Quantum Computing Supremacy in the Internet of Things

Subjects: Computer Science, Cybernetics | Computer Science, Information Systems | Computer Science, Hardware & Architecture
Contributor: Shuhab Shamshad, Farina Riaz, Rabia Riaz, Sanam Shahla Rizvi, Shahab Abdulla

The Internet of Things (IoT) strongly influences the world economy; this emphasizes the importance of securing all four aspects of the IoT model: sensors, networks, cloud, and applications. Considering the significant value of public-key cryptography threats on IoT system confidentiality, it is vital to secure it. One of the potential candidates to assist in securing public key cryptography in IoT is quantum computing. Although the notion of IoT and quantum computing convergence is not new, it has been referenced in various works of literature and covered by many scholars. Quantum computing eliminates most of the challenges in IoT.

Keywords: cryptography ; quantum computing supremacy ; quantum communication ; public-key cryptography ; Internet of Things (IoT) ; quantum computing

1. Introduction

The Internet of Things (IoT) is becoming increasingly popular in biomedical, academic, manufacturing, and other fields that need an extensive network of microcontrollers. Quantum features such as entanglement and superposition are employed to solve complicated problems. However, there are specific points of contention regarding molding and measuring quantum speed. One apparent challenge is the difference in computing capability between conventional and quantum computers.

The encryption procedure is used to safeguard data-in-transit (communications), data-at-rest (stored), data-in-use (in memory), data integrity (digital signature), and all authentication processes (identity validation). With the advent of quantum computing, it will be possible to shorten the time required to break some of the encryption algorithms currently in use, particularly the asymmetric algorithms (i.e., public key algorithms) that are used to establish communication protocols such as SSL and TLS (used for HTTPS) or to sign information digitally.

Data must be processed in a single binary state in classical computing based on the Boolean logic field of science. Several fundamental particles, such as electrons or photons, can be used to represent zero or one in a quantum computer, depending on their charge or polarization. All these particles' properties and performance are referred to as a quantum bit, or qubit, in the quantum computing idea [1].

The two most important aspects of quantum physics are quantum superposition and entanglement. Quantum entanglement enables qubits divided over unbelievable ranges to function immediately (not restricted to the speed of light). Although the gap between the associated particles is large, they remain entangled if separated. Significant processing power gain can be achieved by combining quantum superposition and interposition. In an ordinary computer, only one of four binary configurations (00, 01, 10, or 11) is saved at any time; however, a 2-qubit registry will instantaneously store all four qubits, each representing two numbers. When many qubits are used, the capacity increases exponentially [1].

1.1. Quantum Computation

Just as classical computation involves bits, quantum computation uses quantum bits and qubits, usually denoted using "bra–ket" notation as $|\psi\rangle$. The "state-vector" of the qubit is represented by a ket, which is just a vector representation. The equivalent $|0\rangle$ or $|1\rangle$ states of qubits may be like conventional bits with 0 or 1. It is like a linear combination of the amplitudes of probability for each of the kets α and β, where $\alpha|0\rangle + \beta|1\rangle = 1$ and $|\alpha|^2 + |\beta|^2 = 1$ [2].

A quantum machine can read or "measure" a qubit like a computer can read the value of a conventional bit. In the measurement, the qubit's state is collapsed to one of two values, $|0\rangle$ or $|1\rangle$, depending on the state of the measure. The

likelihood of a vector collapsing into one of two states is proportional to the square of its amplitude. Even if the superposition collapse's precise mechanism is unclear, it is an essential characteristic of quantum mechanics since it was obtained from practical evidence. In the same way that 0 and 1 are binary, these states will be employed for calculation.

Consider the qubit $|\psi\rangle = 1/\sqrt{3}|0\rangle + (2/3)^{1/2}|1\rangle$, which has the value $1/3|0\rangle + \sqrt{3}|1\rangle$. The likelihood that $|\psi\rangle$ will be equal to $|0\rangle$ when measured is $(1/3)^2$, which is one-third. This vector formula may be used to define any qubit or state vector that exists. It is stated that the qubit is in a superposition of the values $|0\rangle$ and $|1\rangle$ if $|\psi\rangle$ is a linear combination of $|0\rangle$ and $|1\rangle$ and neither amplitude is zero in this case. In quantum computing, superposition is a fundamental property that cannot be ignored [2]. To modify probability, quantum operators known as gates are needed. For example, the Z gate inverts the qubit in the way given in Equations (1) and (2). Similarly, the Hadamard gate, or H gate, performs a "quarter turn", shown in Equations (3) and (4).

$$|\psi\rangle = |0\rangle \rightarrow Z \rightarrow |\psi\rangle = |1\rangle \quad (1)$$

$$|\psi\rangle = |1\rangle \rightarrow Z \rightarrow |\psi\rangle = |0\rangle \quad (2)$$

$$|\psi\rangle = |0i \rightarrow H \rightarrow |\psi\rangle = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle \quad (3)$$

$$|\psi\rangle = |1i \rightarrow H \rightarrow |\psi\rangle = 1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle \quad (4)$$

To test this hypothesis, $|\psi\rangle$ in this condition may be measured where the H gate is applied and α and β both equal $1/\sqrt{2}$, and $(1/\sqrt{2})^2 = 1/2$, where it will have the same chance of falling to either $|0\rangle$ or $|1\rangle$ as soon as the H gate is applied.

A basis is a collection of vectors against which to measure, with many different bases. The H gate inserts $|0\rangle \rightarrow |+\rangle$ and $|1\rangle \rightarrow |-\rangle$, but it also converts the Hadamard basis to the standard basis: $|+\rangle \rightarrow |0\rangle$ and $|-\rangle \rightarrow |1\rangle$.

The standard and Hadamard bases are referred to as orthonormal bases because of their perpendicular relationship. That is, if a $|\psi\rangle = |+\rangle$ or $|\psi\rangle = |-\rangle$ value is measured on the standard basis, it has a 50% probability of being $|0\rangle$ or $|1\rangle$ and vice versa [2].

Quantum computers can solve the DLP on an n-bit integer in O ($n2\log n \log\log n$) time [3]. As a result, the rising popularity of quantum computers presents a severe danger to the Diffie–Hellman KEP and asymmetric encryption security. The BB84 protocol is a quantum key distribution (QKD) protocol that enables two parties to utilize a verifiably secure channel to co-create a shared key that can then be used to encrypt communications symmetrically.

Scholars debate on many forms of quantum speed and quantum computers, each of which is meant to handle a particular set of problems. Existing cryptographic approaches might be revolutionized by quantum computers, which are expected to appear soon. According to experts and academics who have analyzed technical literature, quantum computers can execute algorithms that enable the decryption of encrypted communications without needing a decryption key. These quantum algorithms, they claim, will make "existing cryptography approaches easier to break". When these algorithms are broken, the victims are exposed to significant strategic and security concerns.

Although there has been a significant interest in quantum cryptosystems, more studies on their IoT application are still required. This article explains how to create quantum-resistant solutions for the future generation of Internet of Things developers. This system deals with implementing the BB84 protocol using the simulation package SimuloQron. The proposed architecture ensures the security of the Internet and other cryptographic-based systems. It is essential to expand the mathematical analysis to construct a quantum-resistant design for future encryption.

2. Quantum Computing Supremacy in the Internet of Things

The Internet of Things (IoT) is a concept in which devices and gadgets connect without requiring human engagement. This happened earlier in the SCADA and ICS industries when conventional networking protocols became accessible through the Internet. For instance, commands can be issued to instruct the use of IP protocols based primarily on MPLS over open communication networks in hundreds of thousands of homes, to guide the connection of intelligent meters or instruct the connection of devices that support smart cities, or to direct the connection of hundreds of thousands of autonomous vehicles on the roads. IoT technology has increased the demand for smart appliances in various industrialized health insurance, logistics support, and agricultural sectors [4]. Data integrity is checked to guarantee that data division performed by globally scattered IoT devices is suitable and effective. Because of such revolutionary infrastructures, new defense weaknesses emerge. The attack vectors' scale is unparalleled, with a single successful infiltration potentially affecting millions of devices [5].

A single photon is a minimal amount of light that obeys the laws of quantum physics. This means that an eavesdropper cannot measure the value of a photon while allowing the other half to continue its path. In QKD, the two legitimate parties work together to prevent eavesdropping by forcing the eavesdropper to introduce errors. One of the pioneers or founders, Richard Feynman, suggested and demonstrated that quantum mechanical features could be exploited in communication if information bits can be physically described [6]. Encoding transmission of information can be done via electron spin, photon dispersion, or other quantum features.

2.1. Quantum-Based Communications

Because of the features of quantum information, quantum communication and information processing outperform conventional communication and information processing in many ways. Quantum information attributes include, but are not limited to, the concept of uncertainty, the non-clone quantum theory, quantum teleportation, and hidden quantum information traits that may be exploited for resistance attacks during cyberspace transmission [7]. The main idea of the principle of uncertainty is the impossibility of determining the particulate position in the micro-world. German physicist Heisenberg introduced the uncertainty principle in 1927 [8].

The unclosed and undeleted characteristics of an unknown quantum state are quantum non-cloning theory. Cloning means that another system can produce an identical quantum state. Researchers have shown that machines cannot replicate quantitative approaches [9]. The undeleting principle may ensure that the enemy's removal and damage of quantum information are reflected in the secure communication of security and communications networks. In nature, it was suggested that linearity in quantum theory is not permitted to delete a copy of an arbitrary quantum [10].

2.2. Quantum Teleportation

The sender measures the quantum state of the original, which the sender classically communicates. Quantum information is the remaining information not extracted in the measurement by the sender and sent on by metric measurement to the recipient. In 1993, an unknown quantum state was proposed to be introduced into televisions [11]. Quantum information has features that classical details do not have. Only standard measurement can expose the quantum code's information while the quantum code is in its entangled state, and this information cannot be accessed by local measure [11]. While desktop quantum code breakers are no longer available, quantum ciphers may still be bought, putting defenders one step ahead of attackers. Symmetric-key cryptography is theoretically secure if a few conditions are met. The single significant drawback to this strategy is the key exchange between Alice and Bob, which requires frequent contact or a considerable investment in infrastructure (e.g., mobile cellular networks).

The non-cloning theorem results from the postulates ensure this criterion is met by quantum key distribution methods such as BB84 and B92 and their management [12]. Previously, conventional computer information could be copied without limitation. Although this quality is usually good, it can be dangerous in some instances (e.g., quantum information has features that classical details do not have). The orthogonal nature of the classical states |0i and |1i makes them simpler to identify. The non-cloning theorem allows quantum computing to separate only orthogonal and known states [13].

Since no computer hardware can distinguish between two nonorthogonal qubits, this problem exists. Continuous-variable quantum key distribution techniques may be implemented since existing key distribution systems employ coherent states rather than single photons. Herein, it then move on to another key communication challenge, capacity, while wthe comforting answer was possessed for future secure communications in the hands. Entanglement-assisted classical capability enhances the degree of independence by permitting entangled (i.e., correlated) states at the input encoder and joint measurement at the receiver end. Although this technology can potentially increase power, the size of the gain is uncertain.

2.3. Public-Key Cryptography and Quantum Computing

Cryptographers manage the power to hide and unhide information using a "key". The terms "symmetric key" and "public key" are sometimes used interchangeably. Since the emergence of quantum parallelism, quantum computers have performed far better than conventional computers. No matter how fast a computer can process information, the processing capacity of quantum computers will be restricted due to physical considerations. When constructing an algorithm, its spatial and temporal complexity maybe considered. This requires not only large-scale quantum computers but also a reasonably lengthy quantum coherence period. If the above two requirements are not satisfied, the operation cannot be completed.

Shor's algorithm reduced the processing cost of significant integer factorization to a polynomial level [14]. This complexity is equivalent to the RSA public-key cryptography protocol's encryption and decryption, demonstrating that the RSA is vulnerable in universal quantum computing. Other quantum algorithms, such as Grover's search algorithm [15] and its improved versions, as well as the Harrow, Hassidim, and Lloyd (HHL) algorithm, display various types of higher speeds for addressing many difficulties [16]. Because of the enormous processing capability of quantum algorithms, researchers have begun to hunt for suitable physical devices for quantum computing implementation. The public key encryption strategy must be modified regularly due to the rapid growth of quantum computing technologies. As a result, cryptologists are continuously on the lookout for public-key protocols that can survive quantum computing assaults, resulting in post-quantum cryptography creation.

Traditional cryptographic algorithms are unsafe or need larger key sizes if large-scale quantum computers are on the market. T

This has resulted in the wide spread of public-key cryptosystems such as RSA, ECC, and DH [17]. They are now included in critical Internet protocols such as the TLS, which conventional computer systems and connected devices use to communicate with one another. On the other hand, recent technology innovations and telecommunications have simplified the computing work required to crack asymmetric systems, raising the suggested minimum key size. For instance, since 768-bit and 1024-bit RSA implementations were compromised in 2010, the minimum recommended key size for RSA is between 2048 and 4096 bits (depending on the protected information type). Expansion of the key size is a stopgap measure until technology catches up and delivers the required computing effort [18][19].

If the present state of technology allows for the development of great large-scale quantum computing devices, the performance of the Shor algorithm on these systems may be explored. The time complexity of the conventional cracking strategy on RSA is roughly Ex (O (log N) $e^{(1/3)}$ (log N) $e^{(2/3)}$), while the time complexity of the modern cracking approach on RSA is approximately O (log3 N). Because Shor's factoring algorithm has an O (log3 n) temporal complexity and is implemented in a neighbor-only, two-qubit-gate, competitor-like (NTC) architecture, the quantum algorithm of Shor poses a significant threat to the security of public-key-encrypted RSA encryption keys.

A classical computer may have a clock frequency of around 10 GHz, implying that the gate speed is approximately 0.1 ns. The trapped ion system and superconducting circuits are, without a doubt, terrible. This can only be done in a 10 s and 20 ns quantum operation. After considering quantum-resistant solutions, the National Security Agency (NSA) suggested in 2015 that the Suite B group's ECC security be increased. Current public-key cryptosystems are vulnerable to quantum computing, according to the NSA. Quantum computers, according to a new *Technology Review* study, will be able to readily break sophisticated cryptosystems within the next 20 years [20].

In previous studies, the researchers used different techniques to improve public-key cryptography. Keshavarzian suggested an improved deep residual network model for human activity identification based on IoT technologies. Using a range of smartphone sensors, the human body signals were recognized and analyzed on the cloud computing platform. Moreover, a function-as-a-model for real-time measuring activity in the cloud was proposed. The suggested approach outperformed various state-of-the-art decision-making methods [21]. A secure IoT-based network architecture based on blockchain technology was proposed in [21] for hybrid industrial applications. Accordingly, the benefits of IoT-based service delivery include cost-effectiveness and precision. Blockchain technology was used to ensure real-time data and guarantee transparency among industrial users.

In 2019, Thigale et al. introduced a breakthrough in IoT, namely a framework for safeguarding data transfer; an IoT protocol resistant to cross-layer assaults was offered . Moreover, the system was designed to deal with time constraints and accessible delivery [22]. In 2019, J. Cao created a quantum-resistant access authentication and data allocation approach for large-scale Internet of Things networks. The suggested approach decreased network bandwidth while offering the highest security and privacy against quantum threats. The proposed model was evaluated in real time and yielded the best results [23].

The intelligence service and its analysis can be improved by combining quantum cryptography, ML, and AI techniques. These intelligence services claim to be able to decrypt 2048-bit RSA encryption in 8 h or less, a job that would take the fastest supercomputers in the world roughly 300 trillion years to perform using brute force. Quantum computers may need over 20 million qubits. This field's developments indicate that such machines might exist in 25 years. If results in quantum decryption outpace progress in quantum encryption, there is a possibility that malicious use of such computers might endanger national and international security because of the reduction in duration from millions of years to a few seconds [24][25].

The National Quantum Initiative Act of 2018 established a coordinated government initiative with USD 1.275 billion in financing over five years to speed up quantum research and development. Additionally, it defined the duties of the National Quantum Coordination Office, the National Quantum Initiative Advisory Committee, and the National Science and Technology Council Subcommittee on Quantum Information Science. Notably, funding in 2019 and 2020 exceeded the budget set by Congress, demonstrating the importance placed on quantum research and development by the United States [26].

Rosa M. Gil Iranzo discusses the drawbacks of interfaces for quantum computing that make it easier to master the new paradigm. A layer to establish appropriate learning conditions for carrying out computations without enhancing mastery of the fundamental ideas of quantum computing was suggested. The emphasis of planned work is human-centered computing, which will support levels such as high school, university, and research. This study uniquely integrates science and technology to build interfaces for quantum computing [27].

U. Chukwu used two quantum-ready techniques, quadratic unconstrained binary optimization (QUBO) and constrained-optimization sampler, to tackle the NP-Hard graph issue of graph partitioning. Both methods frequently produced better partitions than the standard graph partitioners designed for that specific purpose [28].

The idea of quantum computing has advanced to the point that it is no longer considered science fiction. As they are entirely new fields, quantum clinical medicine and quantum surgery have yet to reach their total growth and potential. These fields are conceptual extensions of quantum computation and many body systems. To allow these fields to ultimately materialize and mature into secure clinical applications that benefit humanity, novel formalisms and methods must develop [29].

As a result, the cybersecurity sector is preparing for future development by using cutting-edge technologies such as AI, quantum computing, blockchain, and data science. Quantum computing is an emerging field that uses the ideas of quantum mechanics and combines them with computer science, physics, and mathematics to accomplish calculations. This new computing technique can solve various complex scientific problems and open new possibilities. Soon, cybersecurity infrastructure will be rendered obsolete by the development of futuristic technology [30].

References

1. Eleanor, R.; Wolfgang, P. Quantum Computing: A Gentle Introduction; The MIT Press: Cambridge, MA, USA, 2011.
2. Nielsen, M.A.; Chuang, I.L. Quantum Computation and Quantum Information, 10th ed.; Cambridge University Press: New York, NY, USA, 2011.
3. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.
4. Jiang, C.; Chen, Z.; Su, R.; Soh, Y.C. Group greedy method for sensor placement. IEEE Trans. Signal Process. 2019, 67, 2249–2262.
5. Bacsardi, L. Resources for Satellite-Based Quantum Communication Networks. In Proceedings of the 2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES), Las Palmas de Gran Canaria, Spain, 21–23 June 2018; pp. 97–102.
6. Shen, J.; Zhou, T.; He, D.; Zhang, Y.; Sun, X.; Xiang, Y. Block design-based key agreement for group data sharing in cloud computing. IEEE Trans. Dependable Secur. Comput. 2017, 99, 996–1010.
7. Heisenberg, W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. In Original Scientific Papers Wissenschaftliche Originalarbeiten; Blum, W., Rechenberg, H., Dürr, H.P., Eds.; Werner Heisenberg Gesammelte Werke Collected Works, Vol A/1; Springer: Berlin/Heidelberg, Germany, 1985.
8. Ballentine, A.P. Quantum Theory: Concepts and Methods. Am. J. Phys. 1995, 63, 285–286.
9. Braunstein, A.K. Impossibility of deleting an unknown quantum state. Nature 2000, 404, 164–165.
10. Terhal, B.M.; DiVincenzo, D.P.; Leung, D.W. Hiding Bits in Bell States. Phys. Rev. Lett. 2001, 86, 5807–5810.
11. Niemiec, M.; Pach, A.R. Management of security in quantum cryptography. IEEE Commun. Mag. 2013, 51, 36–41.
12. Shor, P.A. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.

13. Imre, S.; Balazs, F. Quantum Computing and Communications—An Engineering Approach; John Wiley and Sons Ltd.: Hoboken, NJ, USA, 2005.
14. Grover, L. Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. 1997, 79, 325–328.
15. Long, G.L.; Zhang, W.L.; Li, Y.S.; Niu, L. Arbitrary phase rotation of the marked state cannot be used for Grover's quantum search algorithm. Commun. Theor. 1999, 32, 335–338.
16. Diffie, W.; Hellman, M.E. New directions in cryptography. IEEE Trans. Inf. Theory 1976, 22, 644–654.
17. Menezes, N.K. A Riddle Wrapped in an Enigma. IEEE Secur. Priv. 2016, 14, 34–42.
18. Keshavarzian, A.; Sharifian, S.; Seyedin, S. Modified deep residual network architecture deployed on the serverless framework of IoT platform based on human activity recognition application. Future Gener. Comput. Syst. 2019, 101, 14–28.
19. Thigale, S.B.; Pandey, R.K.; Gadekar, P.R.; Dhotre, V.A.; Junnarkar, A.A. Lightweight novel trust-based framework for IoT-enabled wireless network communications. Period. Eng. Nat. Sci. PEN 2019, 7, 1126–1137.
20. Cao, J.; Yu, P.; Xiang, X.; Ma, M.; Li, H. Anti-quantum fast authentication and data transmission scheme for massive devices in 5g nb-IoT system. IEEE Internet Things J. 2019, 6, 9794–9805.
21. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the Ninth International Conference on Computational Intelligence and Security, Emeishan, China, 14–15 December 2013.
22. Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys. Rev. Lett. 2003, 91, 057901.
23. Gilyén, A.; Lloyd, S.; Marvian, I.; Quek, Y.; Wilde, M.M. Quantum Algorithm for Petz Recovery Channels and Pretty Good Measurements. Phys. Rev. Lett. 2022, 128, 220502.
24. Burek, E.; Wronski, M.J.; Mank, K.; Misztal, M. Algebraic attacks on block ciphers using quantum annealing. IEEE Trans. Emerg. Top. Comput. 2022, 10, 678–689.
25. Tang, Y.; Ba, Y.; Li, L.; Wang, X.; Yan, X. Lattice-based public-key encryption with conjunctive keyword search in multi-user setting for IIoT. Clust. Comput. 2022, 25, 2305–2316.
26. Subcommittee on Quantum Information Science. National Quantum Initiative Supplement to the President's F.Y. 2021 Budget. January 2021. Available online: https://www.quantum.gov/wp-content/uploads/2021/01/NQI-Annual-Report-FY (accessed on 14 July 2021).
27. Iranzo, R.M.G.; Cairol, M.T.; González, C.G.; García, R. Learning Quantum Computing: An Interaction Protocol for Quantum Computing Interfaces. ACM Int. Conf. Proceeding Ser. 2021, 13, 1–5.
28. Chukwu, U.; Dridi, R.; Berwald, J.; Booth, M.; Dawson, J.; Le, D.; Wainger, M.; Reinhardt, S.P. Constrained-optimization Approach Delivers Superior Classical Performance for Graph Partitioning via Quantum-Ready Method. In Proceedings of the 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 22–24 September 2020.
29. Davids, J.; Lidströmer, N.; Ashrafian, H. Artificial Intelligence in Medicine Using Quantum Computing in the Future of Healthcare. In Artificial Intelligence in Medicine; Lidströmer, N., Ashrafian, H., Eds.; Springer: Cham, Switzerland, 2022.
30. Faruk, J.H.; Tahora, S.; Tasnim, M.; Shahriar, H.; Sakib, N. A Review of Quantum Cybersecurity: Threats, Risks and Opportunities. In Proceedings of the 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, 24–26 May 2022; pp. 1–8.