Distributed Secure Credential Encryption in the Quantum Era

Afonso Ventura, David Marinho, Axel Carapinha

Abstract

In this article, it will be explored the potential of quantum computers, providing brief and succinct explanations of their operation. Topics like Superconducting Qubit, Trapped-Ion Qubit, and Neutral-Atom Qubit and how external factors affect them will be discussed. These will give the reader a comprehensive summary of what is a quantum computer and how it works. Additionally, it will be discussed the possible consequences that these computers will bring to the technological world. Some of these threatened systems encompass distributed services like the blockchain, such as its private and decentralized storage capabilities. Nevertheless, Quantum-resistant algorithms (QRA) are being standardized, and a secure communication channel has already been achieved between quantum computers. Consequently, unprepared entities may be dependent on quantum-as-a-service for information protection, and that's where distributed services come into reconsideration, like Multi-party Threshold Schemes (MPTS's). Finally, a single-point-of-failure could expose all information, so alternatives to Lightweight Cryptography (LWC) are already being deployed for internet solutions.

Keywords: Quantum, Qubit, Blockchain, Distributed Credentials, Quantum Key Distribution, MPTS, Quatum-as-a-service

1 Introduction

Humanity lives in a world where nearly everyone feels that they are safe online. However, it has been very challenging for the information security sector to keep up great security systems required due to the daily advances in the information technology field. Devices are becoming smarter but their security is not keeping up. Now, despite that concern, imagine that the security of the classic devices that we use daily, the laptop, the smartphone... are in danger because a supercomputer has been built and now it can perform calculations so fast that almost every encryption algorithm will be able to be exploited in seconds. Regrettably, we must convey concerning news, as the present day brings us closer to that aforementioned scenario

than the preceding day.

In the digital security landscape, password encryption's strength directly impacts the complexity of potential attacks. Robust encryption methods are essential for fortifying defenses against unauthorized access.
And what kind of relation does this topic have with quantum computing?
Quantum computing opens new horizons in the science world, however, it also heavily threatens the information security field with its incredibly fast calculations. With Quantum computing it will be a straightforward task to ruin systems like blockchain cryptography, and even the public key cryptography.

Furthermore, this article will discuss what a quantum computer is and how it may affect cryptographic systems that are extensively used in daily services. Additionally, it will provide an in-depth explanation of blockchain technology and examine its vulnerabilities to quantum computing. Finally, the article will discuss solutions by detailing quantum-resistant algorithms and their integration with blockchain technology.

2 Quantum Computers and Information Security

2.1 Quantum Computers

In the past, the necessity to study quantum systems emerged but since they were very fragile, the concept of building a quantum systems simulator emerged to help observe the quantum systems phenomena. However, Quantum Computers arose because computers were not capable of making the necessary calculations for the construction of a supercomputer.

2.2 How do Quantum Computers work?

Classical computers use bits, a two-state system that can be *1* when there is the presence of an electrical signal or *0* when electrical signals are absent. Quantum computers do not **only** use *0's* and *1's* to control the data flow, they use a superposition of both states, which are named qubits.
Qubits are the basic unit of information that is used by quantum computers to control the data flow. Due to their versatility, qubits can represent an electrical circuit, an atom, a photon, or even an electron, they can represent any state.[1]
Mathematically, they are described as a vector in a complex Hilbert space, with two mutually orthogonal basis states which can be labeled $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1, \quad |\psi\rangle \sim e^{i\alpha}|\psi\rangle \tag{1}$$

2.3 Qubits Technologies

Crafting a qubit is still an area in research and development and there is no one right technique to do it yet. The three most successful qubits until this date are the following:

Table 1 Types of Qubit crafting[2]

Superconducting Qubit	The "superconducting" qubit, preferred by industry leaders like Google and IBM, consists of tiny loops or lines of metal, often aluminum or a mix of aluminum and niobium. Controlled by microwave pulses, it behaves like an atom, with two energy states: the ground state and the excited state. Its compatibility with existing electronic transistor technologies is an advantage, but operation requires cooling to a few hundredths of a degree above absolute zero, necessitating costly dilution refrigerators. Scalability is challenged, with ongoing efforts to overcome limitations.
Trapped-Ion Qubit	Trapped-ion qubits use charged atoms or molecules resembling tiny bar magnets. Its state manipulation is achieved via laser interactions. Companies like Alpine Quantum Technologies, IonQ, and Quantum explore this technology, although scalability is hindered by complex ion interactions. However, trapped-ion qubits offer relatively long quantum information retention compared to superconducting qubits.
Neutral-Atom Qubit	Neutral-atom qubits employ light traps to hold atoms in place, potentially offering scalability advantages. Demonstrated with arrays of two to a thousand qubits, these systems provide relatively long quantum information retention. However, operational complexities persist, with current systems performing calculations slower than both superconducting and trapped-ion qubits. Overcoming these challenges could lead to neutral-atom qubits surpassing other types in computing power, but significant technical hurdles remain in error correction and operational efficiency.

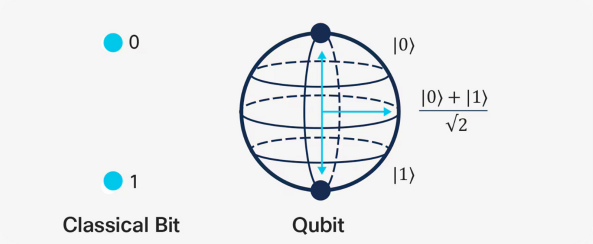


Fig. 1: Schematic representation of a Qubit

Furthermore, it is evident from the aforementioned instances that several external factors may change qubits results and behaviors. Let's examine some of these errors and briefly discuss possible solutions.[3]

2.4 Solutions for External Influences on Qubits

One vulnerability of quantum computers is the occurrence of quantum errors, often for trivial reasons. Correcting these errors has been a significant challenge, which can be addressed in two ways: through error correction programs integrated into the quantum computer's operating system or by reducing error incidence. These errors result from small external noises that can interfere with the delicate internal system responsible for producing qubits.
One approach could be to install the computer in a quieter environment, such as a server room, and implement seismic mitigation techniques to reduce the effects of tremors. Additionally, a security service could be established to allow the computer to boot only when properly connected to the environment.
Quantum computers have stringent cooling requirements, needing to operate at extremely low temperatures, often close to absolute zero. Cooling systems are needed to maintain qubits in a superposed state and reduce decoherence effects.
Another option would be to place the computers in server rooms, thereby reducing interference from particle waves and providing a cooler environment, which would contribute to correcting this error. Additionally, tubes of distilled water with additives could be implemented, known for their effectiveness, although this would inevitably increase the final project cost.

3 Threats to Distributed Services - Blockchain

3.1 What is the Blockchain?

To provide initial context on distributed systems, let's first clarify the concept of one of them: Blockchain. A Blockchain is a registration technology that facilitates the creation of a shared database. It is made up of blocks of information interconnected in an encrypted manner. Each block contains a record of transactions that are validated and added to the blockchain by a network of distributed computers, known as nodes. [4]
Blockchain works like a registration system, keeping a registration permanent and unalterable to transactions. The transactions are grouped into blocks, each of them containing a set of recent transactions and a header with a hash of the previous block in the chain. Before being included in a block, transactions go through a validation process, where network participants, typically computational nodes, execute complex algorithms to check their authenticity and integrity. Once validated and accepted, the block is added to the existing chain, forming a continuous and immutable sequence of transaction records. [4]

3.2 Applications of Blockchain Technology

The Blockchain is the technology behind cryptocurrencies, such as Bitcoins, which is the one we hear most about, among other cryptocurrencies. But its applications go far beyond the financial sphere. This has the potential to revolutionize several sectors, such as supply chain, healthcare, real estate, electronic voting, and others,

ensuring the integrity and security of data. [5][6]

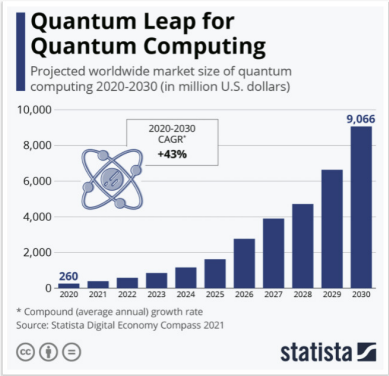
3.3 What Makes Blockchain Special?

One of the fundamental characteristics that make the blockchain exceptional is its immutability. That means that once a transaction is recorded in a block and added to the chain, it cannot be changed or removed without the consent of the majority of network participants. This immutability provides security and transparency to transactions, removing the need for a centralized intermediary, such are the banks that need to validate the transactions. Because of this nature, any attempt to modify would require a significant amount of computing power and the consensus of the majority of network participants, making it extremely difficult and expensive to accomplish. [4]

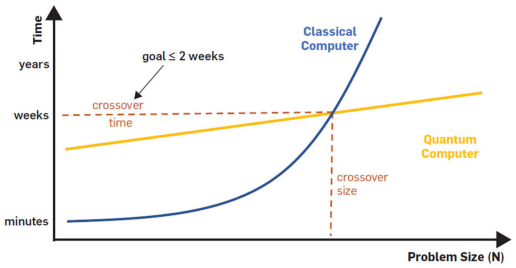
3.4 Risks Brought by Quantum Computers

However, this powerful encryption may face significant risks in the future, as highlighted by *Peter Shor* in 1994: *"A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems that are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer."*. Blockchain will be among these, so quantum computers have the potential to easily decrypt it. [7][8][9]

However, there's no need to fear just yet, quantum computers currently don't have the potency that is predicted for them in the future, they are also extremely expensive and rare worldwide. While today TLS and VPN encryption are considered quite difficult to decrypt, quantum computing could potentially breach security layers using Shor's algorithm, decrypting in just ten seconds what current computers would take ten billion years to achieve. [6][10]
So in the future what could be done to protect the data of decrypt quantum computers? Quantum computers will not only endanger data, they could be a possible solution! These will have the ability to offer opportunities to improve blockchain's security and performance. [11][12]
In a future where good quantum computers exist, not everyone will have access to them. What could companies do to protect civilians with their quantum computers? Investing in some solutions is possible. Educational institutions could enter into contracts with companies that own these computers to protect at least student data. Another possible solution could be for the government itself to encourage companies to protect civilians' computers within the same country and provide some amount of funding for using quantum computers to encrypt civilians' data.



(a) Quantum Predicts Expenses



(b) Quantum Preditcs Resolving Time

However, it's crucial to ensure a specific and private connection for these companies, thereby avoiding internet vulnerabilities that could compromise consumer data security. One alternative would be to implement secure quantum networks (QKD - Quantum Key Distribution), which leverage principles of quantum mechanics to generate secure encryption keys, ensuring communication security even against quantum computer attacks. To initiate this communication, a regular computer would only need to send a request to the company's Quantum Computer. Subsequently, the Quantum Computer would verify if the IP of the regular computer has any data protection contracts. If such contracts exist, the Quantum Computer establishes the secure Quantum network, otherwise, the request would be disregarded.[12]
More of this will be detailed in the next section.

4 Quantum Resistant Algorithms

To better understand the importance of quantum resistant algorithms in the foreseeable years, it's important to contextualize a bit on the history of cryptographic primitives[1] and cryptanalysis methods[2].

4.1 Evolution of cryptography

Even centuries before, there was what we call today as classical cryptography[13]. It was based on substitution[3] and transposition[4] techniques, being considered no longer secure with the rise of computing power in the 20th century.
The ability of computers to execute cryptanalysis methods, such as brute-force and frequency analysis, made protected information vulnerable, and algorithms like DES became the *de facto* for protecting information, in conjunction with others, such as RSA.[14]

[1] fundamental building blocks used in cryptography to construct secure cryptographic systems, protocols, and algorithms
[2] techniques used to analyze and break cryptographic systems without the decryption key
[3] replacing each plaintext's character with another character according to a predetermined key or rule
[4] rearranging the order of the plaintext characters according to a specific system

This was the beginning of modern cryptography, and its foundations can be described as summarized by Jason Deign, "it all comes down to multiplication"[15]: complex mathematical problems that demand extensive computational cycles to brute-force, although far less to produce.
That computational demand was once considered intractable by normal computers, but quantum algorithms like Shor's or Grover's leveraged the potential of quantum computers to exploit encryption standards as ECC.[16] For a better perception of the simultaneously admirable and terrible impact, a 256-bit ECC key provides a security level roughly equivalent to a 128-bit symmetric key, equivalent to 2^{128} iterations to crack the protection (in practice, only half of the key's size is considered).[16]
In addition, in 2022 it was considered that there are 15 years remaining for quantum computers to be more easily targeted at specific tasks like decryption[17], and even "within the coming years"[15]. enforces the need for Post-quantum Cryptography (PQC).

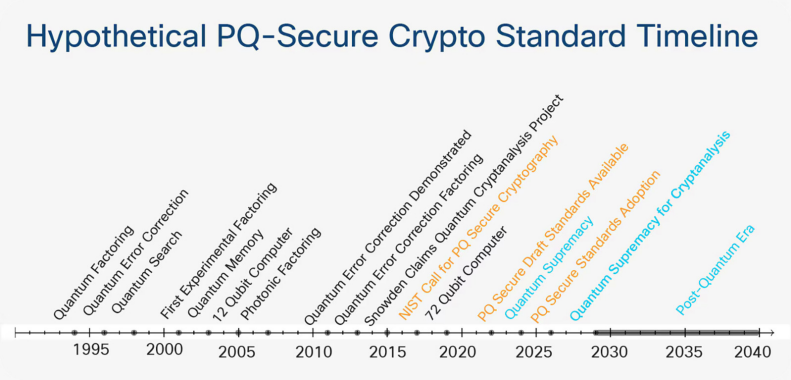


Fig. 3: Timeline for various quantum cryptography standards[18]

4.2 Quantum-resistant algorithms (QRA)

Among the realm of PQC, there's already a list of QRA's, based on problems that are considered hardly tractable, even by quantum computation.
Considering this, and after 6 years of study(started on 2016[19]), testing and selection from top cryptographers all around the world, NIST[5] selected algorithms for a new standardization.[19] They were divided into 3 categories: public-key encryption and key-establishment algorithms, digital signature algorithms and alternative algorithms, for the same goals, but to encompass different underlying approaches.[19]
This cycle of concurrent advancement in protection and vulnerabilities do not end here: CRYSTALS-Kyber (one of the selected by NIST), has been broken by using AI and side channel attacks[6], solely with conventional computers.[20] This development

[5]National Institute of Standards and Technology
[6]type of security breach that targets a system's physical implementation rather than its theoretical functionalities

marks a significant setback in its reliability and long-term viability, questioning the effectiveness of the protection of other QRA's.[20]

4.3 Multi-party Threshold Schemes (MPTS)

All these fragilities may be part of the cause for the NIST's algorithm independent approaches that are in the current implementation: in 2023, NIST started a workshop on MPTS[21], a solution with similarities to the blockchain and Shamir's Secret Sharing[22][7]. As described by them, *using a "secret sharing" mechanism, the secret key is split across multiple "parties"*[23]. This way, the secret key isn't compromised if one of the nodes is, likewise with the miners[8] of the blockchain.[24] This represents a decentralized solution for the entire community in oncoming years, not making it dependent on single-entity solutions, allowing for privacy-oriented methods alongside secure solutions.

4.4 Quantum Key Distribution (QKD)

We consider that this single-entity management could naturally originate from what we consider the greatest key exchange method, *quantum key distribution*. Because of its nature, it's *not* based on mathematical problems, but in the wave function collapse (or quantum collapse).
The act of measurement or observation can cause the wave function of qubits to collapse, affecting the outcome of computations performed using those qubits. This way, it would be able to detect information transmission errors and eavesdropping. This is commonly described as the Alan, Bob, and Eve communication.[25]
The secure exchange described above was already achieved by quantum computers[26], but they are still susceptible to side-channel attacks (as with the above-mentioned CRYSTALS-Kyber) and the signal's quality decays with increasing distances. Therefore, using more quantum computers as propagators would represent more targets to side-channel attacks, and increasing the distance could decrease the quality of the signal, in a way that would not allow to detect eavesdroppers, specially if passive detection methods[9] were used.

4.5 Quantum-as-a-service

This potential of QKD can be leveraged with the help of *quantum-as-a-service*, that allow users to remotely control a conventional computer to manipulate the qubits (in these cases generally photons, a type of qubit[27]), to send the content over the secure channel referred above. Furthermore, the protection of the client's data can be done with "blind quantum computing": so that "clients can access remote quantum computers to process confidential data with secret algorithms and even verify the results are correct, without revealing any useful information."[26]

[7] any subset of a certain size of these shares can be used to reconstruct the original secret, but smaller subsets cannot provide any information about it
[8] nodes that make the verification of operations
[9] techniques used by potential eavesdroppers to intercept or gather information about the quantum signals being transmitted between the communicating parties

If used in conjunction with MPTS[10], it could represent a more decentralized way of dealing with information, instead of relying only in the provided service from an entity, thus enhancing user privacy in a distributed manner, as today's blockchain, and allowing the use of rewarding resources, such as IBM's Qiskit[28].

4.6 Quantum communication in the internet

There's another challenge to face: if quantum computers achieve the speculated potential, the low capacity of some devices, like routers, may not allow to use of methods like the previously mentioned. We are considering that LWC[11] algorithms would not secure these devices, as superior ones did not accomplish these tasks.[29]
Considering this, there are already in-development solutions, like Cisco's SKIP, which needs a "co-located key provider" near each encryption-enabled router in order to protect the keys used for the communication channel. This can be already implemented, even on top of TLS[12].[18]
TLS, as mentioned, represents a use case of *hybrid-key establishments*[13], and shows the importance for companies of joining multiple strategies.

5 Conclusion

In one pessimistic but possible situation, the access to quantum computing could get limited to some entities, and the (now considered) "quantum-resistant" algorithms could be exploited by these computers. In this case, the remaining interconnected community worldwide would depend on resources from some of the quantum-capable entities that offered quantum-as-a-service. We consider this may pose a challenge for user's privacy, because of the dependency on this type of entity, even with *blinded quantum-computing* implemented in QKD. This conclusion arises from the fact that the data will need to arrive at the a conventional computer for the server exactly as the client sent it. Considering this preoccupation, we can divide the measures into three groups: governments, companies and clients.
Considering the companies, we believe that the new NIST's call for MPTS will foster the protection of privacy and data, being to decentralized practices. This is where MPTS can be crucial: to enable quantum-capable entities not only to protect existing distributed systems like blockchain, with some miners being quantum computers, but also enabling the chance for newer ones. Noteworthy, security over the communication channels for the access to these services remains crucial, and that's where Cisco SKIP and other similar solutions can facilitate this. In addition, brute-force prevention mechanisms would be helpful, specially where public-keys are not disclosed.
Regarding governments, some incentive and helping measures, like the one given by the NSA[30] can enable guidance and some alert on the global community to take

[10] Multi-party Threshold Schemes
[11] Lightweight Cryptography, NIST's Ascon family, announced in 2023
[12] cryptographic protocol that includes symmetric encryption algorithms like AES and asymmetric encryption algorithms like RSA or ECC
[13] cryptographic technique that combines elements of both symmetric and asymmetric cryptography to establish secure communication channels

the necessary action. Also, they could promote dynamic password policies with support from password managers and companies.
From the client side, the developers may prioritize future-proof software practices by easing an incoming implementation of the newest algorithms, and current protection technologies (like SSL/TLS, VPNs, ...) can be used with more abstraction, for a wider and easier use for the clients. This is necessary because no solution matters if it is not implemented, as we know happens widely, even with the needed resources. On top of this, other security practices such as salting[14] passwords and support for MFA[15] can increase the effectiveness of protecting information.
Lastly, the spread of information about quantum technology can help the community to become sensible to this important topic, and develop tools that empower everyone. In conclusion, and as the history shows, awareness about the incoming technologies allows better (informed) decisions, an aspect that the authors of this article expect to have contributed positively.

6 Contributions

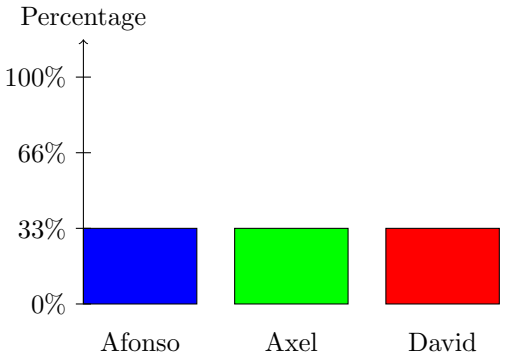


Fig. 4: Contributions of the group members in this project

References

[1] Preskill, J.: Quantum computing 40 years later (2023)

[2] Wright, K.: What's a Qubit? 3 Ways Scientists Build Quantum Computers. [Online; accessed 28-April-2024] (2023). https://www.scientificamerican.com/article/whats-a-qubit-3-ways-scientists-build-quantum-computers/

[14] technique used in cryptography to strengthen the security of stored passwords
[15] Multi-factor authentication

[3] Ezratty, O.: Perspective on superconducting qubit quantum computing. The European Physical Journal A **59**(5), 94 (2023) https://doi.org/10.1140/epja/s10050-023-01006-7

[4] Venturelli, M.: BLOCKCHAIN NA INDÚSTRIA - Como Utilizar a Tecnologia de Blocos Digitais na Cadeia de Produção Industrial (2024). https://www.linkedin.com/pulse/blockchain-na-ind%C3%BAstria-como-utilizar-tecnologia-de-venturelli-v1i0c/

[5] NIST: NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers (2023). https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

[6] Inc, D.H.: What is the Impact of Quantum Computing on Blockchain and Cryptocurrency? (2022). https://hackernoon.com/what-is-the-impact-of-quantum-computing-on-blockchain-and-cryptocurrency

[7] cisa.gov: Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now (2023). https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/

[8] Kumar, M., Mondal, B.: Study on implementation of shor's factorization algorithm on quantum computer. SN Computer Science **5**(4), 413 (2024) https://doi.org/10.1007/s42979-024-02771-y

[9] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing **26**(5), 1484–1509 (1997) https://doi.org/10.1137/s0097539795293172

[10] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994). https://doi.org/10.1109/SFCS.1994.365700

[11] Regina Tupinambá, S.T.: Computadores quânticos colocam a segurança da blockchain em risco? (2018). https://cryptoid.com.br/blockchain/computadores-quanticos-colocam-a-seguranca-da-blockchain-em-risco/

[12] Shrivas, M., Hiran, K., Doshi, R., Bhansali, A.: Advancements in Quantum Blockchain With Real-Time Applications, (2022)

[13] Oommen, B., Zgierski, J.: Breaking sustitution cyphers using

[14] Kahn, D.: The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Simon and Schuster, ??? (1996)

[15] Newsroom, C.: Quantum computers will crack your encryption—maybe they already have. [Accessed May 1, 2024] (2022). https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m03/is-2022-the-year-encryption-is-doomed.html?source=rss

[16] Suo, J., Wang, L., Yang, S., Zheng, W., Zhang, J.: Quantum algorithms for typical hard problems: a perspective of cryptanalysis. Quantum Information Processing **19**(6), 178 (2020) https://doi.org/10.1007/s11128-020-02673-x

[17] Mosca, M., Piani, M.: 2021 quantum threat timeline report. Global Risk Institute (2022)

[18] Cisco: Post Quantum Security Brief. https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html. [Accessed May 1, 2024] (2020)

[19] NIST: Post-Quantum Cryptography PQC. [Accessed May 1, 2024] (2024). https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

[20] Dubrova, E., Ngo, K., Gärtner, J., Wang, R.: Breaking a fifth-order masked implementation of crystals-kyber by copy-paste. In: Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop, pp. 10–20 (2023)

[21] Brandao, L., Peralta, R.: Nist first call for multi-party threshold schemes. National Institute of Standards and Technology (2023)

[22] Brandão, L.T., Mouha, N., Vassilev, A.: Threshold schemes for cryptographic primitives: challenges and opportunities in standardization and validation of threshold cryptography (2018)

[23] Aumasson, J.-P.: Serious Cryptography: a Practical Introduction to Modern Encryption. No Starch Press, ??? (2017)

[24] Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y.: Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation, pp. 365–382 (2016)

[25] Mink, A.: Quantum key distribution (qkd) and commodity security protocols: Introduction and integration (2009)

[26] Drmota, P., Nadlinger, D.P., Main, D., Nichol, B.C., Ainley, E.M., Leichtle, D., Mantri, A., Kashefi, E., Srinivas, R., Araneda, G., Ballance, C.J., Lucas, D.M.: Verifiable blind quantum computing with trapped ions and single photons. Phys. Rev. Lett. **132**, 150604 (2024) https://doi.org/10.1103/PhysRevLett.132.150604

[27] Kevin Delaney: The Quantum Revolution: networking and security for tomorrow's internet. [Accessed May 1, 2024] (2023). https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m06/the-quantum-revolution-networking-and-security-for-tomorrows-internet.html

[28] Barabasi, S., Barrera, J., Bhalani, P., Dalvi, P., Dimiecik, R., Leider, A., Mondrosch, J., Peterson, K., Sawant, N., Tappert, C.C.: Student user experience with the ibm qiskit quantum computing interface. In: Arai, K., Bhatia, R. (eds.) Advances in Information and Communication, pp. 547–563. Springer, Cham (2020)

[29] Turan, M.S., Turan, M.S., McKay, K., Chang, D., Bassham, L.E., Kang, J., Waller, N.D., Kelsey, J.M., Hong, D.: Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process. US Department of Commerce, National Institute of Standards and Technology, ??? (2023)

[30] U.S. Government Publishing Office: Quantum Computing Cybersecurity Preparedness Act. Public Law 117-260. 117th Congress, December 21, 2022 (2022). https://www.congress.gov/bill/117th-congress/house-bill/7535/text