1

Introduction to Quantum Computing

V. Padmavathi[1], C. N. Sujatha[2], V. Sitharamulu[3], K. Sudheer Reddy[4]* and A. Mallikarjuna Reddy[5]

[1]Dept. of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, India
[2]Dept. of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, India
[3]Dept. of Computer Science and Engineering, GITAM (Deemed to be University), Hyderabad, India
[4]Dept. of Information Technology, Anurag University, Hyderabad, India
[5]Dept. of Artificial Intelligence, Anurag University, Hyderabad, India

Abstract

Over the past few decades, tremendous growth has been witnessed in cryptography in which different security techniques and concerns were projected and put into practice. The classical methods of cryptography are depended on binary bits, which are susceptible to predicting the key during transit. Hence, moving the classical cryptographic scheme to a new fast, and non-vulnerable scheme is time. The principles of quantum mechanics are applied in quantum computing to enhance security which uses qubits for communication. The advantage of using qubits is that it is impossible to make copies of qubits due to the no-cloning theorem. The computations are performed through photons or qubits produced using the photon's polarization. The qubits are disturbed when measured at an incorrect polarization angle due to the principle of uncertainty. The photons are quantized features used to encode the information. They can be applied in Quantum Key Distribution (QKD), in which distantly apart communicators share a standard secret key.

***Keywords*:** Quantum computing, quantum mechanics, qubits, photon polarization, quantum gates, quantum cryptography, quantum key, Fredkin gate

**Corresponding author*: sudheercse@gmail.com

Sachi Nandan Mohanty, Rajanikanth Aluvalu and Sarita Mohanty (eds.) Evolution and Applications of Quantum Computing, (1–14) © 2023 Scrivener Publishing LLC

1.1 Quantum Computation

The study of information processing based on quantum mechanics is known as quantum computing and quantum information. Quantum mechanics is a set of mathematical rules used to build physical hypotheses. Building tools to refine the notion of quantum mechanics is one of the objectives of quantum computation [7–11]. There was a debate on whether it was possible to make a duplicate of an unknown quantum state. Quantum mechanics might be used when replication is conceivable to send signals faster than light, which is highly impractical. Wooters and Zurek [3] proved that the theorem of no cloning, was the first result of quantum computation and information. Since then, there have been several improvements.

1.2 Importance of Quantum Mechanics

Quantum mechanics-based communications are safe since they stand on inalienable quantum mechanics concepts. The principles of Heisenberg Uncertainty and Photon Polarization are essential concepts.

The Heisenberg principle of Uncertainty refers to an entity's inability to discern two connected physical attributes [4]. In light of this assertion, two examples are worth considering. The first is the example generally stated: For every P, the momentum and the location cannot be calculated alongside. Second, the photon cannot be measured concurrently on either of it [1, 2, 18], then properties are impacted. According to the theorem of no-cloning [1, 3, 18], replicas of qubits are not feasible.

1.3 Security Options in Quantum Mechanics

Figure 1.1 demonstrates that a bit corresponds to a qubit by polarizing photons and with the help of a rectilinear and diagonal basis. In a rectilinear base, the binary 0 is represented by 0° photon polarization and 45° on a diagonal basis. In Figure 1.2 [4], binary one is represented by 90° rectilinear photon polarization and 135° diagonal photon polarization.

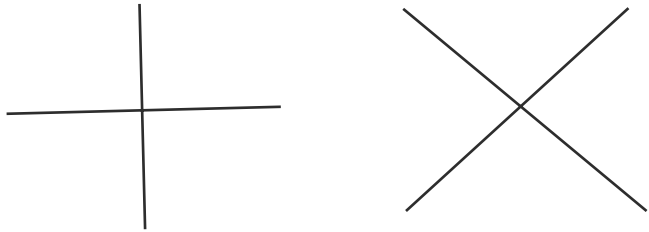

Figure 1.1 Rectilinear, diagonal basis.

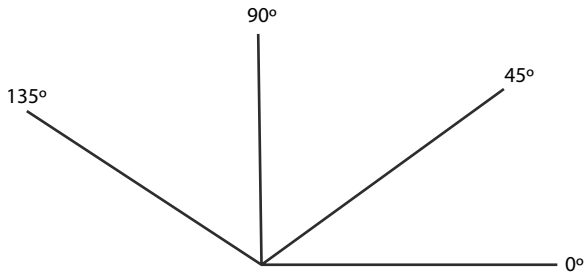

Figure 1.2 Photon polarizations.

1.4 Quantum States and Qubits

Qubit exists in two states, symbolized as $|0\rangle$ and $|1\rangle$ in quantum mechanics. It is stated as a state, a ket, which Paul Dirac created [1, 6]. A bit can be 0 or 1, whereas a qubit can be $|0\rangle$ or $|1\rangle$ state. It also happens in the superposition state that is nothing more than a linear arrangement of the quantum states $|0\rangle$ and $|1\rangle$. The symbol $|\phi\rangle$ indicates a form, and a superposition state is denoted by the symbol $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers [6].

A qubit exists in superposition state $|0\rangle$ and $|1\rangle$ in most cases, but the state is not calculated. When it is calculated, though, it is either in $|0\rangle$ or $|1\rangle$. The chance of realizing a qubit is either $|0\rangle$ or $|1\rangle$ equals the square of the modulus of α, β. It is stated that in state $|0\rangle$, the likelihood of obtaining $|\phi\rangle$ is $|\alpha|^2$, and in state $|1\rangle$, the likelihood of obtaining $|\phi\rangle$ is $|\beta|^2$. Squaring coefficients yield likelihood of attaining a measurement's result. Thus, $|\alpha|^2 + |\beta|^2 = 1$ [6, 18] is the state.

1.5 Quantum Mechanics Interpretation

The state is shown by the expression $\alpha|0\rangle + \beta|1\rangle$. It can alternatively be represented as a vector or a column. It is represented as a two-dimensional complex unit vector by stacking two complex integers $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ [1, 12].

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ where $\alpha = 1$ and $\beta = 0$

And

$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ where $\alpha = 0$ and $\beta = 1$

$|\phi\rangle = \cos\theta\,|0\rangle = \sin\theta\,|1\rangle = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$.

1.6 Quantum Mechanics Implementation

The following notations are used to implement quantum mechanics:

1) $|0\rangle = |\,—\rangle$
2) $|1\rangle = |\,|\,\rangle$
3) $\frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) = |/\rangle$
4) $\frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle) = |\backslash\rangle$

In rectilinear basis, 1 and 2 indicates 0° and 90°, respectively. In diagonal basis, the 3 and 4 indicates 45° and 135°, respectively.

1.6.1 Photon Polarization Representation

i) A binary 0 is represented in rectilinear basis as a 0° state using polarization, as demonstrated below using a linear layout with x and y axes both set to 1. Figure 1.3 depicts the situation.

$$|0\rangle = |\,—\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1\,|\,x\,\rangle + 0\,|\,y\,\rangle$$

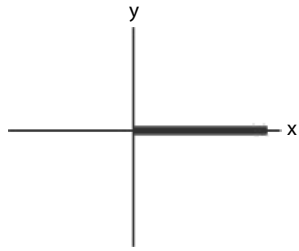

Figure 1.3 Representation of photon polarization.

ii) Using the linear configurations of 0 on the x axis and 1 on the y axis, respectively. Polari-zation isused to represent the binary 1 in rectilinear basis as a 90° state. The illustration is shown in Figure 1.4.

$$|\,|\,\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0\,|\,x\,\rangle + 1\,|\,y\,\rangle$$

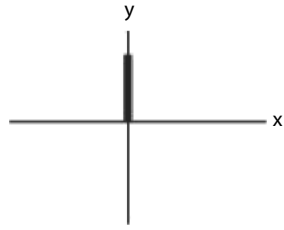

Figure 1.4 Representation of photon polarization.

iii) Using polarization and the linear combinations listed below, a 0 in binary is shown as 45° state on a diagonal basis. Figure 1.5 depicts the situation.

$$|/\,\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \frac{1}{\sqrt{2}}\,|\,x\rangle + \frac{1}{\sqrt{2}}\,|\,y\rangle$$

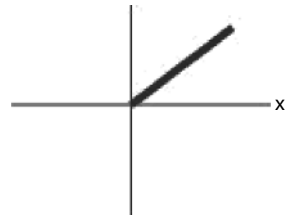

Figure 1.5 Photon polarization in diagonal basis (of binary 0).

iv) Using polarization and the linear combinations listed below, 1 in binary corresponds to 135° in diagonal basis. The representation is shown in Figure 1.6.

$$|\backslash\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \frac{1}{\sqrt{2}}|x\rangle - \frac{1}{\sqrt{2}}|y\rangle$$

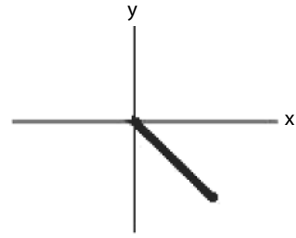

Figure 1.6 Representation of photon polarization.

1.7 Quantum Computation

Quantum computation has led to a new way of thinking about computation. The notion of quantum computation explains changes in state stirring. A classical computer, like a method, is built with the help of an electrical circuit with logic wires and gates, whereas a quantum computer is built with the help of a quantum circuit with quantum wires and gates.

The quantum gates are employed to control or manipulate and act on the quantum bit [5].

The matrix representation is the best way to understand linear combinations. Unitary matrix U is the proper state on the matrix to represent the gate. Specifically, U†U = I, in which U† is the adjoint of U, that is the complex conjugate of the transpose of matrix U, and I is a two-by-two identity matrix. It is simple to validate X†X = I for a gate, for example. Surprisingly, quantum gates are only limited by the unitary check. It denotes the presence of a logical quantum gate [5].

1.7.1 Quantum Gates

Gates are used to carry out computations in quantum computers. Quantum gates are unitary operators with n inputs and outputs that may be expressed using matrices. As a result, they have a 2^n degree. A two-degree matrix is used to represent one qubit. As a result, a two-by-two matrix is required for a quantum gate acting on a qubit. A matrix of 2^2 degrees is used to represent a two-qubit gate. As a result, a four-by-four unitary matrix [5, 6] is used to represent it. As a result, the quantum gates have a temporal complexity of 2^n. It has been proved that exponential complexities are secure. The tensor product is used to obtain the matrix depiction of quantum gates. Tensor product is represented as ⊗.

It creates a single vector space out of two. XY is a space with mxn dimension if X and Y are vector spaces with mxn n dimensions. The components of |x| of X and |y| of Y are the elements of XY, which are linear combinations of these tensor products. The matrix is represented as given if A is an m x n matrix and B is a p x q matrix.

$$A \otimes B = \overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}}^{nq} \Bigg\} mp$$

A. One-Qubit Gate

A quantum gate that operates on a single qubit requires a single qubit as input and output. The computation requires a two-by-two unitary matrix. The several forms of one-qubit gates are explained in the following sections [17, 18].

i) H-Gate

The Hadamard gate is represented by H and depicted:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

ii) Quantum NOT Gate or Pauli X-Gate

The quantum not gate is shown in matrix form as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

iii) Pauli Y-Gate

The gate is depicted as below

$$\mathrm{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

iv) Pauli Z-Gate

It is portrayed as

$$\mathrm{Y} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

v) Pauli S-Gate

Pauli S-gate is described:

$$\mathrm{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

A $|0\rangle$ when operated atop on it returns $|0\rangle$, but when $|1\rangle$ is acted upon, Pauli S-gate returns $i|1\rangle$

B. Two-Qubit Gate

A two-qubit quantum gate accepts two qubits as an input and two qubits as an output. The computation requires a four-by-four matrix. The many forms of two-qubit gates are detailed in the following sections.

i) Controlled NOT

It is well-known as the CNOT gate. The CNOT gate's initial input serves as a control qubit. The target qubit is unaffected if the control qubit is $|0\rangle$. If it is $|1\rangle$, CNOT operates on the qubit by flipping it. $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are the states. On two qubits a, b, the function of the CNOT gate is $|a, b\rangle \rightarrow |a, b \oplus a\rangle$.

The CNOT matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

ii) Swap Gate Swaps Two Qubits

The Swap matrix is shown as:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

iii) Controlled-Z Gate

cZ is another representation for it. The gate's qubits behave in a predictable manner.

The cZ matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

iv) Controlled Phase Gate

It is commonly represented as cS gate. The process is identical to that of a Phase gate.

The cS matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

C. Three-Qubit Gate

Three qubits are the input and three qubits are the output of a three-qubit quantum gate. The computation requires an eight-by-eight matrix. The many forms of three-qubit gates are detailed in the following sections.

i) Toffoli Gate

It is a three-qubit quantum gate, as it receives three inputs, produces three outputs a, b, and c out of a total of 2^3 [5]. Figure 1.7 depicts the situation. T gate is the short name for it. The gate operation has no effect on the inputs a, b, the two control qubits. The target is flipped when control qubits is set as 1 or not when the input c is set to 0. T gates have the property of being reversible when applied twice on qubits $|a, b, c\rangle \rightarrow |a, b, c \oplus ab\rangle \rightarrow |a, b, c\rangle$

An eight-by-eight matrix is used to represent it

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

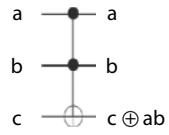

Figure 1.7 Toffoli gate.

ii) Fredkin (controlled swap) gate
The controlled swap gate is a three-qubit gate. 'a' is the control qubit, and 'b' and 'c' are the target qubits. If control qubit 'a' is set to 1, it swaps target qubits 'b' and 'c,' otherwise they pass through untouched [26, 27].

An eight-by-eight matrix is used to represent it

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

1.8 Comparison of Quantum and Classical Computation

The operations in the classical computation are based on probability and employ stochastic matrices. In classical computation, the chance of obtaining state i is Pi, where Pi is an actual number. $0 \leq Pi \leq 1$ and $\sum Pi = 1$. The probability of getting state Y in quantum computation is $|aY|2$, where a is the amplitude and ai as a complex number,

$$0 = |ai|2 = 1, ? \text{ i } |ai|2 = 1.$$

The transition is based on amplitudes in this case. Unitary matrices [5] are used in quantum computation [22–25].

1.9 Quantum Cryptography

The researcher [1], discovered the notion of uncertainty. As a result, the phenomena evolved into Quantum Cryptography, a particularly promising topic for cryptographers. Later, Wiedemann built on this idea by proposing a quantum key distribution mechanism known as QKD [2, 16–21], which follows the laws of quantum physics. Later, the BB84 protocol [4, 22–25] employed for verifiably secure quantum physics concepts.

1.10 QKD

QKD begins by transmitting photons that are generated at random in four quantum states, employing rectilinear and diagonal basis. A rectilinear basis has two states: a 0 in binary is polarized horizontally to 0° and 1 in binary 1 is polarized vertically to 90°. Likewise, the two states of diagonal basis, binary 0 and 1, are polarized at 45° and 135°, respectively [13–15]. QKD starts by sending out a message. For communication, it requires a classical and a quantum channel. Classical messages are sent over a traditional channel, while qubits or polarized photons are sent through a quantum channel.

1.11 Conclusion

The fact that quantum computing techniques are used in cryptography is a good sign in the new research. The objective of quantum computing is made evidently for safe and secure transmission by using quantum mechanics. The qubit is prepared by polarizing photon basis. The computing of classical and quantum computers is investigated. Also mentioned are the limitations of traditional computers. The quantum computer's computations utilize various quantum gates, as indicated. The building blocks are the quantum gates that act on qubits. The introduction to QKD, which follows quantum mechanics laws to provide secure key transfer, is mentioned.

References

1. Wiesner, S., Conjugate coding. *ACM Sigact News*, 15, 1, 78–88, original manuscript written circa 1969, 1983.
2. Wiedemann, D., Quantum cryptography. *ACM Sigact News*, 18, 2, 48–51, Sept. 1986-March 1987.
3. Wootters, W.K. and Zurek, W.H., A single quantum cannot be cloned. *Nature*, 299, 802–803, 1982.
4. Bennett, C.H. and Brassard, G., Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, December 1984.
5. Nielsen, M.A. and Chuang, I.L., *Quantum Computation and Quantum Information*, Cambridge University Press, University of Cambridge, Cambridge, 2000.
6. McMahon, D., *Quantum Computing Explained*, IEEE Computer Society, Wiley-Inderscience, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2008.
7. NSA seeks to build quantum computer that could crack most types of encryption. *Washington Post*, January 2, 2014. https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.
8. https://en.wikipedia.org/wiki/Quantum_computing.
9. World's first silicon quantum logic gate brings quantum computing one step closer. http://gizmodo.com/worlds-first-silicon-quantum-logic-gate-brings-quantum-1734653115.
10. Corcoles, A.D., Magesan, E., Srinivasan, S.J., Cross, A.W., Steffen, M., Gambetta, J.M., Chow, J.M., Demonstration of a quantum error detection code using a square lattice of four superconducting qubits. Nature Publishing Group. *Phys. Rev. Lett.*, 6, 1–10, 2015.
11. Gaudin, S., Researchers use silicon to push quantum computing toward reality, 2014. http://www.computerworld.com/article/2837813/researchers-use-silicon-to-push-quantum-computing-toward-reality.html.
12. Vazirani, U.V., *Quantum Mechanics and Quantum Computation*, University of California, Berkley, 2006, https://www.youtube.com/watch?v=Gfpzke48K9E&list=PL3XnKI-cY52yHBKN3z1n_-hrvjEcmaLW&index=3.
13. Bennett, C.H., Brassard, G., Robert, J.M., Privacy amplification by public discussion. *SIAM J. Comput.*, 17, 210–229, April 1988.
14. Brassard, G. and Salvail, L., Secret-key reconciliation by public discussion in advances, in: *Cryptography—EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, T. Helleseth (Ed.), pp. 410–423, Springer-Verlag, Berlin, Germany, 1994.
15. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M., Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41, 6(part 2), 1915–1923, Nov. 1995.

16. Brassard, G. and Crepeau, C., 25 years of quantum cryptography. *ACM Sigact News*, 27, 3, 13–24, 1996.
17. Bennett, C., Bessette, F., Brassard, G., Salvail, L., Smolin, J., Experimental quantum cryptography. *J. Cryptology*, 5, 3–28, 1992.
18. Padmavathi, V., Vardhan, B.V., Krishna, A.V.N., Quantum cryptography and quantum key distribution protocols: A survey. *2016 IEEE 6th International Conference on Advanced Computing*.
19. Padmavathi, V., Vardhan, B.V., Krishna, A.V.N., Provably secure quantum key distribution by applying quantum gate. *Int. J. Netw. Secur.*, 20, 1, 88–94, Jan. 2018.
20. Aluvalu, R., Kamliya, V., Muddana, L., Hasbe access control model with secure key distribution and efficient domain hierarchy for cloud computing. *Int. J. Electr. Comput. Eng.*, 6, 2, 770, 2016.
21. Langaliya, C. and Aluvalu, R., Enhancing cloud security through access control models: A survey. *Int. J. Comput. Appl.*, 112, 7, 8–12, 2015.
22. Chennam, K.K., Muddana, L., Aluvalu, R.K., Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud, in: *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, IEEE, pp. 2030–2033, 2017.
23. Reddy, K.S., Varma, G.P.S., Reddy, S.S.S., Understanding the scope of web usage mining & applications of web data usage patterns. *2012 International Conference on Computing, Communication and Applications*, pp. 1–5, 2012.
24. Ayaluri, M.R., Reddy, K.S., Konda, S.R., Chidirala, S.R., Efficient steganalysis using convolutional auto encoder network to ensure original image quality. *Peer J. Comput. Sci.*, 7, e356, 2021. https://doi.org/10.7717/peerj-cs.356.
25. Kavati, I., Reddy, A.M., Babu, E.S., Reddy, K.S., Cheruku, R.S., Design of a fingerprint template protection scheme using elliptical structures. *ICT Express*, 7, 4, 497–500, 2021. https://doi.org/10.1016/j.icte.2021.04.001.
26. Santhosh Kumar, C.N., Pavan Kumar, V., Reddy, K.S., Similarity matching of pairs of text using CACT algorithm. *Int. J. Eng. Adv. Technol.*, 8, 6, 2296–2298, 2019.
27. Reddy, K.S. and Santhosh Kumar, C.H.N., Effective data analytics on opinion mining. *IJITEE*, 8, 10, 2073–2078, 2019.