JOURNAL OF NANOSCOPE
ISSN(P): 2707-711X | ISSN(O): 2788-7456 Volume 4, Issue 2, December 2023, pp 83-96

Quantum Computing: Principles of Breaking Encryption

Gulfraz Naqvi*, **Muhammad Burhan Umar, Saqib Ali**

School of Commerce and Accountancy, University of Management Technology, Lahore.

Corresponding Email: gulfraz.naqvi@umt.edu.pk

Received: 15 June 2023 **Published:** 31 December 2023

Abstract:
The basis of modern security relies on encryption methods that are practically impossible, but theoretically possible, to break. Quantum computing is a process by which a computer takes advantage of quantum mechanics to solve complex problems. IBM has been working on and has made quantum computers available for almost a decade now. These machines can be used for cryptography related problems like decrypting complex encryptions much faster than the classical computers we have today. So much faster in fact, that a quantum computer can factor a 300-digit number in the same amount of time that a normal computer could multiply the two numbers together, making our current encryption methods obsolete.

Keywords: Quantum Computer, Qubit, RSA, ECC, AES, Private key, public key.

DOI Number: https://10.52700/jn.v4i2.95

Introduction:

Quantum computing was first proposed in 1980 by Richard Faynman. He proposed an idea to build a device that would be composed of a controlled quantum environment. That would be then used for analogue quantum simulations. Quantum Computers nowadays consist of qubits, which are also called Quantum Bits. Qubits are a two-state version of the normal "bit" we are familiar with, that consists of 0s and 1s. Now, Qubits also consists of these 0s and 1s but they are in a state of superposition, meaning that they can be 0 and 1 at the same time. The first quantum computer was developed by D-wave in 2013, and it had 128 qubits. The latest quantum computer developed by Atom Computing is to have 1225 qubits [8].

Principle:

Quantum computers work on the principle of qubits. Qubits use electrons to encode data using two-state quantum mechanics. Qubits, unlike classical bits, can be both 0 and 1 at the same time. This means that complex expressions can be solved faster than a classical computer. Qubits are expressed as $|0\rangle$ and $|1\rangle$ [3].

Qubits can be expressed as a vector:

$$\psi=\alpha|0\rangle+\beta|1\rangle$$

Where α and β are complex numbers $\mathbb{C}$.

However, quantum mechanics are not like the natural rules of physics, so it is difficult to precisely solve these complex questions. Quantum Computers are especially good at breaking encryption, by using two key principles, those being: super positioning and entanglement.

- Superposition: As discussed previously, a qubit can be in a superposition of two states, which means that it can be both a 0 and a 1 at the same time. This allows quantum computers to perform calculations on multiple values at the same time, which makes them much more efficient.
- Entanglement: Two or more qubits can be entangled, which means that they are linked together so that they can share information instantly. This allows quantum computers to perform calculations that are impossible for classical computers.
- Decoherence: It is when a qubit loses its quantum state due to environmental factors like radiation, resulting in the collapse of the quantum state of qubit. This results in the fall of qubits, and dysfunction Ing of the quantum computer.

An algorithm known as Shor's algorithm uses these two principles to find the prime factors of large numbers. The algorithm starts by creating a superposition of all possible factors of the number. Then, it uses entanglement to link the qubits together so that they can share information about the factors. Finally, it measures the qubits to determine the prime factors of the number. Classic computers from today would take billions of years to find the factors of a 256-bit number whereas quantum computers might even have the possibility to solve problems based on 1024 or even more bits.

One of the biggest challenges of building these super machines is to create structures that would delay the decoherence effect by shielding the qubits from external factors.

Literature:

Encryption:

The study of cryptography and cryptanalysis is known as cryptology. The process of protecting data transmission and storage such that only the intended recipient can comprehend it and others cannot is known as cryptography. The art of cracking codes, cipher messages, and cryptosystems without knowing the method or the key is known as cryptanalysis. The act of transforming plain text into cipher text utilizing straightforward schemes, algorithms, and keys is known as

encryption. This ensures that the encrypted communication can only be unlocked by the intended recipient with the use of certain decryption keys and methods. The Greek word "Kryptos," which means concealed, is where the names "encryption" and "decryption" come from.

Humanity has been concerned in preventing the unintentional dissemination of sensitive information since the invention of written language. In the past, folks from the Middle Ages would substitute symbols, numbers, or visual depictions for some information. Various people have occasionally employed cryptography for diverse goals. For example, the Chinese sought to safeguard their trade secret of producing silk, while the Germans sought to safeguard their military secrets.

Modern cryptography is required by corporations, industries, firms, offices, etc. to safeguard their official data from hackers in light of the improvements in computer and communication technology. Using computers and mathematical formulae to convey digital data in a more secure manner is known as modern cryptography. Different data encryption techniques fall into one of two categories:

- Symmetric Key Algorithm
- Asymmetric Key Algorithm

Symmetric Key Algorithm:

A symmetric key algorithm makes use of the same key (parameters) for both the encryption and decryption of data. To be precise, the encryption and decryption sites use the very same key. There can also be cases where the keys at encryption and decryption sites are different, but they can be computed from each other using some mathematical formula for the process and hence are same in essence.

The approach in which the data that is to be ciphered, can be classified as Block cipher or Stream cipher. The data can be represented as a whole block or a chunk that is to be encrypted (Block Cipher) or follow character-by-character encryption (Stream Cipher). Models like AES and DES follow block cipher while models like RC4 follow stream cipher.

One of the ways of ciphering data is the hash cipher. Through this way, the input information that is to be encrypted is taken, and a short message of fixed length is given as the output, completing the encryption. MD4 and MD5 were some strong hash functions but have since been compromised. MD5 was taken as inspiration to make Secure Hash Function series like SHA-0, SHA-1, SHA-2. Each version promises better security and functionality than the previous version. A new SHA-3 Hash Algorithm was made the US standard in 2012 [1].

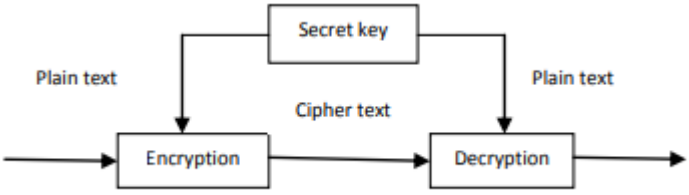

Fig. 1: Symmetric Key Algorithm

Asymmetric Key Algorithm:

While the public key can be exchanged in a public or private setting, private keys must be provided in the strictest of confidence as the public key is just used to encrypt data; the private key is required to decode it. It is quite unlikely to extract a single private key from a given public key, notwithstanding the mathematical relationships between public keys. Diffie and Hellman made an effort to develop a workable public key encryption scheme. Ronald Rivest, Adi Shamir, and Len Adleman didn't discover the answer to this conundrum until 1978; this solution is now known as the RSA algorithm. This encryption technique quickly became the most common algorithm ever utilized, with users using it all around the world. Digital signatures can also make use of asymmetric key techniques.[1]

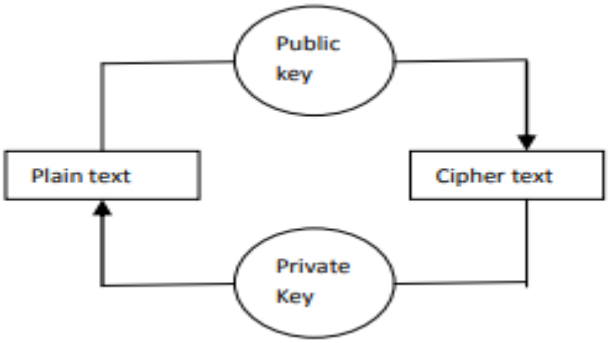

Fig. 2: Asymmetric Key Algorithm

Quantum Encryption:

Introduction:

By taking use of the weaknesses in the principles of quantum physics, quantum cryptography provides the most secure means of transmitting information between two parties. The application of quantum mechanics is founded on two main principles:

- The uncertainty principle of Hoffmann.
- Principle of Photon Polarization.

The uncertainty principle of Heisenberg:

This concept states that two attributes of a single thing cannot be measured or seen at the same time. For photons, this holds true. Photons are polarized, or slanted, in one direction, and have wave-like structures. One of the main issues is that this concept only holds true while the photon is being seen. This is crucial in hindering attackers' attempts to exploit quantum cryptography.[7]

Photon Polarization principle:

According to this theory, a transmission tapper cannot duplicate the individually unique "qubits," or quantum bits, since they exist in an unknown quantum state as a result of the no-cloning principle [6]. Any attempt to quantify one of their qualities will cause the knowledge about the other attributes to change.

Quantum Key Distribution:

The flaws of classical key distribution were overcome by Quantum key Distribution or QKD. In 1984, Charles H. Bennett and Gilles Brassard proposed and brought about the very first key-distribution-protocol which was called to be “BB84” (Big Brother 1984), based on Heisenberg’s Uncertainty Principle. Two channels are used by QKD. First, there is the quantum channel, which may be created from optical fiber or space and is used to send a single photon over a transparent path. The second is a traditional channel, like a phone line or internet connection, that is used to send encoded data.

History:

Charles Bennett received a proposal from Stephen Wiesner in the late 1960s or early 1970s. The concept proposed using quantum physics to create banknotes that would be impossible to counterfeit because of natural principles. Additionally, he proposed the creation of a channel known as "Quantum Multiplexing," which would let one person to transmit two messages to

another party and have that party choose which of the two messages to read—but only if doing so meant permanently destroying the other message.

Wiesner attempted to submit "Conjugate Coding," one of his works, to the IEEE Transactions on Information Theory. Regretfully, the publication was refused for unclear reasons. Bennett was so enthralled with Wiesner's work that, even after his work was rejected, he would frequently use it to share his views with other people years later. Bennett contacted Gilles Brassard in late October 1979, and the two of them talked about the concepts Wiesner had given. They combined some of the then-novel concepts of public key cryptography with Wiesner's coding technique. Quantum cryptography, quantum teleportation, entanglement distillation, and privacy amplification were further explored by these two. Their study was the first on quantum cryptography to be published. This resulted in the delayed release of Wiesner's article "Conjugate Coding" in 1983, after Rabin's autonomous creation of his first iteration of Oblivious Transfer.

The concepts of Bennett and Gilles centered on the necessity of preserving quantum information's localization. The endeavor was rendered almost hard by the employment of photon polarization as a transport of quantum information. A few years later, they revised their concepts to transfer sensitive data using quantum channels.

In the initial theoretical effort, the transmitter's secret information was encoded using a quantum signal so that the receiver could only decode it if there was no eavesdropping. Additionally, the communication would ruin itself without disclosing any information in the event that someone tried to listen in. This would also notify the intended recipient about the eavesdropper.

They considered employing quantum channels to send an arbitrary-length random secret key later in 1983. The key would be discarded if any inevitable disruptions that may allow for eavesdropping were discovered in the quantum channel; if not, the intended recipient could securely utilize it to decipher the communication. Together with John Smolin, Francois Bessette, and Louis Salvail, Bennett and Brassard created the first-ever covert quantum transmission in history in October 1989 across a distance of 32.5 cm. Motivated by their achievements, scientists and researchers in physics started observing their efforts to enhance the complexity of their prototype.

Rather than reimagining the BB84 protocol in the early 1990s, Arthur Ekert used quantum entanglement and a breach of Bell's theorem to reimagine quantum key distribution. With the development of quantum distillation and quantum privacy amplification, this proved to be quite fruitful. Using entanglement might be a crucial step toward a satellite-based quantum cryptography system that is genuinely safe. Lastly, entanglement-based cryptography will provide a key

distribution mechanism that outperforms conventional approaches by ensuring security against both physical theft and eavesdropping once long-term storage of quantum information becomes a reality [2].

Quantum Decryption:

The electrical One-Time Pad (OTP) invented by Gilbert Verman in 1917 was for telegraph encryption. In classical form of cryptography, the OTP supplies the perfect confidentiality i.e. in case we are unable to find about the key that were used for encryption, we will not be able to decipher the encoded transmission and hence unable to fetch the encrypted data. To further explain in terms of formula, let

a= a1, a2…ai, be the message of length "i" bits,

x= x1, x2…xi, be the key to the exact length as that message i.e. "i",

If we consider a single bit message "a" and key "x" then-

The encryption function "z" can be written as:

$$z=a\oplus x$$

Where $\oplus$ is the XOR gate.

And similarly, the decryption function can be written as:

$$a=z\oplus x$$

In quantum cryptography, quantum OTP is used to encrypt qubits. To understand it better, let H1 send to H2 a qubit "|a> "using the key" x". H1 uses some operants on the message "|a> "using key "x" which changes the actual message into an encrypted one, ″m″. When "reaches H2, they decrypt the message by using the key "x" and the decryption function.[7]

The quantum encryption function is:

$$|z\rangle = m \times |a\rangle$$

Where a=message,

x=key,

z=encryption,

m=plain text.

Similarly, the quantum decryption function is:

$$|a\rangle = m \times |z\rangle$$

The difference between classical and quantum decryption can be clearly seen as a massive leap as classical decryption is based on the use of XOR gate which consumes an enormous amount of time for high bit encryption like 256 bits. It may even take up to many years for such high bit encryption to be deciphered. Meanwhile the formula of Quantum decryption enables us to decrypt the very same encryption within a few minutes as it exploits the laws of quantum mechanics to unveil the encoded message and takes the key as the power of the plain text, which can solve enormous bits of coded messages rapidly and easily.

Methodology:

The concerned methodology of the findings was done purely through selected publications on the topic of Cryptography and its Quantum counterpart. Since the research was done through conceptual means, no empirical evidence was used, or referred to in this paper. Conceptual papers may often end up being opposed to or being proven wrong with further study and new discoveries in the regarding field.

Findings:

Quantum computers have the potential to revolutionize decryption by exploiting the principles of quantum mechanics to break certain types of encryptions that are currently considered secure. This is because quantum computers can perform certain calculations, such as factoring large numbers, much faster than classical computers. Quantum computers can use several algorithms such as Shor's algorithm to break different encryption schemes such as RSA Encryption and ECC Encryption. RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are the methods used to encrypt data currently. RSA encryption is based on the difficulty of factoring large numbers to create a RSA key pair, two large prime numbers are multiplied to form a modulus, then the public key is modulus, and the private key is the product of the two prime numbers.

RSA encryption:

Steps of RSA:

- Key generation:
    - Two random, large prime numbers, x and y, are chosen.
    - The public key (a, b) is generated using x, y, and a mathematical function.
    - The private key (d) is derived from x, y, and n using another mathematical operation.
- Encryption:

- When the sender wants to send a message M to any recipient, then the sender obtains the recipient's public key (a, b).
- Using mathematical operations and the public key, the sender encrypts the message M into a ciphertext C: C = M^e mod n.
- The ciphertext C is then sent to the recipient.

- Decryption:
  - The recipient receives the ciphertext C.
  - Using their private key (d) and the mathematical relationship between the keys, the recipient decrypts the ciphertext back into the original message M: M = C^d mod n.
  - The recipient then can read and understand the decrypted message.

RSA, however, relies heavily on the secrecy of private keys. If the private key is compromised, the security of the system is broken. RSA is computationally expensive, especially for large key sizes. This can limit its use in some applications. Despite these limitations, RSA remains a highly secure and widely used encryption algorithm. Its robustness and long history make it a trusted solution for protecting sensitive data.[2] As mentioned earlier, the security of RSA depends on the key size. Larger key sizes offer greater security but require more computational resources. Currently, a 2048-bit key size is considered the minimum for most applications, but using quantum computers, these bits can easily be more than doubled due to the nature of said quantum computers. Consecutively, Quantum Computers can also be used to easily decrypt this form of encryption, since the RSA encryption methods nowadays use up to 2048 bits.

ECC Encryption:

Steps of ECC:

- Key Generation:
  - A user selects a specific elliptic curve (hence the name) and a point on it.
  - Using mathematical operations, they generate their private and public keys.
  - Private key (K) is generated by taking a large random integer.
  - The Public key is computed by multiplying the base point G, which is selected on an elliptic curve with the private key k.
- Encryption:
  - To encrypt a message, the sender uses the recipient's public key and points on the curve to create a ciphertext.

- This ciphertext can only be decrypted using the recipient's private key.

- Decryption:
  - The recipient uses their private key and the curve's properties to reverse the encryption process and reveal the original message.

Advantages of ECC:

- Smaller Key Sizes: ECC achieves the same security level as RSA with significantly smaller keys, making it ideal for resource-constrained devices and bandwidth-limited applications.
- Enhanced Security: ECC is generally considered more secure than RSA due to the difficulty of solving the underlying mathematical problems.
- Faster Computation: ECC operations often require less processing power, leading to faster encryption and decryption speeds.

However, the security of ECC hinges on the hardness of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). This problem involves finding an unknown integer k, given a point on the curve (k * G).

Quantum Advantage of ECC and RSA:

Shor's algorithm, specifically designed for quantum computers, can solve the ECDLP significantly faster than any known classical algorithm. This means a powerful enough quantum computer could theoretically break ECC keys much quicker.

But as discussed previously, Today's quantum computers are still in their early stages and lack the necessary scale and capabilities to effectively break practical ECC keys. This is likely to hold true for a few years yet. Besides this, increasing the key length of ECC can significantly raise the bar for quantum attackers. Even though factoring up to 512-bit numbers with a quantum computer is theoretically possible, it becomes much more difficult with 1024-bit or higher keys. Despite that, Quantum computers will reach a point in upcoming years that even 2048-bit keys will easily be able to be decrypted. Most implementations of RSA rely on at least 2048-bit keys, which is equivalent to a number 617 digits long. Fujitsu researchers recently calculated that it would take a completely fault-tolerant quantum computer with 10,000 qubits 104 days to crack a number that large.

RSA, compared to ECC, is much more secure. The current recommendation of a 2048-bit RSA number would require 4096 qubits to break. An ECC cipher with 'n' bits in the key takes (2n/2) steps with a conventional computer system, even a sophisticated one by today's standards; with a

quantum computer, the complexity is fixed and never increases. When quantum computing technology advances enough, it might virtually quickly crack any ECC encryption. Similar to RSA, decrypting any ECC-encrypted data on a quantum computer would take no longer than it would on a conventional computer [4].

Grover's Algorithm is another algorithm used in quantum computing. It is essentially a search algorithm for unstructured data searching that uses only "O (sqrt(N))" evaluations of the function, where N is the function's domain size, to find, with high probability, the unique input to any function that yields a given output value. [5]

5.4. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a powerful encryption algorithm that safeguards sensitive information across the digital world. It can be visualized as a complex lock, scrambling data into an unreadable format before allowing authorized access with the correct key.

Overview:

- A symmetric block cipher, meaning it uses the same secret key for both encryption and decryption.
- Processes data in 128-bit blocks, meaning it encrypts data in chunks of 128 bits at a time.
- Supports three key sizes: 128, 192, and 256 bits, offering varying levels of security.

How it works:

- Data is divided into 128-bit blocks.
- The key is expanded into a series of round keys.
- Each block undergoes multiple rounds of operations:
    - Substitution: Bytes are replaced with others based on a predefined table.
    - Shifting: Rows and columns of the data are shifted in specific patterns.
    - Mixing: Data is blended in a non-linear way to increase diffusion and confusion.
- The transformed block becomes ciphertext, unreadable without the key.

Importance:

- Widely adopted: Used in countless applications, from secure communication protocols like HTTPS to protecting files and financial transactions.
- Highly secure: Considered resistant to known attacks, making it a reliable choice for safeguarding sensitive data.
- Efficient: Designed for both software and hardware implementation, offering good performance even on resource-constrained devices.

Future Prospect:

The future of encryption and its vulnerability to quantum computers is a complex and fascinating topic with significant implications for cybersecurity, finance, and even national security. Here's a breakdown of the key points:

The Threat:

- Current encryption methods: Public-key cryptography, like RSA and ECC, relies on the difficulty of factoring large numbers. For example, cracking a 2048-bit RSA key with a classical computer would take billions of years.
- Quantum advantage: By harnessing the principles of superposition and entanglement, Quantum computers could theoretically solve these factoring problems in minutes using algorithms like Shor's algorithm. This would render current encryption methods obsolete, hence we would need new kinds of encryption, preferably constructed using Quantum Computers.

The Timeline:

- Not immediate: Building a quantum computer powerful enough to break real-world encryption is still years, if not decades, away. Current quantum computers are noisy and have limited error correction capabilities.
- Moving forward: Governments, universities, and tech companies are pouring resources into quantum research, both to develop quantum computers and find post-quantum cryptography solutions.

The Impact:

- Vulnerability: If quantum computers crack encryption, it could have a devastating impact on online security. Financial transactions, medical records, and government communications could all be compromised.
- Arms race: The development of post-quantum cryptography could lead to a new arms race between attackers and defenders, as each side tries to stay ahead of the other, again, needing new types of encryptions.

The Solutions:

- Post-quantum cryptography: Researchers are already developing new encryption algorithms that are resistant to quantum attacks. The National Institute of Standards and Technology (NIST) has initiated a competition to select new standards for post-quantum cryptography.

- Quantum-safe infrastructure: Organizations need to start transitioning to quantum-resistant infrastructure now to avoid being caught off guard when quantum computers become a reality.

Discussion and Conclusion:

The document provides a comprehensive overview of quantum computing, encryption principles, and the potential impact of quantum computers on current encryption methods. It begins by tracing the history of quantum computing from Richard Feynman's proposal in 1980 to the development of quantum computers with qubits (quantum bits) capable of superposition and entanglement. The document also delves into classical encryption methods, particularly symmetric and asymmetric key algorithms, and their vulnerabilities. It provides detailed explanations of RSA and ECC encryption, emphasizing the security challenges posed by quantum computers.

The concept of encryption began hundreds of years ago to hide the transmission of sensitive information from the exploiters of such information. Digital encryption was brought about to the top of life by the combined efforts of brilliant minds like Brassard, Heisenberg, Bennett and Wiesner. Decryption is a process that is just as necessary as encryption as without it, there would be no point in simply encoding a message or data. Through the use of quantum mechanics, we can not only decrypt the quantum encrypted message, but also decrypt a classically encrypted message which would normally take a really long amount of time, if it were to be decrypted via classical systems.

Certain formulas and expressions are also discussed in how they can help us in the understanding of the principles of quantum computing, as well as the importance of encryption in new ways, possibly quantum encryption, which would be even harder for quantum computers to break, essentially meaning that quantum decryption and quantum encryption would work against each other, in the same way that Encryption and Decryption work against each other in today’s computers.

The most recent studies on the topic have highlighted that the algorithms like Shor and Grover’s algorithms, previously unutilized due to the limitations of the technology of the time, are now able to be decrypt RSA and ECC encryptions (which would take hundreds of thousands of years with classic computers), through the principles of quantum computing.

The Advanced Encryption Standard (AES) is outlined as a widely adopted and secure encryption algorithm in use today. The document concludes by addressing the future prospects of encryption

in the face of quantum computing, emphasizing the need for post-quantum cryptography and quantum-safe infrastructure to mitigate potential risks in the evolving landscape of cybersecurity.

References:

1. Dwiti P., Khushboo R.N., Sneha T., Tanvi M., B.S. Thakare, 2015, "Brief History of Encryption", "International Journal of Computer Applications (0975 – 8887)" Volume 131 – No.9.
2. IEEE, 2005, "Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005", DOI: 10.1109/ITWTPI.2005.1543949.
3. Georgios M. Nikolopoulos, 2018, "Applications of single-qubit rotations in quantum public-key cryptography." Volume II. B.
4. Zach K., Ming C., "Quantum Computing: The Risk to Existing Encryption Methods"
5. Grover, Lov K., 1996, "A fast quantum mechanical algorithm for database search", Pages: 212-219, DOI: 10.1145/237814.237866
6. Jeffrey Bub, 2007, "Philosophy of Physics, 2007", "QUANTUM INFORMATION AND COMPUTATION", ISBN: 978-0-444-51560-5.
7. Harshad R. Pawar; Dinesh G. Harkut, 2018, "IEEE International Conference on Research in Intelligent and Computing in Engineering (RICE)", "Classical and Quantum Cryptography for Image Encryption & Decryption", DOI: 10.1109/RICE.2018.8509035.
8. Jianxin C. , Dawei D. , Cupjin H. , and Linghang K., 16 June, 2022, "Linear Cross Entropy Benchmarking with Clifford Circuits". Fig. 5