quantum computer is offered by D-Wave Systems.
2012 1QB Information Technologies (1QBit), the first dedicated quantum computing software company is founded.
2013 Google teams up with NASA to fund a lab to try out D-Wave's hardware.
2015 NASA publicly displayed the world's first fully operational quantum computer, D-Wave Systems.
2016 IBM Research announced it is making quantum computing publicly accessible via cloud.
2017 IBM unveils 17-qubit quantum computer.
2018 Google announces 72-bit quantum chip called Bristlecone.
2019 IBM launches first 2-qubit commercial quantum computer (Q System One), IBM announces 53-qubit quantum computer.
2020 Amazon Braket, AWS Cloud Quantum Computing Service launched.
2021 Honeywell Computer Solutions: The System Model H1 became the first Quantum Model achieving 1024 Quantum Volume.
2022 Quantinuum announces Quantum Volume 4096 achievement.

The use of Quantum computers has many advantages. For example, they could transform the financial system, too. They could perform, almost in real time, more accurate Monte Carlo simulations which are used to predict the behavior of markets through pricing and risk simulations. Quantum computers could also solve optimization tasks, such as allocating capital, determining portfolio investments, or managing the cash in ATM networks. Quantum computers could also speed the training of machine learning algorithms. The time it takes digital computers to do this increases exponentially with each dimension that is added. But this does not happen with quantum computers.

However, there are many risks, as well. The computing power of these mighty quantum machines could threaten modern cryptography. This has many implications for financial stability and privacy.

Quantum computers will be able to solve hard mathematical problems exponentially faster than digital supercomputers. Theoretically, a fully functioning quantum computer could break an asymmetric key in a matter of minutes. Public keys are especially vulnerable because most of them are based on the factorization problem: it is hard for digital computers to find two prime numbers from their product. Quantum computers, by contrast, can do it very easy.

"…Asymmetric keys are widely used to secure communications over the internet. Successful attacks against these algorithms would compromise connections used by the financial system, including mobile banking, e-commerce, payment transactions, ATM cash withdrawals, and VPN communications, to name just a few. Vulnerable applications that rely on public-key cryptography also include popular digital assets such as Bitcoin and Ethereum, as well as password-protected web applications. The best known of these protocols, HTTPS, is used by 97 of the world's top 100 websites…" (see [56])

III. QUANTUM COMPUTING ROLE IN CRYPTOGRAPHY

Two of the main types of cryptographic algorithms in use today for the protection of data work in different ways:

- **Symmetric algorithms** use the same secret key to encrypt and decrypt data.
- **Asymmetric algorithms**, also known as public key algorithms, use two keys that are mathematically related: a public key and a private key.

The development of public key cryptography in the 1970s was revolutionary. It enabled new ways of communicating securely. However, public key algorithms are vulnerable to quantum attacks. The mathematician Peter Shor discovered that these types of problems can be solved very quickly using a sufficiently strong quantum computer. Grover's Algorithm, devised by computer scientist Lov Grover, is a quantum search algorithm. Using Grover's algorithm, some symmetric algorithms are impacted and some are broken. [55]

Let us see them in more details:

SHOR'S 1994 ALGORITHM

In 1994, Shor proposed a polynomial - time (efficient) algorithm [15] for solving integer factorization and discrete logarithm problems. Peter Shor showed that QC can efficiently solve integer factorization and discrete logarithm problems used on existing public key crypto systems, becoming these systems impotent (Shor's algorithm), as a result.

The algorithm relies on the existence of quantum computers. So, Shor's quantum algorithm and its variants can be used for breaking most of the currently used public-key cryptosystems. [3]

All widely used public-key cryptographic algorithms are theoretically vulnerable to attacks based on Shor's algorithm, but the algorithm depends upon operations that can only be achieved by a large-scale quantum computer. Many cryptographic researchers have contributed to the development of algorithms whose security is not degraded by Shor's algorithm or other known quantum computing algorithms. These algorithms are sometimes referred to as quantum resistant. (see [22])

Shor's algorithm can attack Public Key Cryptosystems. The impact of Shor's algorithm reduces the time complexity of Integer Factorization and Discrete Logarithm from sub-exponential to polynomial, and targets keys that can have long cryptoperiods.

The CRQC running Shor's algorithm can be used to attack two aspects on the application protocols in the order of importance.

1. Key Exchange

- Attacks against Key Exchange aim to recover the SESSION KEYS used for encrypting data and therefore being attacks towards data confidentiality.

- If the data transferred over a protocol needs to retain its confidentiality for a long period of time, it is important to prepare for the emergence of CRQC. This is because an eavesdropper that has read access to an encrypted session today can record the data. Then, later on, when CRQC's have evolved, can use one to recover the session key and get access to the data.

2. Digital signatures

- Attacks against Signatures aim to recover signature keys and to forge signatures used for authenticating data, user, or server by calculating the private signature key. These attacks pick out data integrity and authentication. An attack against signatures can only be launched when CRQC is available (day one) and the impact depends on the protocol.
- Signatures constructed with classical PKC and verified before day one are safe. After day one, the bad actor may use CRQC to acquire a signature key and use that to sign arbitrary documents still verifying correctly - as if the original key had been revealed. Classical PKC Signatures will not be usable for their purpose.

GROVER'S 1996 ALGORITHM

In 1996, Grover proposed an $O(pN)$ query complexity of quantum algorithm for functions with N-bit domains [16]. This quantum algorithm once realized on quantum computers can be used for breaking symmetric-key cryptosystems. Lev Grover described an algorithm allowing a Quantum computer to perform a brute force key search using quadratically fewer steps than would be required classically (Grover's algorithm).

To defend against attacks based on Grover's algorithm, it's needed to double the key sizes in order to achieve a similar level of security against conventional computers.

For example, for 128-bit symmetric-key security, we need to use symmetric - key cryptosystems which are originally designed for achieving 256-bit security against attacks based on Grover's quantum algorithm. [3]

Grover's algorithms can attack Symmetric Key Crypto systems. Grover's algorithm for key search suggests that an attacker with CRQC could break a symmetric cipher with a key up to twice as long as without Quantum computers. But, as Crystof Zalka proved in 1997, the algorithm must be performed in series to obtain the full quadratic speedup. In the real world, where attacks on cryptography use massively parallel processing, the advantage of Grover's algorithm will be smaller.

Taking this into account along with the cost of building CRQC it is quite likely that Grover's algorithm will provide only little or no advantage in attacking AES, and AES 128 will remain secure.

Even if Quantum computers were less expensive than anticipated, the problems on parallelizing Grover's algorithm suggests that AES with a longer key size will be safe for a very long time, assuming new attack vectors are not found.

The application of Grover's algorithm is even more reduced considering the current protocol trend of having short symmetric cryptoperiods and the dynamic nature of symmetric encryption keys. [54]

IV. POST-QUANTUM CRYPTOGRAPHY

Acknowledging the threat of quantum computers to existing cryptography, the US National Security Agency (NSA) published warnings of the need to transition to new quantum-resistant algorithms in 2015. So, in 2017 the US National Institute of Standards and Technology (NIST) launched a standardization initiative to select quantum safe algorithms for future use by government and industry. The new algorithm proposal is referred to as post quantum cryptography.

According to ETSI, "Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and Quantum computers, to keep information assets secure even after a large-scale quantum computer has been built." [55]

Quantum-safe cryptography covers all cryptography systems that resist to quantum attacks. As in today's cryptography, this covers both complexity-based protocols and provably secure systems. The first ones consists in merely replacing the problem of factoring in which RSA rests by another problem. This problem is claimed to be intractable both for classical and for quantum computers, since factoring was claimed to be intractable. The great advantage of this approach is being flexible, cost-effective and relatively similar to today's approach, hence security experts don't need to change much. But, on the other hand, it has the great disadvantage that one is again betting on the unknown to secure our information-based society. [22]

Post-Quantum Cryptography (PQC) is Quantum-Safe Cryptography (QSC) designed to be quantum-safe and operate on existing computers and networks.[54]

It is a new field of cryptographic research which has emerged to counter the threat to today's asymmetric cryptography by Quantum computers.

The goal of post-quantum cryptography is to develop cryptographic systems that are secure against both quantum and conventional computers and can interoperate with existing communication protocols and networks [2]

Some PQC algorithms are based on problems of Lattice such as Modulo Learning With Errors [Kyber] , Modulo Learning with Rounding [Saber], Ring Learning With Rounding [NTRU] and Learning With Errors [FrodoKEM], or problems of codes such as Goppa codes [Classic McEliece]. [54]

Various approaches are going after to realize post-quantum cryptography in current research, including:

- Hash-Based Cryptography: The security of hash-based signature schemes is based on the security properties of the hash function used. [1] Hash-based cryptography focuses on designing digital signature schemes based on the security of cryptographic hash functions, e.g., SHA-3. These schemes are based on the security of hash functions (as a one-way function, collision-resistant property, and hardness of second pre-image attacks). They require fewer security assumptions than the number-theoretic signature schemes (e.g. RSA, DSA). Ralph Merkle in 1989 introduced Merkle Signature Scheme (MSS) [4], which is based on one-time signatures (e.g., the Lamport signature scheme) and uses a binary hash tree (Merkle tree). The MSS is resistant to quantum computer algorithms. More details can be found in this survey on hash-based schemes Butin (2017) [5]
- Code-Based Cryptography: The security of code-based schemes is based on the difficulty of efficiently decoding general error-correcting codes. [1] Code-based cryptography [6, 7] has its security relying on the hardness of problems from coding theory, for example, syndrome decoding (SD) and learning parity with noise (LPN). These cryptosystems are based on error-correcting codes to construct a one-way function. The security is based on the hardness of decoding a message which contains random errors and recovering the code structure.
- Multivariate Cryptography: The security of multivariate cryptography is based on the assumption that multivariate polynomial systems of equations over finite fields are hard to solve. [1] Multivariate cryptography has its security relying on the hardness of solving multivariate systems of equations. These schemes are based on systems of multivariate polynomial equations over a finite field F. There are several variants of multivariate cryptography schemes based on hidden field equations (HFE) trapdoor functions, such as the unbalanced oil and vinegar cryptosystems (UOV). UOV is used for signatures. Other examples of multivariate cryptography are Rainbow, TTS, or MPKC schemes. More about the current state of the multivariate cryptography schemes can be found in [8]

- Lattice-Based Cryptography: The security of lattice-based schemes is based on the difficulty of solving certain computational problems in mathematical lattices. [1] Lattice-based cryptography seems to be one of the most active directions in recent years, for several key reasons. First, it has strong security guarantees from some wellknown lattice problems, for example, shortest vector problem (SVP) and the ring learning with errors (RLWE) problem [9]. Second, it enables powerful cryptographic primitives; for example, fully homomorphic encryption (FHE) and functional encryption [10]. Third, some new lattice-based cryptographic schemes have become quite practical recently, for example, the key exchange protocol NewHope [11], and a signature scheme BLISS [12]
- Isogeny-Based Cryptography schemes: Isogeny-based schemes base their security on the fact that it is difficult to find an isogeny between two super-singular elliptic curves, if one exists. [1] Isogeny-based cryptography is a specific type of post-quantum cryptography that uses certain well-behaved maps between abelian varieties over finite fields (typically elliptic curves) as its core building block. Its main advantages are relatively small keys and its rich mathematical structure. These schemes are based on supersingular elliptic curve isogenies [13] that are secure against quantum adversaries. These schemes are secured under the problem of constructing an isogeny between two supersingular curves with the same number of points. Isogeny-based schemes may serve as digital signatures or key exchange, such as the supersingular isogeny Diffie–Hellman (SIDH) scheme [14] (see [3])

We note that none of the above proposals have been shown to guarantee security against all quantum attacks. A new quantum algorithm may be discovered which breaks some of these schemes. However, this is similar to the state today. Although most public key cryptosystems come with a security proof, these proofs are based on unproven assumptions. Thus, the lack of known attacks is used to justify the security of public key cryptography currently in use. Nonetheless, NIST believes that more research and analysis are needed before any of the above proposed post-quantum algorithms could be recommended for use today. They have not received nearly so much critical examination from the cryptographic community compared with the currently deployed algorithms. One exception is hash-based signatures, whose security is well-understood. For certain specific applications, such as digital code signing, hash-based signatures could potentially be standardized in the next few years. [21]

As it is stressed out in Lidong Chen's article, "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?" [23], it is likely that future post-quantum cryptographic standards will specify multiple algorithms for different applications because of differing implementation constraints (e.g., sensitivity to large signature size or large keys).

The replacement of algorithms generally requires changing or replacing cryptographic libraries, implementation validation tools, hardware that implements or accelerates algorithm performance, dependent operating system and application code, etc. Security standards, procedures, and best practice documentation need to be changed or replaced, as well. And the same for installation, configuration, and administration documentation.

Public-key cryptography has been integrated into existing computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms. Examples of public-key cryptography uses include:

A) Digital signatures used to provide source authentication and integrity authentication as well as support the non-repudiation of messages, documents, or stored data,

B) Identity authentication processes used to establish an authenticated communication session or authorization to perform a particular action,

C) Key transport of symmetric keys (e.g., key-wrapping, data encryption, and message authentication keys) and other keying material (e.g., initialization vectors), and

D) Privilege authorization processes.

Many information technology (IT) and operational technology (OT) systems are dependent on public-key cryptography, but many organizations have no inventory of where that cryptography is used. This makes it difficult to determine where and with what priority post-quantum algorithms will need to replace the current public-key systems. To make more easy the discovery of where and how public-key cryptography is being used in existing technology infrastructures, tools are urgently needed.

Similarly, cybersecurity standards and guidelines and the operational directives and mandates derived from them generally specify or presume the use of public-key cryptography. There is currently no inventory of these that can guide updates to the standards, guidelines, and regulations necessary to accommodate the migration to post-quantum cryptography. [22]

V. CONCLUSION

Today's secrets, such as Internet communication, digital banking, and electronic commerce, are protected from inquisitive people by powerful computer algorithms.

The next-generation information security is facing quantum threats from the recent progress in quantum technologies. Quantum cryptography can provide true randomness and secure distribution of keys, but is prevented from wide applications due to challenges in real implementation. [33]

A quantum algorithm is a sequence of manipulations of qubits. As we mentioned above, among the best known quantum algorithms are the search algorithm of Lov Grover (1996) and the algorithms of Peter Shor (1994). They can be used to factorize integers and compute discrete logarithms. In particular, the latter algorithms break current public-key cryptography such as RSA, (Elliptic Curve) Diffie-Hellman or ElGamal. But, despite the immense impact on current cryptography, the development of quantum computers is mainly motivated by the potential applications in areas such as pharmacy, material science, chemistry or logistics. [1]

Many researchers have pointed out the great importance of using the quantum cryptography in many fields. So, the authors in [57] have underlined this importance writing:

"…Considering cryptography as a kind of art form that allows hiding secret information in a sequence of zeros and ones, it can be noted that even today quantum cryptography is in demand not only in government communications and in big business. In addition, the constant increase in the transmission speed and the reduction in the cost of implementing a number of processes allow one to hope for an increasingly widespread use of quantum cryptosystems in various fields already in the future…"

Inspired by the great scientific and technological progress in this domain, we try to highlight the more significant points becoming the quantum computing so important in current cryptography. We hope that this paper will be a simple contribution on this direction.

REFRENCES

[1]. Quantum-safe cryptography – fundamentals, current developments and recommendations, Federal Office for Information Security (BSI), October 2021.

[2]. Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, The Impact of Quantum Computing on Present Cryptography, arXiv:1809.00371v2 [cs.CR] 12 Sep 2018.

[3]. Chithralekha, T.; Singh, K.; Ganeshvani, G.; Rajarajan, M. Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions. Cryptography 2021, 5, 38. https://doi.org/10.3390/cryptography5040038 .

[4]. Merkle, R. A certified digital signature. In Advances in Cryptology – CRYPTO'89; Springer: Berlin/Heidelberg, Germany, 1989; pp. 218-238..

[5]. Butin, D. Hash-based signatures: State of play. IEEE Secur. Priv. 2007, 15, 37–43. [CrossRef].

[6]. Cayrel, P.L.; ElYousfi, M.; Hoffmann, G.; Meziani, M.; Niebuhr, R. Recent Progress in Code-Based Cryptography. International Conference on Information Security and Assurance; Springer: Berlin/Heidelberg, Germany, 2011; pp. 21–32.

[7]. Sendrier, N. Code-Based Cryptography: State of the Art and Perspectives. IEEE Secur. Priv. 2017, 15, 44–50. [CrossRef].

[8]. Ding, J.; Petzoldt, A. Current state of multivariate cryptography. IEEE Secur. Priv. 2017, 15, 28–36. [CrossRef].

[9]. Chi, D.P.; Choi, J.W.; Kim, J.S.; Kim, T. Lattice Based Cryptography for Beginners. Available online: https://eprint.iacr.org/2015/938 (accessed on 20 November 2020.

[10]. Lepoint, T. Design and Implementation of Lattice-Based Cryptography. Ph.D. Thesis, Ecole Normale Euérieure de Paris—ENS, Paris, France, 2014 .

[11]. Alkim, D.; L.Ducas.; Pöppelmann, T.; Schwabe, P. Post-Quantum Key Exchange—A New Hope. Available online: https://eprint.iacr.org/2015/1092 (accessed on 20 November 2020).

[12]. Ducas, L.; Durmus, A.; Lepoint, T.; Lyubashevsky, V. Lattice Signatures and Bimodal Gaussians. Available online: https://eprint.iacr.org/2013/383 (accessed on 20 November 2020).

[13]. Jao, D.; Feo, L.D. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. PQCrypto 2011, 7071, 19–34.

[14]. Supersingular Isogeny Diffie–Hellman Key Exchange (SIDH). https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange (accessed on 4 February 2021).

[15]. Shor, P.W. Algorithms for quantum computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994 pp. 124–134.

[16]. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadephia, PA, USA, 22–24 May 1996; pp. 212–219.

[17]. Benioff, P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. J. Stat. Phys. 1980, 22, 563–591. [CrossRef].

[18]. Manin, Y. Mathematics and Physics; American Mathematical Society: Providence, RI, USA, 1981.

[19]. Feynman, R.P.U. Simulating physics with computers. Int. J. Theor. Phys. 1982, 21, 467–488. [CrossRef].

[20]. Deutsch, D. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proc. R. Soc. Lond. **1985**, A400, 97–117.

[21]. Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone, Report on Post-Quantum Cryptography, http://dx.doi.org/10.6028/NIST.IR.8105 2016.

[22]. William Barker, William Polk, Murugiah Souppaya, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, April 28, 2021 https://doi.org/10.6028/NIST.CSWP.04282021.

[23]. Chen L (2017) Cryptography Standards in Quantum Time: New Wine in an Old Wineskin? IEEE Security & Privacy 15(4):51-57. https://doi.org/10.1109/MSP.2017.3151339.

[24]. Campagna M., LaMacchia B., & Ott D. (2020) Post Quantum Cryptography: Readiness Challenges and the Approaching Storm. https://cra.org/ccc/resources/ccc-led-whitepapers/#2020-quadrennial-papers.

[25]. Dr. Manish Kumar, Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis.

[26]. Jao, D.; De Feo, L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. PQCrypto 2011, 7071, 19–34.

[27]. Chithralekha Balamurugan, Kalpana Singh, Ganeshvani Ganesan, Muttukrishnan Rajarajan, Code-based Post-Quantum Cryptography, 2021, doi:10.20944/preprints202104.0734.v1.

[28]. McEliece, R.J. A public-key cryptosystem based on algebraic. Coding Thv 1978, 4244, 114–116.

[29]. Merkle, R. Secrecy, Authentication, and Public Key Systems; Computer Science Series, UMI Research Press, 1982.

[30]. Patarin, J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. International Conference on the Theory and Applications of Cryptographic Techniques, 1996, pp. 33–48.

[31]. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A ring-based public key cryptosystem. International Algorithmic Number Theory Symposium. Springer, 1998, pp. 267–288.

[32]. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) 2009, 56, 34.

[33]. Leilei Huang, Kai Feng, Chongjin Xie, A practical hybrid quantum-safe cryptographic scheme between data centers, Proc. SPIE 11540, Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III, 1154008 (20 September 2020); doi: 10.1117/12.2573558.

[34]. Gilles Brassard, Brief History of Quantum Cryptography: A Personal Perspective arXiv:quant-ph/0604072v1 11 Apr 2006.

[35]. John Preskill, Quantum computing 40 years later, arXiv:2106.10522v3 [quant-ph] 6 Feb 2023.

[36]. Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In Proceedings of the twenty-ninth annual ACM Symposium on Theory of Computing, pages 176 -188, 1997.

[37]. Emanuel Knill, Raymond Laamme, and Wojciech H Zurek. Resilient quantum computation, Science, 279(5349):342-345, 1998.

[38]. Aleksei Yur'evich Kitaev. Quantum computations: algorithms and error correction. Uspekhi Matematicheskikh Nauk, 52(6):53-112, 1997.

[39]. John Preskill. Reliable quantum computers. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 454(1969):385-410, 1998.

[40]. John Preskill. Fault-tolerant quantum computation. In Introduction to quantum computation and information, pages 213-269. World Scientific, 1998.

[41]. Peter W Shor. Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52(4):R2493, 1995.

[42]. Andrew M Steane. Error correcting codes in quantum theory. Physical Review Letters, 77(5):793, 1996.

[43]. Peter W Shor. Fault-tolerant quantum computation. In Proceedings of 37th Conference on Foundations of Computer Science, pages 56-65. IEEE, 1996.

[44]. David Deutsch. Quantum theory, the Church - Turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818):97-117, 1985.

[45]. Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. SIAM Journal on Computing, 26(5):1411-1473, 1997.

[46]. Daniel R Simon. On the power of quantum computation. SIAM journal on Computing, 26(5):1474 -1483, 1997.

[47]. Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2):303-332, 1999.

[48]. Rolf Landauer. Is quantum mechanics useful? Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences, 353(1703):367-376, 1995.

[49]. William G Unruh. Maintaining coherence in quantum computers. Physical Review A, 51(2):992, 1995.

[50]. Serge Haroche and Jean-Michel Raimond. Quantum computing: dream or nightmare? Physics Today, 49(8):51-54, 1996.

[51]. Ioannis P. Antoniades, Vasilios G. Chouvardas, Miltiades K. Hatalis, Georgios L. Bleris, Quantum Cryptography A Short Historical overview, Traditional Mathematics and Mechanics (2004).

[52]. Einstein, A., Podolsky, B. and Rosen, N., (1935), Phys. Rev. 47, 777–780.

[53]. Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., (2002), Rev. Mod. Phys., 74(1), 145-196.

[54]. https://www.ssh.com/academy/cryptography/what-is-quantum-safe-cryptography.

[55]. https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it.

[56]. https://www.imf.org/en/Publications/fandd/issues/2021/09/quantum-computings-possibilitiesand-perils-deodoro.

[57]. Valerii V. Arutyunov, Kirill A. Gradusov, Quantum cryptography. The history of its origin, current status, and development prospects, Vestnik_isism_3(2021).