Prospectus

The Benefits of Quantum Computing and its Potential Threats

Jacqueline Lainhart

University of Virginia, School of Engineering and Applied Science

STS 4500: STS and Engineering Practice

Dr. Richard Jacques

November 21, 2023

On my honor, as a student, I have neither given

nor received unauthorized aid on this assignment.

Introduction

With the ever-changing landscape of technology and computing, the desire for efficiency grows stronger. Therefore, computational scientists are looking towards quantum computing as the solution to increase efficiency due to their advantages over classical computers for solving problems faster. While quantum computing is still in development and being researched upon, the field is rapidly developing. However, the existence of quantum computers poses a threat to cybersecurity, including the potential to break numerous forms of encryption like RSA, ECC, and Diffie-Hellman (Abuarqou, 2020). This could not only impact the individual storing their personal data on their computer, but organizations storing sensitive data about the masses and energy structures that use computers. Preventive measures for a post-quantum world must be explored to minimize the harm that quantum computing could potentially cause.

Technical Discussion

Classical computing is binary in nature. It can only be in one state at a time and is sufficient in solving numerous kinds of problems. However, it falls short on handling substantial amounts of data. With quantum computing, it computes with qubits which means it can exist in a multi-state, not just a binary one. This means that instead of searching a singular branch of an algorithm one at a time until the optimal solution is found, “eliminating” branches probabilistically, quantum computing can go on these branches at the same time, finding the optimal solution quicker (Wallden & Kashefi, 2019). Binary bits can be imaged as two axes on a plane while a qubit is like a 3D sphere (Deshpande 2022).

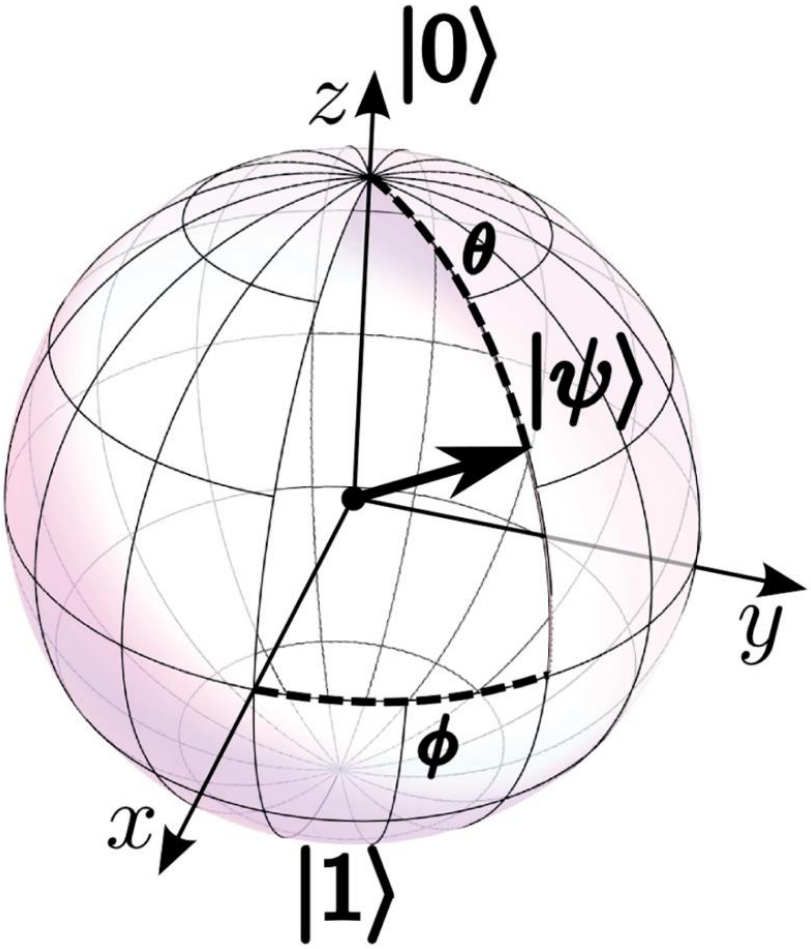

Figure 1: Diagram of a qubit (Adapted from Brieler et al., 2018)

While with classical computing a bit can either be 0 or 1, quantum computing can be of any value on its sphere, “The qubit can also simultaneously take intermediate positions between 0 and 1. As a result, for n qubits, the same operation can be performed on all the possible combinations of 0 and 1 for all the qubits — that is, 2^n combinations are possible” (Deshpande 2022). It falls in line with the concept of quantum mechanics. The 0 or 1 comes from the transistors managing electrical current on a computer. The electrical current on would be 1 and off would be 0. Brieler et al. (2018) describes how this differs in quantum computing, “It operates by directing large clouds of carriers of electrical current using engineered materials and

quantum-based principles (band structure, localized states, etc.). They produce behavior unusual for naturally found materials – an ability to precisely control current with current, or current via light, or light via current." To have these qubits able to exist, they need to have extremely low temperatures and pure enough material for quantum behavior to occur (Brieler et al., 2018). This allows for an exponential speed of solving problems in comparison to classical computing that solves problems linearly (Bozzo-Rey et al., 2019). This type of problem solving can then be transferred to numerous fields such as cybersecurity to make computing faster and more efficient.

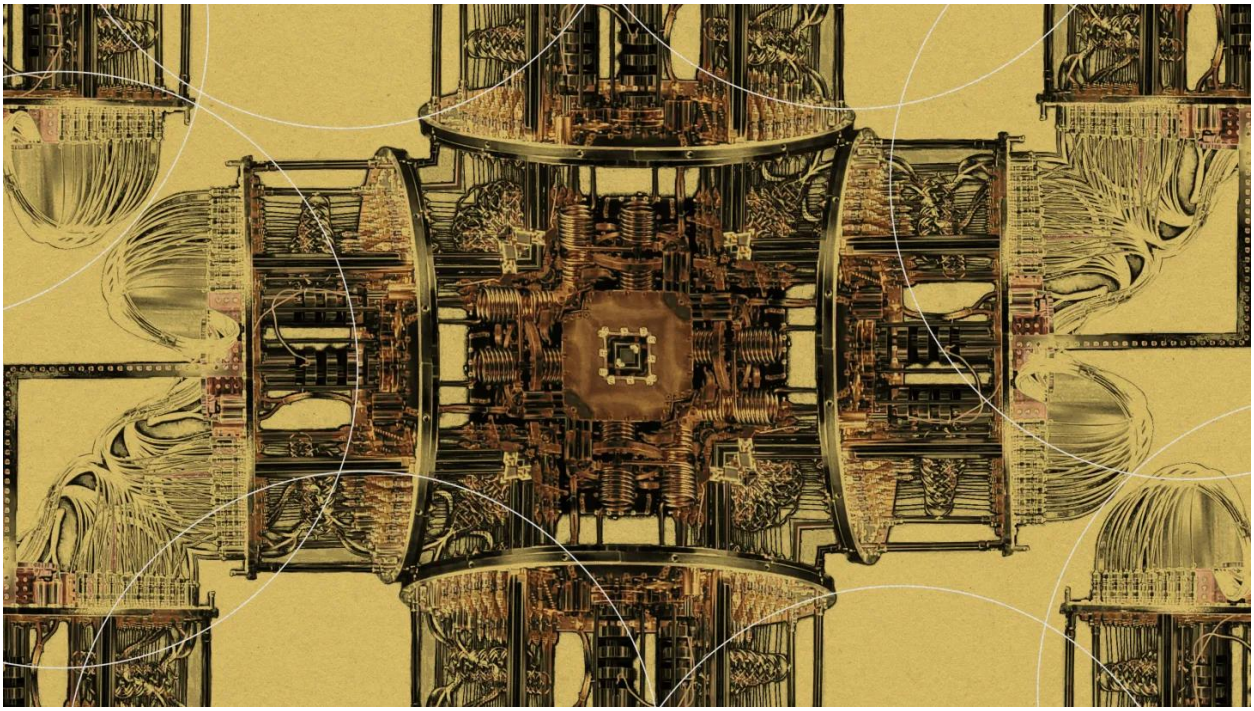

Figure 2: IBM's 433-qubit quantum processor, currently the highest qubit quantum computer (Accessed by Brooks, 2023)

There are quantum computers that exist; the highest qubit quantum computer is IBM's with 433 qubits. They have plans on making a 100,000-qubit processor within 10 years (Brooks, 2023). However, making a quantum computer with higher qubits has its difficulties since the

larger the qubits the more hardware issues are to occur, and there are more qubits to be kept stable (Deshpande 2022). Theoretically, quantum computing can solve problems that were not possible with traditional computing. However, with this ability to manage large data, quantum computing poses threats such as having the ability to decrypt most any encryption algorithms. Cryptography is the study of hiding information. Encryption is within cryptography, and it makes words secret by converting them into a code that cannot be understood by humans (Radanliev, 2023). To decrypt something would be to take that secret coded message and turn it back into plain text. Cryptographic algorithms are used for security to hide information. There are numerous kinds such as Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (3DEA), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), etc. Different ones apply to different situations such as internet communication or communication between two parties (Radanliev, 2023). These algorithms are extremely popular and used by many. People seldom get the opportunity to comment on how their data and communications are encrypted. There are quantum algorithms that exist that can break these encryption algorithms. One of the most notable ones is by a mathematician named Peter Shor called Shor's algorithm which was created in 1994 (Radanliev, 2023). It has the potential to break RSA and ECC encryption algorithms if used on quantum computers. The current hardware limitations prevent this from happening as a much larger quantum computer will be required to run this algorithm than the ones that currently exist. It is said that a quantum computer with one million qubits is needed to break the RSA algorithm (Castelvecchi, 2023). Eventually, this could become a reality.

The NIST and NSA are currently considering potential solutions to the concerns and risks that quantum computers will bring (Abuarqou, 2020). These concerns can be addressed through regulations and post-quantum cryptographic algorithms. If we understand what the threats of

quantum computing are, we can be proactive in addressing these threats. Developing regulations has its own complicated process in which there are many people involved, from lawmakers to the engineers who develop the technology. It is even more complicated considering that developing technology to support quantum computing is new and emerging. The time frame in which regulations and post-quantum cryptographic algorithms can be developed cannot be pinpointed.

STS Discussion

Both governments and private investors are interested in developing quantum computing and are financially involved in it. Therefore, governments and private investors are the ones who are currently in charge of the direction it goes. This also includes implementing safety measures. Kashefi & Wallden (2019) describe what would need to be adjusted in a post-quantum world, "All security concepts, such as authentication, encryption but also more involved concepts as computation on encrypted data and secure multiparty computation, would need to be modified to apply to quantum information and quantum computation." They continue to state how there cannot exist a "blind quantum computation" in which the input/output of a user is unknown to the quantum computer. Therefore, there needs to exist controlled data leakage or the creation of protocols (ways in which a quantum computer is used). There are currently some protocols for a post-quantum world such as the one created by Mahadev that includes, "a mechanism to use a classical ciphertext to apply a (generic) quantum gate conditional on the corresponding plaintext, without ever decrypting and without leaking any information" (Kashefi & Wallden, 2019). Regardless of what is implemented, it is important that regulations are put in place that benefit more than just the stakeholders involved. If monetary gain is prioritized over the betterment of society, the potential harms of quantum computing could have a stronger impact than what proactive regulation could have prevented.

Cyberwarfare is already rampant in modern day society. Many people think the most harm that can be done is their passwords getting leaked. This is a major issue as it opens the potential for identity theft, but there are more dangers that occur from cyberwarfare than people realize. One example is how the Idaho National Laboratories conducted a demonstration, Aurora, where they were able to cause electrical grid failures using cyber-attacks (Duggan & Parks, 2011). Something like the outage of electrical grids can cause widespread deaths including those in hospitals where electricity is needed for medical procedures and patient care. If quantum computing can assist in these kinds of cyber-attacks to make it easier to break into systems, then cyberterrorism can become more dangerous to society. This is a critical concern that needs to be addressed.

The question I intend to answer is, is there a way to combat the potential threats of quantum computing while its research and development are actively occurring? This would involve imagining an existing "post-quantum" world. I plan to investigate who should be regulating this research and developing regulations. I also plan to research what the potential regulations and post-quantum resistant cryptosystems might look like. Although quantum computing has its benefits, it is crucial to consider its application preventatives due to how powerful its potential is in decryption. This can mean everyone's data, from governments to individuals, could be broken into and accessed. Unquestionably, there is a clear and present threat to national security and personal privacy. When cyber wars occur in a post-quantum world, they can have the potential to bring down countries and their economies. The scope of this research is theoretical and will involve a considerable number of conceptual proposals given that we are looking for a solution to a problem that does not currently exist but can exist in the future.

In terms of my Capstone project, this topic relates strongly to it. In my Capstone report, I will be discussing the topic of artificial intelligence to improve cybersecurity and a way to improve artificial intelligence with quantum computing. Both consider cybersecurity and the potential influence of quantum computing. Therefore, I believe I will be conducting similar research for both and identify an overlap.

Conclusion

Engineers and people who work in the tech industry need to not only be the creators of change but also anticipate its effects. It is about finding the balance between encouraging growth in this field while being aware of the negative aspects of quantum computing. Do the benefits outweigh the risks? Many people look at the benefits of emerging technologies and do not want to bring themselves down with the harm that it could cause. If it has the potential to bring down economies and cause mass murder, then as much effort needs to be put into combatting quantum computing as there is in developing it.

References

ABUARQOU, A. (2020). Security Challenges Posed by Quantum Computing on Emerging Technologies. In: Paper presented at the Proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS). https://doi-org.proxy1.library.virginia.edu/10.1145/3440749.3442651

BOZZO-REY, M., LONGBOTTOM, J., & MÜLLER H. A. (2019). Quantum computing: challenges and opportunities. *In Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering (CASCON '19)*. IBM Corp., USA, 393–394. https://dl-acm-org.proxy1.library.virginia.edu/doi/10.5555/3370272.3370336

BRIELER, J., SCHERRER, J. F., & SOLENOV, D. (2018). The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine. *Missouri medicine*, *115*(5), 463–467.

CASTELVECCHI, D. (2023). *Are Quantum Computers about to Break Online Privacy?* Scientific American. https://www.scientificamerican.com/article/are-quantum-computers-about-to-break-online-privacy/#:~:text=But%20implementing%20Shor's%20technique%20would,more%20qubits%20to%20crack%20RSA.

DESHPANDE, A. (2022). Assessing the Quantum-Computing Landscape. *Communications of the ACM*, *65*(10), 57–65. https://doi.org/10.1145/3524109

DUGGAN, D. P., PARKS, R. C. (2011) Principles of Cyberwarfare. *IEEE Security & Privacy*, vol. 9, no. 5, pp. 30-35. doi: 10.1109/MSP.2011.138.

KASHEFI, E., WALLDEN, P. (2019). Cyber Security in the Quantum Era. *Communications of the ACM*, *62*(4), 120. https://doi.org/10.1145/3241037

RADANLIEV, P. (2023). Cyber-attacks on Public Key Cryptography. Preprints. https://doi.org/10.20944/preprints202309.1769.v1