IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

Decrypting the Future: Quantum Computing's Role in Modern Cryptography

Yashwant Shukla

Dominion Energy Services Inc, Cayce - SC, USA

Abstract: Quantum computing is new advancement of computer technology. Now with quantum computing we will achieve great computational capabilities which can handle very complex tasks easily which are very difficult for regular computers. Quantum computing is transforming today's technology by offering massive computational capabilities that can handle problems which are very difficult for regular computers. In this paper we will explain the influence of quantum computing on existing cryptography. Also, we will focus on both the obstacles and the positive prospects of quantum computing. We will cover many challenges of quantum computing like the need for effective error correction techniques, scaling the technology, preparing required hardware, and constructing innovative quantum algorithms. On the brighter side, quantum computing holds the great potential to improve cryptographic security through the formation of quantum-resistant algorithms, quantum key distribution, and enhanced problem-solving abilities. Furthermore, this paper addresses the ethical issues and security risks linked to quantum computing. It also uncovers insights into the future of quantum computing and its capacity to transform cryptography, and the pressing necessity to apply post-quantum cryptographic standards. We will talk about real world issues and what other sections of world are doing to defend against security risks due to quantum computing. This paper also details what kinds of research leading organizations are doing to take advantage of quantum computing. In addition to investigations aimed at enhancing cryptographic algorithms, efforts are being made to address concerns regarding the potential vulnerabilities of established cryptographic systems such as RSA, AES, and ECC.

Keywords: Quantum computing, Cryptography, Quantum Algorithms, Quantum Error Correction, Quantum Supremacy.

I. INTRODUCTION

Researchers and scientists are constantly striving to enhance modern computer capabilities by leveraging advancements in material physics and applied mathematics. This includes ongoing improvements in semiconductors, discovering new methods to increase the efficiency of storage device materials, and developing better algorithms through mathematical formulas.

Major breakthroughs in quantum mechanics have been utilized by researchers and scientists to improve computer capabilities, leading to the emergence of cutting-edge computational devices are referred as quantum computers. These devices are exceptionally fast and capable of performing millions of operations with remarkable accuracy in significantly reduced timeframes. This prompts the inquiry of whether this speed could be misused to dent current security algorithms, which are fundamentally mathematical formulas designed to secure information through encryption.

Current cryptographic algorithms can be easily compromised if the key numbers involved in the calculations are known. Consequently, an individual could execute a program on a computer to explore all possible number combinations to deduce the key information. However, the extensive size of the keys employed in these calculations complicates this process. Without knowledge of the keys, standard computers would take years to arrive at the correct key. To enhance security, regularly changing the encryption keys necessitates that the computer restarts its prediction processes. Thus, by adhering to effective security measures, such as timely key updates and ensuring a minimum key length of 256 bits, it becomes virtually impossible for an interceptor or computer to successfully crack the encryption.

With the emergence of quantum computers, researchers have developed various algorithms designed to optimize the efficiency of these computers by effectively utilizing quantum computer hardware. The enhancement in computational power between classical and quantum computers is so significant that they can now process millions of iterations in few seconds. This is a primary reason how quantum computers can potentially decipher encryption keys even before users opt to change them.

Given the continuous increase in data, quantum computers are essential for efficiently retrieving information and performing complex calculations on large databases, which will greatly enhance human life. However, if such power falls into the wrong hands, it could be exploited to compromise data security. Consequently, researchers and scientists worldwide are focused on advancing quantum computing capabilities. Simultaneously, efforts are underway to develop

DOI: 10.17148/IJARCCE.2024.13837

cryptographic algorithms that can withstand the challenges posed by the quantum computing era, ensuring the safety of our data and personal information.

II. BACKGROUND

What is Quantum computing?

Quantum computing [1] is an emerging field that leverages quantum mechanics to process information in ways traditional computers cannot match. Key concepts include:

- **Qubits**: Short for quantum bits, these are the fundamental units of information in quantum computing. Unlike classical bits, qubits can exist in a state of 0, 1, or both simultaneously, based on the quantum concept of superposition.
- **Superposition**: This principle allows qubits to exist in multiple states concurrently, enabling quantum computers to explore numerous possibilities simultaneously.
- **Quantum gates**: These tools manipulate qubit states and are essential components of quantum circuits. Quantum circuits perform calculations by applying a series of these gates to qubits, similar to how logic gates function in classical circuits.
- **Entanglement**: This phenomenon occurs when qubits become interconnected, causing the state of one qubit to affect another, regardless of distance. This strong link facilitates more efficient complex calculations, as measuring one entangled qubit instantly reveals the state of its partner.
- **Quantum speedup**: This concept refers to quantum computers' ability to solve certain problems significantly faster than classical computers. This advantage is particularly evident in tasks such as factoring large numbers, optimizing solutions, and simulating quantum systems.

While still in its early stages, quantum computing has the potential to revolutionize fields like data security, drug discovery, and materials science. It represents a leap in computational power, capable of tackling problems beyond the reach of today's classical computers.

What is Cryptography?

Cryptography plays a crucial role in protecting our digital communications and data. It functions as a specialized code that ensures information security. With cryptography, you can transform your message into a code that only the intended recipient can decipher and comprehend. It is based on the following concepts:

- **Data Encryption**: Encryption is like to securing your diary in a safe with a unique key. Only the person possessing that key can access and read its contents, shielding them from prying eyes. In the digital realm, encryption safeguards your data, allowing access only to authorized individuals.

- **Authentication**: Consider a secret handshake between you and your best friend. You use this handshake to verify each other's identity upon meeting. Similarly, cryptography employs digital signatures and certificates to confirm identities online, ensuring you interact with the intended person or website.

- **Data Integrity**: Imagine sending a sealed letter. If the seal is broken upon arrival, it indicates potential tampering. Cryptographic hash functions create a unique "seal" for your data, enabling you to verify if it has been altered during transmission.

- **Secure Communication**: Picture having a private conversation in a sealed room. Cryptographic protocols like SSL/TLS establish a secure "room" for your online interactions, protecting sensitive information such as credit card details from eavesdroppers.

- **Non-repudiation**: Think of signing a contract with your unique signature. Once signed, you cannot deny agreeing to its terms. Digital signatures function similarly, providing evidence that a message or document originates from you and remains unaltered.

The significant advancements in processing speed and the emergence of superintelligent capabilities in contemporary quantum computers suggest heightened vulnerability in existing cryptographic algorithms. Understanding the implications of these developments requires examining the distinctions between classical and quantum computing.

Classical vs. Quantum Computing

Classical computers excel at everyday tasks like reading emails and browsing the internet. In contrast, quantum computers are powerful machines capable of solving complex problems that challenge traditional computers.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

Classical Computing

Bits: Classical computers use binary switches (0 or 1).
Processing: Sequential, step-by-step task handling.
Speed: Quick for many tasks, but processes calculations individually.
Applications: Ideal for daily tasks like document creation, internet browsing, and app usage. Excels at jobs with straightforward instructions and data.

Quantum Computing [2]

Qubits: Quantum computers use qubits, which can be 0, 1, or both simultaneously.
Processing: Explores multiple possibilities concurrently due to unique properties.
Speed: Utilizes quantum speedup.
Applications: Potential game-changer in cryptography, drug discovery, and other fields. Solves problems challenging for classical computers.

Key Differences between Classical and Quantum Computing

Parallelism: Quantum computers evaluate multiple solutions simultaneously; classical computers work sequentially.
Complexity: Quantum computers efficiently solve certain problems that would take classical computers an impractically long time.
Development Stage: Classical computers are everywhere and well-established; quantum computers are still in development and not widely accessible.

Current Cryptographic Methods:

RSA (Rivest-Shamir-Adleman): RSA is an asymmetric encryption method using two keys: a public key for encryption and a private key for decryption. Its security relies on the difficulty of factoring large composite numbers into their prime factors, a problem known as integer factorization. Currently, no efficient method exists for factoring these large numbers, ensuring RSA's security against modern computational capabilities.

AES (Advanced Encryption Standard): AES is a symmetric encryption method using the same key for both encryption and decryption. It processes data in fixed-size blocks through a series of transformations, including substitution, permutation, and mixing. AES's security depends on the impracticality of cracking the key through brute force methods. With key sizes of 128, 192, or 256 bits, attempting every possible key combination would require an unfeasible amount of time with current technology.

ECC (Elliptic Curve Cryptography): ECC is another asymmetric encryption method utilizing the mathematical properties of elliptic curves over finite fields. It offers comparable security to RSA but with smaller key sizes. ECC's security is based on the difficulty of solving the elliptic curve discrete logarithm problem, making it a secure and efficient alternative to RSA.

All these cryptographic methods rely on the assumption that certain mathematical problems are computationally challenging. This implies that breaking the encryption by solving these problems would take an impractical amount of time with current algorithms and computing power.

However, advancements in algorithms or the emergence of quantum computers could potentially challenge these assumptions, highlighting the importance of ongoing cryptographic research.

Quantum Algorithms

Since the discovery of quantum computing concepts researchers and scientists have been working on algorithms to utilize the potential of quantum mechanics in computer processing. Currently, two prominent quantum algorithms are Shor's algorithm and Grover's algorithm. Here's an overview of each:

Shor's algorithm [3]

In the year of 1994 an American scientist “Peter Shor” developed this quantum algorithm which can process complex calculations and retrieve results faster than regular computing. This algorithm specializes in decomposing large numbers into their prime factors. It's significant because it could potentially undermine popular encryption methods like RSA, which rely on the difficulty of factoring large numbers. Shor's algorithm leverages quantum parallelism and entanglement to identify prime factors of a large number much quicker than the best classical techniques.

DOI: 10.17148/IJARCCE.2024.13837

It also employs the quantum Fourier transform to detect periodicity, a crucial step in the factoring process. Development of large-scale quantum computers capable of running Shor's algorithm might expose vulnerabilities in current encryption systems. This could drive scientists to devise new quantum-resistant information security methods.

Grover's algorithm

Gover's Algorithm [4] is a well-known quantum algorithm which was developed in 1996 by one Indian American computer researcher "Lov Grover". It is designed for navigating unsorted databases or addressing unstructured search problems, Grover's algorithm claims a quadratic speed improvement over classical processing method. For example, while a classical search through a database of N items would take O(N) time, Grover's algorithm can find the target item in approximately O(√ N) time. It applies a quantum process called the Grover iteration, which amplifies the probability of the correct result while reducing the probability of incorrect ones. This is achieved through a series of quantum gates that modify qubit profusions.

Although not as groundbreaking as Shor's algorithm, Grover's algorithm still provides significant improvements for search-related tasks and has applications in various fields, including cryptography, optimisation, and machine learning. These algorithms showcase quantum computing's potential to undertake problems far more effectively and faster than the conventional computers.

Developments Around Quantum Computing

In recent years, the field of quantum computing has made remarkable developments, showcasing several significant milestones that stand out in its advancement.

1. **Google's Work in Quantum Computing**
   In late 2019, just before covid outbreak. Google's designed a quantum computer called as Sycamore, which was big development in field of quantum computers. Google claimed that this new quantum computer finished one task in less than 4 mins which was not possible for a regular computer in 10,000 years.
   This task was specially designed to measure efficiency of quantum computers. However, it was very convincing that Google's quantum computer is super-efficient and capable to handle last calculations in a very short span of time.

2. **IBM's Research to Quantum Computing**
   IBM was also working on quantum computing and almost after 2 years of Google's quantum computer launch. IBM also announced their quantum computer which had 127-qubit processors. They called this IBM Eagle [5]. IBM also has designed some quantum processors via their "IBM Quantum Experience Platform" and they are promoting to allow others to use these new quantum processors to. IBM's work has really pushed quantum computing forward & made it easier for researchers & developers to get their hands on it.

3. **Microsoft's Quantum Machine** [6]
   Microsoft is developing a powerful quantum computer that can tackle some of the toughest problems in the world. To do this, it needs at least 1 million stable qubits that can handle 1 quintillion operations with only one mistake allowed. The company is focused on creating a special, stable qubit and building a complete, reliable quantum machine for Azure. Achieving this will require many important advancements throughout the whole system.

4. **Intel's research on Quantum Computing** [7]
   Tunnel Falls is the latest and most advanced silicon spin qubit chip created by Intel. This chip represents a big leap forward in developing a complete commercial quantum computing system. Intel is also sharing this chip with the quantum research community to help encourage new discoveries in the field.

5. **Amazon's Center for Quantum Computing** [8]
   Amazon has initiated a comprehensive development plan in the quantum computing sector. They have established several divisions to facilitate this progress. Amazon Bracket has been launched to aid research in quantum hardware, while the AWS Center for Quantum Computing will unite leading experts from top research institutions to work together on technological advancements in this field. Additionally, the Amazon Quantum Solutions Lab will cater to customers by providing access to quantum computing specialists from Amazon and its partners, promoting expertise in quantum computing and speeding up the creation of significant applications.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

In addition to the prominent technology leaders, numerous other firms are actively developing quantum computers. The list of these companies is extensive and continues to expand. Some are focusing on utilizing quantum technology as a foundational element for their computer processors.

Breaking Classical Cryptography

Quantum computing is about to shake entire cryptography world, especially with the introduction of Shor's algorithm. Here's where things get interesting. Quantum computing is about to turn the cryptography world upside down. There's this thing called Shor's algorithm that's got everyone worried. It's like a superpower for breaking down big numbers FAST. That's a big deal cause lots of cryptographic systems (like RSA & ECC) rely on how hard it is to factor those numbers or solve tricky math problems.

Take RSA, for example. It's based on the idea that multiplying two big prime numbers is easy, but figuring out what those numbers were from the result is HARD. Well, Shor's algorithm makes that "hard" part a piece of cake. And ECC? It's all about solving something called the elliptic curve discrete logarithm problem. Shor's algorithm can crack that too.

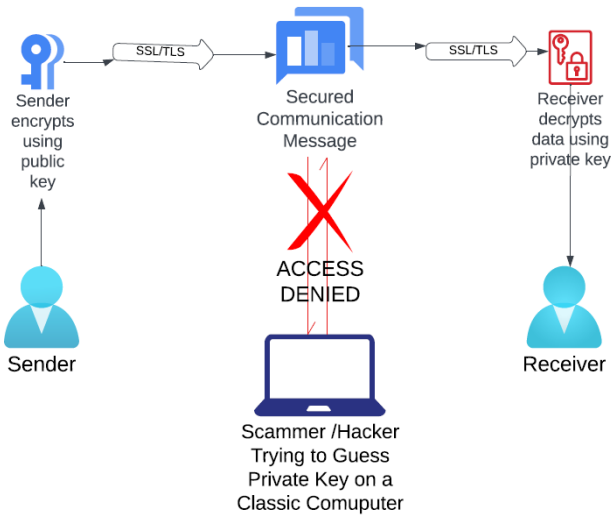

Fig. 1 Attempt to break 256 key RSA encryption for a regular computer.

Above picture explains how existing cryptography like RSA, AES or ECC work. A sender is transferring data over secure channel encrypted with 256 bit cypher key and in case any hacker tries to recover private key it will take years to decode it. And meanwhile sender changes the cypher key before an year typically in 3 months and hacker will have to restart from 0. So conceptually hacker will never be able to access private key or be able to read data.

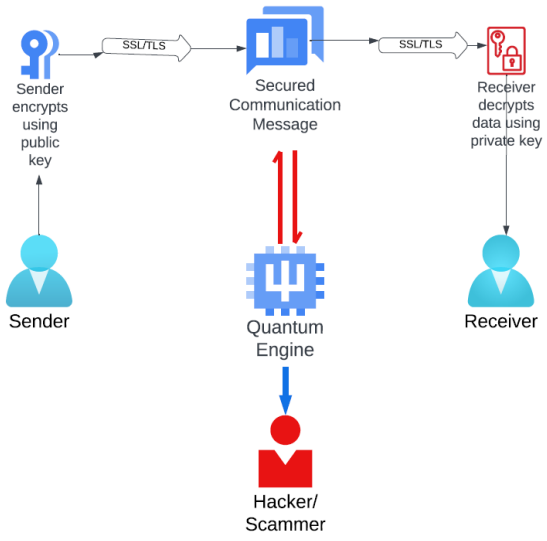

Fig. 2 Attempt to break 256 key RSA encryption for a quantum computer.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

On the other hand if hacker is using a quantum computer he will be able to perform required iterations to find out private key quickly in few minutes. And it's not practical for Sender to change password in each few minutes. We will understand this difference in following paragraphs with some graphs and numbers discovered by some researchers and computer scientists.

Below is a high level how Classical Cryptography works:

Most of the classical cryptography algorithms work on prime number principal [9] for calculating public and private keys to make it difficult to decrypt a message. However as of now in decimal systems biggest prime number is "24,862,048". It is a very big number, and it will many years for getting the private key using normal computers. However, it will be few minutes of work for a quantum computer.

Let's try to understand the difference of time between classic and quantum computers via below images,

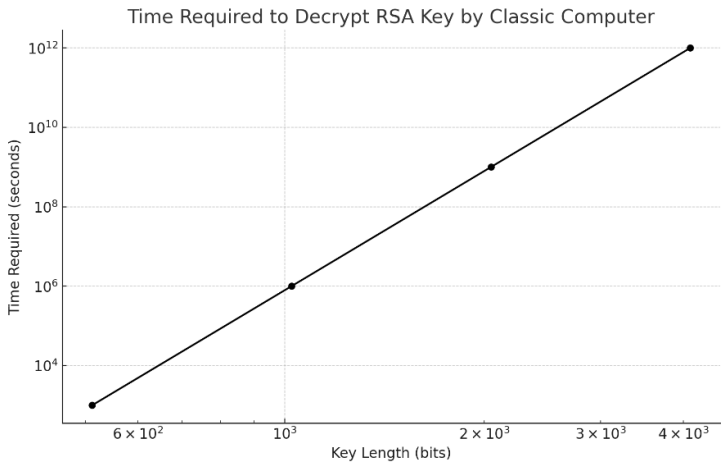

Fig. 3 Time required for a regular computer

If someone tries to decrypt an RSA key of $2x10^3$ = 2000 bits so it will take 10^{10} = 10,000,000,000 Seconds which is equivalent to 316.98 years.

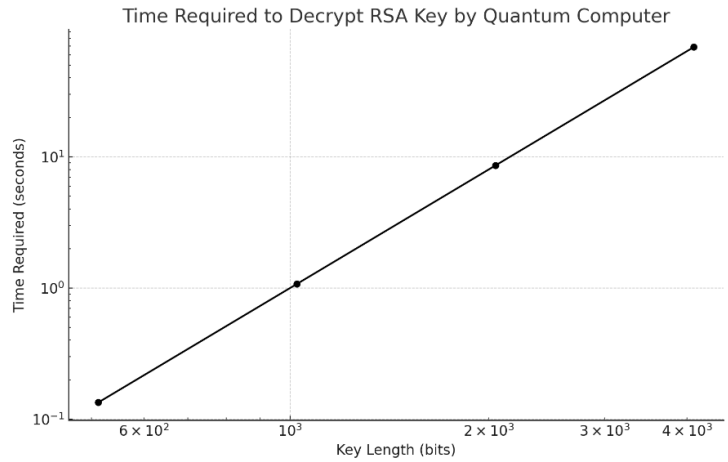

Fig. 4 Time required for a quantum computer

On the other hand, if you try to find private key for same encryption using a quantum computer, it will take merely 10^2 = 100 seconds.

So, what are our action times now? We need to come up with quantum-resistant cryptography, sooner the better. Since continuous development in the field of quantum computing is going to develop smarter and faster computers. Researchers

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

are working on new techniques that can stand up to quantum threats. They're calling them post-quantum cryptographic algorithms [1]. Here are a few:

• **Lattice-Based Cryptography**: This one uses tricky lattice problems that even quantum computers struggle with. It's super versatile & can be used for securing data which can survive quantum computing.

• **Hash-Based Cryptography**: This uses hash functions to make secure digital signatures. It doesn't rely on number theory, so it's thought to be safe from quantum attacks.

• **Code-Based Cryptography**: This method uses error-correcting codes to protect data. There's a famous example called the McEliece cryptosystem that people think can resist quantum threats.

• **Multivariate Quadratic Equations**: These methods focus on solving systems of multivariate quadratic equations. It's a mouthful, but basically, it's TOUGH for both classical & quantum computers.

So far, Quantum Key Distribution (QKD) is seen as a possible solution, but it needs communication to occur over special QKD lines instead of the usual SSL or TLS channels. QKD uses the same quantum principles to take advantage of the changing states of photons for sending data and verifying secure data transfers, ensuring that no one can intercept the information.

Following is one high level diagram of secure data transmission between two people Yash and Thomas.

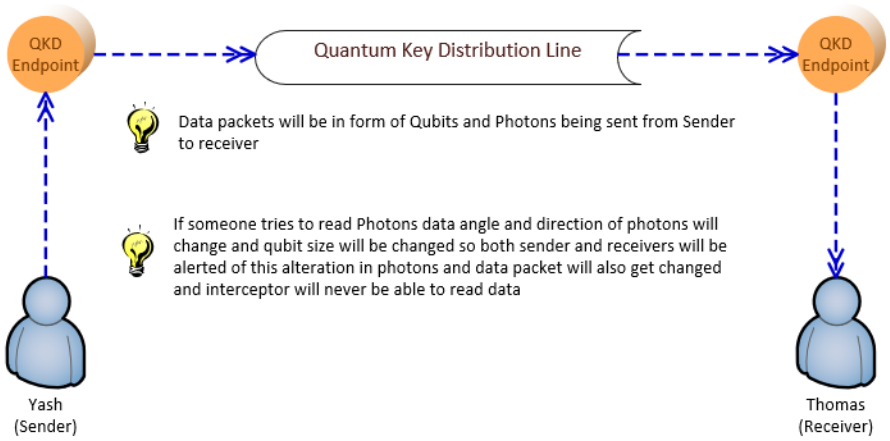

Fig. 5 Secure data communication using QKD system.

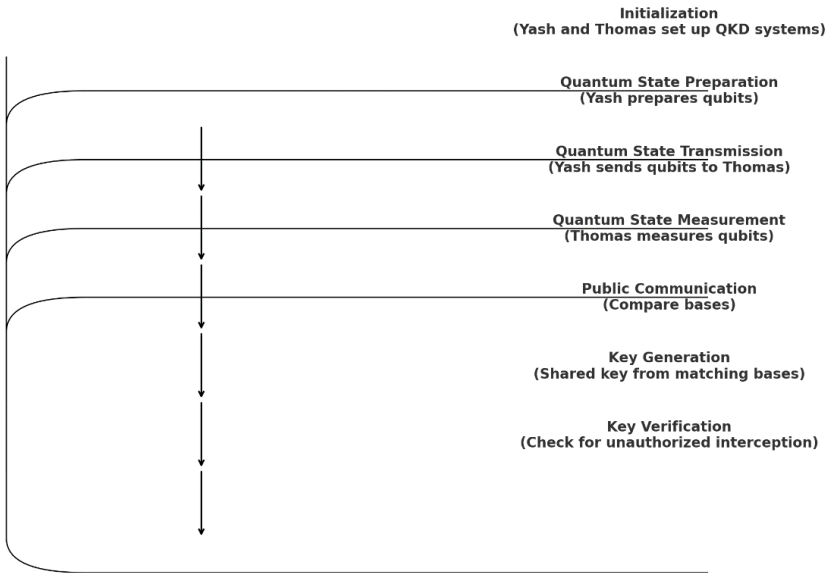

Fig. 6 Sequence diagram of communication using QKD system.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

In the diagram above, Yash is the one sending a secure message to Thomas using qubits. While transmitting the data, Yash includes details about the quantum keys within the size of the qubits. As the data moves from Yash to Thomas, it is checked to ensure the quantum keys are the right size. If someone tries to intercept the data during this process, both Yash and Thomas will be alerted to any changes in the qubit size, and the data will be altered if someone attempts to read it using the photons involved in Quantum Key Distribution (QKD).

So, there you have it, however quantum cryptography will need compatible hardware support too which can handle photon transmission. The world of cryptography is changing FAST, and we need to change our security algorithms also to handle this. All these new cryptography algorithms use complex cipher keys which will not be easier to break. There are still research going on to develop better cryptography algorithms which have lighter footprint but can withstand quantum computing power.

III. CASE STUDIES AND EXAMPLES

Problem Due to Quantum Computing

Quantum computing's got the security world on edge, especially when it comes to our current encryption methods. Banks & healthcare folks are particularly worried - they've got a lot to lose if things go south.

Effect on Banking: Let's talk banking first. These guys rely on some pretty fancy coding to keep our money safe & sound. But here's the thing: quantum computers could crack those codes like they're nothing. That's bad news for our cash & personal info. On the flip side, these super-smart machines might help catch fraudsters faster. They could spot fishy patterns that regular computers miss. Plus, they might give banks a leg up on predicting market shifts.

Effect on Healthcare: Now, healthcare's in a similar boat. They're all about keeping patient data under wraps. But quantum computers? They could blow those locks wide open. It's not all doom & gloom, though. These brainy machines could speed up drug discovery big time. Imagine finding new treatments in half the time! They might even help us understand genetic diseases better.

Think of "Quantum computers" as the Usain Bolt of problem-solving. Their incredible speed allows them to break down our current security codes in the blink of an eye. This alarming capability has driven numerous industries to explore cutting-edge strategies to protect our data and personal information.

The advent of quantum computing has the potential to enhance numerous processes through the utilization of accelerated artificial intelligence systems. This technological advancement could lead to a transformative impact across nearly all sectors.

Research and Developments for The Solution

- **NIST's Project for Post-Quantum Cryptography** [10]
  The National Institute of Standards and Technology (NIST) [11] has working on to develop cryptographic algorithms that can stand up to the power of quantum computing. For almost a decade, they've been working hard on a project to find and standardize these cutting-edge cryptographic solutions. In 2022, they made a big announcement, introducing the first four algorithms designed to resist quantum attacks:
  - CRYSTALS-Kyber [10]
  - CRYSTALS-Dilithium
  - FALCON
  - SPHINCS+

  These new algorithms are poised to replace the current encryption methods that could be compromised by the advancements in quantum technology.

- **The PQCRYPTO Project by European Union**
  Since almost same time as NIST started the PQCRYPTO Project is also an initiative backed by the European Union that focuses on developing strong and reliable cryptographic algorithms. Which should be efficient of surviving the challenges posed by quantum computing.

- **VIPRE's Work on Quantum-Resistant Cryptography**
  There is one more major development on research of quantum computing proof cryptographic algorithm is being worked upon by VIPRE. In a recent blog on VIPRE's website they claimed to have some development really soon on new cryptographic algorithm which can service quantum computing.

DOI: 10.17148/IJARCCE.2024.13837

- **Other Global Research Efforts**
  Computer scientists and researchers worldwide are collaborating to develop robust cryptographic algorithms that can withstand the power of quantum computing. Various cybersecurity organizations, such as CISA, NCSA, and other government agencies, are actively working on creating Post-Quantum Cryptography (PQC) algorithms. Numerous conferences and events are held regularly across the globe, with countries like the USA playing a significant role in this security initiative.

As quantum computing continues to advance on quantum computing, major corporations are also focusing on developing quantum-ready cryptographic algorithms to secure their platforms. For instance, Amazon is working on integrating these algorithms into AWS, while Microsoft is enhancing the security of its quantum computing-based Azure platform. Similarly, Google is planning to secure its Google Cloud environment with quantum-resistant solutions.

IV. CONCLUSION

This article highlights the immense potential of quantum computing and its ability to revolutionize heavy data processing and execute intricate operations at lightning speed. As we face an ever-growing influx of quintillions of bytes of data daily, the need for advanced computing solutions becomes increasingly urgent. Traditional processors will soon struggle to keep up with our daily searches and other essential tasks, making the transition to quantum computing not just beneficial, but necessary to stay aligned with the rapid pace of digital advancement. In today's world, everything is becoming digital—from our finances and vehicles to our entertainment and software applications, even our identities are now online. Now challenge is to create hardware which can support quantum computing, since a regular computer cannot store qubits properly.

Major corporations are racing to develop their own quantum computers or platforms for quantum computing. The advent of Shor's and Grover's algorithms has sparked a surge of interest in harnessing quantum mechanics to build these advanced machines. Tech giants like Google, IBM, Microsoft, and Amazon are in fierce competition to be the first to launch a functional quantum computer that can be integrated into their applications and cloud services.

This urgency is underscored by the realization that these powerful processors can effortlessly execute millions of attempts to crack current cryptographic algorithms, raising significant concerns about data security. In response, both large corporations and government entities are diligently working to create new cryptographic systems designed to safeguard sensitive information. The potential threat is alarming: if a hacker gains access to a quantum computer, they could easily infiltrate and exploit classified data. It is essential to implement security measures to ensure that only authorized individuals have access to this system.

Numerous organizations are currently engaged in the development of advanced cryptographic algorithms to mitigate these risks. Furthermore, quantum computers encounter difficulties associated with error correction. Due to the swift processing abilities of quantum systems, even a slight error can develop into a substantial problem that is challenging to resolve. We have examined the potential of blockchain technology in enhancing data security to a certain degree; however, it remains vulnerable to the formidable capabilities of quantum computing. There is a pressing need for improved digital signatures to bolster the security of our digital currencies as well.

Quantum computing heralds a transformative era in technology, offering substantial potential to enhance human life. However, it simultaneously exposes vulnerabilities related to security breaches, attributable to its formidable processing capabilities. In response, there has been a growing interest in employing quantum key distribution (QKD) to bolster blockchain technology. If we can effectively manage the security and error-related challenges associated with quantum computing, it could significantly facilitate advancements across various sectors, including healthcare, finance, process digitization, retail, and other research domains.

The influence of quantum computing is particularly pronounced in areas such as cryptography, which is essential for protecting sensitive information. While there are significant obstacles to overcome, the opportunities for developing innovative technologies and enhancing security protocols are remarkable. By proactively preparing for these changes and embracing new technologies, we can harness the potential of quantum computing to foster a more secure and advanced digital landscape. Indeed, quantum computing is revolutionizing the landscape. However, with the expertise of numerous talented individuals in the field, we can remain at the forefront of innovation. It is an exciting era ahead, so prepare yourselves for the journey.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13837

REFERENCES

[1] D. &. N. A. &. K. V. L. T. &. R. R. &. N. N. &. M. M. Kumari, "Quantum Computing in Cryptography.," 2023.

[2] "What is quantum computing?," McKinsey, [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing.

[3] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer".

[4] L. K. Grover, *https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.79.325*, 1997.

[5] IBM, "Quantum Safe | IBM Quantum Computing," [Online]. Available: https://www.ibm.com/quantum/quantum-safe.

[6] Microsoft, "Azure Quantum," [Online]. Available: https://azure.microsoft.com/en-us/solutions/quantum-computing.

[7] Intel, "Quantum Computing Systems Achieving Quantum Practicality," [Online]. Available: https://www.intel.com/content/www/us/en/research/quantum-computing.html.

[8] Amazon, "AWS Announces New Quantum Computing Service (Amazon Braket) along with AWS Center for Quantum Computing and Amazon Quantum Solutions Lab," 02 Dec 2019. [Online]. Available: https://press.aboutamazon.com/2019/12/aws-announces-new-quantum-computing-service-amazon-braket-along-with-aws-center-for-quantum-computing-and-amazon-quantum-solutions-lab.

[9] N. P. A. B. A. O. A. W. R. E. E. Joshua J. Tom1, "Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems".

[10] J. Pinto, "Post-Quantum Cryptography," 2022.

[11] "NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers," 24 August 2023. [Online]. Available: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers.

[12] K. R. Vaishali Bhatia, "An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm," 2020.