Beyond Binary: The Capabilities of Classical and Quantum Computing for Securing Data Transmission

B V N Prasad Paruchuri[1], Madhu Latha Veerapaneni[2], *G. Ramesh*[3*], *Vinay Kumar Awaar*[4], Abhilasha Chauhan[5]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Guntur, India
[2]Department Master of Business Administration, VR Siddhartha Engineering College, Vijayawada, India
[3]Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India
[4]Department of Electrical and Electronics Engineering, Gokaraju Rangaraju Institute of Engineering and Technology Hyderabad, India.
[5]Uttaranchal Institute of Management, Uttaranchal University, Dehradun,India

Abstract. In the present times, the demand for sophisticated encryption methods has escalated, especially for securing data transmission in vulnerable environments. These methods leverage diverse algorithms to fortify the integrity of communication channels. Quantum mechanics plays a pivotal role in two specific areas: quantum key distribution and property-based cryptography, both of which contribute to establishing secure communication protocols. This study focuses on conducting a comparative evaluation of classical and quantum cryptography, employing various cryptography algorithms. The objective is to ascertain the optimal algorithm within each realm classical and quantum cryptography for ensuring robust security.

1. Introduction

In general, computational mechanics can be categorized into two distinct paradigms: classical mechanics and quantum mechanics [1]. Within classical computational mechanics, an object's position and time are precisely determined. However, in the realm of quantum computing, objects reside in a realm of probabilistic ambiguity. This signifies that objects hold potential to occupy either point A or point B.

*Corresponding author: ramesh680@gmail.com

Theoretically, quantum computers are more intricate compared to their classical counterparts, yet they offer heightened computational potential. Conversely, classical computers exhibit limited computing power in comparison to quantum computers and face challenges in seamless scalability [2-3].

1.1 Classical vs Quantum

The CP-ABE & QKD Algorithm provides privacy and security over the different applications such as cloud, IoT, Ect. [4-7]. Eavesdropping will be the process of easily monitoring any classic private channel without the knowledge of the sender or receiver.

Applying the principles of macroscopic object theory alongside classical physical phenomena, like radio signals, presents an avenue for non-invasive measurement of an object's physical attributes without causing disruption to other properties. This key aspect involves computations that extract such information from signals or objects endowed with these physical traits. In contrast, classical cryptography harbors an inherent vulnerability to passive eavesdropping, a susceptibility that remains open and potentially exploitable.

Quantum theory is the basis of quantum cryptography and will guide all objects, the consequences of which will be noticed mainly in microscopic systems such as individual atoms or subatomic particles. Computing power doubles every 18 months, IT costs

2. Technologies and Algorithms Used

The exponential growth in the number of connected devices today produces a plethora of data. Therefore, data privacy has become a major concern in CC. We use this CP-ABE policy because the security of the data generated has become a major concern to guarantee the security of transactions on the Internet. Here, the ciphertext is analyzed according to the input model and with less time and space than the private key character [8]

3. Related Work

The IoT's limited resources mean that cloud computing is often used to handle the large amounts of data produced by IoT devices [15, 16]. However, using the cloud It can compromise user privacy and lead to data breaches. To solve these problems, Attribute-Based Encryption (ABE) is one of the best ways to provide greater security for data stored in the cloud.

Table 1: Quantum Key Distribution and its Artifacts.

S.No.	Artifacts of Algorithm	Description
1	Inputs:	.PDF, .PNG, .DOC, .PPT Etc .. Files.
2	Cloud web page	Cloud hosting is the ability to use the cloud to make. Applications and websites available on the Internet. Cloud hosting provides the scalability and flexibility to make changes quickly by pooling computing resources from a network of virtual and physical servers.
3	Python libraries	Open-ABE library - Open encryption library with behavior-based encryption in Python
4	DGK Function	This the function we developed in our earlier project to generate different key for every attempt of login into page to access resources based on personal data of the users.

5	QKD (Quantum Key Distribution)	Quantum key distribution (QKD) is a secure communication method for exchange of cryptographic keys between parties. It uses the features of quantum physics to exchange encryption keys in a proven and secure way.

The combination of dynamic nonlinear polynomial chaotic quantum hash technology and secure blockchain structure can enhance cloud data security while protecting user privacy [9]. The proposed method uses dynamic chaotic mapping functions for key initialization, encryption and decryption. The simulation results show that this method is more accurate than the current model in terms of minor changes and significant signs. encryption, and decryption time.[10] In this paper the authors explored a novel algorithm centered around blind quantum computing, aimed at fortifying the communication between a data owner and a cloud service provider (CSP). Additionally, we enhanced the hierarchical attribute-based encryption (ABE) algorithm by integrating BCQ (Blind Quantum Computing) key sharing. This integration serves to streamline user data sharing and group access to cloud-stored data. The experimental findings showcased the effectiveness of our approach, surpassing the efficiency of prior enhancements made to the CP-ABE (Cipher Policy Attribute-based Encryption) technique. In [11-14] the authors have been discussed the resumption of the median form and its physical Believable resumption results Quantum deformed double and triple positive potential. Although the limited instantons do not cause the energy spectrum in the quasi-classical order of quantum deformations, they can cause some quantum deformations where energy level correlation occurs. If the deformation is not well quantified, the instanton effect disappears, but the high degrees in the semi-classical remain. Saddle contributions are classified as fading or robust. Additionally, the paper demonstrates the perturbative/nonperturbative relation in quantum deformed triple-well potential using period integrals and Mellin transform computations.[17] The advancement in electronic communication has led to a need for secure data transmission, and key distribution algorithms are crucial in modern cryptography.

The RSA and Diffie-Hellman are two classical algorithms used for key distribution, which rely on mathematical manipulations involving large prime numbers. These algorithms are designed to provide strong security measures and make it practically impossible to break the encryption within a reasonable timeframe. [18] This paper discusses how quantum mechanics reveals Physical information is separate because the properties of quantum mechanics are the only properties that can be seen in the context of physical interactions and from a single point of view. He argues that Hermann's solution to the objective problem of quantum mechanics is based on neo-Friesian theory, if not a solution from Kant's doctrine of word discipline.

A mathematical framework that unifies stochastic processes and quantum mechanics, demonstrating that non-relativistic quantum mechanics of a single particle on a flat space can be described by a rotated Wiener process[19]. The framework is then extended to relativistic stochastic theories on manifolds using second order geometry. The paper also shows that consistent path integral formulations of quantum theories on Lorentzian (Riemannian) manifolds require an Itˆo deformation of Poincar´e (Galilean) symmetry due to the coupling of the quadratic variation to the affine connection.[20-24] Without direct control over the data stored in the data center, cloud users face security challenges that create integrity, confidentiality, security and privacy concerns.

Addressing the previously outlined difficulties, this article an innovative solution: the Quantum Hash-centric Cryptographic Policy Attribute-based Encryption (QH-CPABE) framework. The primary objective of this framework is to bolster the levels of security and confidentiality concerning data within cloud-based applications. The proposed model uses large medical data, and as a recommendation, does not form a large cloud and makes it more efficient, about 92% change bit hashing, chaotic dynamic key generation, encryption and decryption time accuracy about 96% information compared to the traditional model.[24-29] The paper proposes the implementation of Quantum Key Distribution (QKD) algorithm using photon polarization property for ultimate security assurance.

A complex and expensive experimental setup is used to generate photon stream with laser light and stepper motor with arduino for polarization.. The algorithm allows for the aring of secure keys while detecting any attempt of eavesdropping.[30-36] Across the globe, cloud providers facilitate the migration of cloud-based applications, software, and substantial data repositories into expansive data centers. However, a notable dilemma emerges as cloud users lack direct oversight over the information housed within these data centers. This absence of control leaves them uncertain about the safeguarding, confidentiality, integrity, and privacy of their vital data. This distinctive aspect of cloud services gives rise to a plethora of intricate security concerns and potential conflicts[37-40].

Addressing the pressing security challenges, we present an innovative solution: the Quantum Hash-centric Cipher Policy-Attribute-based Encipherment (QH-CPABE) framework. This framework serves to elevate the levels of security and privacy surrounding sensitive data stored within the cloud. Our approach encompasses both structured and unstructured clinical data within the cloud environment. Empirical findings underscore the precision of our proposal, boasting an impressive accuracy rate of approximately 92% for bit hash alteration detection and around 96% for the generation of dynamically chaotic keys. Moreover, our framework outperforms established benchmarks in terms of efficiency, as evidenced by the expedient encryption and decryption times in comparison to conventional standards documented in existing literature.

4. Qhcpabe For Key Generation Algorithm

The QHCPABE algorithm combines QKD standard for the generation of dynamic randomized keys with HCPABE standard for effective encryption.

```
#Algo: QHCPABE for Key Generation
1. Function: generate_key()
1.1. Set key_len = 100.
1.2. Create empty lists user_1_bits, user_2_bits, user_1_bases, and user_2_bases.
1.3. For i = 1 to key_len:
1.3.1. Generate a random number user_1_basis between 0 and 1 and append it to user_1_bases.
1.3.2. Generate a random number user_2_basis between 0 and 1 and append it to user_2_bases.
1.3.3. Create a new quantum circuit qubit with 1 qubit and 1 classical bit.
1.3.4. If user_1_basis is 0, apply the Hadamard gate to qubit.
1.3.5. Else, apply the X gate and then the Hadamard gate to qubit.
1.3.6. If user_2_basis is 0, apply a barrier to qubit.
1.3.7. Else, apply a barrier, then the Z gate to qubit.
1.3.8. Measure the qubit and store the result in measurement variable.
1.3.9. Append the first bit of the measurement variable to user_1_bits and user_2_bits.
1.4. Create an empty list key.
1.5. For i = 1 to key_len:
1.5.1. If user_1_bases[i] is equal to user_2_bases[i], append user_1_bits[i] to key.
1.6. Return key.
#algorithm for Encrypting and decrypting
2. Function: encrypt_file(key, file_path)
2.1. Open the file located at file_path in read binary mode and read its contents into data variable.
2.2. Create an empty list encrypted_data.
2.3. For i = 1 to length of data:
2.3.1. Append the result of the XOR operation between data[i] and key[i modulo length of key] to encrypted_data.
2.4. Open a new file with file_path + ".encrypted" in write binary mode.
2.5. Write bytes(encrypted_data) to the file.
2.6. Close the file.
3. Function: decrypt_file(key, file_path)
the file.
3.1. Open the encrypted file located at file_path in read binary mode and read its contents into data variable.
3.4. Open a new file with file_path minus the ".encrypted" extension in write binary mode.
                                3.5. Write bytes(decrypted_data) to the file.
                                           3.6. Close the file.
3.2. Create an empty list decrypted_data.
3.3. For i = 1 to length of data:
3.3.1. Append the result of the XOR operation between data[i] and key[i modulo length of key] to decrypted_data
4. Call generate_key() to generate a new key.
5. Call encrypt_file(key, "my_file.txt") to encrypt the "my_file.txt" file.
6. Call decrypt_file(key, "my_file.txt.encrypted") to decrypt the encrypted file.
```

5. Comparisons and Results

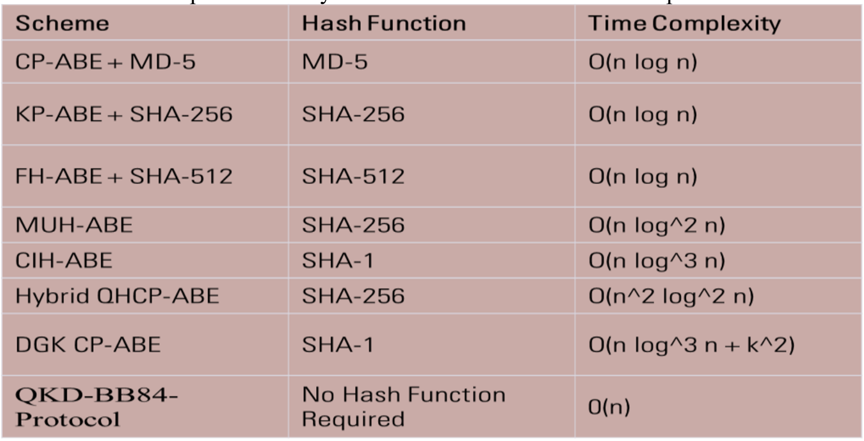
After a comparative analysis of classical and quantum computers, the following conclusions can be drawn:

- Classical computers are based on binary bits, while quantum computers use A qubit that can exist in more than one state at the same time.

- Quantum computers exhibit the capability to outpace conventional counterparts in solving specific problems, particularly within cryptography and optimization domains. Nonetheless, the progression of quantum computing remains at an early developmental phase, and commercial availability of such computing power has not yet been realized. Classical computers were efficient and widely used, performing many tasks efficiently and reliably.

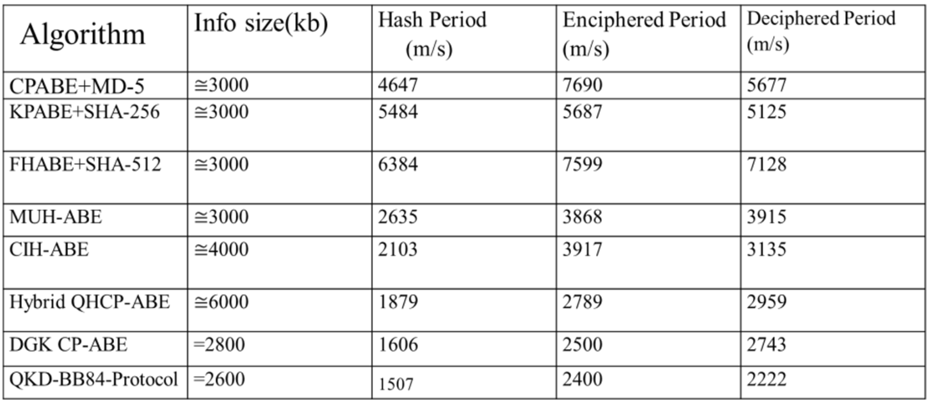
The programming languages used for classical and quantum computers are different, and programming a quantum computer requires specialized knowledge and expertise. Quantum computers are very sensitive to external factors such as noise and interference which can affect their performance

Table 2: Comparative Analysis of Various Schems w.r. to Computational time



Scheme	Hash Function	Time Complexity
CP-ABE + MD-5	MD-5	O(n log n)
KP-ABE + SHA-256	SHA-256	O(n log n)
FH-ABE + SHA-512	SHA-512	O(n log n)
MUH-ABE	SHA-256	O(n log^2 n)
CIH-ABE	SHA-1	O(n log^3 n)
Hybrid QHCP-ABE	SHA-256	O(n^2 log^2 n)
DGK CP-ABE	SHA-1	O(n log^3 n + k^2)
QKD-BB84-Protocol	No Hash Function Required	O(n)

Table 3: Comparative Analysis of Various Schems w.r. to Hash period, Encryptin and Decrypiton perions.



Algorithm	Info size(kb)	Hash Period (m/s)	Enciphered Period (m/s)	Deciphered Period (m/s)
CPABE+MD-5	≅3000	4647	7690	5677
KPABE+SHA-256	≅3000	5484	5687	5125
FHABE+SHA-512	≅3000	6384	7599	7128
MUH-ABE	≅3000	2635	3868	3915
CIH-ABE	≅4000	2103	3917	3135
Hybrid QHCP-ABE	≅6000	1879	2789	2959
DGK CP-ABE	=2800	1606	2500	2743
QKD-BB84-Protocol	=2600	1507	2400	2222

6. Conclusion

In conclusion, although quantum computers have the potential to revolutionize computing, it's crucial to acknowledge that these machines are currently in their early phases of development and have limitations that need to be addressed. Classical computers, on the other hand, were built and widely used to perform various tasks efficiently and reliably. Ultimately, the choice between using a classical computer or a quantum computer will depend on the specific requirements of the task at hand and the state of the art in the field.

References

1. Biamonte, Jacob, et al. Nature, **549**(7671), 195-202 ,(2017).
2. Ciliberto, Carlo, et al. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **474**(2209), 20170551 (2018):.
3. Mezquita, Yeray, et al. "*A review of k-nn algorithm based on classical and quantum machine learning*." Distributed Computing and Artificial Intelligence, Special Sessions, 17th International Conference. Springer International Publishing,(2021).
4. Singamaneni, Kranthi Kumar, Pasala Sanyasi Naidu, and Pasupuleti Venkata Siva Kumar. J. Eur. Systèmes Autom **51,** 283, (2018).
5. Huang, H. Y., et al. arXiv preprint arXiv:2011.01938 **12**,2631, (2021).
6. Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. Contemporary Physics **56**(2), 172-185 ,(2015).
7. Singamaneni, Kranthi Kumar, and Pasala Naidu. Ingénierie des Systèmes d'Information **23**(5) (2018).
8. Steane, Andrew., Reports on Progress in Physics **61**(2),117, (1998).
9. Kamata, Syo, et al. Physical Review D **107**(4), 045019 ,(2023):.
10. Singamaneni, Kranthi Kumar, and Pasala Sanyasi Naidu. Rev. d'Intelligence Artif. **33**(1) , 33-37 ,(2019).
11. Jammer, Max. "Philosophy of Quantum Mechanics. the interpretations of quantum mechanics in historical perspective." (1974).
12. E. Poornima, Srinivasulu Sirisala, P. Dileep Kumar Reddy, & G. Ramesh. International Journal of Intelligent Systems and Applications in Engineering, 10(4), 634–640, (2022).
13. Reddy, N.M., Ramesh, G., Kasturi, S.B. et al. Appl Nanosci **13**, 2449–2461 (2023). https://doi.org/10.1007/s13204-021-02174-y.
14. Thirupathi Nallella, Madhavi K, Ramesh G, Priya K, Data Storage in Cloud Using Key-Policy Attribute-Based Temporary Keyword Search Scheme (KP-ABTKS). 10.1007/978-3-030-33846-6_67, (2020).
15. Singamaneni, Kranthi Kumar, et al. Sensors **22**(18), 6741, (2022).
16. Dhanke Jyoti Atul, R. Kamalraj, G. Ramesh, K. Sakthidasan Sankaran, Sudhir Sharma, Syed Khasim,Microprocessors and Microsystems, **82**, 2021, 103741, (2021)
17. Cuffaro, Michael E. "Grete Hermann, quantum mechanics, and the evolution of Kantian philosophy." Women in the History of Analytic Philosophy: Selected Papers of the Tilburg–Groningen Conference, 2019. Cham: Springer International Publishing, 2023.
18. Kuipers, Folkert. arXiv preprint arXiv:**2301**(05467) (2023).
19. Singamaneni, Kranthi Kumar, et al. Electronics **11**(21), 3510, (2022).
20. Jaeger, Gregg. Quantum Information: An Overview (2007): 203-217.
21. Poonia, Ramesh C., and Manish Kalra, Journal of Information and Optimization Sciences **37**(2), 279-283, (2016).
22. Singamaneni, Kranthi Kumar, and Sanyasi Naidu Pasala. International Journal of Knowledge-Based and Intelligent Engineering Systems **24**(2), 145-156, (2020).
23. Hardy, Yorick, and Willi H. Steeb. Classical and quantum computing: with C++ and Java simulations. Birkhäuser, (2012).
24. Tang, Wei, et al. , Proceedings of the 26th ACM International conference on *architectural support for programming languages and operating systems*, (2021).
25. Manin, Yuri I. , Asterisque-Societe Mathematique De France **266,** 375-404, (2000).
26. Singamaneni, Kranthi Kumar, et al, Sensors **21**(21), 7300, (2021).

27. Kitaev, Alexei Yu, Alexander Shen, and Mikhail N. Vyalyi. Classical and quantum computation. American Mathematical Soc., 47, (2002).
28. Galindo, Alberto, and Miguel Angelo Martin-Delgado, Reviews of Modern Physics **74**(2), 347, (2002).
29. Gyongyosi, Laszlo, and Sandor Imre., Computer Science Review **31**, 51-71 ,(2019).
30. Singamaneni, Kranthi Kumar, and P. Sanyasi Naidu, International Journal of Advanced Intelligence Paradigms, **22**(3-4), 336-347, (2022).
31. Dragoman, Daniela, and Mircea Dragoman. Quantum-classical analogies. Vol. 92. Berlin: Springer, (2004).
32. Khan, Tariq M., and Antonio Robles-Kelly. "Machine learning: Quantum vs classical." IEEE Access 8 (2020): 219275-219294.
33. Rieffel, Eleanor G., and Wolfgang H. Polak. Quantum computing: A gentle introduction. MIT Press, (2011).
34. Gruska, Jozef. Quantum computing. Vol. 2005. London: McGraw-Hill, (1999).
35. Singamaneni, Kranthi Kumar, et al., Security and Communication Networks (2022).
36. Klco, Natalie, et al., Physical Review A **98**(3), 032331,(2018).
37. Chuang, Isaac L., and Yoshihisa Yamamoto., Physical Review A **52**(5), 3489, (1995).
38. Bandyopadhyay, S. , Superlattices and Microstructures **37**(2), 77-86 ,(2005).
39. Bernhardt, Chris. Quantum computing for everyone. Mit Press, 2019.
40. Cacciapuoti, Angela Sara, et al., IEEE Network **34**(1) ,137-143 ,(2019).