Quantum Computing: An Assessment into the Impacts of Post-Quantum Cryptography

Roger G. Massmann
Department of CSIT
Saint Cloud State University
St. Cloud, Minnesota, 56301
roger.massmann@go.stcloudstate.edu

Nick M. Grantham
Department of CSIT
Saint Cloud State University
St. Cloud, Minnesota, 56301
nmgrantham@stcloudstate.edu

Akalanka B. Mailewa
Department of CSIT
Saint Cloud State University
St. Cloud, Minnesota, 56301
amailewa@stcloudstate.edu

Abstract

Quantum Computing continues to expand and rapidly approach large scale commercial usage. The advancement of quantum computing poses a threat to current cryptographic techniques and solutions are being researched rapidly to determine the correct course of action, culminating in a field known as Post-Quantum Cryptography, or PQC. This research gathers sufficient information and evidence to prove that quantum computing can be formally introduced into society where individuals can feel a sense of assurance that this technology is used for good rather than evil. For quantum computing, we weighed up whether the capabilities outweigh the costs, and if we can truly imagine a world where quantum computers can be a commercialized product. Quantum key distribution facilitates key exchange so that users can safely transmit messages over a quantum channel where the receiver will have access a key that will be the baseline for communication. Along with this comes the theorems that compensate for the possibility of photon leakage, or the possibility of an eavesdropper. With the evaluation of strength for a quantum computer comes the posed threat as to whether quantum computers can be used for the wrong reasons, therefore, post-quantum cryptography acts as the quantum proof measure, which may defend against quantum attacks and although PQC is currently limited to companies investing billions of dollars in research, the impact on the end-user is imminent. The objective of this review is to compile the current research and data in order to assess the impacts of Post Quantum Cryptography on organizations and agencies, and to approximate when and how these impacts will arrive at the end-user.

Keywords: Attacks; Quantum-Computing; Security; Vulnerabilities; Risks; Threats; Cryptography; Post-Quantum-Cryptography

1 INTRODUCTION

A technologically driven society stems from the structures and foundations of those who came well before us. From Stephen Wiesner's development of conjugate coding in the late 60's [1], onto Alexander Holevo who inspired the introduction of "Holevo's Bound" theorem, these individuals were just very few of the scientists that paved the way for Isaac Chung, Neil Gershenfeld and Mark Kubinec to successfully administer the first representation of two, three, five, and seven quantum bit quantum computers in 1998. The group's initial computation allowed for a two-qubit input/output scheme, and while recognized as a minor result mathematically, it can alternatively be viewed as a spark in opportunity for the future of quantum computing. Some may ask, why has quantum computing resurfaced as a 'new' generational phenomenon when it has been studied and implemented for over twenty years? The short answer to that question would be that it is based on interpretation and perspective as to how you understand the present versus the past of quantum computing. For years, quantum computing has been vastly a concept, but now, organizations are beginning to speak out about the properties, potential, and risk that quantum computing obtains. Now that quantum computing has transitioned from theoretical to realistic implementation, government agencies must now think of ways that will carry out or mirror the cryptographic algorithms that a standard computer would demonstrate in asymmetric or symmetric encryption onto a quantum-based computer. This leads us to the topic of quantum cryptography, better known as quantum key distribution (QKD), which was invented by Bennet and Brassard [2] as well as Ekert [3]. This essentially acts as the secure transmission of communication through a quantum channel that ensures both speed and security. The opportunities that arise through QKD are limitless, and it tends to be the driving factor to most organizations that are reassuring their customers that they should not be afraid of a quantum inspired future. See, Quantum keys are deemed unbreakable, which make them beneficial for secure message transmission, however on the other hand, message transmission might not always be used for good [4][2].

On the other end of the quantum spectrum comes the risk evaluation and assessment through post-quantum cryptography. As mentioned earlier, quantum computing has raised some very valid questions around how data is going to be protected, considering the power of message transmission and retrieval. Post-quantum cryptography aims to counteract and mitigate the risk factor around quantum computing, as well as reassure organizations and customers that their data is being handled sufficiently. U.S. Secretary of Homeland Security, Alejandro Mayorkas is adamant on embracing the transition to a quantum environment [5]. According to Mayorkas, the transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption [5]. His statement suggests that there is a push for strong encryption practices within quantum computing, and that there is a priority around confidentiality of data now, and in the future. However, it isn't just Homeland Security and the US Government making statements about the potential and dangers of quantum computers, it's basically every major tech company. IBM, Google, Intel, Microsoft, just to name a few, are both embracing and preparing quantum computing, and have standards and roadmaps in place to ensure that when the day comes where quantum computing because natural practice, they will have all bases covered, whether it be through encryption to CVSS. With encryption in

mind, there are various algorithms that are already being implemented in the IBM quantum lab, which can visualize what a quantum computer is capable of. From Shor's, to Grovers Algorithm, these methods will be analyzed and evaluated through the virtual quantum compiler, which is a great resource to enable us to get a gauge on how useful quantum systems can be in solving bulk data.

2 BACKGROUND

For this review, the referenced works had to meet several criteria to be considered. To have a full spectrum of perspectives, references were taken from the private sector publications, public sector publications, and from well-reviewed field experts. For the public sector publications, the references were only taken from well-known sources containing bodies of work in both classical computing as well as quantum computing to ensure the sources were unbiased and thoroughly researched. The sources from field experts all contained several references to other reviewed published works, as well as some sources that contained cited expert opinion. One of our first citations came from the Stanford Encyclopedia [6], a publication maintained by Stanford University, a private research institution with dedicated facilities for Computer Science, Theoretical Physics, and Quantum Information. Another source with a rich history in the field in computing is IBM [7], a corporation dedicated to advancing technology for business, which also was one of the first entities to begin research in quantum computing in the 1980's. In the public sector, sources used include the United States Department of Homeland Security [27], a long-standing contributor to the field of cryptography and cybersecurity that is publicly funded by the United States government. Each source was thoroughly vetted to ensure they were peer reviewed and approved by experts and contained well documented, accepted and most importantly accurate theory and information.

3 QUANTUM COMPUTERS

Quantum refers to the smallest particle in a physical state. It inherits the same properties of atomic or subatomic matter, involving electrons, neutrinos, and photons [8]. The reason why quantum computers are so relevant in society today, is due to the potential that they carry, as well as the threats that could arise. The characteristics of a quantum computer can essentially change the way technology operates as a whole. "Quantum supremacy" has been a term used to describe quantum computers. This is because there are abilities that a quantum computer inherits, that cannot be achieved by a classical computer. For example, Google's latest quantum computer claims to be able to complete a computation in around 200 seconds, whereas a classical computer would take 10,000 years [9][10]. Tech giants have publicly committed millions, if not billions of dollars toward large-scale quantum computers, and we could see fully functioning, publicly implemented quantum computers in as little as 5 years from now [10].

Classical computers function through binary states, this means that message transmission utilizes 0's and 1's to communicate and determine results [11][12]. Quantum computers on the other hand function on a qubit system, which factors in various possible states, expanding the functionality of message transmission. Quantum computers require temperature levels just shy of absolute zero to operate. Another drawback to quantum

computers is that the price of processing has been a concern for many, where it can costs 10's of millions of dollars to function a commercialized quantum computer. This pulls into question, whether it is worth the investment, and to balance out our wants and needs as a society. The low scale quantum computers can function from as little as $5,000, with limited problem-solving capabilities. On the other hand, there is IBM, who acquires a 127 qubit quantum computer that would cost an exponentially large sum, exceeding the $15 million dollar mark.

IBM [13] mentions that they use cooled super fluids to avoid overheating. But with this extremely low temperature comes other perks of transmission for electrons in particular. Electrons attain a quantum mechanical effect where they travel with ease through a channel, making them superconductors. A term known as "Cooper pairs" describes the way that the electrons meet up and travel through the superconductors, carrying a charge over insulators that facilitate the transmission. These electrons are being passed through what is known as a quantum tunnel. IBM in particular, use a structure called Josephson junctions as their superconducting qubits. Therefore, when microwave photons are directed to the qubits in transmission, they can dictate their state, and note results.

Say there are two individuals living together. Both individuals need to decide what shirt they are going to wear for the day. Person one is in their room and has a selection of two shirts to wear for the day. The color of the shirts for person one is black and the other is white. For person two, they have many shirts to select from. Not only do they have many shirts to choose from, but they have shirts that range from black, to a grey, all the way onto a plain white. The bottom line is, person two has the option to wear a shirt that acquires both white and black, with various shades involved as well. Person one is the classical computer. This individual can only choose from two options, the black shirt representing a 0, and the white representing a 1. Individual two has an overflowing wardrobe, this person can choose from a huge selection of shirt colors. This is our quantum computer. This analogy represents superposition, where the states of a quantum particle can represent anything within the possibility of a binary digit [8].

The correlation between the photons that flow throughthe quantum channel is known as entanglement. To reach the state of entanglement, quantum particles follow a process where they flow through a laser lightinto crystal, by which they are then converted by crystal into entangled pairs of photons. Based on various QKD protocols, the entanglement process canbe perceived differently in each process.

4 QUANTUM KEY DISTRIBUTION

When looking at standard key distribution, there is always an element of whether Alice and Bob will be able to communicate safely without Eve intercepting the message in the middle. Many cryptographic practices will attempt to protect the key, however there can never be full protection guaranteed on classical methods. Classical cryptography bases encryption around the CIA triad, with the aim for messages to be confidential in nature, transmission being impenetrable or difficult to hinder through integrity, and finally available for both parties to access. Additionally, the CIA triad hasn't been the only thing referred to when verifying a secure method of communication, rather the objectives of

authentication, digital signatures, and non-repudiation all mound into the structures of a successful cryptographic system [14][15][16].

The basic approach to cryptography is that plaintext message will be encrypted into ciphertext, which then becomes decrypted by the time it reaches the receiver. The properties of cryptography involve symmetric key, (also deemed as private key cryptography), which only has one key exchanged. Symmetric encryption is great for fast transfer and bulk encryption [17][18]. The image 1 below demonstrates how symmetric encryption works.

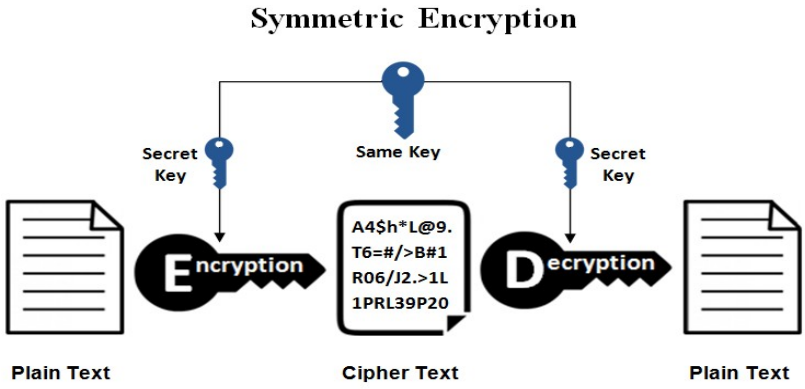


Figure 1: Symmetric Encryption [12]

Having one main key facilitating the communication. On the other hand, Asymmetric, or public key encryption utilizes a public channel that functions as a means of encryption, and the private channel functions as a decryption utility [19][20]. So, in the case of a user attempting to connect to a HTTPS server for instance, Alice (web server) attempts to communicate with Bob (browser). When Bob receives the public key from Alice, the message encrypts as a one-time symmetric key. Then the symmetric, private key acts as a baseline for the rest of the communication for both encryption and decryption [21].

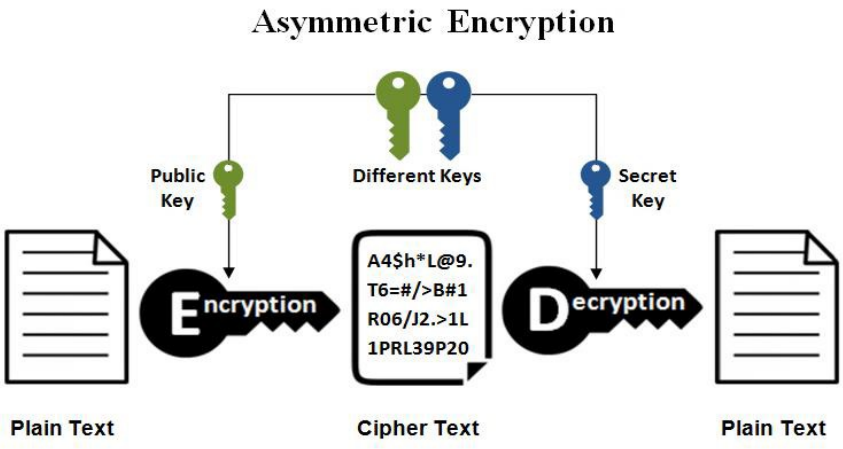


Figure 2: Asymmetric Encryption [17]

QKD is essentially the first application of quantum information science, and through years of study, analysis and finally, implementation, there have been products now available that acquire properties used through quantum based commercialized products. Although quite limited through key distribution over 100km, the progress of QKD is astonishing [22]. Just like classical key distribution, quantum key distribution uses an exchanged, shared key to communicate, however this method is facilitated through the quantum channel. The principle that separates quantum key distribution from classical.

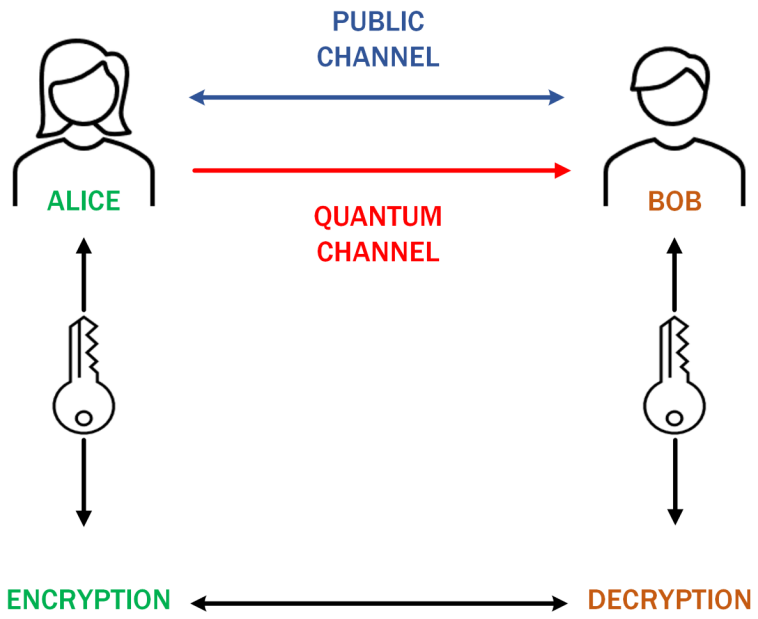


Figure 3: Quantum Key Distribution Diagram

Key distribution is the method of distribution that include the laws of physics to send and receive the qubits sent through the quantum stream. The distribution, capturing and development of the residual key is why quantum cryptography is deemed unbreakable, making it very controversial from all levels of the technological industry. To explain how QKD works with reference to the BB84 protocol by C.H Bennet and G. Brassard, we will use the standard Alice and Bob concept to demonstrate how message transmission successfully reaches the end user. During communication between Alice and Bob, Alice initiates the message through the production of a stream of photons. The photons flow through a polarizer, which then determines the quantum state of the cryptographic bits that will eventually reach Bob. However, the state of these quantum bits will be characterized as not only vertical and horizontal, but they can also carry a -45- degree or +45-degree angle that will travel towards Bob. [23].

- H (horizontal) codes for 0+
- V (vertical) codes for 1+
- +45 codes for 0×
- +45 codes for 1×

As a means of more advanced key determination, Bob will meet the quantum photon states with a randomizedphoton splitter, that will establish whether the photons. Will either pass through or be dropped in the case of an unmatched state? This is where the unbreakable nature comes into the picture. When Alice and Bob match up their sending and receiving keys, there will be inconsistencies as to whether Alice's photon state matches up with Bob's photon splitter state. The keys will correlate, and a residual/sifted key of the matched states will determine the final quantum key.

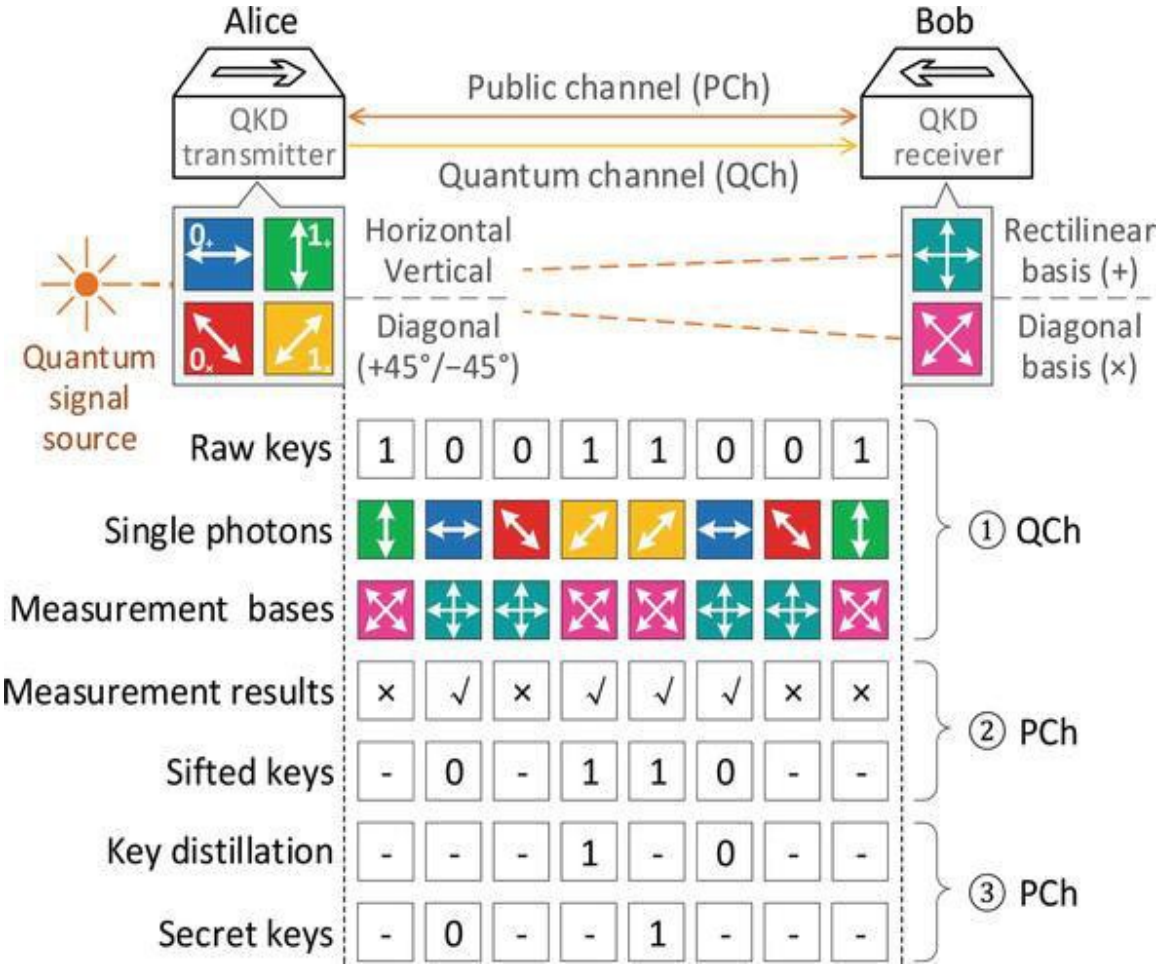


Figure 4: QKD Based on BB84 [24]

The characteristics of QKD assume correctness and secrecy [22] over the channel that are near impossible to ensure. There are many factors that must be considered in quantum cryptography that can alter the state of the initial key or be intercepted by an eavesdropper. While we might believe that an ultimate secure method has been arranged by Alice and Bob through quantum key distribution, we must still factor in the possibility of an eavesdropper (Eve) intercepting or hindering transmission from Alice to Bob. For the QKD protocol to be deemed secure, it is important to understand that everything that can go wrong, very well will go wrong in the transmission. We have an equaling Alice and B equaling Bob. Ultimately, because QKD bases itself off randomness and estimation, if A = B, this is a successful key exchange. But the probability of this occurring without some

type of interference is very low, therefore, it is paramount to account for the interference. In average instances of a long key distribution, Eve will gather about 50% of the raw key through eavesdropping over the fully exposed quantum channel (IE). With an error rate of about 25% (Q), we must factor in how successful the communication will be under the assumption of an eavesdropper within message transmission. With reference to Shannon information theory around parallelism as well as the Korner-Csiszar-Marton theorems [25], we will unpack the demonstration of how Alice maps to Bob with knowledge of a potential eavesdropper interference. For:

$$r = \max\{I(A : B) - IE , 0\} \quad [18]$$

Where I(A : B) = H(A) + H(B) − H(AB) is the mutual information between Alice's and Bob's raw keys [15]. Variable H factors in Shannon entropy, meaning the amount of information within the variable is dependent on user input [26]. Having said this, if

$$H(A) =(B) = 1, \text{ one has } I(A : B) = 1 - H(Q), \text{ with a resend attack of } I(A : B) < IE \quad [19]$$

Eve will then have more information as opposed to Bob through her manipulation of the quantum channel, and this will cause Bob to abort the communication.

This is an example of how quantum cryptography drops communication over any suspicion or inconsistency over transmitted messages. In another example, asymptotic and finite-key bound draws upon the corrections [27] important in the efficiency and robustness [28] of quantum key distribution. Additionally, these regimes determine whether through fault tolerance and error rate, can a quantum key still be developed? For these methods, Alice will devote as many signals toward Bob in attempts for Bob to receive as much data as possible, which outweighs the leakage to Eve. Similarly, to the previous example, if a substantial amount of data is exposed to Eve, the transmission will be aborted [29].

The asymptotic limit displays r as the running exchange of the key, N as the total number of signals exchanged by Alice towards Bob, and L being the length of the secret key.

$$r \infty = \lim (L/N) \to \infty \; N = \min H (A | E) - H (A | B) \quad [11]$$

On the other hand, the finite key bound factors in the element of uncertainty within the communication, analyzing the level of leakage that can be withstood in a key distribution. [27]

$$r \, N = N = n \, N \min E | V \pm \Delta V \, H (A | E) - \Delta(n) - leak \quad [11]$$

These theoretical distribution methods test the fault tolerance factor of quantum key distribution, and while it is great to suggest that Shannon theorem and parallelism will be secure enough to account for an absent eavesdropper, the fault tolerant based methods tend to be more practical

5 POST QUANTUM CRYPTOGRAPHY

As Quantum Cryptography grows and evolves, issues in security and vulnerabilities grow with it. While many companies seek to advance knowledge on the subject and improve the technology, other organizations seek to find the issues and risks with using Quantum Cryptography, and the risks associated with refusing to adopt these advancements as common business practice [30] [31].

The private and public sector have worked closely in the past to develop classical computing and security, and to create rules, regulations, and protocols. This is no different in quantum computing. While Google, IBM, and Intel work to expand the capabilities and usage of this technology, NIST and other agencies are quick to respond with common standardizations [30]. As of November of 2022, NIST is completing a third round of evaluating and selecting algorithms to be standardized in the field for PQC. The most recent status report updated in September of 2022 details the candidates and evaluation process, as well as algorithms no longer being considered. The report and operation as a whole set the precedent for the treatment of standardizing the field. The research, analysis, and results will impact the development of current and future algorithms to be standardized, while ensuring that the advancement of PQC is still under the control of the public.

While standards are being set, private corporations continue to make strides to be the leader in the field. While classical computing continues to grow, it will eventually run into physical limitations [7] that can be effortlessly surpassed by quantum computing. With these advancements, however, the obsolescence of classical cryptography is also approaching. While quantum machines will be able to complete computations in minutes that would take classical computing decades, current cryptography simply won't hold up to PQC. The most important issue for private corporations and government agencies is determining how to respond to PQC, when to respond, and when will all these factors make more sense financially for the companies. Recently, companies have even begun live testing of PQC algorithms. As of 2016, google announced a live experiment using their own post quantum key exchange algorithm on a small fraction of connections to Chrome servers [32]. This experiment demonstrated that practical applications of PQC in the real world are indeed feasible and are closer than most users are aware. More analysis into other private entities and public agencies are instrumental in determining exactly when PQC will overtake classical computing. With the private sector taking steps to revolutionize their own PQC power, the end user can already access an abundance of education material. Currently, IBM offers QISkit [33], a software that interprets high level languages such as Python and applies them to IBM's quantum machine algorithms. This allows users to experiment and learn about quantum computing through the curriculum designed by IBM, or by experimenting individually in the quantum lab. The focus of this technology is not to allow the end user to execute complex quantum algorithms, the simulation has a timeout limit of roughly 10000 seconds, but to allow the user to gain a baseline understanding of quantum computing to educate the public. Ultimately, QISkit is a tool that is currently incapable of posing any form of a security threat. In fact, it is extremely unreasonable to consider any entity without access to a physical quantum machine be a true threat in the real of PQC, thus for the foreseeable future, quantum computing will remain virtually unaffected by script kiddies.

To understand what corporations are essentially racing towards, a quantifiable goal allows for a more concrete analysis. In quantum computing the term Quantum Advantage describes a machine that would be able to compute problems that no classical computer can [34]. As of right now, this goal is not immediately commercially viable, with no tangible outlook on when it might be. However, a more attainable benchmark is the 50-qubit quantum computer. In 2018, IBM announced the functional IBM Q, a 50-qubit quantum computer. This machine displayed the ability to compute problems previously considered unsolvable by machines [35]. Almost immediately after, Google responded with a processor that contained 72 qubits. Although these computers are far from being commercially available, they demonstrate that the technology currently exists to allow quantum computing to surpass classical computing, making PQC innovation a necessary field.

5.1 IBM QUANTUM COMPOSER

In our data findings, we will be using the IBM Quantum Composer to analyze how various algorithms work in quantum computing [36]. This will demonstrate the power of a quantum processor, and give a gauge around why quantum computing can be seen as both an advantage and disadvantage for the present and future of technology. As we open the Quantum Composer shown in figure 6, there are an overwhelming number of options as to how we, as the user, can input and output the data. Starting with the operations section; there are various inputs that can dictate the output of the quantum computation. The function, whether it's a classical gate, phase, non-unitary/modifier, or quantum operation, can be a building block to support a quantum algorithm or outcome. This is why it is so revolutionary for IBM to have this platform as an open-source space for individuals to be inspired by the potential of quantum algorithms. Next, the section to the right of the operations tab displays a staging type- environment, where the operations can be dragged and dropped to fulfil the users' algorithm choice.

In Figure 5, a Hadamard Gate has been placed in the staging environment. A Hadamard gate in particular convert |0⟩ and |1⟩ to |+⟩ and |-⟩ and linked to the super positioning states mentioned earlier [37].

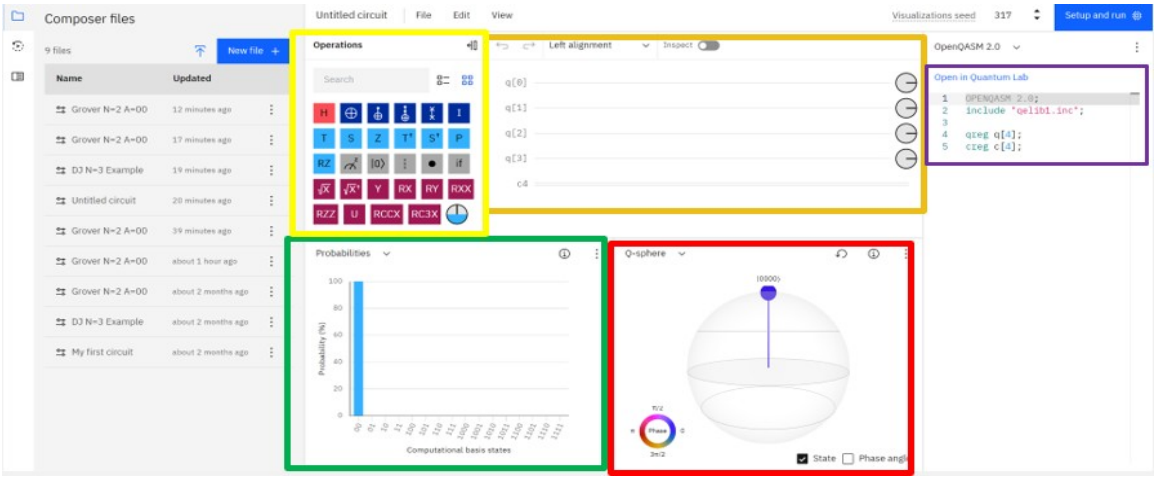


Figure 5: IBM Quantum Composer: Individuals to create own Quantum Algorithms

Next, there is a command line interface that will carry out the code that links to the staging environment. Therefore, the more code, the more changes to the CLI. When we added the 'h' gate, the CLI will then display an 'h' gate located at index 1, or qubit 1. The probabilities section displays the percentage of the outcome occurring based on the state, and the Q-sphere, gives a visual idea of the state, and phase angle, as well as the probability of the state occurring.

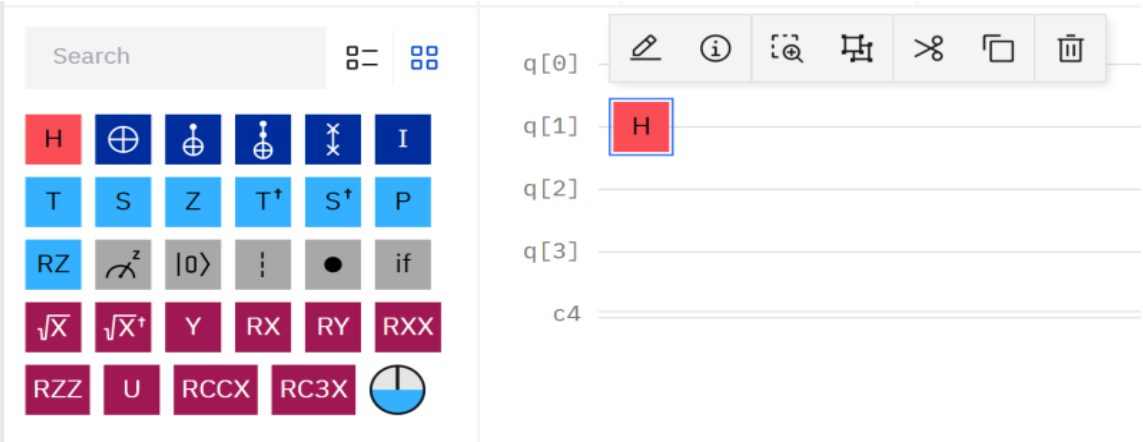


Figure 6: Operational structure with Hardamand Gate

5.2 SHOR'S ALGORITHM

In number theory, the former most efficient algorithm for finding prime factors of an integer was the general number field sieve or GNFS. That was until 1994, when mathematician Peter Shor introduced Shor's algorithm, a polynomial-time quantum algorithm [38]. Shor's algorithm allows for a near exponential decrease in the amount of time it takes to factor integers with digits greater than 1000.

The implications of Shor's algorithm on PQC are immense, as future quantum computers with greater processing power might be able to apply the algorithm towards decrypting keys that would otherwise take hundreds of years to decrypt with classical computing. RSA encryption is reliant on the assumption that classical computing cannot efficiently factor large prime and semi-prime numbers. Because of this, in future applications of quantum computing, Shor's algorithm could render RSA and other classical encryption techniques useless. To visualize this, it is known that the GNFS can be reasonably expected to be limited to roughly 200 digits. According to IBM's QISkit's current data [36], factoring a polynomial N with d decimal digits, GNFS would take exp(const * d1/3), almost exponentially longer than Shor's which can be displayed as const *d3. While the classical algorithm's record might take 1030 operations, Shor's might take 10^7. With the IBM quantum composer, Shor's algorithm can be displayed using IBM's circuits and operations.

First, the reset operation is used to return the qubit to the state |0⟩. Then, an H gate, followed by a T gate and another H gate are applied to rotate the state and alter the angle. These figures demonstrate the application of Shor's algorithm, as well as the written code in the quantum lab.

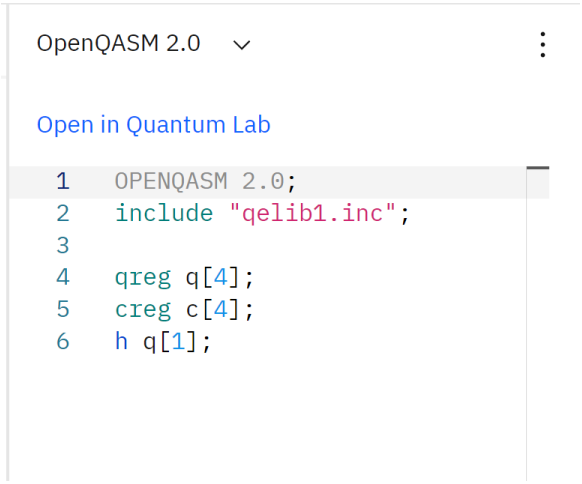


Figure 7: circuit code in IBM's quantum lab

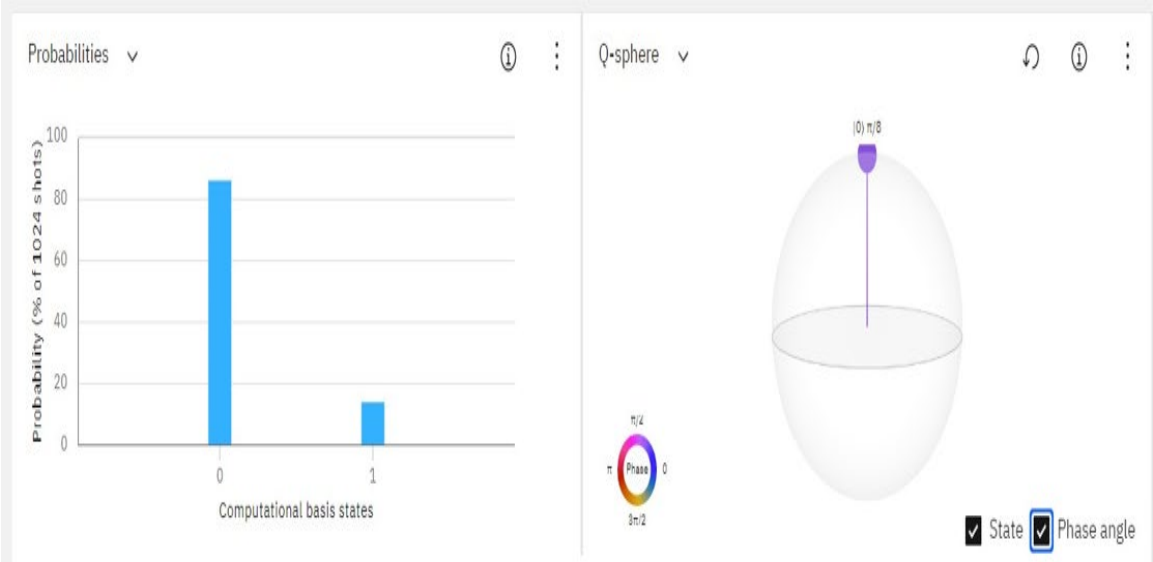


Figure 8: Shor's Algorithm probabilities and Q-Sphere

Figure 9: operational structure for Shor's Algorithm

5.3 GROVERS ALGORITHM

In 1996, Lov Grover introduced quantum search function now known as Grover's algorithm. The database search algorithm has the ability to analyse large amounts of data and narrow down the results to find the desired product [38]. To give a greater understanding around how powerful Grover's Algorithm can be, think about a brute force attack, and how efficiently Grover's algorithm could be implemented to gain access to a password. Grover's algorithm is known to create a quadratic speedup, meaning it will drastically narrow down the tries it attempts before it gains a result. For example, if we have four cups, and one of these cups had a rock under it, the average amount of times it would take a classical computer to guess the right cup would be 2 and ¼ attempts. On the contrary, if a classical computer was to guess the correct cup, it would take 1.

Now, we will move into the IBM Quantum Composer to demonstrate how Grover's Algorithm works. Using a template created from the IBM Quantum Composer, we can display the structure of Grover's Algorithm, where the outcome that is sought after is in state 00. As shown below, we have both of our $|0\rangle|0\rangle$ states in qubit 1 and qubit 2. This is known as the reset operation.

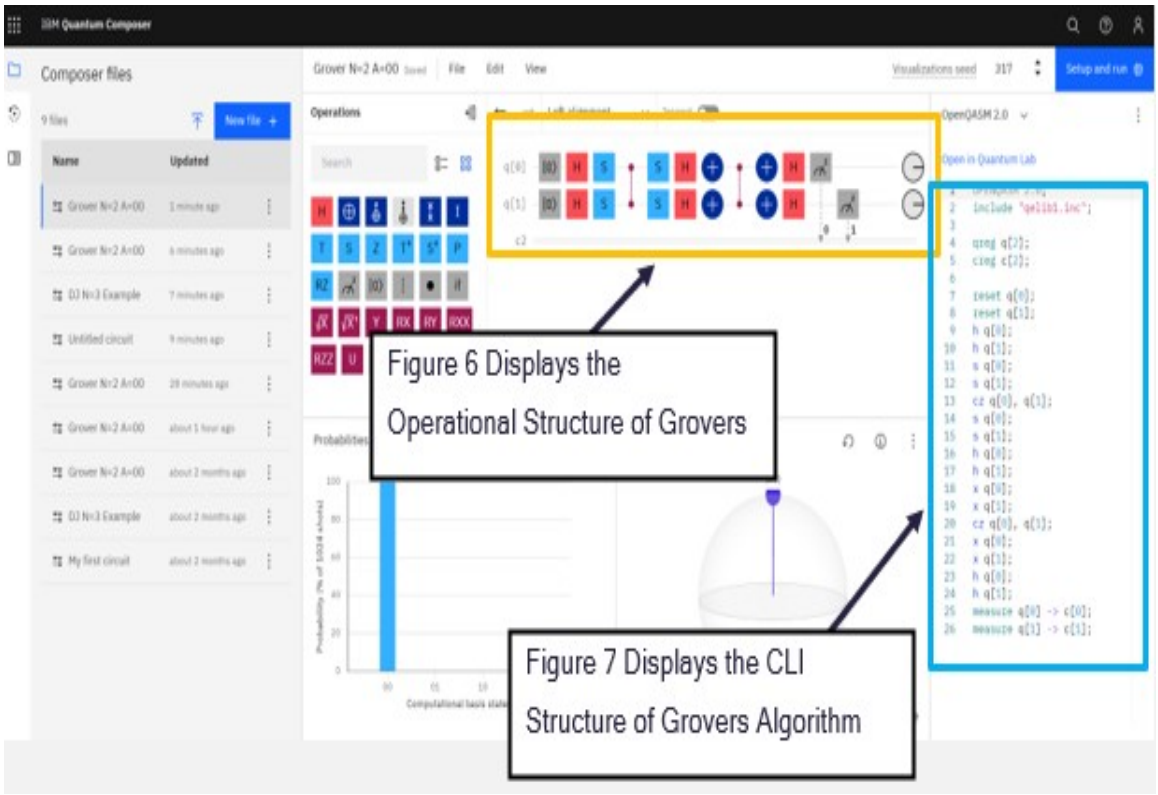


Figure 10: IBM Quantum Composer with Grover's Algorithm

5.3.1 Data Extraction of GROVER'S algorithm

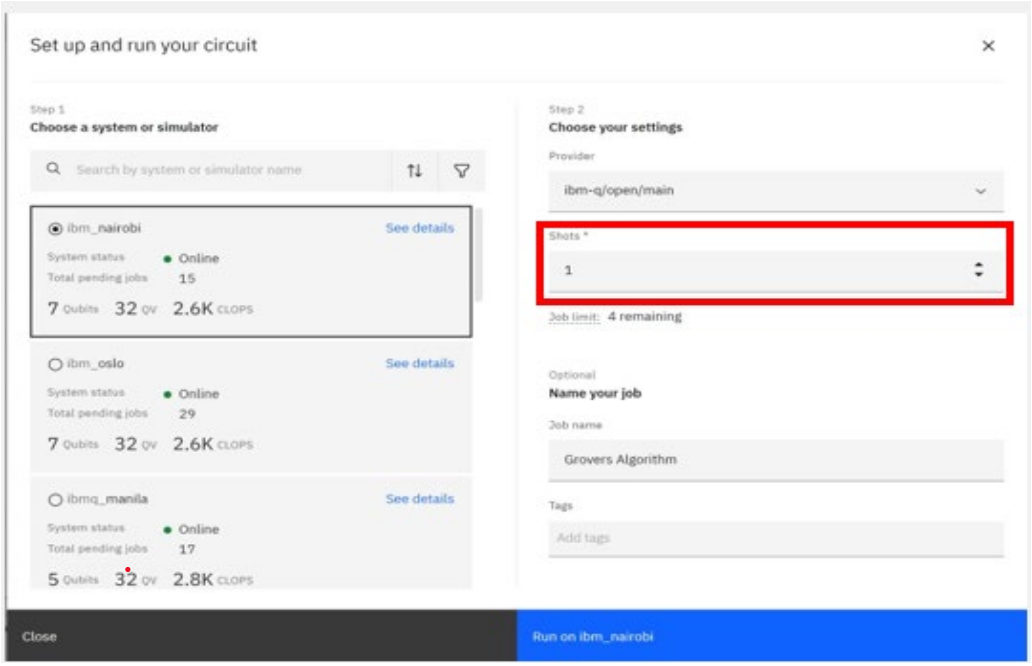
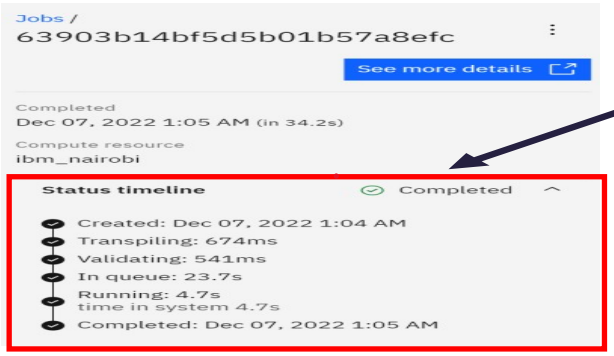


Figure 11: Run with 1 Shot



The job on the left displays a must faster result time, due to the size of the results that aresought out

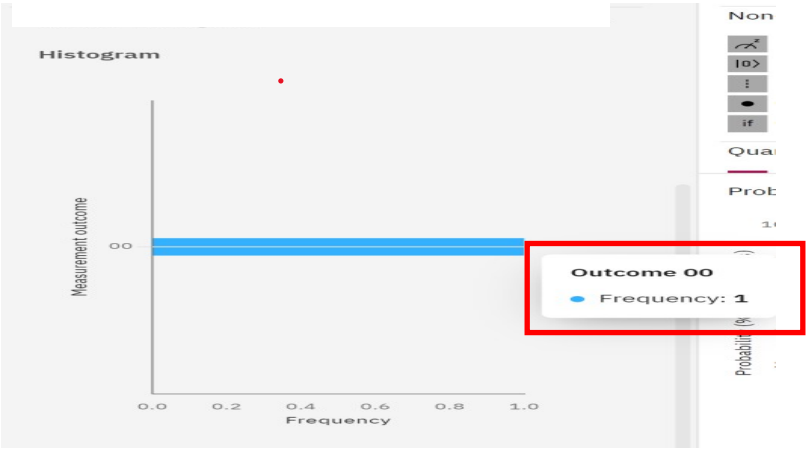


Figure 12: Shows the test 1 histogram

As we would like to receive the result of 00, and only have 1 attempt to do so, this proves the accuracy of the algorithm**.**

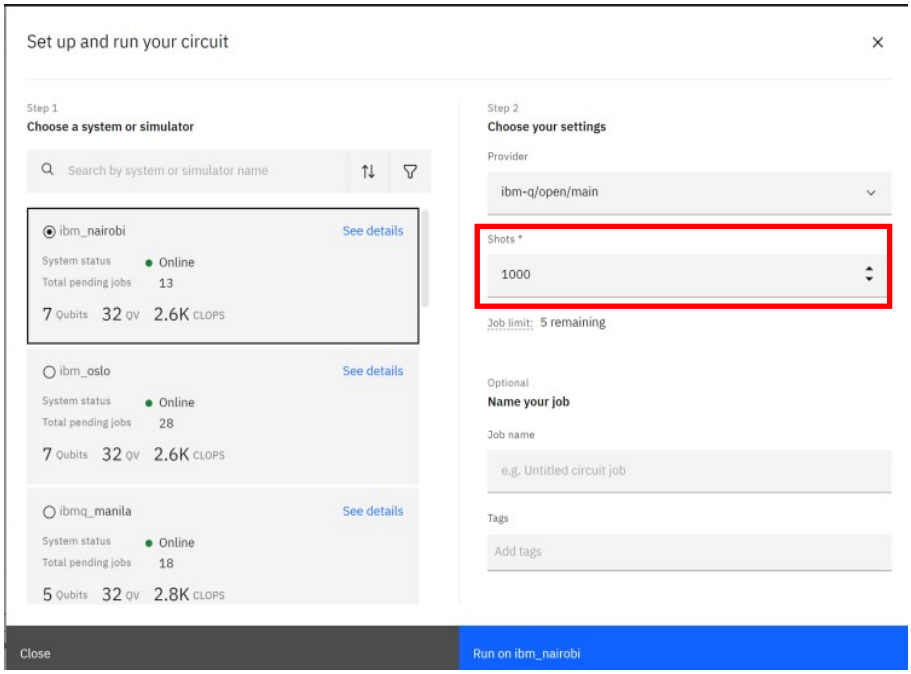


Figure 13: Run with 1000 shots

Alternatively, the size of the algorithm affects the queue time of the results to occur

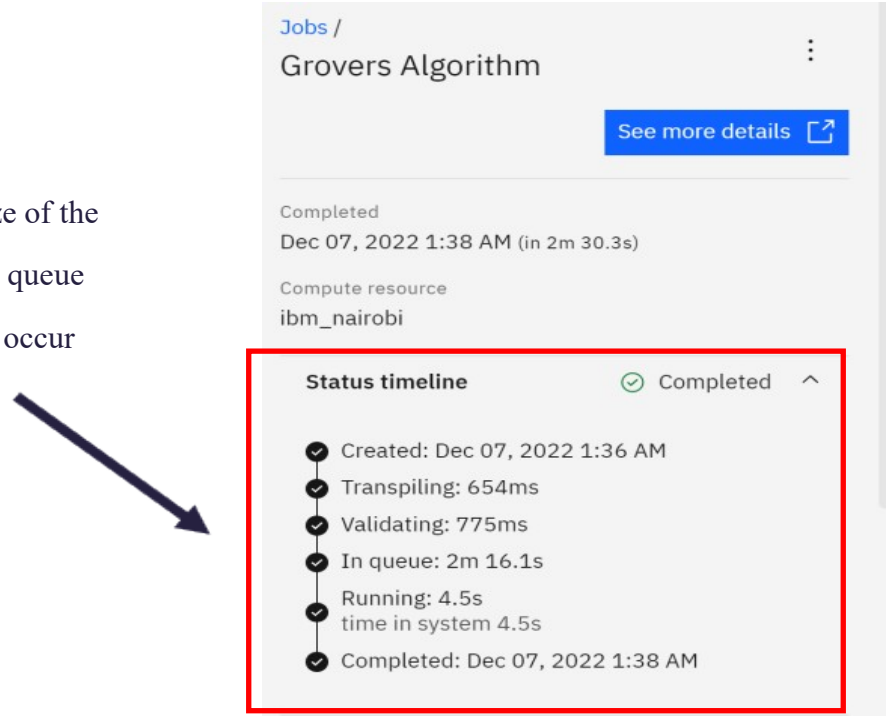


Figure 14: Details of status timeline 2

To receive the result from a bulk set of attempts, we can see that the result shows a 96.8% success rate for 00

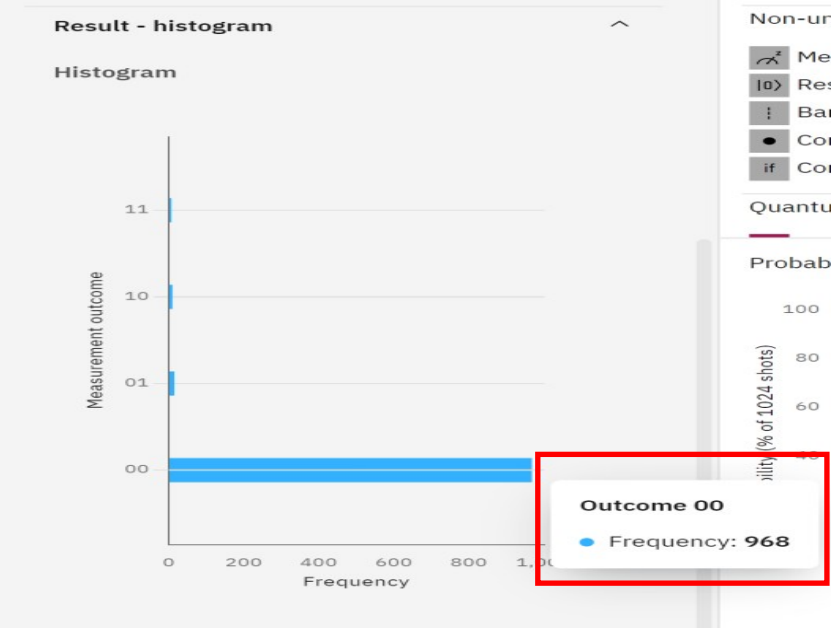


Figure 15: Shows the test 2 histogram

5.4 ALGORITHM ANALYSIS

In the analysis of Grovers Algorithm using the IBM Quantum Composer, the program is very impressive in how it simulates quantum processes. The functionality within the program is great from an educational point of view, and clearly outlines how Grovers algorithm works. The findings expressed that Grovers algorithm is very accurate in searching for items within an array. Working on a theoretical basis is a great way to demonstrate processes, however from further research, it is not necessarily certain that Grovers algorithm can be exploited through quantum computation. [1] Grovers algorithm proves to be a great searching utility, however from a cryptographic tool standpoint, there may be implications that any quantum computer may face, such as noise or other physical interferences. On the other hand, Shor's algorithm provides not only a strong display of the advantages of quantum cryptography, but also an insight into how the field of cryptography will need to adapt to changes that were not previously predicted. The ability of Shor's algorithm to factor large prime numbers poses a new challenge for researchers everywhere. Although quantum computers do not currently have the capabilities to execute the algorithm in a way that could impact current encryption standards, the implication that it could is enough to help advance the research of post-quantum cryptography to search for a solution when it is eventually needed. It also alerts researchers to the idea that many classical cryptography techniques will simply not be viable in the near future, and the progress of cryptography is benefiting from this push for new technology.

6 CONCLUSION

In this paper, our aim was to gather sufficient information and evidence to prove that quantum computing can be formally introduced into society where individuals can feel a sense of assurance that this technology is used for good rather than evil. For quantum computing, we weighed up whether the capabilities outweigh the costs, and if we can truly imagine a world where quantum computers can be a commercialized product. Quantum key distribution facilitates key exchange so that users can safely transmit messages over a quantum channel where the receiver will have access a key that will be the baseline for communication. Along with this comes the theorems that compensate for the possibility of photon leakage, or the possibility of an eavesdropper. With the evaluation of strength for a quantum computer comes the posed threat as to whether quantum computers can be used for the wrong reasons, therefore, post-quantum cryptography acts as the quantum proof measure, which may defend against quantum attacks. And although PQC is currently limited to companies investing billions of dollars in research, the impact on the end-user is imminent. Regardless of the commercial viability, or lack thereof, of quantum computing, the current innovations clearly demonstrate a commercial need for corporations to pursue Quantum Advantage. This means Post- Quantum Cryptography, if not now, will be a pressing concern for companies in the near future. The first organization or entity to attain quantum advantage will acquire an insurmountable lead in the field and cause a shift in the entire landscape of computing, not just quantum. Ultimately, however, the end-user currently only feels the impact in a theoretical sense. Access to education material on quantum computing is as close to PQC as any individual not affiliated with a large agency will attain within this decade, if not century. The current most pressing issue to the end-user is data confidentiality, which likely will not be breached with quantum computers for decades. When it is, companies and government entities will be well prepared, having already been working towards post-quantum cryptography for years. And with various algorithms just like Grover's and Shor's, we can see that extraordinary research and results will be carried on throughout the years and built upon at an advanced rate that we cannot even comprehend.

References

[1] SGate at qiskit.org. Available at: https://qiskit.org/documentation/stubs/qiskit.circuit.library.SGate.html (Accessed: December 6, 2022).

[2] Bennett, C. H. & Brassard, G. in Proc. IEEE Int. Conf. on Comp. Sys. and Signal Processing 175–179 (Bangalore, India, 1984)

[3] Ekert, A. K. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67, 661–663 (1991).

[4] Gamnis, Steven, Matthew VanderLinden, and Akalanka Mailewa. "Analyzing Data Encryption Efficiencies for Secure Cloud Storages: A Case Study of Pcloud vs OneDrive vs Dropbox." Advances in Technology (2022): 79-98. (DOI:10.31357/ait.v2i1.5526)

[5] Post-Quantum Cryptography | Homeland Security. Available at: https://www.dhs.gov/quantum#:~:text=%E2%80%9 CThe%20transition%20to%20post%2Dquantum,lat ter%20remains%20in%20its%20infancy. (Accessed: December 5, 2022).

[6] Hagar, A. and Cuffaro, M. (2019) Quantum computing, Stanford Encyclopedia of Philosophy. Stanford University. Available at: https://plato.stanford.edu/entries/qt-quantcomp/ (Accessed: December 5, 2022). Homeland sec

[7] Barde, Nilesh, et al. "Consequences and Limitations of Conventional Computers and Their Solutions through Quantum Computers." Issue, vol. 19, 2011, p. 161, lejpt.academicdirect.org/A19/161_171.pdf.

[8] What is Quantum Computing: Microsoft Azure, What is Quantum Computing | Microsoft Azure. Available at: https://azure.microsoft.com/en- us/resources/cloud-computing-dictionary/what-is- quantum-computing/#introduction (Accessed: December 5, 2022). IBM

[9] Gisin, N. et al. (2001) Quantum cryptography, arXiv.org. Available at: https://arxiv.org/abs/quant- ph/0101098v2 (Accessed: December 5, 2022).

[10] Gillis, A.S. (2022) What is quantum cryptography?, Security. TechTarget. Available at: https://www.techtarget.com/searchsecurity/definitio n/quantum-cryptography (Accessed: December 5, 2022).

[11] Khan, Muhammad Maaz Ali, Enow Nkongho Ehabe, and Akalanka B. Mailewa. "Discovering the Need for Information Assurance to Assure the End Users: Methodologies and Best Practices." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 131-138. IEEE, May 2022. (DOI:10.1109/eIT53891.2022.9813791)

[12] Mailewa, Akalanka, and Jayantha Herath. "Operating Systems Learning Environment with VMware" In The Midwest Instruction and Computing Symposium. Retrieved from http://www.micsymposium.org/mics2014/ProceedingsMICS_2014/mics2014_submission_14 .pdf. 2014.

[13] Quantum encryption vs. Post-Quantum Cryptography (with infographic) (2022) QuantumXC. Available at: https://quantumxc.com/blog/quantum-encryption- vs-post-quantum-cryptography-infographic/ (Accessed: December 5, 2022).

[14] Mailewa, Akalanka, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Mechanisms and techniques to enhance the security of big data analytic framework with mongodb and Linux containers." Array 15 (2022): 100236. (DOI:10.1016/j.array.2022.100236)

[15] Sanyal, A. (2021) Symmetric, asymmetric and quantum encryption- an introduction to quantum cryptography, LinkedIn. Available at: https://www.linkedin.com/pulse/symmetric-asymmetric-quantum-encryption-introduction- sanyal/ (Accessed: December 5, 2022).

[16] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities." Cluster Computing 23 (2020): 1955-1971.

[17] Sanyal, A. (2021) Symmetric, asymmetric and quantum encryption- an introduction to quantum cryptography, LinkedIn. Available at: https://www.linkedin.com/pulse/symmetric-asymmetric-quantum-encryption-introduction- sanyal/ (Accessed: December 5, 2022).

[18] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs." In Companion Conference of the Supercomputing-2018 (SC18). 2018.

[19] Rathore, A. (2022) Quantum key distribution: The Future of Secure Communication, Electronics For You. Available at: https://www.electronicsforu.com/technology-trends/quantum-key-distribution-future-secure- communication (Accessed: December 5, 2022).

[20] Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. "A review of MongoDB and singularity container security in regards to hipaa regulations." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91-97. 2017.

[21] Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL based medical data processing and retrieval: the exposome project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. 2017.

[22] Tomamichel, M., Lim, C., Gisin, N. et al. Tight finite-key analysis for quantum cryptography. Nat Commun 3, 634 (2012). https://doi.org/10.1038/ncomms1631

[23] Rathore, A. (2022) Quantum key distribution: The Future of Secure Communication, Electronics For You. Available at: https://www.electronicsforu.com/technology-trends/quantum-key-distribution-future-secure- communication (Accessed: December 5, 2022). www-nature

[24] Zhao, Y. et al. (2018) Quantum key distribution (QKD) over software-defined optical networks, IntechOpen. IntechOpen. Available at: https://www.intechopen.com/chapters/63116 (Accessed: December 8, 2022).

[25] Muchnik, A. A. (2002). Conditional complexity and codes. Theoretical Computer Science, 271(1), 97–109. https://doi.org/10.1016/S0304- 3975(01)00033-0

[26] J. Lin, "Divergence measures based on the Shannon entropy," in IEEE Transactions on Information Theory, vol. 37, no. 1, pp. 145-151, Jan. 1991, doi: 10.1109/18.61115.

[27] Quantum Cryptography and Computing: Theory and Implementation, edited by R. Horodecki, et al., IOS Press, Incorporated, 2010. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/stcloud- ebooks/detail.action?docID=3014999.

[28] Meyer, T. (2007) Finite key analysis in quantum cryptography. Available at: https://www.osti.gov/etdeweb/servlets/purl/2106051 5 (Accessed: December 5, 2022).

[29] Singh, Nicholas, Kevin Bui, and Akalanka Mailewa. "Robust Efficiency Evaluation of NextCloud and GoogleCloud." Advances in Technology (2021): 536-545. (DOI:10.31357/ait.v1i2.5392)

[30] Moody, D. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/nist.ir.8413-upd1

[31] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with mongodb on singularity linux containers." In Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis, pp. 58-66. 2020.

[32] Venables, Phil. “How Google Is Preparing for a Post-Quantum World.” Google Cloud Blog, 6 July 2022, cloud.google.com/blog/products/identity- security/how-google-is-preparing-for-a-post- quantum-world.

[33] “QISKit -- Quantum Information Software Kit for Quantum Computation.” IBM Research Blog, 20 Feb. 2018, www.ibm.com/blogs/research/2018/02/qiskit- index

[34] Preskill, John. “Quantum Computing in the NISQ Era and Beyond.” Quantum, vol. 2, 6 Aug. 2018, p. 79, 10.22331/q-2018-08-06-79.

[35] Pierce, Alan. “The IBM Q Is a Working 50 Qubits Quantum Computer - ProQuest.” Www.proquest.com, May 2018, www.proquest.com/openview/67be7836dbb91b17e9d118359f1a02ca/1.pdf?pq- origsite=gscholar&cbl=182.

[36] Shor’s algorithm. (n.d.). IBM Quantum. https://quantumcomputing.ibm.com/composer/docs/iqx/guide/shors-algorithm

[37] Jozsa, R. (1999) Searching in grover's algorithm, arXiv.org. Available at: https://arxiv.org/abs/quant-ph/9901021 (Accessed: December 6, 2022).

[38] IBM Quantum Experience - Dashboard. (n.d.). IBM Quantum Experience. https://quantum- computing.ibm.com/