Secured - Quantum Key Distribution (SQKD) for solving Side Channel Attack to enhance Security, based on Shifting & Binary Conversion for Securing Data (SBSD) Frameworks

Gopinath N (gopinathit14@gmail.com)
Sathyabama Institute of Science and Technology https://orcid.org/0000-0002-2530-0312
Prayla Shyry D
Sathyabama Institute of Science and Technology

Research Article

Keywords: QKD, Q- bits, SBC, SQKD and SQSC

Posted Date: January 5th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1208654/v1

Secured - Quantum Key Distribution (SQKD) for solving Side Channel Attack to enhance Security, based on Shifting & Binary Conversion for Securing Data (SBSD) Frameworks

N.Gopinath[a] , Dr. S.Prayla Shyry [b]

[a]*Research Scholar, School of computing, Sathyabama Institute of Science & Technology, Chennai, India, gopinathit14@gmail.com.*
[b]*Associate Professor, Faculty of Computer Science and Engineering, Sathyabama Institute of Science & Technology, Chennai, India, praylashyry.cse@sathyabama.ac.in*

I. Abstract

Network security is critical for both personal and business networks. Most homes with high – speed internet have one or more wireless routers, which can be hacked if not adequately secured. Even though, if more number of solutions were addressed for security, still the security is challenging one in networks.

Quantum Key Distribution was proposed to enhance security in the past literature. In this QKD, the secret message was converted in to Q-bits. Through this side channel, there is a chance to hack the data by the Eavesdropper which cannot be identified by the receiver side. So, receiver will send the acknowledgement to the sender for sending encrypted data in the classical channel.

From this, the hacker can easily fetch the encrypted data from the classical channel. To address this issue, Security in Quantum side Channel (SQSC) framework has been proposed in which Shifting and Binary Conversions (SBC) algorithm has been implemented. This proposed security model attains good performance to a greater extent.

Keywords: QKD, Q- bits, SBC, SQKD and SQSC.

II. Introduction

The development of information technology and quantum physics has been growing quickly. The quantum communication technology and quantum computing has been used for establishing a well communication in the information network[9-10]. Quantum computing has the ability to provide more security in cloud environment [11-12]. For ex: searching will be faster in the unsorted database for finding the factorial of a number.

Quantum communication technology plays a major role for protecting communication channels [27] from unauthorized users. In the past research, quantum cryptography [20] were addressed enormously in which the QKD is derived from the quantum cryptography. This QKD is used for creating the random key between two authorized users in the remote area [13].

Recently, some new QKD techniques and advances have been suggested and developed. The Quantum Secure Direct Communication (QSDC) [14] protocol is intended for unidirectional communication in which the sender specifies the information content of Mobile Netw Appl.

The first QSDC protocol was proposed by Long et al. Later, Bostrom and Felbinger proposed the "Ping-Pong" protocol, a well-known QSDC protocol based on EPR pairings Since then, various improvements and modifications to the ping-pong protocol have been published, including superdense coding and the use of GHZ states. The ultra-short storage duration of a quantum state is a challenging factor and yet to be addressed. Heifei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics now holds the world record for quantum state storage time of under 3ms. All protocols that require the storage of quantum states[19] in process have some operational limits, such as the ping-pong protocol, which requires the storage of one photon for a duration equal to twice the distance between them.

Rest of the paper is structured as follows. The first section depicts the network's introduction. The topics of related work are explained in Section 2. The Proposed Work and its Architecture are introduced in Section 3.Section 4 reveals the proposed framework with algorithm. Section 5 describes the implementation and results. Finally conclusion and references are described in section 6.

III. Related Work

Nowadays, security in cloud computing is a challenging factor. Because, in quantum based channels, secret keys are sent as photons which is travelled in Fibre optics cable. To establish communication, traverse from Fibre optic cable to cloud environment is a challenging one. It is inferred that without fibre optic cable the communication should be established in cloud. More number of research works was explored in the past literature. But still some research issues did not addressed with respect to the security. The following related works are reviewed to address the Quantum Key Distribution [17] in cloud environment for securing secret message from eavesdropper.

Jian Li et., al., investigated the security of a novel QKD protocol, revealing that it is quasi-secure. The proposed protocol is implemented using an efficient circuit simulation.
The author claims that the proposed work is only quasi secure. So, he is not assuring the security in cloud environment at a greater extent.

The effect of source faults on the secure key generation rate of the Round Robin Differential Phase Shift – Quantum Key Destribution (RRDPS-QKD) protocol was investigated using four-intensity decoy states by Qian-Ping Mao et al. We have set stringent constraints for the key generation rate when

the count rate of the k-photon state for the signal source is bounded. The performance of the four-intensity decoy-state RRDPS-QKD protocol with source errors was addressed using WCS as an example. The results show that the RRDPS-QKD has a considerable impact on the secure key generation rate in practise with source flaws.

Zhuo Zhang et., al., Generative Reversible Data Hiding (GRDH) is a new Reversible Data Hiding (RDH) approach based on the Generative Adversarial Network was proposed. A powerful image generator was trained using the GAN model to produce realistic images. After that, the image is sent into the CycleGAN model, which generates images with various semantic information... i.e., the proposed method's efficiency, has been demonstrated by experimental data. Despite the fact that due to CycleGAN's current performance, 100 percent reversibility is not attainable, the proposed method can generate the first RDH scheme without modifying the cover.

Hoi-Kwong Lo et. al., explained the motivation for quantum cryptography research as well as the current state of the art. The current security paradigm, as well as its assumptions, merits, and limitations, are addressed in detail. The newest achievements in quantum hacking and defenses against it were evaluated after a brief introduction to current experimental successes and obstacles.

Shujing Li and Linguo Li, On the basis of one decoy state, a Round Robin Differential Quadrature Phase Shift Quantum Key Distribution[21] – Odd Coherent State (RRDQPS-QKD-OCS) was presented. RRDQPSQKD- OCS has a significantly greater key generation rate than other RRDQPSQKD and RRDPS-QKD protocols, according to simulation data. The maximum transmission distance of RRDQPS-QKD-OCS, on the other hand, is significantly longer. Furthermore, a single decoy state strategy is adequate for RRDQPS-QKD-OCS to achieve asymptotic performance with infinite decoy states [25].

Based on the quantum private database query protocol, Jian Li et al. proposed Round-Robin Differential Phase-Shift Quantum Key Distribution (RRDPSQKD). Compared to previous quantum private database query protocols, the new approach has the following distinguishing advantages: Alice can only acquire one key bit, ensuring the present protocol's efficiency and security[23] and it is substantially easier and more practical because it does not require adjusting the length difference between the two arms interferometer and instead, passively interferes with two pulses. Furthermore, the existing protocol has been demonstrated to be safe for both users and databases.

Zhen-Qiang Yin proposed an hybrid algorithm namely RFI QKD and measurement-device-independent QKD[18]. Used Polaraization control and phase compensation are very much useful in some circumstances. However, all detector side channels have been deleted, removing the possibility of data theft from the side channel[19].

Symmetric-side-channel-assisted private capacity of a quantum channel[16] has been examined, according to Graeme Smith. There are quantum key distribution protocols [26] that use one-way classical post-processing[15]. Our findings show that collective attacks are far more powerful than individual attacks. Even though more number of research works were explored in the past literature review, but there is some research issues for not rectifying the data hacking by the third party. In this paper, a new SQSC framework has been proposed in which SBC algorithm is implemented in this framework to stop the hacking of data through side channel in the quantum channel. The detailed analysis of the above survey is listed in the table 3.1.

Table 3.1: Survey

S. No	Name of the Researcher	Title of the Research	Concept	Disadvantage
1	Jian Li et., al.,	A Quantum Key Distribution Protocol Based on the EPR Pairs and its Simulation[1]	The safety of a novel QKD protocol is investigated, revealing that it is quasi-secure. In addition, the proposed protocol is implemented using an efficient circuit simulation.	• Theoretical model was used • Faulty equipment and noisy environments were not taken into account.
2	Qian-Ping Mao et., al.,	Decoy-state round-robin differential-phase-shift quantum key distribution with source errors[3]	• RRDPS-QKD protocol was investigated. • Using WCS as an example, the performance of the four-intensity decoy-state RRDPS-QKD protocol with source faults has been explored • The results show that the RRDPS-QKD has a considerable impact on the secure key generation rate in practise with source flaws.	Did not address secure in side channel
3	Zhuo Zhang et., al.,	Generative Reversible Data Hiding by Image-to-Image Translation via GANs[2]	• GRDH algorithm was proposed based on GAN model and fed in to CycleGAN which produces various realistic images.	Implemented with different images but not addressed in side channel attack
4	Hoi-Kwong Lo et. al.,	Secure quantum key distribution[4]	Researched the most recent breakthroughs in quantum hacking and countermeasures.	• The author only conducted a survey • Data security was not implemented at both the design and implementation

				levels.
5	Shujing Li and Linguo Li,	Round robin differential quadrature phase shift quantum key distribution by using odd coherent states[6]	• For securing data, RRDQPS-QKD-OCS is presented. • Compared to other RRDQPSQKD, it has a faster key generation rate and a longer maximum transmission distance. Furthermore, a single decoy state strategy is adequate for RRDQPS-QKD-OCS to achieve asymptotic performance with infinite decoy states.	The author implemented the concept at simulation level
6	Jian Li et. Al.,	Practical Quantum Private Database Queries Based on Passive Round-Robin Differential Phaseshift Quantum Key Distribution[5]	• A unique quantum private database query mechanism is proposed: passive round-robin differential phase-shift quantum key distribution. Follow adv: • The user Alice can acquire only one key bit, ensuring the current protocol's efficiency and security; and it is substantially easier • More practical because the length difference between the two arms does not need to be changed.	The concept has been implemented at simulation level.
7	Zhen-Qiang Yin	Reference-free-independent quantum key distribution immune to detector side channel attacks[8]	• A new QKD protocol is proposed which is a mixture of RFI QKD and measurement-device-independent QKD. • Used Polarization control and phase compensation are very much useful in some circumstances. But here all detector side channels are removed in which there is a chance of hacking the data from the side channel.	Deleted the side channel. So, easy to hack the data through side channel.
8	Graeme Smith	Private classical capacity with a symmetric side channel and its application to quantum cryptography[7]	• A quantum channel's symmetric-side-channel-assisted private capacity has been investigated. • Our findings show that collective attacks are far more powerful than individual attacks..	In case of individual attacks, there is a chance of eavesdropping [16] the data.

IV. Proposed Architecture

The framework SBSD has been implemented using the javascript and the proposed algorithm is executed inside this framework. Sender enters the original image to Receiver with some secret data through the communication channel which can be performed by the following steps which is showing in figure 4.1.

1. Encrypt the original image using AES Encryption Techniques
2. Compress the encrypted image
3. Embedding the secret data in the encrypted image
4. Sending process
    a. Encryption key through quantum channel as Q-bits[22]
        1. Filter has been used to convert the encryption key into Q-bits
        2. There are two types of filters are used under Polarization process
            a. Rectilinear and Orthogonal [24]
        3. Encrypted image with secret data as a classical data (0's and 1's) through classical channel
4. Framework has been constructed while key transmission phase. Inside the framework, more security measures are added along with the secret key.
5. The sender will send the message what type of polarizer has been used, depends on this message the receiver will use the same polarizer to get the key from the Q-bits.
6. If any Eavesdropper tries to hack the key (Q-bits), receiver will be able to identify the hacker by two properties. 1. Heisenberg Uncertainty theorem and 2. No Cloning Theorem. By using these two properties, if anybody disturbs the quantum channel which will be identified by the receiver.
7. If the receiver recognizes the correct Q bits, acknowledgment has been sent to the sender side for sending the encrypted data.
8. Based on the secret key (Q bits) and encrypted data (0's and 1's), the receiver will decrypt the image and the secret data (passing data hiding key) is obtained.
9. Finally the receiver has the following information
    a. Original Image
    b. Secret data

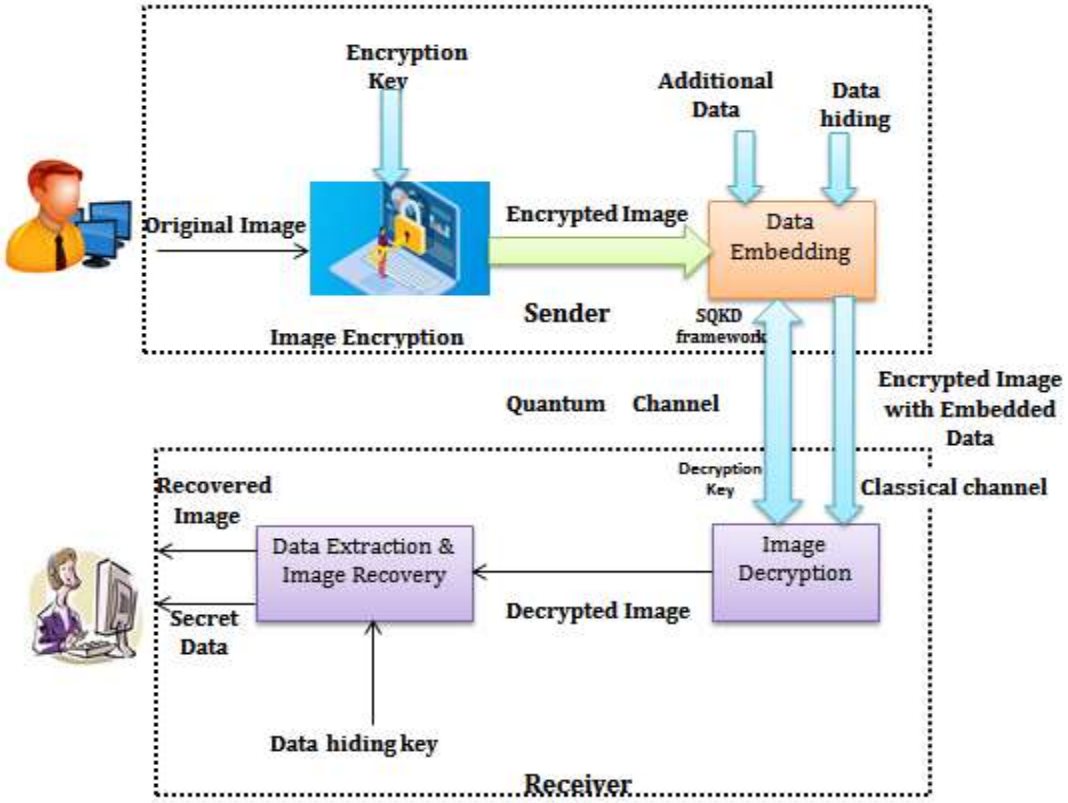

Figure 4.1 : Proposed Architecture

4.1 SBSD (Shifting & Binary for Securing Data) Framework

The SBSD framework, which comprises of two types of algorithms, has been developed for safeguarding data across the network. The sender must determine which sort of polarizer will be used to encrypt the key. For example, if the sender chooses to use rectilinear polarizer, they must first do a 1-bit right shift and then 1's complement. Otherwise, the sender opts for orthogonal polarizer, 1-bit left shift, and 2's complement.

There is no algorithm for safeguarding data via a quantum channel in the current system. Secret data was transformed into Q-bits and sent across the quantum channel directly. Eavesdropper via the side channel has the potential to hack the data. The side channel could not be identified by the receiver. As a result, the data from the side channel has a 50% risk of being hacked. Because two polarizer were used. To overcome this issue, some complexity will be added to the secret data before converting q-bits which uses two mathematical approaches. It will not allow the provision to hack the original data. So 100% secret data has been saved.

4.2 Shifting & Complement Algorithm (S & C A)

Input: Classical bit (type of polarizer)

Output: Q-bits

Attributes: Po,Rl,Og, RS, LS, OC, TC // Po-Polarizer, Rl –Rectilinear, Og-Orthogonal, Right Shift (RS), Left Shift (LS), One's Complement (OC), Two's Complement (TC)

```
Begin
    Input Cb // Input the Classical bit
    If(Po==Rl) // Checking type of Polarizer in which whether it is rectilinear or orthogonal
      Begin
        RS=Cb >>1 // do the right shift of Classical bit
        Print RS
       L=  Length (RS) // Finding length of Right shifted bit and stored in the L
        For (i=1 to L) //
        Begin
          OC=flip(RS) //Do the one's complement of RS using flip function and stored into OC
          Print OC
        End
      End
    Else
      Begin
          LS=Cb <<1// Do the left shift of classical bit and stored into LS
          Print LS
       L1=  Length (LS) // finding the length of LS and stored into L1
       For(i=1 to L1)
       Begin
            OC1=flip (LS) // do the ones complement of LS and stored to OC1
       End
            TC=OC1+'1'// Again ones complement result is complemented which forms the two's complement and stored into TC
            Print TC
        End
    End
```

4.3 Implementation Results

The SBSD framework has been implemented using javascript language. Initially sender passes the secret key to the receiver. To safeguard the key as well as data, polarizers are implemented through quantum channel in the side channel. The proposed algorithm maintains the security 99% than the existing systems. The proposed algorithms are compared with the existing approaches and with the help of mathematical testing; the proposed work is quantified at 99% security.

The security key has been calculated by using two steps. In the first step, number of side channels has been calculated by multiplying number of photons with 2. In the second step, the number of photons has been multiplied with side channels to find the security in percentage

Side Channel (SC) =No. of photons (N)*2

Security (Sec) =N*SC/3 (1)

Table 4.1: Number of photons vs Number of side channels

S.No	Number of photons (N)	Number of side channels (SC)
1	10	20
2	15	30
3	20	35
4	30	42
5	40	50
6	47	58
7	60	70
8	70	82
9	75	90
10	80	95

The following figure 4.2 shows the plot of number of photons with number of side channels using the table 4.1.

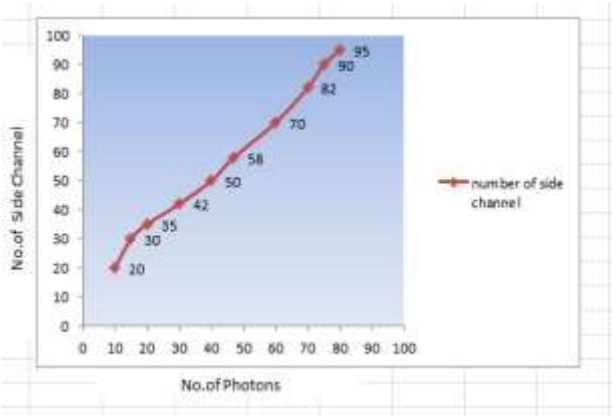

Figure 4.2: No of Photons vs No of side channels

Using the formula 1 the security key has been calculated. The following table shows the tabulation of data for number of side channels and security loss in percentage.

Table 4.2: Calculation of Security loss percentage

S.No	Number of side channels (SC)	Security loss in percentage
1	20	3.4
2	30	5
3	35	8.7
4	42	16
5	50	23
6	58	27
7	70	36
8	82	42
9	90	45
10	95	48

Using the table 4.2 values , the graph is drawn with respect to security loss and number of side channels as shown in the figure 4.3.

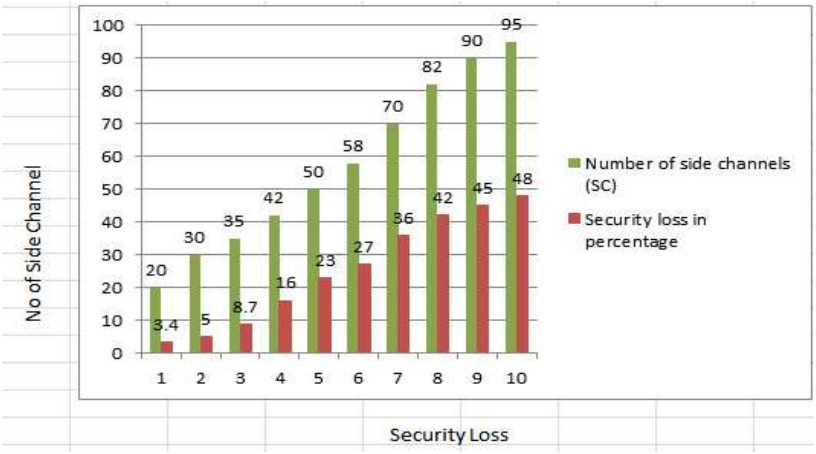

Figure 4.3: Security loss vs Number of side channels

Existing QKD system and Proposed System Implementation and Results

Proposed System

The security loss can be calculated using the formula 2. First multiply the value of shifting and complements with number of bits. Finally probability value is divided by the above multiplied value which gets security loss.

$$S_L = {}^{PS}/_{ST\&C * n} \qquad 2$$

Where

S_L : Security Loss

N : The number of bits

ST&C : Two shifting technologies and two complements (4)

P.S : Probability of getting security loss. Because two polarizers are been used (12.5).

Using the formula 2, the security loss is calculated for the proposed algorithm and which can be tabulated as shown in the table 4.3.

Existing System

$$S_L = {}^{PS}/_{ST\&C * n} \qquad 3$$

Where

S_L : Security Loss

N : The number of bits

ST&C : Two shifting technologies and two complement (2)

P.S : Probability of getting security loss. Because two polarizers are been used (50).

Table 4.3 Calculation of security loss based on the size of the secret data

Size of secret Data (in Bits) SSD	Security loss in Percentage: S&CA	Security loss in Percentage QKD
1	3.1250	25.0000
2	1.5625	12.5000
3	1.0375	8.3330
4	0.7812	6.2500
5	0.625	5.0000
6	0.5208	4.1666
7	0.4464	3.5714
8	0.3906	3.1250
9	0.3472	2.7777
10	0.3125	2.5000

Using the formula 3, the security loss is calculated for the Existing algorithm and which can be tabulated as shown in the table 4.3.

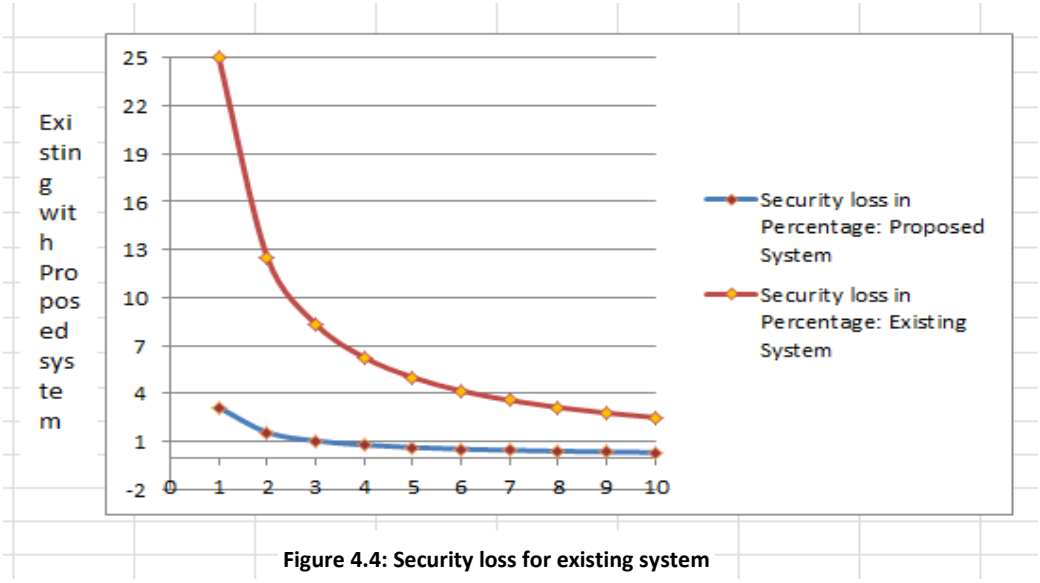

Figure 4.4: Security loss for existing system

Figure .4.4 show the security losses which is present in the existing systems

V. T. Test

It can be used to determine if two sets of data are significantly different from each other, and is most commonly applied when the test statistic would follow a normal distribution if the value of a scaling term in the test statistic were known. When the scaling term is unknown and is replaced by an estimate based on the data, the test statistic (under certain conditions) follows a Student's t distribution.

$\bar{x}_2 = \sum \frac{x_2}{n}$= 0.91487

$\bar{x}_2 = \sum \frac{x_2}{n}$ =7.32237

$\sigma^2 \mathrm{d} = {\sigma_1}^2/n_1 + {\sigma_2}^2/n_2$=7.6403+65.60967=73.2500

Where ${\sigma_1}^2$ is the value of standard deviation for Proposed system (S&CA) and ${\sigma_2}^2$ is the value of standard deviation for existing system (QKD).

Standard Deviation (S.D) σd =$\sqrt{\sigma^2 d}$ =8.5586

T= $\overline{x_1} + \overline{x_2}$/ σd = 0.962452

Where T is obtained by subtracting the value first mean and second means which is divided by standard deviation. Enter T-table at (n1 + n2-2) degrees of freedom.ie 10 +10-2 = 6. The calculated value is 8.55 and Tabulated value for 18 degrees of freedom in p = 0.5 is = 1.067 in table (Foster H). So, concluding that the calculated value is greater than the tabulated value. So there is a difference between these two..i.e. p = 0.3, 93% difference with the model Existing (QKD) and Proposed System (S&CA).

VI . Conclusion

Personal and business networks both require network security. Most high-speed internet houses have one or more wireless routers, which can be hacked if they are not properly secured. Even if a greater number of solutions are addressed for security, network security remains a challenge.

In the past, Quantum Key Distribution (QKD) was offered as a way to improve security. The secret message was transformed to Q-bits in this QKD (while conversion the side channel has been created). The Eavesdropper may be able to hack the data through this side channel without being detected by the receiver. As a result, the receiver will acknowledge receipt of the message to the sender.

The hacker can then easily retrieve the encrypted data using the traditional channel. To address this problem, the Shifting & Binary Conversion for Securing Data (SBSD) framework has been proposed to secure the data through the side channel. This framework has two goals such as shifting technology and binary conversions are two examples. To a greater extent, the proposed security model achieves good performance.

In future, this QKD along with side channel will be implemented in the cloud environment to secure the data in a real world.

Ethical Approval

Any of the authors' investigations with human participants or animals are not included in this article.

Funding

The authors declare that no finances, subventions, or other support were entered during the medication of this article.

Conflict of Interest

The authors have no applicable fiscal or non-financial interests to expose this article.

Informed Consent

Any of the authors' investigations with human participants or animals are not included in this article.

Authorship Contributions

Conceptualization: N.Gopinath ; Methodology: N.Gopinath ; Formal analysis and investigation: N.Gopinath, Dr.S.Prayla Shyry; Writing - original draft preparation: N.Gopinath ; Writing - review and editing: N.Gopinath ; Resources: N.Gopinath, Dr.S.Prayla Shyry ; Supervision: Dr.S.Prayla Shyry.

Data Availability

The datasets created during development and analyzed during this work can be found in the Image repository, http://www.vision.caltech.edu/Image_Datasets/Caltech101/ and Quantum bit repository, https://pure.strath.ac.uk/ws/portalfiles/portal/92638035/dataset.zip.

VI. References

1. Jian Li, Hengji Li, NaWang, Chaoyang Li, Yanyan Hou, Xiubo Chen, Yuguang Yang, "A QuantumKey Distribution Protocol Based on the EPR Pairs and its Simulation", International Conference on Simulation Tools and Techniques, Springer, pp. 288-301, vol. 295, 2019.
2. Zhuo Zhang, Guangyuan Fu, Fuqiang Di, Changlong Li, and Jia Liu, "Generative Reversible Data Hiding by Image-to-Image Translation via GANs", Security and Communication Networks, vol.2019, pp.1-11, 2019.
3. Qian-Ping Mao, Le Wang1, Sheng-Mei Zhao, "Decoy-state round-robin differential-phase-shift quantum key distribution with source errors", vol.19, no. 56 pp. 1-12, 2019.
4. Hoi-Kwong Lo (Hewlett-Packard, Bristol), H.F. Chau (Hong Kong, Chinese U.), "Security of Quantum Key Distribution", nature photonics, vol. 283, pp. 2050-2056,1999.
5. Jian Li, Yu-Guang Yang, Xiu-Bo Chen, Yi-Hua Zhou & Wei-Min Shi, "Practical Quantum Private Database Queries Based on Passive Round-Robin Differential Phase shift Quantum Key Distribution", Scientific Reports, pp. 1-6, 2016.
6. Li, Linguo Li, "Round Shujing robin differential quadrature phase shift quantum key distribution by using odd coherent states",Journal of Optik,, Vol. 227, Elsevier 2020.
7. Graeme Smith, "Private classical capacity with a symmetric side channel and its application to quantum cryptography", physical Review, vol. 78, no.2, 2008.
8. Zhen-Qiang Yin · Shuang Wang · Wei Chen·Hong-Wei Li · Guang-Can Guo · Zheng-Fu Han, Reference-free-independent quantum key distribution immune to detector side channel attacks" , Quantum Inf Process, 2014.
9. Bennet,Ch.H., Brassard.G., Quanum Cryptography "public key Distribution and coin tossing". IEEE conference on computer,systms,signalprocessing,1984,pp175-90.
10. MehrdadS,. Sharbad, "Quantum Cryptography : A New Generation of information technology security system" Published by IEEE Computer Society, Proceeding of the international conference on information technology: New Generation., p. 1644-1648.
11. Morio Toyoshima, Takayama, Yohikisa, WarnerKlaus,HirooKunimori.MikioFujiwara "Free space quantum cryptography with quantum and telecommunication channel"v. Science Direct. Volume 63, Issues 1–4, July–August 2008, Pages 179-184 8 feb 2008.
12. P.A.Shemina , Prof. vipinkumar K S, Prof. "E-Payment system using visual and quantum cryptography". Science Direct Procedia Technology 24 (2016) 1623 – 1628.
13. Mitch Leslio "Quantum Cryptography via satellite". 2017.
14. Mahdi H. A l Hasani Kais A. Al Naimee "Impact security enhancement in chaotic quantum cryptography", Volume 119, November 2019, 105575.

15. P. Siva Lakshmi , G. Murali "Comparison of Classical and Quantum Cryptography using QKD Simulator"International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017).
16. Stefano Pirandola, Stefano Mancini, Seth Lloyd Samuel , L. Braunstein "Eavesdropping of two-way coherent-state quantum cryptographyvia Gaussian quantum cloning machines"2009 Third International Conference on Quantum, Nano and Micro Technologies IEEE conference on computer society.
17. Sayantan Gupta, Kartik Sau, Jyotirmoy Pramanick, SwarnavaPyne, Rizwan Ahamed, Rahul Biswas "Quantum computation of perfect time-eavesdropping in position-based quantum cryptography: Quantum computing and eavesdropping over perfect key distribution" IEEE conference, 16-18 Aug. 2017.
18. Feihu Xu ; Marcos Curty ; Bing Qi ; Hoi-Kwong Lo,"Measurement-Device-Independent Quantum Cryptography", IEEEMeasurement-Device-Independent Quantum Cryptography,18 December 2014.
19. Yi Zhao ; Bing Qi ; Hoi-Kwong Lo,"Quantum key distribution with an untrusted source",IEEE publisher,2009 Conference on Lasers and Electro-Optics and 2009 Conference on Quantum electronics and Laser Science Conference,28 August 2009.
20. Z. Sakhi ; R. Kabil ; A. Tragha ; M. Bennai,"Quantum cryptography based on Grover's algorithm",IEEE,Second International ConferenCE,18-20 Sept. 2012.
21. Zbinden H, Gisin N, Huttner B, Muller A and Tittel W 2000 Practical aspects of quantum cryptographic key distribution J. Cryptol. 13 207–20
22. A. Ac´ın, J. Bae, E. Bagan, M. Baig, L. Masanes and R. Mu˜noz-Tapia, Secrecy content of two-qubit states, Phys. Rev. A 73 (2006) 012327
23. E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury, A proof of the security of quantum key distribution, Journal of Cryptology 19 (2006) 381–439.
24. C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68(21) (1992) 3121–3124.
25. D. Bruss, Optimal eavesdropping in quantum cryptography with six states, Phys. Rev. Lett. 81 (1998) 3018.
26. R. Canetti, Universally composable security: A new paradigm for cryptographic protocols, in Proc. 42nd IEEE Symp. Foundations of Computer Science (FOCS) (2001), pp. 136–145.
27. A. Winter, Coding theorem and strong converse for quantum channels, IEEE Trans. Inform. Theory 45(7) (1999).