Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

Tipo de artículo: Artículo originales
Temática: Seguridad informática
Recibido: 18/08/2022 | Aceptado: 06/09/2022 | Publicado: 02/11/2022

Quantum computing and post-quantum cryptography

Computación cuántica y criptografía post-cuántica

Ernesto Dominguez Fiallo 0000-0003-3831-2889[1*]
Daymé Almeida Echevarria 0000-0002-7573-4637[2]
Ramsés Rodríguez Aulet0000-0001-7653-324X[3]

[1]Instituto de Criptografía. Facultad de Matemática y Computación. Universidad de La Habana.
[2]Instituto de Criptografía. Facultad de Matemática y Computación. Universidad de La Habana.
[3]Instituto de Criptografía. Facultad de Matemática y Computación. Universidad de La Habana.

[*]Autor para correspondencia: (edominguezfiallo@nauta.cu)

RESUMEN

Los avances en el campo de la computación cuántica obligan a desarrollar e implementar algoritmos criptográficos resistentes a ataques en ordenadores cuánticos (criptografía post-cuántica) de forma urgente. La seguridad de los criptosistemas asimétricos actuales se basa en la dificultad de factorizar números enteros grandes o resolver problemas de logaritmos discretos. Sin embargo, estos problemas matemáticos se pueden resolver en tiempo polinomial (eficientemente) usando ordenadores cuánticos. En respuesta, se realiza una intensa investigación sobre la criptografía pos-cuántica. Esta ciencia es el estudio de los esquemas criptográficos que serían seguros contra los adversarios que tienen computadoras cuánticas y clásicas y que a su vez pueden implementarse sin cambios drásticos en las redes y protocolos de comunicación existentes. Este artículo ofrece una descripción general del estado del arte de los esquemas asimétricos alternativos que tienen la capacidad de resistir ataques en ordenadores cuánticos y considera sus principales características.

Palabras clave: Computación cuántica; Criptografía pos-cuántica.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

ABSTRACT

Due to developments within the field of quantum computers, the need for developing and implementing quantum-resistant cryptographic (post-quantum cryptography) algorithms has become more urgent. The security of current public-key cryptosystems relies on the hardness of factoring large integers or solving discrete logarithm problems. However, these mathematical problems can be solved in polynomial time (efficiently) using a quantum computer. In response, there has been intense research into post-quantum cryptography. This science is the study of cryptosystems that would be secure against adversaries who have both quantum and classical computers and that can be deployed without drastic changes to existing communication networks and protocols. This paper gives an overview of the current state of the art of the alternative public-key schemes that have the capability to resist quantum computer attacks and consider their main characteristics.

Keywords: Quantum computing; Post-quantum cryptography.

Introduction

Quantum computing is an emerging field that uses the concepts of quantum mechanics to perform computations (Sigov et al., 2022). It is an intersection of fields such as mathematics, physics and computer science. The starting point for quantum computers can be traced back to the 1980s when physicists asked whether a universal device can simulate quantum mechanical systems (Feynman et al., 1982). In recent years, quantum computing has become attractive as a research topic due to the acceleration of technology (Hidary, 2021; Hota and Dash, 2022; Gill et al., 2022). Recently, Google claimed having achieved Quantum Supremacy using a processor with programmable superconducting qubits to create quantum states on 53 qubits (Arute et al., 2019). As of the year 2020, organisations have built quantum computers with up to 50 qubits and are increasing it up to 100 qubits. Large companies such as Google, IBM and Microsoft and startups such as Rigetti, D-Wave and Xanadu have built quantum computers.

Cryptography is one of fundamental technologies for keeping the information society secure. In particular, publickey cryptography has been used in cryptographic protocols such as SSL/TLS, IPSec, SSH, copyright protection of DVD, and so on. The most widely used public-key cryptosystems are the RSA cryptosystem (Rivest et al., 1978) and elliptic curve cryptosystem (Miller, 1985; Koblitz, 1987). The security of these

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

cryptosystems is based on the mathematical difficulty of the integer factorization problem (IFP) and discrete logarithm problem (DLP) (Abuarqoub et al., 2021; Schöffel et al., 2022).

While the security of the aforementioned schemes cannot be practically challenged by conventional computer systems, this would not be the case in a post-quantum world where a large scale quantum computer has become a reality (Mosca, 2018). In 1994 Shor proposed a quantum polynomial time algorithm for solving the IFP and DLP in Abelian groups (Shor, 1994), and thus put in question the security of public-key cryptography. Since then, the research on post-quantum cryptography, also known as quantum-resistant cryptography, has progressed (Bernstein et al., 2009; Buchmann et al., 2016; Bernstein and Lange, 2017). 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 (Das and Sadhu, 2022; Sajimon et al., 2022; Joseph et al., 2022; Hekkala et al., 2022; Döring and Geitz, 2022; Tandel and Nasrıwala, 2022).

In August 2015 the U.S. National Security Agency (NSA) announced a transition to quantum-resistant algorithms (Koblitz and Menezes, 2016) and in 2016, the U.S. National Institute of Standards and Technology (NIST) published a standardization plan for post-quantum cryptography (Chen et al., 2016). In January 2018, NIST published the results of the first round. In total 82 algorithms were proposed from which 59 are encryption or key exchange schemes and 23 are signature schemes. After 3 to 5 years of analysis NIST will report the findings and prepare a draft of standards. At the moment of this writing, NIST's evaluation process has moved to the final round (Alagic et al., 2020). In May 2018, the China Association for Science and Technology (CAST) has released a report on the 60 major science and technology problems in twelve research fields, which considers the design of quantum-resistant cryptographic algorithms as one of the six major problems in the field of information technology.

Post-quantum cryptography is usually constructed by using mathematical problems which can be proven to be NP-hard (Bennett et al., 1997). However, for post-quantum cryptography to be practical, we need to evaluate the explicit sizes of the secure parameters used in the applications. The candidates of post-quantum cryptography include lattice-based cryptosystems (Ajtai, 1996; Gebremichael et al., 2022), code-based cryptosystems (McEliece, 1978; Fiallo, 2021; Esser et al., 2022), multivariate polynomial cryptosystems (Matsumoto and Imai, 1988; Hashimoto, 2021) and hash-based signatures (Merkle, 1989; Zeydan et al., 2022).

This paper gives an overview of the current state of the art of the alternative public-key schemes that have the capability to resist quantum computer attacks and consider their main characteristics.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

Mathematical foundations of quantum computing

The basic idea behind a quantum computer is to replace binary digits with quantum bits, or qubits for short. As opposed to binary bits, qubits can exist in additional states in between the two binary states. This is defined as a superposition of the digital states (Wang, 2012). In other words, the state of a qubit can be described by a two-dimensional state space in $\mathbb{C}^2$ with orthonormal basis vectors $|0\rangle$ and $|1\rangle$ (which well known as Dirac notation):

$$\alpha|0\rangle + \beta|1\rangle$$

where α and β are the probability amplitudes for the states 0 and 1 respectively and must satisfy the constraints

$$|\alpha|^2 + |\beta|^2 = 1$$

ensuring a collected probability of 1. The fact that a quantum computer can contain numerous such states concurrently, ensures its potential dominance over traditional computers. Like classical computers, quantum computers use quantum registers made up of multiple qubits. Quantum registers are a relatively straightforward extension of quantum bits. A register of n qubits is a superposition of all 2^n possible bit strings that could be represented using n bits. The state space of a size-n quantum register is a linear combination of n basis vectors, each of length 2^n:

$$\sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

Here i is the base-10 integer representation of a length-n number in base-2 and the the squares of the absolute values of the amplitudes of all 2^n possible bit configuations of an n-bit register sum to unity:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2$$

In classical computing, one way of thinking about algorithm design and computation is via universal Turing machines. Quantum universal Turing machines were first described by David Deutsch in 1985 (Deutsch, 1985) and operations on a quantum computer are most often described using quantum circuits made up of qubits and quantum logic gates, a concept also introduced by Deutsch a few years after his specification of the quantum analog to a Turing machine (Deutsch, 1989). Mathematically, classical logic gates are described using boolean algebra and quantum logic gates act in a similar way, in that quantum logic gates applied to quantum registers map the quantum superposition to another, together allowing the evolution of the system to some desired final state, a correct answer.

Despite the inherent superiority of a quantum computer, there are many challenges in quantum computing. Quantum algorithms are mainly probabilistic. This means that in one operation a quantum computer returns many solutions where only one is the correct, weakens the advantage of quantum computing speed. Qubits are susceptible to errors. Qubits suffer from bit-flips as well as phase errors. Direct inspection for errors should be avoided as it will cause the value to collapse, leaving its superposition state. Another challenge is the difficulty of coherence. Qubits can retain their quantum state for a short period of time (Muhonen et al., 2014). In 2017, IBM introduced the definition of Quantum Volume: a metric to measure how powerful a quantum computer is based on how many qubits it has, how good is the error correction on these qubits, and the number of operations that can be done in parallel. Increase in the number of qubit does not improve a quantum computer if the error rate is high. However, improving the error rate would result in a more powerful quantum computer (Jurcevic et al., 2021).

Some important quantum algorithms

Shor's algorithm

As mentioned in the introduction, the most important quantum algorithm for cryptography is Shor's algorithm (Shor, 1994). This algorithm uses quantum computers to efficiently solve two hard problems: IFP and DLP in Abelian groups. The idea behind Shor's algorithm is to compare the phases of prime numbers as sinus waves to factorise great integers. Peter Shor himself explained how this works, by comparing it to shining lights onto a diffraction grating to get a pattern. Using number theory, the problem of number factorisation can be converted into a search for the period of a really long sequence, or rather, the length at which a sequence repeats itself. Then, just as with light diffraction, this periodic pattern is run through a quantum computer which functions as a computational interferometer, creating an interference pattern. This will output the period, which can be processed using a classical computer, to factorise the number.

The reason why this works is that instead of finding a number, we are aiming towards finding a period, which is a global property rather than a singular point. While this is by no means easier if we were to use a traditional computer, a quantum computer can solve this efficiently. By using the qubits, we can create an extensive superposition across factors from the period, which can be obtained using a traditional computer. To do this, we must find a nontrivial factor of the number which is to be factorised. This factor is then used in the calculations which are done on the quantum computer. While quantum physics is no easy thing, the most essential part of these calculations is the quantum Fourier transform (QFT). The QFT maps two vectors of complex numbers to each other, effectively mapping a periodic sequence to its period.

The classical and quantum complexities for finding the order of a random element in $\mathbb{Z}_n^*$ are summarized below:

- Quantum complexity is in $\mathcal{O}\left((\log n)^2 \log\log(n) \log\log\log(n)\right)$.
- Best-known rigorous probabilistic classical algorithm has complexity in $e^{\mathcal{O}\left(\sqrt{\log n \log\log n}\right)}$.
- Best-known heuristic[1] probabilistic classical algorithm has complexity in $e^{\mathcal{O}\left(\sqrt[3]{\log n}\sqrt[3]{(\log\log n)^2}\right)}$.

Vazirani explored in detail the methodology of Shor's algorithm and showed how it can be used to solve DLP's (Vazirani, 1998). Starting from a random superposition state of two integers, and by performing a series of Fourier transformations, a new superposition can be set-up to give us with high probability two integers that satisfy an equation. By using this equation we can calculate the value r which is the unknown exponent in the DLP.

The classical and quantum complexities for finding discrete logarithms problem in $\mathbb{F}_q^*$ are summarized below:

- Quantum complexity is in $\mathcal{O}\left((\log q)^2 \log\log(q) \log\log\log(q)\right)$.
- Best-known rigorous probabilistic classical algorithm has complexity in $e^{\mathcal{O}\left(\sqrt{\log q \log\log q}\right)}$.
- Best-known heuristic probabilistic classical algorithm has complexity in $e^{\mathcal{O}\left(\sqrt[3]{\log q}\sqrt[3]{(\log\log q)^2}\right)}$.

Other quantum algorithms

There are other important quantum algorithms that also directly impact in cryptography but with a much less devastating effect than Shor's algorithm. While the best classical algorithm for a search over unordered data has complexity $\mathcal{O}(n)$, Grover's algorithm (Grover, 1996) performs the search on a quantum computer in only $\mathcal{O}(\sqrt{n})$ operations, a quadratic speedup. It works by replacing the qubits in a superposition of all possible states using Hadamard gates, and then enhancing the probability of the sought element. Grover's algorithm increases the speed at which it is possible to do a brute-force search for cryptographic keys (Grassl et al., 2016; Jang et al., 2020; Jaques et al., 2020). This affects all cryptographic algorithms, but a suficient counter-measure is to double the key-size.

The collision problem models collision-resistant hash functions in cryptography (Mittelbach and Fischlin, 2021). When building secure digital signature schemes, it is useful to have a family of hash functions $\{H_i\}$, such that finding a distinct (x,y) pair with $H_i(x) = H_i(y)$ is computationally intractable. The best known upper bound on the number of queries needed by a quantum computer to solve this problem with bounded error probability is $\mathcal{O}\left(\sqrt[3]{n}\right)$ (Brassard et al., 1997). This means that it is necessary to at least triple the length of the outputs of the hash functions to reach the current levels of security.

Post-quantum schemes

We now review the algorithmic hardness assumptions that are currently being used as the security basis of post-quantum public-key cryptography and we consider the main post-quantum schemes.

Lattice-based schemes

From the mathematical point of view, historically lattices have been studied since the 18th century by mathematicians such as Lagrange and Gauss. However, the interest in cryptography starts more recently with Ajtai's work, that proves the existence of one-way functions based on the hardness of the shortest vector problem (SVP). Ajtai showed how to construct provable secure hash functions based on hard lattice problems.

Definition 1: Let $\mathbb{R}^m$ be a m-Dimensional Euclidean Vector Space, and $B = \{b_1, \ldots, b_n\}$ be a set of n linearly independent vectors, the lattice $\mathscr{L}$ in $\mathbb{R}^m$ is the additive subgroup, that consists of all linear combinations of B with integer coefficients, in other words:

$$\mathscr{L}(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} x_i b_i : \; x_i \in \mathbb{Z}\}$$

where the vectors $b_1,\ldots,b_n$ are the called basis vector of $\mathscr{L}$ and the set B is called lattice basis.

The most important computational problem in lattices is the shortest vector problem (SVP). This problem is known to be NP-hard under random reduction (Ajtai, 1996) and it is defined as follows.

Definition 2 (SVP): Given the lattice $\mathscr{L}(B)$, one has to find a nonzero vector with minimum norm, typically in the Euclidean norm.

The following problems are also important for cryptographic purposes:

- closest vector problem (CVP): Given the lattice $\mathscr{L}(B)$ and a vector $t \in \mathbb{R}^m$, the goal is to find the vector $v \in \mathscr{L}(B)$ closest to t.
- shortest independent vector problem (SIVP): Given basis $B \in \mathbb{Z}^{m\times n}$, we must find n linearly independent lattice vectors $(v_1,\ldots,v_n)$, such that maximum norm among these vectors is minimum.

The versatility and flexibility of lattice based cryptography, in terms of possible cryptographic features and simplicity of the basic operations, make it one of the most promising lines of research in cryptography. Moreover, some lattice schemes are supported by security demonstrations that rely on the worst-case hardness of certain problems.

In 1997, Ajtai and Dwork proposed the first public-key cryptosystem from lattices, whose average-case security is based on the worst-case of the unique shortest vector problem (SVP) (Ajtai and Dwork, 1997). They claimed that their cryptosystem is provably secure, but in 1998, Nguyen and Ster refuted it (Nguyen and Stern, 1998). Furthermore, the AD public key is big and it causes message expansion making it an unrealistic public key candidate in post-quantum era.

The Goldreich-Goldwasser-Halevi (GGH) was published in 1997 (Goldreich et al., 1997). GGH makes use of the closest vector problem (CVP). Despite the fact that GGH is more efficient than Ajtai-Dwork (AD), in 1999, Nguyen proved that GGH has a major flaw; partial information on plaintexts can be recovered by solving CVP instances (Nguyen, 1999).

NTRU was published in 1998 (Hoffstein et al., 1998). It was originally constructed over polynomial rings but can also be defined over lattices, because the underlying problem can be interpreted as being SVP and CVP.

NTRU relies on the difficulty of factorizing certain polynomials making it resistant against Shor's algorithm. It is used for both encryption (NTRUEncrypt) and digital signature (NTRUSign) schemes. To provide 128-bit post-quantum security level NTRU demands 12 881-bit keys (Hirschhorn et al., 2009). A result reduces the security of NTRU-based cryptosystems to the worst-case problem over ideal lattices (Stehlé and Steinfeld, 2011). In 2013, Damien Stehle and Ron Steinfeld developed a provably secure version of NTRU (SS-NTRU) (Stehle and Steinfeld, 2013). In May 2016 a new version of NTRU called *NTRU Prime* was released (Bernstein et al., 2016). NTRU Prime countermeasures the weaknesses of several lattice based cryptosystems, including NTRU, by using different more secure ring structures.

Code-based schemes

Another class of hard algorithmic problems that is used as a basis of postquantum public-key cryptography comes from coding theory. Let $k \leq n$ be positive integers and let $\mathbb{F}_q$ be a finite field. The Hamming weight $w(u)$ of a vector $u \in \mathbb{F}_q^n$ is the number of nonzero components of u. The Hamming distance between two vectors u and v in $\mathbb{F}_q^n$ is $w(u-v)$.

Definition 3: A $[n,k]$ binary linear code $\mathscr{C}$ of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$, which can be represented by two matrices; a $k \times n$ generator matrix G, such that $\mathscr{C} = \{mG,\ m \in \mathbb{F}_q^k\}$ or by a $(n-k) \times n$ parity check matrix H, such that $\mathscr{C} = \{c \in \mathbb{F}_q^n,\ Hc^T = 0\}$, where $c \in \mathscr{C}$.

Several computational problems involving codes are intractable. The following problems are important for code-based cryptography. The general decoding problem (GDP) is defined as follows.

Definition 4 (GDP): Let $\mathbb{F}_q$ be a finite field, and let (G,t,c) be a triple consisting of a matrix $G \in \mathbb{F}_q^{k \times n}$, an integer $t < n$, and a vector $c \in \mathbb{F}_q^n$. The question if there is a vector $m \in \mathbb{F}_q^k$ such that $e = c - mG$ has Hamming weight $w(e) \leq t$.

The search problem associated with the GDP is to calculate the vector m given the word with errors c, known as the syndrome decoding problem (SDP).

Definition 5 (SDP): Let $\mathbb{F}_q$ be a finite field, and let (H,t,s) be a triple consisting of an $H \in \mathbb{F}_q^{(n-k)\times n}$, an integer $t < n$, and a vector $s\mathbb{F}_q^{(n-k)}$. The question is whether there is a vector $e \in \mathbb{F}_q^n$ with Hamming weight of $w(e) \leq t$ such that $He^T = s^T$.

Both the GDP and the SDP for linear codes are NP-complete (Berlekamp et al., 1978). In contrast to the overall results, the knowledge of the structure of certain codes makes the GDP and SDP soluble in polynomial time. A basic strategy to define code-based cryptosystems is therefore keep secret the information about the structure of the code and publish a code associated without any apparent structure (hence, by hypothesis hard to decode).

The first code-based cryptosystem is McEliece, which was proposed by Robert McEliece in 1978 (McEliece, 1978) and has not been broken during the last forty years. Encryption and decryption in the McEliece scheme can be performed very efficiently (Biswas and Sendrier, 2008) but has much larger key size than that of the RSA encryption (Rivest et al., 1978) and the Elgamal encryption (ElGamal, 1985) proposed almost at the same period, which prevented it from being widely used in applications. In addition, the McEliece cryptosystem adds redundancy during encryption, therefore the ciphertexts are longer than their corresponding cleartexts.

The security of the McEliece cryptosystem is very sensitive to the use of the binary Goppa code (Goppa, 1970, 1971), many attempts have been made to reduce the key sizes by replacing the binary Goppa code with other error-correcting codes, but failed in preserving the security of the cryptosystem. Although the security of code-based cryptography is related to the fact from the complexity theory that syndrome decoding in an arbitrary linear code is difficult, most known code-based cryptosystems typically use codes with special algebraic structures that allowefficient syndrome decoding, and the designers mainly focus on finding appropriate tricks (usually without theoretical guarantees) to hide the structures of those codes (Bucerzan et al., 2017). A well-known variant of the McEliece cryptosystem is the so-called Niederreiter cryptosystem (Niederreiter, 1986). However, both cryptosystems are equivalent in term of security when employing the same code (Li et al., 1994).

Multivariate polynomial cryptosystems

In 1983, Ong and Schnorr made the first attempt to construct multivariate signature (Ong and Schnorr, 1984). Although this signature scheme was found insecure (Pollard and Schnorr, 1987), it seemed to initiate the study of multivariate polynomial cryptography.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

The security of multivariate public key cryptosystems schemes is based upon the difficulty of solving nonlinear system of equations over finite fields (MQ), which is known to be NP-hard (Garey and Johnson, 1979). In particular, in most cases, such schemes are based upon multivariate systems of quadratic equations because of computational advantages. However, there are no multivariate polynomial cryptosystems whose security is guaranteed by the NP-hardness of the MQ problem. The past few decades have witnessed several multivariate cryptosystems, but most of them have been broken. The reason is that the MQ problems underlying most multivariate cryptosystems can be efficiently solved given some trapdoors, and the designers usually failed to hide those trapdoors in their multivariate cryptographic constructions from the adversary.

There exists a large variety of practical multivariate signature schemes. The best known of these are UOV (Kipnis et al., 1999), Rainbow (Ding and Schmidt, 2005), and pFlash (Ding et al., 2007). Additionally, there exist multivariate signature schemes from the HFEv- family, which produce very short signatures (e.g. 120 bit). The most promising scheme in this direction is Gui (Petzoldt et al., 2015). Signing and verifying with all of these schemes is very fast, presumably much faster than RSA and ECC (Chen et al., 2009). It was shown that, in general, encryption schemes were not as secure as it was believed to be, while signatures constructions can be considered viable.

Hash-based signatures

Just like the name suggests, this direction only focuses on constructing digital signatures from hash functions. The concept of digital signatures was introduced by Diffie and Hellman (Diffie and Hellman, 1976) and became popular after Ralph Merkle's work (Merkle, 1979). By relying on the Merkle-hash tree, one can construct digital signatures with multiple security solely from hash functions (Merkle, 1989). Hash-based signatures can be made very efficient if one allows the signer to keep a state of previously signed messages. There are also stateless hash-based signatures with worse efficiency. For now, the community still does not know how to construct other public-key cryptosystems beyond signatures solely from hash functions. Currently, the hash-based signature schemes Stateless Practical Hash-based Incredibly Nice Collision-resilient Signatures (SPHINCS) (Bernstein et al., 2015) is under evaluation for standardization (Alagic et al., 2020).

Conclusions

Year by year it seems that we are getting closer to create a fully operational universal quantum computer that can utilize strong quantum algorithms such as Shor's algorithm and Grover's algorithm. The consequence of this technological advancement is the absolute collapse of the present public key algorithms that are considered secure, such as RSA and Elliptic Curve Cryptosystems. The answer on that threat is the introduction of cryptographic schemes resistant to quantum computing using mathematical-based solutions like lattice-based cryptography, hash-based signatures, and code-based cryptography.

Post-quantum cryptography is aiming to provide cryptographic primitives that are secure against attacks using quantum computers. It is using mathematical problems that are believed to be hard to solve by both classical and quantum computers. Several post-quantum schemes are well understood and are considered strong candidates for standardization and practical application. Some post-quantum schemes have been known and investigated for many years. The efforts of the cryptographic community have been invaluable in analyzing and implementing schemes throughout the NIST process. NIST expects to select a small number of candidates for standardization by 2022 or 2023.

Referencias

Abdelrahman Abuarqoub, Simak Abuarqoub, Ahmad Alzu'bi, and Ammar Muthanna. The impact of quantum computing on security in emerging technologies. In *The 5th International Conference on Future Networks & Distributed Systems*, pages 171–176, 2021.

Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108, 1996.

Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 284–293, 1997.

Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the nist post-quantum cryptography standardization process. *US Department of Commerce, NIST*, 2020.

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

D Bernstein, J Buchmann, and E Dahmen. Post-quantum cryptography springer-verlag. *Berlin Heidelberg*, 2009.

Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017.

Daniel J Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. Sphincs: practical stateless hash-based signatures. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 368–397. Springer, 2015.

Daniel J Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine Van Vredendaal. Ntru prime. *IACR Cryptol. ePrint Arch.*, 2016:461, 2016.

Bhaskar Biswas and Nicolas Sendrier. Mceliece cryptosystem implementation: Theory and practice. In *International Workshop on Post-Quantum Cryptography*, pages 47–62. Springer, 2008.

Gilles Brassard, Peter Hoyer, and Alain Tapp. Quantum algorithm for the collision problem. *arXiv preprint quant-ph/9705002*, 1997.

Dominic Bucerzan, Vlad Dragoi, and Hervé Talé Kalachi. Evolution of the mceliece public key encryption scheme. In *International Conference for Information Technology and Communications*, pages 129–149. Springer, 2017.

Johannes A Buchmann, Denis Butin, Florian Göpfert, and Albrecht Petzoldt. Post-quantum cryptography: state of the art. *The new codebreakers*, pages 88–108, 2016.

Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang. Sse implementation of multivariate pkcs on modern x86 cpus. In *International workshop on cryptographic hardware and embedded systems*, pages 33–48. Springer, 2009.

Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography*, volume 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

Kunal Das and Arindam Sadhu. Challenges and trends on post-quantum cryptography. *Internet of Things*, pages 271–293, 2022.

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.

David Elieser Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 425(1868):73–90, 1989.

Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *International conference on applied cryptography and network security*, pages 164–175. Springer, 2005.

Jintai Ding, Bo-Yin Yang, Chen-Mou Cheng, Owen Chen, and Vivien Dubois. Breaking the symmetry: a way to resist the new differential attack. *Cryptology ePrint Archive*, 2007.

Ronny Döring and Marc Geitz. Post-quantum cryptography in use: Empirical analysis of the tls handshake performance. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pages 1–5. IEEE, 2022.

Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

Andre Esser, Alexander May, and Floyd Zweydinger. Mceliece needs a break–solving mceliece-1284 and quasi-cyclic-2918 with modern isd. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 433–457. Springer, 2022.

Richard P Feynman et al. Simulating physics with computers. *Int. j. Theor. phys*, 21(6/7), 1982.

ED Fiallo. A digital signature scheme mcfsˆqc-ldpc based on qc-ldpc codes. *Mathematical Aspects of Cryptography*, 12(4):99–113, 2021.

Michael R Garey and David S Johnson. *Computers and intractability*, volume 174. freeman San Francisco, 1979.

Teklay Gebremichael, Mikael Gidlund, Gerhard P Hancke, and Ulf Jennehag. Quantum-safe group key establishment protocol from lattice trapdoors. *Sensors*, 22(11):4148, 2022.

Sukhpal Singh Gill, Adarsh Kumar, Harvinder Singh, Manmeet Singh, Kamalpreet Kaur, Muhammad Usman, and Rajkumar Buyya. Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*, 52(1):66–114, 2022.

Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *Annual International Cryptology Conference*, pages 112–131. Springer, 1997.

Valerii Denisovich Goppa. A new class of linear correcting codes. *Problemy Peredachi Informatsii*, 6(3): 24–30, 1970.

Valerii Denisovich Goppa. A rational representation of codes and (l,g)-codes. *Problemy Peredachi Informatsii*, 7(3):41–49, 1971.

Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. Applying grover's algorithm to aes: quantum resource estimates. In *Post-Quantum Cryptography*, pages 29–43. Springer, 2016.

Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

Yasufumi Hashimoto. Recent developments in multivariate public key cryptosystems. In *International Symposium on Mathematics, Quantum Theory, and Cryptography*, pages 209–229. Springer, Singapore, 2021.

Julius Hekkala, Kimmo Halunen, and Visa Antero Vallivaara. Implementing post-quantum cryptography for developers. In *ICISSP*, pages 73–83, 2022.

Jack D. Hidary. Superposition, entanglement and reversibility. In *Quantum Computing: An Applied Approach*, page 3-13. Springer International Publishing, Cham, 2 edition, 2021.

Philip S Hirschhorn, Jeffrey Hoffstein, Nick Howgrave-Graham, and William Whyte. Choosing ntruencrypt parameters in light of combined lattice reduction and mitm approaches. In *International Conference on Applied Cryptography and Network Security*, pages 437–455. Springer, 2009.

Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *International algorithmic number theory symposium*, pages 267–288. Springer, 1998.

Lopamudra Hota and Prasant Kumar Dash. A taxonomy of quantum computing algorithms: Advancements and anticipations. In *Technology Road Mapping for Quantum Computing and Engineering*, pages 36–56. IGI Global, 2022.

Kyoungbae Jang, Hyunjun Kim, Siwoo Eum, and Hwajeong Seo. Grover on gift. *Cryptology ePrint Archive*, 2020.

Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. Implementing grover oracles for quantum key search on aes and lowmc. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 280–310. Springer, 2020.

David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909):237–243, 2022.

Petar Jurcevic, Ali Javadi-Abhari, Lev S Bishop, Isaac Lauer, Daniela F Bogorin, Markus Brink, Lauren Capelluto, Oktay Günlük, Toshinari Itoko, Naoki Kanazawa, et al. Demonstration of quantum volume 64 on a superconducting quantum computing system. *Quantum Science and Technology*, 6(2):025020, 2021.

Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer, 1999.

Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

Neal Koblitz and Alfred Menezes. A riddle wrapped in an enigma. *IEEE Security & Privacy*, 14(6):34–42, 2016.

Yuan Xing Li, Robert H Deng, and Xin Mei Wang. On the equivalence of mceliece's and niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.

Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

Ralph C Merkle. A certified digital signature. In *Conference on the Theory and Application of Cryptology*, pages 218–238. Springer, 1989.

Ralph Charles Merkle. *Secrecy, authentication, and public key systems.* Stanford university Ph.D. thesis, 1979.

Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

Arno Mittelbach and Marc Fischlin. *The Theory of Hash Functions and Random Oracles: An Approach to Modern Cryptography*. Springer, 2021.

Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.

Juha T Muhonen, Juan P Dehollain, Arne Laucht, Fay E Hudson, Rachpon Kalra, Takeharu Sekiguchi, Kohei M Itoh, David N Jamieson, Jeffrey C McCallum, Andrew S Dzurak, et al. Storing quantum information for 30 seconds in a nanoelectronic device. *Nature nanotechnology*, 9(12):986–991, 2014.

Phong Nguyen. Cryptanalysis of the goldreich-goldwasser-halevi cryptosystem from crypto'97. In *Annual International Cryptology Conference*, pages 288–304. Springer, 1999.

Phong Nguyen and Jacques Stern. Cryptanalysis of the ajtai-dwork cryptosystem. In *Annual International Cryptology Conference*, pages 223–242. Springer, 1998.

Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.

H Ong and Claus-Peter Schnorr. Signatures through approximate representations by quadratic forms. In *Advances in Cryptology*, pages 117–131. Springer, 1984.

Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design principles for hfev-based multivariate signature schemes. In *International conference on the theory and application of cryptology and information security*, pages 311–334. Springer, 2015.

J Pollard and C Schnorr. An efficient solution of the congruence $x^2 + ky^2 = m(modn)$. *IEEE Transactions on Information Theory*, 33(5):702–709, 1987.

Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

PC Sajimon, Kurunandan Jain, and Prabhakar Krishnan. Analysis of post-quantum cryptography for internet of things. In *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 387–394. IEEE, 2022.

Maximilian Schöffel, Frederik Lauer, Carl C Rheinländer, and Norbert Wehn. Secure iot in the era of quantum computers-where are the bottlenecks? *Sensors*, 22(7):2484, 2022.

Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

Alexander Sigov, Leonid Ratkin, and Leonid A Ivanov. Quantum information technology. *Elsevier*, page 100365, 2022.

D Stehle and R Steinfeld. Making ntruenrypt and ntrusign as secure as standard worst-case problems over ideal lattices. *Cryptology ePrint Archive, Report 2013/004*, 2013.

Damien Stehlé and Ron Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 27–47. Springer, 2011.

Purvı H Tandel and Jıtendra V Nasrıwala. Post-quantum cryptography: A solution to quantum computing on security approaches. In *Pervasive Computing and Social Networking*, pages 605–617. Springer, 2022.

Umesh Vazirani. On the power of quantum computation. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 356(1743):1759–1768, 1998.

Yazhen Wang. Quantum computation and quantum information. *Statistical Science*, 27(3):373–394, 2012.

Engin Zeydan, Yekta Turk, Berkin Aksoy, and S Bugrahan Ozturk. Recent advances in post-quantum cryptography for networks: A survey. In *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, pages 1–8. IEEE, 2022.

Conflicto de interés

Los autores no poseen conflictos de intereses.

Contribuciones de los autores

1. Conceptualización: Ernesto Dominguez Fiallo.
2. Curación de datos: Daymé Almeida Echevarría
3. Análisis formal: Ernesto Dominguez Fiallo, Daymé Almeida Echevarría, Ramsés Rodríguez Aulet.
4. Adquisición de fondos:
5. Investigación: Ernesto Dominguez Fiallo.
6. Metodología: Daymé Almeida Echevarría.
7. Administración del proyecto: Ernesto Dominguez Fiallo.
8. Recursos: Ernesto Dominguez Fiallo.
9. Software:
10. Supervisión: Ernesto Dominguez Fiallo.
11. Validación: Ramsés Rodríguez Aulet.
12. Visualización: Daymé Almeida Echevarría.
13. Redacción - borrador original: Ernesto Dominguez Fiallo.
14. Redacción - revisión y edición: Ramsés Rodríguez Aulet.

Financiación

La investigación no requirió fuente de financiamiento.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 114-133

Notes

[1]By heuristic algorithm, we mean the proof of its running time makes some plausible but unproven assumptions.