Cloud Computing in the Quantum Era

Mustafa Kaiiali, *Senior Member, IEEE*
The Center for Secure Information Technologies (CSIT),
Queen's University Belfast (QUB),
Belfast, United Kingdom
mustafa_kaiiali@ieee.org

Sakir Sezer
The Center for Secure Information Technologies (CSIT),
Queen's University Belfast (QUB),
Belfast, United Kingdom
s.sezer@qub.ac.uk

Ayesha Khalid, *Member, IEEE*
The Center for Secure Information Technologies (CSIT),
Queen's University Belfast (QUB),
Belfast, United Kingdom
a.khalid@qub.ac.uk

***Abstract*—Cloud computing has become the prominent technology of this era. Its elasticity, dynamicity, availability, heterogeneity, and pay as you go pricing model has attracted several companies to migrate their businesses' services into the cloud. This gives them more time to focus solely on their businesses and reduces the management and backup overhead leveraging the flexibility of cloud computing. On the other hand, quantum technology is developing very rapidly. Experts are expecting to get an efficient quantum computer within the next decade. This has a significant impact on several sciences including cryptography, medical research, and other fields. This paper analyses the reciprocal impact of quantum technology on cloud computing and vice versa.**

Keywords*—*Cloud Computing, Quantum Computing, Post-Quantum Cryptography, Quantum Resistant TPM, Quantum Driven PUF, Homomorphic Encryption, Quantum Annealing.

I. Introduction

There is a popular thought that a quantum computer is a set of classical computers working in parallel to process all of the possible states at once and then ends up with the correct answer. And that once an efficient quantum computer comes into existence, we can solve all of the problems that we have in no time and there will be no need for any classical super computer where we used to submit our extensive computational problems. However, unfortunately, this is not true. A quantum computer does not process all of the possible states at once, rather it is in a superposition state of all possible classical states, i.e., a kind of combination of all classical states with a probability associated with each one based on the problem being solved. So, it does not process all the states individually, rather it tries to find an underlying structure to these states that can be utilized to amplify the probability of the state with the correct answer giving it more chance to be selected at the end [1]. In fact, all of the NP-complete problems are believed to be outside BQP, i.e., the problems that can be solved by a quantum computer in polynomial time, as illustrated in Fig. 1.

Consequently, there is no proof that a quantum computer can be exponentially more efficient than any classical computer for solving any problem. It is currently true for some problems, e.g., factoring a large number, because there is no known efficient algorithm to solve them using a classical computer. However, there is no proof that such an algorithm does not exist. In fact, factorization is not yet proven to be an NP-compete problem. This means that it is not very unlikely that somebody will be able to come up with a polynomial factoring algorithm breaking out all of the current security in use even before a quantum computer exists. For instance, people have long believed that there is no efficient algorithm for primality-testing, an algorithm for determining whether a number is prime or not, until a group of three scientists from the Indian Institute of Technology (IIT) - Kanpur have proven that such an algorithm exists [3] no earlier than 2002! Before that, primality-testing was thought to be as hard as factoring a number, and who knows, we may end up in a situation where we find that P = BQP.

As stated before, when a quantum computer factors a large number, it does not do so by trying all the possible prime factors at once. Instead, it utilizes Shor's algorithm [4] to reduce the factorization problem into the period-finding problem. The period itself is a global property of the quantum superposition of the given number [1]. It is a fact about the entire waves created by this superposition. This reducibility gives more hope that a classical polynomial algorithm may exist.

On the other hand, even if a quantum computer exists, it is not going to be affordable to eliminate the need for the client-server model of computing. In fact, it will increase the necessity for this model as people will be in need to utilize the efficiency of quantum computers to solve some of their problems. As cloud has played a major role in flourishing IoT technology by making a tiny thin-client device as efficient as a super computer [5], it is going to play a major role in bringing the quantum computing power to individuals via its pay as you go pricing model.

The paper is organized as follows: Section II illustrates the impact of quantum technology on cloud computing. Section III discusses the impact of the cloud on quantum technology. Finally, Section IV concludes the paper.

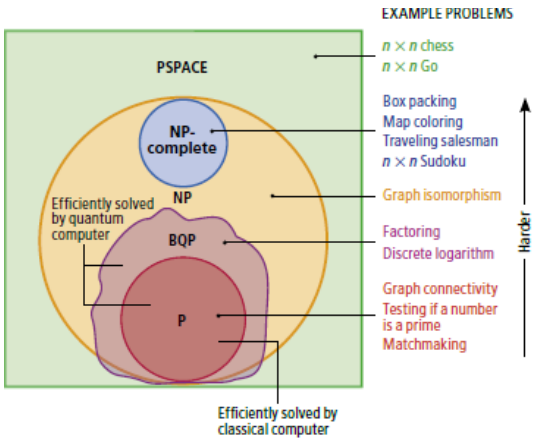

Fig. 1. The complexity of computational problems categorized into different classes accordingly [2].

II. The Impact of Quantum Technology on The Cloud

A. Cloud Security

Cloud is a multi-tenant environment where customers can share computing resources and may co-reside with hackers on the same host. For that, cloud security heavily relies on the security of the underlying Trusted Execution Environments (TEE) [6], e.g., Intel SGX [7], AMD Secure Processor (SP) [8], and ARM TrustZone (TZ) [9]. Thus, a quantum-resistant TEE has to be developed in order to be ready for the quantum era when a large-scale quantum computer becomes a reality, otherwise the security of the cloud will be at risk.

The good thing is that the impact of quantum computers on symmetric key based algorithms, including AES (FIPS- 197), SHA-1/2/3 (FIPS- 180/202), HMAC (FIPS- 198) etc. is milder. Their search space in the face of an exhaustive key search brute force attack is reduced to half by virtue of the Grover algorithm [10]. A quick fix could be to double the key size for these schemes, i.e., use AES-256 instead of AES-128. Therefore, TEE solutions that are based on symmetric cryptography, such as the Intel Advanced Encryption Standard New Instructions (AES-NI) [11], are still valid to work in the quantum era.

However, this is not the case for asymmetric cryptosystems. Mosca [12] has estimated that quantum technology will be able to break RSA-2048 with a 1/7 chance by 2026 and with a 1/2 chance by 2031 as some sort of Moore's law scaling is found to be valid for quantum computers, reaching recently a 72 qubits quantum chip as announced by Google [13]. This impending realization of a scalable quantum computers has led to active research in a set of new quantum-resistant cryptographic schemes or the Post-Quantum Cryptography (PQC) [14]. The public key cryptographic algorithms, ensuing the confidentiality and integrity of digital communications on the Internet and elsewhere today, i.e., the digital signatures standard (FIPS 186) and key establishment schemes (800-56A/B/C) need to be completely discarded and replaced with cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. The National Institute of Standards and Technology (NIST) has initiated a public competition to invite, evaluate, and eventually standardize quantum-resistant public-key cryptographic algorithms suite [15]. The 1st call of proposal schemes received an active response from the research community with 70 submissions in Nov. 2017, the 2nd round candidates narrowed them to 26 proposals, announced in Feb. 2019. The finalist suite is expected around 2022-2023. The security, practicality, efficiency, and side channel vulnerabilities of these schemes on multiple implementation platforms are currently under active research. A successful adaptation of these new schemes into the current security protocols is going to be daunting and challenging, due to the massive number of nodes requiring the upgrade and the potential new vulnerabilities that might result. To reduce the adaptation risks of these post-quantum schemes, the agility of the current schemes is already taken up by Google [16] and strongSwan [17].

In addition, the EU Horizon 2020 research and innovation programme has funded a project entitled FutureTPM to provide a new generation of Trusted Platform Module that are quantum-resistant, i.e., QR-TPM [18]. QR-TPM has to adopt Quantum-Safe Cryptography, e.g., the Lattice-based cryptography [19] which is one of the leading candidates for NIST PQC standardization [20], instead of the popular RSA and ECC cryptosystems. Moreover, the possibilities of using intrinsic Physical Unclonable Functions (PUFs) [21] to derive keys for platform authentication replacing the traditional TPMs have been explored [22]. Furthermore, Quantum Driven PUFs [23] is currently under development to provides end-to-end security for connected devices based on unclonable quantum properties.

On the brighter side of the post-quantum cryptography adaptation, is the added value in terms of advanced security schemes it brings along for the cloud. Some of these security constructs, that come with the Lattice-based cryptographic constructions are listed below:

- The Fully Homomorphic encryption (FHE) or the "Holy Grail" of cryptography, that allows computations on encrypted data, hence protecting data privacy during communication and storage on the cloud, presented by Gentry in his land mark work [24] is based on Lattice-based post-quantum cryptographic schemes.
- Functional encryption (FE) includes identity-based encryption (IBE) [25], its extension hierarchical IBE (HIBE) [26], and attribute-based encryption (ABE) [27], which have shown to be practical using lattices. These constructs provide an alternative to large-scale public key infrastructures on the cloud by utilizing existing user information, such as user identity or characteristics to generate public keys. Rather than binding a user to its public key via a certificate, the already-established user property becomes its public key. This allows for sending of messages without prior certificate lookup, or even prior registration of the receiver to the public key database. Furthermore, it allows integration of timestamps to assign life cycles to keys, or encrypt messages with decryption possible in the future. HIBE eases the workload of the master key extractor through delegation and ABE restricts decryption capabilities to users with certain attributes.

Conversely, as quantum technology is going to break several contemporary cryptosystems, it opens the way for new quantum-based security leveraging the unique properties of quantum physics rather than the computational hardness assumptions of classical cryptography. For example, quantum entanglement [28] can serve as an impenetrable method for secure transmission. Though scientists are unable to send information using this property as the outcomes of quantum measurements are quite random and if we measure an entangled particle in a way that forces it to be in a particular state, the entanglement breaks. Yet, it can still be used to generate and exchange a key for the one-time pad, a cryptosystem that is perfectly secure against all types of cryptanalysis. E91 [29] is a quantum key distribution (QKD) protocol based on quantum entanglement. Likewise, the BB84 scheme [30] is another QKD protocol that leverages the no-cloning theorem [31] of quantum mechanics. It has been tested successfully for secure key distribution over a 200 km quantum channel [32]. Additionally, the inherent randomness of quantum mechanics makes quantum systems a perfect source of entropy for random number generators which plays a key role in cryptography [33].

Therefore, quantum computing can be looked at as a two-edged sword. While it breaks several asymmetric cryptosystems currently in use, it creates more advanced ones that are even harder to break. So, we do not think that quantum technology is going to threaten cloud security, rather it may even enhance it with its new bundle of quantum-based security solutions.

B. Searching Services

Considering a database of unsorted elements, then on average, half of the elements have to be checked before we can find the correct one. This is an O(N) complexity. In [10], Grover proposed a quantum-based searching algorithm that is quadratically faster than the classical one, i.e., $O(\sqrt{N})$. This is a great performance boost. For instance, if N=1,000,000, then the classical approach will have to check 500,000 elements on average, whereas the quantum one takes only 1,000 checks.

Nevertheless, the classical binary search takes O(log N) time to find the correct element. This is exponentially more efficient than the quantum approach. However, the binary search works on sorted data only. Thus, the database has to be sorted before we can be able to run a binary search on it. The best known sorting algorithm is of O(N log N) complexity. This is still better as we are going to sort data for once and search within it forever. However, in the era of unstructured big data that we are living in today, it is challenging to guarantee that we are going to work only on sorted data.

Therefore, we can imagine that cloud database servers are going to employ quantum-based search functionalities in the future to tremendously improve the search time. This can encourage businesses and research communities to outsource their data onto the cloud in order to leverage the quantum search services which is not usually affordable to have on premises as illustrated in Section III.

C. AI Services

AI algorithms learn by analyzing large volume of cases one by one looking for patterns. However, scientists claim that quantum superpositions could escalate the learning process by interfering with each other and avoid looking at each case individually [34]. In fact, quantum computing has already proved itself in the AI field. The D-Wave systems [35], which is not a universal quantum computer, rather it is a quantum annealer famous for finding the global minimum of a given function over a given set of solutions [36], has proven its efficiency in its problem domain. Google announced that D-Wave is 100 million times faster than the classical simulated annealing running on a single core processor [37]. Even when Google ran the test using Quantum Monte Carlo [38], an approach that simulates running quantum problems on classical processors, it found that the D-Wave quantum annealer was still 100 million times faster [37].

Quantum annealer has already been involved in several areas requiring optimization, simulation, and machine learning services. It has been used in: NASA space research [39], medical science for optimal radiation therapy [40], material simulation [41], the financial sector [42], traffic flow optimization [43], and even intrusion detection [44]. Therefore, besides other cloud-based innovative AI solutions, quantum annealing is expected to be the 1st quantum service to be offered on public clouds.

III. The Impact of The Cloud on Quantum Technology

A. Reachability

Quantum technology is expensive. In fact, once a quantum computer comes into reality, it is expected to be costlier than a super computer. Today, D-Wave offers its 2000Q quantum annealer by $15 million [45]. Conversely, IBM offers its 50-qubits universal quantum chip by $15 million as well [46]. According to [47], the average SMB spending on IT is 6.4% of its annual revenue. Whereas, the average revenue of small businesses is not expected to exceed $50 million ending up with a maximum of $3.2 million for the total IT spending on software, communication, and infrastructure. Obviously, it is far away from what a quantum computer may cost.

Conversely, quantum technology requires very specific working conditions to activate the quantum state. For instance, the D-Wave 2X processor operates at 15 Milli-Kelvin temperature $\approx$ -273 Celsius [48]. This means, current quantum technology is not going to be handy and physically affordable to individuals as the traditional classical computing today which can operate at 67 Celsius. Therefore, the only option for quantum technology to reach SMBs and individuals is the cloud computing pay as you go service offering model.

Indeed, IBM has already made its 5-qubit and 16-qubit quantum processors accessible via its online platform, IBM Q Experience [49]. Likewise, Google has launched its online Quantum Computing Playground that can simulate up to 22 qubits quantum registers as of today [50]. Moreover, D-Wave has made its real-time QPU accessible over its online platform, Leap [51], with only 1 minute of QPU time free per month.

B. Efficient Utilization

Despite its powerful computational capabilities, quantum technology has specific application areas. In that, it is not going to replace the deterministic classical computing model. Instead, they are going to work aside. Large businesses, even if they can afford to pay the cost of a quantum computer, are not going to fully rely on it. It is expected that the majority of the time, quantum computer will stay idle. Thus, the cloud multi-tenant environment is the only way to increase the efficient utilization of the quantum computing power.

IV. Conclusion

This paper discusses, for the first time, the potential impact of quantum technology on cloud computing and vice versa. It has been shown that both technologies are going to complement each other. The power of quantum computing is going to enhance the computing capabilities of the cloud and allow it to offer more efficient computing services. Whereas, the cloud is going to fully unleash quantum technology by bringing it to individuals and make it more affordable to SMEs.

Acknowledgment

We would like to thank Dr. Ahmad Elkhateb for proofreading the paper.

REFERENCES

[1] S. Aaronson, "Shor, I'll do it," *The Blog of Scott Aaronson*, 2007. [Online], Available: https://www.scottaaronson.com/blog/?p=208.

[2] S. Aaronson, "The limits of quantum computers," *Scientific American*, vol. 298, no. 3, 2008, pp. 62–69.

[3] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in P," *Annals of Mathematics*, vol. 160, no. 2, 2004, pp. 781-793.

[4] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 41, no. 2, 1999, pp. 303-332.

[5] M. Kaiiali, "Designing a VM-level vertical scalability service in current cloud platforms: a new hope for wearable computers," *Turk J Elec Eng & Comp Sci*, vol. 25, No. 4, 2017, pp. 2555-2566.

[6] The Trusted Execution Environment (TEE), *Wikipedia*. [Online], Available: http://en.wikipedia.org/wiki/Trusted_execution_environment. [Accessed Mar. 11, 2019].

[7] Intel Software Guard Extensions. https://software.intel.com/en-us/sgx.

[8] Secure Processor (AMD-SP) - AMD, *WikiChip*, 2018. [Online], Available: http://en.wikichip.org/wiki/amd/secure_processor. [Accessed Mar. 11, 2019].

[9] ARM TrustZone, *Wikipedia*. [Online], Available: https://en.wikipedia.org/wiki/ARM_architecture#TrustZone_.28for_Cortex-A_profile.29. [Accessed Mar. 11, 2019].

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," *the 28th annual ACM symposium on Theory of computing (STOC'96)*, NY, USA, 1996, pp. 212-219.

[11] J. Rott, "Intel® Advanced Encryption Standard Instructions (AES-NI)," *Intel*, 2012. [Online], Available: https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.

[12] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security and Privacy*, vol. 16, 2018, pp. 38-41.

[13] J. Kelly, "A Preview of Bristlecone, Google's New Quantum Processor," 2018. [Online], Available: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

[14] Post-Quantum Cryptography, *Wikipedia*. [Online], Available: https://en.wikipedia.org/wiki/Post-quantum_cryptography. [Accessed Mar. 11, 2019].

[15] Post-Quantum Cryptography, *The National Institute of Standards and Technology (NIST)*, 2017. [Online], Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. [Accessed Mar. 11, 2019].

[16] M. Braithwaite, "Experimenting with Post-Quantum Cryptography," *Google Security Blog*, 2016. [Online], Available: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[17] New Hope Post-Quantum Key Exchange Algorithm, *strongSwan*. [Online], Available: https://wiki.strongswan.org/projects/strongswan/wiki/Newhope.

[18] The 1st FutureTPM Workshop on Quantum-Resistant Crypto Algorithms. [Online], Available: https://futuretpm.eu/1st-futuretpm-workshop.

[19] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," *the 37th Annual ACM Symposium on Theory of Computing (STOC'05)*, NY, USA, 2005, pp. 84-93.

[20] D. Micciancio, "Lattice-Based cryptography," *Encyclopedia of Cryptography and Security (2nd Ed.)*, 2011, pp. 713-715.

[21] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *the 9th ACM Conference on Computer and Communication Security*, Washington, DC, Nov. 2002, pp. 148-160.

[22] The Physically unclonable functions found in standard PC components (PUFFIN) project, http://puffin.eu.org.

[23] Crypto Quantique (CQ), https://www.cryptoquantique.com.

[24] C. Gentry, "Fully homomorphic encryption using ideal lattices," *the 41st annual ACM symposium on Theory of computing (STOC'09)*, New York, NY, USA, 2009, pp. 169-178.

[25] L. Ducas, V. Lyubashevsky, and T. Prest, "Efficient identity-based encryption over NTRU lattices," *Advances in Cryptology - ASIACRYPT 2014*, Springer, Taiwan, 2014, pp. 22-41.

[26] X. Boyen, "Attribute-based functional encryption on lattices," *the 10th conf. on Theory of Cryptography*, Springer, Japan, 2013, pp. 122-142.

[27] P. Campbell and M. Groves, "Practical post-quantum hierarchical identity-based encryption," *the 16th IMA International Conference on Cryptography and Coding*, Oxford, 2017. [Online], Available: http://www.qub.ac.uk/sites/CSIT/FileStore/Filetoupload,785752,en.pdf.

[28] Quantum Entanglement, *Wikipedia*. [Online], Available: https://en.wikipedia.org/wiki/Quantum_entanglement. [Accessed Mar. 11, 2019].

[29] E91 protocol, *Wikipedia*. [Online], Available: https://en.wikipedia.org/wiki/Quantum_key_distribution#E91_protocol:_Artur_Ekert_.281991.29. [Accessed Mar. 11, 2019].

[30] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *the IEEE International Conference on Computer Systems and Signal Processing*, India, 1984, pp. 175–179.

[31] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, 1982, p. 802-803.

[32] R. Pease, "'Unbreakable' encryption unveiled," *BBC News*, 2008. [Online], Available: http://news.bbc.co.uk/1/hi/sci/tech/7661311.stm.

[33] M. Herrero-Collantes and J.C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys., vol. 89, no. 1, pp. 015004, 2017.

[34] F. Ghafari, et al., "Interfering trajectories in experimental quantum-enhanced stochastic simulation," *Nature*, vol. 10, no. 1, 2019.

[35] D-Waves Systems Inc., https://www.dwavesys.com.

[36] Quantum annealing, *Wikipedia*. [Online], Available: https://en.wikipedia.org/wiki/Quantum_annealing. [Accessed Mar. 11, 2019].

[37] M. A. Russon, "Google: Controversial D-Wave quantum computer works and is 100 million times faster than PCs today," *International Business Times*, 2015. [Online], Available: https://ibt.uk/A6QgS.

[38] Quantum Monte Carlo, *Wikipedia*. [Online], Available: https://en.wikipedia.org/wiki/Quantum_Monte_Carlo. [Accessed Mar. 11, 2019].

[39] NASA Quantum Artificial Intelligence Laboratory (QuAIL). https://ti.arc.nasa.gov/tech/dash/groups/physics/quail.

[40] D.P. Nazareth and J.D. Spaans, "First application of quantum annealing to imrt beamlet intensity optimization," *Phys. Med. Biol.*, vol. 60, no. 10, 2015, pp. 4137-4148.

[41] R. Harris, et al., "Phase transitions in a programmable quantum spin glass simulator," *Science*, vol. 361, no. 6398, 2018, pp. 162-165.

[42] P. Rebentrost, B. Gupt, and T.R. Bromley, "Quantum computational finance: Monte Carlo pricing of financial derivatives," *Phys. Rev. A*, vol. 98, no. 2, 023823 (2018).

[43] F. Neukart, G. Compostella, C. Seidel, et al., "Traffic Flow Optimization Using a Quantum Annealer," *Front. ICT*, vol. 4, no. 29, 2017.

[44] T. Aldwairia, D. Perera, and M. A. Novotny, "An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection," Computer Networks, vol. 144, 2018, pp. 111-119.

[45] J. Temperton, "Got a spare $15 million? Why not buy your very own D-Wave quantum computer," *Wired*, 2017. [Online], Available: https://www.wired.co.uk/article/d-wave-2000q-quantum-computer.

[46] S. Anthony, "IBM will sell 50-qubit universal quantum computer 'in the next few years'," *Ars Technica*, 2017. [Online], Available: https://arstechnica.com/?post_type=post&p=1214637.

[47] Understanding Technology Costs, *Network Alliance*. [Online], Available: https://networkalliance.com/understanding-technology-costs.

[48] The D-Wave 2X™ Quantum Computer Technology Overview, *D-Wave Systems Inc.*, 2015. [Online], Available: https://www.dwavesys.com/sites/default/files/D-Wave%202X%20Tech%20Collateral_0915F.pdf.

[49] IBM Q Experience, https://quantumexperience.ng.bluemix.net/qx.

[50] Quantum Computing Playground, https://opensource.google.com/projects/quantum-computing-playground.

[51] D-Wave Leap, https://cloud.dwavesys.com/leap.