ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse97932020.pdf
https://doi.org/10.30534/ijatcse/2020/97932020

Simulation of Resources for Quantum Algorithms and Quantum Communication Protocols based on a Novel Framework

Giao N. Pham[1], Binh A. Nguyen[2], Viet Q. Tran[2], Khoa D. Ta[2],Phong H. Nguyen[3], and Duc M. Nguyen[4]

[1]Dept. of Computing Fundamentals, FPT University, Hanoi, Vietnam; giaopn@fe.edu.vn
[2]ICT Department, FPT University, Hanoi, Vietnam;binhnase04865@fpt.edu.vn, viettqse06178@fpt.edu.vn, khoatdhe130813@fpt.edu.vn
[3]Center of Machine Vision & Signal Analysis, University of Oulu, Finland; phong.nguyen@oulu.fi
[4]Dept. of Electrical engineering, University of Ulsan, Ulsan, South Korea, nguyenmanhduc18@gmail.com

ABSTRACT
Recently, Samsung Electronic just released a new type of mobile phone model named Galaxy A71 where the quantum RNG chip is boasted inside for advanced security by capable of generating truly random and unpredictable numbers. It is no doubt that the quantum mechanism-based communication protocols or quantum information technologies are gradually changing the world with its advantages. It promises the new information generation where quantum-based computer can be seen in many living fields. Since the quantum algorithms and quantum communication protocols need to be verified before applying on chip set system, or hardware systems, the verification frameworks need to be done. In this discussion, we first propose a novel framework by MATLAB emulators. Then, we analysis the quantum resources or quantum basic elements such as quantum entanglements, quantum super positions state, quantum Fourier transformation, and quantum Arithmetic in proposed novel framework. The open problems to consider quantum algorithms based on proposed framework is discussed.

Key words: Quantum communication protocols, Quantum algorithms, Quantum circuit model, MATLAB.

1. INTRODUCTION

We are experiencing the benefits of information technology every day [1]. However, there are challenges that today's information systems are not be able to solve, to be security the certain huge and complexity of data [2]. Therefore, quantum information system, which is a generalization of classical information system, is a promised candidate to be a next generation information system [3]. Quantum information system is quantum mechanism-based computation where we use the properties of particle and wave to perform computation and transformation of the state of information system such as superposition [4] and entanglement [5].

The quantum information systems have the advantages of security, for example Shor factoring algorithm [6] and efficient on computation [7], for example Grover search algorithm. Consequently, there are many researches involved on quantum communication protocols [8] and quantum algorithms [9]. However, quantum information systems have faced many imperfectly noise, decoherence, and unwanted transformation which affect the practical design, efficient of quantum algorithms and quantum communication protocols. Quantum error control codes (QECC) are a suitable solution since they bring the advantages from classical error control codes [10-15]. Since the first QECC was proposed by Shor [16] for 9-qubits, there are many proposed methods for construction of QECC with various purposes such as adaptive code length [17-20], minimum distance [21-24] etc.

Quantum algorithms and quantum communication protocols are the main application of quantum information system. Till now, there are many quantum-based products have been discussed such as chipset QRNG in Galaxy-A71, quantum teleportation [25]. There are many theoretical applications are discussed with various fields [26] which will be reality soon and promise to be a next generation information system. Before implementation of quantum-based algorithms or quantum communication protocols, we need to verify it in classical computers, or we need to make the hybrid quantum-classical communication system. Therefore, a novel framework is needed to design to handle the simulation of quantum information system. However, they are mostly focused on the programming language and not flexible pre-design of resources. In this discussion, a MATLAB based framework is discussed and the quantum resources, which are popularly used in quantum algorithms and quantum communication protocols, are explained therein.

We organize the paper as follows. In Section 2, the basic about quantum information of quantum states, Hilbert transformation of quantum computation is discussed. In Section 3, we first propose a novel framework based on MATLAB for verification quantum algorithms on classical computers. Then, the quantum resources are implemented in proposed framework. Finally, Section 4 is to discuss open problems on simulation quantum algorithms on our proposed framework.

2. HILBERT TRANSFORM OF QUANTUM COMPUTATION

2.1. Basics of Quantum Information System

Quantum information is to use the quantum mechanism to explain of information. Hence, we are going to associate the information to the particle and waves. In classical computation system, bits with two elements '0' and '1' are the basic elements to build up all data. In quantum information, we have the basic element named 'qubit'. The most basic quantum information system is quantum information system with one qubit which has two basic elements denoted as Dirac ket notation ($|0\rangle$ and $|1\rangle$). Since the particle is always moving, we not only have two basic state, we have something called superposition state. Therefore, the two basic state must satisfy the orthogonal condition and we have the Hilbert space to explain the quantum information system. Hilbert space gives us the mathematical model of quantum information system as following,

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{and} |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}. \quad (1)$$

And a superposition can be expressed as:

$$|\alpha\rangle = \begin{bmatrix}x\\y\end{bmatrix} = x\begin{bmatrix}1\\0\end{bmatrix} + y\begin{bmatrix}0\\1\end{bmatrix}, \quad (2)$$

where x and y are complex numbers and $|x|^2 + |y|^2 = 1$ as norm condition. Consequently, there are infinite state in just 1-qubits system.

A multi qubits system of *n*-qubits is also defined from *n* basis elements:

$$\begin{cases} |a_1\rangle = [1\,0\,0\,\dots\,0]^T \\ |a_2\rangle = [0\,1\,0\,\dots\,0]^T \\ \vdots \\ |a_n\rangle = [0\,0\,0\,\dots\,1]^T \end{cases}. \quad (3)$$

And we can use the tensor product to explain from 1-qubit system.

$$|\rho\rangle = \sum_{i=0}^{2^n-1} \rho_i |i\rangle = \sum_{i_k=\{0,1\}} \rho_{i_1 i_2 \dots i_n} |i_1\rangle |i_2\rangle \dots |i_n\rangle. \quad (4)$$

where $i = \sum_{j=0}^{n-1} 2^j i_j$.

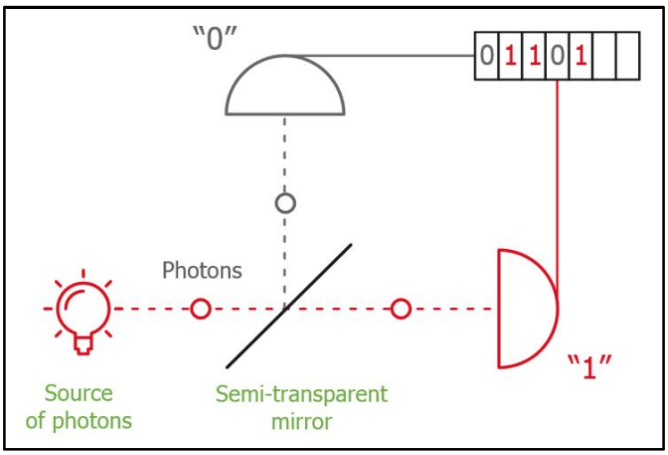

Figure1: Optic system to generate qubit.

Since in quantum mechanism the particle always moves around the axis, quantum information can see that movement as the change of a quantum state to another quantum state. As Hilbert space of qubits, we have the *Hilbert* transformation of quantum states. Modeling as mathematic space, the movement can be expressed as a multiplication of a matrix and we will consider the *Hilbert* transformation of matrices. Assume that we have a quantum state $|\psi\rangle$, it can be change to next state $\boldsymbol{U}|\psi\rangle$. As the energy reservation, and the revertible of transformation, the matrix **U** must satisfy $\boldsymbol{U}^{-1} = \boldsymbol{U}^{\dagger}$, the matrices which satisfy that pre-condition are called Unitary matrices. Unitary matrices can be expressed by four Pauli element matrices such as **I**, **X**, **Z**, and **Y**. And any Unitary matrices can be view as their combination.

2.2. Proposed a MATLAB based Framework for Simulation of Quantum Algorithm

Nowadays quantum information system, optics is the source to generate quantum bits since light consists of many elementary "particles" called photons and photons exhibit in certain situations a random number. The detail of an optics system is given as figure 1where light emitting diode LED is used to generate photons; the Semi-transparent mirror will decide the probability a photon is in each basis state. One such situation, LED is used as optical source for qubits on Samsung mobile phone Galaxy A71.

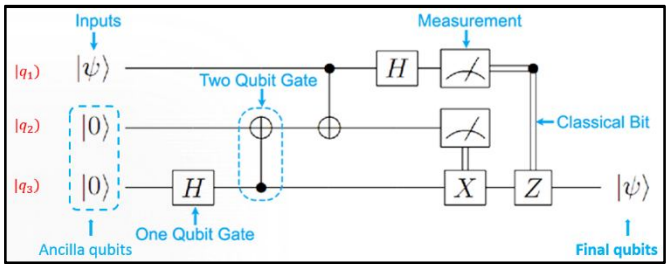

Figure 2: An example of a novel system model.

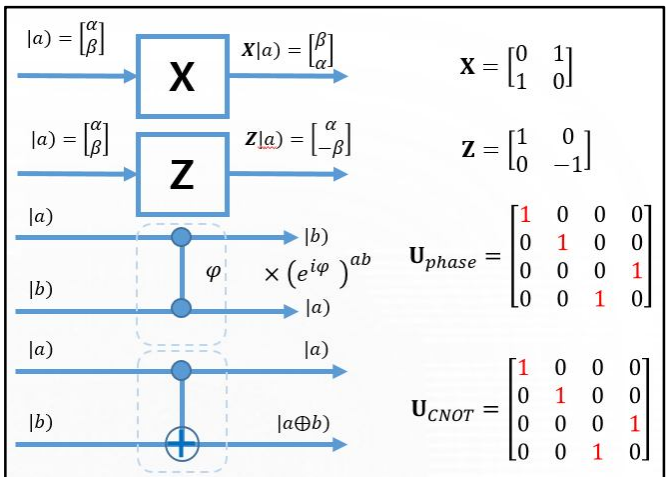

Figure 3: System model and MATLAB predefinition of some quantum basic resources.

Working with light or setup a system by LED will need to spend a lot of human resource and time. To fast verify and simulation of quantum algorithm or quantum communication protocol, a novel system model needs to be considered. And quantum circuit model is popular used to explain the quantum algorithms and quantum communication protocol. Figure 2 gives an example of a novel quantum information system with

three qubits. Three qubits include an information qubit ($|q_1\rangle$) and two ancilla zeros qubits ($|q_2\rangle = |0\rangle, |q_3\rangle = |0\rangle$). The full start qubits are combined of those three qubits by a tensor product, and it is denoted by: $|q_1q_2q_3\rangle = |q_1\rangle\otimes|q_2\rangle\otimes|q_3\rangle$. Transformation of initial qubits to next step are given by Unitary matrices. In system of figure 2, 1-qubit gate is Hadamard gate, 2-qubits gate is Controlled-NOT gate, **X** and **Z** are bit-flip gate and phase-flip gate.

MATLAB or matrix laboratory is a multi-paradigm numerical computing environment and proprietary language developed by MathworksInc. with a programming language that expresses matrix and array computation. Since the Hilbert space and Hilbert transformation be matrix expression and matrix multiplication, MATLAB is suitable environment for us to build a novel framework for simulation of quantum circuit model. The MATLAB pre-definition of those gates and qubits in quantum system in figure2 are given as figure 3.

3. SIMULATION OF QUANTUM ALGORITHMS OVER A PROPOSED FRAMEWORK

3.1. Simulation ofQuantum Superposition States

Hadamard matrix can be seen everywhere in quantum algorithms and quantum computation. It is from a fact that Hadamard matrix help to create a 50/50 superposition quantum state with 2-qubits system. In addition, general *Hadamard* matrix will create a balance superposition quantum state which is generating super positions of all basis states. Hence, *Hadamard* matrices are used as encoding part to generate superposition state and decoding part to rollback superposition state to initial state of a quantum information system. The matrix form and the *Hadamard* transformation in 1-qubit is given in figure 4.

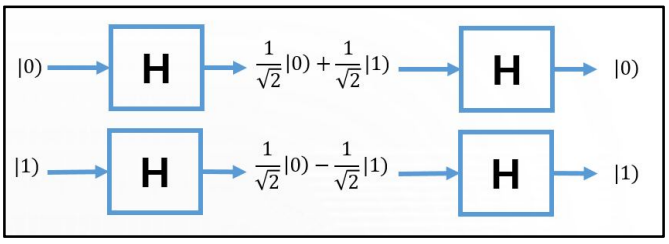

Figure 4:*Hadamard* matrix for 1-qubit system.

To make a superposition of *n*-qubits, we are going to use a general *Hadamard* matrix which is tensor product of *n Hadamard* matrices. And we can use the tensor product to explain from 1-qubit system. The general matrices of *Hadamard* is expressed as follows,

$$\mathbf{H}_2 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}(-1)^{0\wedge 0} & (-1)^{0\wedge 1}\\ (-1)^{1\wedge 0} & (-1)^{1\wedge 1}\end{bmatrix}. \quad (5)$$

$$\mathbf{H}_2^{\otimes n} = \mathbf{H}_2\otimes\mathbf{H}_2 \ldots \otimes\mathbf{H}_2. \quad (6)$$

As equation (5) and (6), we can obtain the formula for general Hadamard matrix as $\mathbf{H}_2^{\otimes n}[\mathbf{i},\mathbf{j}] = \frac{1}{\sqrt{2^n}}(-1)^{\langle \mathbf{i},\mathbf{j}\rangle}$, where **i**, **j** are the row and column numbers in binary. The main properties of *Hadamard* matrix is to generate the superposition state as follows,

$$\boldsymbol{H}_2^{\otimes n}|\mathbf{0}\rangle = \frac{1}{\sqrt{2^n}}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix} = \frac{1}{\sqrt{2^n}}\sum_{\boldsymbol{x}\in\{0,1\}^n}|\boldsymbol{x}\rangle, \quad (7)$$

$$\boldsymbol{H}_2^{\otimes n}|\mathbf{y}\rangle = \frac{1}{\sqrt{2^n}}\sum_{\boldsymbol{x}\in\{0,1\}^n}(-1)^{\langle \boldsymbol{x},\boldsymbol{y}\rangle}|\boldsymbol{x}\rangle. \quad (8)$$

The implementation of Hadamard matrix in *n*-qubits system are shown in **Figure** 5.

```
%Implementation of Hadamard gate based on proposed framework
function H = hadamard(n)
if n==1
    H=[1 1;1 -1]/sqrt(2);
else
    H=kron(hadamard(n-1),hadamard(1));
end
```

Figure 5:MATLAB-based implementation of general *Hadamard* matrix.

3.2. Simulation of Quantum Entanglement States

Entanglement is the most important role of quantum-based information system. Highly quantum entangled state such as *BELL*,*GHZ*, *W*-states are using a lot in many theoretical and reality application such as quantum teleportation system, quantum random number generators, quantum error correction codes, quantum super dense coding etc. In this part, they areanalysedby proposed framework.

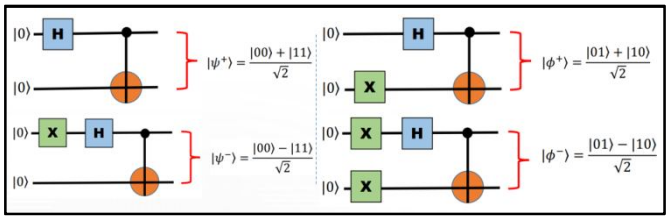

Figure 6:*BELL* state preparation by circuit model.

The MATLAB-based framework to prepare of *BELL* state is given in figure 6, 7.

```
%Implementation of BELL state based on proposed framework
function q=qubit0(n)
if n==1
    q=[1;0];
else
    q=kron(qubit0(n-1),qubit0(1));
end
%Setup qubit input:
q_one      = qubit0(1);
q_two      = qubit0(1);
firstState = kron(q_one,q_two);
Xgate      = [ 0 1; 1 0];
gate1      = kron(hadamard(1),eye(2));
gate2CN    = [ 1 0 0 0;
               0 1 0 0;
               0 0 0 1;
               0 0 1 0;];
finalState = gate2CN*gate1*firstState;
```

Figure 7: MATLAB-based implementation of *BELL*state.

3.3. Simulation of Quantum Fourier Transformation

Quantum Fourier transform (*QFT*) and its invert $QFT^{\dagger}$ are a variant of Discrete Fourier Transform (*DFT*) and *DFT* invert in quantum information system. The purpose of QFT are shown in figure 8 where we consider *QFT* in case of 1, 2, and 3-qubits.

In figure 9, the implementation based on quantum circuit model is considered. It is proven that *QFT* is more suitable for quantum computers since it requires n Hadamard gates and $\frac{n(n-1)}{2}$ phase shifts gates. Therefore, the complexity or the size of network is $\frac{n(n+1)}{2}$.

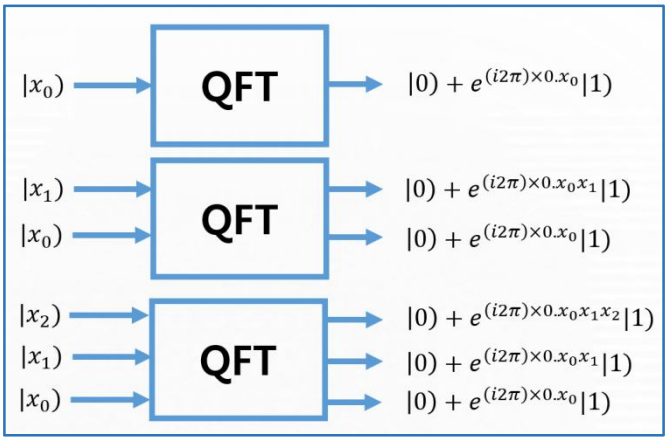

Figure 8: Purpose of *QFT*.

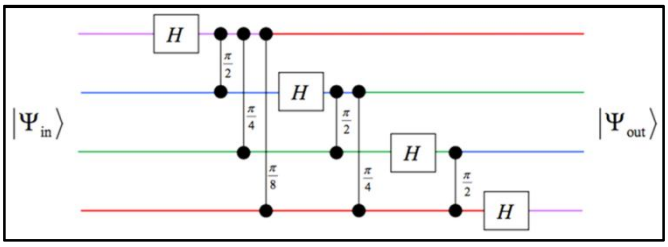

Figure 9: Implementation of *QFT*.

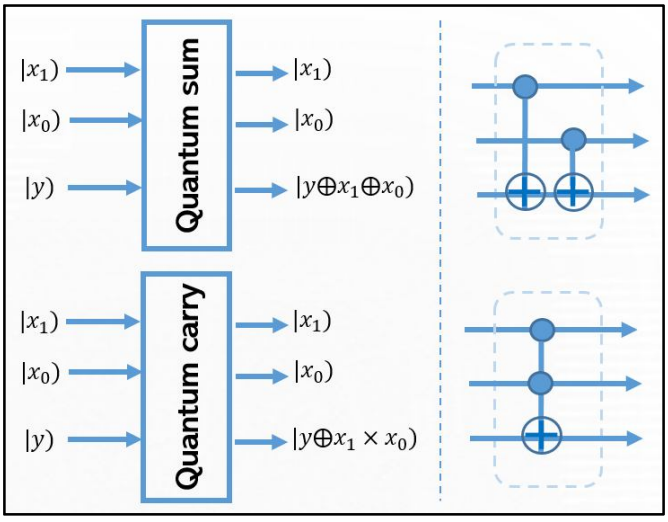

Figure10: Implementation of Quantum Arithmetic on quantum circuit model.

3.4. Quantum Arithmetic

Quantum equivalents of conventional arithmetic modulo 2 can be implanted from basic 2-qubits quantum gates. The equation and implementation of arithmetic is explained in figure 10. The MATLAB-based framework to prepare of quantum arithmetic states are given in figure 11.

```
%Implementation of Quantum Arithmetic state based on
proposed framework
gateCN = [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 0 0 1;
          0 0 0 0 0 0 1 0;
          0 0 0 0 0 1 0 0;
          0 0 0 0 1 0 0 0];
gateCT = [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 0 0 0 1;
          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 1 0 0 0 0];
```

Figure 11:MATLAB-based implementation of Quantum Arithmetic state.

4. CONCLUSION

The discussion has presented firstly a basic view and contents of quantum-based information system. The novel framework, which is based on MATLAB tool, has been presented. Many quantum resources such as quantum entanglements, quantum superposition states, quantum Fourier transformation, and quantum arithmetic are implemented by using proposed tool and which gives us an outstanding result.

The visible result proves that the proposed framework is novel for further uses of this framework for implementation and simulation of many quantum algorithms, quantum communication protocols, quantum teleportation, quantum key distribution protocols, quantum walks, quantum image system, etc. We are going to implement and investigatethem based on proposed framework.

ACKNOWLEDGEMENT

This work is supported by FPT University, Hanoi, Vietnam;University of Oulu, Oulu, Finland; and University of Ulsan, Ulsan, Republic of Korea (by the Research Program through the National Research Foundation of Korea NRF-2019R1A2C1005920).

Conflict of Interest

On behalf of all authors, the corresponding author declares that there is no conflict of interest.

REFERENCES

1. Bennett, C.H., Shor, P.W. **Quantum information theory**. (1998). *IEEE Transaction on Information theory*. 44(6):2724-2742. https://doi.org/10.1109/18.720553

2. Edeh Michael Onyema et al. **Cloud Security Challenges: Implications on Education**. (2020).*International Journal of Computer Science and Mobile Computing*, 9(2), 56-73.

3. Shor, P.W. **Algorithms for quantum computation: discrete logarithms and factoring**. (1994). *Proceedings 35th Annual Symposium on Foundations of Computer Science*. *IEEE Comput. Soc. Press.*

4. Grover, L.K. **Quantum Mechanics Helps in Searching for a Needle in a Haystack**. (1997). *Phys. Rev. Lett*. 79:325. https://doi.org/10.1103/PhysRevLett.79.325

5. Nguyen, D.M., Kim, S. **Quantum Key Distribution Protocol Based on Modified Generalization of Deutsch-Jozsa Algorithm in d-level Quantum System**. (2019*). Int. J. Theor. Phys.* 58(1):71-82. https://doi.org/10.1007/s10773-018-3910-4

6. Nguyen, D.M., Kim, S. **Multi-Bits Transfer Based on the Quantum Three-Stage Protocol with Quantum Error Correction Codes**. (2019). *Int. J. Theor. Phys.* 58(6):2043-2053. https://doi.org/10.1007/s10773-019-04098-4

7. Nguyen, D.M., Kim, S. **The fog on Generalized teleportation by means of discrete-time quantum walks on N-lines and N-cycles.** (2019). *Modern Physics Letters B.* 33(23):1950270.

8. Peter W. Shor, **Scheme for reducing decoherence in quantum memory.** (1995). *Phys. Rev. A.* 52(4). https://doi.org/10.1103/PhysRevA.52.R2493

9. Nguyen, D.M., Kim, S. **Quantum stabilizer codes construction from Hermitian self-orthogonal codes over GF(4).** (2018). *Journal of Communications and Networks*. 20(3):309-315.

10. Nguyen, D.M., Kim, S. **New Constructions of Quantum Stabilizer Codes Based on Difference Sets.** (2018). *Symmetry*. 10(11):655.

11. Nguyen, D.M., Kim, S. **New construction of binary and nonbinary quantum stabilizer codes based on symmetric matrices.** (2019). *International Journal of Modern Physics B.* 33(24):1950274. https://doi.org/10.1142/S0217979219502746

12. Nguyen, D.M., Kim, S. **Construction and complement circuit of a quantum stabilizer code with length 7.** (2016). *Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*. 332 - 336.

13. Noson.S. Yanofsky, Micro.A. Mannucci, **Quantum computing for computer scientists.** (2008). Cambridge University Press New York, NY, USA.

14. Zidan, M., et. al. A Novel **Algorithm based on Entanglement Measurement for Improving Speed of Quantum Algorithms.** (2018). *Appl. Math. Inf. Sci.* 12(1):265-269.

15. Zidan, M., et. al. **Quantum Classification Algorithm Based on Competitive Learning Neural Network and Entanglement Measure**. (2019). *Appl. Sci*. 9(7):1277. https://doi.org/10.3390/app9071277

16. Zidan, M., et. al**. A quantum algorithm based on entanglement measure for classifying Boolean multivariate function into novel hidden classes**. (2019). *Results in Phys*. 15:102549.

17. K. Ravi, N. K. Pandy, A. S. Kumar, and N. Kushal. **Quantum Computer-Hardware,** *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 5, No. 4, pp. 46-53, 2016.

18. K. Ravi, N. K. Pandy, A. S. Kumar, and N. Kushal. **Quantum Computer-Algorithms,** *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 5, No. 4, pp. 54-60, 2016.

19. A. Naincy, B. Pratap. **Develop a Hybrid Method to Encode Data,***International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 6, No. 3, pp.51-56, 2017.

20. Nguyen, D.M., Kim, S. **A novel construction for quantum stabilizer codes based on binary formalism**. (2020). *International Journal of Modern Physics B.* 34(8): 2050059. https://doi.org/10.1142/S0217979220500599

21. Nguyen, D.M., Kim, S. **Quantum stabilizer codes based on a new construction of self-orthogonal trace-inner product codes over GF(4)**. (2020). *International Journal of Modern Physics B*. 34(5): 2050017.

22. Nguyen, Binh A., et. al. **A Novel Framework for Simulation of Quantum Information System**. (2020) *International Journal of Advanced Trends in Computer Science and Engineering*. 9(2):1752-1756. https://doi.org/10.30534/ijatcse/2020/129922020

23. Nguyen, Binh A., et. al.**Simulation of Quantum Computation via MAGMA Computational Algebra System**. (2020) *International Journal of Advanced Trends in Computer Science and Engineering*. 9(2):1757-1761. https://doi.org/10.30534/ijatcse/2020/130922020

24. Nguyen, D.M., Kim, S. **A Novel Quantum No-Key Protocol for Many Bits Transfer with Error Correction Codes**. (2020)*Advances in Science, Technology and Engineering Systems.* 5(2): 781-785. https://doi.org/10.25046/aj050298

25.Jeong-Woon Choi, et. al. **Random number generating method and apparatus using light source and single photon detector**. US patents number, US9588737B2 https://patents.google.com/patent/US9588737B2/

26. Nguyen, D.M., Kim, S. **Minimal-Entanglement Entanglement-Assisted Quantum Error Correction Codes from Modified Circulant Matrices.** (2017). *Symmetry*. 9(7):122. https://doi.org/10.3390/sym9070122