https://rijournals.com/biological-and-applied-science/

RESEARCH INVENTION JOURNAL OF BIOLOGICAL AND APPLIED SCIENCES 3(2):28-31, 2024

©RIJBAS Publications

Online ISSN: 1115-6171

Print ISSN: 1597-2879

The Impact of Quantum Computing on Cryptography

Nzeyimana Eric Titus

Faculty of Engineering Kampala International University Uganda

ABSTRACT

The advent of quantum computing represents a significant challenge to modern cryptography, particularly in the realm of public key cryptosystems. This paper explores the potential implications of quantum computers on current cryptographic techniques, focusing on how quantum algorithms, such as Shor's algorithm, could render widely used encryption methods like RSA and Elliptic Curve Cryptography vulnerable. It also examines the role of quantum key distribution (QKD) in maintaining secure communication in a post-quantum world and discusses the importance of developing quantum-resistant cryptographic algorithms. As quantum computing progresses, the need for post-quantum cryptography becomes increasingly urgent to ensure the continued security of digital information.

Keywords: Quantum Computing, Cryptography, Public Key Cryptosystems, Quantum Key Distribution (QKD), Shor's Algorithm.

INTRODUCTION

This essay will discuss the radical impact that quantum computing is expected to have on modern public key cryptography. The introduction of a reliable and functional quantum computer is expected to have a major influence on the state of information security. Symmetric key encryption is expected to be safe, as current techniques utilized in symmetric key encryption will block cryptanalysis through quantum computing. Quantum Key distribution is expected to be utilized for data transfer worldwide in the future. The impact on decrypting public key systems, like RSA and Elliptic Curve Cryptography, would be catastrophic. The current internet infrastructure would be vulnerable to quantum computing [1]. The advancement of a reliable and practical quantum computer is more difficult than it appears. This essay will discuss why the advancement of quantum computers is slow and will give an analysis of the future possibilities in this field. Since public key cryptography depends on the complexity of problems which are easy for a computer to solve, but hard for a computer to reverse, large scale quantum computers could solve these problems by applying Shor's quantum algorithm. This would make public key systems, like RSA and Elliptic Curve Cryptography, breakable. This would make the internet unsafe for data transfer. Only quantum resistant cryptosystems will ensure the safeness of the internet when large scale quantum computers become a reality [2].

FOUNDATIONS OF CRYPTOGRAPHY

Since the beginning of the 21st century, with the advent of online platforms, enormous dependencies have been created on the web by enabling different complex operations online. This has come with inherent gaps in the system and the need to bridge them through secure connectivity. Significantly, its ubiquity in business, as well as governance, has led to tremendous revision to the design of all network protocols, security for mobile communication, and secure e-commerce. Electronic document security, therefore, is becoming an essential service on the internet leading to research with increased effort in effective methods of algorithm and cryptographic protocol. The concerned content dwelt on the data security on the internet's electronic commerce and electronic document. The knowledge of modern secure devices and algorithms necessitates the understanding of cryptographic tools, the method of applications, and their efficacy. Consistently, information security is the key that can open the door to the positive potentials of IT [3]. The only practical modern form of the encryption of data is secure and robust. It stretches the shortened word - peer to peer - and is twice non-repudiation. The symmetric key algorithm and the public key become the two-table system (asymmetric key algorithm) that will come into use should a state

appear for that of their data payload. 106 Because of preference their safety every one of the enciphered and deciphering the data computer to the data is only one Omniscient controlling the Panel implements because of what single house GPIOs all available. In both above systems: Pop up list can be formed based on using the decrypted password to carry out the cryptography process. The stream cipher algorithm and the block cipher algorithm are two types of firefox phenomena. Stream cipher encrypts the encryption key messages one by one, while Opera adds block into cipher text then encrypts them [4].

CLASSICAL CRYPTOGRAPHY

Classical cryptography is the study of methods for private communications in a public domain where anonymous attacks are expected. The basic principles behind cryptographic methods have not changed significantly over thousands of years. The basic idea involves concealing the messages and then physically protecting the transmission system from unauthorized access. The entirety of human history forms the background for the development and use of these methods including such notable figures as Julius Caesar, Thomas Jefferson, and Alan Turing [5]. The first ciphers were mainly for governments to encode and decode military messages. They have been used by various organizations, such as universities for puzzle competitions and computer security practitioners for education. The Caesar cipher is a basic symmetric encryption that uses integer value for bit shifting. Transposition ciphers involve simple letter transpositions. Complex ciphers like DES and AES use substitution, transposition, and XOR with a key. RSA is a two-key encryption system that can resist quantum computers. Refer to cryptography references for more details [6].

QUANTUM CRYPTOGRAPHY

Quantum cryptography is the study of cryptographic techniques that take advantage of the principles of quantum mechanics, rather than the computational power or assumptions of modern computers. The primary application of quantum cryptography is to securely establish a key, which can subsequently be used as the root of a symmetric cryptographic policy to communicate over an insecure channel [7]. Quantum Key Distribution Quantum key distribution (QKD) protocols allow for the secure establishment of a classical bit exchange between two parties. The most famous QKD protocol, designed by Charles Bennett and Gilles Brassard in 1984, is the BB84 protocol. The BB84 protocol uses a quantum channel and a public authenticated classical channel to distribute a binary string, secure from eavesdroppers. In 1991, Artur Ekert proposed a realizable QKD scheme based on the idea of mutual information and a singlet state. The result of the second QKD protocol, also often referred to as the BB84-like protocol, played a significant role in realizing that certain implementations of QKD were vulnerable to certain types of attacks [8]. A shallow understanding of quantum cryptography is useful in giving an overview of what we might be able to say about the impact of quantum computation on existing cryptographic systems. Quantum Key Distribution (QKD) protocols largely follow this high-level design. They use quantum principles to exchange information and classical principles to resolve the information into a secret key. The significance of this is that it allows the secure establishment of a communication channel between parties who have never met and between whom no trusted secure channels have ever been established [9].

QUANTUM COMPUTING BASICS

Quantum computing is the study, design, and development of computers based on the principles of quantum theory, which explains the behavior of energy and material on the atomic and subatomic levels. A classical computer has a memory made up of bits, where each bit is represented by either a one or a zero. A quantum computer maintains a sequence of qubits. A single qubit can represent a one, a zero, or any quantum superposition of those two qubit states. A pair of qubits can be in any quantum superposition of 4 states and three qubits in any superposition of 8 states. In general, a quantum computer with 'n' qubits can be in a superposition of up to 2^n states simultaneously. In other words, quantum computing has the potential to perform complex calculations and simulate systems beyond the capacity of classical hardware [10]. Quantum computing employs quantum gates that alter probability amplitudes of having particular states of qubits throughout the computation. Commonly employed quantum gates are X Pauli gate (bit-flip gate), Z Pauli gate (phase flip gate), Hadamard gate, Controlled-NOT gate (CNOT), Quantum Fourier transform (QFT) gate, Toffoli gate. Another fundamental quantum mechanic is entanglement, which expresses the notion of correlations that can be established between quantum systems. Those correlations may link particles in a way that makes a pair of particles be found in some specific states. Any changes on one particle will reflect on the other, irrespective of the distance between the two. Entanglement is the reason why quantum bits (qubits) cannot merely be considered separately but are a part of a system. Superposition and entanglement are the underlying concepts exploited by quantum algorithms to gain innovative and unexpected methods for problem-solving and decision-making [11].

QUANTUM ALGORITHMS FOR CRYPTANALYSIS

Quantum computers can break classical cryptographic systems using quantum algorithms and cryptanalysis techniques. They can factorize large numbers quickly with Shor's algorithm, requiring approximately 1600N logical qubits to factor N-bit integers. This algorithm can break widely used public key cryptographic primitives such as RSA, ECC, and ElGamal. Grover's algorithm can search unsorted databases, requiring O(2^(N/2)) operations. This can weaken classical symmetric key ciphers like AES, 3DES, Skipjack by halving the effective key size to maintain security against quantum attacks [12]. In general, limited forms of quantum key exchange such as quantum key distribution (QKD), quantum coin flipping, and quantum digital signatures are secure against attackers that have been presumed to possess quantum computers with sufficiently advanced capabilities. Shor's algorithm could potentially break the cryptographic layer and decrypt the ciphertext without requiring access to the symmetric session keys exchanged between users during the handshake. However, thus far, no one has publicly implemented Shor's algorithm on a quantum computer. The exact amount of time it will take to realize large-scale quantum computers is unknown. However, it is estimated that cryptosystems based on the computational hardness of specific problems (e.g., the factoring problem) will be broken if a large quantum computer can be created, and which can perform enough number of logical qubit operations to sufficiently outperform classical computers [13].

POST-QUANTUM CRYPTOGRAPHY

Various approaches and cryptographic algorithms resistant to quantum computers are known as 'Post-Quantum Cryptography (PQC).' These algorithms provide secure encryption even against future quantum computer attacks. Post-quantum cryptography is divided into 'public key' and 'symmetric key' categories. Public key post-quantum cryptography includes lattice-based, code-based, multivariate, hash-based, and elliptic curve isogeny cryptography [14]. All proposed post-quantum symmetric key cryptographic algorithms are essentially variants of current symmetric key cryptographic algorithms, and they are considered secure regardless of quantum computers. The implications of quantum computing may also impact cryptanalysis. The computations required to break particular cryptographic schemes using classical computers would be infeasible given the cost-performance of today's hardware and software systems; however, with the advent of quantum computers, these computations may become practical. Post-quantum cryptography has emerged to enhance data security in the quantum era. In today's digital world, data is traffic at a phenomenal rate having a shelf life of years or even decades depending on the sensitivity of the information. As long-term data security is essential, there is a growing need for cryptographic algorithms designed to resist encryption-breaking efforts of quantum computers [15].

CONCLUSION

Quantum computing poses an existential threat to the current landscape of cryptography, especially to public key systems that are foundational to internet security. While symmetric key encryption remains largely secure, public key cryptosystems like RSA and ECC are at risk of being easily broken by quantum algorithms. This necessitates the development and implementation of quantum-resistant cryptographic methods to safeguard data in a future where quantum computers are a reality. The transition to post-quantum cryptography will be critical in maintaining the security and integrity of global communications and information systems in the quantum era.

REFERENCES

1. Alexeev Y, Bacon D, Brown KR, Calderbank R, Carr LD, Chong FT, DeMarco B, Englund D, Farhi E, Fefferman B, Gorshkov AV. Quantum computer systems for scientific discovery. PRX quantum. 2021 Feb 1;2(1):017001. aps.org
2. Redkins B, Kuzminykh I, Ghita B. Security of Public-Key Schemes in the Quantum Computing Era–A Literature Review. IEEE Access. 2023. researchgate.net
3. Anerousis N, Chemouil P, Lazar AA, Mihai N, Weinstein SB. The origin and evolution of open programmable networks and SDN. IEEE Communications Surveys & Tutorials. 2021 Feb 22;23(3):1956-71. [HTML]
4. Srinivasan AB, Hemalatha S. A table-based end to end encryption technique without key exchange. Engineered Science. 2022. espublisher.com
5. Shores D. The Evolution of Cryptography Through Number Theory. 2020. gcsu.edu
6. Luukkanen J. Post Quantum Cryptography: impact to the public key cryptography. 2022. theseus.fi
7. Pillai SE, Polimetla K. Analyzing the Impact of Quantum Cryptography on Network Security. In2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) 2024 Feb 23 (pp. 1-6). IEEE. researchgate.net

8. Nandal R, Nandal A. Simulation and Comparison of BB84 and SSP99 QKD Protocols. InInternational Conference on Advanced Network Technologies and Intelligent Computing 2023 Dec 20 (pp. 131-153). Cham: Springer Nature Switzerland. [HTML]
9. Al-Ghamdi AB, Al-Sulami A, Aljahdali AO. On the security and confidentiality of quantum key distribution. Security and Privacy. 2020 Sep;3(5): e111. [HTML]
10. Cruise JR, Gillespie NI, Reid B. Practical quantum computing: The value of local computation. arXiv preprint arXiv:2009.08513. 2020. [PDF]
11. Khatami MH, Mendes UC, Wiebe N, Kim PM. Gate-based quantum computing for protein design. PLOS Computational Biology. 2023 Apr 12;19(4): e1011033. plos.org
12. Nwaokocha BTM. Shor's Algorithm in Quantum Cryptography. 2020. academia.edu
13. Kumar M, Mondal B. Study on Implementation of Shor's Factorization Algorithm on Quantum Computer. SN Computer Science. 2024. [HTML]
14. Balamurugan C, Singh K, Ganesan G, Rajarajan M. Code-based post-quantum cryptography. 2021. preprints.org
15. Malina L, Dzurenda P, Ricci S, Hajny J, Srivastava G, Matulevičius R, Affia AA, Laurent M, Sultan NH, Tang Q. Post-quantum era privacy protection for intelligent infrastructures. IEEE Access. 2021 Feb 24; 9:36038-77. ieee.org

CITE AS: Nzeyimana Eric Titus. (2024). The Impact of Quantum Computing on Cryptography. RESEARCH INVENTION JOURNAL OF BIOLOGICAL AND APPLIED SCIENCES *3*(2):28-31.