Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Binary Phase Shift Key And Block Reordering Framework To Avoid Side-Channel Attacks And Multiphoton Attacks In Quantum Key Distribution

S.Prayla Shyry[1], Walter Priesnitz Filho[2], Maria Emilia Camargo[3], Mithileysh Sathiyanarayanan[4]

[1] Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India.
[2,3] Universidade Federal de Santa Maria, Brazil, 4 MIT Square, London
praylashyry.cse@sathyabama.ac.in

Technology development in recent days has achieved a greater level in terms of many industries and network applications. In those, network security has important factor in maintaining the data to be transmitted securely. For this process of data transfer, cryptography has a significant role in algorithms for maintaining the data secured using complex computations. RSA algorithms are used to encrypt data

using the enhanced bit insertion to protect RSA from various attacks. Quantum Key Distribution is one of the advanced methods for key transmission. Nowadays, in all practical implementations of quantum, Photonic systems are applied. Quantum states are encoded by photon pulses provided by Alice and those states are measured and selected. Actually it is very hard to discriminate the amount of photons and it is used by Bob for mathematical calculations. With these Bob get the knowledge of the real pulses obtained after the acceptable loss and flaws. The multiphoton pulses are tracked and it is broadcasted, Bobs calculation choices are measured and the breaching of security protocol is mitigated. Hence we develop a new framework to avoid and analyze the multiphoton attacks. The proposed framework Binary Phase Shift Key and block reordering (BPSK-BRO) Framework removes the side channel attacks in QKD and provides more than 99.9% of security in QKD. In the Future, photons can be manipulated using nanoscale devices like waveguides and beam splitters for quantum computing applications including quantum entanglement and communication. Also superconducting nanomaterials can behave quantum at higher temperatures and so the complex circuits required for these qubits can only be built via nanofabrication techniques.

Keywords: Security, Encryption, decryption, Qubits and Quantum Key Distribution.

1. Introduction

Security is the most challenging area in the communication over the internet. The most crucial part of communication is data tampering, data modification and data loss and methodologies must be employed to ensure the integrity and confidentiality of data. Now the advancements in internet has geared the data transfer, mutually transfer data with new communication device. Data is the most important factor in the financial, government and private sectors. Usually the original data is gained access and modified by the hackers during the transit period. To avoid this situation, standard encryption techniques are developed and employed. Traditionally data is encrypted with standard secret key either through private or public key cryptography. The receiver decrypts the transit data with the

sender's private key to ensure authentication. The data is transmitted with the help of sender's public key to ensure the confidentiality [3]. In those traditional techniques both the data and the key are transmitted through the same channel. [4][5]. As the data and key are transmitted in same channel, there is a high risk of unauthorized accesss. So It is better to employ quantum key distribution with modern techniques.

Quantum cryptography satisfies the polarization technique and the Heisenberg's uncertainty principle. Quantum cryptography is based on fundamental physics concepts like Heisenberg's Uncertainty Principle and Photon Polarization Technique. According to Heisenberg, Measuring the variable of a particle has some inherent certainty and if the eavesdropper tries to monitor and gain the qubits, it is not possible to duplicate it. So focus is to be given to distribute the quantum key with novel methods to ensure the security of the qubits.

The no cloning theorem asserts that a quantum bit cannot be duplicated or reproduced, and the Heisenberg uncertainty theory claims that it is impossible to measure a particle's initial state without upsetting it. In order to strengthen the security of the secret key, both the post quantum QKD and the standard EPR protocols are used. Using any of the existing encryption algorithms, such as AES and DES, the given data is first encrypted in QKD methods. After that, we have two sorts of information encrypted data and encryption key, both of which are binary data.

In conventional data transmission systems (classical channel), both encrypted data and key are transmitted over the same channel. Although the data is encrypted using conventional techniques,eavesdroppers and other outside parties can easily access it utilizing cutting-edge systems and algorithms. The fact that the encryption key and encrypted data are transmitted over the same channel is another drawback of the current approach. Because both are present on the same channel, a hacker has multiple opportunities to obtain data. These problems were

addressed by developing the BB84 protocol. Following the encryption process, the encrypted data and encryption key are transmitted using two channels: the normal channel and the quantum channel.The encryption key is sent through a quantum channel, while the encrypted data is sent over a traditional channel. If the listener attempts to gather information from the main channel that the receiver can recognize, there is a problem. The receiver might fail to detect the eavesdropper if heattempts to obtain the q-bit from the side channel, which would allow him to approve the delivery encrypted data. In the QKD systems, the main challenging area is the side channel attacks. [16]. As both sender and receiver are communicating in the same quantum channel, it is the need of the hour to develop novel approaches to mitigate the side channel attacks in quantum channel. [17]. The Heisenberg uncertainty theory will not becontradicted while eve gets the q-bit from the side channel. Because the data that has been disrupted is in the side channel. While eavesdropper traces the q-bit, there is a 50% risk of makingan erroneous prediction and a 50% chance of making an accurate prediction at the same time. If the eavesdropper is correct in his prediction, he will be able to quickly recover the original encrypted data. As a result, in the QKD, side channel prediction and avoidance play an importantrole.

Quantum Key Distribution use measurement device independent to overcome the changes in conventional QKD methods. [18]. Even in the Phase Shift QKD, there is a big challenge in the side channel attacks as hacker can gain access the data through the channel. The solution for this insecurity is to increase encryption by the double encryption technique. The data is encrypted as usual and it is sent to the receiver. Then the key forthe decryption of the sent data is again encrypted with phase shifting and block reordering. The process of encrypting key first undergoes phase shifting. In phase shifting, the process measures the key whether it is in odd parity or even parity. If it is in odd parity, it is shifted right or if it is ineven parity, it is shifted left. After the process of phase shifting, then the

process undertakes the method of block reordering. In this method, 1mb of data is divided into 36 blocks of data which contains 36mb of data each. These 36 blocks are then reordering or rearranged in particular form to secure it more sophisticated. Thus, the key is being double encrypted and sent to the receiver which in turn decrypts the same process in reverse direction to get the original key and to decryptthe main information.

Aim of the Project

The Quantum Key Distribution(QKD) method enables a pair of authorized remote users toshare secret keys with one another. In the transmission even when eavesdroppers are present, it works on the fundamental ideas of the no cloning theorem and Heisenberg's uncertainty theory. The main drawback of quantum key distribution is Side channel attack, which reduces the accuracy, secrecy, and authenticity of the secret information and results in security losses. When the data is transmitted with QKD method, hackers are aware of only the quantum channel. There is a 50% chance of making an incorrect finding while the eavesdropper tracks the q-bit and a 50%chance of making an accurate guess at the same time. Because of Side channel attack, Data Privacyand Accuracy of the original information is reduced. Also problem arises in Integrity and efficiency of the data transmission. So enhanced novel approaches are developed to enhance the security and maintain the integrity and efficiency

Objectives of the Project

In Quantum Computing, there is a chance for security loss during transmission using the current QKD methods; the security of the secret key poses the biggest challenge to quantum key distribution. In the conventional Quantum Key Distribution paradigm, the side channels could beused by hackers to obtain the secret key. Therefore, the primary goal of the proposed model is to secure the secret key. Hence the objectives of the proposed work is to,

- To develop a Secured Quantum Key Distribution Framework.
- To Secure the Secret data (Encryption key) with Double Shifting and Binary ConversionSystem.
- To improve the security of the secret data (Encryption key) with Binary 90-degree PhaseDouble Shift Key and Block Re-Order Framework.
- To Ensure the Confidentiality and Data Privacy of the communication channel with Binary 90- degree Phase Double Shift Key and Block Re-Order Framework.

Research Questions

- How can existing quantum key distribution (QKD) protocols be improved to enhance security against various types of side channel attacks?
- How can countermeasures be designed and implemented to mitigate the impact of side channel attacks on quantum key distribution, without compromising the efficiency and performance of the system?

Expected Outcomes

As far as the security of the data and the key is concerned, the expected outcomes are

- The security of the encryption key can be strengthened with the BPSK-BRO framework and then transmitted through the quantum channel
- The increase in number of side channels is directly proportional to the possibility of attacks and loss of security. So the loss of security can be estimated in the data transmission

between the source and the destination.

Section 1 discusses about Basic cryptographic ideas, quantum cryptography, quantum key distribution, and QKD methods. The primary goals, research questions and expected outcomes of the research projects are listed. Section 2 identifies the related articles, analyze and find the research gaps and provide inspiration for the research. Section 3 elaborates the Secured Quantum Key Distribution technique employing binary conversion and shifting techniques to improve the secrecy and accuracy of the secret key. Section 4 reveals the implementation results with quantifying reports.

2. Related Works

The works on side channel attacks in quantum key distribution are collected in this system various related articles and implementation papers. The relative examination of various methods for side channel attacks and their drawbacks are in the following table. The various QKD techniques linkedto Side channel attacks are shown in the table.

Table 1 A survey on the Related Articles

S. No	**Area of the Research**	**Concept**	**Disadvantage/ Gaps**

1	Multipho ton and Side-Channel Attacks	Instead of employing a single photon, they used a multi photon approach to create the QKD in this study .	The system complexity increases.
2	Assignment of Secret key in QKD	Probability of Success is improved by secret key assignment priority. [19].	Not focused on security issues such as side channelattacks.
3	Quantum based Random number generation	True random data is used to substitute random looking periodic sequences. [20].	Through quantum key distribution, the proposed QTRNG can be employed in end-to-end secure communications. With the random numbers created, a novel method of security can be offered. No guaranteed solution to side channel attacks.

4	Resource Allocation with Secured Quantum Key Distribution	Rate of secret key is determined. Integer Linear programming formulation is used to allocate network resources. [21].	The concepts for recognizing noise sources and providing solutions for noise channel related concerns is implemented. No remedy for side channel attacks.
5	Post Quantum Signature schemes in side channel attack	Security systems is ensured in signature systems using multivariate quadratic equations [22].	Limited to certain circumstances. To find the solution,lot of phrases are used.
6	Side-Channel-Free Quantum Key Distribution	Both real and virtual channels are used to detect side-channel assaults [23].	It can only detect side channel attacks and cannot provide a precise solution for real-time channel difficulties.

7	Quantum Key Distribution in cloud	QKDP in Cloud improves the security [24].	There is a 50% chance of correctly predicting the data bythe hackers.
8	Identity based secure authenticati on in Quantum	To increase cloud security, a viable long-distance entanglement-based QKD method is utilized. Shifted keys is created with a 4.11 bits per second key rate and error rate is 9.21 across a 100-kilometer optical fiber [25].	The qubit can be reached through the channel with a 50 percent chance of success.
9	Security enhanced in cloud with QKD	The Quantum Key Distribution technique is	BB84 protocol has no solution for side channel attacks

		used to protect datacenters [26].	
10	Quantum Key Distribution in IOT	To increase cloud security, post-quantum cryptography and artificial intelligence (AI) a reemployed [27].	It prevents data from being exchanged between two communicating devices unless they have both verified each other but limited to cloud.
11	QKD with novel Security Method	Examined the latest recent advances in quantum defenses and hacking.[28]	Neither the design nor the implementation phases include data security
12	Reference-free-independent QKD	RFID QKD created the hidden key frames. [29]	Although polarization control correction was used, itserved no purpose in this composition.

13	Symmetric side channel	To ascertain the quantum coherence, a conventional post-processing method was used. [30]	This work does not provide a real-time countermeasureto side channel attacks.
14	Phase shift in QKD	As a brand-new quantum private database query technique, passive round-robin differential phase- shift quantum key distribution is presented. the advice. [31]	Because the distance between the two arms doesn't need tobe changed, it is more practical.

3. Proposed Architecture

Any encryption standards can be used to secure data in a communication system. Secret data is initially encrypted using the RSA Algorithm in the suggested approach. The data owner convertsthe original information into encrypted text using the RSA method in the first phase. Following the encryption procedure, the user may be required to transmit two pieces of information: encrypted data and the encryption key. The encrypted data, or cypher text, is sent via a traditionalclassical channel, and the encryption key is shared via a quantum channel, as shown in Figure 1. To strengthen the security of the encryption key, it is processed through the BPSK-BRO framework before being sent through the quantum channel. The Binary Phase Shift key algorithmand the Block Re-Ordering algorithm are both part of the BPSK-BRO framework. The encryption key is given as an input to the BPSK algorithm, which is then processed. If the number of Parity bits is odd, the bits are shifted to the left, otherwise they are shifted to the right. The shifted bits are then fed into the Block Re-Ordering algorithm as an input. The key size is then divided into the number of blocks based on the block size. The blocks are then relocated to the left or right. sothat the encryption key's security is strengthened before the polarization process.

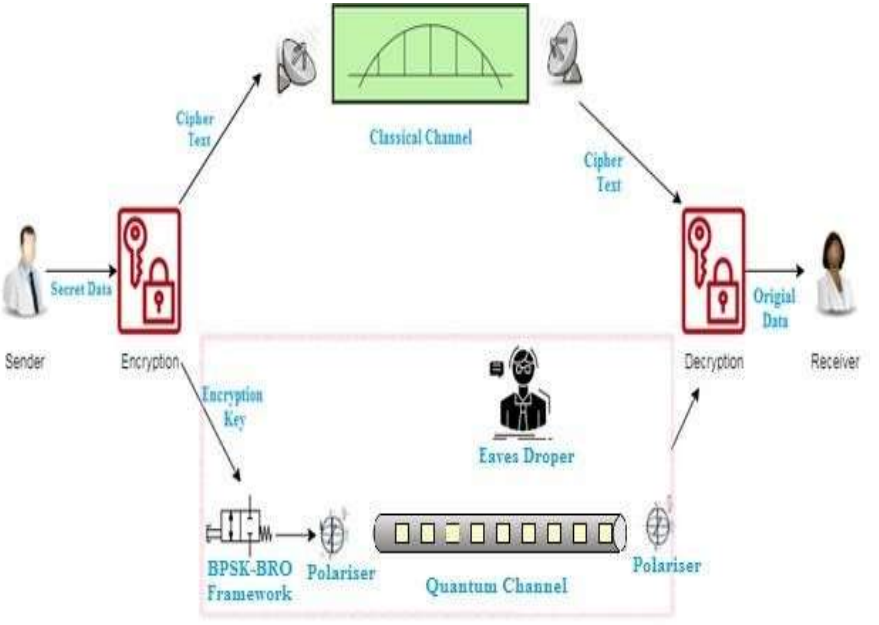

Cipher Text
Classical Channel
Cipher Text
Secret Data
Origial Data
Sender
Encryption
Decryption
Receiver
Encryption Key
Eaves Droper
BPSK-BRO Framework
Polariser
Quantum Channel
Polariser

Figure.1 BPSK-BRO Architecture

The processed data is sent as an input to the polarizer after the BPSK-BRO framework, and the polarizer converts the processed key into qubits. The qubits are then sent across the quantum channel and received by the receiver. On the receiver side, reverse operations are used to obtain the reordered original data. If the receiver determines that the key obtained is authentic and has not been tampered with by any Eavesdroppers, he will authorize the sender to send the encrypted data through the traditional channel, and then the receiver will decrypt the original data sent by thesender with the help of encryption key which is already sent by the receiver.

3.1 Binary Phase Shift Key and block reordering (BPSK-BRO) Frame work

Input: Binary DataOutput: Qubit

3.1.1 Algorithm: 1 Binary Phase Shift Key

Algorithm: 1 Binary Phase Shift Key

```
Primary Input: Classical
Data/Binary DataOutput:
Reordered classical data
Attributes: BD, OP,EP,LB,C=0,i=0 // BD-Binary Data, OP – Odd Parity, EP-
Even Parity,LB-Length of binary data, C-Count, I = index.
Begin
        Input BD        // Get the
        Binary Data as a inputLB =
        Length(BD)
Begin
        For I in range LB
                If (BD[I]==1)
                        C =C + 1
If(C%2==0)
        EP=BD>>1
        Print EP
ENDEND
Else Begin
OP=BD<<1
Print OP
END
```

3.1.2 Algorithm: 2 Block Reordering

Algorithm: 2 Block Reordering	
Input data	: OP/EP (Type of Polarizer)
Output	: Block Reordered Data

```
Attribu : KS, BS, ,PL,OL,RL // KS –Key Size , BS-Size, BR – Block Reordering , NB-Number of Blocks ,PL-Polarizer, OL-Orthogonal,RL-Rectilinear ,BL-Blocks
nput OP||EP&BS // getting the output of BPSK as a input, and Block SizeKS=Length (OP||EP) //finding the Key Size
NB = KS/BS // finding the number of Blocks and form the Blocks
For I in range OP||IP
BL= BL[i] to NB; // divide the key into blocks
    If (PL==RL) // finding the polarizer type whether it is a Orthogonal or Rectilinear
BR = BL>>1
Print BR Else BR=BL<<1
Print BR
END
```

Algorithm Description:
BPSK Binary Phase Shift Key and Block Re-Ordering are two algorithms included in the BPSK-BRO architecture. We implement two different sets of data after the RSA encryption process.

1. Encrypted data
2. Encryption Key

The cypher text, is transmitted through a traditional communication channel. The encryption key is another result of the encryption process. That key will be used as a parameter in the BPSK algorithm. The BPSK method determines the length of the key that will be stored in the BD in thefirst stage. After then, the number of odd and even parity will be determined. If the parity is even,the BD is right-shifted; otherwise, the BD is left-shifted and placed in the EP and OP, respectively.The BPSK result is then used as an input to the BRO Algorithm, which broke the key into key chunks or blocks using the block size. After conducting block conversion, the blocks will be reordered. The type of polarizer used for converting binary data to Qubit is used for block reordering. If the sender uses a rectilinear polarizer, the blocks is arranged by right shifting them one block, otherwise they will be left shifted one block. The BPSK-BRO Framework converts theSecret key into a Secured version of Qubits using the two algorithms discussed above. In order to recover the encryption key's original order that was sent by the sender, the reverse block reordering approach is used on the receiver side. Then quantum bit is converted as classical bit. The sender sends the encrypted data using the

conventional channel once the receiver has received the secretkey safely. The receiver then decrypt the data and receive the original data supplied by the sender.

4. Performance and Validation:

The Python Programming Language is used to implement the proposed algorithm BPSK PRO. The proposed architecture is used to ensure the best level of security for both encrypted data and secret keys. With the use of polarizers, greater key security can be obtained. The suggested framework provides 99 percent more security than the current system. Using mathematical calculations and testing, the new algorithms are compared against current methods. The BPSK PRO framework achieved a security rating of 99 percent. The following calculations can be used to ensure the security of the secret key. The number of probable side channels can be estimated inthe first step by multiplying the photon count by two. The security loss is estimated in the secondstep using the side channel count.

Number of Side Channels (NSC) = Number of Photons(N) * 2Security Losses in Percentage = NSC / 2
Loss due to Probability of Guessing with the Photon Count is calculated with the values ofTable.2

Table : 2 Number of photon vs Number of Side Channels

S.No	Number of Photons (N)	Number of Side channels (NSC)
1	10	20
2	15	30
3	20	40
4	25	50
5	30	60
6	40	80
7	50	100
8	60	120
9	80	160
10	100	200

The rising of side channel count with tiny variations in the number of photons is depicted in theFigure.2 using the given tabular values.

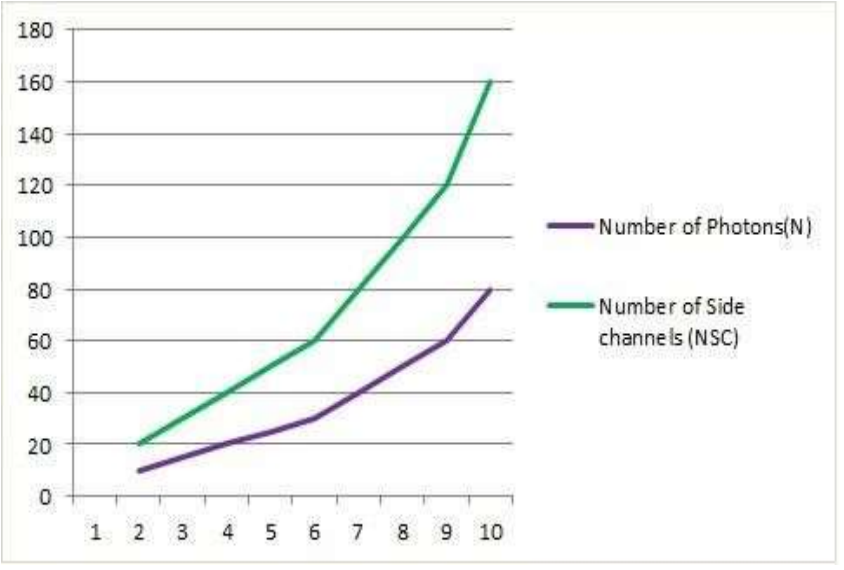


Figure 2. Side channel count vs number of photons

Figure 2 shows that as the number of photons increases, so does the number of

side channels, implying that attack possibilities have increased as well. Two polarizers were utilized for photon polarization according to the existing quantum key distribution approach. Given the possibility ofattacks due to side channels, security losses can be computed using the method below.

Security Losses (SL) = N*NSC/3

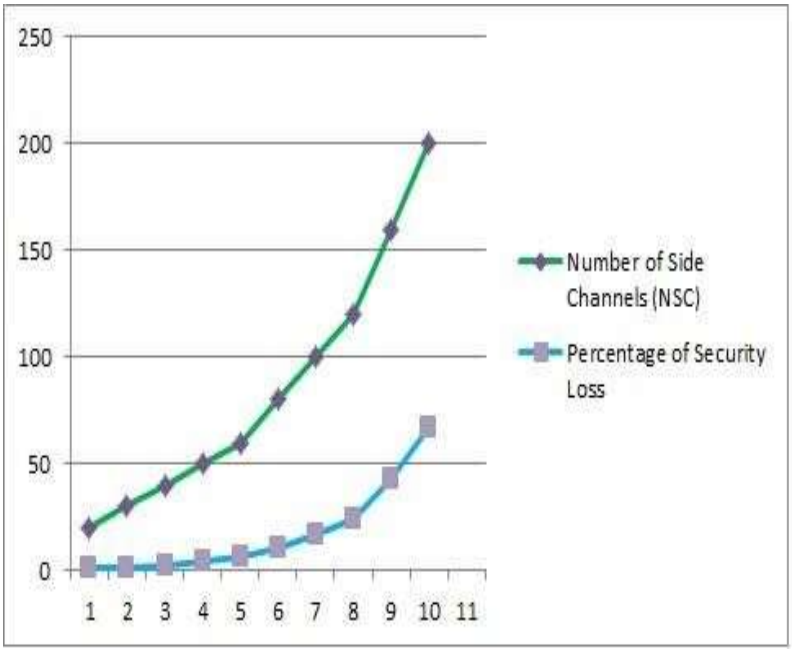
Where n denotes the number of photons, the security losses are estimated and presented in Table.3.

Table 3: Number of Side channel vs Percentage of Security Losses in Percentage

S.No	Number of Side channels (NCC)	Percentage of Security Loss(SL)
1	20	0.67
2	30	1.5
3	40	2.67
4	50	4.17
5	60	6
6	80	10.67

7	100	16.67
8	120	24
9	160	42.67
10	200	66.67

We can see from table 3 that increasing the photon count automatically raises the security lossesby a percentage


250
200
150
100
50
0
1 2 3 4 5 6 7 8 9 10 11
Number of Side Channels (NSC)
Percentage of Security Loss

.

Figure 3. Increasing the photon count automatically raises the security losses When the number of side channels grows, the security losses grow as well.

5. Performance Comparison and Discussion

The Proposed systems security implementation can be calculated with the following formula.

Security Losses (SL)= $SL = \frac{2}{BPSK\&BR*n}$

Where SL is Security Losses

2 – types of polarizers used

BPSK – Binary Phase Shift Key with Parity bitBR-Block Reordering method
N= number of bits in the Secret key.

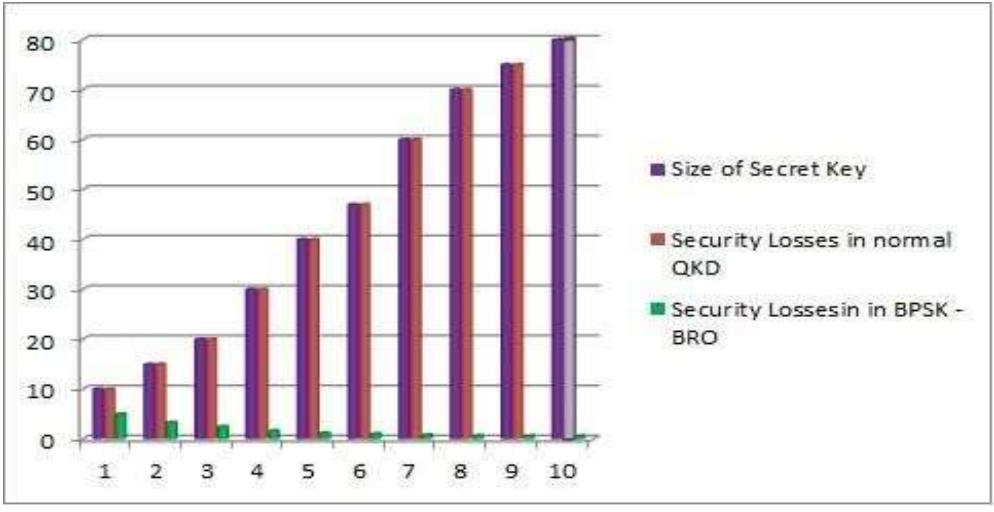
From that above formula the security losses in existing QKD vs BPSK-BRO has been tabulated inthe table.4

Table : 4 Security Loss in QKD vs Security Losses in BPSK-BRO Framework

S. No	Number of Bits inSecret Key	Security Lossesin percentage (QKD)	Security Losses inBPSK-BRO
1	10	0.67	0.05
2	15	1.5	0.03
3	20	2.67	0.03
4	30	4.17	0.02
5	40	6	0.02
6	47	10.67	0.013
7	60	16.67	0.01
8	70	24	0.008

9	75	42.67	0.007
10	80	66.67	0.005

From that values of table 4 the figure.4 has been developed. From the calculated values the abovetable we can easily identify that the security



losses in proposed work i.e BPSK-BRO frame work is very low when compare with the existing QKD algorithms.

Figure 4. Security Losses in BPSK-BRO vs QKD

The figure .4 indicates that when compare with the existing system the proposed model BPSK- BRO framework provide more than 99% security.

The test statistic will most likely follow a normal distribution if the scaling component value in the test statistic is known orelse the test statistic is replaced withan approximation based on the data that follows a Student's T distribution (under certain conditions)

x_1

x_2

$$= \sum \frac{x1}{n} = 0.018708 \text{ - } 1$$

$$= \sum \frac{x2}{n} = 17.7666\text{-- } 2$$

The mean value of security losses in BPSK-BRO is 0.018708, and the mean value of QKD is approximately 17.77, according to the results of the previous analysis, with standard deviations of 0.014156 and 21.62 for BPSK-BRO and QKD, respectively. The two-tailed t value is -2.56579, and the P value is .019447 , which is less than 0.05, indicating that the differences are statistically significant in both scenarios. The mean value of the BPSK-BRO (0.018708) is much lower than that of QKD (17.7666). When the security losses of the BPSK-BRO framework are compared to the security losses of the QKD framework, it is clear that the BPSK-BRO framework's security losses are significantly smaller and appear to be better.

6. Conclusion

For both personal and business networks, network security is becoming increasingly important. QKD was proposed as an effective approach to improve security by converting the secret message to Q-bits. The eavesdropper, on the other hand, could be able to hack the data without being discovered by the recipient by using the side channel. As a result, the sender will receive an acknowledgement from the receiver. Using the usual method, the hacker can

readily obtain the encrypted data. This work has proposed a novel BPSK-BRO framework to achieve maximum security in order to overcome these difficulties. The proposed approach primarily focuses on the development of a BPSK-BRO method to add complexity to secret data prior to q-bit conversion using two processes: shifting and binary conversion. During the polarization process, rectilinear and orthogonal filters are also used. A complete experimental analysis is carried out to examine the better security performance of the BPSK-BRO technique, and the resultsare analyzed under many performance indicators. The experimental findings showed that the proposed model outperforms the present method in terms of security to the greatest extent possible.In the future, the QKD can be used in conjunction with the side channel to safeguard data in the real world. In addition, intensive experimental analysis with real-time data can be prioritized. Thesame algorithm can be experimented for any kind of typical attack and the results can be improved with any soft computing techniques. Also generative AI in conjunction with QKD can be implemented to mitigate or avoid the side channel attacks. Nano scale structures like quantum interconnects ensure the qubit communication among different parts of quantum processor. Also highly sensitive quantum sensors can be created by nanotechnology.

Ethical Approval

This page does not include any of the authors' studies involving human or animal participants.

Funding

The authors state that they did not receive any funding for this study.

Conflict of Interest

There are no relevant financial or non-financial interests for the authors to expose this paper.

Informed Consent

This article does not include any of the authors' studies involving human or animal participants.

Data Availability

Any of the authors' experiments involving human or animal participants are not included in thisarticle.

http://www.vision.caltech.edu/Image_Datasets/Caltech101/ and Quantum bit repository,https://pure.strath.ac.uk/ws/portalfiles/portal/92638035/dataset.zip.

References :

[1] Abdulshaheed, Haider Rasheed, I. Al Barazanchi, H. T. Jaya, and D. Tunggal. "Smart solutions based-on cloud computing and wireless sensing." Int. J. Adv. Sci. Technol 28, no. 8 (2019): 526-542.

[2] Dijesh, P., SuvanamSasidhar Babu, and Yellepeddi Vijayalakshmi.

"Enhancement of e-commerce security through asymmetric key algorithm." Computer Communications 153 (2020): 125-134.

[3] Pandey, Krishna Kumar, Vikas Rangari, and Sitesh Kumar Sinha. "An enhanced symmetric key cryptography algorithm to improve data security." International Journal of Computer Applications 74, no. 20 (2013).

[4] Osamor, Victor Chukwudi, and Imuetinyan Boma Edosomwan. "Employing scrambled alpha-numeric randomization and RSA algorithm to ensure enhanced encryption in electronic medical records." Informatics in Medicine Unlocked 25 (2021): 100672.

[5] Mojisola, Falowo O., Sanjay Misra, C. Falayi Febisola, Olusola Abayomi-Alli, and Gokhan Sengul. "An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA)." Egyptian Informatics Journal 23, no. 2 (2022): 291-301.

[6] Joshi, Abhishek, Mohammad Wazid, and R. H. Goudar. "An efficient cryptographic scheme for text message protection against brute force and cryptanalytic attacks." Procedia Computer Science 48 (2015): 360-366

[7] Khalid, Roszelinda, and Zuriati Ahmad Zukarnain. "Cloud computing security threat with quantum key distribution defense model." In Proc. of the 3rd International Conference on Green Computing, Technology and Innovation (ICGCTI2015), pp. 49-54. 2015.

[8] Murali, G., and R. Sivaram Prasad. "CloudQKDP: Quantum key distribution protocol for cloud computing." In 2016 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1-6. IEEE, 2016.

[9] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78 (2018): 964-975.

[10] Thangavel, Ms, P. Varalakshmi, Mukund Murrali, and K. Nithya. "An enhanced and secured RSA key generation scheme (ESRKGS)." Journal of information security and applications 20 (2015): 3-10.
[11] Raja shree, S., A. Chilambu Chelvan, and M. Rajesh. "An efficient RSA cryptosystem by applying cuckoo search optimization algorithm." Concurrency and Computation: Practice and Experience 31, no. 12 (2019): e4845.
[12] R. Shree, C. Chelvan and M .Rajesh ‘‘An Efficient RSA Cryptosystem by Applying Cuckoo Search Optimization Techniques,” Concurrency and Computation: Practice and experience. Wiley Online Library, vol. 31, no. 12. http:/doi.org/ 10.1002/cpe.4845, 2019.
[13] Yu, Hoyoung, and Youngmin Kim. "New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices." Electronics 9, no. 2 (2020): 246.
[14] Shankar, K. "An optimal RSA encryption algorithm for secret images." International Journal of Pure and Applied Mathematics 118, no. 20 (2018): 2491-2500.
[15] Bangera, Kripa N., NV Subba Reddy, Yashika Paddambail, and G. Shivaprasad. "Multilayer security using RSA cryptography and dual audio steganography." In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 492-495. IEEE, 2017.
[16] Abdullah, Alharith A., and Yasser H. Jassem. "Enhancement of quantum key distribution protocol BB84." Journal of Computational and Theoretical Nanoscience 16, no. 3 (2019): 1138-1154.
[17] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Linesh Raja & Ramesh C.Poonia , Cryptography An enhanced quantum key distribution protocol for security authentication September 2019Journal of Discrete Mathematical

Sciences and Cryptography22(4):499507,DOI:10.1080/09720529.2019.1637154
[18] R.C. Diovu J.T. Agee Enhancing the security of a cloud-based smart grid AMI network by leveragingon the features of quantum key distribution ,March 2019Transactions on Emerging Telecommunications Technologies 30(1) , DOI:10.1002/ett.3587.
[19] E. E. Moghaddam, H. Beyranvand and J. A. Salehi, "Resource Allocation in Space Division Multiplexed Elastic Optical Networks Secured With Quantum Key Distribution," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 9, pp. 2688-2700, Sept. 2021, doi: 10.1109/JSAC.2021.3064641.
[20] Mathieu Bozzio, Adrien Cavaillès, Eleni Diamanti, Adrian Kent, and Damián Pitalúa-García, ”Multiphoton andSide-Channel Attacks in Mistrustful Quantum Cryptography”, PRX Quantum 2, 030338 – Published 1 September 2021.
[21] Vaishnavi Kumar, John Bosco Balaguru Rayappan, Rengarajan Amirtharajan, Padmapriya Praveenkumar, Quantum true random number generation on IBM’s cloud platform, Journal of King Saud University - Computer and Information Sciences, 2022,https://doi.org/10.1016/j.jksuci.2022.01.015.
[22] E. E. Moghaddam, H. Beyranvand and J. A. Salehi, "Resource Allocation in Space Division Multiplexed Elastic Optical Networks Secured With Quantum Key Distribution," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 9, pp. 2688-2700, Sept. 2021, doi: 10.1109/JSAC.2021.3064641.
[23] Park, Aesun & Shim, Kyung-Ah & Koo, Namhun & Han, Dong-Guk. (2018). Side-Channel Attacks on Post- Quantum Signature Schemes based on Multivariate Quadratic Equations: - Rainbow and UOV -. IACR Transactions on Cryptographic Hardware and Embedded Systems. 500-523. 10.46586/tches.v2018.i3.500-523. https://doi.org/10.13154/tches.v2018.i3.500-523.

[24] Samuel L. Braunstein, Stefano Pirandola,"Side-channel-free quantum keydistribution",https://doi.org/10.48550/arXiv.1109.2330.
[25] Murali, Gudipati and R. Siva Rama Prasad. “CloudQKDP: Quantum key distribution protocol for cloud computing.” 2016 International Conference on Information Communication and Embedded Systems (ICICES) (2016): 1-6.
[26] Sharma, Geeta and Sheetal Kalra. “Identity based secure authentication scheme based on quantum key distribution for cloud computing.” Peer-to-Peer Networking and Applications 11 (2018): 220-234.
[27] Sureshkumar P.H, Ambily Pramitha and Dr. Rajesh R “The Quantum Key Distribution(Qkd) Based Security Enhanced Cloud Data Center Connectivity” International Journal of Latest Trends in Engineering and Technology, Vol.(7)Issue(4), DOI: http://dx.doi.org/10.21172/1.74.051, e-ISSN:2278-621X, pp.378-382
[28] Ankur Lohachab, Karambir , ”Using Quantum Key Distribution and ECC for Secure Inter-Device Authenticationand Communication in IoT Infrastructure”, Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India)on March 26-27, 2018.
[29] Lo, HK., Curty, M. & Tamaki, K. Secure quantum key distribution. Nature Photon 8, 595–604 (2014). https://doi.org/10.1038/nphoton.2014.149
[30] Yin, Zhen-Qiang, et al. "Reference-free-independent quantum key distribution immune to detector side channelattacks." Quantum information processing 13.5 (2014): 1237-1244.
[31] Graeme Smith, Phys. Rev. A 78, 022306 – Published 5 August 2008.
[32] Li, Jian, et al. "Practical quantum private database queries based on passive round-robin differential phase-shiftquantum key distribution." Scientific reports

6.1 (2016): 1-6.