CSE 4471 Report

Jeremy Sawyer, Nate Crowder and Matt Russotti
Department of Computer Science and Engineering
The Ohio State University
Columbus, OH 43210
{sawyer.201, crowder.81 , russotti.1}@osu.edu

Abstract

Our research aimed to discover potential applications of quantum computing to cybersecurity, as well as highlight general information about quantum computing. We found there to be many potential applications both good and bad, but most are solely theoretical until technology advances. Algorithms such as Shor's algorithm, which is theoretically able to break RSA 2048 encryption, present future opportunities for bad actors to utilize quantum computing and necessitate further development of quantum computing technology on the defense side. Quantum computing is an exciting technology with a lot of potential that the industry clearly notices but has failed to materialize in something groundbreaking thus far. It is prone to errors that seem to get worse with scale, which has impeded progress and presented challenges for researchers. Despite these issues, researchers have been making strides and are creating quantum systems at larger scales as time goes on. Due to the increasing power of quantum and its potential to render popular encryption schemes useless, it is imperative that governments and well-meaning corporations gain a solid understanding of this technology to prepare for the potential new era of cyber-attacks involving quantum computing.

1. Introduction

Quantum computing is an up-and-coming technology with seemingly limitless potential, with many nations and organizations across the world pouring time and money into research for it. Quantum mechanics are complex and hard to understand which has led to a very long development process before quantum computing has been able to solve problems in the real world. However, we are approaching a time where quantum computing systems are closer to becoming a practical reality and we need to prepare ourselves to maximally utilize quantum computing and protect against any threats that it may pose. We created this project to explore the implications of quantum computing on cybersecurity. Quantum computing is a type of technology with the potential to shatter the current paradigm in the computing world, but it has not come to fruition yet. This presents the perfect opportunity to get out ahead of attackers and make a plan that allows us to create quantum systems with security in mind and get an idea of the potential technical capabilities of quantum computing. With these new technological capabilities come more things that can be broken into, more things that need to be secured, and more methods that attackers can use to access private data. We aim to discover some of the specific threats that quantum computing poses to the world of cybersecurity as well as figure out what we can do to protect against these threats.

The most notable threat we found that cybersecurity poses is its ability to break popular encryption schemes such as RSA 2048-bit encryption [1]. This is an example of a technical problem that quantum computing can solve, and traditional computing can't. This kind of groundbreaking advancement is a big part of what motivates us to research quantum computing and its implications on cybersecurity. its simplest, quantum computing can be defined as computing utilizing quantum mechanics. There are key differences between traditional and quantum computing that give quantum computing an advantage in certain scenarios. Traditional computing relies on binary bits which can either be a 1, or a 0. For example, if we had 4 bits we could store up to 2^4, or 16 values. Quantum computing takes this principle a step further, with qubits that can simultaneously be 0 and 1, referred to as superposition. [1]. This means that if we had 4 qubits, we could store 2^4 variables, which allows for much greater data representation with the same number of bits and qubits. Another identifying feature of quantum computing is its utilization of entanglement. This means that qubits in completely different locations can have an effect on each other. [2] This has great implications for computing, potentially allowing us to immediately transmit information across long distances with no physical means of connection. It is the basic principle behind many current quantum projects, such as the 2019 National Quantum Initiative created by the United States government [2].

2. Background

There are many reasons that we decided to research quantum computing and its relation to cybersecurity. The first reason was simply how unfamiliar we were with the topic. Quantum computing is abundant with complexity and mystique, so we sought out to elucidate this topic for both us and the readers, as well as get an insight into how it can be used for good and bad. We have all heard of quantum mechanics, quantum computing, and other related topics, but most people have very little understanding beyond the surface level. Thus, this was our opportunity to learn about

it and see the tangible benefits and threats that it presents.

Another reason we decided to research this topic was because of its potential impact on the world. Quantum computing represents an entirely new paradigm in technology and has the potential to change everything about how we use technology. It has the potential to render useless the most trusted and reliable encryption algorithms and could potentially allow for instantaneous long-distance data transmission utilizing quantum entanglement [3]. Even these very impactful features barely scratch the surface of its potential which led us to really want to dive into quantum computing, leading us to choose it as our topic.

The final reason we decided to research this topic was to get an idea of how it can be used for malicious purposes. Given that this research was conducted for a cybersecurity class, it is only natural to understand the implications of this technology on cybersecurity and how it will be used by attackers. We must develop a great understanding of quantum technology to successfully defend against quantum-based attacks and to create secure and robust quantum systems. It is inevitable that groups will attempt to attack quantum systems in any way possible. Because of this, it would be foolish to implement any practical quantum system without first understanding what potential vulnerabilities it may have, especially since we have no history to work from.

3. Research and Findings

Our research revolved around how a quantum computer works and some of the challenges quantum computing faces.

The first and most important part of quantum computing is identifying which kinds of problems would benefit from using a quantum computer rather than a classical one. First, we must define time complexity. Problems that can be solved in polynomial time are known as P, problems that can be solved in exponential time but the answer can be checked to see if its correct in polynomial time are known as NP. The existence of NP problems is crucial as many internet security features, like encryption, rely on this to create problems that would take too long to solve on a classical computer. In short, P problems are easy to solve on a classical computer, NP problems are hard to solve on a classical computer [4]. BQP problems are the class of problems that are solvable in polynomial time on a quantum computer (basically P for classical computers) however, due to the probabilistic nature of quantum computers they must be able to solve these problems correctly at least two-thirds of the time [5]. Running that program multiple times will produce the correct answer with high confidence. While the exact relationship between BQP and P/NP is unknown there are problems, like integer factorization that are not in P but are in BQP, like integer factorization. In summary, quantum computers can solve some problems easily that classical computers cannot solve efficiently.

Two examples of this that we found were Grover's and Shor's algorithms. Grover's algorithm offers a quadradic time speedup when searching an unstructured list. The algorithm starts by putting all N elements in the list in a state of superposition, next, we apply an oracle function (black box function) to apply a phase shift to the item in the list we are looking for called X, and then we apply Grover's diffusion operator to amplify the amplitude of X which increases the probability it is the state returned when we have to observe and collapse the quantum state. Those last two steps should be repeated $\sqrt{N}$ times to ensure correctness [6]. Shor's algorithm offers an exponential speedup when factoring large non-prime integers. The first step to factoring a large number N is to randomly choose a number a such that $1 < a < N$, next we calculate the greatest common divisor of a and N using the Euclidean algorithm, next we do the quantum part called period finding which finds the period r which is the smallest positive integer such that $a^r \equiv 1 \bmod N$ which can be found efficiently using the Quantum Fourier Transform, once r is determined a series of classical steps can be performed to find the prime factors of N [7].

Part of our research included the general steps behind how a quantum computer works. The first part of any quantum program is to select a problem that could benefit from a quantum speedup, we already covered this extensively earlier in this section. The next step once you pick a problem that benefits from a quantum speedup is to choose the appropriate algorithm to address you problem, we covered two examples of this but there are many more algorithms such as Simon's Algorithm, the Deutsch-Joza Algorithm, and the quantum phase estimation algorithm. Each of those applies a quantum speedup to one kind of problem. Next, we must initialize a register of qubits to a superposition of all possible inputs, once the register is loaded we can put those qubits into superposition by applying the Hadamard gate [9]. Then we move to step four which is applying relevant quantum gates to manipulate the state of the qubits in parallel. An example of this is applying the oracle in Grover's algorithm. Next, we do amplitude amplification, in the context of Grover's algorithm which is the Grover diffusion operator which is a Hadamard transform, an X gate, a multi-controlled Z gate, another X gate, and another Hadamard gate to top it off [6]. Next, we measure the state that causes the collapse of the superposition and the output of one of the possible states. Due to the probabilistic nature of quantum computers, this answer must be checked to see if it is the answer we wanted [9].

The final part of our research was learning about where the current state of quantum computing is at. A common comparison is that quantum computers are today where classical computers were during the 1950s [9]. While

it is unlikely quantum computers will scale down and be in every device as classical computers did, we are reaching the point where quantum computers are advanced enough to actually be useful. The largest quantum computer released to date is IBM's Osprey QC which has 433 qubits that can perform more calculations than there are atoms in the universe [10]. However, we will need millions of qubits to do impactful things like break encryption [11].

5. Impact

Being so early in the development of quantum computing technology it is easy to speculate what some potential impacts may be. Whether or not these actually happen remains to be seen. The easiest example of a use case is simulating quantum systems. That would enable us to discover all kinds of drugs to cure diseases, improve quality of life, and increase life expectancy [12]. Advancements in material science will allow us to develop better, cheaper, and more sustainable materials. This is especially important as climate change and sustainability are at the forefront of some of the issues today. Another important development would be improved batteries. That addresses the issue of finding an efficient way to store electricity and would overall lead to less harmful waste from current disposable batteries made from rare earth metals that are gathered in unethical manners. Another example of the benefits of developing quantum computers is optimization problems. This could mean anything from "reducing materials waste on a production line, scheduling delivery fleets more efficiently, and minimizing risk while maximizing gains across a financial portfolio" [13]. Improving the efficiency of our societal systems allows for the better utilization of finite resources which is generally considered a good thing. Better financial models can help hedge against unforeseen market forces and reduce the impact of recessions on our economy.

Those are some of the positive impacts of quantum computing. Unfortunately, it's not all sunshine and rainbows. The most talked about issue coming from the development of quantum computers is the threat to internet security. To fully understand this threat we must understand what encryption is, why its important, and how it is at risk. Encryption, put simply, is the process of converting information or data into a code to prevent unauthorized access [14]. The importance of encryption is pretty obvious, not all information on the internet should be accessed by everyone. If this were the situation, online shopping would become untenable, anyone could access the passwords safeguarding your accounts, and the concept of privacy would essentially vanish. In an age where we rely on the Internet for so many things, not having Internet privacy isn't feasible and is something to be concerned about. In the late 90's a mathematician named Peter Shor developed an algorithm that can theoretically break public key encryption which is the basis for internet communication, e-commerce, and encryption protocols like SSL, TLS, and HTTPS [15]. The process of how this is done was talked about earlier during our research.

While these seem significant it is important to remember that the biggest impacts are often the ones that no one can predict. When the internet took off no one thought social media would be so popular. It is impossible to predict the future so all we can do is act on what we know. That means investing in developing quantum computing for all its benefits as well as the protection we need to live in a post-quantum world. Like quantum-proof encryption, which is being researched by the NIST and will hopefully be adopted soon [16].

5. Conclusion

Our research into the implications of quantum computing on cybersecurity has shed light onto the seemingly endless potential of this emerging technology. The complicated world of quantum physics is now able to be harnessed, and it will no doubt revolutionize computing as we know it.

The immense potential of quantum computing ranges from drug discovery to sustainability. It also poses a significant threat to internet security due to its ability to break modern encryption methods. While we can try our best to anticipate some impacts, many remain very much unpredictable. It is crucial to invest in quantum computing development while preparing for post-quantum security, including research into quantum-proof encryption. In this evolving landscape, we must balance the technology's benefits with security concerns. While the potential is incredible, the actual technology isn't quite there yet. Recent research has shown that RSA 2048 encryption could be broken in just 8 hours with the use of 20 million qubits [11]. Yet as of 2022, researchers have only been able to manage 433 qubits in a physical device. By 2023, that number will increase to 1,121 [17]. This clearly demonstrates that while progress is being made, we are still quite far off, and much more research and time will be needed.

There is still so much research to do for quantum applications within cybersecurity. As the industry currently stands, most research is spent asking the questions as opposed to answering them. From our research, we have seen that one of the biggest obstacles is most simply time. Quantum computing is such a relatively young field that already has a lot of funding and research that is going into it. Different private companies like Google and IBM are working in the field, not to mention leading government agencies. Again, the effort is there – patience is needed. With quantum computing, the landscape of cybersecurity is poised for a transformation. As we prepare for this technological paradigm shift, it is important that we anticipate and do our best to mitigate these associated threats. Quantum computing represents not only an opportunity to improve our defenses against cyber threats but also as a jumping off point for redefining the boundaries of computing itself. The combination of quantum mechanics and cybersecurity is an

intersection of top-of-the-line innovation and security, where the fusion of these fields will play a pivotal role in shaping our digital future. The research that has been done marks the beginning of this journey, and it is important that we continue to explore, adapt, and evolve in the face of this quantum computing revolution.

REFERENCES

[1] J. Chu, "The beginning of the end for encryption schemes?," MIT News | Massachusetts Institute of Technology, https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303 (accessed Oct. 12, 2023).

[2] W. Clavin, "Proving that quantum entanglement is real," California Institute of Technology, https://www.caltech.edu/about/news/proving-that-quantum-entanglement-is real#:~:text=Experiments%20have%20since%20proven%20that,also%20at%20very%20great%20distances. (accessed Oct. 12, 2023).

[3] D. Llewellyn et al., "Chip-to-chip quantum teleportation and multi-photon entanglement in Silicon," Nature News, https://www.nature.com/articles/s41567-019-0727-x (accessed Oct. 13, 2023).

[4] A. Gunzi, "P, NP, PSPACE and BQP," Arnaldo Gunzi Quantum, Nov. 06, 2020. https://medium.com/arnaldo-gunzi-quantum/p-np-pspace-and-bqp-44d42a842c6a (accessed Oct. 12, 2023).

[5] S. Aaronson, "BQP and the Polynomial Hierarchy.". Available: https://www.scottaaronson.com/papers/bqpph.pdf (accessed Oct. 13, 2023).

[6] "Introduction to Grover's Algorithm," GeeksforGeeks, May 15, 2023. https://www.geeksforgeeks.org/introduction-to-grovers-algorithm/ (accessed Oct. 12, 2023).

[7] "Shor's Factorization Algorithm," GeeksforGeeks, Jan. 24, 2021. https://www.geeksforgeeks.org/shors-factorization-algorithm/ (accessed Oct. 12, 2023).

[8] A. Jain, "6 Quantum Algorithms That Will Change Computing Forever," Analytics India Magazine, Feb. 17, 2023. https://analyticsindiamag.com/6-quantum-algorithms-that-will-change-computing-forever/ (accessed Oct. 13, 2023).

[9] J. D. Hidary, QUANTUM COMPUTING : an applied approach. S.L.: Springer Nature, 2019.

[10] "How Many Qubits Are Needed for Quantum Supremacy?," IEEE Spectrum, May 21, 2020. https://spectrum.ieee.org/qubit-supremacy (accessed Oct. 13, 2023).

[11] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for Quantum Computing." Available: https://arxiv.org/pdf/2110.14701.pdf (accessed Oct. 13, 2023).

[12] F. Bova, A. Goldfarb, and R. Melko, "Quantum Computing Is Coming. What Can It Do?," Harvard Business Review, Jul. 16, 2021. https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do (accessed Oct. 13, 2023).

[13] J. Tyrrell, "What are the benefits of quantum computing?," TechHQ, Nov. 15, 2022. https://techhq.com/2022/11/what-are-the-benefits-of-quantum-computing/ (accessed Oct. 13, 2023).

[14] "What is encryption? How it works + types of encryption – Norton," us-stage.norton.com. https://us-stage.norton.com/blog/privacy/what-is-encryption (accessed Oct. 13, 2023).

[15] Golden, Deborah "Preparing the trusted internet for the age of quantum computing," Deloitte Insights. https://www2.deloitte.com/us/en/insights/topics/cyber-risk/crypto-agility-quantum-computing-security....html (accessed Oct. 13, 2023).

[16] NIST, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," NIST, Jul. 2022, Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed Oct. 13, 2023).

[17] J. Gambetta, "IBM's roadmap for Scaling Quantum Technology," IBM Research Blog, https://research.ibm.com/blog/ibm-quantum-roadmap (accessed Oct. 13, 2023).