Lattice-Based Cryptography in the Quantum Era: A Survey

Mauricio Cisneros
20192624@aloe.ulima.edu.pe
https://orcid.org/0009-0007-4056-4467
Universidad de Lima, Perú

Javier Olazabal
20191425@aloe.ulima.edu.pe
https://orcid.org/0009-0003-2728-8614
Universidad de Lima, Perú

Recibido: 31 de agosto del 2023 / Aceptado: 2 de octubre del 2023
doi: https://doi.org/10.26439/interfases2023.n018.6631

ABSTRACT. The advent of quantum computing reveals current classical cryptography's incapacity to withstand attacks within the new paradigm. Quantum algorithms break such encryption with impressive ease, with Shor and Grover algorithms being the main perpetrators. Lattice-based key encryption is the suggested solution in multiple instances, as the complexity and randomness that these methods add to message encryption make them one of the best short- and medium-term solutions. In 2016, NIST launched a contest to find algorithms to incorporate into its security standard. Four algorithms from the third round were selected to be standardized, including the lattice-based CRYSTALS-kyber. Of the latter, variants have been and are still being developed that manage to amend some weaknesses found in its implementation, such as side-channel attacks or performance issues. This investigation discusses different publications on lattice-based cryptography in conjunction with cryptanalysis in the quantum era.

KEYWORDS: post-quantum / lattice-based / quantum computing / kyber / quantum cryptanalysis

Criptografía *lattice-based* en la era cuántica: una revisión

RESUMEN. La llegada de la informática cuántica anuncia la inadecuación de la criptografía clásica actual para resistir los ataques dentro de este nuevo paradigma. Los algoritmos cuánticos rompen este tipo de cifrado con una facilidad impresionante, siendo los algoritmos de Shor y Grover los principales culpables. El cifrado de claves basado en celosías es la solución propuesta en múltiples ocasiones, ya que la complejidad y aleatoriedad añadidas al cifrado de mensajes mediante estos

métodos los convierten en una de las mejores soluciones a corto y medio plazo. En 2016, el NIST lanzó un concurso para encontrar los algoritmos que formarán parte del estándar de seguridad, y en la tercera ronda se seleccionaron cuatro algoritmos para ser estandarizados, entre ellos uno basado en celosía, CRYSTALS-kyber. A partir de él, se desarrollaron y se están desarrollando variantes que consiguen solventar algunas debilidades encontradas en la implementación, como ataques de canal lateral o problemas de rendimiento. En la presente investigación se discuten diferentes publicaciones relativas a la criptografía basada en celosías en conjunción con el criptoanálisis en la era cuántica.

PALABRAS CLAVE: post-quantum / lattice-based / quantum computing / kyber / quantum cryptanalysis

1. INTRODUCTION

Quantum computing is the latest effort to combine physics and computer science. This novel computing paradigm was first introduced by Paul Benioff (1980) in his 1980 investigation, where he used Schrödinger's equation to describe the Turing machine. (Mor & Renner, 2014). These quantum computers can generate information by exploiting the principles of quantum mechanics, especially quantum entanglement and superposition through the use of qubits, or quantum bits, which are the building blocks of quantum circuits (Schumacher, 1995).

The primary study for the use of qubits is quantum superposition and error correction. Quantum superposition consists of a qubit's ability to take a probabilistic state of two values. As is shown in Figure 1, qubits are represented by spheres known as "Bloch's spheres" with two opposing poles that represent "1" and "0" respectively. These spheres also include a vector that "points" in an arbitrary direction to signify an increased or decreased chance of measuring "1" or "0". This distribution of probabilities is presented in the following linear combination:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad (1)$$

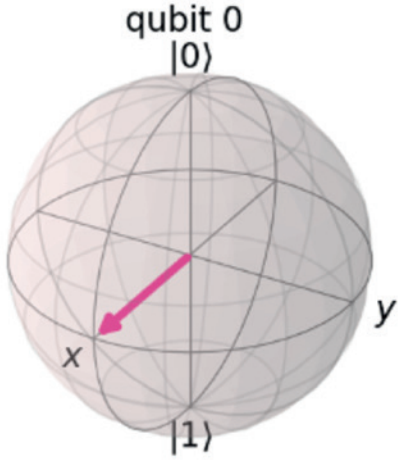
where ψ is the probability column vector and follows the next restriction:

$$|\alpha|\,\hat{}\,2 + |\beta|\,\hat{}\,2 = 1 \qquad (2)$$

where "α" presents the probability of "0" and "β" a measurement of "1". However, because these machines are mostly made of physical components, they generate noise when being used; for this reason, error correction is utilized. (Nielsen & Chuang, 2000)

Figure 1

Qubit representation through Bloch's sphere



Note. qiskit.visualization library

Because of the ability to effectively use quantum superposition, this computing paradigm poses a threat to the public key encryption protocols, currently regarded as the most resilient protocols in use (Allende et al., 2023). In 1994, Peter Shor developed the super algorithm now known as Shor's algorithm. This algorithm is capable of factoring integers in logarithmic time using quantum computing (Hekkala et al., 2023).

Presently, cryptographic keys based on complex mathematical operations like AES, RSA, ECC, Diffie-Hellman, and Blowfish are trusted. A longer key involves more complex mathematical operations. These mathematical operations utilized by cryptographic methods are nearly impossible to crack using classical computers. However, as we have stated, quantum computing utilizes qubits instead of regular bits, which changes the codification of data and allows for multiple stages to be completed simultaneously. As the number of qubits increases, so does the calculation speed. This should be worrying, as it is a threat to the current encryption protocols for public keys (Vaishnavi & Pillai, 2021).

Peter Shor's discovery in 1994 effectively marks the introduction of this threat. His algorithm efficiently solves the IFP (Integer Factoring Problem) in logarithmic time (Wang & Zhang, 2021), as well as the DLP (Discrete Logarithm Problem). What it demonstrated was that, by starting with the superposition of two integers and executing a series of Fourier transforms, it is possible to achieve a new superposition with a high probability of yielding two integers that satisfy the equation (Mavroeidis et al., 2018). Furthermore, the work of Schwebe and Westerbaan (2016), demonstrated that over time, as the quantity of qubits needed for cracking encryption decreases, so does the complexity of the implementation of quantum algorithms. In short, this will lead to a vulnerability in the cryptographic algorithms and will be exploited for cyberattacks.

Cyberattacks are as old as computers. The value perceived in having access to confidential information makes the data an enticing target for cybercriminals. The reasons behind cyberattacks are outside the scope of this research, but it's worth pointing out that according to the book "Psychology and Crime" most attacks are motivated by a monetary incentive; the perceived value of accessing private networks or sensitive and confidential information is very high. Additionally, the intrinsic anonymity of cyberattacks protects the attackers (Sammons & Putwain, 2018).

The introduction of quantum computing at a commercial level will create an uncomfortable situation for industries and companies that don't prepare ahead of time. Focusing solely on public key encryption algorithms, the prowess of quantum computers will phase out most of these algorithms, forcing information systems to make a radical change in their encryption systems (Alyami et al., 2022).

Google and IBM are already developing quantum processors. In 2019, Google released Sycamore, a 56-qubit processor capable of making a million quantum measurements in 200 seconds. Google claimed to have reached quantum supremacy, as the same measurements would take a classical supercomputer 10,000 years, by their estimation. (Arute

et al., 2019). However, security is bound to get better. Three years before this release, the National Institute of Standards and Technology (NIST) launched a contest for the standardization of post-quantum algorithms, that is to say, a call for algorithms capable of resisting cyberattacks launched through quantum computers and algorithms (Moody, 2022).

It was found that the lattice-based algorithm family provides enough protection against quantum attacks. Consequently, this research will now be centered around lattice-based encryption algorithms, which are generally computationally efficient and resilient against quantum attacks (Kumari et al., 2022). These algorithms work by creating two sets of n 'n' vectors that replace public and private keys. The number of dimensions factored in increases or decreases the complexity, and with it, the security. Analogous to typical private and public key encryption, the private set will make it easier to calculate the lattice (Bernstein et al., 2017).

The development and implementation of new post-quantum algorithms or variants of existing algorithms is necessary for the maintenance of the present information systems. For this reason, there appears to be a necessity to explore and develop novel approaches to fortify the security and efficiency of these algorithms, in preparation for the quantum era. At present, relatively few algorithms are designed to be resistant to quantum attacks. There are existing inquiries into algorithms resistant to quantum attacks, such as the work of Xiao et al. (2023), where a lattice-based cryptosystem is presented and compared with other cryptosystems in order to demonstrate that their proposal is better in terms of resilience. Another situation where lattice-based cryptography has proven to be better is in the application of the Regev scheme to the LWE problem (Learning With Errors), which, in its worst-case scenario, can be reduced to the SIVP (Shortest Independent Vector Problem), enhancing the performance and security of the algorithm. (Nejatollahi et al., 2019). This performance can also be improved with the new paradigm, as shown in Ura et al. (2023), where quantum annealing is used to solve the SVP for the search of states in qubits.

Based on the given context, this survey will serve to answer the following questions:

- What advances have there been regarding quantum computing?
- What is necessary to know in order to analyze the weaknesses of current cryptography?
- What is the proposal of lattice-based cryptography for protection?

The research papers presented in this survey will answer these questions.

2. STATE OF THE ART

This state-of-the-art section will be divided into three parts: advances in quantum computing, that is, the advances on quantum hardware such as processors, computing

supplies; the creation of quantum modules to enhance the speed of classic computers; and quantum algorithms that pose a threat, basically Shor and Grover's algorithms. However, it's worth noting that there are more algorithms that present a threat, such as Simon's algorithm. The second subsection will touch on quantum cryptanalysis. In this survey about lattice-based post-quantum cryptography, we have to discuss the reason why it is such a good alternative to current public and private key encryption. Metrics for the analysis will be surveyed as well. Finally, the most important part of this paper is lattice-based post-quantum cryptography as an algorithm family. This section will address the algorithm CRYSTALS-Kyber and its variants.

2.1. Quantum computing advances

This section details the latest discoveries, research and developments in quantum computing, including advances in hardware and algorithms, as well as the construction of stable and reliable qubits. As mentioned previously, in general, the use of qubits needs to factor in error correction; this is a weakness inherent to this technology. However, different architectures and qubit distributions are being experimented with in order to address this. From a hardware perspective, quantum computing is a very recent development. Because of this, the research papers considered for this survey date to 2019 and onward. Unless it covers an algorithm developed in the past that is important to note, such as Grover's or Shor's, it won't be taken into account.

It is important to note that these studies began approximately 50 years ago with Stephen Wiesner's description of conjugate coding (Mor & Renner, 2014), a system in which multiple messages are transmitted and reading one destroys the others. In the following years, Paul Benioff would describe Turing's machine employing Schrödinger's equation, and in 1982, he made a model for the quantum computer (Mor & Renner, 2014). Based on this model, mathematician Peter Shor and computer scientist Lov Grover developed their corresponding famous algorithms, of which the former was able to break present encryptions by means of quantum Fourier transform (Shor, 1997) and the latter could find collisions through the concept of speeding up database search (Grover, 1996).

2.1.1. *Hardware advances*

At present, progress in quantum hardware is the result of a race between different companies. Most breakthroughs are published by researchers working for IBM and Google; there are others, like Intel, who are working on quantum computers, as well as big tech companies like Amazon and Microsoft. Quantum processing units are mainly designed using two different technologies: superconductors and silicon-based semiconductors. Both technologies are presented in Table 1, but they are largely dependent on extremely low temperatures to work correctly. Semiconductor technology has an inherent advantage in that it is practically immune to noise, which eliminates the need to work

with error correction. This immunity is not perfect, and the development of quantum processing units resistant to errors is still a subject of ongoing effort and work. It will take a significant amount of time and work to arrive at error-resistant quantum processing units (Zhilong et al., 2022).

Table 1

Comparison between superconductors and semiconductors between processor units

Metric	Superconductors	Semiconductors
Temperature	10 miliKelvin	1 - 1.5 Kelvin
Advantages	Relatively easier manufacture	Noise resistant
Disadvantages	Susceptible to noise	Relatively difficult manufacture

In 2019, Google researchers published a paper introducing Sycamore, their new 53-qubit quantum processor, which they claimed to have achieved quantum supremacy. Quantum supremacy is understood as the ability of a quantum computer to be orders of magnitude better than any classic computer at quantum measurements. The same paper stated that Sycamore could perform its measurements in 200 seconds, compared to the 10,000 years that classical computer would take to complete the task, for which quantum supremacy had been achieved (Arute et al., 2019). This statement would have been confirmed based on the complexity theory described by Aaronson and Chen (2017). However, researchers were able to replicate this by using 512 GPUs, disproving quantum supremacy.

IBM does not lag behind in the quantum race. In 2022, Riel (2022) published the roadmap for quantum development. Presently, they have managed to unveil a 127-qubit processor called Eagle; it has been used in contests conducted by the company to promote Qiskit, their quantum library for quantum development. The roadmap outlines the scaling of the development, looking at suppression and error mitigation as developmental steps that lead to in a 4158-qubit processor, the Kookaburra, for the year 2025.

Intel has also participated in the development of quantum processing units, opting for silicon-based rather than superconductors, and have released a 12-qubit chip using this technology (Intel, 2023). As stated earlier, silicon-based qubits are noise-resistant and may be the best bet for developing larger systems. This resistance can be improved: Kobayashi et al. (2023) proposed a method for reducing errors by means of a feedback-based reboot protocol with which the necessary fidelity for scaling the system could be achieved.

Table 2 shows the aforementioned technologies in some detail. In summary, the research revolves around superconductor and semiconductor qubits, both exhibit and

could contain the necessary fidelity for scaling into larger quantum computers. Both Google and IBM are actively researching superconducting qubits, while other companies, like Intel, research silicon-based semiconductor qubits.

Table 2

Technologies presented in the section

Authors	Paper	Presented Technology
Zhilong et al. (2022)	Superconducting and Silicon-Based Semiconductor Quantum Computers: A review.	Semi and superconducting qubits
Arute et al. (2019)	Quantum supremacy using a programmable superconducting processor.	Sycamore processor
Cho (2023)	Ordinary computers can beat Google's quantum computer after all.	Classic computers
Riel (2022)	Quantum Computing Technology and Roadmap.	127-qubit Eagle processor
Intel. (2023)	Intel's New Chip to Advance Silicon Spin Qubit Research for Quantum Computing.	12-qubit Tunnel Falls semiconducting processor
Kobayashi et al. (2023)	Feedback-based active reset of a spin qubit in silicon.	Semiconducting Qubits

2.1.2. *Algorithms*

Based on the context provided in 2.1.1., we will touch on the reasons why advances in quantum computing are a threat to cryptography. The development of Shor's algorithm makes it possible to factorize numbers in a super-efficient way. Unfortunately, this is a big threat, as it can crack the encryption of public keys. In 2021, Gouzien and Sangouard (2021) and Gidney and Ekerå (2021) demonstrated that it is possible to crack RSA encryption in 177 days and eight hours, correspondingly.

Quantum computers pose a threat to data communication systems in general. At present, quantum computers do not have the capability to be a total threat; therefore, it is necessary to make the best of time and prepare for the imminent arrival of the quantum threat. Zeydan et al. (2022) argued that asymmetric encryption systems will be vulnerable to attacks using Shor's algorithm, while Blockchain systems and data centers will be vulnerable to Grover's, although to a lesser extent (Allende et al., 2023), (Zeydan et al., 2022).

2.2 Quantum cryptanalysis

This section will cover studies that revolve around cryptanalysis. This is an area of study in cryptography that aims to locate weaknesses and crack cryptographic security systems. Currently, the classic cryptanalysis schemes are not strong enough to crack the current security systems like AES and RSA. Therefore, there is a trend of analyzing cryptographic systems using quantum computing, known as quantum cryptanalysis. This section is divided into two subsections; quantum cryptanalysis techniques and evaluation metrics.

2.2.1. *Quantum cryptanalysis techniques*

Currently, quantum cryptanalysis techniques are at the forefront of advances in theoretical quantum computing, the reason being that they allow to test for vulnerabilities in cryptographic systems, in preparation for the arrival of quantum computers that could crack these algorithms. Consequently, different techniques of quantum cryptanalysis are plotted. In their paper, Xie and Yang (2019) propose different quantum methods to attack cipher blocks according to a scheme of three Feistel rounds in order to partially obtain the Even-Mansour construction key; this new quantum algorithm has the Bernstein-Vazirani algorithm a as subroutine. Three types of cryptanalysis are described in said paper: quantum differential analysis, quantum differential analysis of low probability and impossible quantum differential analysis. Another work describing novel techniques is a paper by Jing et al. (2020), where Shor's algorithm is part of a cryptanalysis scheme of digital signatures. To ascertain that the scheme is vulnerable to quantum attacks, they can transform the public keys of the scheme into a system of linear equations using Shor's algorithm. Another work that explores this paradigm's virtues in the cryptanalysis context is the work of Roman'kov et al. (2023). In the paper, an algebraic attack is performed on two digital signature schemes. Finally, another work that explores the virtues of quantum cryptanalysis is the work of Ding et al. (2018), in which a cryptanalysis of a cryptosystem based on Diophantine equations is conducted. This attack is directed towards the LLL algorithm, which is a post-quantum algorithm in classical computing, in contrast to other works that use quantum algorithms instead. Table 3 analyzes different papers on quantum techniques in which the cryptanalysis studies classical and post-quantum algorithms. In addition, different cryptographic schemes are explored in order to understand how quantum algorithms could threaten them.

Table 3

Papers on quantum cryptanalysis techniques

Authors	Paper	Utilized Algorithm	Cryptographic scheme
Xie y Yang (2019)	Using Bernstein–Vazirani algorithm to attack block ciphers.	Bernstein-Vazirani	3-round Feistel
Jing et al. (2020)	Cryptanalysis of a Public Key Cryptosystem Based on Data Complexity under Quantum Environment	Shor	Public key and signature
Roman'kov et al. (2023)	Algebraic and quantum attacks on two digital signature schemes	Shor	2 digital signatures
Ding et al (2018)	Cryptanalysis of a public key cryptosystem based on Diophantine equations via weighted LLL reduction	Lattice-based Weighted LLL	Performance Based on Diophantine equations

2.2.2 *Evaluation metrics*

In cryptanalysis, it is necessary to consider the theoretic-formal demonstration of a vulnerability in a cryptosystem. This encompasses the use of quantitative metrics that allow evaluation on a numerical level, as is the case with the cryptosystem attacked. Seck et al. (2022) talk about the different metrics, the primary one being attack and execution time. In this case, the attacks used were two Veron variants and the two schemes were compared by key and signature size. In another instance, Jaques and Schanck (2019) suggest applying cryptanalysis to a cryptosystem based on super singular isogeny key encapsulation, known as SIKE, and employing different metrics such as the quantum computational cost of memory. To this end, they tested Grover, Tani, and VW quantum attacks. Finally, Banegas (2020) conducts these cryptanalysis methods on the ECC encryption algorithm, this time based upon the quantum gate computational cost regarding the depth of the gates and the number of qubits used by the quantum attack. Table 3 provides a summary of the research presented. Table 4 compares the different metrics used in the different quantum algorithms. The comparison is based on the public key bit size and digital signature, the quantum cost mentioned in Banegas (2020) and computational cost. The computational space of the RAM usage was also factored in.

Table 4

Research papers on cryptanalysis evaluation metrics

Authors	Paper	Utilized Algorithm	Metrics
Seck et al. (2022)	Cryptanalysis of a Code-Based Identification Scheme Presented in CANS 2018	Veron	Public and private size in bits
Jaques y Schanck (2019)	Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE	Grover, Tani y VW	Quantum computational cost in RAM
Banegas (2020)	Concrete quantum cryptanalysis of binary elliptic curves	Shor	Quantum logic and computational cost

2.3 Lattice-based algorithm family

This section discusses research on different public and private KEM and similar algorithm implementations. It first touches on some lattice-based variants, before moving on to some CRYSTALS-Kyber related works. This last section is the starting point for this survey and it introduces some issues in the latest release. Finally, some original implementations will be discussed that are not CRYSTALS-Kyber variants.

2.3.1 *Variants*

There are a series of variants within the lattice-based algorithm family that have been and are continuously being developed. This algorithm family was predominant in the NIST contest, as it has proven to be resilient enough against different crypto schemes based on public keys, digital signatures and key exchange mechanisms. As shown in Table 5, there are multiple variants within the lattice-based family, each one a particular example of a special utilization of the aforementioned schemes. As part of the same family, they all share basic problems to solve.

These problems are Learning with Errors (LWE), Shortest Vector Problem (SVP), Closest Vector Problem (CVP), Shortest Integer Solution (SIS), Learning with Rounding (LWR), etc. Furthermore, the size of both generated keys must be compared in order to demonstrate which algorithms are the most computationally efficient. Lastly, it is worth noting that, because of the particularities of each algorithm due the schemes that they are based on, the performance comparison is subjective, for which Table 5 is, in a way, a summary of the most relevant algorithms.

Table 5

Lattice-based algorithm family variants

Authors	Variant name	Scheme	Solved problem	Secret Key (Size in bytes)	Public Key (Size in bytes)
Bos et al. (2018)	Kyber light	Key Exchange	LWE	832	736
Bos et al. (2018)	Kyber Paranoid	Key Exchange	LWE	1664	1440
Hülsing et al. (2017)	NTRU KEM	Key Encapsulation	NTRU	1422	1140
Bernstein et al. (2016)	NTRU Prime	Key Encapsulation	NTRU	1417	1232
Saarinen et al. (2017)	HILA5	Key Encapsulation / Public key	Ring - LWE	1792	1824
Cheon et al. (2017)	Lizard.CCA	Public Key Encryption	LWE / LWR	557056	6553600
Alkim et al. (2015)	TESLA-128	Digital Signature	LWE	1010000	1330000
Alkim et al. (2015)	TESLA-256	Digital Signature	LWE	1057000	2200000
Ducas et al. (2017)	Dilithium rec.	Digital Signature	MLWE	3504	1472
Ducas et al. (2017)	Dilithium High.	Digital Signature	MLWE	3856	1760
Alkim et al. (2020)	Frodo-976	Key Encapsulation	LWE	31272	15632
Alkim et al. (2020)	Frodo-640	Key Encapsulation	LWE	19872	9616
D'Anvers et al. (2018)	SABER	Public Key Encryption / Key encapsulation	LWR	3040	1312

2.3.2 *CRYSTALS-Kyber related works*

Because our main focus is the lattice-based algorithm family, the most relevant algorithm to this paper is CRYSTALS-Kyber, an algorithm that was selected for standardization. In July 2022 (Moody, 2022), NIST reported the status of their global contest in search of

resilient cryptographic algorithms against quantum attacks to be added to the standard. The first lattice-based model that met the necessary indicators was CRYSTALS-Kyber (Avanzi et al., 2020). This algorithm solves the LWE problem. The problem is based on the premise that linear equations are harder to solve when random noise is added. This random noise is added to the lattices in the finite body created through the set of vectors created as keys.

Most research about CRYSTALS-Kyber focuses primarily on solving weaknesses present in the algorithm. In Y. Yang et al. (2023), the scientists go above and beyond the scope of cryptographic algorithms. When any given algorithm is implemented, it has to be run on a physical computer. This physical aspect entails a series of weaknesses that can be exploited by using a "side-channel attack". These types of attacks are based on the idea that it is possible to measure the energy being used for each operation. The paper mentioned above presents a CPA attack on the CRYSTALS-Kyber. Researchers used the referential implementation of the algorithm, and employed the input of a preselected ciphertext to measure the amount of energy expended. It was observed that CRYSTALS-Kyber can effectively hide if it knows the ciphertext from a previous use. The researchers later tried to present a variant of it, but it was unable to hide traces of known ciphertexts.

There have been other instances lattice-based family algorithm implementation. In Soni et al. (2022), the researchers developed an algorithm based on the Diffie-Hellman key exchange. The main idea was to find a method that made it possible to use a relatively small key without losing any flexibility or security; here, resilience was tested by implementing Shor's. In N. Yang et al. (2024), the proposal was to encrypt the vectors with inner product encryption. Instead of using the basic version of LWE, the scientists opted to use middle-product learning with errors, or MP-LWE, where the error generation is made with the product of two polynomial equations. The method would add security given that it is no longer based on linear equations.

Table 6 details the primary research as well as the research mentioned above. The table lists the algorithms used, which are either combinations of lattice-based algorithms or a variant of CRYSTALS-Kyber. In general, when studying these algorithms, they are studied using a Shor's algorithm attack for its ability to factorize (Soni et al., 2022). However, other researchers focus on the physical aspects of the systems. Lastly, there are others that land on completely original algorithms, or a compatible combination of algorithms that improve upon a past iteration.

Table 6

Presented papers on lattice-based algorithm

Author	Paper	Algorithm used	Metric used	Attack studied
Y. Yang et al. (2023)	Chosen ciphertext correlation power analysis on Kyber.	Kyber	Quantity of utilized energy	Side-channel attack
Soni et al. (2022)	Quantum-resistant public-key encryption and signature schemes with smaller key sizes	Lattice-based, Diffie-Hellman	Size, efficiency, and security of keys	Shor's Algorithm
Bos et al. (2018)	CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM.	Kyber	Flexibility Security Performance	CCA IND-CPA
N. Yang et al. (2024)	Inner product encryption from Middle-Product Learning With Errors.	Lattice-based MP-LWE Inner product encryption	Performance Computational complexity Flexibility	None presented
Chen, S., & Chen, J. (2023)	Lattice-based group signatures with forward security for anonymous authentication	Lattice-based Family of algorithms	Security Performance Computational lightness	Shor

3. CONCLUSIONS

This survey has attempted to analyze different research papers dealing with post-quantum cryptography and the imminent arrival of quantum computing. Scientific development is at the vanguard of its eventual arrival, for which different cryptosystems and cryptanalysis methods are proposed in order to meet future needs. We analyzed the present state of lattice-based variants and the different ways to evaluate the vulnerabilities of new post-quantum cryptosystems.

The advancement of quantum computing is making big strides. At this time, it is still in an incubation stage of sorts; however, the advances and competition between big tech companies accelerate the conversation and achievements in the field. This new computational paradigm will most likely become the new computing revolution. IBM and Google dominate the research at present, with both companies having already designed quantum computers that are physically similar to early computers, whose development

into household computers is to be expected. In addition, this is a very exciting paradigm and research topic. There are new achievements and developments on a weekly basis. During the production of this paper, Intel released their 12-qubit processor.

To analyze the vulnerabilities of current cryptography, it is necessary to take the limits and abilities of quantum computing to crack encryptions into account. We must first look at quantum cryptanalysis, as its use will be of help in detecting weaknesses against quantum attacks. Section 2.2 dealt with quantum cryptanalysis, exploring different evaluation metrics such as quantum computational cost in quantum gates, the use of quantum memory and algorithmic complexity.

Finally, we explored the lattice-based algorithm family. In our survey, we discussed the different variants present in this family. This family studies different lattice problems as well as different cryptographic schemes such as KEM, PK, SK, and Digital Signatures. These algorithms have proved resilient enough to be a great alternative against the imminent quantum threat. As of today, CRYSTALS-Kyber has gained significant relevance and traction thanks to its future standardization by NIST. The NIST contest, however, has not come to a close yet and is still in search of new algorithms.

4. FUTURE WORK

This work dealt with the topic of lattice-based algorithm family, with a special focus on the CRYSTALS-Kyber algorithm. This is an IND-CCA2-secure key encapsulation mechanism based on the security of LWE, or Learning With Errors. There is a method based on LWE known as learning with rounding. In future work, we recommend exploring this alternate module in order to develop a variant based on a different point of view for the algorithm.

REFERENCES

Aaronson, S., & Chen, L. Q. (2017). Complexity-theoretic foundations of quantum supremacy experiments. *Quantum Physics*, *67*. https://doi.org/10.5555/3135595.3135617

Allende, M., León, D. L., Cerón, S., Pareja, A., Pacheco, E., Leal, A., Da Silva, M., Pardo, A., Jones, D., Worrall, D. J., Merriman, B., Gilmore, J., Kitchener, N., & Venegas-Andraca, S. E. (2023). Quantum-resistance in blockchain networks. *Scientific Reports*, *13*(1). https://doi.org/10.1038/s41598-023-32701-6

Alkim, E., Bindel, N., Buchmann, J., Dagdelen, Ö., Eaton, E., Gutoski, G., Krämer, J., & Pawlega, F. (2015). *Revisiting TESLA in the quantum random oracle model*. Cryptology ePrint Archive, Paper 2015/755. https://eprint.iacr.org/2015/755

Alkim, E., Bos, J. W., Ducas, L., Easterbrook, K., LaMacchia, B., Longa, P., Mironov, I., Naehrig, M., Nikolaenko, V., Peikert, C., Raghunathan, A., & Stebila, D. (2020). *FrodoKEM: Learning with errors key encapsulation*. https://frodokem.org/.

Alyami, H., Nadeem, M., Alosaimi, W., Alharbi, A. G., Kumar, R., Gupta, B. K., Agrawal, A., & Khan, R. A. (2022). Analyzing the Data of Software Security Life-Span: Quantum Computing Era. *Intelligent Automation Soft Computing*, *31*(2), 707-716. https://doi.org/10.32604/iasc.2022.020780

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandão, F. G. S. L., Buell, D. A., Burkett, B. J., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., . . . Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505-510. https://doi.org/10.1038/s41586-019-1666-5

Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2020). *Algorithm Specifications And Supporting Documentation*. NIST Report.

Banegas, G. (2020). *Concrete quantum cryptanalysis of binary elliptic curves*. https://ia.cr/2020/1296

Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, *22*(5), 563-591. https://doi.org/10.1007/bf01011339

Bernstein, D., Buchmann, J., & Dahmen, E. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188-194. https://doi.org/10.1038/nature23461

Bernstein, D. J., Chuengsatiansup, C., Lange, T., & Van Vredendaal, C. (2016). *NTRU Prime: reducing attack surface at low cost*. Cryptology ePrint Archive, Paper 2016/461. https://eprint.iacr.org/2016/461

Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2018). *CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM*. https://doi.org/10.1109/eurosp.2018.00032

Cheon, J. H., Park, S., Lee, J., Kim, D., Song, Y., Hong, S., Kim, D., Kim, J., Hong, S. M., Yun, A., Kim, J., Park, H., Choi, E., Kim, K., Kim, J., & Lee, J. (2017). *Lizard. Lizard Public Key Encryption Submission to NIST proposal*. National Institute of Standards and Technology.

Chen, S., & Chen, J. (2023). Lattice-based group signatures with forward security for anonymous authentication. *Heliyon*, *9*(4). Elsevier BV. https://doi.org/10.1016/j.heliyon.2023.e14917

Cho, A. C. (2023, June 25). Ordinary computers can beat Google's quantum computer after all. *Science | AAAS*. https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all

D'Anvers, J., Karmakar, A., Roy, S. S., & Vercauteren, F. (2018). Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM. En *Progress in Cryptology - AFRICACRYPT 2018* (pp. 282-305). Springer eBooks. https://doi.org/10.1007/978-3-319-89339-6_16

Ding, J., Kudo, M., Okumura, S., Takagi, T., & Tao, C. (2018). Cryptanalysis of a public key cryptosystem based on Diophantine equations via weighted LLL reduction. *Japan Journal of Industrial and Applied Mathematics*, *35*(3), 1123-1152. https://doi.org/10.1007/s13160-018-0316-x

Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehle, D. (2017). *CRYSTALS - Dilithium: Digital Signatures from Module Lattices*. Cryptology ePrint Archive, Paper 2017/633. https://eprint.iacr.org/2017/633

Gidney, C. & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.22331/q-2021-04-15-433

Gouzien, E. & Sangouard, N. (2021). Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory. Physical Review Letters, 127, https://doi.org/10.1103/PhysRevLett.127.140503

Hekkala, J., Muurman, M., Halunen, K., & Vallivaara, V. (2023). Implementing Post-quantum Cryptography for Developers. In *SN Computer Science* (vol. 4). Springer Science and Business Media LLC. https://doi.org/10.1007/s42979-023-01724-1

Hülsing, A., Rijneveld, J., Schanck, J. M., & Schwabe, P. (2017). *High-speed key encapsulation from NTRU*. Cryptology ePrint Archive, Paper 2017/667. https://eprint.iacr.org/2017/667

Intel. (2023, June 15). *Intel's New Chip to Advance Silicon Spin Qubit Research for Quantum Computing*. https://www.intel.com/content/www/us/en/newsroom/news/quantum-computing-chip-to-advance-research.html#gs.1o8uud

Jaques, S., & Schanck, J. M. (2019). Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE. En *Lecture Notes in Computer Science* (pp. 32-61). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-26948-7_2

Jing, Z., Gu, C., Ge, C., & Shi, P. (2020). *Cryptanalysis of a Public Key Cryptosystem Based on Data Complexity under Quantum Environment*. Mobile Networks and Applications. https://doi.org/10.1007/s11036-019-01498-y

Kobayashi, T., Nakajima, T., Takeda, K., Noiri, A., Yoneda, J., & Tarucha, S. (2023). Feedback-based active reset of a spin qubit in silicon. *Npj Quantum Information*, *9*(1). https://doi.org/10.1038/s41534-023-00719-3

Kumari, S., Singh, M., Singh, R. P., & Tewari, H. (2022). A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for

IoT devices. *Computer Networks*, *217*, 109327. https://doi.org/10.1016/j.comnet.2022.109327

Mavroeidis, V., Vishi, K., Zych, M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/ijacsa.2018.090354

Moody, D. (2022). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. https://doi.org/10.6028/nist.ir.8413-upd1

Mor, T., & Renner, R. (2014). Preface. *Natural Computing*, *13*(4), 447-452. https://doi.org/10.1007/s11047-014-9464-3

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-Quantum Lattice-Based Cryptography Implementations. *ACM Computing Surveys*, *51*(6), 1-41. https://doi.org/10.1145/3292548

Riel, H. (2022). *Quantum Computing Technology and Roadmap*. https://doi.org/10.1109/essderc55479.2022.9947181

Roman'kov, V., Ushakov, A., & Shpilrain, V. (2023). Algebraic and quantum attacks on two digital signature schemes. En *Journal of Mathematical Cryptology* (vol. 17). Walter de Gruyter GmbH. https://doi.org/10.1515/jmc-2022-0023

Sammons, A., & Putwain, D. (2018). *Psychology and Crime* (2.ª ed.). Routledge

Saarinen, M.-J. O. (2017). *HILA5: On Reliability, Reconciliation, and Error Correction for Ring-LWE Encryption*. Cryptology ePrint Archive, Paper 2017/424. https://eprint.iacr.org/2017/424

Schumacher, B. (1995). Quantum coding. *Physical Review A*, *51*(4), 2738-2747. https://doi.org/10.1103/physreva.51.2738

Schwabe, P., & Westerbaan, B. (2016). Solving Binary {MQ with Grover's Algorithm. In *Lecture Notes in Computer Science* (pp. 303-322). Springer Science+Business Media. https://doi.org/10.1007/978-3-319-49445-6_17

Seck, B., Cayrel, P., Diop, I., & Barbier, M. (2022). Cryptanalysis of a Code-Based Identification Scheme Presented in CANS 2018. En *Communications in computer and information science* (pp. 3-19). Springer Science+Business Media. https://doi.org/10.1007/978-3-031-23201-5_1

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5). https://doi.org/10.1137/S0097539795293172

Soni, L., Chandra, H., Gupta, D., & Keval, R. (2022). *Quantum-resistant public-key encryption and signature schemes with smaller key sizes*. Cluster Computing. https://doi.org/10.1007/s10586-022-03955-y

Ura, K., Imoto, T., Nikuni, T., Kawabata, S., & Matsuzaki, Y. (2023). Analysis of the shortest vector problems with quantum annealing to search the excited states. In *Japanese Journal of Applied Physics* (vol. 62). IOP Publishing. https://doi.org/10.35848/1347-4065/acba21

Vaishnavi, A., & Pillai, S. (2021). Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods. *Journal of Physics*, *1964*(4). https://doi.org/10.1088/1742-6596/1964/4/042002

Wang, Y., & Zhang, H. (2021). Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point. *Wuhan University Journal of Natural Sciences*, *26*(6), 489-494. https://doi.org/10.1051/wujns/2021266489

Xiao, K., Chen, X., Huang, J., Li, H., & Huang, Q. (2023). A lattice-based public key encryption scheme with delegated equality test. *Computer Standards & Interfaces*, *87*. https://doi.org/10.1016/j.csi.2023.103758

Xie, H., & Yang, L. (2019). Using Bernstein–Vazirani algorithm to attack block ciphers. *Designs, Codes and Cryptography*, *87*(5), 1161-1182. https://doi.org/10.1007/s10623-018-0510-5

Yang, N., Yang, S., Zhao, Y., Wu, W., & Wang, X. (2023). Inner product encryption from Middle-Product Learning With Errors. *Computer Standards & Interfaces*, *87*. https://doi.org/10.1016/j.csi.2023.103755

Yang, Y., Wang, Z., Ye, J., Fan, J., Chen, S., Li, H., Li, X., & Cao, Y. (2024). Chosen ciphertext correlation power analysis on Kyber. *Integration*, *91*, 10-22. https://doi.org/10.1016/j.vlsi.2023.02.012

Zeydan, E., Turk, Y., Aksoy, B., & Ozturk, S. B. (2022). Recent Advances in Post-Quantum Cryptography for Networks: A Survey. In *2022 Seventh International Conference On Mobile And Secure Services* (pp. 1-8). IEEE. https://doi.org/10.1109/mobisecserv50855.2022.9727214

Zhilong, J., Fu, Y., Cao, Z., Cheng, W., Zhao, Y., Dou, M., Duan, P., Kong, W., Cao, G., Li, H., & Guo, G. (2022). Superconducting and Silicon-Based Semiconductor Quantum Computers: A review. *IEEE Nanotechnology Magazine*, *16*(4), 10-19. https://doi.org/10.1109/mnano.2022.3175394