An Innovative Predictive Quantum Computer Modeling ; The Power of R2022A+ Cryptography Technology

Ndagijimana, P.; Shabani, J.; Nahayo, F.; Et al.

2023
Contemporary Engineering Sciences, Vol. 16
https://repository.ub.edu.bi/handle/123456789/1297

Contemporary Engineering Sciences, Vol. 16, 2023, no. 1, 43 - 54
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ces.2023.93065

An Innovative Predictive Quantum Computer Modeling; The Power of $\mathcal{R}2022\mathcal{A}^{+}$ Cryptography Technology

P. Ndagijimana [1], F. Nahayo [2], J. Shabani [1], M. Kokou Assogba [3] and V. Havyarimana [4]

[1] Doctoral School and Faculty of Science, University of Burundi
[2] LURMISTA-ISTA and Director of Agence Universitaire de la Francophonie AUF-Burundi
[3] EPAC, Ecole Polytechnique d'Abomey-Calavi; Université d'Abomey-Calavi, Cotonou-Bénin
[4] ENS, Ecole Normale Supérieure, Bujumbura-Burundi

Abstract

Due to the revolution of technology since the beginning of the 20^{th} century, it is considerable to develop efficient tools on the quantum level in order to improve confidentiality and interoperability of data. The Quantum computer, with Quantum mechanics as its basic principle, still promises to bring great surprises even though we are at the beginning of its development. Quantum Computer is the only known model for computing that could offer exponential speedup classic computer. The current major challenges of the Quantum Computer include increasing or reducing the number of qubits for a given system, coherence management to preserve the properties of the superposition and entanglement state of a quantum system to perform data operation, of course through appropriate quantum algorithms. In this paper, we will give an overview of a quantum computer, will describe the evolution of cryptography and the theory related to computational performance, efficiency and predictive modeling of Quantum Computers. Prototype and Quantum simulation algorithm will be proposed to improve the life of new quantum universe.

Keywords: Quantum Computer, Cryptography, Prototype, Modeling and algorithm

1 Introduction

Before dealing with the Quantum computer concept, we first refer to Quantum mechanics. We admit the possibility of dealing with the principle of quantum superposition, it means to reduce the number of quantum binary digits(Qubits) needed to perform a computation, to adapt with a new concept convincing that one object could be in several places or states at the same time, even though reportedly, it seems to be impossible! When I am in Laboratory analyzing medical data, I cannot be at a beach enjoying the floating water and soft wind at the same time. According to the classical physics law, we all have a perfectly defined state[1]. When we are there, we cannot be anywhere else! But on the other hand, when we are in the infinitely small world at the level of atoms, then the rules of the day are completely different. It is not easy to be understood, even very difficult to conceive, however every thing could be possible in the Quantum world. The quantum computer, a funny mechanic! How can a particle be in two places or two states at the same time? Example: a living and dead Cat at the same time, a key of our car in two places at the same time and two basketballs always on the same side. We should know that physicists have been trying to explain the phenomena they observed from the origins of quantum physics to the first computer prototype.

I cannot find the key of my car! You haven't seen it by chance? No, there you see, you will find it exactly where you left it. Because here our cat, our key, our juice, our plant, our TV and so on. In short, everything that surrounds us has a well defined mass, position and velocity. For example, the key weighs 48 grams, you put it on the living room table and of course its velocity is zero. All these values define the physical state of your key. It has only one perfectly defined state. This vision of the world is clear, our daily objects are well described by the physics known as classical.

But in a world of science fiction, imagine your key being in several places at once, both in living room and in kitchen. This is usually seems impossible for objects on our scale, but it is common for microscopic objects. If we extract for example an atom from your key and isolate it in a free vacuum without light, we observe a situation that requires us to radically change our view of the world.

As answer to the previous question in the first paragraph of this section, the atom can of course be placed in 2 or 3 even an infinite number of places at the same time. The atom is then said to be in a quantum coherent superposition of states. This phenomenon is a particular case of a basic principle of quantum physic, a branch of physics that describes well the microscopic world. At the microscopic scale, the atom has a property that is not equivalent to our everyday life! It behaves sometimes like an atom, sometimes like a wave. When it is not well observed, the atom must be assimilated to a wave. The

same atom, is present everywhere at the same time in the same way as water is a fluid present everywhere along a surge. We provide a quick briefing to the concept *Superposition*.

Superposition: As one of Quantum Computer fundamental properties leads on quantum mechanics to store, present and perfom operations on data in such away so that it can compute exponentially faster than any classical computer[2].

Superposition in quantum computing refers to the ability of Qantum system when quantum particule or Qubit can exist in two positions or say, in multiple states at the same time. Let's dig into the following experment. The h gate makes a new state: $|+\rangle = H|0\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ that is a uniform superposition of the $|0\rangle$ and $|1\rangle$ state. The measurement forces the system to be in ether the $|0\rangle$ state or $|1\rangle$ with an equal probability.

In the second experment, we made a new state: $|-\rangle = H|1\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$, that is still a uniform superposition of $|0\rangle$ and $|1\rangle$ with different sign.

In the last case, we can take the sum of two previous experments $H|0\rangle$ and $H|1\rangle$.

After adding the two experments together, the $|1\rangle$ state cancels out because of the minus sign.

From now , we can see the difference between classical probability p and the quantum amplitudes ψ, which can be positive, negative, or even complex. The relationship between classical probabilities and quantum amplitudes is $p = |\psi|^2$, and is known as Born rule.

Putting all this together gives: $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$, and using $|+\rangle = H|0\rangle$ and $|-\rangle = H|1\rangle$, uniquely defines the Hadamard gate in computational basis by the following matrix:

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

Sum, from the following relation, you see that Qubits can be in the quantum superpositions, and these superpositions can have a sign that leads to interference. The given physical system in a definite state could still befave randomly.

2 Quantum Computer prototype Modeling

In this section we will identify the gape between Classical computer and the Quantum one . The prototype and short algorithm to be implemented will be also proposed. Since the Quantum Computer is based, as its name indicates, on quantum mechanics, we prefer to go back to the essential notions of quantum mechanics and quantum computing[3]. The power of Quantum computing

is estonishing and not many people benefiting from the full potentialities it has to offer. We look first at what makes quantum computing different from todays common place classical computing [4]. Quantum Computer uses quantum bits QUBITs and they are distinguished from classical BITs by their properties. The qubits obey all the rules of the quantum physics and ,in particular, principle of superposition $|0\rangle + |1\rangle$, that means they can take all the values at the same time.

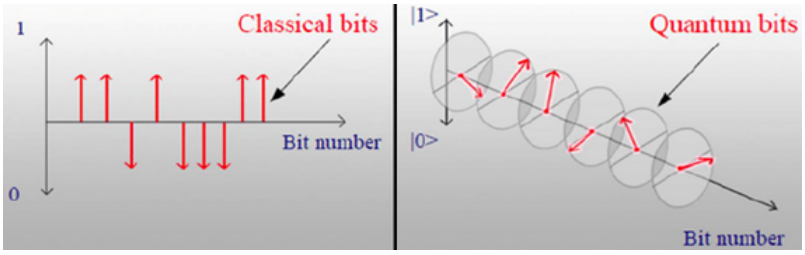

Fig.1: Graphical representation of BITs alongside QUBITs[4].

2.1 Qubits modeling

(a) The Qubit (quantum binary digit): is the basic unit of quantum information. It is a quantum system with two states, which means that it evolves in a Hilbert space of dimension 2. While a classical bit can take the values 1 or 0, a Qubit can rather be, in an analogous way, in two states, but also in a superposition of both states: $|0\rangle$ and $|1\rangle$. This is what differentiates the *classical bit* from the *quantum bit*. Instead of just two values, we have a vector with two components, and single qubits operations:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2}$$

The state of a qubit is generally noted as follows:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle; \tag{3}$$

where α and β are coefficients such that : $|\alpha|^2$ is the probability of being in the state$|0\rangle$ and $|\beta|^2$ that of being in the state $|1\rangle$.In the real world where bits are perceived as 0 or 1, only one of the four possible states can exist at any time in space.

01	00
10	11

However in a quantum superposition state, all four of the possible states can coexist in time and space simultaneously. It is in this principle of quantum superposition that the interest of quantum computation lies.

(b) With two Qubits: Let us examine the case of two qubits. Consider now electons in two hydrogen atoms:  . Classically, the two electrons

are in one of four states: 00, 01, 10, or 11 and represente two bits of classical information. But Quantum mechanically, they are in a superposition of those four states: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle| + \alpha_{11}|11\rangle$;
where $\sum_{ij} |\alpha_{ij}|^2 = 1$.

2.2 Qubit Logic Gates

Since we know what qubits are, we need to know how to manipulate them. This means taking a quantum state as input and obtaining another quantum state as output, because this is what a computer does. To do this, we use *Quantum Logic Gates* which are the analogue of the logic gates which constitute quantum computers. Since our qubits $|0\rangle$ and $|1\rangle$ can be represented by column vectors as explained before, we can thus represent the NOT gate by a matrix X as follows:

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4}$$

we then see directly that:

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \Leftrightarrow X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \tag{5}$$

$|\psi\rangle = \alpha_{00}|\uparrow\uparrow\rangle + \alpha_{01}|\uparrow\downarrow + \alpha_{10}|\downarrow\uparrow\rangle|\alpha_{11}|\downarrow\downarrow\rangle\rangle$;

In fact, we can always represent a quantum logic gate by a matrix. This comes from the linearity of the equations determining quantum mechanics. In order to perform any algorithm in quantum system, there must be operations that correspond to some universal set of quantum gates. These criteria can be used to test the adequacy of realisation of a quantum computer.

2.3 Large scale Computer architecture

To build a large scale of quantum computing that can efficiently impliment quantum properties in its operation is a great challenge for researchers[6]. One of the most challenging problems is that the quantum information is quickly loste during operations due to the decoherence. So, it is not easy to construct a large scale of quantum computation with a large quantity of Qubits.The proposed solution to this problem is to find a way on how to minimize the total volum of physical hardware for topological quantum computation.

Fugure2 also describes the architecture of Quantum calculator and the implementation of its work in order to overcome its common technical problem.

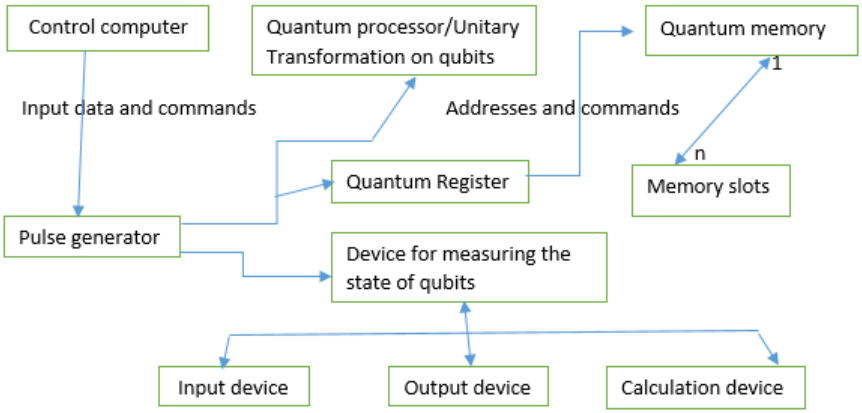

Fig.2: Quantum Computer architecture.

Especially, computer capability has the potential to challenge the way we use encryption to secure much of our digital life, whether it is the protection of confidential data, the privacy of our online communications.
The encryption and decryption system is composed of a quintuplet[8]; example:
$(P, C, C_k, D_{k'}, K)$ o:
-P is a set called clear text space(plain text)
-C is a set called space of cipher text
-K is a set called key space
-Gen_k a key generation algorithm (= the elements of K);
-C_k: $P \rightarrow C$ is a left invertible function called the encryption function and which depends on a parameter k called key;
-$D_{k'}$: $C \rightarrow P$ is a left invertible function of C_k (i.e $D_{k'}$ o $C_k(m) = m$, $\forall m \in P$) and is called the decryption function (depending on the key k') .

Unlike a classical computer, a quantum computer can therefore calculate several values at the same time
By Ecnrypting the Quibit in relation(3), we consider an operation where an attacker can not determine the probability emplitude of the number of measurements already performed[10]. Once the key generation procedure is defined, we can also define the qubit encryption procedure.
Suppose Alice wants to encrypt the qubit in the relation(3) for Bob. Encryption is done as follows:

1) Alice generates randomly a set of r natural numbers ranging from 1 to n. This set is noted with R=$\{r_0, r_1, ...r_n\}$, $1 \leqslant r_i \leqslant n$.

2) We denote with U_R, the composition with the transformations $U_{r_1}, U_{r_2}, ...U_{r_n}$. Alice applies the transformation U_R to the Qubit in relation(3).
The Qubit new state (encrypted) is now $|\psi\rangle = U_R|\psi\rangle$. Alice sends then Bob via an unsafe channel the Qubit in its new state(encrypted).

Encryption of a Qubit is a cryptographic operation that does not allow an attacker to access a probability amplitudes that define the superposition of the qubits. The encryption operation assures that the attacker can not reconstruct through quantum tomographic the content of message during its transmission.

2.4 Quantum Computer Efficiency proof

It is already known that quantum computer relies on Qubits[11] to run and solve multidimentional quantum algorithms to conduct measurements and observations. I am looking for the book. Don't you know where it is stored? No, but you have to find the answer with the computer in this library. Careful, I will tell you how it works! First of all, you must know that a classic computer uses a particular language "binary language" that is to say for image, sound, video issue, text, even the titles of books in this library. In short, all information stored and processed by a computer are translated into a sequence of 0 and 1, each 0 and each 1 is called a BIT, these sequences of 1^s and 0^s are filed in a numbered memory with specific addresses, as the address that indicates where you live for example.
But what does this computer do with these 1^s and 0^s at this or that address? Well, it adds them, multiplies them or even compares them via small electronic circuits called "Logic Gates" as seen before. These gates perform all sorts of simple logical operations; they deliver themselves as a result in form of a 1 and a 0. But, this still doesn't tell me how these logic gates will find the location of my book? To understand this, let's take the title of the book you are looking for:

- The computer saves it in a box in its memory;
- In other boxes the titles of the books are already recorded;
- Each one has an address corresponding to its place in the library;and
- The computer will use a network of logic gates to compare the Bits of any of each title in the list. This gate array is often called ORACLE.

An oracle gate in quantum gate is usually a "variable" gate. It enables the encoding of a problem instances and representes in this way the input of a quantum algorithm.
By using a quantum type, it must be an intervention of quantum bits so called q-bits and they are distinguished of course from classical bits. These q-bits obey all the rules of quantum physics and in particular principle of superposition. With this new paradigm, our logic gate array is called q-Oracle. According to the following example, q-oracle will be responsble to find the location of the book in the Library. According to this quantum mechanic, the

needed book has been found at the position number 2 on the first floor up of this Library(Fig.3).

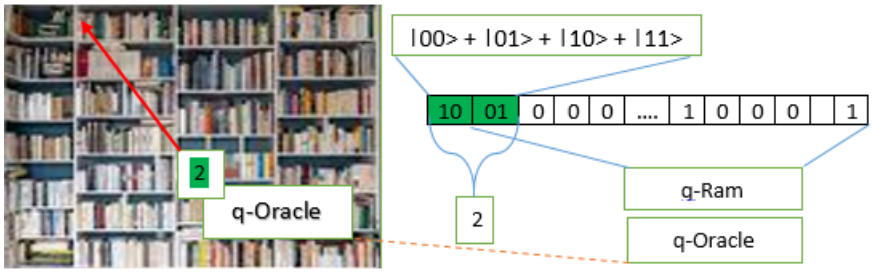

Fig.3: Book searching from Library via q-Oracle.[1]

It is therefore very necessary to respect the algorithm if one wants to be totally certain of the answer. Anyway, the Quantum Computer remains efficient to solve some mathematical calculations which become impossible to solve using classical computers beyond a certain volume of data.
Especially, Quantum Computer is not intended to replace our classical ones because its applications will be different. It should improve and meet specific needs, example for the army, banks, in the field of artificial intelligence, Internet of things(IoT), e-Learning, sorting and analyzing very quickly information in gigantic databases, more precise medical diagnoses or simply in the search engines more powerful on the Internet. Anyway, the current researches are fertile for the fundamental research because it allows to better understand this quantum universe and more necessarily they open the life to a new technological revolution.

3 $\mathcal{R}2022\mathcal{A}^{+}$ Algorithm

The construction of quantum computers represents many challenges but also potential major contributions both technologically and theoretically. Most of the applications of quantum computers concern computer science and algorithms. Even in information security, encrypted data to be vulnerable to a quantum computer they must become first discoverable and exposed to a quantum cryptographic algorithm.

Algorithm: Quantum algorithms require a different way of thinking than a way one normally approaches programming. It is not possible to store quantum states on a working memory for accessing later in the algorithm[12][13]. This is due to the so called *no-cloning* principle of quantum physics. It is not possible to make a copy of quantum system. But it is possible to move the state of a set of qubits to an other set of qubits. Quantum algorithm consists of thee basec steps:

-Encording of data, which could be classical or quantum into the state of a set of input quibits;
-A sequence of quantum states applied to this set of input quibits;
-Meseaurement of one or more of the qubits at the end to obtain a classical interpretable results.
A quantum computer can perform the simulation of dynamic much more efficiently. Quantum simulation seems to be an important application of Quantum Computer.
A quantum computer similation means"***predicting***" the state of a system at some functional time t_f as efficientely as possible given an initial system state. Let the n-qubit $|\psi\rangle$ approximate a given system. Then, the quantum computer similation algorithm can be presented as follows:

Algorithm 1 :Quantum Simulation Algorithm

Input:
$\psi_0 = 10,\ \ \varepsilon_0 = 10^{-1000}$
maxiter $= N$
Time step size $\Delta t\ ,\ \ t_f$

Output:
$|\psi_{t_f}\rangle\ ,\ \ t_f$

Step1:

For $1 \leqslant$ j $\leqslant$ N *do*
$|\psi_{j+1}\rangle = \Delta t\ |\psi_j\rangle$;
$j = j + 1$;

Step2:

$if\ \ j\Delta t \leqslant t_f,\ \ \frac{|\psi_N - \psi_{N-1}|}{N+1} \leqslant \varepsilon_0$;
write $|\psi_{t_f}\rangle$;
End For
else
return to step1.

The purpose of this algorithm was to give a proof of concept of how quantum computer perform based on how the state of its system at some functional time regarding to simulation state and the process . Each step presents the simulation in practice consistent with the theory and literature.

Quantum Computing and algorithms meet some specific requirements such as the number of qubits, fiting of hardware architecture and will have a brighter common future. Algorithms could be implemented so that they can run and be tested on quantum computer. Especially, a good quantum algorithm solves the order finding problem during data processing partucularly under a quantum system.

4 Conclusion

Apart the overview of a Quantum computer, in this paper, we described the evolution of cryptography and the theory related to computationnal performance, efficiency, prototype and predictive modeling of a quantum computer. The properties of the superposition state of a quantum system to perform data operation has been described.
However, the development of quantum computer could pose different challenges for research and society today, example on the possible global impact on digital security. Quantum computing capabilities and technologies will serve as the foundation of a second information age[14].
The Quantum computer, apart it is in its experimental phase, it is not intended to replace our classical ones because its applications will be different.

The following elements are among those which make Quantum computing different from conventional or classical computing[4]:
-Classical computing calculates with Transistors which can represent either 0 or 1 while Quantum computation calculates with Qubits,which can represent 0 and 1 at the same time.
-Classical computing encreases power in a 1:1 relationship with the number of transistors while for Quantum computation power encreases exponantially in proportion to the number of Qubits.
-Only specifically defined results are available, inherently limited by algorithm's design while Quantum answers are probabilistic because of suporposition and entanglement, multiple possible answers are considered in a given computation.

The current researches allow to better understand this quantum universe and more necessarily they open the life to a new technological revolution.

Acknowledgements. The authors would like to thank all the reviewers for their very constructive comments. Many thanks to the Doctoral School of University of Burundi, and many thanks to the authorities of Antenne Afrique des Grands lacs de lAUF-Burundi for their support.

Conflucts of Interests. The authors hereby declare not confluct of interests regarding the publication of this paper. The information contained in this paper is original and any work done by others or by the authors themselves previously has been aknowledged and referenced accordingly.

References

[1] J. Fauquet and C. Vastine, L'Esprit Sorcier: Le principe de lordinateur quantique, 2020. https://youtu.be/2aCS5mEeiwg

[2] Marella, Surya Teja, and Hemanth Sai Kumar Parisa, Introduction to quantum computing, in *Quantum Computing and Communications*, IntechOpen, 2020.

[3] C. Linnhoff-Popien, Quantum Computinga new hype?, *Digitale Welt*, **3** (2019), no. 2, 9-10. https://doi.org/10.1007/s42354-019-0159-x

[4] With CB Insights Center: Quantum Computing Vs. Classical Computing In One Graphic (February, 2021).

[5] Song, G., Jang, K., Kim, H., Eum, S., Sim, M., Kim, H., ... and Seo, H., SPEEDY Quantum Circuit for Grovers Algorithm, *Applied Sciences*, **12** (2022), no. 14, 6870. https://doi.org/10.3390/app12146870

[6] Lov K. Grover, Fast Quantum Mechanical Algorithm for Database Search, STOC96: *Proceedings of the Twenty-Eighth annual ACM Symposium on Theory of Computing*, July 1996, 212-219. https://doi.org/10.1145/237814.237866

[7] Landry Bretheau, Les ordinateurs quantiques: comment ca marche?, July, 2021. https://doi.org/10.48556/sif.1024.18.35

[8] Vergnaud, Damien, *Primitives et Constructions en Cryptographie Asymetrique*, PhD diss., Ecole normale superieure, 2014.

[9] Vitaliy Konyukhov: American University in Bulgaria, Mathematics of Post-Quantum Cryptography, 5-11-2022.

[10] Plesa, Mihail-Iulian and Togan Mihai, A new quantum encryption scheme, *Advanced Journal of Graduate Research*, **4** (2018), no. 1, 59-67. https://doi.org/10.21467/ajgr.4.1.59-67

[11] Bhaskar, M. K., Hadfield, S., Papageorgiou, A., and Petras, I., Quantum algorithms and circuits for scientific computing, *Quantum Information and Computation*, **16** (2016), 197-236. https://doi.org/10.26421/qic16.3-4-2

[12] P. Shor, Algorithm for Quantum Computation: Discrete Logarithms and Factoring, *Proc. 35 th Annual Symposium on Foundations of Computer Science*, IEEE Press, November 1994, quant-ph/9508027, 124-134. https://doi.org/10.1109/sfcs.1994.365700

[13] Lov K. Grover, A Fast Quantum Mechanical Algorithm for Database Search, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC 96, Philadelphia, Pennsylvania. https://doi.org/10.1145/237814.237866

[14] Piattini, Mario, Petersen, Guido and Perez-Castillo, Ricardo, Quantum computing: A new software engineering golden age, *ACM SIGSOFT Software Engineering Notes*, **45** (2021), no. 3, 12-14. https://doi.org/10.1145/3402127.3402131

[15] Ndagijimana, P., Nahayo, F., Assogba, M.K., Ametepe, A.F.X. and Shabani, J., Towards Post-Quantum Cryptography Using Thermal Noise Theory and True Random Numbers Generation, *Journal of Information Security*, **11** (2020), no. 3, 149. https://doi.org/10.4236/jis.2020.113010

Received: September 27, 2023; Published: December 11, 2023