Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Post-Quantum Cryptography Challenges

Jose Pinto*

ISLA – Polytechnic Institute of Management and Technology, Vila Nova de Gaia, Portugal
Email: spintoj@gmail.com

Abstract

Cryptography is used broadly in the digital age, making our communications secure, ensuring our data is safe, and enabling secure transactions on which we rely daily. Our reality is connected, we send an email without thinking about all the underlying protocols, we buy online, and we check the weather on our fridge. Utilizations are countless and so is our exposure. Cryptographic systems keep us safe, a shield for our privacy and our fundamental rights. However, we have arrived at the dawn of a new age, the quantum computing era. Seen for a long as a theoretical emanation of quantum mechanics it gives the first baby steps in the real world, making the world as we know it less safe and more dangerous. Post-quantum cryptography is the paladin that is coming to the rescue, but will it be up to the challenge of keeping our world safe.

Keywords: Cybersecurity; Cryptography; post quantum, PQC; quantum computing

* Corresponding author. Email address: spintoj@gmail.com

1. Introduction

(Cryptography is a technic used to make data secure, it doesn't intend to hide the fact that communication between parties exists, but it assures that data is unreadable to any unauthorized entity that tries to access it. Cryptographic primitives like symmetric encryption, public key algorithms, and hash functions among others are the building blocks to provide, through several combinations, cybersecurity services. Since more advanced cryptographic technics exist to deal with privacy challenges one can say that privacy goes beyond encryption [1], [2].

That's why when thinking about cryptography we must consider the following:

- The implementation of cryptographic algorithms
- The management of cryptographic keys
- How will it be applied, to what, and by whom.

The advent of new technologies can make more vulnerable technics that were considered secure so far. In 1982 Feynman introduced the concept of quantum computing. The difference from classical computing is that instead of data being represented in a bit (0 and 1) it's now represented in quantum bits or qubits (particles that can exist not only as 0 or 1 state but in both at the same time), thanks to this quantum computers can perform certain operations, like factorizing large numbers, much faster than classical computers. Quantum computers pose a threat to current cryptographic technics because they can break the keys rapidly either by calculating or exhaustively searching the possible secret keys [3].

Although a quantum computer is not one that we can have sitting on the desk there it won't be long until some company's offers could start to make available this kind of technology, which means that now is already too late to start working on mechanisms that allow everyone to protect everyone more efficiently from this threat.

However, it is still uncertain how far the advantages of quantum computing can be pushed or the actual gap between classical and quantum models. There isn't a predicted date for the start of a quantum era, and its effects or dangers are not completely clear work must be done to prepare the information systems and ensure a smooth transition from the currently used cryptographic systems to their quantum counterparts [4].

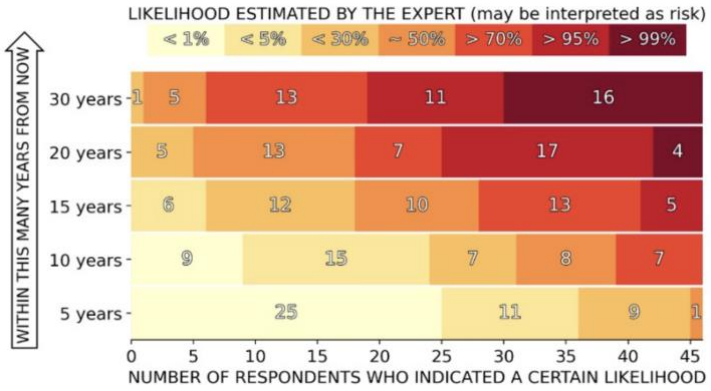

Figure. 1 Experts were asked to indicate their estimate of the likelihood of a quantum computer being able to break the RSA-2048 quickly.[5]

There are already official institutions doing efforts to identify the impact of quantum computing in common cryptographic algorithms [4].

Looking at this impact table and that together with the advent of IoT, in which everything is connected, our cars, our fridges, and the blinds of our households. it's easy to understand that systems like the ones below will be compromised if nothing is done

- Financial systems.
- Military and government systems.
- Medical records.
- e-Commerce.
- E-mail and messaging.
- Personal and public transport

Looking at the examples above it's easy to understand how cryptography touches different dimensions of modern societies, by ensuring the safety of data, either on transport or at rest, the privacy of individuals and institutions, and by protecting the financial assets of this digital age.

2. Research Methodology

This review was conducted according to the PRISMA Model.

Research Question

This systematic review aims to answer the following research question: *Is cryptography ready for post-quantum computers?*

The following references and research content were obtained from Google Scholar, and Research Gate, and include the following information:

Keyword	Operator
Cryptography	AND
Post-Quantum	AND
Cybersecurity	AND

On figure 2 is possible to see the PRISMA flow to select the records.

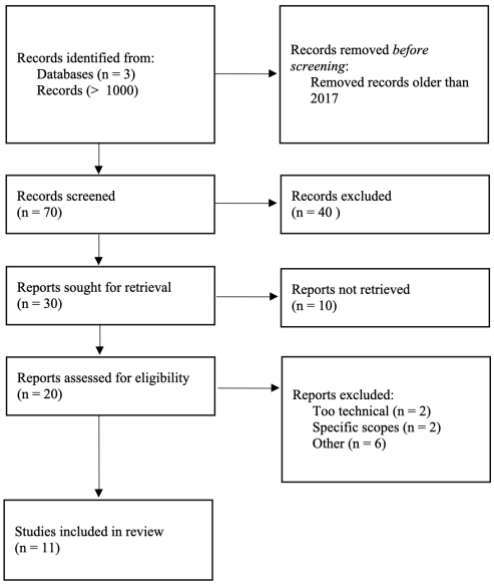

Figure 2. PRISMA flowchart

Only records from 2019 onwards were considered. Due to the large number of entries returned a few were selected based on the title matching the purpose of the study. Following records were excluded after reading the abstracts and the conclusions. From the records selected some were not available for retrieval. Some additional studies were included to complement the information of the selected records. No automated procedures were used for the selection.

3. Results

The selected articles allow to make a state of the art of the current options to quantum resistant cryptography. These algorithms and approaches of implementation consider not only the applicability in a quantum world but still valid for classic computers.

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Figure 3. Predicted impact of quantum computers on common algorithms by NIST [4]

3.1. Overview of quantum-resistant algorithms

As shown in Figure 3, the impact of quantum computing on the security of symmetric keys and hash functions is less relevant, so the greatest focus of research is to find public key algorithms that are resistant to attacks both from classical and quantum computers. The most notable approaches for quantum age cryptography are the following:

- **Lattice-based cryptography:** This approach is based on the difficulty of solving certain mathematical problems over very high-dimensional lattices. In Lattice-based encryption multiplication of primes is substituted by multiplication of matrices [3]. New applications like fully homomorphic encryption, code obfuscation, and attribute-based encryptions were made possible, with the advantage these algorithms are simple, efficient, and highly parallelizable [4].
- **Code-based cryptography:** This approach is based on the difficulty of decoding error-correcting codes, which are used in many communication systems. Although fast it needs very large key sizes, to address that some new variants are making attempts to reduce the key size [4].
- **Multivariate cryptography:** This approach relies on the difficulty of solving multivariate equations systems, which are used to encrypt and decrypt messages. Historically this approach has been seen as more successful in signatures [4].
- **Hash-based cryptography:** This approach is based on the use of cryptographic hash functions, it's a well-understood approach, even against quantum attacks, which are used to create a fixed-length "fingerprint" of a message. The main drawbacks are that the signer must keep a record of the exact number of previously signed messages and that it can produce only a limited number of signatures [4].

  Based on these approaches several algorithms have been proposed to address post-quantum cryptography.

Approach	Advantages	Disadvantages
Code-based encryption (using Goppa codes)	High confidence in security; very fast encryption; short ciphertexts	Large public keys
Lattice-based encryption (using NTRU or related)	Short ciphertexts and keys; very fast encryption	Require more security analysis
Lattice-based signatures	Short keys and signatures; fast	Require more security analysis; side-channel attacks on discrete Gaussians
Multivariate-quadratic-equation signatures	Very short signatures	Require more security analysis
Hash-based signatures (stateful version)	High confidence; simple description	Management of state
Hash-based signatures (stateless version)	High confidence; simple description	Large signatures

Figure 4. Qualitative overview of post-quantum systems

3.1.1. The Learning with Errors (LWE) algorithm

This algorithm is based on the hardness of solving the Learning with Errors problem, which is a mathematical problem that is believed to be difficult to solve with a quantum computer. It involves the difficulty of finding which values that solve [6]:

$$B = A.s+e \qquad (1)$$

Matrixes A and B are known values (and thus public keys), while s is the secret key, while e is a small list of random numbers (random errors). It starts by defining the secret value (s), our private key. Afterward, generate a list of random numbers for our public key (A). With *A*, *s*, and random errors *e* (a small list of random numbers) it's possible to calculate the value of the other public key (B). A and B can be distributed to anyone who wants to encrypt a message, but s must remain secret.

To encrypt a message, it's done using samples of A and B and a message bit (M). So, each 0 and 1 are encrypted. The decryption process reverses the operation to identify if the original message was either 0 or 1 [6].

*3.1.2. **The McEliece cryptosystem***

This algorithm is based on the difficulty of decoding a special type of error-correcting code known as a Goppa code, which is linear code with a fast-decoding algorithm. Although considered secure it presents some drawbacks, listed below [7]:

- A very large size public key. With the parameters suggested by McEliece, the public key would consist of 2^{19} bits, which would bring implementation problems.

- The size of the encrypted message is larger than the original, increasing the bandwidth and making the system more prone to transmission errors.

- It's not used for authentication or signature schemes, since the encryption algorithm is not one-to-one, and encryption and decryption do not commute.

3.1.3. ***The NTRU crypto system***

The NTRU crypto system is a type of post-quantum cryptographic algorithm. It is based on the difficulty of solving systems of quadratic equations, which are used to encrypt and decrypt messages. NTRU fits into the general framework of a probabilistic crypto system, which means encryption includes a random element, so each message has many possible encryptions. With this system encryption and decryption is extremely fast and key creation is easy. Studies show that compared with this system the "soon-to-be-obsolete" pre-quantum RSA underperform in parameters such as speed, reliability, and performance.[8][9]

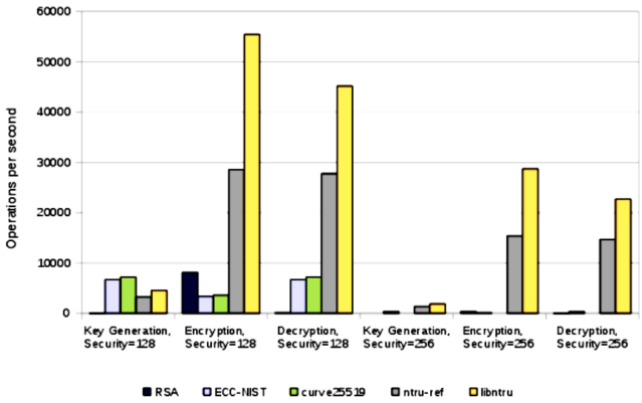

Figure 5. Comparison of NTRU performance with other algorithms [9]

3.1.4. ***The Merkle-Damgård hash construction***

The Merkle-Damgård hash construction is a type of cryptographic algorithm that is used to create a fixed-length "fingerprint" of a message. It is based on the use of cryptographic hash functions, which are mathematical functions that take an input of any size and produce an output of a fixed size. Famous hash functions like MD4, MD5, and SHA-1 follow the abbreviated Merkle-Damgård (MD) method. Being very well-known and very flexible makes it suitable to create a wide range of hash functions with different properties, which allows the designers of cryptographic systems to adapt the method to the specific needs of their applications.[10]

3.1.5. ***Quantum key Distribution***

One of the challenges of implementing schemes that involve the exchange of cryptographic keys is how two parties can do it through an insecure channel. Quantum key distribution (QKD) relies on the fundamentals of quantum mechanics. Two main approaches are being used [3]:

- Prepare-and-measure (P&M) – uses the Heisenberg uncertainty principle, which makes it hard for someone to eavesdrop on a key exchange without leaving a trace, allowing the parties to discard a compromised key.

- Entanglement-based (EB) – entanglement is a quantum physical phenomenon that links two or more objects, that after entanglement are considered as one. This means that one that intercepted a legitimate exchange would alter the entire system and reveal the presence of an attacker

These two approaches are then divided into three families [3]:

- Discrete variable coding protocols

- Gaussian protocols

- Distributed phase reference coding protocols

The first protocol that is still in use is BB84 (belongs to the discrete variable coding family) which uses four non-orthogonal polarized single photon states or low-intensity light pulses. Although considered provable secure it was broken already, due to its hardware implementation. Improvements have been proposed although not yet considered secure.[3] However this approach is dependent of the creation of quantum enable networks, which could be dimmed as impossible to foresee that all devices (including IoT) would be quantum enabled [13].

3.2. Path towards standardization

As was mentioned above the research to find public-key crypto-systems that are prepared to be secure against not only classical computers but also quantum computers have intensified. The National Institute of Standards and Technology (NIST) together with other international institutions is setting a path toward standardization. To address that NIST made a public competition to select quantum-resistant public-key cryptographic algorithms. After the 3rd round of evaluation, the public-key encapsulation mechanism (KEM) that will be proposed to standardize is CRYSTALS–KYBER. Regarding he digital signatures that will be proposed are CRYSTALS–Dilithium, FALCON, and SPHINCS+ [11].

3.2.1. CRYSTALS-Kyber

KYBER is a module learning with errors (MLWE)-based key encapsulation mechanism. Regarding security, although, many of the results remain speculative but are in line with the lattice cryptanalysis state of the art. Additionally KYBER's public key and cipher-text sizes are on the order of a thousand bytes, which should be acceptable for most applications [11].

Candidate	Claimed Security	Public key	Private key	Ciphertext
KYBER512	Level 1	800	1 632	768
KYBER768	Level 3	1 184	2 400	1 088
KYBER1024	Level 5	1 568	3 168	1 568

Figure 6. Key and cipher-text sizes (in bytes) for Kyber, adapted from [11]

Compared with other KEM candidates Kyber has excellent performance both on software and hardware backed by the evidence so far supporting MLWE [11].

3.2.2. CRYSTALS–Dilithium

Dilithium is a lattice-based digital signature algorithm based on the Fiat-Shamir paradigm (built on top of MLWE). The establishment of Dilithium security is based on the decisional Module-LWE assumption, which is enough to demonstrate that the public key does not leak any information about the secret key. Additionally, the strong binding property may be useful for non-repudiation, since a unique public key and message identify a given Dilithium signature. Overall, it was considered efficient and easy to implement with a strong theoretical basis [11].

3.2.3. FALCON

FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU) is a lattice-based signature scheme utilizing the "hash-and-sign" paradigm.

It should be noted that FALCON does not offer certain desirable beyond unforgeable security properties, although they may be attained through modifications with small performance costs.

It has two big advantages, the smallest bandwidth (amongst the NIST candidates) and fast signature verification. Both these characteristics might make this candidate a good fit for some applications [11].

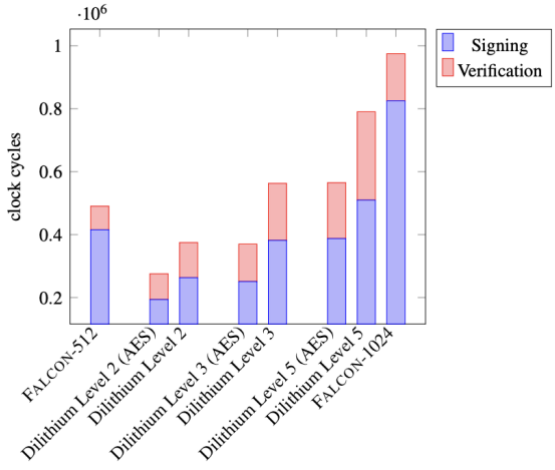

Figure 7. Signature Benchmarks on x86-64 processor with AVX2 extensions [11]

*3.2.4. **SPHINCS+***

SPHINCS+ is a stateless hash-based signature scheme, which combines the use of one-time signatures, few-times signatures, Merkle trees, and hyper-trees to construct a digital signature scheme that is suitable for general use. Since it's stateless the user does not need to keep the state across signatures which can lead to disastrous consequences if the state is mismanaged. However, the complexity of this signature makes it challenging to implement and evaluate security. On the other hand, since it relies on the underlying hash functions it gives a fallback to cryptanalytical attacks.[11]

Candidate	Claimed Security	Public key	Private key	Signature
Dilithium	Level 2	1 312	2 528	2 420
	Level 3	1 952	4 000	3 293
	Level 5	2 592	4 864	4 595
FALCON-512	Level 1	897	7 553	666
FALCON-1024	Level 5	1 793	13 953	1 280
SPHINCS$^+$-128s	Level 1	32	64	7856
SPHINCS$^+$-128f	Level 1	32	64	17 088
SPHINCS$^+$-192s	Level 3	48	96	16 224
SPHINCS$^+$-192f	Level 3	48	96	35 664
SPHINCS$^+$-256s	Level 5	64	128	29 792
SPHINCS$^+$-256f	Level 5	64	128	49 856

Figure 8. Key and signature sizes (in bytes) for the signature finalists, adapted from [11]

For this signature scheme, both key generation and verification are much faster than the signing itself, with very short public keys contrasting with quite long signatures. Since it's based on a different mathematical foundation from Dilithium and FALCON it was considered a good candidate for the sake of diversity [11].

3.3. Security Analysis

From time-to-time developments in new technologies may lead to exposing weaknesses in established cryptographic methods. Post-quantum cryptography is not invulnerable to all attacks. Some of the potential vulnerabilities of post-quantum cryptographic systems include:

- Side-channel attacks: attacks that exploit information that is leaked by the physical implementation of a cryptographic system, memory usages, CPU cycles or even the power consumption of a device (FALCON is an example of a scheme that has this vulnerability since it is more resource hungry) [11].

- Mathematical attacks: attacks that exploit mathematical weaknesses in the underlying cryptographic algorithms used by a system (one of the candidates for NIST standardization, Rainbow, didn’t pass the 3rd round due to this vulnerability) [11].

- Quantum attacks: These are attacks that are specifically designed to exploit the unique properties of quantum computers, like the photon number splitting attack, in which a photon is deterministically split by an attacker and stored in quantum memory to later measure the captured photons and obtain information about the key [3].

- Hardware attacks: These are attacks that involve physically tampering with a cryptographic device to extract sensitive information or disrupt its operation, like the one that allowed to break the BB84 protocol by blinding the APD-base detector (avalanche photodiode) [3].

4. Discussion

We're closer and closer to having fully operational quantum computers able to implement Shor's and Grover's algorithms. Many cryptographic systems in use today will no longer be safe, but that doesn't mean that all secured data in the world is vulnerable. Most algorithms on which we depend are used for storage, processing, communications, and storage but unfortunately, the underlying systems lack crypto agility, this means the ability to rapidly adapt to new cryptographic algorithms without the need for significant changes in the system itself. This means that organizations may lack the autonomy by themselves to have control of the cryptographic processes without the need for intense manual effort [12]. So we hit the first challenge, compatibility, either new protocol are somehow compatible with existing ones to allow a wide adoption, but we know already the new algorithms will have different mathematical foundations and requirements.

The second challenge is the performance of the new algorithms, NIST considered that when evaluating the candidates, the time to generate the keys, the size of keys, and the time for verifying signatures. All these parameters need to fall within real-world values to enable adoption, otherwise, they will not be practical. As seen above security is one of the other challenges, if the approaches that are being evaluated can be broken a lot will be at stake, we need to ensure that our sensitive information is secured and that the trust that exists between individuals, and organizations are assured. Once again one challenge takes to another, and we already know that for a cryptographic system to be secure that is tied to its computational complexity which may impact performance or on the hand-tied with the hardware that in which it's implemented that could come at an extra cost. At this point, there's a need to make the fine balancing act between cost and benefits [17].

So, there's a need to set up a plan for the migration of post-quantum cryptography. Security standards, procedures, and documentation need to be replaced or changed. Migration playbooks must be developed that consider all this [12].

There’s also the need to identify where the current public-key algorithms are being used and for what purpose. But this usage goes deep inside the operating systems and computer hardware itself, such as:

- Digital signatures for source and integrity authentication [12].
- Identity authentication processes [12].
- Key transport of symmetric keys [12].
- Privilege authorization [12].

So, one more challenge arises, do organizations have the inventory of all these public-key reliant systems, and if not, is there tooling to support organizations identifying these systems. In the same way, there's the need to

make an inventory of all the recommendations in cybersecurity standards that recommend public-key cryptography to reflect the new reality [14].

So, once we know where and what we're employing public-key systems we can determine some relevant use characteristics already identified by NIST and summarized below [12]:

- Current key sizes and hardware/software limits for future key/signature sizes.
- Latency and throughput thresholds
- Processes and protocols used for crypto negotiations.
- Invocation of each cryptographic process.
- Suppliers or owners of each cryptographic system.
- Contractual clauses.
- Expected end-of-life of implementation.
- Is the implementation crypto-agile?
- Sensitivity of information being protected.

With the information above we should be ready to draw up our plan, which to some extent is not different from any other migration plan. We should define our future requirements, define priorities, and in an ideal world influence the roadmap of cryptographic systems developers to address the critical requirements. Some of these requirements are already taken into consideration when NIST evaluated candidates for standardization [15]. Although the path to standards is still long, the security of cartographic algorithms is only as good as the best know attacks to it, so there's still a lot of attacks to be done by researchers to determine the optimal implementation of each algorithm, knowing that sometimes small changes in the implementation might cause a huge effort in the deployment of these new solutions [13], [16].

5. Conclusion

Going through the cryptographic approaches for a post-quantum world shows that organizations are aware of the dangers.

I don't believe we're ready yet for a post-quantum world. If a quantum computer is made available to an attacker tomorrow certainly it would be the dawn of a new dark age, cause a lot of things we consider safe would no longer be. But although time is urging organizations like NIST in its roadmap to release the final list of candidates for standardization in 2023. Of course, defining the standards is not all and there is still a lot of work ahead. Organizations, both governmental and private, need to invest time and money to get ready for the challenges of a post-quantum world.

It's already possible to outline the steps to be taken. Weighting all the change management that will be required it's certain that any plan will be an ambitious one, with a lot of bottlenecks.

If this plan is addressed with success, crypto-system designers will be the silent heroes of the future, with the knowledge we have today new systems will be more crypto-agile to make them more robust and future-proof.

Like in many other branches of Cybersecurity, cryptography is part of a cat-and-mouse race between those who try to keep data secure and those who try to break the systems with illegitimate interests.

Science has proven to be a savior of mankind throughout history and once again mathematics will have to show its value in ensuring that keys are only available to those who have permission.

A lot is certainly left to be said, including the variants of each algorithm, the different approaches to each implementation, and how each can be made more secure for different attacks. A deeper knowledge and more widespread availability of quantum computers in the future will bring more challenges, and more attacks but looking at all the published articles regarding the subject, it's an alive community that is up for current and future challenges.

References

[1] K. Limniotis, 'Cryptography as the Means to Protect Fundamental Human Rights', *Cryptography*, vol. 5, no. 4, p. 34, Nov. 2021, doi: 10.3390/cryptography5040034.

[2] Kenny Paterson, 'Applied_Cryptography_KA_webinar_slides.pdf', 2021.

[3] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, 'The Impact of Quantum Computing on Present Cryptography', *ijacsa*, vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090354.

[4] L. Chen *et al.*, 'Report on Post-Quantum Cryptography', National Institute of Standards and Technology, NIST IR 8105, Apr. 2016. doi: 10.6028/NIST.IR.8105.

[5] 'pkc2022-march2022-moody.pdf'. Accessed: Dec. 09, 2022. [Online]. Available: https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

[6] P. B. B. OBE, 'Learning with Errors and Ring Learning with Errors', *A Security Site: When Bob Met Alice*, Jun. 12, 2019. https://medium.com/asecuritysite-when-bob-met-alice/learning-with-errors-and-ring-learning-with-errors-23516a502406 (accessed Dec. 10, 2022).

[7] 'M5410 McEliece Cryptosystem'. http://www-math.ucdenver.edu/~wcherowi/courses/m5410/ctcmcel.html (accessed Dec. 10, 2022).

[8] J. Hoffstein, J. Pipher, and J. H. Silverman, 'NTRU: A ring-based public key cryptosystem', in *Algorithmic Number Theory*, vol. 1423, J. P. Buhler, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 267–288. doi: 10.1007/BFb0054868.

[9] L. Cherckesova, O. Safaryan, P. Razumov, V. Kravchenko, S. Morozov, and A. Popov, 'Post-Quantum Cryptosystem NTRUEnCrypt and Its Advantage over Pre – Quantum Cryptosystem RSA', *E3S Web Conf.*, vol. 224, p. 01037, 2020, doi: 10.1051/e3sconf/202022401037.

[10] H. Tiwari, 'Merkle-Damgård Construction Method and Alternatives: A Review', vol. 41, no. 2, p. 22, 2017.

[11] D. Moody, 'Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process', National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8413-upd1, 2022. doi: 10.6028/NIST.IR.8413-upd1.

[12] W. Barker, W. Polk, and M. Souppaya, 'Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms', National Institute of Standards and Technology, Apr. 2021. doi: 10.6028/NIST.CSWP.04282021.

[13] Pirandola et al, 'Advances in quantum cryptography.pdf', p.147, 2020.

[14] Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. In: Guarda, T., Portela, F., Santos, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2021. Communications in Computer and Information Science, vol 1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36

[15] F. Alves, N. Mateus-Coelho and M. Cruz-Cunha, "ChevroCrypto – Security & Cryptography Broker," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800797.

[16] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," 2022 *10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800779.

[17] Nuno Mateus-Coelho, A New Methodology for the Development of Secure and Paranoid Operating Systems, Procedia Computer Science, Volume 181, 2021, Pages 1207-1215, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.01.318.