Importance of Quantum Computing in the field of CyberSecurity

Shripad Ambure (942364)
Vickysingh Baghel (964952)

Abstract

As the Quantum computing competition developers, enterprises, institutions, and research organizations could become targets of nation-state actors, cybercriminals, and hacktivists for damage, surveillance, and financial gain. Quantum applications have spread into traditional commercial information systems and services, prompting companies to consider how to defend their networks, software, hardware, and data from digital attacks. This study examines the current state of quantum computing technology as well as the Quantum computing's existing state of the art, and its prospective applications in computer science and cybersecurity.The goal of this research is to not only raise awareness about this cutting-edge technology, but also to act as a comprehensive reference guide for anybody interested in exploring alternative quantum computing applications in fields such as finance, biochemistry, and data science.We next go over threat vectors for quantum computing environments, as well as the appropriate defensive mechanisms.Following that, we make advice on how to limit the cyberattack surface proactively by using threat intelligence and assuring the security of quantum hardware and software components by engineering.Here in this study, we look at a study area that sits at the crossroads of cyber security and quantum technology.

Keywords

CyberSecurity,quantum computing,security,cryptography threat

[1] *Department of Computer Science, Universita degli studi di Milano, Milan, Italy*
[2] *Department of Data Science and Economics, Universita degli studi di Milano, Milan,Italy*

Contents

Introduction

Quantum computing combines quantum physics, computer science, and information theory in a beautiful way. The goal of this research is to make an intriguing scientific topic accessible to a wide range of people. Quantum computing, which includes networking, quantum sensing, and quantum simulation, is an area of quantum information science that makes use of the capacity to produce and utilize quantum bits and qubits. Quantum computers have the ability to tackle certain problems significantly faster than traditional or other classical computers. They use quantum physics principles to conduct numerous tasks at the same time in a manner that is fundamentally different from traditional computers. While quantum computers are unlikely to completely replace traditional computers, there are two essential aspects of qubits that radically alter how quantum computers store and manage data when compared to traditional computers. Quantum computing is a computational paradigm that takes advantage of many quantum phenomena discovered via the study of quantum physics. These processes enable the emergence of a new kind of information unit known as a quantum bit, or ”qubit” for short. A qubit, unlike a traditional bit, takes advantage of three basic principles: superposition, interference, and entanglement. These three principles give the described qubit the feature of spin, which allows it to exist in a superposition of states rather than the binary on/off state that classical systems have. To put it another way, a quantum system can execute logic operations if a classical system can do n operations. This skill may be used to a variety of fields, including scientific computing and cybersecurity.

1. Understading Quantum Computing

These supercomputers are based on the quantum physics concepts of superposition and entanglement. This enables quantum computers to perform tasks at rates that are orders of magnitude faster than traditional computers while using much less energy.

In the 1980s, the area of quantum computing was born. It was later observed that quantum algorithms were more efficient than their conventional equivalents in solving certain computer problems.

Finance, military affairs and intelligence, drug design and research, aircraft design, utilities (nuclear fusion), polymer design, machine learning and artificial intelligence (AI) and Big Data search, and digital manufacturing might all benefit from quantum computing.

IBM, Microsoft, Google, D-Waves Systems, Alibaba, Nokia, Intel, Airbus, HP, Toshiba, Mitsubishi, SK Telecom, NEC, Raytheon, Lockheed Martin, Rigetti, Biogen, Volkswagen, and Amgen have all shown interest in working in the area of quantum computing due to its potential and expected market size.

1.1 Quantum Computer vs. Classical Computer

Quantum computers process data in a unique way. Transistors, which are either 1 or 0, are used in traditional computers. Qubits, which may be 1 or 0 at the same moment, are used in quantum computers. Quantum computing power grows exponentially as the number of qubits coupled together grows. Meanwhile, connecting additional transistors increases power in a linear fashion. Traditional PCs are ideal for common chores that require the use of a computer. Quantum computers, on the other hand, are ideal for doing simulations and data analytics, such as for medication or chemical studies. However, these computers must be kept very cold. They are also more costly and harder to construct. Adding memory to computers is a classic example of traditional computing advancement. Meanwhile, quantum computers aid in the solution of increasingly difficult issues. While quantum computers will not be able to run Microsoft Word quicker or better, they will be able to solve complicated issues faster. For example, Google's quantum computer, which is still under development, might aid in a variety of operations, such as accelerating machine-learning training or assisting in the construction of more energy-efficient batteries. Quantum computing may be used for a variety of purposes, including securely transferring data. Other approaches include combating cancer and other health issues, as well as producing new medications. Quantum computers may also aid in the development of radars and their capacity to identify missiles and planes. Other areas of interest include the environment and the use of quantum computing to keep water clean utilizing chemical sensors.

1.2 Computation Performance of Quantum computers

Let's start with the phases of a traditional calculation, such as estimating how much income tax an employee must pay each year. The first step is to choose the input, which in this example is an employee's yearly wage. The real calculation follows the second phase, in which we utilize the input and other relevant variables (constants) to determine how much tax the employee must pay. The output is presented to the user in the third and final stage.

Quantum calculations are fundamentally different from traditional computations, and they also contain various components. Rather of selecting a single beginning state, the first step in a quantum computation is to arrange the input as a superposition of all possible states. Isn't that strange? The following is an example of how this works: Consider preparing three qubits in a condition of equal superposition (50 percent zero and 50 percent one). We can figure out what this state represents by looking at what occurs when the qubits are measured. We see a random collection of zeros and ones every time we measure this state, with an equal chance of getting one of the eight potential classical states. This implies that the qubits are in all conceivable classical states at the same time as long as this superposition state is not measured.

This is a highly important trait in terms of computing since it allows us to compute on several states at the same time. Quantum parallelism is the name for this process.

The input is processed using a set of logical gates in the second stage of a quantum computation. Quantum computers contain more complicated gates that can produce and handle superposition states in addition to the typical logical gates like OR, AND, XOR, and so on. Measurement of the state of the qubits has an impact on their value in addition to gate operations. In reality, measurements of qubits are a critical component of the computing process. This leads to the fascinating conclusion that quantum computing, or the process of conducting operations, must be a black box. Because a measurement involves an action on the data itself[7], we're not permitted to measure the status of the qubits during execution unless it's part of the script.

The output is always produced by a final measurement of the qubits in the third phase of a quantum computation. The state of the qubits before the measurement may (but does not have to be) a superposition state. If the state isn't superposition, the measurement will always provide the same result. In this situation, the calculation's ultimate result is produced by the measurement. If the final state, on the other hand, is a superposition, the final measurement will provide different results at each measurement. In this instance, the operation must be done many times in order to discover which outcomes have the greatest likelihood. The calculation's right result is then the output with the greatest probability. The fact that the same calculation may produce various results is perhaps the most perplexing element of quantum calculations.

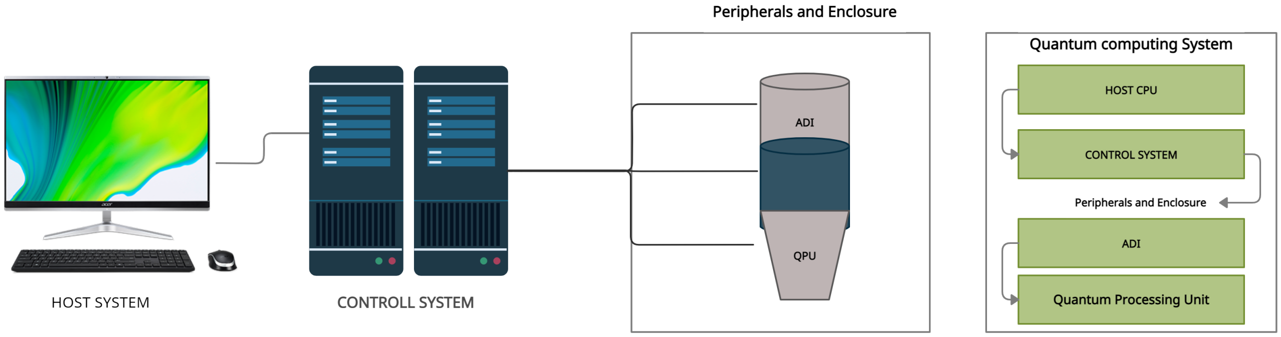

Figure 1. A Quantum Computing Architecture

1.3 Applications of Quantum Computing

Applications of Quantum Computing Quantum computers have a vast and diverse theoretical potential. The computational benefits of addressing problems in a fundamentally different method than traditional computers might assist a wide range of professions. The above-mentioned essential features of qubits make quantum computers highly adept at general optimization problems and issues involving complicated molecules. The following is a list of examples of how quantum computers might be used to solve current concerns and challenges:

- Improve electric car batteries by using molecular modeling.
- Compare and analyze substances that may lead to the creation of new medications.
- Improve a city's traffic flow.
- Improve generative models for creating datasets so that better machine learning algorithms may be trained.
- Decrypt data that has been encrypted using public-key cryptography

While these many uses will undoubtedly be crucial to economic development and long-term global competitiveness, breaking existing public-key encryption with a quantum computer remains one of the most difficult challenges[9].Furthermore, as both adversaries and defenders acquire quantum computing capabilities and update their infrastructure and methods to accommodate for the changes, there are likely to be a range of new changes, dangers, and possibilities in applied cybersecurity. Now we'll look at these effects and see if there are any methods to enhance things.

1.4 Impacts of Quantum Computing on Cybersecurity

Current Encryption: Today, there are two main methods of digital encryption:

- **Symmetric encryption:** To encrypt and decode data, the sender and receiver use the same digital keys. Current symmetric cryptography techniques are thought to be reasonably robust against assaults using quantum computers.
- **Asymmetric (public-key) encryption:** A public key encrypts communications for recipients who have a private key to decrypt them. Algorithmic trapdoor functions are used in public-key cryptography techniques like RSA and elliptical curve cryptography to construct keys that are reasonably cheap to calculate in one direction but very difficult to reverse-engineer using a traditional computer.

Shor's Algorithm: Quantum computing will improve the speed with which present public-key encryption systems may be decrypted. Current public-key encryption depends on the fact that a traditional computer can efficiently multiply big prime numbers but cannot reverse the operation without hundreds of years of computation. Peter Shor proposed in 1994 that a huge, fault-tolerant quantum computer might detect prime factors of integers in a fraction of the time it took to find them. Many of today's conventional encryption standards would be rendered outdated as a result.

This capacity, however, is still out of reach. The biggest functional quantum computers vary from 50-60 qubits without error correction, while cryptographically important quantum computers are anticipated to be on the magnitude of 1,000-10,000 error-corrected quantum bits (which need roughly 1,000 physical qubits per error-corrected qubit). The creation of a quantum computer capable of breaching RSA 2048 or equivalent public-key encryption is believed to be more than a decade away, according to the Belfer Center for Science and International Affairs — Harvard Kennedy School.

Grover's algorithm: searches a list that isn't sorted. This is a general approach that may be used to solve a wide range of computational issues. The disadvantage of this approach is that the speedup it provides is less than that of, say, Shor's algorithm. The outcomes of this approach aren't likely to be as stunning as those of other algorithms, but they're nonetheless useful in certain cases[1].

Quantum Approximate Optimization Algorithm (QAOA): is a quantum approximate optimization algorithm. Under specified circumstances, a generic approach for solving optimization issues. Many issues in banking, manufacturing, and transportation may be phrased as optimization problems, demonstrating the algorithm's potential influence.

Harrow Hassidim Lloyd (HHL) algorithm is as follows: A linear system of equations is solved using this approach. Because linear systems lie at the heart of many scientific and engineering issues, the HHL algorithm's potential speedup may have a significant influence.

The performance of a quantum algorithm in comparison to conventional algorithms is an essential factor in its success. Certain computational problems have been demonstrated to be intractable with traditional computers from a theoretical standpoint (or at least infeasible within a reasonable time). It would be a huge accomplishment to create a quantum algorithm that solves such a problem. On a more practical level, if a quantum algorithm outperforms a conventional algorithm, it is already a huge success.
This sparks a healthy rivalry between classical and quantum algorithm creators. Recent implementations of **QAOA and HHL** that looked to surpass the best-known classical algorithms are interesting instances of this rivalry. This achievement was short-lived, since other classical algorithms were created shortly after that performed even better. The bottom line is that work in this subject is having a favorable impact on the discipline as a whole, even before the first demonstration of a quantum computer.

2. Threats and Counter Measures

Given the significant risk that a massive, failure quantum computer presents to cybersecurity, it is critical that we assess the entire spectrum of consequences today in order to minimize possible damages. Quantum computers may be used in cybersecurity in four different ways.

1. Information intercepted in the past, if correctly captured and maintained, may be deciphered by quantum computers in the future. This is an unavoidable danger that exists today: state actors or criminals may acquire encrypted data in the hopes of decrypting it later with future breakthroughs. There are just a few options for preventing data pre-capture. Migrating apps as fast as feasible to quantum-resistant encryption will assist to avoid this danger.
2. Systemic data insecurity will be a problem for organizations that do not analyze their risks and transition to quantum-resistant encryption in a timely manner. Because of the hyper connected nature of the digital environment, this danger is systemic. As connection grows more widespread, our systems' security becomes more important for crucial data, communications, and services[3]. Furthermore, increased interdependence increases the chance that occurrences in one area of the ecosystem will have an influence on enterprises on the other. To establish resistance to the rising danger of quantum computers[2], we must guarantee that the security of our systems spans end-to-end procedures, supply chains, and common infrastructure.
3. Companies that delay and then hurry to adopt quantum-resistant encryption will be subject to design and implementation problems throughout their IT systems, resulting in mistakes that may be exploited by hackers without quantum computers. Quantum vulnerabilities should be assessed in advance, and a strategy for switching to quantum-resistant encryption should be devised.
4. Without clear disclosure about our plans to address the cybersecurity threats of quantum computing, trust and confidence in the digital ecosystem will continue to erode, according to the BelferCenter for Science and International Affairs — Harvard Kennedy School 11. Public and commercial sector quantum preparedness programs, as well as clear government guidelines on the transition to quantum-resistant encryption, would assist to limit this risk.

2.0.1 Quantum Enabled Security: Safe Use of Quantum Computers

Quantum computers, as we've shown, will provide computing improvements in a wide range of tasks, from exponential to far more modest quadratic or even constant. When such devices become accessible, it is natural to want to put this additional computing capacity to work on jobs that also need privacy and security, in other words, we want security for quantumly enabled protocols. To use quantum information and quantum computing, all security principles, such as authentication and encryption, as well as more complicated concepts like computation on encrypted information and safe multiparty computation, would have to be adjusted. Of course, in order for this sort of issue to be relevant, we need quantum computer devices that are large enough to provide tangible computational benefits for daily applications. This is not the case today,[5] but we are approaching the period of actual quantum speed-ups as we approach the classical simulation limit (real quantum computers that are larger than those that can be simulated by classical supercomputers). It's possible that speed-ups will be used to solve critical daily issues in the not-too-distant future.

Quantum encryption, quantum authentication, quantum non-malleability, blind quantum computing, quantum completely homomorphic encryption, safe multiparty quantum computation, functional quantum encryption, and other protocols are all being developed at a fast pace (for example, see the review of Fitzsimons). There are several protocols that optimize for various figures of merit, such as minimizing quantum (or classical) communication, minimizing total quantum resources or the quantum resources of individual parties, and providing the best degree of security feasible (information theoretic vs. post-quantum computational).

The bulk of these protocols need quantum communication between parties, and quantum computing must be performed on the conveyed quantum information in most circumstances. This presents two issues: a theoretical one and a practical one. Quantum computing devices that are compatible with quantum communication devices are required to complete such activities. On the one hand, photonics is the greatest platform for quantum communication because quantum information stored in photons can be sent across large distances easily. Superconducting qubits, on the other hand, are one of the most promising technologies for quantum processing devices, one that is being adopted by large industrial players and is leading the ”bigger quantum computer” race.[2] The chosen kinds of qubits for communication and computation do not coincide, and it is unclear if they are compatible at this time. It’s unclear if superconducting quantum computers can be part of a ”networked architecture,” since they’re now created in a monolithic design and it’s unclear whether sending and receiving quantum states will ever be viable.

The practical concern is that the two quantum technological developments, namely quantum computing devices and a large quantum network, are independent, and we should be able to use ”local” quantum computation devices before putting in place the infrastructure required for a full quantum Internet network. Even if a single quantum computer is developed in a central university or commercial facility, we may want to utilize it to delegate calculations before putting in place a quantum network architecture. This is exactly the situation with some of today’s small-scale quantum computers (IBM, Rigetti); they provide their quantum computer as a cloud service to the general public through a traditional interface. As a result, we move to an issue that is both practical and theoretically interesting: Can we deliver quantum processing protocols that retain privacy and security guarantees using this conventional interface[2], that is, to clients with no quantum skills, and what would it cost? This is an issue that has gotten a lot of attention lately, and we anticipate it to get a lot more attention after the first big study we look at here.

Blind quantum computation refers to any protocols in which a client with no quantum computing device delegates a calculation to a server with a quantum computer while retaining the secrecy of her input and output. Quantum complexity theory provides significant evidence that information theoretic safe, classical-client, blind quantum computing protocols are not possible. 4 To get a completely classical client, certain assumptions need be weakened: either allow some (well-defined) information leakage or strive towards post-quantum computationally safe protocols.

Another method is to build a mechanism that mimics a quantum channel by having a classical client communicate with a quantum server15, with the result that the protocol is post-quantum computational safe. This capability may allow classical clients to utilize all of the protocols listed in this section, depending on the details of the simulated quantum channel.

Classical clients might employ verifiable blind quantum computing protocols as a result of this. Clients may verify the accuracy of the delegated blind quantum computing here, which is an important feature for commercial usage of the quantum cloud. Finally, whether or not it is employed in a cryptography situation, giving mechanisms for a classical agent to authenticate the authenticity of a general quantum computation is a matter of enormous significance, both theoretically and practically. Mahadev provided another way for achieving quantum computation verification in the post-quantum computational security context that does not need concealing the process.

A quantum channel is substituted by the capabilities of a delegated pseudo-secret random qubit generator in Cojocaruetal. In many protocols, the only quantum communication needed is communicating random (secret) qubits (for example, Broadbentetal and Fitzsimonsetal. The key to achieving this capability is to tell the server to create a state in which certain qubits are entangled and others are not. This is done in such a manner that the client (who has access to trap-door information) is aware of the link, but the server is unaware of it (that does not have access)[3]. The client takes use of this advantage and orders the server to create an output qubit in a random state, about which the client is familiar but the server is completely unaware. This is a perfect representation of a random single-qubit quantum channel. cryptography that is quantum-resistant

2.0.2 A Step Towards CyberSecurity Improvement in the Quantum Future

1. Continue to push the boundaries of quantum computing research

The National Quantum Initiative Act of 2018 allowed financing of 1.275 billion Dollar over the next five years. To construct the hardware, software, and algorithms that underpin quantum computers, both governmental and private sector research activities will need consistent, considerable financing. If quantum computing research does not become economically viable in the near future, the government’s involvement in subsidizing developments in the area will become even more important. For the knowledge and technology transfer required for pre-competitive quantum research and development, close cooperation between the public and commercial sectors will remain critical.

2. Maintain and expand international collaboration

A critical component of improving quantum computing, in addition to finance, is continuing engagement with other nations that are investing in quantum. The National Strategic Overview for Quantum Information Science emphasizes the significance of bilateral agreements for cooperative initiatives, as well as international finance, knowledge, and talent flows. The Tokyo Statement on Quantum Cooperation, the first bilateral diplomatic agreement on quantum information science cooperation, was signed by the United States and Japan in 2019. Continued involvement and openness with other countries in joint efforts to enhance quantum computing would benefit the United States’ investments in research and technical development. Although international norms and standards have received little attention, voices from the corporate sector and academics have started to advocate for a more holistic strategy to developing and deploying quantum technology that includes ethical concerns and standardized advice.

3.Space Industry Quantum technologies, such as quantum metrology and sensing, are expected to have a significant impact on space exploration and industry. Quantum key distribution (QKD) has also piqued attention as a means of securing quantum communications.

China has dedicated a large amount of research and development resources to space-based QKD as a main research topic. China deployed the Micius satellite in 2016, and entangled photons were successfully transferred between the satellite and various ground stations.

While QKD is unlikely to be widely used, it does have certain benefits for extremely long-range secure data transmission. Because of the features of superposition and entanglement, an outsider's observation will disturb the quantum state, allowing QKD to detect infiltration. It's vital to remember that QKD won't provide complete security for space communications since there are a variety of additional access channels that might cause problems. In any case, further research using space-based QKD will help us learn more about how to establish provably secure quantum networks.

3. The Future

Quantum computing opens up great prospects for research, healthcare, machine learning, and communications in the future, but protecting the security of our cyber environment is critical. With the integration of both classical and quantum devices and linkages as quantum technology advances, the networks we use will grow more complicated. We must anticipate the risks and possibilities that quantum computing and communication will bring to our computing and communication ecosystem.

Governments and businesses, in particular, have a difficult problem in preparing for and prioritizing the cybersecurity dangers that large-scale, fault-tolerant quantum computers will bring. We can't afford to squander time developing and implementing quantum-resistant encryption[4, 8, 5, 10, 6].

4. Conclusion

We shouldn't wait until something goes wrong, given the limited resources and funding available for quantum computing research, as well as the restricted number of commercially available devices. For that reason alone, quantum hardware and software components should be built and designed with security in mind. Similarly, the design of related services should be relocated to the left. Sabotage, espionage, and extortion are all probable targets for the Quantum Computing sector. Threat intelligence has the potential to shift security efforts from a reactive to a proactive approach to combating threat actors and securing one's system with foresight. MISP (Malware Information Sharing Tool) is a free threat intelligence platform that may help you comprehend the many sorts of threat actors.

References

[1] Bilgehan Arslan, Mehtap Ulker, Sedat Akleylek, and Seref Sagiroglu. A study on the use of quantum computers, risk assessment and security problems. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–6. IEEE, 2018.

[2] G Arun and Vivekanand Mishra. A review on quantum computing and communication. In *2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking*, pages 1–5. IEEE, 2014.

[3] Adenilton José da Silva, Teresa Bernarda Ludermir, and Wilson Rosa de Oliveira. Quantum perceptron over a field and neural network architecture selection in a quantum computer. *Neural Networks*, 76:55–64, 2016.

[4] Dorothy E Denning. Is quantum computing a cybersecurity threat? although quantum computers currently don't have enough processing power to break encryption keys, future versions might. *American Scientist*, 107(2):83–86, 2019.

[5] Keegan Keplinger. Is quantum computing becoming relevant to cyber-security? *Network Security*, 2018(9):16–19, 2018.

[6] Kyung-Kyu Ko and Eun-Sung Jung. Development of cybersecurity technology and algorithm based on quantum computing. *Applied Sciences*, 11(19):9085, 2021.

[7] Vasileios Mavroeidis, Kamer Vishi, Mateusz D Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*, 2018.

[8] Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.

[9] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[10] Secure Hash Standard SHS and Random Number Generator RNG. Computer security division standards & guidelines (publications).