The Dangers of Quantum Computers in Cryptography

Vivek S. Madala

University of Arizona

CYBV 498: Senior Capstone Engineering

Professor Jordan VanHoy

Abstract

Over the course and lifeline of the unstoppable technological revolution, we have seen the world change through the lens of this evolution and are going through another evolution in technology as we speak that has great benefits. However, this comes with its own challenges, as people have been able to experience the unstoppable revolution of technology and the magnificent problems it has been able to solve around the world. It has also simultaneously created an unfulfilled void in humanity to solve more problems with far more powerful computers than ever before. A world where the flip of a coin not only represents monetary value but also represents the basics of quantum computing, the ability to harvest the power of 0 or 1 to transform every aspect of human life and the planet. A superposition that would disrupt what we know to be a reality now is now inevitable. To wait for such power to land in the hands of our evolving digital world before we could understand its grasp would be devastating. This paper aims to explain and study the evolving nature of quantum computing and its severe impacts on current encryption methodologies. This is performed by demonstrating its potential power using open-source quantum computing samples and architecture such as Azure Quantum In-Memory Simulator and Quantum Resource Estimator and Cryptography.

Keywords: classical computers, quantum, quantum computing, superposition, power, current encryption methodologies, cryptography, Grovers algorithm, Shor's algorithm, analysis.

Table of Contents

Table of Figures

Potential Impact on Cryptography

In this rapidly changing landscape of digital scaling and security, the power that quantum computing will hold would introduce an entirely new paradigm shift with profound implications in the world of cryptography. This is further backed by the empirical data and its current phase of research, "Given its current state of development, experts anticipate that quantum computing could provide unprecedented advantages…However, to date, quantum computing has extensive unsolved challenges in physics and computer science" (Rietsche et al., 2022, p. 2526). Quantum computing solves several problems that classical computers simply cannot. There are problems that would take billions of years to calculate and solve with classical computers that could be solved in several years or even seconds.

The basic principles of quantum computers and their ability to exploit superposition and entanglement to represent a set of data operations would allow quantum computers to solve at a significant rate compared to that of classical computers (Rietsche et al., 2022). The significant risks posed by advancements in quantum computing, specifically with Grover's and Shor's algorithms on current cryptographic standards, have the potential to unveil and break modern encryption processes and signatures. Necessitating an urgent and critical analysis of the significance of quantum power in the field of cryptography. As quantum computers look to accelerate the process of solving entanglement calculations, they simultaneously speed up the process of cracking current encryptions that would undermine national and international data transmission. To put it into perspective, factoring is an aspect of encryption processes that are very complex when it comes to choosing the appropriate set of lengths and calculations of bits. A classical CPU realistically could take 10^145 years to factor a 1,024-bit number or 7.25 x 10^135 times the age of the universe (Mashatan et al., 2021). If this was the calculation required

to crack a current encryption process method such as an RSA or AES signature, a quantum computer would be able to solve it within a fraction of the time it would take classical computers. The ability to resist encryption-breaking quantum methods is a must and one that needs progressively more research to be conducted in the field of cybersecurity and quantum computing alike. While there are laboratories such as the National Institute of Quantum and many alike in physics and computer sciences that have in-depth research and data in the field of quantum mechanics there isn't enough technical background understanding of both quantum computing and cryptography as there should be.

Currently, most organizations are not aware of the implications of quantum computing and cryptography as elucidated in *The Complex path to quantum resistance*. As quantum reality becomes readily available with time the current standardized cryptographic baselines that can be leaned on will become smaller (Mashatan et al., 2021). Governments and organizations alike need to have a regulatory framework and a plan in place to respond to calls for quantum vulnerabilities that will pose significant threats to current cryptographic frameworks that are in place. This comes with resources and research into quantum resistance algorithms such as efforts in place by NIST to produce quantum resistant algorithms in the field of encryption. The effectiveness to readily be prepared for the direct implications of quantum computing and its effects in the world of cryptography lies in the hands of both private and government organizations. The need to conduct progressive research and resources into the field before the ultimate dangers of quantum computing becomes a nightmare to handle all together without a sophisticated plan in place.

Literature Review

Post Quantum Cryptography: Directions For Future Research

The first research publication to be reviewed is from a group of researchers who have established themselves in the world of post-quantum cryptography. Post Quantum Cryptography maintains the position that the field of quantum computing paves a new era of computational power, which promises to solve highly complex problems that are far beyond the scope of current classical computers. The publication emphasizes the significant threats that quantum computing poses to cryptographic algorithms that would underpin the security of digital communications worldwide. In this comprehensive study, the article delves into the highly theoretical yet critical domain of post-quantum cryptography (PQC), an unfortunate reality is that the current techniques incorporated in cryptographic algorithms that rely on complex math problems will become extremely vulnerable and easy to break in the world of digital communications (Bavdekar et al., 2022).

The current symmetric cryptographic algorithms such as AES and 3DES's security will be cut in half with the use of Grover's algorithm, across the board quantum computing poses an unparalleled threat to this world of secure digital communications as never seen before. This publication provides an index of PQC algorithms, separating them into families based on their foundational approaches include lattice-based, hash-based, code-based, and isogency-based cryptography. Each family is thoroughly examined for its potential to offer quantum resistance, with the authors assessing their strengths, weaknesses, and open-ended questions that have yet to be solved. Based on the fundamental approach of quantum computers themselves the publication emphasizes the differences between classical and quantum computers, the concept of quantum computing itself is quite absurd due to its highly theoretical and conceptual frameworks such as

preposition, entanglement, and quantum uncertainty (Bavdekar et al., 2022). As explained by the publication, quantum computing measurement itself is the operation that would take in a qubit and then return what is considered a classical bit; if the qubit $< \psi >= \alpha|0> + \beta|1>$ is measured the probability of 0 or 1 would be returned yet right after that measurement all information about the qubit itself is lost and becomes classical (Bavdekar et al., 2022). The publication emphasizes the ability of various algorithms such as Grovers, Shors, and Simons to have their own mechanisms in place to crack classical computing mathematics. While the nature of the article is profound and lays significant groundwork for future research, it cannot be overstated that this is a theoretical framework and there are no groundbreaking advances or trends that occur overnight, and it would take several decades to develop a concrete framework.

Getting Ready for Post-Quantum Cryptography

For the second publication, following the exploration of quantum computing's potential impacts by Bavdekar et al., the focus is on the National Institute of Standards and Technology (NIST) publication. This publication provides a much-needed bridge between the theoretical underpinnings and practical implementation challenges of post-quantum cryptography (PQC). The article relies heavily on the operational, technical, and policy considerations that organizations must navigate in their steps to PQC. NIST believes that it will only take 5-15 years before governments start to see their highest security encryptions be breached with the use of quantum computing, the use of public-key cryptography needs to be identified by organizations to transition them to PQC resistance as soon as possible (NIST, 2021).

The necessity of a proactive approach in both research and implementation to assess classical cryptology methods along with quantum computing is of great importance. The article lays out a phased plan for adoption, including tracking current cryptographic systems,

prioritizing resources that are based on sensitivity and risk, and engaging in active participation in standardization efforts (NIST, 2021). NIST is aware they cannot predict when the capability of executing an algorithm like Shor's will be publicly available to adversaries but there needs to be preparation for it years in advance or there will be irreversible damage done NIST (2021).

The Impact of Quantum Computing on Present Cryptography

For the third and final publication, (Mavroedis et al., 2018) delve deep into both the theoretical and practical ramifications of quantum computing's emergence, which presents a nuanced view of the cryptographic landscape as it stands and its future as researchers and organizations continue to make progress. The publication outlines the foundational cryptographic schemes that are currently in use, including symmetric and asymmetric algorithms, as well as how these are potentially vulnerable to quantum computing's capabilities (Mavroedis et al. 2018).

There are several key challenges that the publication focuses on in quantum computing being that quantum algorithms are probabilistic, qubits can lead to errors, and difficulty of coherence in conceptuality as there can be two different variations of a qubit; phosphorous atom and an artificial atom which allows them to eliminate magnetic noise for more precise results (Mavroedis et al., 2018). The publication also emphasizes the need for critical analysis of various post-quantum cryptographic algorithms such as quantum key distribution (QKD) and other complex mathematical solutions like lattice-based cryptography, multivariate-based cryptography, hash-based cryptography, and code-based cryptography. The publication provides valuable insight into the field that helps bridge the gap between theoretical quantum computing aspects and the challenges it poses to classical cryptographic methods.

Conclusion

The impending ramifications of quantum computing requires a transformative era for cryptography, it will challenge the foundational security mechanisms and principles that underpin digital communications and data protection. This review synthesizes pivotal contributions from leading researchers and institutions, emphasizing the difficulty and power of quantum computing as both a technological leap and a formidable threat to cryptographic norms. The three publications that this paper has reviewed: Bavdekar et al. (2022), NIST (2021), and Mavroeidis et al. (2018) provided a comprehensive review of vulnerabilities present in cryptographic systems in the face of quantum advancements.

The collective insights from these publications illustrate the critical juncture in which the field of modern cryptography stands. The path forward as emphasized by the reviewed publications calls for proactive research and resources into the field of post-quantum cryptographic solutions, reevaluation of current cybersecurity protocols, and active engagement in new standards. The emerging threat of quantum computing in the field of cryptography cannot be encapsulated into a single document as it's widely agreed upon in all three publications. This requires the most prestigious physicists, academics, and researchers in both the fields of quantum, quantum computing and cryptography to choreograph a stable path forward in which society can answer imminent challenges and threats as well as answer complex problems yet to be solved.

Theoretical and Mechanical Framework

To get a better understanding of quantum computing, there needs to be a baseline of the mechanics and theoretical frameworks that encompass it. Quantum computing leverages various and complex unique properties revolving quantum mechanics, it separates itself from classical

computing very distinctively. The first property to understand is superposition, lightly speaking it's a qubit that is described by its probability to be either zero or one and not by a distinct understanding of the value to be zero or one (Rietsche et al., 2022). To understand this further we need to have knowledge of a qubit; it's a basic unit of quantum information that is inherently a copy of the classical binary bit which also recognizes two states, 0 and 1. The fundamental difference between classical and quantum computers is their ability to store information, so a qubit can either have the probability to be 60% zero and 40% one (Rietsche et al., 2022, p. 2527).

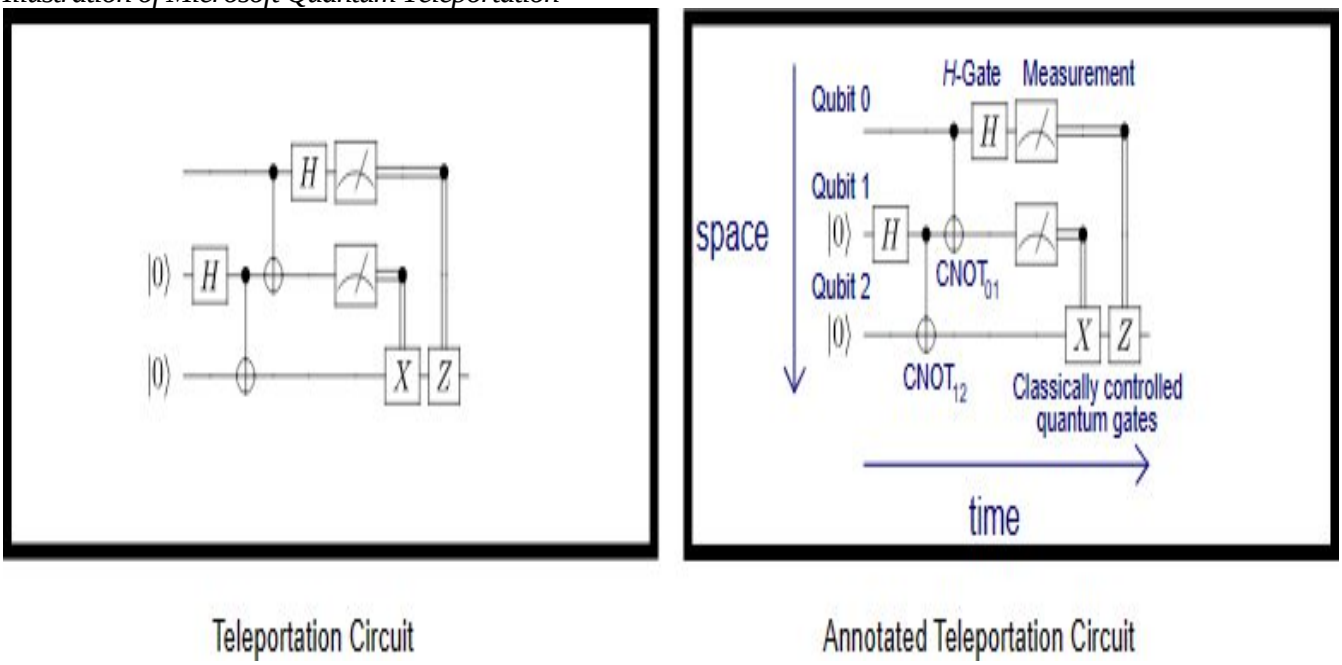
This is partially what makes quantum computers far more efficient and powerful than classical computers, their ability to leverage various mechanisms such as superposition, interference, and entanglement to perform various actions in a matter of a second or less is what makes them far more powerful than classical computers. It allows researchers, academics, and scientists alike to find the exact result value rather than having to test millions or billions of various functions and algorithms to end up with a nearly precise value. There's another mechanism that's extremely vital to understand, which is entanglement.

A common understanding of entanglement is when a qubit is under certain influences such as the measurement of the qubit's state or even when they are separated. The advantage is that these qubits will work together to arrive at the exact solution together; this is the overarching difference between classical bits and qubits (Rietsche et al., 2022). The ability for the solution to arrive at either 0 or 1 based on the algorithm or functions is what separates quantum computing from classical computing. Its ability to solve extremely complex problems in a fraction of the time it would take classical computers is the threat it inherently creates to modern cryptography and the techniques that rely on classical mathematical functions and computing. A visual

understanding of how qubits can display a changed state while providing accuracy can be observed in figure 1 below.

Figure 1 Microsoft Quantum Teleportation

Illustration of Microsoft Quantum Teleportation



Teleportation Circuit Annotated Teleportation Circuit

Note: Figure 1 demonstrates the process of a qubit's quantum state being changed within a quantum computer without needing to know the qubit's exact values using superposition and various other quantum mechanisms.

Quantum Threats to Cryptography

The ability to create relentless breakthroughs in research, academics, technology, medicine, and several other fields is what makes quantum computing such an important and imposing field. Its unparalleled power in leveraging quantum principles such as superposition and entanglement to process data in ways that classical systems simply cannot is the direct threat it poses in the field of modern cryptography. This leap in processing power, while allowing new scientific and technological advances, poses a significant threat to the modern cryptographic frameworks that safeguard digital communications and data privacy. To understand the impacts

of quantum computing in the field of cryptography it is important to understand various quantum algorithms and the advantages they provide case by case, the two algorithms that will be of focus are Grover's and Shor's algorithms. Traditional cryptographic methods are often built on mathematical equations that are far too complex for classical computing, this allows highly advanced algorithms such as Grover's and Shor's Algorithms to be leveraged in solving these complex cryptographic methods in a fraction of the time it would take classical computing (Grimes, 2020). To come to any understanding of what these algorithms can achieve, understanding encryption processes is necessary and what makes current models futile with the involvement of quantum computers.

Encryption itself, specifically through symmetric and asymmetric ciphers serves as the bedrock for securing digital communications by translating readable data into an unreadable format for obfuscation purposes. Except for those that hold the specific keys to decrypt the messages back to their original plaintext format. This is where symmetric ciphers that use the same key for both the process of encryption and decryption make them fast, efficient, and easy to validate (Grimes, 2020). They are the cornerstone of data encryption due to robustness and simplicity with Advanced Encryption Standard (AES) being the most respected symmetric cipher since its creation. On the other hand, we have asymmetric ciphers that emerged for the purpose of solving the limitations of symmetric key distribution by using a pair of keys, public and private for encryption and decryption (Grimes, 2020).

The asymmetric approach allows secure digital communications over untrusted networks by making sure only the holders of the paired public and private keys can decrypt the messages using the same public key to ensure confidentiality for digital signatures. There are popular asymmetric methods such as RSA which heavily rely on difficult factoring of large prime

numbers but provide a foundation for effective and secure digital communications and make them vulnerable to the power of quantum computing advancements by algorithms such as Grover's and Shor's.

The importance of further research and testing with additional quantum computing algorithms cannot be understated, the impact of algorithms such as Grover's and Shor's paves the path to a new era of traditional cryptographic algorithms that require more time and resources than one person can provide. Shor's algorithm, which was first introduced in 1994, specifically has a significant interest in the realm of quantum computation and cryptography. The algorithm addresses two major problems; the first being the ability to factor a large integer into its prime factors and then the ability to find the discrete logarithms over finite groups which is the security focus of RSA, Diffie-Helman and DSA cryptosystems (Kim, 2021). It's an extremely complex algorithm but has some of the greatest implications as its ability to easily decrypt data with RSA by its ability to factor large prime numbers in a fraction of the time it would take classical computers makes it a formidable algorithm.

There has been extensive research specifically on Shor's Elliptic Curve Discrete Logarithm Problem (ECDLP), this is an advanced method of Shor's baseline algorithm that allows researchers through mathematical analysis to use quantum resource estimate simulators to consider fault-tolerant quantum computation (FTQC). This allows them to account for more accurate estimates such as the control of qubits, registers, reduction, and reuse for the algorithms result case efficiently (Kim, 2021). Shor's algorithm is one of the more complex conceptual and theoretical algorithms involving cryptographic systems but lays a heavy burden on modern encryption standards that are unable to be cracked so far, a model for further techniques and implementations can be seen in figure two below.

Figure 2 Shor's Aglorithm (ECDLP)

Illustration of Shor's algorithm for (ECDLP)

Table 1. Mapping of techniques for realizing Shor's algorithm for Elliptic Curve Discrete Logarithm Problem (ECDLP)

No.	Authors	Year	Main/Notable contribution	ECC level	Finite field	Field basis	Curve choice	Coord.	Algorithm for arithmetic circuit	Metrics	Platf. (Lang.)	QC provided?
1	Eicher & Opoku[8]	1997	- Algorithm-level analysis and description on how Shor's ECDLP works -Provide example of Shor's ECDLP on Massey-Omurra cryptosystem -Provide walkthrough example of Shor's algorithm ran four times	on whole Shor's ECDLP	$GF(2^m)$ (example purpose)	–	SW	–	–	–	–	–
2	Proos & Zalka[15]	2003	- First detailed description of PM and PA + simplify addition rule + replace QFT with semiclassical QFT (baseline for recent methods) - Rough resource estimates - First to show that ECC is crackable sooner than RSA	Level 1–3	$GF(p)$	B	SW	A	- PM: R-L Double-and-Add using classically precomputed points - FI: standard Euclidean algorithm - FM: multiplication by doubling + conditional addition	#qubits, time (depth) in "1-qubit addition" unit	-	Description only
3	Kaye [13]	2004	- Adopt PZ for binary curves - Describe naive and optimized implementation of extended Euclidean algorithm	Level 1–2	$GF(2^m)$	P	SW	A	- PM, PA: follow PZ - FI: extended Euclidean algorithm for Ps, also describe long division circuit	#qubit	–	Yes, figures + description
4	Cheung et al. [7]	2008	- Propose linear-depth FM using adopted classical Mastrovito multiplier in projective coordinate	Level 1	$GF(2^m)$	P	SW	SP	- PM: Double-and-Add -PA: Not specified - FM: Adopted classical Mastrovito multiplier	Toffoli + CNOT gates	–	Yes, example figures + description
5	Maslov et al. [14]	2009	- Description of FM in for Linear Nearest Neighbor architecture (lower than logical-level implementation)	Level 2	$GF(2^m)$	P	SW	SP	- PM: Double-and-Add - PA: Not specified - FM: follow Cheung	Circuit depth	–	Yes
6	Amento et al. [1]	2012	- FI using different basis representations to reduce depth - Resource estimates	Level 1	$GF(2^m)$	GH, GNB	–	–	- FM: Ghost-bit basis, Gaussian normal basis -based multiplier - FI: Itoh-Tsujii	Rough circuit depth and gate count (Toffoli + CNOT gates)	–	Yes, figures + description

Note: Figure 2 provides several techniques and their respected authors in understanding various cryptosystems that can be leveraged with Shor's algorithm and their efficiency of resources in a curve that would yield precise results.

The next algorithm of focus is Grover's algorithm, founded by Lov Grover in 1996 it stands out as an essential quantum algorithm due to its ability to search unsorted databases and its potential implications on symmetric cryptography. In classical computing it requires on average, $M \leq N/2$ attempts which, in contrast to Grover's algorithm, can use quantum superposition and entanglement mechanisms to search a database in $\sqrt{N}$ operations. This represents a drastic speedup in quadratics. When Grover's algorithm is applied to a block cipher (SDES) it showcases its ability to search for encryption keys. A classical brute force attack would require 2^k attempts to match every key available. This makes it extremely difficult to

attempt every key possible. Yet Grover's algorithm could theoretically half this to √(2^k) = 2^(k/2) attempts, which halves the key's bit strength overall (Denisenko et. al, 2019). In other words, if a classical encryption process was using a secure 256-bit key, Grover's algorithm would turn its security equivalent to 128 bit key, with the assumption that an attacker has the proper quantum computational resources to carry out this algorithm efficiently.

If a certain function is defined as f(x) = 1 and the element within the set with a number x satisfies the search criteria, using quantum oracles complexity order of O(N/M) then a Grover's quantum algorithm has the complexity of O√N/M when solving this problem with a quantum computer (Denisenko et. al, 2019). Grover's algorithm uses quantum superposition to assess every possible input and series of quantum operations using the "Oracle" method can identify the correct input out of all the possible input's that result. It enables quantum computers to simply collapse the correct answer within the measurement frame within the assumption the correct functions and lengths are being used. The ability for Grover's algorithm to halve the time it takes to crack a classical 256-bit key with the use of qubits, superposition, entanglement, and other quantum forces poses a significant threat to modern encryption methods. While this may not be an immediate threat, as there's further development by research institutions and organizations there will be far more pressure to reevaluate key sizes that are used for modern symmetric ciphers to maintain proper digital communications and security.

Empirical Analysis Through Simulation

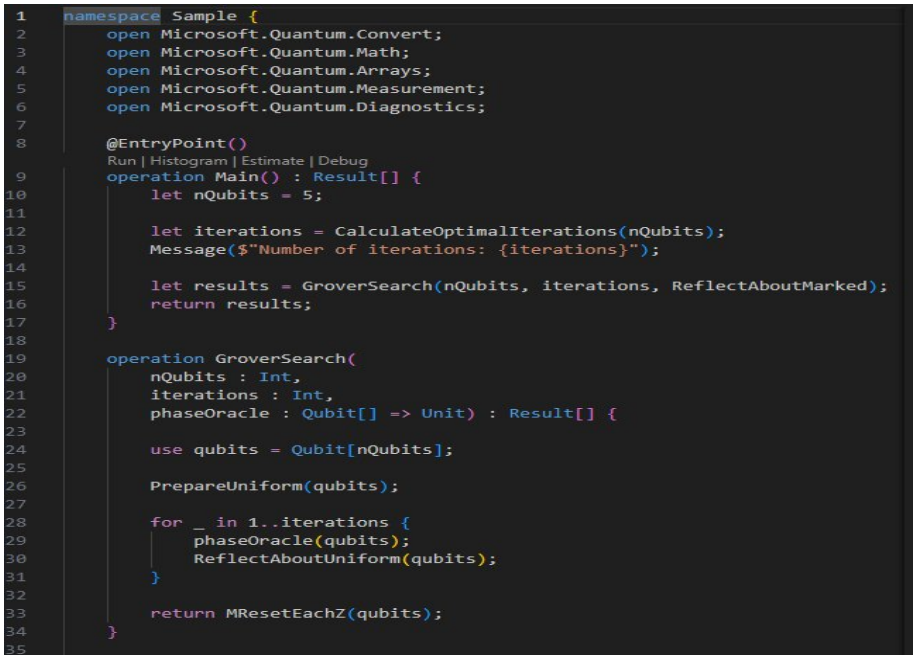
Considering the massive number of resources and capital required to operate a quantum computer, let alone the feasibility to access one for simulation cryptography testing, this paper leverages publicly available quantum resource simulators provided by Microsoft corporation to gather and assess empirical data relevant to quantum algorithm's accuracy and cryptographic

methods. As we move towards a timeline that involves more research in the field of quantum, there are more organizations that are willing to offer free and publicly available quantum simulation models for testing such as IBM, Google and Microsoft, this list will hopefully continue to grow as this field becomes more practical for solving numerous problems that are untouched today. To evaluate the impacts of quantum algorithms on cryptographic systems, this research employs an environment provided by Azure Quantum. Azure quantum leverages the capabilities of Q#, an open-source quantum programming language that's optimized for developing and testing quantum algorithms (Microsoft, 2024). Using Q#, research is conducted using a theoretical implementation of Grover's algorithm and simulation of the results will provide insight into potential vulnerabilities within cryptographic methods when faced with the power of quantum computation.

To gain a better understanding of how powerful quantum computing systems are, the following simulation and shot results are performed using Quantinuum's H-Series Emulator which uses a realistic noise model and set parameters for a System Model H1 20-Qubit system, it allows for simulation of quantum circuits on a classical computer without the need for actual quantum hardware (Microsoft, 2024). The Q# code developed implements Grover's algorithm for quantum search, it provides a square root speedup for specific search problems the entry point for the program defines the number of qubits (**'**nQuibits') to be used in the search and calculates the optimal number of iterations required for Grover's algorithm based on the number of qubits. It proceeds to run the Grover search with a phase oracle operation that marks the correct item to find; Grover Search operation initializes the qubits to a uniform superposition state using Hadamard gates and then applies the Grover iteration for the specified number of times. Refer to figure 3 below for visual understanding of the layout of the program so far.

Figure 3 Part 1 Q# Program

Part 1. Of Q# program illustrating use of Grover's algorithm



```
namespace Sample {
    open Microsoft.Quantum.Convert;
    open Microsoft.Quantum.Math;
    open Microsoft.Quantum.Arrays;
    open Microsoft.Quantum.Measurement;
    open Microsoft.Quantum.Diagnostics;

    @EntryPoint()
    Run | Histogram | Estimate | Debug
    operation Main() : Result[] {
        let nQubits = 5;

        let iterations = CalculateOptimalIterations(nQubits);
        Message($"Number of iterations: {iterations}");

        let results = GroverSearch(nQubits, iterations, ReflectAboutMarked);
        return results;
    }

    operation GroverSearch(
        nQubits : Int,
        iterations : Int,
        phaseOracle : Qubit[] => Unit) : Result[] {

        use qubits = Qubit[nQubits];

        PrepareUniform(qubits);

        for _ in 1..iterations {
            phaseOracle(qubits);
            ReflectAboutUniform(qubits);
        }

        return MResetEachZ(qubits);
    }
```

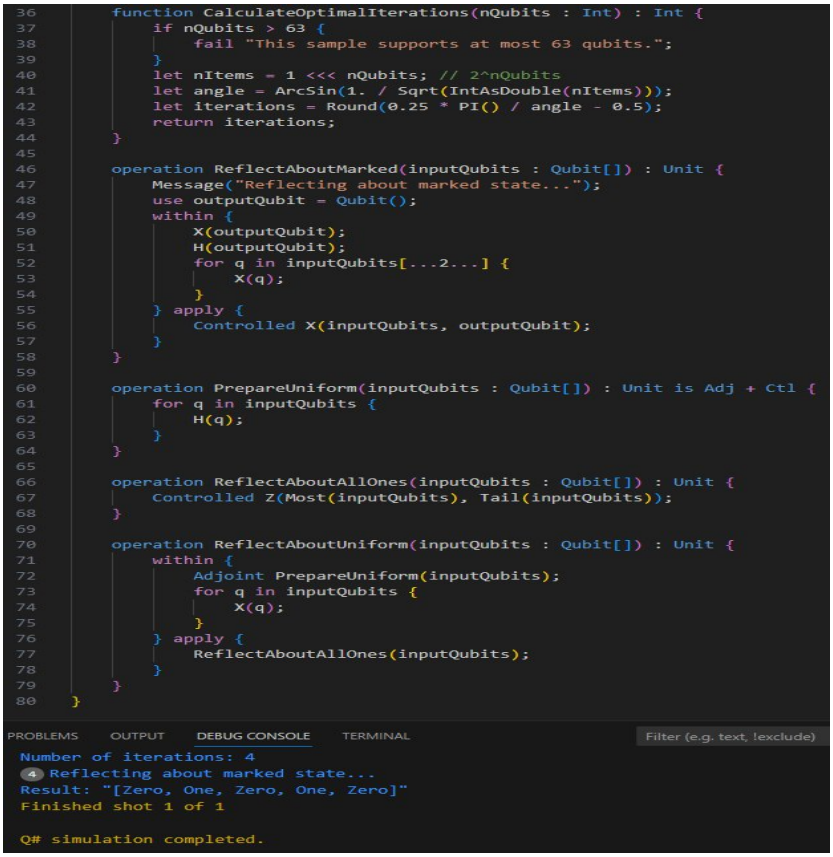
Note: Figure 3 illustrates part 1 of the program illustrating use of Grover's algorithm leveraging Azure Quantum Development kit to create a theoretical testing sample leveraging Q#.

Please refer to the Q# program code in the figure below as it continues by using the 'CalculateOptimalIterations' function which calculates the number of iterations that are needed for the Grover search algorithm to maximize the probability of finding the target item. As we work down the program itself, there is a use of 'ReflectAboutMarked' operation which marks the target state in the context of Grover's algorithm, this is the function that flips the phase of the state that corresponds to the solution. The program then uses 'PrepareUniform' operation that applies Hadamard gate to all the qubits and creates a superposition of all the possible states. And finally, the operations 'ReflectAboutAllOnes' and 'ReflectAboutUnifrom' implement Grover diffusion operator which amplifies the amplitude of the marked state. This program using Quantinuum's H-series Emulator can provide a theoretical framework for Grover's algorithm

and the results that are produced can be seen below in figure 4. The algorithm was tasked to run for four iterations which is a number calculated based on the size of the search space. Each iteration of Grover's algorithm within the program carefully inverts the phase of the state representing the solution and then amplifies to all other states. As referenced in the figure below, this is based on a 100-shot sample testing using Quantinuum's H-series Emulator which resulted in a 100% chance of the result search sequence shown.

Figure 4 Part 2 Q# Program

Part 2 of Q# program illustrating the use of Grover's algorithm and results.



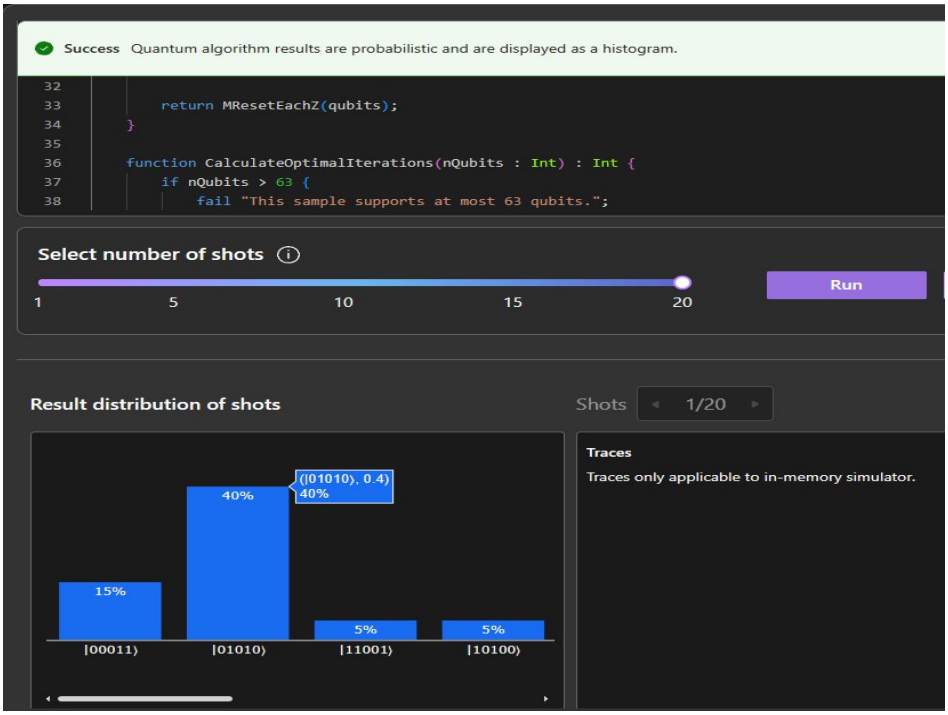
Note: Figure 4 illustrates part 2 of the Q# program showcasing the second half of operations and functions used within as well as the 100-shot result simulation.

Based on the output that's seen below in figure 5 is a simulation result, this was based on a 20-shot testing for the highest probability which resulted in '**Zero, One, Zero, One, Zero'** this

indicates the actual measurement result of the quantum state after completing algorithm's iterations. Each "Zero" and "One" corresponds to the measured value of a qubit as discussed earlier, this binary sequence of 01010 is what the quantum search algorithm has identified as the outcome with the highest probability after the Grover iterations, indicating this is the most likely solution to the search problem based on 20-shot's which resulted in a 40% probability of being the same sequence solution and 100% probability based on 100-shots as seen in figure 4. The number of shots is a reference to the number of times the quantum circuit is executed on a quantum computer (Microsoft, 2024).

Figure 5 20-Shot Histogram Results

Illustration of 20-shot histogram results of running quantum program.



Note: Figure 5 showcases the test results of testing the Q# program using 20-shot distribution using Azure Quantinuum's H-Series Emulator.

Given that a single execution was simulated, the result is very consistent with the expectation of Grover's algorithm that produces a high probability of finding the target state

within a square root of the total number of iterations compared to classical search algorithms. The figure above which illustrates a histogram result for distribution of 20-shots is based on probabilistic nature of quantum computing simulation the highest probability which is 40% as seen is the same result running the program on a 100-shot sample and sequence result being the exact same. This algorithm showcases the power of quantum computing's ability to efficiently search through unsorted database which has massive implications for cryptography, this can be used to speed up the search speed for a secret key in symmetric encryption schemes. While the empirical test results are identical, the purpose of these tests are to showcase the power of Grover's algorithm when implemented with a much larger and more efficient program using realistic quantum computer. The tests conducted are to provide a theoretical framework for understanding the functionality of Grover's algorithm within the scope of cryptography in a small sample size. The tests were successfully conducted thanks to the publicly availability for academics and researchers to leverage Quantinuum's H-series Emulator and Azure Quantum resources for simulation of Q# program testing.

For the next methodology of testing, this research leveraged Azure Quantum Resource Estimator which is a powerful analytical tool that models requirements for running quantum algorithms on a quantum computer that doesn't yet exist and is under development (Learn Microsoft, 2024). This application allows researchers in the field of cryptography to understand and test results that are particularly vital for understanding the potential for quantum computing to break current encryption methods. To assess the quantum threats that persist to current cryptographic standards, this research with the help of Azure Quantum Resource Estimator will use the robust mechanisms in place that are provided by Microsoft Corporation to project the capabilities of a large scale and fault tolerant quantum computers that are able to project millions

of qubits which puts a strain on current encryption methodology. This methodology involves inputting several different cryptographic algorithms into the Resource Estimator along with various key strengths, qubit types and error rates that will produce a matrix of results to reflect the number of physical qubits and runtime needed by a quantum computer to break encryption.

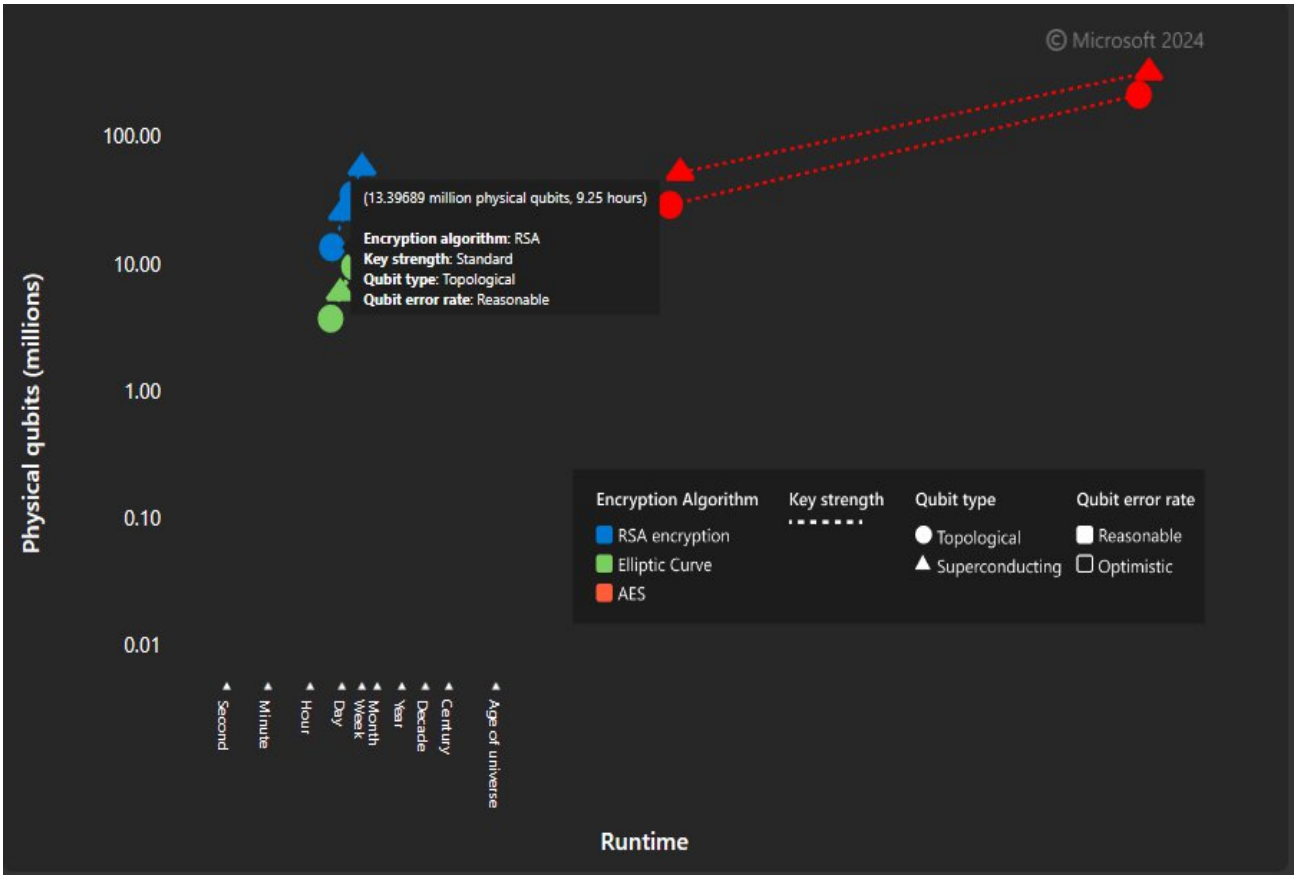
By using Quantum Resource Estimator, we can simulate the computational resources required to compromise RSA and Elliptic Curve encryption while leveraging Shor's algorithm which would require several millions of physical qubits and runtime spanning several hours to days to render encryption methods obsolete (Learn Microsoft, 2024). For the testing to take place there are several key parameters that need to be in use based on the options that are available. In this research the parameters in use will display three encryption algorithms in play, RSA, Elliptic Curve, and AES (Symmetric). For the purpose of this testing, the key strengths parameters chosen will stay 'Standard' through the testing and these include RSA: 2048, ECC: 256, and AES: 128 while there are options for both 'Enhanced' and 'Highest' the baseline for the strengths will stay consistent to what's widely used and available in modern day encryption methods globally. For Qubit Type parameters, researchers are given the options for Topological and Superconducting, these are the building blocks in quantum computers based on future scaled quantum machines, standard and advanced qubit types. Finally, only one qubit error rate will be selected with two being available, reasonable, and optimistic, these qubit error rates will be prone to errors even in scaled quantum machines and will vary for better or worse for reduction of errors.

Using Azure Quantum Resource Estimator, we were able to simulate results with the baseline strategy for testing, keep the parameters as standardized as possible to best reflect the number of physical qubits, runtime and Shor's algorithm's impact on modern encryption

methods using future quantum computers to break encryption algorithms. The parameters that are selected are RSA, Elliptic Curve, AES, Standard and Highest key strength, Topological and Superconducting qubit types, and reasonable Qubit error rate. Please refer to figure 6 below based on the testing results that were collected, as shown resource estimator evaluated the resilience of RSA, Elliptic Curve and AES against quantum attacks powered by Shor's algorithm under standard and highest key strengths to showcase the standard and best-case speeds required. First, the focus was on RSA Encryption as shown in the figure below. While the results based on the legend provided showcase results for both standard and highest key strength, the focus is on standard as well as topological qubit types.

Figure 6 Resource Estimator

Illustration of Azure Quantum Resource Estimator Results



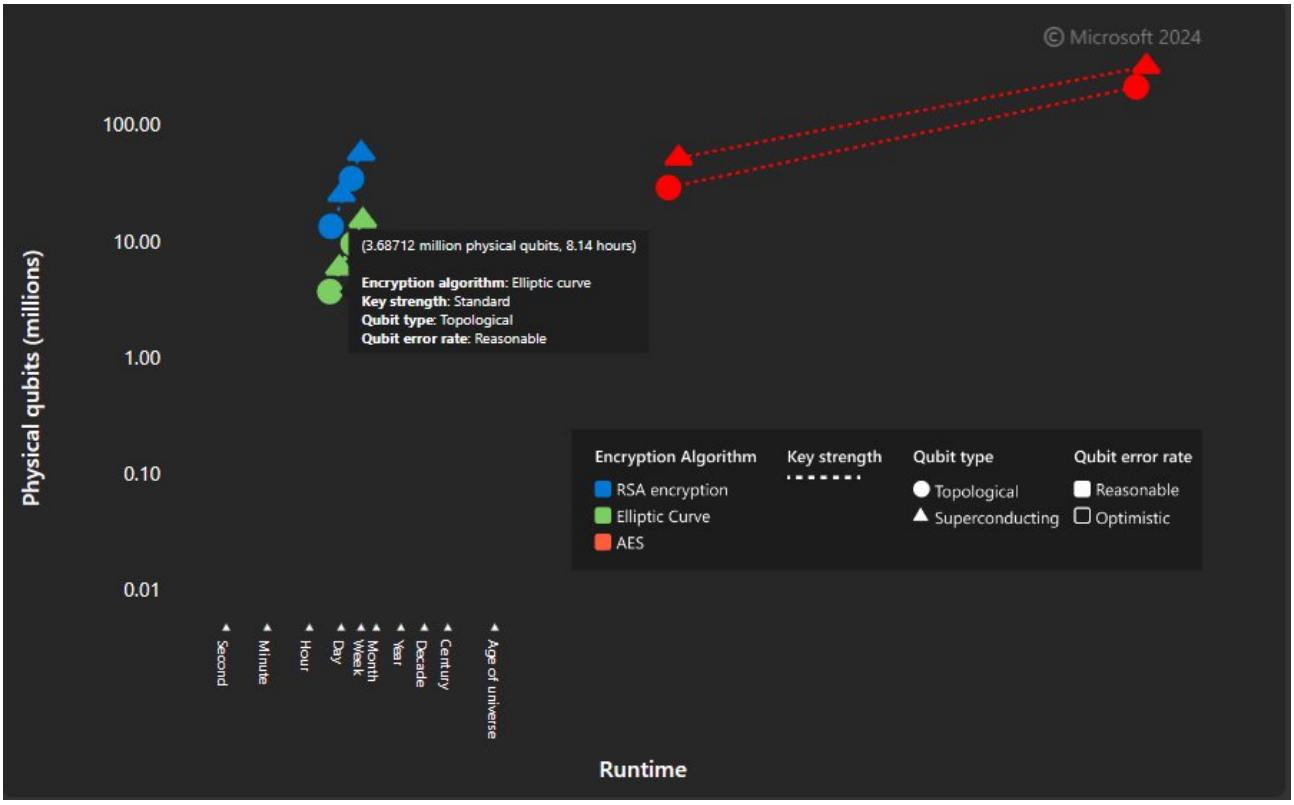
Note: Figure 6 is an encapsulation of the overall quantum resource estimator results using the parameters specified for testing of physical bits, key strength and time required to break RSA encryption.

For RSA Encryption with a standard 2048-bit key as shown in figure 6, the Resource Estimator projects that a quantum computer would require approximately 13.3698 million physical qubits and a runtime of just over 9 hours to break the encryption. This reveals a considerable threat posed by quantum computing to a encryption algorithm that is widely considered to be secured by today's standards. Even with the key strength set to highest, or 4096-bit key strength the amount of time would take is roughly 3 days with 34.5 million physical qubits required using only topological qubit types.

As show in figure 7 below using resource estimator and keeping the parameters consistent with the testing of RSA encryption, the results indicate that for Elliptic Curve encryption algorithm using topological qubit type a quantum computer with these capabilities would need about 6.3872 million physical qubits and a runtime of approximately 8.14 hours. As shown in figure 7 this raises significant considerations for the resilience of Elliptic Curve algorithms leveraging Shor's algorithm. Elliptic Curve cryptography (ECC) is currently considered one of the more robust encryption methods available due to its smaller key sizes and computing efficiency, while ECC based on the results shows it has advantages over RSA in the classical context, it still falls within a reasonable attack range for a quantum computer. The test results also included the highest key strength for ECC, and it would require 9.42 million physical qubits and roughly 3.34 days for a quantum computer with the capabilities leveraging Shor's algorithm to break Elliptic curve encryption. Refer to figure 7 below for the test results using quantum resource estimator referencing the physical bits and runtime that would be required to break the encryption algorithm.

Figure 7 ECC Results

Illustration of Azure Quantum Resource Estimator Results



Note: Figure 7 showcases the test results when using resource estimator to understand the number of physical bits and runtime required to break ECC algorithm.

Finally using Quantum Resource Estimator this research was able to gather results on Advanced Encryption Standard (AES), which would require a monumental quantum effort to decrypt naturally. The projections that are presented in figure 8 below using standard key strength conditions showcase that a quantum computer would need approximately 288.8757 million physical qubits and a duration that would span centuries of runtime when leveraging topological qubits with a reasonable error rate present. The number of resources required to underscore the robustness and efficiency of AES in the face of quantum decryption capabilities suggests the uphill challenge for even advanced quantum computers to break. Compared to RSA

and ECC encryption algorithms, AES displays a resistance that leaves the other methods in the dust with reasonable quantum computer attacks. The estimated number of requirements are on a different level playing field for a quantum computer to break AES, which reinforces its position as a pillar of strength in the encryption landscape. The simulation suggests that AES, when implemented with standard encryption key would remain extremely resilient against quantum attacks for far longer than its public key teammates. The empirical analysis conducted through simulation, leveraging both Grover's algorithm and Shor's algorithm via Azure Quantum resources highlights the emerging quantum threats to cryptography and the necessity for quantum safe research and practices. The simulation test results for RSA, Elliptic Curve, and AES offers a new perspective on which researchers can understand the readiness of the current cryptographic standards in the face of advanced quantum computing systems and will help lay the groundwork for Post-quantum Cryptography (PQC).

Figure 8 AES Results

Illustration of AES Resource Estimator Results

Note: Figure 8 showcases the results when using resource estimator for the physical qubits and runtime needed to break AES encryption standards.

Quantum Resistant Cryptography

As quantum computing systems continue to be tested and developed, the cryptographic landscape faces immense challenges to overcome. Currently with classical computing most organizations do not have the capabilities to adapt to new cryptographic ventures and algorithms without modifying current system infrastructure. Because of this, organizations do not have control over their own cryptographic infrastructure and processes without increased manual effort (NIST, 2021). The need for Post Quantum Cryptography (PQC) is an essential defensive strategy that requires just as much effort and research as quantum systems continue to evolve. PQC is a significant topic to various organizations such as IBM, Google, Microsoft and NIST who are on the frontlines for developing post quantum public key cryptographic standards.

There are various challenges that the development of working PQC algorithms face as classical cryptographic methods continue to be developed and will take at least 5 to 15 years before the publication of these cryptographic standards are fully completed (NIST, 2021). Despite this, there is significant research and work being conducted on specific approaches for post quantum systems in the face of cryptographic standards. These include Goppa code-based encryption, Lattice-based encryption, Lattice-based signatures, Multivariate-quadratic equation signatures and many more that are being encouraged to be developed and researched (Bernstein & Lange, 2017). The development and research of PQC algorithms heavily relies on the challenges of quantum algorithms such as Shor's and Grover's algorithm as seen throughout this research. Code-based encryption requires highly reliant computer systems that have specific logical data and physical memory that can handle error correcting codes using 'generator matrix'

for 64x72 matrix of bits that uses codeword positions to determine the rest of a codeword (Bernstein & Lang, 2017). While Lattice based encryption is of great importance, attackers have been identified using a cyclotomic structure of x^p-1 to break specific lattice-based cryptosystems with the addition of Shor's algorithm (Bernstein & Lang, 2017).

The PQC algorithms are extremely complicated and are constantly being developed and require large amounts of resources and expertise to devise accurate PQC algorithms for when the time comes. The importance of being PQC safe is also of great importance to government organizations such as CISA and NSA that have partnered with NIST to establish a quantum readiness process for post quantum cryptography migration. This collaboration effort highlights several key strategies, including the need to prepare now to proactively prepare for future migration into PQC standards. This also includes a quantum-readiness roadmap that highlights the need for having an inventory of cryptographic inventory for helping organizations become aware of their infrastructure and by making it easier to transition when the time comes (Depart of Defense Cyber Crime Center, 2023). The path to quantum resistance is a massive uphill battle that requires unparalleled amounts of resources, research, and patience to have the most efficient PQC algorithms and response plans in place by organizations to be prepared for when the time comes.

Conclusion

In conclusion the influence of quantum computing in the realm of cryptography and classical computing standards is quite understated. Through the lens of Grover's and Shor's algorithm we were able to understand the importance of these algorithms in the world of cryptography and the direct impact they will have as quantum computing systems continue to evolve. Using Azure Quantum In-Memory Simulator and Quantum Resource Estimator we were

able to conduct and gather important empirical data on the vulnerabilities of standard encryption methods such as RSA and ECC algorithms to quantum attacks, while also showcasing the formidable resilience of AES encryption. We stand in a critical juncture in the world of computing and technology as we face another threat alongside quantum computing that poses just as great of a challenge in combination, this is the emergence of artificial intelligence applications and systems. This stage of technological evolution will define the rate of evolution and reshape the way organizations, researchers and leaders will be able implement drastic changes to the world as we know it. As A.I. is put on a pedestal by organizations around the world the ultimate need for quantum A.I. adoption will be required. The hybrid model of quantum A.I. solutions would drastically speed up testing, research, and development of commercialized quantum A.I. solutions that will have a direct impact on computing and research (Brin & Viggiano, 2023).

We stand facing unparalleled technological advances at the forefront as humanity continues to shock itself in what can be accomplished. As evident with the rise of classical computers in 1959 there will ultimately be repercussions of these advances that need to be accounted for, so that we do not look foolish repeating the same mistakes twice on a larger scale. While quantum computing systems are partially futuristic, these systems currently exist and will continue to evolve as technology and research is advanced. There is a monumental danger at the cost to the ecosystems of cybersecurity and cryptography that highlights the need for quantum resistant computing and PQC's which will need to be further developed. This research would not be possible without the countless amounts of research and tools made available by researchers and organizations that are leading this forefront in the right direction. The stakes that are in play are far too great to ignore based on the impending consequences. This research study

aims to encapsulate the significance and necessity for continuing research in the evolving field of quantum computing and cryptography.

References

Rietsche, R., Dremel, C., Bosch, S. et al. (2022). Quantum computing. Electron Markets, 32, 2525–2536. https://doi.org/10.1007/s12525-022-00570-y

Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., Daniel, S. J., & Atul. (2022). Post Quantum Cryptography: Techniques, Challenges, Standardization and Directions for Future Research. arXiv:2202.02826v1 [cs.CR].

Microsoft. (2024). Quantum circuits [Figure 1]. *Microsoft Azure*. https://learn.microsoft.com/en-us/azure/quantum/concepts-circuits

National Institute of Standards and Technology. (2021). Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms. https://doi.org/10.6028/NIST.CSWP.04282021

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, 9(3). https://arxiv.org/pdf/1804.00200.pdf

Grimes. (2020). *Cryptography apocalypse: preparing for the day when quantum computing breaks today's crypto* (1st edition). https://doi.org/10.1002/9781119618232

Denisenko, & Nikitenkova, M. V. (2019). Application of Grover's Quantum Algorithm for SDES Key Searching. *Journal of Experimental and Theoretical Physics*, *128*(1), 25–44. https://doi.org/10.1134/S1063776118120142

Kim. (2021). Quantum Cryptanalysis Landscape of Shor's Algorithm for Elliptic Curve Discrete Logarithm Problem. In Information Security Applications (Vol. 13009, pp. 91–104). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-89432-0_8

Wim van Dam, Mykhailova, M., & Soeken, M. (2023). Using Azure Quantum Resource Estimator for Assessing Performance of Fault Tolerant Quantum Computation. *arXiv.org*. https://doi.org/10.48550/arxiv.2311.05801

Microsoft. (2024). What is Azure Quantum? - Azure Quantum | Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum#what-is-hybrid-quantum-computing

Microsoft Learn. (2024). Introduction to resource estimation. Retrieved from https://learn.microsoft.com/en-us/azure/quantum/intro-to-resource-estimation

Gerjuoy. (2005). Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers. *American Journal of Physics*, *73*(6), 521–540. https://doi.org/10.1119/1.1891170

Bernstein, & Lange, T. (2017). Post-quantum cryptography. *Nature (London)*, *549*(7671), 188–194. https://doi.org/10.1038/nature23461

Department of Defense Cyber Crime Center. (2023). Quantum Readiness. Retrieved from https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF

David Brin, & Greg Viggiano. (2023). *Convergence: Artificial Intelligence and Quantum Computing*. Wiley. Retrieved from Convergence: Artificial Intelligence and Quantum Computing (oreilly.com)

Atefeh Mashathan & Douglas Heintzman. (2021). *The complex path to quantum resistance,* Vol. 64, Issue 9, pp 46-53. ACM Digital Library. https://dl.acm.org/doi/10.1145/3464905