International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 03 | Mar 2023 www.irjet.net p-ISSN: 2395-0072

Comprehensive Study of BB84, A Quantum Key Distribution Protocol

SujayKumar Reddy M[1], Sayan Mandal[2], Chandra Mohan B[3]

[1]*Student of Vellore Institute of Technology, India*
[2]*Student of Vellore Institute of Technology, India*
[3]*School of Computer Science and Engineering, Vellore Institute of Technology, India*

Abstract - *Quantum Key Distribution (QKD) is a technique that enables secure communication between two parties by sharing a secret key. One of the most well-known QKD protocols is the BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984. In this protocol, Alice and Bob use a quantum channel to exchange qubits, allowing them to generate a shared key that is resistant to eavesdropping. This paper presents a comparative study of existing QKD schemes, including the BB84 protocol, and highlights the advancements made in the BB84 protocol over the years. The study aims to provide a comprehensive overview of the different QKD schemes and their strengths and weaknesses and demonstrate QKD's working principles through existing simulations and implementations. Through this study, we show that the BB84 protocol is a highly secure QKD scheme that has been extensively studied and implemented in various settings. Furthermore, we discuss the improvements made to the BB84 protocol to enhance its security and practicality, including the use of decoy states and advanced error correction techniques. Overall, this paper provides a comprehensive analysis of QKD schemes, focusing on the BB84 protocol in secure communication technologies.*

Key Words: QKD (Quantum Key Distribution), Qubit (Quantum Bit), Quantum Cryptography.

1.INTRODUCTION

Quantum cryptography is a cutting-edge subfield of cryptography that leverages the principles of quantum mechanics to provide fundamentally secure communication between two parties. Classical cryptosystems are widely used for secure communication, but their vulnerability to sophisticated attacks has spurred the development of more advanced cryptographic techniques. Public key cryptosystems have been developed to address this issue, using a pair of keys for encryption and decryption, which allows for secure communication without the need for a shared secret key. However, even public key cryptosystems can be vulnerable to hacking attempts, which has led to the emergence of quantum cryptography.

Quantum cryptography is a secure communication method that uses the principles of quantum mechanics to distribute encryption keys. Unlike classical cryptographic quantum cryptography is based on the fundamental laws of physics and is therefore highly resistant to attacks by even the most advanced computing systems.

Quantum Key Distribution (QKD) is a secure communication protocol that utilizes the principles of quantum mechanics to distribute encryption keys. The fundamental principle behind QKD is that the act of measuring a quantum system will disturb its state, thus making any unauthorized interception of the key immediately detectable which maintains the confidentiality and integrity of communication. This ensures that the key distribution process is secure and any attempts to intercept the key will be detected.

According to Kalaivani et al [8], Quantum cryptography is often misleading to Quantum Key Distribution or vice versa, Quantum Cryptography uses the Heisenberg Uncertainty Principle and Principle of Photon Polarization [7], while Quantum Key Distribution uses Superposition and Quantum Entanglement principles [8].

1.1 Heisenberg Uncertainty Principle

The Heisenberg uncertainty principle is a foundational principle of quantum mechanics that arises from the wave-particle duality of quantum objects. It states that certain pairs of physical properties of a particle or system cannot be precisely measured simultaneously. This principle has important implications for quantum cryptography, which relies on the fact that any attempt to measure or intercept a quantum system carrying a secret key will inevitably disturb its state in a detectable way [9]. Eavesdropping on a quantum message is therefore akin to making a measurement, and the uncertainty principle ensures that any attempt to do so will leave a detectable signature, allowing legitimate parties to detect and prevent eavesdropping.

1.2 Quantum Superposition

Quantum superposition [1] is a fundamental principle of quantum mechanics that has been extensively studied and applied in various fields such as quantum computing and quantum cryptography. It describes the ability of quantum

particles to exist in multiple states simultaneously, and this property has been observed experimentally in numerous systems, ranging from photons to atoms and molecules. One example of quantum superposition is the famous Schrödinger's cat experiment, which has been extensively discussed in the literature. Gerry et al and Knight et al [2] provided a detailed mathematical interpretation of this experiment, showing that the cat is in a superposition state of both dead and alive until it is observed, at which point the wave function collapses into one of the two possible states.

1.3 Quantum Entanglement

In the realm of quantum mechanics, the phenomenon of quantum entanglement is observed when two or more particles become so strongly correlated that their states are interdependent, regardless of the distance between them. This phenomenon was referred to as "Spooky Action of Distance" by Einstein [4]. The unique nature of quantum entanglement ensures that no other system can be correlated to the entangled particles, making it a promising tool for secure communication [11]. The use of entanglement in communication protocols provides a means of detecting any attempts at eavesdropping, since any such attempt would result in a change to the entangled state that would be detectable to the communicating parties [10].

Yixuan et al [3] provide a comprehensive overview of the process of generating entangled photon pairs using the Spontaneous Parametric Down Conversion (SPDC) technique. They discuss the Highly Efficient Source of Photon Pairs based on SPDC in a Single-Mode Fiber (HSPS) method, which is often utilized as the source of photons in Quantum Key Distribution (QKD) systems. The entangled photons generated via the HSPS method allow for the creation of a shared secret key that is inherently secure. Any attempt to eavesdrop or intercept the photons would cause the entanglement to be destroyed, alerting the communicating parties to the presence of an attacker.

2. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a cryptographic technique that allows two parties to distribute a secret key using quantum mechanics principles. QKD protocols, such as BB84, decoy-based QKD, and phase differential shift QKD, have been developed to achieve secure key distribution. By utilizing quantum properties such as the uncertainty principle, QKD enables the generation of a shared secret key that cannot be intercepted without being detected, providing a high level of security for cryptographic communications.

3. BB84 Protocol

The BB84 protocol, devised by Bennett and Brassard in 1984, is a quantum key distribution (QKD) protocol that utilizes a combination of a quantum channel and an insecure classical channel which needs to be authenticated inorder to distribute a secret key between two parties. The protocol ensures the security of the key by detecting any attempts at eavesdropping on the quantum channel, thus providing a means of detecting any potential security breaches.

The BB84 protocol uses four quantum states that are randomly prepared by the sender, Alice, in one of two bases (rectilinear basis or diagonal basis) to transmit information to the receiver, Bob.

The four quantum states used in BB84 are:

1. $|0\rangle$ and $|1\rangle$ in the rectilinear basis (X-basis), where $|0\rangle = (1, 0)$ and $|1\rangle = (0, 1)$
2. $|+\rangle$ and $|-\rangle$ in the diagonal basis (Z-basis), where $|+\rangle = (1/\sqrt{2})(1, 1)$ and $|-\rangle = (1/\sqrt{2})(1, -1)$

The working principle of BB84 protocol is stated below with Alice and Bob.

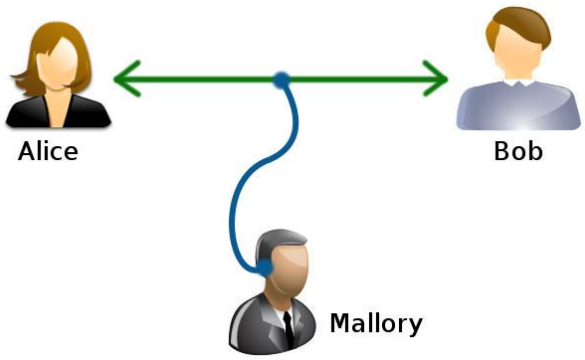

Figure 1: Alice, Bob and Mallory

QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			✓		✓			✓				✓		✓	✓
Presumably shared information			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					✓									✓	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Figure 2: Transmission from Alice to Bob without Mallory

Bases	0	1
+		
x		

Figure 3: Rectilinear and Diagonal Bases according to the Quantum Transmission

In Figure 1, we can see the communication process between Alice and Bob, with Mallory being the potential intruder who may attempt to intercept their communication. In Figure 2, as presented in [16], the transmission of bits between Alice and Bob can be observed, which ultimately leads to the generation of the Shared Secret Key, also known as the sifted key in QKD.

The BB84 protocol consists of the following steps:

1. Alice generates a random sequence of bits and encodes each bit into a randomly chosen polarization state using one of two bases: Rectilinear (R) or Diagonal (D).
2. However, when information is encoded in non-orthogonal quantum states, such as single photons with polarization directions 0, 45, 90, and 135 degrees according to the Figure[3].
3. Alice sends the encoded photons to Bob through the quantum channel.
4. Bob randomly chooses one of the two bases to measure the polarization of each photon he receives from Alice.
5. Bob measures each photon and records the results as either a 0 or a 1.
6. After the transmission, Alice and Bob publicly disclose the bases they used for each bit over the classical channel.
7. Alice and Bob discard the bits where the bases did not match.
8. The remaining bits form the sifted key.
9. To ensure the security of the key, Alice and Bob perform a test to detect any potential eavesdropping by comparing a subset of their sifted key over the classical channel.
10. Finally, they use error correction and privacy amplification techniques to extract a shorter, but secure, shared secret key.

In order to ensure the security of the key generated through the BB84 protocol, Alice and Bob perform a test to detect any potential eavesdropping. This is done by comparing a subset of their sifted key over the classical channel. The subset of the sifted key is randomly chosen by Alice and communicated to Bob over the classical channel. Bob then compares his own subset of the sifted key to the one communicated by Alice, and informs her of the results. If there is a high level of correlation between the two subsets, it indicates that there is no eavesdropper on the quantum channel, and the key is deemed secure.

However, if the subsets do not match, it indicates the presence of an eavesdropper, and the protocol is aborted. This test is known as the "privacy amplification" step, and is crucial in ensuring the security of the key distribution.

Finally, they use error correction and privacy amplification techniques to extract a shorter, but secure, shared secret key.

If Alice and Bob measured in same bases then the accuracy is 100 % or If Alice chooses Rectilinear bases and Bob chose Diagonal Bases and for each bases there are 2 possibilities of getting the exact bit sent by Alice so, the accuracy drops to 50%.

In summary, the BB84 protocol allows two parties to establish a shared secret key over an insecure channel by utilizing the principles of quantum mechanics and classical communication.

4. Related Work

The study done by Meyer et al and his colleagues [12] conducted a survey of the current state of research in quantum cryptography, with a specific focus on the BB84 protocol and the quantum bit commitment (QBC) protocol. The authors provided a detailed explanation of the working principle of the BB84 protocol and presented proofs for three concepts of "unconditional security" in quantum key distribution. These three concepts are the entanglement-based version of the protocol, the equivalent entanglement-based version, and a version where these two versions are shown to be equivalent. The QBC protocol was identified as an active area of research within quantum cryptography.

Sasirekha et al and Hemalatha et al [6] have conducted extensive research on Quantum Key Distribution (QKD) and its practical applications. Their work includes a detailed outline of the six critical steps involved in QKD, as well as proposed methods for detecting eavesdropping. These methods include measuring the polarization of photons, which cannot be done without disturbing the photon, and using entangled photons, which allows Alice and Bob to detect any interference or disturbance in the

protocol. The researchers also highlight the potential applications of QKD, including IoT and secure voting, as demonstrated by a case study in Switzerland [13].

Abushgra et al and Abdulbast et al conducted an extensive investigation[14] into multiple Quantum Key Distribution (QKD) algorithms, which included a comparison of the performance of the BB84 protocol with its various iterations, such as B92, SARG04 [15], KMB09, EPR, S13, and DPS. The study focused on the working principles of these algorithms and evaluated their effectiveness in detecting presence, polarization, state probability, qubit string, classical channel presence, decoy states, sifting phase, and different attacks in QKD. The results of the study showed that the BB84 protocol was vulnerable to some attacks.

Priyanka et al. [16] identified various limitations of the BB84 protocol, including the introduction of noise caused by imperfect detectors, technical difficulties in producing a perfectly single-photon pulse, inefficiency in generating the key, and the assumption that the subset of the total transmission will be used to generate the key. The paper also delves into the modifications made to the BB84 protocol, such as omitting the public announcement of bases, using multilevel encoding, implementing the decoy pulse method, and employing bi-directional QKD with practical faint pulses.

5. Recent Enhancements in BB84

In their study [17], the authors focused on improving the BB84 protocol using the polarization technique, which allows for the transmission of n-bit keys via photons without any loss of information. They proposed an enhanced BB84 protocol (EBB84) that eliminates the need for a classical channel by allowing the sender to randomly encode n-bit keys into photons and transmit them through a quantum channel. The receiver then generates the key using the same polarization, and both parties agree on the basis used for encoding and transmitting the key. The authors used simulations to compare the performance of the BB84 and EBB84 protocols in terms of execution time, key length parameter, and Quantum Bit Error Rate (QBER). The simulations were carried out on a computer with specific hardware and software specifications, and the results were presented in tables and figures.

In the study [18], the authors propose a modified version of the BB84 protocol to overcome security issues caused by various source imperfections, including state preparation flaws and side channels such as Trojan-horse attacks, mode dependencies, and classical correlations between emitted pulses. The proposed protocol exploits basis mismatched events and employs the Reference Technique, a powerful mathematical tool, to ensure implementation security. The authors also compare the achievable secret-key rate of the modified BB84 protocol with that of the three-state loss-tolerant protocol and demonstrate that adding a fourth state significantly improves the estimation of leaked information in the presence of source imperfections, resulting in better performance.

In their research [20], the authors introduce the BB84 protocol as the first quantum confidential communication protocol and propose a QKD network structure specifically designed for power business scenarios, which accounts for the complexity and diversity of power grid environments and communication transmission losses. To evaluate the performance of the QKD system, the study analyzes two tiers - the key tier, which focuses on factors that may affect the secret key rate in the quantum channel, and the business tier, which examines the transmission performance of the system when using a quantum virtual private network (QVPN) for encrypted transmission. The performance of the QKD device and QVPN is then tested in various simulated environments, providing insights into the system's suitability for large-scale applications.

The paper [21] delves into the security concerns and risks that arise when transmitting sensitive medical data through wireless body sensor networks (WBSNs). To mitigate these vulnerabilities, the paper proposes an enhanced BB84 quantum cryptography protocol (EBB84QCP) that uses a bitwise operator for secure secret key sharing between communicating parties. This approach avoids the direct sharing of keys through traditional methods like email or phone, which are susceptible to interception by attackers. The proposed protocol is demonstrated to be efficient in terms of the constrained resources of WBSNs and provides a robust level of security for transmitting sensitive information.

6. Existing Simulations and Results

The paper [22] proposes some existing simulations and we choose do simulations with this tool for different parameters.

6.1 SIMULATION - 1 [23]

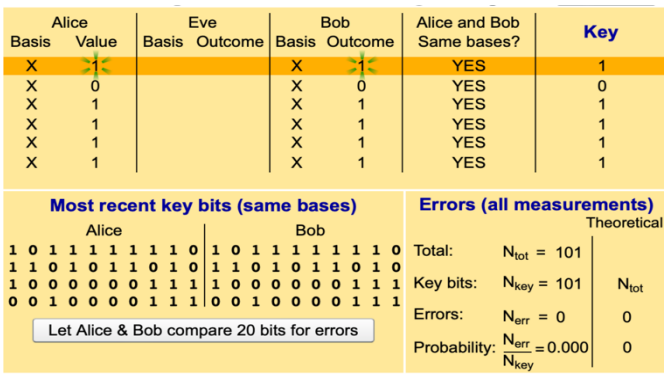

Figure 4: Alice and Bob have same bases(X)

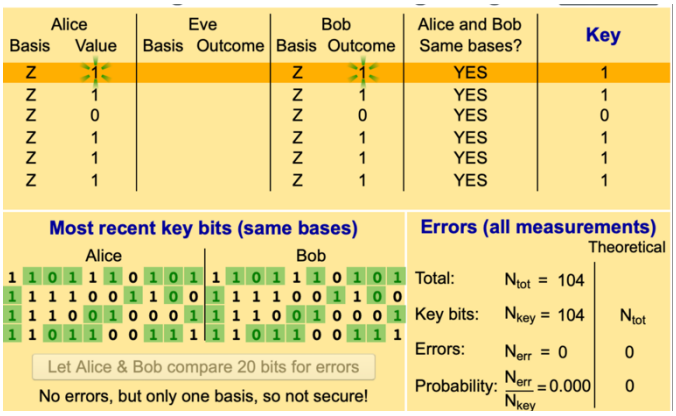

Figure 5: Alice and Bob have same bases(Z)

The figure [4] and [5] shows the experimental outcomes of utilizing X/Z bases for both Alice and Bob, which theoretically should yield zero error, are presented. However, this approach is considered insecure since it utilizes the same bases for both parties, and thereby allowing Eve to potentially possess the same bases and intercept the messages.

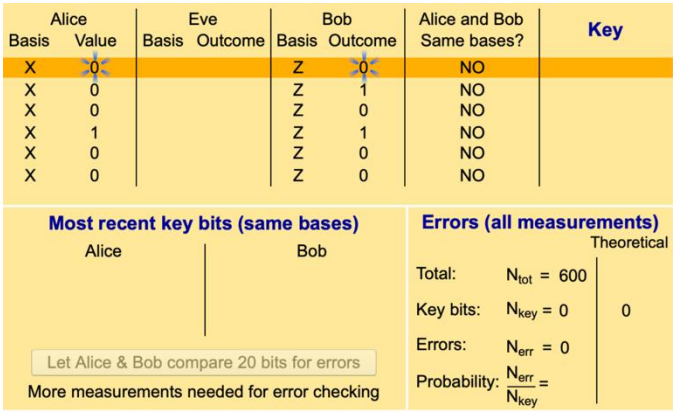

Figure 6: Alice(X) and Bob(Z) have different bases

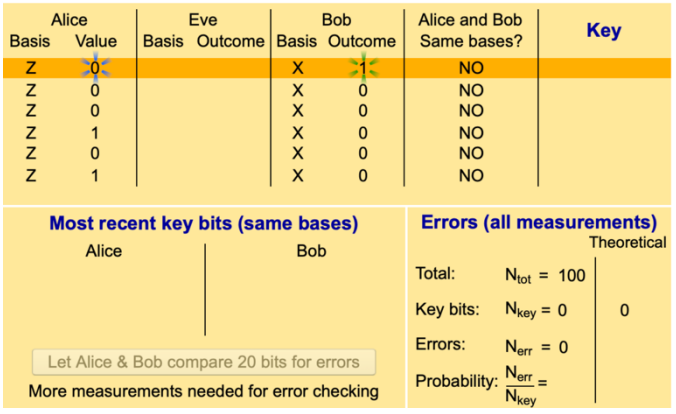

Figure 7: Alice(Z) and Bob(X) have different bases

The figures [6] and [7] indicate that there is no key generation when Alice measures in the X bases and Bob in the Z bases, irrespective of the parameters. However, this was based on a fixed orientation approach. To further explore the subject, we now investigate the outcomes of a random orientation approach.

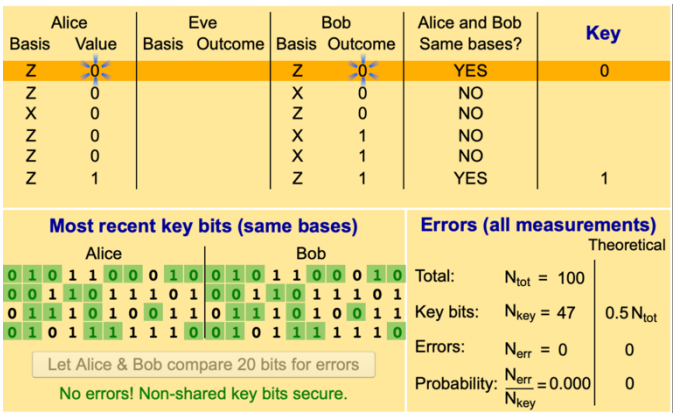

Figure 8: Alice and Bob have random orientation

Figure 8 illustrates that utilizing random bases provides enhanced security between Alice and Bob, as Eve is challenged to select the same basis as Alice.

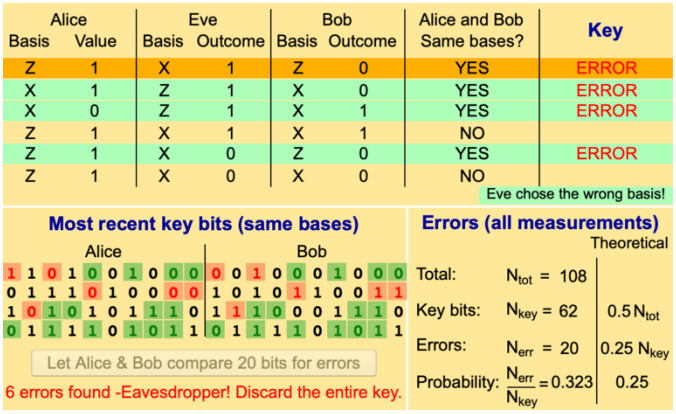

Figure 9: Alice and Bob have random orientation with Eve intercepting and resend particles

The presented data in Figure [9] illustrates the occurrence of an error, indicating a potential interception by Eve. As a result, it is recommended to discard the entire key to prevent any security breach.

6.2 QKDNetSim [24]

QKDNetSim is a network simulation platform that facilitates the implementation of Quantum Key Distribution (QKD) in existing networks. With the increasing complexity of QKD research, simulation technologies have become essential to assess the practical feasibility of theoretical achievements. QKDNetSim allows researchers to create

complex network topologies and conduct repeatable experiments, thereby saving time and costs associated with deploying a complete testbed.

The QKDNetSim utilizes the QKD-Key Management System (KMS) as the central entity to connect applications requiring cryptographic operations to the rest of the QKD network, following the standards set by ETSI004 [26] and ETSI014 [27]. Other components of the simulator include the QKD Key, QKD Buffer, QKD Encryptor, and QKD Post-Processing Application. Notably, QKDNetSim implements custom signalization for communication between two KMS, distinguishing it from other simulators [28].

One major advantage of QKDNetSim is the ability to analyze various attack scenarios, such as DDOS on KMS [25]. Furthermore, it is possible to integrate post-quantum techniques into QKDNetSim, opening up new possibilities for research and development in the field of quantum cryptography.

A basic Simulation is undergone for only with a Key Generator Layer and with QKD KMS as a default layer.

Table -1: Nodes Location for only Key Generator Layer

QKD Nodes		
Node s.no	**LOCATION**	**LAYER**
Node 1	MUMBAI	QKD-KMS Default
Node 2	DELHI	QKD-KMS Default
Node 3	NEAR TO MUMBAI	3-4 Key Generator Layer
Node 4	NEAR TO DELHI	3-4 Key Generator Layer

Table -2: Nodes Parameters for only Key Generator Layer

Layer	Nodes	Parameters
1-2 QKD KMS	Node 1 and Node 2	Key Size (BIT) – 512 PP Packet size – 100 OKD Stop Time – 50sec
3-4 Key Generator Layer	Node 3 and Node 4	Average size of consumed key-pairs (bits)-0 Average size of generated key-pairs (bits)-512 Key rate (bit/sec) 10811 Key-pairs consumed- 0 Key-pairs consumed (bits) - 0 Key-pairs generated-1055 Key-pairs generated (bits)-540160 Link distance (meters)-1441565 QKD Buffer Capacity (bits)-50000000 Start Time (sec)-0 Stop Time (sec)-50

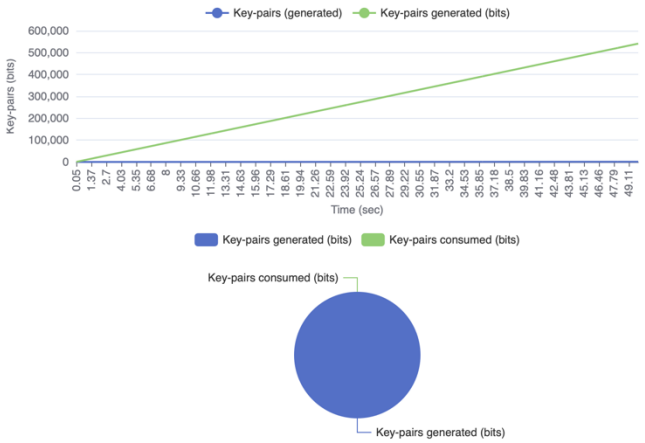

Figure 10: Key Generated Pairs for Key Generated Layer

Table-1 and Table-2 provide detailed information on the node locations, layers, and their corresponding parameters used in the QKDNetSim simulation. In addition, Figure [10] illustrates the statistics of generated key pairs and their storage in QKD buffers, as well as the consumption of key pairs from these buffers by Alice and Bob's QKD systems.

Table -3: Nodes Location for ETSI 014 and Key Generator Layer

QKD Nodes		
Node s.no	**LOCATION**	**LAYER**
Node 1	MUMBAI	QKD-KMS Default
Node 2	DELHI	QKD-KMS Default
Node 3	NEAR TO MUMBAI	3-4 Key Generator Layer
Node 4	NEAR TO DELHI	3-4 Key Generator Layer
Node 5	PUNE	5-6 Key Consumer Layer (ETSI 014)
Node 6	GWALIOR	5-6 Key Consumer Layer (ETSI 014)

Table -4: Nodes Parameters for ETSI 014 and Key Generator Layer

Layer	Nodes	Parameters
1-2 QKD KMS	Node 1 and Node 2	Key Size (BIT) – 512 PP Packet size – 100 OKD Stop Time – 50sec
3-4 Key Generator Layer	Node 3 and Node 4	Average size of consumed key-pairs (bits)- 487 Average size of generated key-pairs (bits)- 498 Key rate (bit/sec)- 100000 Key-pairs consumed- 2938 Key-pairs consumed (bits)- 1432256 Key-pairs generated- 11517 Key-pairs generated (bits)- 5735936 Link distance (meters)- 1410425 QKDBuffer Capacity (bits)- 50000000 Start Time (sec)- 0 Stop Time (sec)- 50
5-6 Key Consumer Layer ETSI 014	Node 5 and Node 6	**Key Consumption Statistics** Average size of consumed key-pairs (bits)- 464 Key-pairs consumed- 1500 Key-pairs consumed (bits)- 696000 **QKDApps Statistics** Authentication- SHA-1 Bytes Received- 154294 Bytes Sent- 154294 Encryption- OTP Key/Data utilization (%)- 74.91 Missed send packet calls- 251 Number of Keys to Fetch From KMS- 3 Packet Size (bytes)- 100 Packets Received- 749 Packets Sent- 749 Start Time (sec)- 10 Stop Time (sec)- 50 Traffic Rate (bit/sec)- 20000 **QKDApps-KMS Statistics** Bytes Received- 978368 Bytes Sent- 572684
		Packets Received- 1439 Packets Sent- 1439 **Signaling Statistics** Bytes Received- 365000 Bytes Sent- 365000 Packets Received- 1000 Packets Sent- 1000

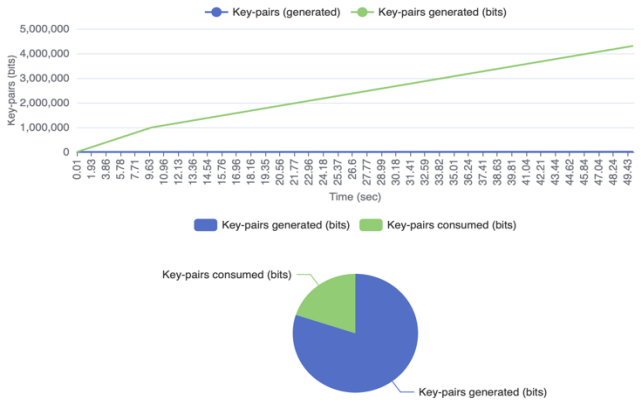

Figure 11: Key Generated Pairs for ETSI 014 and Key Generator Layer

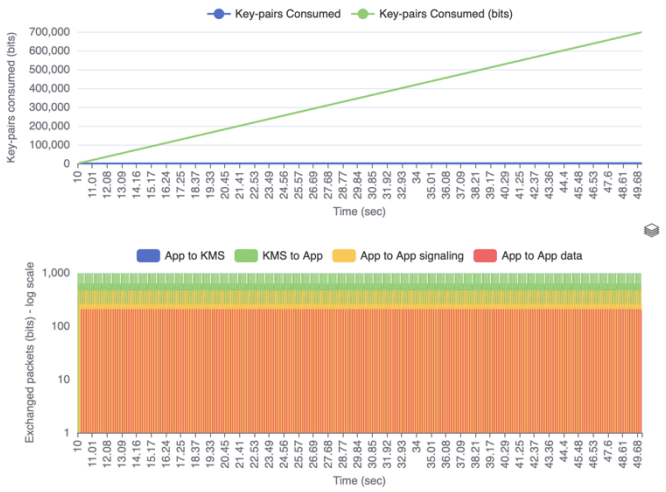

Figure 12: Key Consumer Layer ETSI 014 Statistics

Table-3 and Table-4 provide a comprehensive breakdown of the node locations, layers, and corresponding parameters utilized in the QKDNetSim simulation. Additionally, Figure [11] presents key statistics on the generation and storage of key pairs in the QKD buffers, as well as the consumption of key pairs by Alice and Bob's QKD systems. Figure [12] displays statistics on the Key Consumer Layer ETSI 014 with authentication type VMAC and encryption type One-Time Pad.

Table -5: Nodes Location for ETSI 004 and Key Generator Layer

QKD Nodes		
Node s.no	**LOCATION**	**LAYER**
Node 1	MUMBAI	QKD-KMS Default
Node 2	DELHI	QKD-KMS Default
Node 3	NEAR TO MUMBAI	3-4 Key Generator Layer
Node 4	NEAR TO DELHI	3-4 Key Generator Layer
Node 5	PUNE	5-6 Key Consumer Layer (ETSI 004)
Node 6	GWALIOR	5-6 Key Consumer Layer (ETSI 004)

Table-6: Nodes Parameters for ETSI 004 and Key Generator Layer

Layer	Nodes	Parameters
1-2 QKD KMS	Node 1 and Node 2	Key Size (BIT) – 512 PP Packet size – 100 OKD Stop Time – 50sec
3-4 Key Generator Layer	Node 3 and Node 4	Average size of consumed key-pairs (bits)- 512 Average size of generated key-pairs (bits)- 512 Key rate (bit/sec)- 100000 Key-pairs consumed- 1796 Key-pairs consumed (bits)- 919552 Key-pairs generated- 9767 Key-pairs generated (bits)- 5003456 Link distance (meters)- 1440197 QKDBuffer Capacity (bits)- 50000000 Start Time (sec)- 0 Stop Time (sec)- 50
5-6 Key Consumer Layer ETSI 004	Node 5 and Node 6	**Key Consumption Statistics** Average size of consumed key-pairs (bits)- 462 Key-pairs consumed- 1976 Key-pairs consumed (bits)- 914848 **QKDApps Statistics** Authentication- SHA-1 Bytes Received- 202910 Bytes Sent- 202910 Encryption- OTP Key/Data utilization (%)- 100 Missed send packet calls- 0 Packet Size (bytes)- 100 Packets Received- 985 Packets Sent- 985 Size of Key Buffer for Authentication- 6 Size of Key Buffer for Encryption- 1 Start Time (sec)- 10 Stop Time (sec)- 50 Traffic Rate (bit/sec)- 20000 **QKDApps-KMS Statistics** Bytes Received- 1978801 Bytes Sent- 1716638 Packets Received- 3964 Packets Sent- 3966 **Signaling Statistics** Bytes Received- 1812 Bytes Sent- 1812 Packets Received- 6 Packets Sent- 6

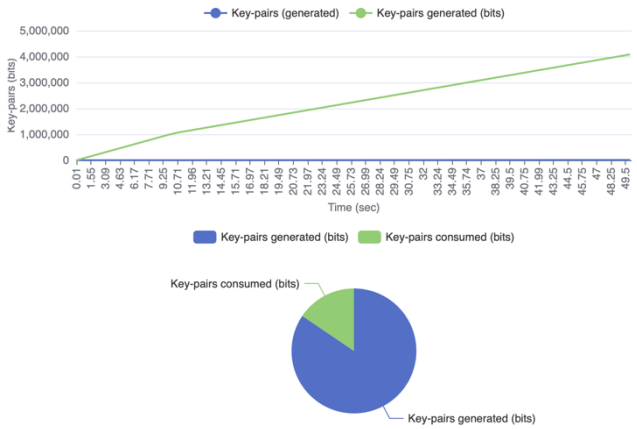

Figure 13: Key Generator Layer for ETSI004 and Key Generator Layer

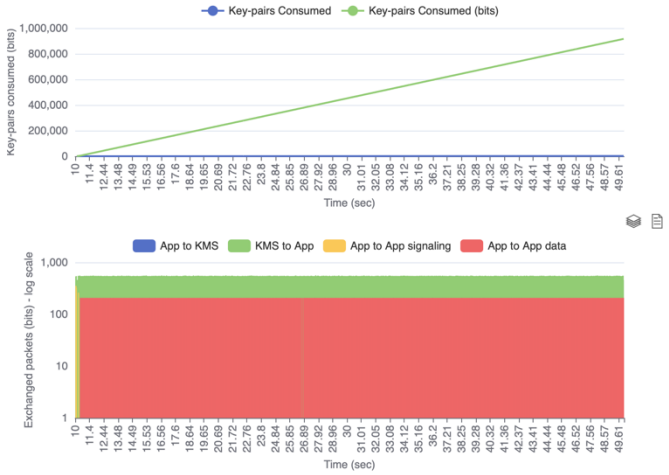

Figure 14: Key Consumer Layer ETSI004 Statistics

Table-5 and Table-6 provide a comprehensive breakdown of the node locations, layers, and corresponding parameters utilized in the QKDNetSim simulation. Additionally, Figure [13] presents key statistics on the generation and storage of key pairs in the QKD buffers, as well as the consumption of key pairs by Alice and Bob's QKD systems. Figure [14] displays statistics on the Key Consumer Layer ETSI004 with authentication type VMAC and encryption type One-Time Pad.

Table -7: Nodes Location for ETSI 004, ETSI 014 and Key Generator Layer

QKD Nodes		
Node s.no	**LOCATION**	**LAYER**
Node 1	MUMBAI	QKD-KMS Default
Node 2	DELHI	QKD-KMS Default
Node 3	NEAR TO MUMBAI	3-4 Key Generator Layer
Node 4	NEAR TO DELHI	3-4 Key Generator Layer
Node 5	PUNE	5-6 Key Consumer Layer (ETSI 004)
Node 6	GWALIOR	5-6 Key Consumer Layer (ETSI 004)
Node 7	Goa	5-6 Key Consumer Layer (ETSI 014)
Node 8	Kolkata	5-6 Key Consumer Layer (ETSI 014)

Table-8: Nodes Parameters for ETSI 004, ETSI 014and Key Generator Layer

Layer	Nodes	Parameters
1-2 QKD KMS	Node 1 and Node 2	Key Size (BIT) – 512 PP Packet size – 100 OKD Stop Time – 50sec
3-4 Key Generator Layer	Node 3 and Node 4	Average size of consumed key-pairs (bits)- 479 Average size of generated key-pairs (bits)- 498 Key rate (bit/sec)- 100000 Key-pairs consumed- 4902 Key-pairs consumed (bits)- 2351584 Key-pairs generated- 11519 Key-pairs generated (bits)- 5739488 Link distance (meters)- 1440197 QKDBuffer Capacity (bits)- 50000000 Start Time (sec)- 0 Stop Time (sec)- 50
5-6 Key Consumer Layer ETSI 004	Node 5 and Node 6	**Key Consumption Statistics** Average size of consumed key-pairs (bits)- 462 Key-pairs consumed- 1976 Key-pairs consumed (bits)- 914848 **QKDApps Statistics** Authentication- SHA-1 Bytes Received- 202910 Bytes Sent- 202910 Encryption- OTP Key/Data utilization (%)- 100 Missed send packet calls- 0 Packet Size (bytes)- 100 Packets Received- 985 Packets Sent- 985 Size of Key Buffer for Authentication- 6 Size of Key Buffer for Encryption- 1 Start Time (sec)- 10 Stop Time (sec)- 50 Traffic Rate (bit/sec)- 20000 **QKDApps-KMS Statistics** Bytes Received- 1978469

		Bytes Sent- 1716656 Packets Received- 3964 Packets Sent- 3966 **Signaling Statistics** Bytes Received- 1812 Bytes Sent- 1812 Packets Received-6 Packets Sent-6
7-8 Key Consumer Layer ETSI 014	Node 7 and Node 8	**Key Consumption Statistics** Average size of consumed key-pairs (bits)- 464 Key-pairs consumed- 1500 Key-pairs consumed (bits)- 696000 **QKDApps Statistics** Authentication- SHA-1 Bytes Received- 154294 Bytes Sent- 154294 Encryption- OTP Key/Data utilization (%)- 74.91 Missed send packet calls- 251 Number of Keys to Fetch From KMS- 3 Packet Size (bytes)- 100 Packets Received- 749 Packets Sent- 749 Start Time (sec)- 10 Stop Time (sec)- 50 Traffic Rate (bit/sec)- 20000 **QKDApps-KMS Statistics** Bytes Received- 978368 Bytes Sent- 572684 Packets Received- 1439 Packets Sent- 1439 **Signaling Statistics** Bytes Received- 365000 Bytes Sent- 365000 Packets Received- 1000 Packets Sent- 1000

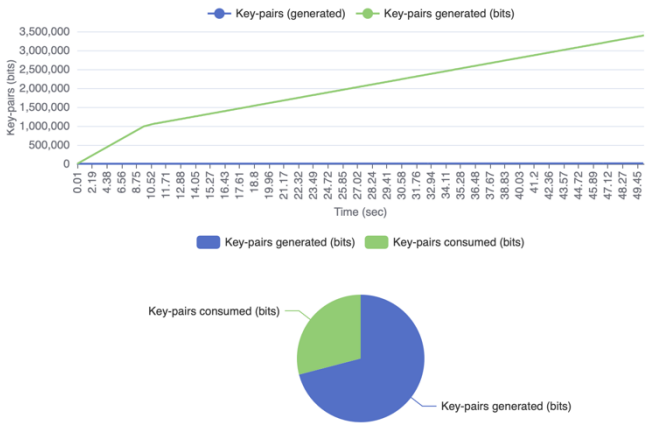

Figure 15: Key Generator Layer for ETSI 004, ETSI 014 and Key Generator Layer

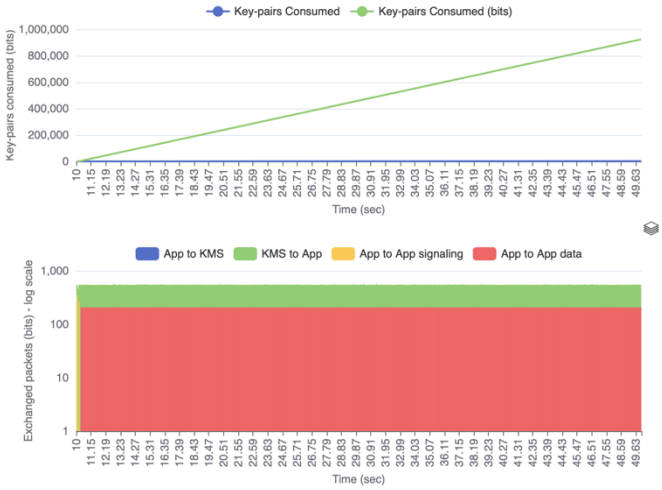

Figure 16: Key Consumer Layer for ETSI 004 Statistics

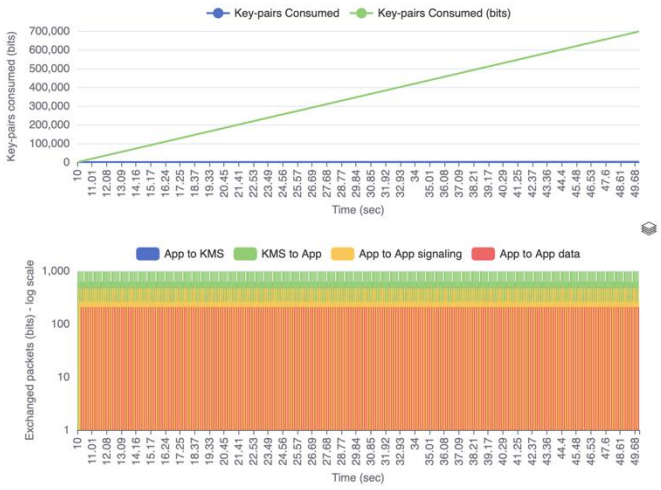

Figure 17: Key Consumer Layer for ETSI 014 Statistics

Table-7 and Table-8 provide a comprehensive breakdown of the node locations, layers, and corresponding parameters utilized in the QKDNetSim simulation. Additionally, Figure [15] presents key statistics on the generation and storage of key pairs in the QKD buffers, as well as the consumption of key pairs by Alice and Bob's QKD systems. Figure [16] displays statistics on the Key Consumer Layer ETSI 004 with authentication type VMAC and encryption type One-Time Pad. Figure [17] displays statistics on the Key Consumer Layer ETSI 014 with authentication type VMAC and encryption type One-Time Pad.

7. CONCLUSIONS AND FUTURE WORK

A comparative analysis in [14] reveals that BB84 protocol is susceptible to various types of attacks, including PNS, IRUD, BS, DoS, MAM, and IRA attacks. Therefore, research in enhanced BB84 protocol is still active, and integration of QKD protocols in IoT and real-time networks can be achieved by creating a key generation layer using the QKDNetSim simulation. The primary advantage of QKD is the provision of a secured shared key (SSK) through secure communication, and the key generated should be robust against attacks. Future research will include working with different QKD protocols, including post-quantum cryptography and lattice-based cryptosystems.

REFERENCES

[1] T. Forcer, A. Hey, D. Ross, and P. Smith, “Superposition, entanglement and quantum computation,” Quantum Information and Computation, vol. 2, no. 2, pp. 97–116, 2002.

[2] Gerry, C. C. & Knight, P. L. Quantum superpositions and Schrödinger cat states in quantum optics. Am. J. Phys. 65, 964 (1997)

[3] Li, Yixuan. "Methods of Generating Entangled Photon Pairs." Journal of Physics: Conference Series 1634, no. 1 (2020): 012172.

[4] Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? Physical review, 47(10), 777. DOI: 10.1103/PhysRev.47.777.

[5] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[6] Sasirekha, N., & Hemalatha, M. (2014). Quantum Cryptography using Quantum Key Distribution and its Applications. International Journal of Computer Applications, 101(18), 31-36.

[7] Aditya, J., & Shankar Rao, P. Quantum Cryptography. https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf

[8] Priyadharshini, S. P., & Kalaivani, J. (2018). A STUDY ON QUANTUM CRYPTOGRAPHY. International Journal of Pure and Applied Mathematics, 119(15), 3185-3191.

[9] National Institute of Standards and Technology (NIST). (2021, March 1). Cryptography in the Quantum Age. Introduction to the New Quantum Revolution. https://www.nist.gov/physics/introduction-new-quantum-revolution/cryptography-quantum-age

[10] Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. Reviews of Modern Physics, 81(2), 865-942. https://doi.org/10.1103/RevModPhys.81.865

[11] ETH Zurich Department of Physics. (2022, July 27). A key role for quantum entanglement: Breakthrough in experimental quantum cryptography. ScienceDaily. https://www.sciencedaily.com/releases/2022/07/220727124104.html

[12] Bruß, D., Erdélyi, G., Meyer, T., Riege, T., & Rothe, J. (2006). Quantum Cryptography: A Survey. Heinrich-Heine-Universität Düsseldorf.

[13] Castelvecchi, D. (2011). Swiss Test Quantum Cryptography. Scientific American. Retrieved from https://www.scientificamerican.com/article/swiss-test-quantum-cryptography/.

[14] Abushgra, A. A. (2020). Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review. Journal of Computer Networks and Communications, 2020, 1-16. doi: 10.1155/2020/6097468.

[15] Y. Zhou, X. Zhou and X. Li, "Performance of Scarani-Acin-Ribordy-Gisin protocol in quantum key distribution," 2010 2nd International Conference on Future Computer and Communication, Wuhan, China, 2010, pp. V2-96-V2-100, doi: 10.1109/ICFCC.2010.5497349.

[16] Priyanka M, and Urbasi Sinha. "Study of BB84 QKD protocol: Modifications and attacks." Summer Research Fellowship Programme of India's Science Academies. Indian Academy of Sciences, 2019,

http://reports.ias.ac.in/report/18088/study-of-bb84-qkd-protocol-modifications-and-attacks.

[17] Abdullah, A. A., & Jassem, Y. H. (2019). Enhancement of Quantum Key Distribution Protocol BB84. Journal of Computational and Theoretical Nanoscience, 16, 1–17.

[18] Pereira, M., Navarrete, Á., Mizutani, A., Kato, G., Curty, M., & Tamaki, K. (2022). Modified BB84 quantum key distribution protocol robust to source imperfections.

[19] Pereira, M., Kato, G., Mizutani, A., Curty, M., & Tamaki, K. (2020). Quantum key distribution with correlated sources. Science Advances, 6.

[20] Zhao, B., Zha, X., Chen, Z., Shi, R., Wang, D., Peng, T., & Yan, L. (2020). Performance Analysis of Quantum Key Distribution Technology for Power Business. IEEE Access, 8, 119733-119746.

[21] V AD, V K. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Pers Ubiquitous Comput. 2021 Mar 18:1-11. doi: 10.1007/s00779-021-01546-z. Epub ahead of print. PMID: 33758585; PMCID: PMC7971400.

[22] Kohnle, A. and Rizzoli, A. (2017). Interactive simulations for quantum key distribution. European Journal of Physics, 38(3), 035403. DOI: 10.1088/1361-6404/aa62c8.

[23] https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-bb84/Quantum_Cryptography.html

[24] Mehic, M., Maurhart, O., Rass, S. et al. Implementation of quantum key distribution network simulation module in the network simulator NS-3. Quantum Inf Process 16, 253 (2017). https://doi.org/10.1007/s11128-017-1702-z

[25] E. Dervisevic et al., "Simulations of Denial of Service Attacks in Quantum Key Distribution Networks," 2022 XXVIII International Conference on Information, Communication and Automation Technologies (ICAT), Sarajevo, Bosnia and Herzegovina, 2022, pp. 1-5, doi: 10.1109/ICAT54566.2022.9811238.

[26] ETSI GS QKD 004 V2.1.1 (2016-07) "Quantum Key Distribution (QKD); Security Requirements and EvaluationFramework". https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf

[27] ETSI GS QKD 014 V1.1.1: Quantum Key Distribution (QKD); Security Proof; Part 1: General, 2011. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

[28] P. Chowdhury, F. Hossain, and K. Mahmud, "A Comprehensive Review on Simulation of Quantum Key Distribution (QKD) Protocols," Simulation Modelling Practice and Theory, vol. 103, pp. 101996, 2020.

[29] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2001). Quantum Cryptography. arXiv. https://doi.org/10.1103/RevModPhys.74.145

[30] Wang, Xiang-Bin. "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography." Physical Review Letters, vol. 94, no. 23, 2005, p. 230503.