International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Ethical and Security Considerations in the Era of Quantum Computing: A Framework for Responsible Implementation Strategies

Arya Brijesh Tiwari[1], *Devesh Amlesh Rai*[2], *Anant Manish Singh*[3], *Krishna Jitendra Jaiswal*[4]

[1,2,3,4] Department of Computer Engineering, Thakur College of Engineering and Technology, Mumbai, India
[1]aryatiwari45@gmail.com, [2] deveshrai162@gmail.com, [3]anantsingh1302@gmail.com, [4]krishnajaiswal2512@gmail.com

DOI: https://doi.org/10.55248/gengpi.5.0524.1295

ABSTRACT

Quantum computing stands as a promising avenue for advancing the capabilities of computers within the realm of computer science. By harnessing the power of qubits, quantum computers diverge from traditional computing models based on bits, enabling the storage of vast amounts of information through the principle of superposition. While quantum computing was once relegated to the realm of theory, recent developments, such as IBM's successful creation of a functional quantum computer, have propelled it into the realm of practical exploration. This newfound capability has ignited interest among scientists, who are actively probing the potential of quantum algorithms like Shor's prime factorization algorithm. Notably, Shor's algorithm possesses the remarkable ability to decipher modern RSA encryption, underscoring the urgent need for the development of alternative encryption methods. Quantum computing thus holds the unique potential to revolutionize the field of computer science. However, grasping the full scope of its impact necessitates careful consideration and dialogue to ensure responsible implementation strategies.

1. Introduction

Moore's Law is a fundamental law that governs computer science. About every two years, computer processors can contain twice as many transistors in the same amount of space, according to Intel CEO Gordon Moore. Stated differently, Moore projected that the power of computers will double every two years. For more than 40 years, this trend seemed unwavering; but, in the last five years, processor makers began to face challenges in maintaining this pace. Transistors are now only a few atoms in size due to their very tiny size. Since it is impossible to create transistors that are much smaller than a few atoms, researchers in computer science have begun to explore alternative methods of boosting processing capacity. In the discipline of computer science, quantum computing offers a relatively new paradigm that functions entirely differently from traditional computers. Since a quantum computer had never been constructed, until recently, quantum computing was not thought to be a practical alternative to conventional computers. When IBM developed the IBM Q, the first quantum computer ever made, this mindset was altered. Since more reliable options like three-dimensional integrated circuits do not improve computers' computational power and because quantum computing can solve issues like breaking cryptographic algorithms, it currently stands as the most promising development in computer technology. In particular, the well-designed quantum computer offered by the IMB Q architecture has certain benefits over traditional computers. Furthermore, quantum algorithms, such as Shor's algorithm, offer answers to issues that were previously unsolvable. It is crucial to have a working technical understanding of how a quantum computer functions in order to appreciate the potential that quantum computing has to radically alter computer science.

2. Background

In traditional computer systems, data is stored in bits. A bit can stand for zero or one, or a low or high voltage, depending on the situation. All of a computer's memory and processing capabilities are composed of these ones and zeros. The differences between classical and quantum computers begin at this basic level. Bits do not exist in quantum computing. Rather, a fundamental component known as a qubit powers quantum system. The spin of an electron or the polarization of a photon are two examples of the several particle attributes that may be used to represent a qubit. Qubits can exist in a superposition of these two states, unlike bits, which are limited to only one of these two states. Any of these qualities have two possible states in which they can exist.

Even while at first glance this distinction might not appear like much, a deeper look exposes the qubit's strength. There are sixteen different ways to arrange ones and zeros when using four bits. These four bits can only indicate one configuration at a time in classical computing. The quantum superposition characteristic allows all 16 potential configurations to be represented simultaneously using four qubits. Taking into account just 100 qubits, which may concurrently represent 1.27×10 〖^30〗 possible configurations, this storage potential becomes stratospheric. There are ramifications for this expertise across several computer science domains. For instance, this feature might completely change the way that data is stored. A petabyte, or one billion gigabytes, is a significant computing memory capacity that can currently be attained by some of the supercomputers that are in use today. With the same number of qubits, a quantum computer may have almost unlimited memory.

Cryptography is more specifically impacted by quantum computing. Information is presently encrypted using powers of very big prime numbers. This system's reasoning is predicated on the idea that it would take an enormously long time for a conventional computer to factor these hundreds of digit integers. A quantum computer may factor any number in a single operation by simultaneously testing all potential factors through the superposition of qubits. Given the abundance of confidential and sensitive data that is now concealed on computer systems by encryption, the ethical issues that quantum decryption raises are many and extremely significant. Some have questioned whether computing is still the best option for computing due to ethical quandaries and other problems with quantum computing. Three-dimensional integrated circuits have been pushed as a better option for quantum computing by some.

3. Evaluation of Three-Dimensional Integrated Circuits as an Alternative to Quantum Computing

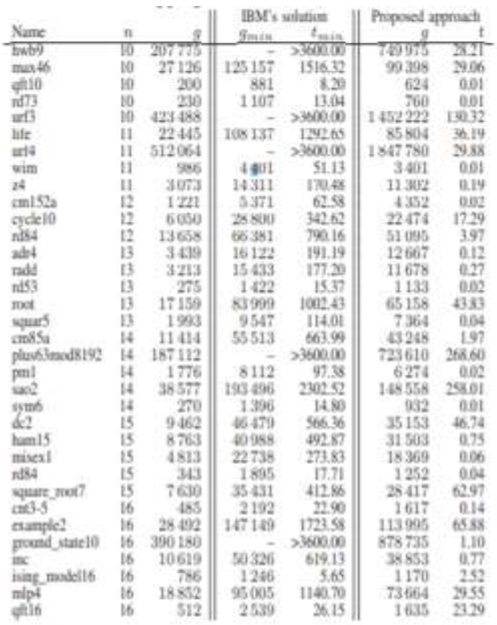
Aside from giving up on traditional computers, numerous alternatives have been put out to address the problem of maintaining the Moore's law trend. An additional option to quantum computing is the use of three-dimensional integrated circuits. In order to create a single processing unit, two-dimensional circuits are stacked and vertically integrated to create three-dimensional integrated circuits. Compared to a conventional two-dimensional circuit, this technique reduces power consumption and speeds up processing. There are many in the computer science industry drawn to this design. Current three-dimensional architecture appears to be a logical choice for computing in the future since it makes use of traditional computer infrastructure while achieving greater speeds at reduced power costs. This conclusion is shortsighted, though. Three-dimensional integrated circuits provide little computational benefit over existing computers, but they do have a noticeable speed advantage. The procedures that a two-dimensional circuit can complete are precisely the same as those that a three-dimensional integrated circuit can do. This restricts the advancements in three-dimensional integrated circuits to just faster performance and its byproducts. At the atomic level, three-dimensional integrated circuits also face problems. Jinwook Song, Seungtaek Jeong, Shinyoung Park, Jonghoon Kim, Seokwoo Hong, and Joungho Kim (2017) investigate three-dimensional integrated circuits and find a significant problem with them. They conducted their research at the Korea Advanced Institute of Science and Technology. The electrons inside the circuit begin to interact with one another and contaminate data when there are several circuits in a small area, as they discovered (Song et al., 2017). It is not possible to argue that the performance boost that three-dimensional integrated circuits offer justifies the hardware constraints and data corruption problem associated with them. Three-dimensional integrated circuits are faster than qubits, but they are not as inventive as qubits when it comes to quantum computing. On the other hand, electron interference may destroy memory just as much as quantum noise.

4. Progress

a) Technical Detail

A steady and well-understood environment is beneficial for conducting research in computer science. Anything that is developed for a computer, such an algorithm or data structure, yields outcomes that can be tested and seen. But until recently, quantum computing lacked this convenience. Since the 1980s, quantum computing has been the subject of theoretical discussion. One of the most well-known algorithms for quantum computing, Shor's Algorithm, was developed in 1994. The discipline of computer science was not greatly affected by quantum computing since there was no quantum environment available to test the idea.

IBM began its IBM Q initiative in March 2017 and by June of the same year, a 16-qubit quantum computer that the general public could utilize over the cloud had been produced. Researchers from Johannes Kepler University, Robert Wille, and Alexandru Paler (2018) explain in their paper on the IBM Q program how having access to a working quantum computer will enable computer scientists to advance the field of quantum computing in a way that has never been possible before (Zulehner, Paler & Wille, 2018, p. 1135). But before quantum research can advance to its full potential, a useful instruction set must be created. A set of instructions exists in classical computers, which are directly converted into machine code upon which all subsequent calculations are based. These operations can be seen with their operation speeds in figure 1 (Zulehner, Paler & Wille, 2018, p. 1138).



			IBM's solution		Proposed approach	
Name	n	g	g_{min}	t_{min}	g	t
hwb9	10	207 775	–	>3600.00	749 975	28.21
max46	10	27 126	125 157	1516.32	99 398	29.06
qft10	10	200	881	8.20	624	0.01
rd73	10	230	1 107	13.04	760	0.01
urf3	10	423 488	–	>3600.00	1 452 222	130.32
life	11	22 445	108 137	1292.65	85 804	36.19
urf4	11	512 064	–	>3600.00	1 847 780	29.88
wim	11	986	4 401	51.13	3 401	0.01
z4	11	3 073	14 311	170.48	11 302	0.19
cm152a	12	1 221	5 371	62.58	4 352	0.02
cycle10	12	6 050	28 800	342.62	22 474	17.29
rd84	12	13 658	66 381	790.16	51 095	3.97
adr4	13	3 439	16 122	191.19	12 667	0.12
radd	13	3 213	15 433	177.20	11 678	0.27
rd53	13	275	1 422	15.37	1 133	0.02
root	13	17 159	83 999	1002.43	65 158	43.83
squar5	13	1 993	9 547	114.01	7 364	0.04
cm85a	14	11 414	55 513	663.99	43 248	1.97
plus63mod8192	14	187 112	–	>3600.00	723 610	268.60
pm1	14	1 776	8 112	97.38	6 274	0.02
sao2	14	38 577	193 496	2302.52	148 558	258.01
sym6	14	270	1 396	14.80	932	0.01
dc2	15	9 462	46 479	566.36	35 153	46.74
ham15	15	8 763	40 988	492.87	31 503	0.75
misex1	15	4 813	22 738	273.83	18 369	0.06
rd84	15	343	1 895	17.71	1 252	0.04
square_root7	15	7 630	35 431	412.86	28 417	62.97
cnt3-5	16	485	2 192	22.90	1 617	0.14
example2	16	28 492	147 149	1723.58	113 995	65.88
ground_state10	16	390 180	–	>3600.00	878 735	1.10
inc	16	10 619	50 326	619.13	38 853	0.77
ising_model16	16	786	1 246	5.65	1 170	2.52
mlp4	16	18 852	95 005	1140.70	73 664	29.55
qft16	16	512	2 539	26.15	1 635	23.29

Figure 1: List of Zulehner's, Paler's, and Wille's operations with speeds

On classical computers, operations like arithmetic, bitwise boolean operations, memory loading and storing, and conditional jumps are all expressed directly in machine code. The utility of this computer is limited if certain operations are not represented on the IBM Q architecture.

By simply reading the current voltage and assigning a zero for low voltage and a one for high voltage, classical logic gates may assign a value to a bit. When this is attempted on a quantum computer, the quantum system becomes a classical computer when the superposition of a qubit is forced to collapse into zero or one. The superposition won't collapse if quantum gates are used, as they can determine the likelihood of a qubit existing in each of the several superpositions (Zulehner, Paler & Wille, 2018, p. 1136). In order to transfer these circuits to certain fundamental computer functions, Zulehner, Paler, and Wille used the Hadamard gates included in the IBM Q architecture. This mapping not only surpasses the prior IBM approach in terms of time complexity and memory utilization, but it also meets all the fundamental requirements needed to construct high level computing and algorithms. Researchers may now investigate more intricate quantum calculations, including Shor's decryption technique, thanks to this advancement.

Several quantum computer algorithms were created by mathematician Peter Shor. And the most well-known of them is Shor's method, which is a method for determining the prime factorization of an integer. Although the speed at which Shor's process factors a number is log(n), where n is the amount of the input and log(n) indicates how long it takes to execute, this prime factorization process may not seem groundbreaking. Numbers cannot be factored in polynomial time by any other algorithm. Stated differently, no alternative approach has a temporal limit on how long it takes to determine a number's prime factorization. To show the algorithm's strength and speed, Shweta Nagaich and Y.C. Goswami (2015) investigate it further in their paper using a quantum computer simulation. Understanding quantum simulations is necessary to explain how Shor's Algorithm was implemented. The requirement to represent qubits with bits makes it challenging to represent a quantum system on a classical system. Ioannis Karafyllidis, Georgios Ch. Sirakoulis, and Panagiotis Dimitrakis (2018) suggest using memristors as a remedy in their study on this problem. Memristors are used in conventional computer systems and perform similar functions to quantum logic gates. By exploiting the basic symmetry relations between current, voltage, charge, and flux in the computer circuits, they imitate the states that a qubit may achieve.

Going on, Shor's method is based on the effectiveness of quantum Fourier transformations, which gives it its speed (Nagaich & Goswami, 2015, p. 165). Using quantum Fourier transformations, several qubits in a quantum state are mapped to a superposition of all conceivable states. For extremely big numbers, this superposition enables quick computation of Euler's Theorem. Although it is presently impossible to create a quantum computer strong enough to factor hundreds of digit long numbers, Nagaich and Goswami's simulation proved effective enough to work with three-digit numbers (Nagaich & Goswami, 2015, p. 165). Figure 3 (Nagaich & Goswami, 2015, p. 166) shows the algorithm's visualization that was also produced by Nagaich and Goswami.

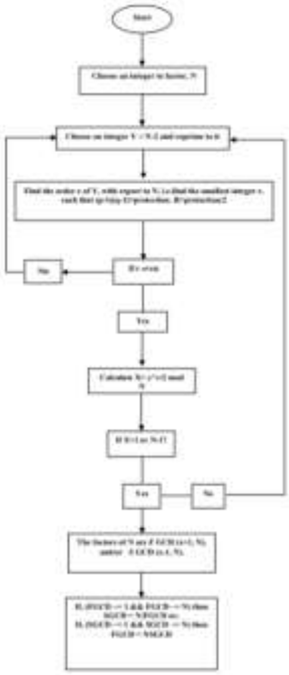


Figure 3: Shor’s Algorithm

Although this may not sound impressive, the fact that the technique functions on a quantum computer indicates that factoring thousands-digit long integers is possible with the development of more potent devices. Decryption is a feature of encryption using quantum computing. The generation of quantum encryption keys is another capability of quantum computers. Compared to their conventional counterparts, these quantum keys have one significant advantage: they can be transferred without worrying about being intercepted. Chris Edwards (2017) writes about a recent Chinese study that used a quantum key distribution protocol to transport a quantum key 750 kilometers from Beijing to Shanghai in his work that was published in Communications of the ACM. The key was encrypted by the Chinese using the angle of polarization of photon particles. The photons' angle of polarization is necessary to decrypt the key; however, estimating the angle incorrectly will change the qubits' state and prevent access to the original state. It is considerably more difficult to estimate the angle since the sender has the ability to alter the polarization angle during transmission. The sender can securely decrypt the key with the recipient after the intended recipient has the key (Edwards, 2017, p. 13). Figure 4 (Krawec, Nelson & Geiss, 2017, p. 1155) shows the helpful visualization that Walter Krawec, Michael Nelson, and Eric Geiss (2017) produced to depict the process in their study on the quantum key distribution protocol.

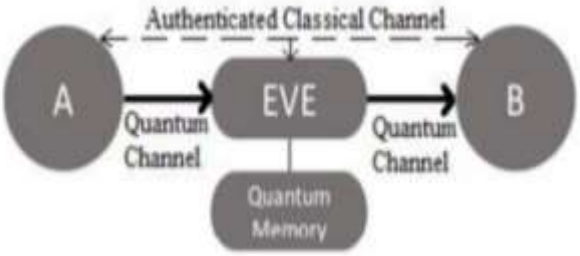


Figure 4: Quantum key distribution protocol

The first people to demonstrate that this procedure could be carried out across a vast distance with our present technology were the Chinese. The furthest a quantum key could reach before quantum noise rendered the signal unusable was around 100 miles prior to this transmission. The Chinese demonstrated that qubits could be sent across any distance with the use of quantum signal boosters that would regenerate the key every 100 miles. The signal boosters worked in tandem with appropriate fiber-optic connections.

b) Social Impact

Although computer scientists believe that quantum computing would have an influence on both general computing and computer science, they have selected a few areas of special interest. Shohini Ghose (2018) delineated three primary areas of focus in her TED talk: quantum encryption, instantaneous information transmission, and molecular modeling. The incapacity of classical computers to completely recreate the quantum realm in a binary system places limitations on molecular simulations. On the other hand, these simulations can produce an actual quantum environment on a computer operating in the quantum domain. This trend primarily affects the pharmaceutical business and, more precisely, medication development (Ghose, 2018). Accurately calculating interactions between various medication compounds at the atomic and quantum levels is very hard to do using classical computers. The ability to simulate these medications correctly might replace the requirement for animal testing as computer data on a drug's effects can be gathered with equal accuracy. Apart from intermolecular communication, the quantum world provides a means of real-time data transport.

Quantum teleportation, or instantaneous information transfer, makes use of a characteristic of quantum particles known as quantum entanglement. Two particles can become entangled, which means that any changes in one particle's state instantaneously reflect in the other, according to the theory of quantum entanglement (Ghose, 2018). In the event that a qubit in a quantum computer is determined by the clockwise or counterclockwise spin of an electron, for instance, altering one qubit from a zero to a one will instantaneously alter all entangled qubits from a zero to a one. Although quantum teleportation has not yet been utilized in any communication system, this feature might prove to be highly valuable in the future for applications such as interplanetary communication. Light travels from the sun to Earth in eight minutes. Although this delay in communications is not unreasonably long, it may take years if humanity ever attempted to inhabit planets outside of our solar system. The limitation of distance would vanish with quantum teleportation. Information may move quickly and effortlessly over the world thanks to quantum teleportation's ability to deliver any file stored on a computer immediately, even in circumstances when traditional transmission would take practically no time at all.

Regarding implications, the effect of quantum computing on encryption is arguably the most talked about. There are significant implications for encryption and decryption from quantum computing. RSA encryption becomes unreliable when factoring arbitrarily big integers is possible using Shor's Algorithm. The great bulk of data on computers is encrypted using RSA, while there are other encryption techniques that are employed as well. The development of a quantum computer capable of computing Shor's Algorithm might pose one of the biggest security risks in computer history to unsuspecting parties. Any system that uses RSA encryption is vulnerable to hacking, putting any data within at danger. Given the significant danger involved, it is imperative to investigate this matter and devise a strategy for handling encryption prior to the development of quantum computers that are able to break RSA.

V. Ethical Analysis

People's basic right to privacy is obviously violated when sensitive data is easily hacked into and stolen, and any organization handling secure data has a duty to safeguard it. The unalienable right to privacy is something that should always be upheld, according to philosopher John Locke. From this perspective, all encrypted data ought to be encrypted as quickly as feasible under a distinct system that would be shielded from quantum computing. This would not be required, though, as the only people who would have access to such technology would presumably be a government agency or research facility with substantial funds. One can argue that RSA has to be replaced if the only persons who have access to quantum computers are those who are unlikely to exploit them for immoral reasons. This argument adheres to philosopher John Stuart Mill's utilitarian frame of view since, in this case, the expenses outweigh the increased privacy that comes with using quantum encryption. Furthermore, it's possible that it will take some time to construct a quantum computer strong enough to run Shor's Algorithm, meaning that any action taken now will be outperformed by a solution that can be implemented in a century.

The use of quantum encryption offers a reliable remedy for this problem. As long as there are no significant changes to our knowledge of quantum physics, quantum key encryption will remain almost impregnable. Although the technology needed to transmit quantum-encrypted data is now much too costly for widespread use, this barrier will vanish as quantum computers advance. More potent quantum computers are advantageous for both Shor's Algorithm and quantum encryption, and when these advancements are realized, both become more affordable and simpler to use on a broad scale. If Shor's Algorithm and quantum encryption advance at the same rate, quantum encryption will catch up to Shor's Algorithm when quantum computers reach a level of power that is sufficient for it

6. Conclusion

The era of quantum computing is rapidly approaching, since IBM has already implemented functional quantum computers. Three-dimensional integrated circuits are one possibility that has certain advantages over the others, but it is not a practical option due to its hardware constraints. It is impossible to overstate how crucial it is to comprehend quantum computing and how this paradigm shifts computer science. The IBM Q architecture's instruction set demonstrates the feasibility of quantum calculations in the present and, with a sufficiently strong computer, the potential implementation of sophisticated algorithms such as Shor's algorithm. Data encryption will need to change once Shor's method is implemented in order to stay safe. Through quantum encryption, quantum computing can also offer a solution to this problem. It is the ethical duty of computer science experts to stay up to date on developments in quantum computing, just as with any other progress in the industry. Even for experts in computer science, understanding quantum computing may be challenging. Without much attention, the quantum realm exists beyond the scope of traditional computer science. This severe undervaluation is a mistake, and understanding quantum computing will be critical to the computer science community's sustained prosperity once quantum supremacy has been achieved.

VII. References

[1] Gharibi, Wajeb, et al. "Quantum technology for analysis and testing computing systems." East-West Design & Test Symposium (EWDTS 2013). IEEE, 2013.

[2] Singh, Harpreet, and Abha Sachdev. "The quantum way of cloud computing." 2014 International Conference on Reliability Optimization and Information Technology (ICROIT). Ieee, 2014.

[3] Fu, Xiang, et al. "A heterogeneous quantum computer architecture." Proceedings of the ACM International Conference on Computing Frontiers. 2016.

[4] Gotarane, M. V., and Mr Sushant Savita Madhukar Gandhi. "Quantum Computing: Future Computing." International Research Journal of Engineering and Technology 3.2 (2016): 1424-1427.

[5] Hey, Tony. "Quantum computing: an introduction." Computing & Control Engineering Journal 10.3 (1999): 105-112.

[6] Marella, Surya Teja, and Hemanth Sai Kumar Parisa. "Introduction to quantum computing." Quantum Computing and Communications. IntechOpen, 2020.

[7] Singh, Shashank. “Assessing Potential Health and Environmental Side Effects of 5G Technology Deployment.” European Chemical Bulletin , vol. 12, no. 3, 2023, https://eurchembull.com/uploads/paper/cf8e3dc4345e5ccc456456013757a2f3.pdf.

[8] Singh, Shashank. “Edge-cloud computing systems for unmanned aerial vehicles capable of optimal work offloading with delay.” 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), 2023, https://doi.org/10.1109/icears56392.2023.10085047.

[9] Kanchan Chaudhary, and Dr. Shashank Singh. “Different machine learning algorithms used for secure software advance using software repositories.” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2023, pp. 300–317, https://doi.org/10.32628/cseit2390225.

[10] Singh, Shashank. “Enhanced particle swarm optimization based node localization scheme in wireless sensor networks.” 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), 2022, https://doi.org/10.1109/icaiss55157.2022.10010896.

[11] Singh, Shashank. “Scheduling in multi-hop wireless networks using a distributed learning algorithm.” 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), 2023, https://doi.org/10.1109/icoei56765.2023.10125909.

[12] Gaur, N. ., and S. . Singh. “A Behaviour Study on Cloud Eco-System: Data Security Perspective”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 6, July 2023, pp. 172-7, https://ijritcc.org/index.php/ijritcc/article/view/7379.

[13] Singh, Dr. Shashank. “IOT security challenges and emerging solutions: A comprehensive review.” INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, vol. 07, no. 09, 2023, https://doi.org/10.55041/ijsrem25662.

[14] A.J.G. Hey and R.W. Allen, eds., ‘The Feynman Lectures on Computation’, (Addison Wesley Longman, Reading MA 1996).

[15] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. 21 (1982) 219. [16] E. Fredkin, unpublished lecture given at Southampton in September 1997.-Wesley, Reading MA, 2nd edition (1992).

[16] E. Fredkin, unpublished lecture given at Southampton in September 1997.-Wesley, Reading MA, 2nd edition (1992).

[17] R.P. Feynman, ‘There’s Plenty of Room at the Bottom’, reprinted in ‘Feynman and Computation’, ibid.; originally published in February 1960 issue of Caltech’s Engineering and Science.

[18] R. Jozsa, “Entanglement and Quantum Computation,” in Geometric Issues in the Foundations of Science, S. Huggett, L. Mason, K. Tod, S. Tsou, and N. Woodhouse, Eds. Oxford University Press, July 1997.

[19] W. Tichy, “Is quantum computing for real?: An interview with catherine mcgeoch of d-wave systems,” Ubiquity, vol. 2017, no. July, pp. 2:1–2:20, Jul. 2017. [Online]. Available: http://doi.acm.org/10.1145/3084688

[20] J. Muhonen and T. Dehollain, “Storing Quantum Information For 30 Seconds In a Nanoelectronic Device,” Nature Nanotechnology, vol. 9, pp. 986–991, 2014. [10] D-Wave, “Quantum Computing: How D-Wave Systems Work,” http: //www.dwavesys.com/our-company/meet-d-wave