As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(02): 236-243, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0802038
Available online at: http://www.ijmtst.com/vol8issue02.html

Blockchain Cryptography Resistant to Quantum Computing Attacks

Sreelakshmi P.S[1] | Amrutha N[2]

[1]Department of Computer Science, St.Albert's College(Autonomous),Ernakulam, India.
[2]Assistant Professor, Department of Computer Science, St.Albert's College(Autonomous),Ernakulam, India.
*Corresponding Author Email Id: sreelakshmisunil2233@gmail.com

To Cite this Article
Sreelakshmi P.S and Amrutha N. Blockchain Cryptography Resistant to Quantum Computing Attacks. *International Journal for Modern Trends in Science and Technology* 2022, *8* pp. 236-243. https://doi.org/10.46501/IJMTST0802038

Article Info
Received: 18 January 2022; Accepted: 20 February 2022; Published: 25 February 2022.

ABSTRACT

A blockchain may be a revolutionary computational arrangement that permits an open, public, distributed ledger with a good range of uses. Any new cryptographic application, on the opposite hand, should take into consideration expected technical improvement during the lifetime of any possibly deployed systems, many of which can be in use for decades. Technological breakthroughs promise the creation of computers that process information according to quantum mechanics rather than traditional physics and probability laws. This indicates a significant gain in processing capability for specific problems, such as Grover's technique for function inversion and Shor's algorithm for factoring big numbers into prime factors. However, quantum computing's rapid advancement has in the not-too-distant future, assaults based on Grover's and Shor's algorithms will be possible. Such Both public-key cryptography and hash functions are threatened by algorithms, prompting blockchains to be redesigned. utilise cryptosystems that can withstand quantum attacks, resulting in post-quantum cryptography Cryptosystems that are quantum-proof, quantum-safe, or quantum-resistant. This article begins by reviewing the current state of the art in post-quantum cryptosystems and how they can be used to blockchains and distributed ledger technologies. Furthermore, the most relevant post-quantum blockchain systems, as well as their primary obstacles, are investigated.

KEYWORDS: Blockchain, DLT, quantum-safe, post-quantum, cryptosystems, cryptography, quantum computing.

1. INTRODUCTION

Blockchain may be a technology that was developed in conjunction with the cryptocurrency Bitcoin and is capable of delivering secure communications, data privacy, resilience, and transparency. A blockchain may be a distributed ledger supported a sequence of knowledge blocks linked by hashes that permits peers who don't necessarily trust one another to share information, thus solving the matter of double-spending. Users interact with the blockchain during a secure manner by using public-key/asymmetric cryptography, which is required for transaction authentication. Hash functions also are important during a blockchain since they permit for the generation of digital signatures and therefore the linking of blocks. the difficulty is that the expansion of quantum computers threatens both public-key cryptosystems and hash functions. Future quantum computing attacks could also be ready to recover secure transaction data quickly within the case of public-key cryptosystems. RSA (Rivest, Shamir, Adleman) [1], ECDSA (Elliptic Curve Digital Signature Algorithm) [2], [3], ECDH (Elliptic Curve Dife-Hellman) [4], or DSA (Digital

Signature Algorithm) [5], which may be broken polynomial time with Shor's algorithm [6] on a sufficiently powerful quantum computer.

Grover's method, which may greatly speed up function inversion, is that the main threat. this enables a signed data block to be updated by generating a modified pre-image from a specified hash (a hash collision). This nullifies the ledger entries' authenticity, compromising the blockchain as an entire . Grover's approach increases the speed of a hash by an element of the root of the amount of potential hashes, so a hash subjected to quantum assault is merely as secure together with half as many bits subjected to classical attack. Shor's algorithm, which applies to any component of blockchain that uses asymmetric key cryptography, is that the second threat. the foremost common issue is that the inability to interrupt RSA encryption. In contrast to the problem of factoring big numbers into prime factors, RSA relies on the convenience of multiplying prime numbers. Shor's method accelerates this process by orders of magnitude, thereby cracking the RSA encryption. Other asymmetric key cryptosystems can enjoy variants of Shor's algorithm.

2.LITERATURE REVIEW

According to norah kappert[7], quantum computers are not yet advanced enough to render the blockchain insecure, Authorities have been working on possible countermeasures since they first realised the harm they pose.As a result, numerous interiguing solutionsnhave already been presented,despite the fact that quantum computing is still in its infancy.Short-term countermeasures such as post-quantum cryptography and other concepts to make the blockchain more resistant to quantum computers are among these possibilities.

Current technologies can be used to implement such safeguards,but they do not provide perfect security or long term countermeasures like quantum cryptography and quantum blockchains.Because present quantum computers are incapable of running Grover's shor's algorihms.it is difficult to predict how long it will take or whether we will ever have quantum computersmcapable of breaking the blockchain.Classical hardware may be far faster by then,and quantum technology may have spread so widely that no one with a quantum computer can manage the network.

3. BLOCKCHAIN BASICS AND SECURITY PRIMITIVES

A blockchain may be a decentralized ledger that records all peer-to-peer transactions. Blockchain, in layman's or commercial terms, may be a platform that permits users to conduct transactions of any kind without the necessity for a central or trusted arbitrator. The constructed database is transparently shared among network participants, allowing anyone to access its contents. Peer-to-peer networks and a time stamping server are wont to manage the database autonomously. Each block during a blockchain is organised in such how that it refers to the previous block's content. the bulk of individuals mistakenly believe that Bitcoin and Blockchain are an equivalent thing. that's not the case, together of the core technologies that powers most applications, including cryptocurrency. Since the introduction of Bitcoin, a blockchain-based application, a slew of other ones have emerged, all attempting to capitalise on the concepts and capabilities of the digital ledger technology. As a result, blockchain history encompasses an extended list of applications that have emerged because the technology has progressed. Concerned about Bitcoin's limits, Buterin began developing a "moldable" blockchain which will fulfil a spread of roles additionally to being a peer-to-peer network. In 2013, Ethereum was launched as a replacement public blockchain. Ethereum and Bitcoin are just the start of the blockchain's history and evolution. A slew of latest ventures have emerged in recent years, many of which make use of blockchain technology. New projects have attempted to remedy a number of Bitcoin and Ethereum's flaws while also developing newfunctionality supported blockchain technology.

A blockchain miner may be a third sort of node that's found in many blockchains and whose contribution is critical during blockchain transaction validations: to execute the validation, they follow a consensus protocol and do particular tasks.

There are numerous consensus protocols [8], including a number of the foremost popular Proof-of-Work (PoW) (used by Bitcoin), Byzantine Fault

Tolerance (BFT) methods [8], and Proof-of-Stake methods (PoS). the thought of a sensible contract is equally important. a sensible contract may be a collection of rules that's kept on the blockchain and performed automatically to hurry up transactions. a sensible contract can specify requirements for bond transfers, also as payment terms for trip insurance.

4. SECURITY PRIMITIVES IN BLOCKCHAIN

Blockchain's security characteristics are primarily supported by public-key/asymmetric cryptography and hash algorithms.

A. Public-key Cryptography

The blockchain protocol is built on public-key cryptography as one of its building pieces. Cryptographic algorithms provide assurances that allow a distributed, decentralised, and secure digital ledger to be implemented. As a result, the blockchain's security and secure usage of public key cryptography are critical. If private keys aren't securely protected, or a widely used algorithm is revealed to be insecure, the blockchain's security is jeopardised as well. To complete diverse tasks, public key cryptography employs a pair of public and private keys. Private keys are kept hidden, while public keys are widely distributed. It is possible to encrypt a message using a person's public key such that only the person with the private key can decrypt and read it. A digital signature can be established with a private key so that anyone having the associated public key can verify that the message was created by the private key owner and has not been modified since.

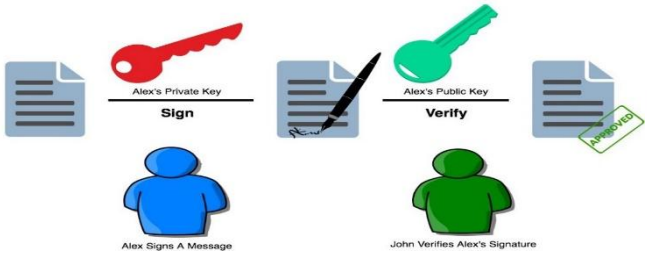

FIG 1: SIGNATURE PROCESS USING PUBLIC KEY CRYPTOGRAPHY

B. Hash Function

The process of having an input item of any length mirror an output item of a defined length is referred to as hashing in blockchain. Take, for example, the use of blockchain in cryptocurrencies, where transactions of variable lengths are passed through a certain hashing algorithm and all produce a fixed-length output. This is true regardless of the input transaction's length.

The result is referred to as a hash. Bitcoin's Secure Hashing Algorithm 256 is a nice example (commonly shortened to SHA-256). When employing SHA-256, the output result is always of a fixed length, which is 256 bits (the output is 32 bytes). This is true whether the transaction is a simple one-word transaction or a sophisticated one including a large quantity of data. The hash size will be determined by the hash function used, but the output from a certain hashing technique will be of a specific size. Blockchains use hash functions to connect their blocks.

5. BLOCKCHAIN FROM PRE-QUANTUM TO POST-QUANTUM

It should be mentioned that the robustness of public-key cryptosystems against classical computer attacks has typically been measured using the so-called bits-of-security level. The work required by a traditional computer to undertake a brute-force assault falls into this category. When the effort necessary to attack an asymmetric cryptosystem with a classical computer is comparable to the work required to carry out a brute-force assault on a 1024-bit cryptographic key, the system is said to have a 1024-bit security. Table 1 shows the security level of some of the most popular symmetric and asymmetric cryptosystems as a guide.

Table1: Reference security levels for popular symmetric and asymmetric cryptosystems.

Security Level	Symmetric Cryptosystem Key Size	RSA Key Size	ECDSA Curve Key Size
80	2TDEA (112 bits)	1024 bits	prime192v1 (192 bits)
112	3TDEA (168 bits)	2048 bits	secp224r1 (224 bits)
128	AES-128 (128 bits)	3072 bits	secp256r1 (256 bits)
192	AES-192 (192 bits)	7680 bits	secp384r1 (384 bits)

Current 80-bit security cryptosystems are expected to cost between tens of thousands and hundreds of millions of dollars to break with traditional computers.

For the next 30 to 40 years, 112-bit cryptosystems are expected to be secure against classical computing assaults [10]. Researchers have shown that a 1000-qubit quantum computer can break 160-bit elliptic curves, whereas a 1024-bit RSA would require around 2,000 qubits [11].

Traditional hash functions, unlike public-key cryptosystems, are thought to be resistant to quantum assaults since the development of quantum algorithms for NP-hard problems appears unlikely [12]. Although novel hash algorithms to resist quantum assaults have recently been developed by academics [13], it is usually recommended to enhance the output size of standard hash functions. To begin, look for hash collisions before replacing entire blockchain blocks. For example, in the work detailed in [14], Grover's approach is presented to find collisions in hash functions, resulting in the conclusion that a hash function must output 3*n bits to guarantee an n-bit security level. As a result of this conclusion, many present hash functions will no longer be valid in the post-quantum period, while others, such as SHA-2 and SHA-3, will need to expand their output size.

Second, Grover's technique can be used to speed up mining in blockchains like Bitcoin (i.e., it can speed up the production of nonces), allowing for the rapid remaking of complete blockchains, so jeopardising their integrity. Furthermore, quantum attacks using Shor's algorithm have an influence on hash functions: if a blockchain hash function is compromised, someone with a powerful enough quantum computer can forge digital signatures, impersonate blockchain users, and steal their digital assets using Shor's algorithm.

6. CLASSICAL AND QUANTUM COMPUTATION

Information processing and administration have been transformed by computing. Information could be processed with physical systems as early as Charles Babbage, and more recently (e.g., Rolf Landauer's work) that information must be represented in physical form and thus be subject to physical rules. Understanding the constraints of computation requires knowledge of the physical principles that apply to the information processing system. Traditional computing equipment are referred to as "classical computers" because they follow the laws of classical mechanics. The proposed "quantum computers" are regulated by quantum physics, which results in a significant change in computational capacity.

Quantum mechanics adds aspects to classical mechanics that aren't present in classical mechanics. To begin with, physical quantities are "quantized," which means they can't be split. Light, for example, is quantized: the photon is the fundamental quantum of light, and it cannot be divided into two photons. Physical states must also evolve in such a way that cloning an arbitrary, unknown state into an independent duplicate is impossible, according to quantum physics. To avoid information copying, this is utilised in quantum cryptography. Furthermore, quantum physics characterises systems in terms of superpositions, which allow many discernible inputs to be processed at the same time, yet only one can be seen at the conclusion of the process, and the outcome is generally probabilistic. Finally, correlations are possible in quantum mechanics that are not possible in conventional physics. Entanglement is a term used to describe such relationships.

The promise of quantum computation is that it will make such speedups for specific tough problems more widely available. Clearly, this has ramifications in many fields of information science and computation, where a system's functionality is dependent on the difficulty of a calculation. A large speedup in such instances can cause a system to fail. This is particularly true for cryptographic systems that rely on asymmetry in processing effort when evaluating a function and its inverse. Multiplication of large primes is straightforward and so fast in RSA encryption, while factoring huge composite numbers into two prime factors is exceedingly complex and thus sluggish. The important aspect of hash functions is that they are simple to calculate but complex to invert. Because it's difficult to take a particular hash value and discover a pre-image that gives that hash, they provide a quasi-unique fingerprint.

7. POST-QUANTUM CRYPTOSYSTEMS

Algorithms used in national security systems, according to the NSA's Information Assurance Directorate (IAD) [15], take twenty years to fully deploy and should be designed to secure information for at least thirty years. We can't say when or if a large-scale quantum computer will be built, but many experts

believe it will happen within these timeframes. As a result, the development of "quantum resistant" encryption algorithms has been designated as a national priority.

Quantum resistant cryptography, sometimes known as post-quantum cryptography, is a branch of cryptography that investigates the use of a quantum computer to attack (classical) cryptographic systems [16][17]. Although there are some insights in this field, it is still a fairly new topic with a lot of uncertainty and no agreed standards, as described above. To address this issue, Congress passed the "American Innovation and Competitiveness Act" in 2017, mandating that the National Institute of Standards and Technology (NIST) "research and identify, or if necessary, develop cryptography standards and guidelines for future cybersecurity needs, including quantum-resistant cryptography standards." This procedure has already begun, and public updates are available on the NIST website <http://www.nist.gov/pqcrypto>. The "NSA expects that the external cryptography community can create quantum resistant algorithms and obtain broad consensus for standardisation within a few years," according to the IAD.

A. Code-Based Cryptosystems

They are based on the principle that underpins error-correction codes. For example, McEliece's cryptosystem [18], which dates from the 1970s and is based on the syndrome decoding issue [19], is an example of a code-based cryptosystem. McEliece's technique has a fast encryption and decryption time, which is beneficial for executing quick blockchain transactions. McEliece's cryptosystem, on the other hand, necessitates the storage and execution of enormous matrices that serve as public and private keys.

When using resource-constrained devices, such matrices typically take up between 100 kilobytes and several megabytes, which can be a limitation. Future researchers will need to look at matrix compression techniques, as well as the usage of various codes (e.g., Low-Density Parity-Check (LDPC) codes, Quasi-Cyclic Low-Rank Parity-Check (QC-LRPC) codes) and specific coding approaches to address this issue [20].

B. Multivariate-Based Cryptosystems

Multivariate-based techniques rely on the difficulty of solving multivariate equation systems, which have been shown to be NP-hard or NP-complete [85]. Regardless of their differences, Due to the included "guess work," further research is needed to improve their decryption performance (due to the associated "guess work," and to lower their huge key size and ciphertext overhead [21].

The usage of square matrices with random quadratic polynomials, cryptosystems developed from Matsumoto-algorithm, Imai's and schemes based on Hidden Field Equations (HFE) are now some of the most promising multivariate-based methods [22][23].

C. Lattice-Based Cryptosystems

This type of cryptographic technique is based on lattices, which are periodic sets of points in n-dimensional spaces. The Shortest Vector Task (SVP) is an NP-hard problem whose goal is to find the shortest non-zero vector within a lattice. Lattice-based security schemes rely on the assumed hardness of lattice problems like the Shortest Vector Problem (SVP).

Other analogous lattice-related issues, such as the Closest Vector Problem (CVP) or the Shortest Independent Vectors Problem (SIVP) [24], are now unsolvable with quantum computers. Because lattice-based techniques are frequently computationally simple, they may be implemented quickly, they are useful for speeding up blockchain user transactions. and in a cost-effective manner However, lattice-based implementations, like other post-quantum methods, require huge keys to store and utilise, as well as substantial ciphertext overheads. For example, lattice-based methods like NTRU [25] or NewHope [26] frequently necessitate the management of keys in the thousands of bits.

D. Super-Singular Elliptic Curve Isogeny Cryptosystem

These techniques are based on the isogeny protocol for ordinary elliptic curves described in [27], but they've been improved to withstand the quantum attack described in [28]. There are a number of intriguing post-quantum cryptosystems of this type [29], [30], with key sizes ranging from a few thousand bits to a few million bits [31].

SIKE [32], [33] is the only isogeny-based public-key encryption technique that made it to the second round of the NIST request. SIKE is based on super singular isogeny graphs and pseudo-random walks. SIKEp434, which uses a 2640-bit public key and a 2992-bit private key for a 128-bit level of classical security, is a good example of SIKE key sizes.

E.Hybrid Cryptosystems

Hybrid schemes appear to be the next step toward post-quantum security, as they combine pre-quantum and post-quantum cryptosystems with the goal of protecting exchanged data from quantum attacks as well as attacks against the used post-quantum schemes, the security of which is currently being evaluated by industry and academia.

A 2640-bit public key and a 2992-bit private key are used for security. Google put these cryptosystems to the test by combining New Hope with X25519, an ECC-based Dife-Hellman key agreement technique. Currently, a second version of the hybrid scheme (CECPQ2) is being tested, which combines X25519 with NTRU instantiations (HRSS (Hülsing, Rijneveld, Schanck, Schwabe) and SXY (Saito, Xagawa, Yamakawa).

8. QUANTUM COMPUTING ALGORITHMS

We need to comprehend Grover's Algorithm and Shor's Algorithm to understand blockchain in the context of quantum computing and quantum enhanced assaults. The former is an input search strategy for finding a unique input to a black box function that is substantially faster than brute force search, putting hash functions of insufficient length in jeopardy. When compared to the general number field sieve (the most well-known factoring procedure), the latter gives an exponential speed gain in factoring integers and can also be used to solve hidden subgroup and discrete logarithm problems. These issues are at the heart of decrypting many known asymmetric cyphers, and are thus relevant to decrypting public key cryptography and digital signatures. Together, the two quantum algorithms pose a substantial threat to blockchain-based systems.

A. Grover's Algorithm

To protect against the change of previous blocks, blockchain relies on hash computation. Because of its distributed nature and the computing cost necessary to re-compute a chain of blocks, the chain is secure against extended revision. The difficulty of establishing a hash collision with the present hash, which equates to the challenge of reversing the hash function, ensures that a single block can be modified.

Grover's algorithm is a solution to the problem of locating a pre-image of a difficult-to-invert value of a function. If we have a signature that is the hash value of some data s=H(d) and the function H(d) can be implemented on a quantum computer, Grover's approach can determine d for a given s in order O(n), where n is the size of the set of valid hashes. To put it another way, it allows us to generate hash collisions faster than brute force search, which is O(n).
This indicates that for a hash length of k bits, we have a considerable speedup of 2k/2. Even for small values of k, this can be rather significant.

B. Shor's Algorithm

Shor's Algorithm improves the efficiency of factoring huge numbers dramatically. As a result, Shor's technique can be used to RSA encryption and associated issues. The general number field sieve (the most efficient known algorithm for factoring numbers) has a super-polynomial complexity (run time longer than any polynomial in the input length) but a sub-exponential complexity (run time shorter than exponential in the input length), whereas Shor's algorithm has a polynomial complexity in the input length, making the speed gain roughly exponential. In reality, this means that 4096-bit RSA keys are unbreakable with conventional computation but can be broken using quantum computation. As a result, any part of a blockchain implementation that uses RSA or comparable techniques is vulnerable to a quantum computing attack.

The factoring of huge composite integers consisting of a product of two large primes was Shor's first goal. Factoring, on the other hand, is a subset of the more general hidden subgroup problem, and Shor's approach can be modified to solve any of these issues. This enables for the solution of difficulties such as the

discrete logarithm problem, rendering ElGamal encryption, Diffie-Helman key exchange, the Digital Signature Algorithm, and elliptic curve cryptography insecure. The existence of Shor's algorithm illustrates that a quantum computer exposes vulnerabilities beyond hash collision creation and Grover's method function inversion, a computational assault.

9. FUTURE SCOPE AND CONCLUSION

Quantum computing is a trendy topic that has piqued the interest of both academics and industry. As a result, it's feasible that new attacks against post-quantum cryptosystems will emerge. The move from pre-quantum to post-quantum blockchains necessitates thorough consideration of the phases involved. Various researchers have created approaches for this aim. For example, when the security of a hash function or digital signatures is compromised, the authors offer a technique to extend the validity of previous blockchain blocks.

However, the transition technique may result in a hard fork of the blockchain, which might be avoided by implementing a soft-fork mechanism. Another technique is that, where a simple commit-delay-reveal protocol is presented that allows blockchain users to migrate funds from pre-quantum Bitcoin to a version that implements a post-quantum digital signature scheme in a secure manner.

Several academics proposed quantum-computing-based blockchains in addition to using cryptosystems to migrate from pre-quantum to post-quantum blockchains. For example, the authors propose that Bitcoin be moved to quantum computers, while others outlined how to speed up mining by changing Grover's method. Furthermore, some authors have suggested that smart contracts be implemented utilising quantum cryptography. Furthermore, more research into key setup physics-based approaches called as Quantum-Key Distribution (QKD) is required.

The recent breakthrough in quantum computing has piqued the curiosity of researchers and developers that work with distributed ledger technologies (DLTs) like blockchain, which rely heavily on public-key cryptography and hash functions. The impact of quantum-computing assaults (based on Grover's and Shor's algorithms) on blockchain was examined in this article, as well as how postquantum cryptosystems might be used to counter such attacks. The most relevant post-quantum methods were studied and their application to blockchain, as well as their primary obstacles, were analysed for this purpose.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, ``A method for obtaining digital signatures and public-key cryptosystems,".

[2] "Elliptic curve cryptosystems," Mathematics Comput. N. Koblitz, "Elliptic curve cryptosystems," Mathematics Comput.

[3] "Use of elliptic curves in cryptography," V. S. Miller.

[4] "New directions in cryptography," by W. Dif e and M. Hellman.

[5] FIPS Standard FIPS Digital Signature Standard (DSS).

[6] P. W. Shor, "Polynomial-time methods for prime factorization and their applications on a quantum computer, discrete logarithms,"

[7] Norah Kappert,quantum computing:An impending end to blockchain?

[8] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P.Wang, Y.Wen, and W. Wang "A survey on consensus methods and mining strategy management in blockchain networks," according to D. I. Kim.

[9] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive maintenance Recovery."

[10] National Institute of Standards and Technology (NIST), Report on Post-Quantum Cryptography, document NISTIR- 8105 (draught).

[11] "Shor's discrete logarithm quantum algorithm for elliptic curves," by J. Proos and C. Zalka, Quantum Inf. Comput.

[12] "Strengths and limitations of quantum computing," by C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani.

[13] "Parametric hash function resistant to attack by quantum computer," S. Krendelev and P. Sazonova, "Parametric hash function resistant to assault by quantum computer."

[14] "Quantum cryptanalysis of hash and claw-free functions," by G. Brassard, P. Hyer, and A. Tapp.

[15] "CNSA Suite and Quantum Computing FAQ," National Security Agency's Information Assurance Directorate

[16] National Institute of Standards and Technology, "Report on Post-Quantum Cryptography."

[17] Cryptography in the Post-Quantum Era, E Dahmen, J Buchmann, and DJ Bernstein

[18] R. J. McEliece, ``A public-key cryptosystem based on algebraic coding Theory.''

[19] "On the inherent intractability of certain coding issues," E. Berlekamp, R. Mceliece, and H. Van Tilborg.

[20] "Punctured Reed Muller code-based McEliece cryptosystems," by W. Lee, J.-S. No, and Y.-S. Kim.

[21] "Selecting parameters for the rainbow signature scheme," by A. Petzoldt, S. Bulygin, and J. Buchmann.

[22] "The cubic simple matrix encryption Scheme," by J. Ding, A. Petzoldt, and L.-C. Wang.
[23] "Cryptanalysis of HFEv and internal perturbation of HFE," by J. Ding and D. Schmidt.
[24] "NTRU: A ring-based public key cryptosystem," by J. Hoffstein, J. Pipher, and J. H. Silverman.
[25] "Post-quantum key exchange A new hope," E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe,"
[26] "Better key sizes (and attacks) for LWE-based encryption," R. Lindner and C. Peikert,"
[27] A. Rostovtsev and A. Stolbunov, "Isogeny-based public-key cryptosystem,"
[28] "Constructing elliptic curve isogenies in quantum subexponential time," A. Childs, D. Jao, and V. Soukharev,"
[29] J.-F. Biasse, D. Jao, and A. Sankar, A Quantum Algorithm for Communication.
[30] putting Isogenies in the Middle Elliptic Curves with Supersingular Elliptic Curves (Lecture Notes) in the field of computing.
[31] "Towards quantum-resistant cryptosystems," L. De Feo, D. Jao, and J. Plût, from isogenies of super singular elliptic curves."
[32] "Efficient algorithms for Super singular isogeny Diffie Hellman," by C. Costello, P. Longa, and M. Naehrig.
[33] SIKE (n.d.) (n.d.) (n.d. On the 2nd of November, 2019, I was able to get a hold of some information. [Online]. https://sike.org is a website where you may learn more about it.