I.J. Wireless and Microwave Technologies, **2023, 4, 18-27**
Published Online on August 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.04.03

Enhancement of S13 Quantum Key Distribution Protocol by Employing Polarization, Secrete Key Disclosure and Non-repudiation

Bello A. Buhari*
Usmanu Danfodiyo University/Department of Computer Science, Sokoto, 234, Nigeria
E-mail: buhari.bello@udusok.edu.ng
ORCID iD: https://orcid.org//0000-0001-7333-1386
*Corresponding Author

Afolayan A. Obiniyi
Ahmadu Bello University /Department of Computer Science, Zaria, 234, Nigeria
E-mail: aaobiniyi@gmail.com

Sahalu B. Jubaidu and Armand F. Donfack Kana
Ahmadu Bello University /Department of Computer Science, Zaria, 234, Nigeria
E-mail: sahalu@abu.edu.ng, donfackkana@gmail.com

Received: 06 November, 2022; Revised: 18 December, 2022; Accepted: 03 March, 2023; Published: 08 August, 2023

Abstract: Quantum cryptography is the most convenient resolution for information security systems that presents an ultimate approach for key distribution. Today, the most viable key distribution resolutions for information security systems are those based on quantum cryptography. It is based on the quantum rules of physics rather than the assumed computational complexity of mathematical problems. But, the initial BB84 quantum key distribution protocol which is the raw key exchange of S13 quantum key distribution protocol has weakness of disclosure of large portion of secrete key or eavesdropping. Also, it cannot make use of most of the generated random bit. This paper enhanced S13 quantum key distribution protocol by employing polarization, secrete key disclosure and non-repudiation. The use of biometric or MAC address ensures non-repudiation. The row key exchange part of the S13 quantum key distribution which is the same as BB84 is enhanced by employing polarization techniques to make use of most of the generated random bit. Then, the tentative final key generated at the end of error estimation phase should be divided into blocks, padding, inverting the last bit of each block and XORing the block to generate a totally different key from the tentative one. Also, the random bits will be from biometric or serve MAC address respectively. The enhanced S13 quantum key is evaluated using cryptanalysis which shows that the enhanced protocol ensures disclosures of large portion of secrete key to prevent eavesdropping, utilization of most of the chosen binary strings to generate strong key and safeguarding against impersonation attack.

Index Terms: S13, Quantum Key Distribution, Quantum Cryptography, Polarization, XORing

1. Introduction

Web security relies on the computational complexity related with the generation of the secret key. This is not enough due to the fast growing approaches to calculate the secret key that cannot be cracked [1]. Public key cryptography was the first solution to key distribution problem. It is among the theoretically breakable computational security solutions because they rely on computationally challenging mathematical problems and assumptions about the computing capability of potential adversaries. As a result, they are in danger as computer power grows and new quantum computing algorithms are developed that can solve some commonly used, computationally demanding mathematical problems in polynomial time [2. 3]. Currently, the quantum cryptography is the most practical resolutions for information security systems that present the ultimate approaches for key distribution. It can allow the exchange of secret keys between users connected using a medium that is vulnerable to eavesdropping [4, 5].

The Quantum key distribution (QKD) security is ensured by the principle of quantum mechanics and the evolving maturity of QKD devices and technologies makes QKD start to becoming widely used [6].

To understand QKD first move away from the traditional key distribution approach of Haliru sending key information to Maryam. Instead, make use of a more private starting point, in which Haliru and Maryam originally create their own, secret independent random binary number sequences. These number sequences having many bits than they require for the key information they will ultimately share. They will usually do a bit-wise comparison of these sequences of binary numbers to identify a shared random subset that will be the key material. And in a situation that attackers are detected with high probability [7]. They use a quantum transmission over a quantum channel and a discus the results over a public channel [5].

It is necessary to appreciate that Haliru and Maryam do not need to identify all of their shared binary numbers or even specific ones; because the only requirements on the key information are that the numbers should be secret and random. QKD does not remove the need for other cryptographic primitives, such as authentication and access control, but it can be used to build systems with new security properties. But, the main challenge that limits its widespread implementation is the low availability and high cost of dedicated fiber equipments [8].

The initial BB84 quantum key distribution protocol which is the raw key exchange of S13 quantum key distribution has weakness of disclosure of large portion of secrete key or eavesdropping [9]. These possibilities expose that for each transmitted qubit, there is 75% probability that Eve's act goes unnoticed. Also, it cannot make use of most of the generated random bit. It can just utilize about 40%–50% of the generated bits [10].

This paper enhanced S13 quantum key distribution protocol by combining polarization, secrete key disclosure, biometric and MAC address to resolve the above mentioned problems. The row key exchange part of the S13 quantum key distribution is enhanced by employing polarization techniques to make use of most of the generated random bits. Then, the final key generated at the end of Error Estimation phase would be divided into blocks, padding, inverting the last bit of each block and XORing the block thereby generating a totally different key. Additionally, the random bits x_H by Haliru or Server in some cases and random seed string $x_1x_2...x_N$ by either Maryam or Haliru, or Maryam or Sever will be from biometric or serve MAC address respectively. The enhanced S13 quantum key is analyzed using cryptanalysis and the results of analysis shows that the enhanced protocol ensures disclosures of large portion of secrete key to prevent eavesdropping, utilization of most of the chosen binary strings to generate strong key and safeguarding against impersonation attack.

The contributions of this research are as follows:

1) Polarization, blocks and XORing is combined to eliminate the weakness of disclosure of large portion of secrete key and allow utilization of large portion of generated bits for key generation.
2) Biometric or serve MAC address is employed as the random seed of S13 quantum key distribution protocol to ensure security against impersonation attack.

The rest of this paper is organized as follows. Section two is review of related works, section three is discussion of BB84 quantum key distribution, section four is discussion of S13 quantum key distribution, section five is limitations of S13 quantum key distribution, section six is the enhances S13 quantum key distribution, section seven is evaluation of the enhanced S13 quantum key distribution and section eight is conclusion.

2. Related Works

Guskind and Krawec in [11] proposed a fresh mediated semi-quantum key distribution protocol. The former work is extended that provide great efficiency. This is a solution to key distribution problem. Their modification allows fully deployment of every quantum signals. There difference between their work and previous works is that raw key bits may be generated in respective of the server's message and can allows flip his raw key bit by Bob if the server transmit the message '2' or '3'. But if care is not taken on this flipping option, the correlation may be destroyed thereby creating more errors in the raw key.

Xu et al. in [11] introduced a device independent QKD protocol to solve key distribution problem with random post selection. In their scheme the extraction of secrete keys is only from the outcomes of post-selected subsets. This could not disclose the loopholes of detection as far as the post-selected entropy is evaluated from the entire data. But it has high errors even though it will not summon detection gaps. They proved their defense against collective attacks and also reduce the information cost of error correction has been illustrated as the result of the post selection. They therefore facilitate the improvement of loss tolerance.

Wang et al. in [13] studied quantum key distribution problem in respect of the construction of BB84 and proposed a new quantum key distribution scheme consisting of two steps. This is an enhancement of quantum key distribution protocol. Step one involving unidirectional channel 1 for quantum and step two involving classic bidirectional channel 2 for general information. It can be employed to improve the security of the key distribution scheme because every two cases give different test results. Theoretical analysis was carried out to express the advantage of the given QKD scheme.

Abdullah & Jassem in [10] established that the initial BB84 protocol random bit cannot consume most of the bits generated. Therefore, enhanced BB84 QKD protocol by making it to use the largest likely percentage of the generated bits as a secure key as an enhancement. It therefore guarantees a strong key for cryptography purposes. Both the BB84 and EBB84 are simulated using Java programming in order to compare their results. Results of comparison indicated that

EBB84 protocol is more secure but it takes little longer time than BB84 protocol.

Kumar et al. [14] attempt to enhance the security of QKD by increasing the size of the key shared between two parties. Even if attacker is successful in getting the initial authentication keys, the extracted keys from the both sphere of the proposed QKD scheme ensures unconquerable security. Their result shows that the proposed protocol is getting to 75% of efficiency.

Tannous & Langlois in [15] review a range of protocols from the simplest protocols like QC and BB84 to BBM92, DPSK, SARG04 and finally MDI. Also, those with largest possible communication distance and highest secret key bitrates are taken into consideration. They analyze the various phases and make basic presumption right to every protocol with the related result in each case. Their results show that the most responsive way to increase communication distance significantly is to decrease the Dark count rate (DCR).

Abdullah et al. in [16] proposed a new method of encoding a stream of bits into polarized photons using Legendre Symbol called MBB94. Here, both of the sender and the receiver agree by means of the function of Legendre symbol. They use only quantum channel and so the efficiency is high. .

Saha et al. in [9] enhanced BB84 Protocol by solving disclosure of large portion of secret key or attacker dipping problem which may perhaps not be detected. Therefore, the shared secret key will be strong enough to use in secret communication even if presence of attacker is not detected. Phases of the existing BB84 algorithm along with the customized one is described in detail with example and pseudo code. Due to extra operations performed including block division, padding, inverting of last bit of each block and XORing will add computational overhead to the enhanced scheme.

Trushechkin et al. in [17] consider a class of prepare-and-measure QKD protocols, utilizing additional pseudorandomness in the creation of quantum states. They merge classical pseudo randomness with quantum encoding of data and express that, for single-photon sources, the considered protocol gives better secret key rates than the BB84 and the asymmetric BB84 protocols. The proposed scheme enables averting of shifting operation but half of the key is lost.

Meslouhi et al. in [18] proposed a new protocol called "QKDPRB" based on random bases. It allows selection of infinite number of bases as an alternative of two bases. It involves use of standard encoding bases moving circularly with a variable rotational angle α which depends on angular velocity ω(t). This turns traditional bases into relative ones. They verified a universal security proof where they confirmed the minimum security level guaranteed by QKDPRB. They also confirmed that the proposed protocol is the same as a perfect random channel where attacker gained the lowest possible mutual information.

Esteban & Serna in [19] presents a quantum protocol using public- private key cryptography for transmission security enhanced data over a public channel. A different phenomenon to BB84 and many of its variants is that sender knows the key in advance to broadcast, the qubits are exchanged in only one side and classical information is transmitted afterward. Their communication remains quantum in each stage. It is secure against man-in-the-midle attack because it does not use classical channel. This protocol is harder to implement because the qubits is transmitted multiple times.

Ahonen et al. in [20] proposed and investigate a quantum key distribution protocol based on sending entangled N-qubit states as an alternative to single-qubit ones as in the trail-blazing scheme by BB84. Their outcomes show that entanglement can be applied to significantly enhance the BB84-type key distribution, even in the case of two-qubit entanglement. This protocol can be straightforwardly adapted to the several variants of the BB84 scheme. Regrettably, loss of qubits may create a problem not only for attacker, but also for legitimate user. This protocol cannot be suggested for use at extreme distances where most transmitted qubits are lost because if one of the entangled qubits is totally lost, the quantum bit error rate (QBER) of the remaining qubits is likely to increase.

Wu & Wu in [21] enhanced QKD protocol based on the basic principle of QKD to lift up the utilization ratio of photons and security. The dissimilarity between this improved protocol and the 3 popular protocols is that the sender and receiver is the same person. The authentication process of the proposed protocol is secure against middle-man attack efficiently. The security is improved because the messages are transferred only in quanta channel.

3. BB84 Quantum Key Distribution (QKD) Protocol

Bennett and Brassard proposed BB84 in 1984 [22]. It was the first employment of quantum physics in information and communication theory that initiate the explosive study of quantum communication and cryptography.

The BB84 protocol proceeds as follow [23]:

1) Haliru produce two strings $x_H = x_{H1}x_{H2}...x_{HN}$ and $y_H = y_{H1}y_{H2}...y_{HN}$ of random classical bits.
2) Haliru make use of x_H and y_H to form a quantum state as a tensor product of N qubits.

$$|\psi\rangle = \otimes_{k=1}^{n} |\psi_{x_{HK}y_{HK}}\rangle, \tag{1}$$

where $\psi_{x_k y_k}$ depends on the values of x_{Hk} and y_{Hk}

$$|\psi_{00}\rangle = |0\rangle, \tag{2}$$

$$|\psi_{10}\rangle = |1\rangle, \tag{3}$$

$$|\psi_{01}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{4}$$

$$|\psi_{11}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{5}$$

Really, the string y_H is used to choose between the bases of the operators $Z(\{|0\rangle,|1\rangle\})$ and $X(\{|+\rangle,|-\rangle\})$, and the string x_H is used to attach the distinct qubit in the basis.

3) Haliru transmits the sequence of qubits to Maryam through the quantum channel.
4) Maryam accepts the qubits and perfoems measurement on the qubits using either the basis X or Z for each qubit according to a randomly generated sequence y_M. The measurement x_M results in a bit value 0 (1) if the measurement correlate with the positive (negative) eigenvalue of X or Z. Maryam then make public that she received the qubits through the public classical channel.
5) If Maryam's measurement basis is the same as Haliru's preparation basis, Maryam's measured bit value in x_M will be the same as Haliru's bit value in x_H. If the bases are different because the basis sets X and Z are mutually unbiased then Maryam's resulting measured bit value will have a probability of 0.5 being correct. Haliru makes public the string y_H in the classical channel to decide whether they use the same set of bases.
6) Haliru and Maryam debate through the classical channel to discard those bits in x_H and x_M that the preparation basis by Haliru and the measurement basis by Maryam are not the same..
7) For every remaining bits in x_H (called the sifted key $x_H^{'}$), Haliru's preparation basis and Maryam's measurement basis are the same. If no errors are experience in the qubits during the transmission in the quantum channel, Maryam's measured states for those qubits should give rise to bit values $x_M^{'}$ matching the bits in $x_H^{'}$, i.e., $x_H^{'} \,{}^1\!/_4\, x_M^{'}$. However, it is very likely that errors experienced in the qubits during the transmission. Haliru thus selects a subset of $x_H^{'}$ and tells Maryam which bits are selected through the classical channel.
8) Haliru and Maryam check the values of the selected bits through the classical channel. If the quantum bit error rate (QBER) r in those bits is higher than a threshold, the protocol is terminated. If not, they proceed to the next step. The threshold is aborted by the security analysis that makes sure privacy amplification can be carried out.
9) Haliru and Maryam carry out error correction and privacy amplification through the classical channel

4. S13 Quantum Key Distribution Protocol

S13 [24] protocol is a new quantum protocol. It is actually identical to the BB84 protocol for all the quantum manipulation. The only difference is that it uses private reconciliation from a random seed and asymmetric cryptography, and it can be implemented in the existing devices without modification [25]. As such, it allows the generation of larger secure keys.

So, Haliru and Maryam exchange a set of encoded photons according to four states $|0\rangle,|1\rangle,|+\rangle,|-\rangle$, which convene establishing two basis with orthogonal states $\beta_0 = \{|0\rangle,|1\rangle\}$ and $\beta_1 = \{|+\rangle,|-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Coding the binary value 0 to the states $|0\rangle$ and $|+\rangle$, and the binary value 1 to the states $|1\rangle$ and $|-\rangle$. Which is denoted by $\psi_{00} \equiv |0\rangle$, $\psi_{01} \equiv |1\rangle$, $\psi_{10} \equiv |+\rangle$ and $\psi_{11} \equiv |-\rangle$ for simplicity.

The protocol consists of such activities [24] as raw key exchange, random seed, missing key exchange, asymmetric cryptography and private reconciliation

4.1 Row Key Exchange

The raw key exchange is the same as BB84.

4.2 Random Seed

1) Haliru or Maryam publishes a random binary string $w_1 w_2 ... w_N$.

4.3 Missing Key Exchange

1) Haliru sums $x_{Hk} \oplus w_k$, k = 1,2,3,…,N. Getting a sequence of binary basis $t_1 t_2 ... t_N$ and generates other random string of binary values $j_1 j_2 ... j_N$ that will match to other key that he wants to exchange with Maryam. Haliru gets the coupled state $|\psi_{t_k j_k}\rangle$ and sends it to Maryam through a quantum channel from the elements k that is occupying a concrete position of the preceding strings
2) Maryam sums $(1 \oplus x_{Mk}) \oplus w_k$, k = 1,2,…N. Getting the string of binary basis $n_1 n_2 ... n_N$ and measures each received state $|\psi_{t_k j_k}\rangle$ with the matching base β_{n_k} generating the string $b_1 b_2 ... b_N$.

4.4 Asymmetric Cryptography

Haliru and Maryam interchange a set of binary strings and apply in different binary arrangements the function f defined as follows:

$$f(x, y, z) := \begin{cases} x, z=0 \\ y, z=1 \end{cases} \tag{6}$$

1) Haliru sums $t_k \oplus j_k$, k = 1,2,…,N. Getting the binary string $y_{H1} y_{H2} ... y_{HN}$ that sends to Maryam.

2) Maryam encrypt x_{Mk} in u_k and v_k with

$$u_k = n_k \oplus f(x_{Mk}, a_k, b_k \oplus y_k), \tag{7}$$

$$v_k = n_k \oplus f(x_{Mk}, b_k, a_k \oplus y_k) \tag{8}$$

K = 1,2,…N. Getting the public string $u_1 u_2 ... u_N$ y $v_1 v_2 ... v_N$ that it sends to Haliru.

3) Haliru sums $t_k \oplus f(x_{Hk}, (1 \oplus y_{Hk}) \oplus u_k, j_k \oplus v_k)$

Decrypting m_k for k = 1,2…N. getting the private string $x_{M1} x_{M2} ... x_{MN}$ of Maryam.

4.5 Private Reconciliation

1) Haliru contrast the strings $x_{H1} x_{H2} ... x_{HN}$ and $x_{M1} x_{M2} ... x_{MN}$, sending to Maryam the binary sequence $l_1 l_2 ... l_N$ with

$$l_k = x_{Hk} \oplus x_{Mk} \tag{9}$$

2) Maryam sums $x_{Mk} \oplus l_k$, k = 1, 2, ...,N. getting the private string $x_{H1} x_{H2} ... x_{HN}$ of Haliru and apply:

$$f(l_k, a_k, b_k \oplus y_k) \equiv i_k \tag{10}$$

$$f(l_k, a_k, y_k \oplus b_k) \equiv j_k \tag{11}$$

k.= 1,2,3,…N getting the private strings of Haliru $y_{H1} y_{H2} ... y_{HN}$, y $j1 j2 ... jN$

5. Limitations of S13 Quantum Key Distribution

This section highlights the limitations of S13 quantum key distribution. These include disclosures of large portion of secrete key or eavesdropping, non utilization of most of the generated bits and impersonation attack. These limitations are discussed in the following sub-sections of this section.

5.1 Disclosures of large portion of secrete key or eavesdropping and non utilization of most of the generated bits.

The initial BB84 quantum key distribution protocol has weakness of disclosure of large portion of secrete key or eavesdropping [9]. The key can be derived with the presence of an eavesdropper Eve as follows [26]:

1) Eve chooses the wrong basis: $x_E = \overline{x}_H \rightarrow$ qubit is distorted
2) Maryam chooses correctly: $x_M = x_H \rightarrow$ Eve introduces 50% error probability
3) Maryam chooses incorrectly: $x_M = \overline{x}_H \rightarrow$ random result, Eve is not detected.
4) Eve chooses the correct basis: $x_E = x_A \rightarrow$ qubit is not distorted.

5) Maryam chooses correctly: $x_M = x_H \rightarrow$ Eve is unnoticed and has one bit of the key.

6) Maryam chooses incorrectly: $x_M = \overline{x}_H \rightarrow$ random result, Eve is not detected.

These possibilities expose that for each transmitted qubit, there is 75% probability that Eve's act goes unnoticed.

Also, BB84 protocol cannot make use of most of the generated random bit. It can just utilize about 40%–50% of the generated bits [10] .

5.2 Impersonation attack

An impersonation attack is an attack in which an attacker successfully assumes the identity of one of the legal users in a system or in a communications protocol. As seen earlier attacker Eve can chooses the wrong basis: $x_E = \overline{x}_H \rightarrow$ thereby distorting the qubit and making attacker unnoticed. So, the attacker can impersonate Haliru such that Maryam will see the attacker as Haliru.

Also, if the random binary string $x_1x_2...x_N$ published by either Haliru or Maryam during random seed stage of S13 protocol is stolen by Eve, Maryam or Haliru can impersonated.key from the tentative one. Also, the random bits x_H by Haliru or Server in some cases and random seed string $x_1x_2...x_N$ by either Maryam or Haliru, or Maryam or Sever will be from biometric or serve MAC address respectively.

6. Enhanced S13 Quantum Key Distribution

In this section, we enhance the S13 quantum key distribution. The row key exchange part of the S13 quantum key distribution which is the same as BB84 is enhanced by employing polarization techniques to make use of most of the generated random bit and add an extra phase of security in order to enable generation of secure key. The extra phases of security are division of the final key into blocks, padding, inverting the last bit of each block and XORing the block to generate a totally different key from the tentative one. Also, the random bits x_H by Haliru or Server in some cases and random seed string $x_1x_2...x_N$ by either Maryam or Haliru, or Maryam or Sever will be from biometric or serve MAC address respectively.

6.1 Enhanced S13 Quantum Key Distribution Steps

The enhanced S13 quantum key distribution also consists of five (5) steps namely: row key exchange, random seed, missing key exchange, asymmetric cryptography and private reconciliation. These are discussed as follows:

1) Raw Key Exchange

Raw key exchange which is initially BB84 is enhanced by employing polarization techniques to make use of most of the generated random bit and add an extra phase of security in order to enable generation of secure key and one of the random seed of Haliru or Maryam will be from their biometric and that of Server in some cases will be from Server MAC address. This can be express as follows:

a. Haliru chooses random n-bits string $S_{Hi} = s_{H1}s_{H2} ... s_{Hn}$ and polarization of the i-th bit $p^i = p^1p^2...p^n$.

b. Haliru creates and generates the corresponding photons into one of four states as following $|\psi_{Hi}, P^i\rangle$ related to the bit information of B_H and polarize P^i where $1 \le i \le n$.

c. If $S_{Hi} = 0$ $S_{Hi} = 0$, then P^i is encoded to diagonal basis and if $S_{Hi} = 1$, then P^i is encoded rectilinear basis based on the encoding process as follows:

$$|\psi_0, +\rangle = \nearrow = |+\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + |1\rangle\right) \tag{12}$$

$$|\psi_0, -\rangle = \nwarrow = |-\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - |1\rangle\right) \tag{13}$$

$$|\psi_1, +\rangle = \rightarrow = |0\rangle = \left(\frac{1}{\sqrt{2}}|+\rangle + |-\rangle\right) \tag{14}$$

$$|\psi_1, -\rangle = \uparrow = |1\rangle = \left(\frac{1}{\sqrt{2}}|+\rangle - |-\rangle\right) \tag{15}$$

d. Then, Haliru transmits photons to Maryam in sequence over a quantum channel.
e. On the other receiving the photons side, Maryam polarization are $p^i = p^1 p^2 ... p^n$ for $1 \le i \le n$. If $P^i = |+\rangle$ or $P^i = |-\rangle$ then $S_{Mi} = 0$, if $P^i = |0\rangle$ or $P^i = |1\rangle$ then $S_{Mi} = 1$.
f. Then the n-bit string for Maryam is $S_{Mi} = S_{M1} S_{M2} ... S_{Mn}$, which is the final key
g. Haliru and Maryam both must have to agree with a number of bits in each block 'n' because the n-bit must be divided into blocks. If the key is not completely divisible by 'n' then Padding is required for equally division of blocks.
h. If the last bit is 0, then change that to 1 and if it is 1 then changed that to 0. That is, inverted. This will further confuse the attacker.
i. Now keep the first block remain same. Then XOR the next block with the first block and store the result. After that, XOR the next block with the result of the previous block and store the result. This process will continue up to the last block.
j. Final key will be generated by sequentially puting each block where the result of XORing is stored from the first one

2) Random Seed

a. Haliru or Maryam provide a binary string from their biometric $b_{Hi} = b_{H1} b_{H2} ... b_{Hn}$ and $b_{Mi} = b_{M1} b_{M2} ... b_{Mn}$ respectively. Or if the communication is with the server, a binary string from server MAC address $mc_i = mc_1 mc_2 ... mc_n$.

3) Missing Key Exchange

a. Haliru sums $s_{Hk} \oplus b_{Hk}$, $k = 1, 2, ... n$. Obtaining a sequence of binary basis $t_1 t_2 ... t_n$. Haliru generates the corresponding photons into one of four states as following $|\psi_{ti}, P_H^i\rangle$ related to the bit information of t_i and polarize P_H^i where $1 \le i \le n$ using equations (12) to (15) and sends it to Maryam through a quantum channel.
b. Maryam sums $(1 \oplus s_{mk}) \oplus b_{Mk}$, $k = 1, 2, ... n$. Obtaining the string of binary basis $n_1 n_2 ... n_N$ and then decode the received photons. That is, If $P_H^i = |+\rangle$ or $P_H^i = |-\rangle$ then $S_{Mi} = 0$, if $P_H^i = |0\rangle$ or $P_H^i = |1\rangle$ then $S_{Mi} = 1$ generating the string $m_1 m_2 ... m_n$.

4) Asymmetric Cryptography

Haliru and Maryam exchange a set of binary strings and apply in different binary arrangements the function f defined as follows:

$$f(x, y, z) := \begin{cases} x, z=0 \\ y, z=1 \end{cases} \tag{16}$$

a. Haliru sums $S_{Hk} \oplus t_k$ $s_{Hk} \oplus t_k$, $k = 1, 2, ... N$. Obtaining the binary string $y_1 y_2 ... y_N$ that sends to Maryam.
b. Maryam encrypt s_{Mk} in u_k and v_k with

$$u_k = n_k \oplus f(s_{Mk}, n_k, m_k, \oplus y_k), \tag{17}$$

$$v_k = n_k \oplus f(s_{Mk}, m_k, n_k, \oplus y_k) \tag{18}$$

Where

$$n_k = 1 \oplus b_{Mk} \oplus s_{Mk} \tag{19}$$

$k = 1, 2, ... N$. Obtaining the public string $u_1 u_2 ... u_N v_i v_2 ... v_N$ that sends to Haliru.

c. Haliru sums $t_k \oplus f(s_{Hk}, (1 \oplus i_k) \oplus u_k, j_k, v_k)$

$$i_k = s_{Hk} \oplus s_{Mk} \tag{20}$$

Decrypting s_{Mk} for $k = 1, 2, ... N$ obtaining the private string $s_{M1} s_{m2} ... s_{mN}$ of Maryam.

5) Private Reconciliation

a. Haliru compares the strings $s_{H1}s_{H2}...s_{HN}$ and $s_{M1}s_{M2}...s_{MN}$, sending to Maryam the binary sequence $l_1 l_2 ... l_N$ with

$$l_k = s_{Hk} \oplus s_{Mk} \tag{21}$$

b. Maryam sums $s_{Mk} \oplus l_k$, k = 1, 2, ...,N. Obtaining the private string $s_{H1}s_{H2}...s_{HN}$ of Haliru and apply:

$$f(l_k, n_k, m_k \oplus y_k) \equiv s_{Hk} \tag{22}$$

$$f(l_k, n_k, y_k \oplus m_k) \equiv t_k \tag{23}$$

$k = 1, 2, ...N$. Obtaining the private strings of Haliru $s_{H1}\ s_{H2}\ ...\ s_{HN}$

7. Evaluation of the Enhanced S13 Quantum Key Distribution

In this section, we evaluate the security of the enhanced S13 key distribution protocol using cryptanalysis. The security of the enhanced protocol is based on disclosures of large portion of secrete key to prevent eavesdropping, utilization of most of the chosen binary strings to generate strong key and safeguarding against impersonation attack.

7.1 Utilization of Most of the Chosen Binary Strings to Generate Strong Key

The size of the key is one of the most important factor for determining the strength of a key. Sharing of secret key between Haliru and Maryam without using classical channel will ensure utilization of most of the key generation information. This work employs polarization technique unlike in the BB84 QKD protocol. In the enhanced protocol, Haliru creates and generates the corresponding photons into one of four states as following $|\psi_{Hi,}P^i\rangle$ related to the bit information of B_H and polarize P^i where $1 \le i \le n$, encode and sends the corresponding bits to Maryam via quantum channel. On the other receiving the photons side, Maryam polarization are $p^i = p^1 p^2 ... p^n$ for $1 \le i \le n$. If $p^i = |+\rangle$ or $p^i = |-\rangle$ then $S_{Mi} = 0$, if $p^i = |0\rangle$ or $p^i = |1\rangle$ then $S_{Mi} = 1$. This is the key to be shared by them.

7.2 Disclosure of Large Portion of Secret Key

This is ensured by providing some phase of securities after error estimation of raw key exchange of the S13 quantum key distribution protocol which are not previously available in the S13 QKD protocol. In the enhanced protocol, the tentative final key generated at the end of error estimation phase should be divided into blocks. So, Haliru and Maryam must have to agree with ‘n’ number of bits in each block. If the tentative final key is not completely divisible by ‘n’, then Padding is required for dividing the blocks equally. The last bit of each block is inverted followed by XORing. Here, the first block is remain the same, then XORing the next block with first block, the XORing the next block with the first result up to the last bock. These will result in disclosure of large portion of the secrete key.

7.3 Security against Impersonation Attack

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol. Here, the random bits $b_{H1}b_{H2}...b_{Hn}$ by Haliru or $mc_1 mc_2 ... mc_n$ by Server in some cases or random seed string $b_{M1}b_{M2}...b_{Mn}$ by Maryam will be from biometric or serve MAC address respectively. These are hard to copy and share, cannot be forgotten or easily guessed and is hard to forge or distribute. This also ensures non-repudiation unlike in S13 quantum which used binary numbers as the random bits.

8. Conclusion

Information security depends on the computational complexity involves in generating the secret key which is not enough as the fast growing methods to calculate the secret key that cannot be compromise. The initial method for resolving the key distribution issue was public key cryptography. Because they rely on computationally difficult mathematical issues and presumptions about the processing power of prospective adversaries, it is one of the theoretically breakable computational security methods. They consequently face risk as computing power increases and fresh quantum computing techniques are created that can quickly solve some widely utilized, computationally challenging mathematical problems. The most realistic solutions for information security systems right now that offer the best key distribution strategies are provided by quantum cryptography. It may enable users connecting over a channel that is susceptible to eavesdropping to exchange secret keys. Currently, the quantum cryptography is the most practical solution for information security systems, which presents the ultimate method for key distribution. The initial BB84 quantum key distribution protocol which is the raw key exchange of S13 quantum key distribution has weakness of disclosure of large portion of secrete key or eavesdropping. These possibilities expose that for each transmitted qubit, there is 75% probability that Eve's act goes unnoticed. Also, it cannot make use of most of the generated random bit. It can just utilize about 40%–50% of the generated bits. This paper enhanced S13 quantum key distribution protocol by combining polarization, blocks and XORings with biometric and MAC address to resolve the problems mentioned above. The row key exchange part of the S13 quantum key distribution which is the same as BB84 is enhanced by employing polarization techniques to make use of most of the generated random bit. Then, the tentative final key generated at the end of Error Estimation phase should be divided into blocks, padding, inverting the last bit of each block and XORing the block to generate a totally different key from the tentative one. Also, the random bits x_H by Haliru or Server in some cases and random seed string $x_1x_2 ... x_N$ by either Maryam or Haliru, or Maryam or Sever will be from biometric or serve MAC address respectively. The enhanced S13 quantum key is analyzed using cryptanalysis. And the results of the analysis shows that the enhanced protocol ensures disclosures of large portion of secrete key to prevent eavesdropping, utilization of most of the chosen binary strings to generate strong key and safeguarding against impersonation attack.

References

[1] Buhari, B. A., Obiniyi, A. A., Junaidu, S. B., & Roko, A. (2020). Elgamal Cryptographic Scheme based on Quantum Key Distribution (QKD). IAR Journal of Engineering and Technology, 1(4).

[2] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee.

[3] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505-510.

[4] Roumestan, F., Ghazisaeidi, A., Renaudier, J., Vidarte, L. T., Leverrier, A., Diamanti, E., & Grangier, P. (2022). Experimental Demonstration of Discrete Modulation Formats for Continuous Variable Quantum Key Distribution. *arXiv preprint arXiv:2207.11702*.

[5] Abbas, S. A., & Al-Shareefi, N. A. (2022). Secure quantum key distribution system by applying decoy states protocol. *Telkomnika*, *20*(4).

[6] Ren, S., Wang, Y., & Su, X. (2022). Hybrid quantum key distribution network. *Science China Information Sciences*, *65*(10), 1-7.

[7] Christensen, R. B., & Popovski, P. (2022). Private Randomness Agreement and its Application in Quantum Key Distribution Networks. *arXiv preprint arXiv:2210.05408*.

[8] Cao, Y., Zhao, Y., Zhang, J., & Wang, Q. (2022). Demonstration of SDN-Based Heterogeneous Quantum Key Distribution Chain Orchestration over Optical Networks. *arXiv preprint arXiv:2209.09528*.

[9] Saha, K., Ghosh, S. S., & Shaw, D. K. (2018). QUANTUM KEY DISTRIBUTION SCHEME: AN IMPROVEMENT BASED ON BB84 PROTOCOL. International Journal of Advanced Research in Computer Science, 9(2).

[10] Abdullah, A. A., & Jassem, Y. H. (2019). Enhancement of quantum key distribution protocol BB84. Journal of Computational and Theoretical Nanoscience, 16(3), 1138-1154.

[11] Guskind, J., & Krawec, W. O. (2022). Mediated semi-quantum key distribution with improved efficiency. *Quantum Science and Technology*, *7*(3), 035019.

[12] Xu, F., Zhang, Y. Z., Zhang, Q., & Pan, J. W. (2022). Device-Independent Quantum Key Distribution with Random Postselection. *Physical Review Letters*, *128*(11), 110506.

[13] Wang, B., Zhang, B. F., Zou, F. C., & Xia, Y. (2021). A kind of improved quantum key distribution scheme. Optik, 235, 166628.

[14] Kumar, A., Dadheech, P., Singh, V., Poonia, R. C., & Raja, L. (2019). An improved quantum key distribution protocol for verification. Journal of Discrete Mathematical Sciences and Cryptography, 22(4), 491-498.

[15] Tannous, C., & Langlois, J. (2019). Quantum Key Distribution Protocol Optimization. Annalen der Physik, 531(4), 1800334.

[16] Abdullah, A. A., Khalaf, R. Z., & Habib, H. B. (2019, March). Modified BB84 quantum key distribution protocol using legendre symbol. In 2019 2nd Scientific Conference of Computer Sciences (SCCS) (pp. 154-157). IEEE

[17] Trushechkin, A. S., Tregubov, P. A., Kiktenko, E. O., Kurochkin, Y. V., & Fedorov, A. K. (2018). Quantum-key-distribution protocol with pseudorandom bases. Physical Review A, 97(1), 012311.

[18] Meslouhi, A., Amellal, H., Hassouni, Y., El Baz, M., & El Allati, A. (2016). Quantum key distribution protocol using random bases. International Journal of Modern Physics B, 30(10), 1650061.

[19] Esteban, E., & Serna, H. (2012). Quantum Key Distribution protocol with private-public key. arXiv preprint arXiv:0908.2146.

[20] Ahonen, O., Möttönen, M., & O'Brien, J. L. (2008). Entanglement-enhanced quantum key distribution. Physical Review A, 78(3), 032314.

[21] Wu, T. W., & Wu, G. H. (2008, September). An improved quantum key distribution protocol. In Optics and Photonics for Information Processing II (Vol. 7072, p. 707214). International Society for Optics and Photonics.

[22] Bennett, C. H., & Brassard, G. (1984, December). Quantum cryptography. In Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (pp. 175-179).

[23] Verma, P. K., El Rifai, M., & Chan, K. W. C. (2018). Quantum Key Distribution. Signals and Communication Technology, 59–84. doi:10.1007/978-981-10-8618-2_3

[24] Serna, E. H. (2013). Quantum key distribution from a random seed. *arXiv preprint arXiv:1311.1582*.

[25] Singh, H., Gupta, D. L., & Singh, A. K. (2014). Quantum key distribution protocols: a review. Journal of Computer Engineering, 16(2), 1-9.

[26] Mina, M. Z., & Simion, E. (2020, November). A Scalable Simulation of the BB84 Protocol Involving Eavesdropping. In International Conference on Information Technology and Communications Security (pp. 91-109). Springer, Cham.

Authors' Profiles

Bello Alhaji Buhari, Obtained B.Sc. in Computer Science at Usmanu Danfodiyo UniversitySokoto – Nigeria and M.Sc. in Computer Science at Ahmadu Bello University Zaria –Nigeria. He is now pursuing Ph.D. in Computer Science at Ahmadu Bello University Zaria – Nigeria. He is a Lecture in the Department of Computer Science, Usmanu Danfodiyo University Sokoto – Nigeria since 2004. His research interest include: Web Security and Cryptography.

Prof. A.A. Obiniyi received his Ph.D degree in Computer Science from Ahmadu Bello University (ABU), Zaria in Kaduna State of Nigeria in 2009. He is a Professor of Computer Science and a member of Nigeria Computer Society (NCS), Internet Society (ISOC), Academia in Information Technology Professionals (AITP), Institute of Electrical and Electronic Engineers (IEEE) and a Chartered member of Computer Professionals (Registration Council of Nigeria)[CPN]. He lectures in the Department of Computer Science of Ahmadu Bello University, Zaria – Kaduna State. Presently, he is co-supervising eight Ph. D. and thirteen Master of Computer Science students with many Ph.D. and Master of Computer Science scholars completed their studies. He also has many publications to his credit. His research interests include Computer Networking, Cyber Security and Database Development among others.

Prof. Sahalu B. Junaidu is a Professor at the Ahmadu Bello University, Zaria Kaduna State Nigeria. He is a Life Member of Association of Computing Machinery (ACM); Member, Institute of Electrical and Electronic Engineers (IEEE); Member, Computer Professionals (Registration Council) of Nigeria; Member, Nigerian Computer Society. He is the Pioneer Head of Department, Department of Computer Science, Ahmadu Bello University Zaria since 2016.

Dr. Armand F. Donfack Kana received his B.Sc. degree in computer science from the University of Ilorin, Nigeria, M.Sc. and Ph.D. degrees in computer science from the University of Ibadan, Nigeria. He is currently a READER at the Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria. His research interests include Knowledge Representation and Reasoning, Machine Leaming, Formal Ontologies and Soft Computing.

How to cite this paper: Bello A. Buhari, Afolayan A. Obiniyi, Sahalu B. Jubaidu, Armand F. Donfack Kana, "Enhancement of S13 Quantum Key Distribution Protocol by Employing Polarization, Secrete Key Disclosure and Non-repudiation ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.4, pp. 18-27, 2023. DOI:10.5815/ijwmt.2023.04.03