IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 1, February 2019
ISSN (Online): 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Secure Wireless Sensor Network Using Toffoli and Peres Logic Gates Based Quantum Cryptography

Gaudence StanslausTesha

School of Telecommunications Engineering, Xidian University, Xi'an 71007, China.

Abstract-The wireless sensor network is a self-organized network and data distribution system. The article focus on the data security using the application of quantum cryptography that ensure transmission of data from source node to the sink node within the wireless sensor network. Toffoli and Peres logic gates applied for secure communication within the Wireless sensor network indicates the security improvements and the energy suitability. We present the random Einstein Podolsky Rosen paradox (EPR-pair) allocation scheme that overcomes the susceptibility caused by possible compromised nodes. The EPR-paradox pairs are pre assigned quantum bit to sensor nodes randomly. The quantum entanglement through the entangled pair used by the nodes with the quantum teleportation to form a secure network link within the Wireless network. The results indicated both Toffoli and Peres gates generated the model output mathematical expression for transmitting data from source sensor node to sink sensor node. The simulation results indicates the output results is equal to the model mathematical expression.

Keywords: *Quantum cryptography; Quantum bit; Sensor node; Quantum teleportation, wireless sensor network*

1. Introduction

The wireless sensor network (WSNs) is type of network built of sensor nodes and each node connected to one another. The sensor nodes have communication components such as radio receiver, a microcontroller and an energy source, which enable the processing of data. The sensor nodes communicate over the short distance via a wireless communication medium [1].

The development of WSNs inspired by the military application, particularly surveillance in conflict areas. Today rapid technological expansions through sensors and WSN, which use the sensors, as node is the key technology for Internet of Things (IoT) [2]. The word IoT is the network of physical devices, vehicles, home appliances, which applied to social life application such as smart electric meter reading, intelligent transportation system use electronic cards, smart home monitoring or smart cite control management.

The IoT does not have a specific communication technology like traditional existing network such as Transmission Control Protocol (TCP), Hyper Text Transfer protocol (HTTP) or Internet protocol (IPv6), but the wireless communication technology plays a major role and in particular, a WSN proliferate many applications in various industries to ensure the IoT networking.
Nowadays, the vision of smart home, smart grid, smart network and even the smart city have become true with the implementation of IoT through the WSN. The WSN are part of IoT and researchers studied for many years [3], [4]. Furthermore, the integration of the sensors and actuators that form a WSN in the IoT require new technology and protocol for full implementation.

Data privacy protection is one of the application challenges of IoT [5]. The IoT does not have the same security issues as WSNs, mobile communications networks like ad-hoc network and the Internet. Thus, the lowest layer in IoT known as perception layer is responsible for information collection and the WSN is responsible for data collection from the network. In the process of collecting data, the message may be subject to eavesdropping, malicious routing, message tampering and other security issues linkage, which affect the security of the entire IoT network.

The mainly function for the network is to sense the environmental condition then send recorded data to destination node or base station (BS) for processing and storage [6], [7]. However, technology delivers maximum flexibility to respond to almost all types of industry application global that is, online purchase monitoring like using online websites, electronic mails, mobile money transaction and other online application. These makes the application of the WSN a greatly contribution to the world industrial development.

Due to the important of the online application for today human daily activities, there is a need for researchers to ensure the security mechanism for

this business as it touches everyday human activities.

Thus, the main issue to addressing is data security within the WSN. Assuming an example of bank security system using the sensor network and global system for mobile (GMS) network. The security network using the sensors for sensing the banking theft and send short message or call nearby police or (banker authentic person) for alerting the theft. Thus, if the robbery hacking the communication between the sensors and GSM network they will successful stealing money from bank. The hacker steal money without the system to alert police or (banker authentic person) noted which affect the security of the entire IoT or via the GSM network hackers stealing your bank details then they will do the same and any others places where we use the mobile authentication to get access. Many studies have demonstrated and suggesting of using the traditional security mechanism such as watermark, routing algorithm, Elliptic Curve Cryptography (ECC), and classical cryptography [8], [9], [10] and [11].

The aforementioned problem can be overcome using the reversible logic gates through the quantum teleportation that transfer the quantum information from source sensor node to sink sensor node within the WSN using the EPR pairs as qubits through the quantum Channel.

The main objective is to investigate the communication between source sensor nodes to the sink node and provide safe communication by applying quantum teleportation through the adoption EPR pair and the reversible quantum logic gate. The manuscript contribution are:

a) Utilization of using the logic gate to WSN for security mechanism.
b) Maintain lifetime for sensor nodes due to less processing mechanism of the logic gates
c) Deployment of quantum entanglement to WSN and adoption of using the reversible quantum logic gates overcome the suspicions of the hackers
d) Ensure the unbreakable for message transmitted from source sensor node to sink sensor node within the WSN when using the quantum teleportation.

2.Related Works and Motivation

The idea of WSN security system using application QC as defined in this paper is to incorporate different types of situations that in common secure management of information in presence of quantum devices. Security in WSN, however is an important issue for widely available wireless networks that has been studied less extensively than other properties of these networks such as for example, their reliability [12]. The [12] said that the QC has advantages than classical cryptography system namely as unbreakable keys and therefore unbreakable message when applied to WSN. The [13] elaborate demerit of using the ECC enhances the encrypted message size compared to RSA encryption. Moreover, the implementation of the ECC is highly complex than RSA and also increasing the implementation errors and thus, decreasing the algorithms security. The application of using QC can reduce complexity of the ECC [14]. Quantum cryptograph is presumably secure against any eavesdropped and thus labelled as providing unconditional security [15]. The QC [16] is a new authentication mechanism that enables a legal user with a single credential authenticated by multiple service providers in a distributed computer network.

The authors, [17], [18] justify the application of the quantum logic gate that provide low power for optical computing and quantum cryptography. A quantum logic gate is a basic circuit operating on a small number of Qubits. Quantum logic gates are reversible, unlike many classical logic gates represented by unitary matrices. However, [19] identifying universal quantum gates in 1989 by generalizing the three-bit Toffoli gate, that known to be universal for reversible Boolean logic gate, he identified a three-qubit gate that is universal for quantum logic gate that operates on the three qubits at a time. The universal quantum logic gates known as quantum gates are NOT, XOR and Walsh − Hadamardgates [19].

We consider figure (1a) presents $3 * 3$ Toffoli gate [17], [20], with inputs and output vectors (A,B,C) and (P,Q,R) respectively. Output P equal to A, Q is equal to B and R equal $AB \otimes C$.

In addition, figure (1b) present the Feynman logic gate with 2 inputs 'A' and 'B' respectively. Their outputs 'P' equals to 'A' and 'Q' equal to $A \otimes B$, the Feynman gate also called CNOT gate or quantum XOR [17].Thus, the expression of the inputs and output from the gates as indicated on Eq. (1) and (2).

$$(A,B,C) \Rightarrow (P,Q,R) = (A,B,AB \otimes C) \quad (1)$$

$$(A,B) \Rightarrow (P,Q) = (A,A \otimes B) \quad (2)$$

The representation of this Eq. (1) and (2) indicates that the output bit $'P'$ is just the same as its input$A$, whereas on the output of the second with Q the operation $A \otimes B$ performed. This operation (XOR of A and$B$) is a standard logic operation. A linear gate is the one that all its output is linear functions of input variables. Assuming $2 * 2$ Feynman gate, $P = A$, $Q = A \otimes \mathrm{B}$, when $A = 0 \text{then} Q = B$, when $A = 1$ then$Q = B$. The Feynman gate used as a fan out gate figure (1b). The Hadamard logic gate refers figure (1c) acts on a single qubit. It maps the basic state of $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ [13], [14] this means that a measurement will have equal probabilities to become $0\ or\ 1$

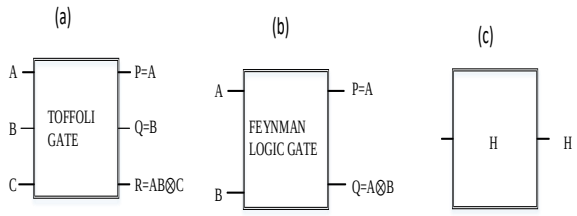

Fig.1: Representation of gates symbols. (a) Toffoli logic gate three inputs, three outputs (3*3) (b) Feynman logic gate two inputs, and two outputs (2*2) (c) Hadamard Logic gate, one input, and one output (1*1).

2.1 Challenges of Quantum Cryptography in Wireless Sensor Networks

Quantum cryptography is one of the technics for security in WSN but does not confront the security problems alone [14]. It is essential to use the key management process carefully in order to achieve higher security system networks [9], [21]. In security development, the technical challenges using the QC is on the key management process based resources constrained like low processing power for sensor node, bandwidth, and low battery lifetime.

The suggesting is to use then lightweight security protocols, which consume less energy but provide high security system to WSN as the idea of [22]. Turkanovic and Holbl [13] said that, although the quantum for WSN do not exist yet but it is necessary to analyse the possible challenges and problems for application use. Phatia and Sumbaly [23] suggest that, main challenges for classical cryptographic security in WSN is the key distribution that improved by applying the Quantum key distribution (QKD). Moreover, Hu et al [24] point out that, traditional internet style key management protocols based on infrastructures using trusted third parties are impractical for large scale WSNs because of the unknown network topology prior to deployment and serious node constraints such as limited power and limited transmission range.

Thus, QC using the quantum teleportation with the application of the quantum logic gates offer solution for the aforementioned challenges by provide the secure data communication, energy lifetime and data privacy. Using the quantum cryptography generate true randomness keys superposition and it can allow two part on communication to generate encryption and description secure key for description process through the application of reversible logic gates using the quantum teleportation.

2.2 Security Algorithm Model

In quantum computing, quantum bit is a unit of quantum information (qubits). A qubit is a two state quantum mechanical system, such as the polarization of a single photons means that two state are vertical and horizontal polarization. In a classical system, a bit would have to be in one state or other like $(0\ or 1)$ [25]. However, quantum mechanics allows the qubit to be in a superposition of both states at the same time. A qubit has a few similarities to a classical bit, but is overall very different. By consider qubit there are two possible measurements as $'0'$ and $'1'$, like a bit. The difference among the two is that whereas the state of a bit is either$(0\ or 1)$, the state of a qubit can also be a superposition of both at the same time. It is possible to full encode one bit in one qubit. Furthermore, a qubit can hold even more information. The two state in which a qubit may be measured known as basis state or basis vector. That indicates $'2'$ computational basis states as$|0\rangle$ and $|1\rangle$ [14], [25], [26]. A pure qubit is a linear superposition of the basis states. So qubit is therefore a unit of quantum information associated with two-dimensional.

The state of qubit can be changed using quantum logic gates, which are equivalent to the classical logic gates for example, XOR, NOR, and NAND gates. By changing the state of qubit, the quantum information of a qubit actually manipulated. The quantum logic gates are crucial for quantum computation and teleportation. Thus, for this study the quantum logic gates change the classical bit

information to qubit and transport using the quantum teleportation through the quantum channel.

Classical computation has the ability to store and operate information on combination of bits, quantum computation works on quantum systems called qubits. In contrast to classical bit, which has either of the two mutually exclusive states, a qubit exists in a superposition of two states. The most model of a qubit as from the superposition principles, which state that if there are two or more stimuli at a given point in time, the response will be the result of adding all the responses [8], the expression formulated as refer Eq. (3).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (3)$$

Where variables of α and β are complex numbers as shown Eq. (4).

$$|\alpha|^2 + |\beta|^2 = 1 \text{ and } |1\rangle = [1,0]^T, |1\rangle = [1,0]^T (4)$$

That means α and β have the physical meanings that any given measurement of qubit indicates the system to be in state $|1\rangle$ with a probability of $|\alpha|^2$and state$|1\rangle$ with a probability$|\beta|^2$. However, $\alpha|0\rangle + \beta|1\rangle$ and $\alpha|0\rangle - \beta|1\rangle$ have the same probabilities for their measurements. The vector $\binom{\alpha}{\beta}$ can be represented as $\alpha|0\rangle + \beta|1\rangle$.Therefore; quantum entanglement has applications in the emerging technologies of quantum computing and quantum cryptography, and used to realize quantum teleportation experimentally. Most considerable usage of quantum entanglement is in the area of quantum teleportation. Bennett et al. [27] in 1993 first proposed a quantum technique for teleportation. His protocol implements intangible transfer of states a system to remote system. After a measurement made causing one member of such a pair to take a definite value like clockwise spin, then the other member of entangled pair found to have correctly taken the correlated value. Hence the correlation exists between the measurements performed on entangled pairs, and this correlation is still observed even the pair is departed by large distances. Thus, the manipulation of the two-dimensional complex vector space as a $'n'$ qubit system can exist in any superposition of the 2^n basis states as Eq. (5).

$$\alpha_0(|000\rangle + \alpha_1|001\rangle + \cdots \alpha_{2^n-1}|111\rangle \quad (5)$$

Whatever state it can be decomposed into the state of individual bits as refer to Eq. (6)

$$\frac{1}{2}(\left|00\right\rangle + \left|01\right\rangle + \left|11\right\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (6)$$

Considering the quantum entanglement when comparing the two (2-qubit) will have consider Eq. (7). If, we measure the first qubit in the first case we can see it has $|0\rangle$ with a probability of 1 and state remain unchanged as from two-dimensional complex vector space. If the second case qubit pair measured, the first bits gives $|0\rangle$ or $|1\rangle$ with equal probability [28] thereafter, the second qubit is also determined.

$$\frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|01\right\rangle), and\ \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (7)$$

The entanglement does not depend on the distance, meaning that if we would separate these two particles example entangled pairs, the bond would still hold, and the changes on one entangled pair would immediately affect the states of the other. Scientists have already successfully tested this phenomenon on the distance over 144km [29].The feature that distinguish between a qubit and a classical bit is that multiple qubits can exhibits quantum entanglement. Entanglement is a non-local property that allows a set of qubits to express higher correlation than is possible in classical systems. Example, two entangled qubits in the bell state measurement [29] as refer to Eq. (8).

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (8)$$

In this state, called an equal superposition, there are equal probabilities of measuring either $|00\rangle$ or $|11\rangle$ as $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$. Imagine that these two entangled qubits are separated, the instantaneous effect of entangled pairs, regardless on the distance, implicates that the information about the change, between the pairs, regardless on the distance, indicates that the information about the change, between the pair flow faster.

3. Quantum Teleportation

Quantum teleportation is the process in which qubits transmitted from one location to another location using the classical communication, shared the quantum entanglement between the sending, and receiving locations. The most remarkable usage of quantum entanglement is the quantum teleportation. In 1993, Bennet et al [27] propose

quantum teleportation. The protocol implements disembodied transport of the state of a system to a remote system. An unknown quantum state of a system to a remote system. A quantum state $|\Theta\rangle$ initially prepared by tensor product of the three separate states that kept by sender and receiver respectively. The qubit transmitted using the quantum teleportation that use classical communication, that shared quantum entanglement pair between the sending (source node) and receiving (sink node) [30]. According to the nature of the quantum entanglement, if any third part try to use the key will be detected both side in receiver and sender instantaneously and noticed that they are hacked.

4. Proposed Security Model

The environmental for the quantum teleportation has many applications, like transmission of quantum states in noisy environments and sharing states in distributed networks. Previously application of quantum teleportation [28] have being using the quantum teleportation through the controlled not gate (CNOT) gate). The CNOT gate is the $2*2$ gates, although indicates the performance but it is less security because it uses only 2 inputs and have 2 outputs. This study, introduce quantum teleportation on a $3*3$ using the Toffoli and $3*3$ Peres logic gate that improve and ensure more security than CNOT gate.

By considered the Feynman logic gate $2*2$ as indicated from figure (1b). The quantum state $|\psi_0\rangle$ initially formed by tensor product of three separate states that kept by sender and receiver respectively as depicted from Eq. (9a), (9b), and (9c).These are the basic for the quantum states.

$$|\psi_0\rangle = |\psi\rangle \otimes |0\rangle \otimes |0\rangle \quad (9a)$$

$$|\psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle \otimes |00\rangle) \quad (9b)$$

$$|\psi_0\rangle = \alpha|000\rangle + \beta|100\rangle \quad (9c)$$

Let's applying the Hadamard logic gate to the second qubit $|\psi_1\rangle = \alpha|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \beta\left|1\right\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes|0\rangle$

Therefore,

$$\left|\psi_1\right\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + \left|010\right\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (10)$$

Then, the $2*2$ Feynman gate applied from the second to the third qubit as Eq. (11).

$$\left|\psi_2\right\rangle = \frac{\alpha}{\sqrt{2}}(\left|0\right\rangle + (\left|00\right\rangle + \left|0\right\rangle + \left|10\right\rangle)) + \frac{\beta}{\sqrt{2}}(|1\rangle + (|01\rangle + |1\rangle + |10\rangle))$$

$$\left|\psi_2\right\rangle = \frac{\alpha}{\sqrt{2}}(\left|000\right\rangle + \left|011\right\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |111\rangle) \quad (11)$$

Furthermore, the Feynman gate applied from the first to the second qubit, which transform $|\psi_2\rangle$ into $|\psi_3\rangle$

$$|\psi_3\rangle = \frac{\alpha}{\sqrt{2}}(|00\rangle \otimes |0\rangle + |01\rangle \otimes \left|1\right\rangle) + \frac{\beta}{\sqrt{2}}(|10\rangle \otimes |1\rangle + |11\rangle \otimes |1\rangle)$$

Therefore,

$$|\psi_3\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|111\rangle + |101\rangle) \quad (12)$$

Then if the Hadamard gate is applied to the first qubit it produce the $|\psi_4\rangle$ as Eq. (13)

$$|\psi_4\rangle = \frac{\alpha}{\sqrt{2}} * \frac{1}{\sqrt{2}}(\left|1\right\rangle + \left|0\right\rangle) \otimes (\left|00\right\rangle + \left|11\right\rangle) + \frac{\beta}{\sqrt{2}} * \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|11\rangle + |01\rangle)$$

$$|\psi_4\rangle = \frac{\alpha}{2}(\left|1\right\rangle + \left|0\right\rangle) \otimes (\left|00\right\rangle + \left|10\right\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle) \otimes (|01\rangle + |10\rangle) \quad (13)$$

According to figure (2) that indicates WSN environment using the quantum teleportation in which two nodes *A* and *B* are communicating to remote BS. Each node assigned a qubit pair. The nodes are communicating with each other through a mechanism of quantum teleportation using the quantum logic gates. The quantum teleportation transmits the quantum information after the conversion. The logic gates through the normal classical communication as shared with the quantum entanglement between the sending process and receiving side. The quantum entanglement ensures the message travel between the two side Node *A* and node *B* instantaneously. It provides way of transporting qubits from node *A* and node*B*. The use of the quantum gates makes the environment a more reliable and secure.

The second $3*3$ Toffoli gates were applying by consider the quantum state $|\psi_0\rangle$ as prepared early Eq. (9a), (9b) and (9c).

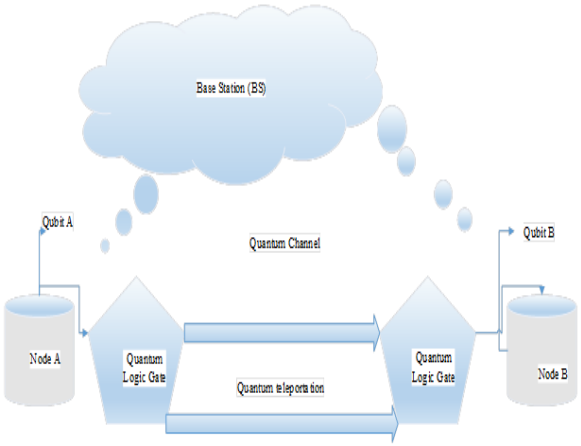

Fig.2: Quantum teleportation using the Quantum logic gate in wireless sensor network. Data move from Node 'A' as a source node to Node 'B' that is sink node through quantum channel. Key exchange between the quantum logic gate through quantum channel by comparing the qubits states between the sender and receiver.

Applying the Hadamard gate to the second qubit to obtain quantum state $|\psi_1\rangle$ as:

$$|\psi_1\rangle = \alpha|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \beta\left|1\right\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

$$\left|\psi_1\right\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (14)$$

When applying the $3x3$ Toffoli gate from the second to the third qubit, refer Eq. (15)

$$|\psi_2\rangle = \frac{\alpha}{\sqrt{2}}(\left|000\right\rangle + \left|010\right\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle)$$

$$|\psi_2\rangle = \frac{\alpha}{\sqrt{2}}(\left|001\right\rangle + \left|010\right\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (15)$$

Generate Toffoli gate from $|\psi_2\rangle$ we will have $|\psi_3\rangle$ Eq. 16

$$|\psi_3\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (16)$$

Thus, by applying the Hadamard gate to the first qubit, it produce $|\psi_4\rangle$ as:

$$|\psi_4\rangle = \frac{\alpha}{\sqrt{2}} * \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (|00\rangle + \left|10\right\rangle) + \frac{\beta}{\sqrt{2}} * \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|01\rangle + |10\rangle)$$

$$|\psi_4\rangle = \frac{\alpha}{2}(|0\rangle + |1\rangle) \otimes (\left|00\right\rangle + \left|10\right\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle) \otimes (|01\rangle + |10\rangle) \quad (17)$$

The third $3 * 3$ Peres gate as well compares with the previous Eq. (9a), (9b) and (9c).Applying a Hadamard gate to the second qubit to obtain quantum state $|\psi_1\rangle$ as

$$|\psi_1\rangle = \alpha|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \beta\left|1\right\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

$$|\psi_1\rangle = \frac{\alpha}{\sqrt{2}}(\left|000\right\rangle + \left|010\right\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (18)$$

Next apply the $3 * 3$ Peres gate from the second to third qubit refer to Eq. (19)

$$\left|\psi_2\right\rangle = \frac{\alpha}{\sqrt{2}}(\left|Peres|000\right\rangle) + Peres\left|010\right\rangle + \frac{\beta}{\sqrt{2}}(Peres|101\rangle) + Peres|110\rangle$$

Therefore;

$$|\psi_2\rangle = \frac{\alpha}{\sqrt{2}}(\left|001\right\rangle + \left|010\right\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (19)$$

If now we apply the Peres gate to $|\psi_2\rangle$ we generate the $|\psi_3\rangle$

$$|\psi_3\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle) \quad (20)$$

By applying the Hadamard gate to the first qubit, it produce $|\psi_4\rangle$ as:

$$\left|\psi_4\right\rangle = \frac{\alpha}{\sqrt{2}} * \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (|00\rangle + \left|10\right\rangle) + \frac{\beta}{\sqrt{2}} * \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|01\rangle + |10\rangle)$$

$$|\psi_4\rangle = \frac{\alpha}{2}(|0\rangle + |1\rangle) \otimes (\left|00\right\rangle + \left|10\right\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle) \otimes (|01\rangle + |10\rangle) \quad (21)$$

5. Results and Discussion

In this model, we describe that Alice want to communicate with Bob. At the beginning, an EPR

pair generated by EPR entanglement source. Secondly, one of the particles sent to Alice and other to the receiver Bob through quantum channel as shown in figure (2). Thirdly, transmission of information, Alice needs to measure the particles in the EPR entangled pairs and the pending bits holds. Then Alice informs Bob the results and finally, based on the results of Alice and the results measured from the EPR pair of himself, Bob can obtain information about the particles transmitted.

Let us reflect Alice has a system in state $|\psi_1\rangle$as applied to our expression and his Bob has a system in state $|\psi_1\rangle$, as depicted from our aforementioned expressions, then the state of their combined system is $|\psi_1\rangle \otimes |\psi_1\rangle$ .If Alice applying U to her state then its equivalent to applying the operator $U \otimes I$ to the combined state. The separable state refers as Eq. (22).

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle) \quad (22)$$

For the key distribution among the two parts as refer figure (2) using the polarized photons the Node A is the source node that has a random classic bit and produce the qubits states $|0\rangle$ and $|1\rangle$ and through logic gate which transmitting using the quantum teleportation. The Node B is the sink node that descript the message by measuring the incoming qubits either on $|0\rangle, |1\rangle$ or in basis states of $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Now, assume there is an eavesdrop intercepts the qubits transmitted from node A to node B by copy without measuring them and then re-transmit to node B and then wait for the basis to be announced. The node B when comparing with receiving bits it will bounced out the completely received bits because it is not the same with the shared keys from node$A$.

Thus, to ensure attack cannot intercept the communication we applying the no cloning theorem that state that a result of quantum mechanics which forbids the creation of identical copies of an arbitrary unknown quantum state. Quantum message as quantum information are travelling instantaneously seems to demonstrate by measuring the polarization of the two entangled photons.

According to Eq. (13), (17) and (21) respectively, they express the possible outcomes of measuring the first two qubits. The state of the third qubit transforms into one of the four states $\alpha|1\rangle + \beta|0\rangle,\ \alpha|0\rangle + \beta|1\rangle, \alpha|1\rangle - \beta|0\rangle and \alpha|0\rangle - \beta|1\rangle$ corresponding to the measurements of the first two qubits namely$|100\rangle, |101\rangle, |110\rangle and |111\rangle$. Thus, the receiver can change the state of the third qubit to $|\psi\rangle$ by applying the appropriate operations, according to the measurements of the first two qubits received from the sender. Finally, the quantum state is teleport from the sender to receiver.

We compare both Eq. (13) for Feynman and the proposed Eq. (17) and (21) for Toffoli and Peres logic gates respectively. Both generate the same output expression as Eq. (13). Thus, indicates more improvement from previous work for CNOT [28], however using the Toffoli and Peres logic gates ensure security for information transmission among the WSN.

6. Simulation Results

The simulation results using the Proteus 8 professional design indicates that both Toffoli and Peres logic gates produce the similar output as shown figure (3) and (4). The output for the Toffoli and Peres gate are $P = A,\ Q = B and R = AB \otimes C$ whereas for Peres are $P = A, Q = A \otimes B\ and\ R = AB \otimes C$ the only different between the two gate are on the output Q, which produce dissimilar output.

When the inputs for Peres logic gate changed to (1,1,1), then the output produced is (1,0,0) whereas for Toffoli logic gate produce (1,1,0) as shown figures (5) and (6) respectively. The different indicates their output different from their expression from the model mathematical that output Q for Peres is , $Q = A \otimes B$ and for Toffoli is $Q = B$

Comparing both Toffoli and Peres with the simulation output results as figure (3) and (4) indicates, the processing output produce the same results, which also indicates the same outputs as model Eq. (17) and (21) respectively.

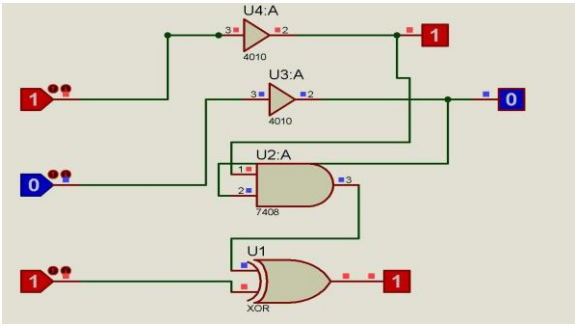

Fig. 3: Schematic representation of Toffoli Logic gates with three inputs (1, 0, 1) that generate three outputs (1, 0, 1)

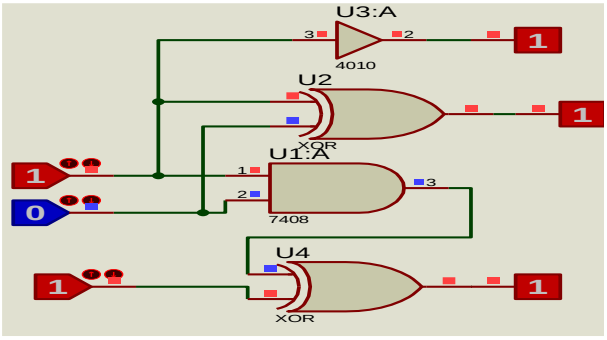

Fig. 4: Schematic representation of Peres Logic gates with three inputs (1, 0, 1) that generate three outputs (1, 1, 1)

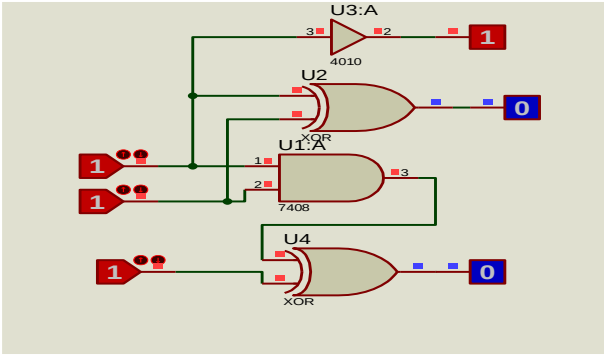

Fig.5: Peres gates output result when input is (1,1,1) produce (1,0,0)

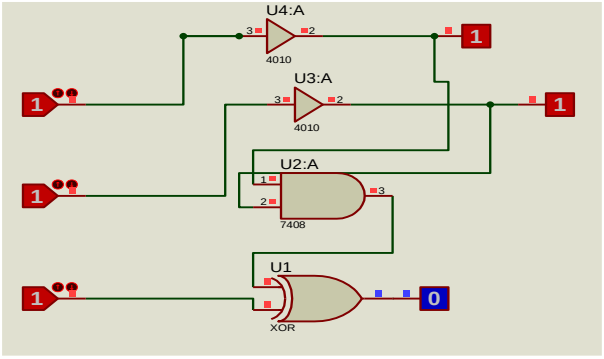

Fig.6: Toffoli gate output results when input is (1,1,1) produce (1,1,0)

7. Conclusion and Future Work

Based onto conventional WSN in today industrial, the quantum cryptography is the coming security for WSN. The Key distribution for encryption and description process for authentication is challenging problem in all-cryptographic algorithm for WSN but for this novelty approach provide healthier solution compare to traditional key distribution.

In this study, we have achieved the goal purpose for security in WSN using the quantum cryptography through the quantum teleportation deployment. We have seen that a secure communication of quantum data in a WSN can be achieved using quantum teleportation. The novelty application of using the reversible logic gate both Toffoli and Peres gates with quantum cryptography application have ensure suspicions for an eavesdropped from intercept the information through sensor network transmission.

The mathematical framework indicated that either the gates used in any stage they can generate the same output information. The simulation results indicates the same output comparing with the mathematical model expression.

For future study, this research suggests further studies on some other gates that ensure the low energy consumption and high security could be study for improvement security system in sensor network and a general ensure the safety to Internet of Things.

Acknowledgments

The author acknowledge the financial support received from China Scholarship Council (CSC) and Xidian University for their support and encouragement in carrying out this research work under supervision of Associate Prof. Lingling An from School of Computer Science and Technology, Xidian University.

References

[1] S. P. Singh and S. Sharma, “A survey on cluster based routing protocols in wireless sensor networks,” *Procedia computer science*, vol. 45, pp. 687–695, 2015.

[2] A. Yang, Y. Li, F. Kong, G. Wang, and E. Chen, “Security control redundancy allocation technology and security keys based on internet of things,” *IEEE Access*, vol. 6, pp. 50187–50196, 2018.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad hoc networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[4] M. Ozger, O. Cetinkaya, and O. B. Akan, “Energy harvesting cognitive radio networking for iot-enabled smart grid,” *Mobile Networks and Applications*, vol. 23, no. 4, pp. 956–966, 2018.

[5] I. T. Union, “The internet of things—executive summary,” *ITU Internet Reports*, 2005.

[6] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, “Protocols for self-organization of a wireless

sensor network," *IEEE personal communications*, vol. 7, no. 5, pp. 16–27, 2000.

[7] M. Indhumathi and S. Kavitha, "Distributed intrusion detection system for cognitive radio networks based on weighted fair queuing algorithm," 2018.

[8] A. A. Mugheri, M. A. Siddiqui, and M. Khoso, "Analysis on security methods of wireless sensor network (wsn)," *Sukkur IBA Journal of Computing and Mathematical Sciences*, vol. 2, no. 1, pp. 52–60, 2018.

[9] S. Henningsen, S. Dietzel, and B. Scheuermann, "Challenges of misbehavior detection in industrial wireless networks," in *Ad Hoc Networks*. Springer, 2018, pp. 37–46.

[10] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[11] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad hoc networks*, vol. 3, no. 3, pp. 325–349, 2005.

[12] C. Thota, R. Sundarasekar, G. Manogaran, R. Varatharajan, and M. Priyan, "Centralized fog computing security platform for iot and cloud in healthcare system," in *Exploring the convergence of big data and the internet of things*. IGI Global, 2018, pp. 141–154.

[13] M. Turkanovic and M. Hölbl, "The (in) adequacy of applicative use of quantum cryptography in wireless sensor networks,"′ *Quantum information processing*, vol. 13, no. 10, pp. 2255–2275, 2014.

[14] M. Y. Pandith, "Role of cryptography in wirelesses sensor: Future potential," *European Journal of Computer and Information technology*, June 2014.

[15] B. Jana, S. Singha, and S. Jana, "Key distribution in wireless sensor networks using quantum cryptography," *International Journal of Mobile & Adhoc Network|Vol 3|issue 4|November 2013*, 2013.

[16] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future internet and the security analysis," *Security and Communication Networks*, vol. 2018, 2018.

[17] M. Arun and S. Saravanan, "Reversible arithmetic logic gate (alg) for quantum computation," *International Journal of Intelligent Engineering and Systems*, vol. 6, no. 3, pp. 1–9, 2013.

[18] P. Botsinis, D. Alanis, Z. Babar, H. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, 2018.

[19] S. Mamataj, D. Saha, and N. Banu, "A review of reversible gates and its application in logic design," *American Journal of Engineering Research*, vol. 3, no. 4, pp. 151–161, 2014.

[20] P. R. Yelekar, S. S. Chiwande *et al.*, "Introduction to reversible logic gates & its application," in *2nd National Conference on Information and Communication Technology*, 2011, pp. 5–9.

[21] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," Computers & Electrical Engineering, vol. 66, pp. 274–287, 2018.

[22] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," Future Generation Computer Systems, vol. 78, pp. 956–963, 2018.

[23] P. Bhatia and R. Sumbaly, "Framework for wireless network security using quantum cryptography," arXiv preprint arXiv: 1412.2495, 2014.

[24] F. Hu, J. Ziobro, J. Tillett, and N. K. Sharma, "Secure wireless sensor networks: Problems and solutions," Rochester Institute of Technology, Rochester, New York, USA, 2004.

[25] N. Nagy, M. Nagy, and S. G. Akl, "Quantum security in wireless sensor networks," Natural Computing, vol. 9, no. 4, pp. 819–830, 2010.

[26] S. Suchat, W. Khunnam, and P. P. Yupapin, "Quantum key distribution via an optical wireless communication link for telephone networks," Optical Engineering, vol. 46, no. 10, p. 100502, 2007.

[27] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing." Theor. Comput. Sci., vol. 560, no. P1, pp. 7–11, 2014.

[28] J.-S. Li and C.-F. Yang, "Quantum communication in distributed wireless sensor networks," in Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on. IEEE, 2009, pp. 1024–1029.

[29] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek et al., "Free-space distribution of entanglement and single photons over 144 km," arXiv preprint quant-ph/0607182, 2006.

[30] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," Nature, vol. 390, no. 6660, p. 575, 1997.

Author Biography

Gaudence Stanslaus Tesha. He received proficiency in certificate level in Multimedia for Music Production from SAE College Bangkok Thailand in 2013.Full Technician certificate in Computer Engineering (FTC) from Dar Es Salaam Institute of Technology, Dar Es Salaam, Tanzania East Africa in 2003. He received Bachelor of Engineering (BEng) in Electronics and Telecommunication from Dar Es Salaam Institute of Technology, Dar Es Salaam, Tanzania East Africa in 2007. Master in Engineering (MEng), Electronics and Communication from Chongqing University, Chongqing, China in 2011. He is working with the Dar es Salaam Institute of Technology (DIT) in Tanzania as Assistant Lecturer. He is currently pursuing PhD with School of Telecommunications Engineering, Xidian University, Xi'an, China. His research interests include Communication Networks, Multimedia Security, Information Security and Wireless Sensor Network.