Simulation and Analysis of DL04 and Ping-Pong Quantum Secure Direct Communication Protocols using MATLAB and Simulink

Amanullah Bashir
Department of Physics,
COMSATS University Islamabad,
Pakistan

ABSTRACT

Quantum Secure Direct Communication (QSDC) enables the direct transmission of confidential information through quantum channels without requiring prior secret-key establishment. This paper presents a simulation-based study of two representative QSDC protocols: the DL04 protocol and the Ping-Pong protocol. A MATLAB/Simulink implementation of the DL04 protocol is developed to model quantum state generation, random phase preparation, message encoding, transmission, detection, and Quantum Bit Error Rate (QBER) evaluation under ideal channel conditions. Randomness is generated using a Binary Bernoulli Generator, providing statistically independent and reproducible bit sequences for quantum state preparation. In parallel, the Ping-Pong protocol is analyzed in MATLAB under different channel noise levels and eavesdropping scenarios using performance metrics such as fidelity, QBER, and Security Bit Error Rate (SBER). Results demonstrate the successful implementation of DL04 secuirity check with negligible QBER using binary Bernoulli generator in an ideal channel and illustrate the sensitivity of Ping-Pong communication to noise and attacks. The study provides a comparative understanding of practical single-photon and entanglement-based QSDC schemes and establishes a foundation for future experimental implementations.

Keywords

Quantum Secure Direct Communication, QSDC, DL04 Protocol, Ping-Pong Protocol, MATLAB, Simulink, Quantum Cryptography, QBER.

1. INTRODUCTION

With the rapid advancement of quantum computing, many conventional cryptographic systems face potential security risks. Classical public-key cryptographic algorithms rely on computational assumptions that may become vulnerable to future large-scale quantum computers. Quantum communication addresses this challenge by exploiting the fundamental laws of quantum mechanics to ensure information security.

Quantum Key Distribution (QKD)[1] enables secure key exchange between communicating parties; however, encrypted data must still be transmitted through classical channels. Quantum Secure Direct Communication (QSDC) [2] extends this concept by allowing confidential messages to be transmitted directly through quantum states without establishing a separate encryption key.

Among various QSDC schemes, the DL04[3] protocol offers practical implementation through single photons or weak coherent pulses, whereas the Ping-Pong protocol utilizes quantum entanglement for direct secure communication. This work investigates both protocols using simulation tools and analyzes their operational characteristics and security properties.

The main contributions of this work are:

- MATLAB/Simulink implementation of the DL04-QSDC protocol.
- Random quantum state preparation using a Binary Bernoulli Generator.
- Verification of DL04 operation under ideal channel conditions.
- MATLAB analysis of the Ping-Pong protocol under multiple noise and attack scenarios.
- Comparative evaluation of practical and entanglement-based QSDC techniques.

2. BACKGROUND

2.1 DL04 Quantum Secure Direct Communication Protocol

The DL04 protocol, proposed by Deng and Long, is one of the most widely studied QSDC protocols. Alice prepares quantum states and transmits them to Bob. After performing a security check on selected photons, Bob encodes secret information using unitary operations and sends the photons back to Alice for decoding. Security is evaluated through Quantum Bit Error Rate (QBER) measurements.

2.2 Ping-Pong Protocol



Figure 1 DL04 Protocol Workflow

The Ping-Pong protocol is an entanglement-based QSDC scheme that employs Bell states for secure communication. Information is encoded using unitary operations applied to one particle of an entangled pair. The receiving party performs Bell-state measurements to recover the message. Any unauthorized measurement disturbs the entangled state and can therefore be detected. [5]

The Bell state used in the protocol is

$|\Phi^+\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$

Depending on the message bit, unitary operations are applied to encode information before transmission.

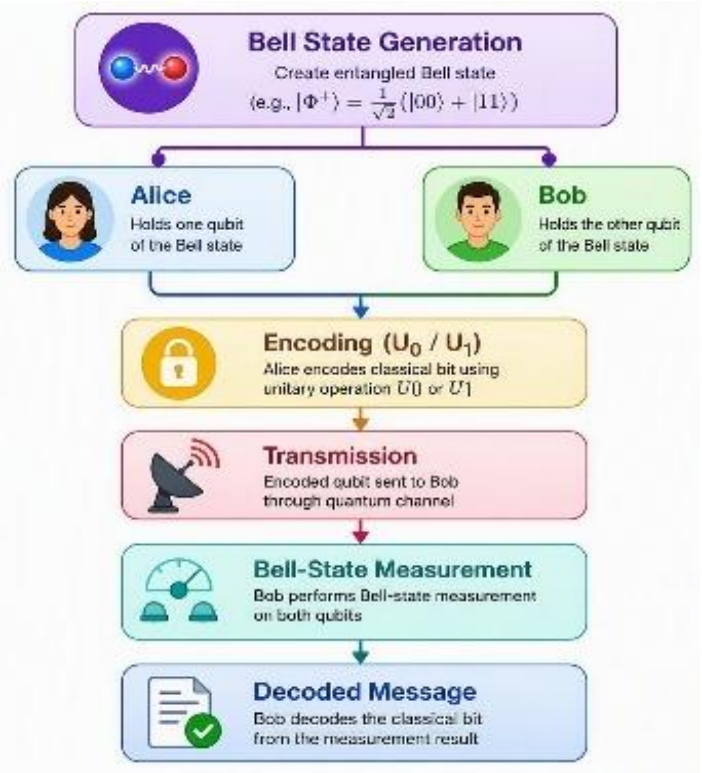


Figure 2.Ping-Pong Protocol Operation

3. SYSTEM IMPLEMENTATION

3.1 DL04 MATLAB/Simulink Implementation

The DL04 protocol was implemented in MATLAB Simulink as a modular discrete-time communication system. The model consists of five major subsystems:

1. Source Module
2. Quantum State Preparation Module
3. Quantum Channel Module
4. Detection Module
5. Post-Processing and QBER Module

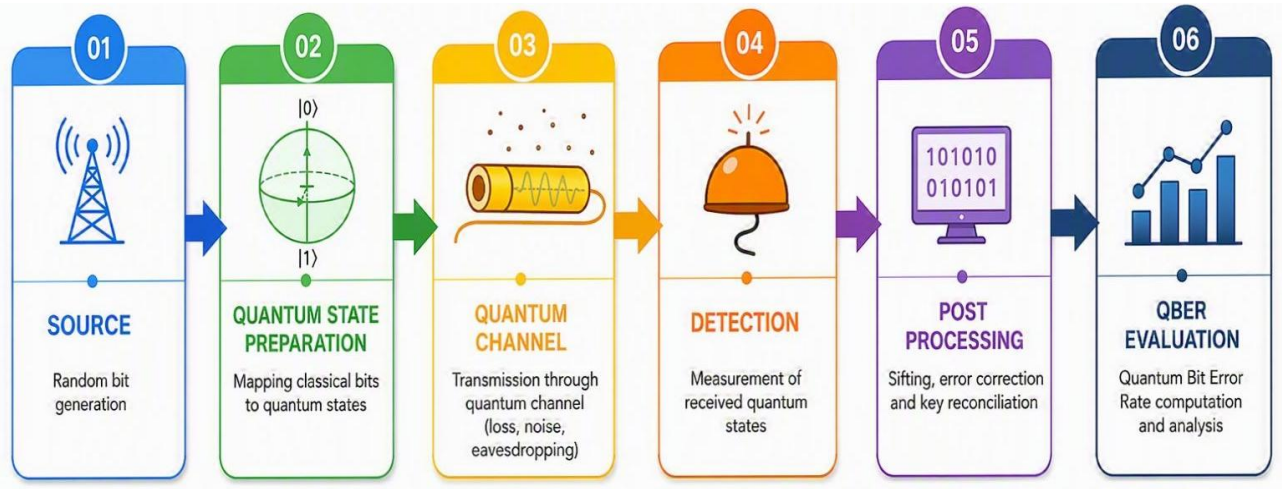


Figure 3.Overall DL04 Simulink Architecture

3.1.1 Source Module

A continuous-wave laser source is used to generate optical pulses.[3] The generated signals are attenuated using a Variable Optical Attenuator (VOA) to emulate weak coherent pulses suitable for quantum communication.

Implemented blocks include:

- Laser Source
- Variable Optical Attenuator
- Pulse Generator.

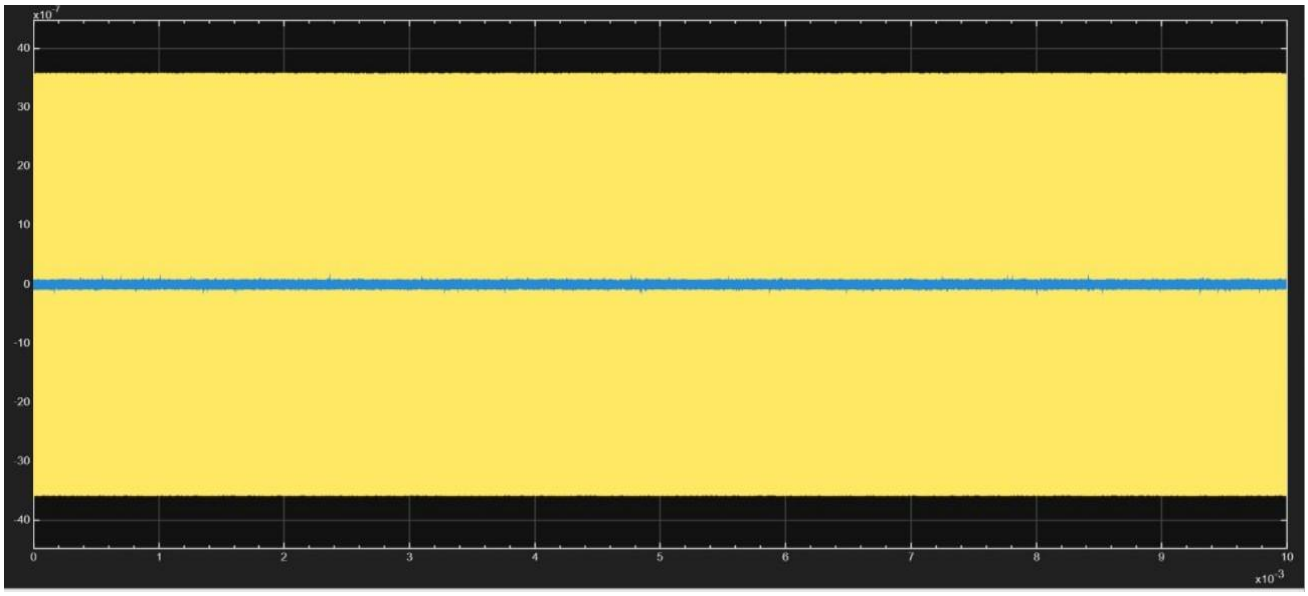


Figure 4.Energy Output after Laser

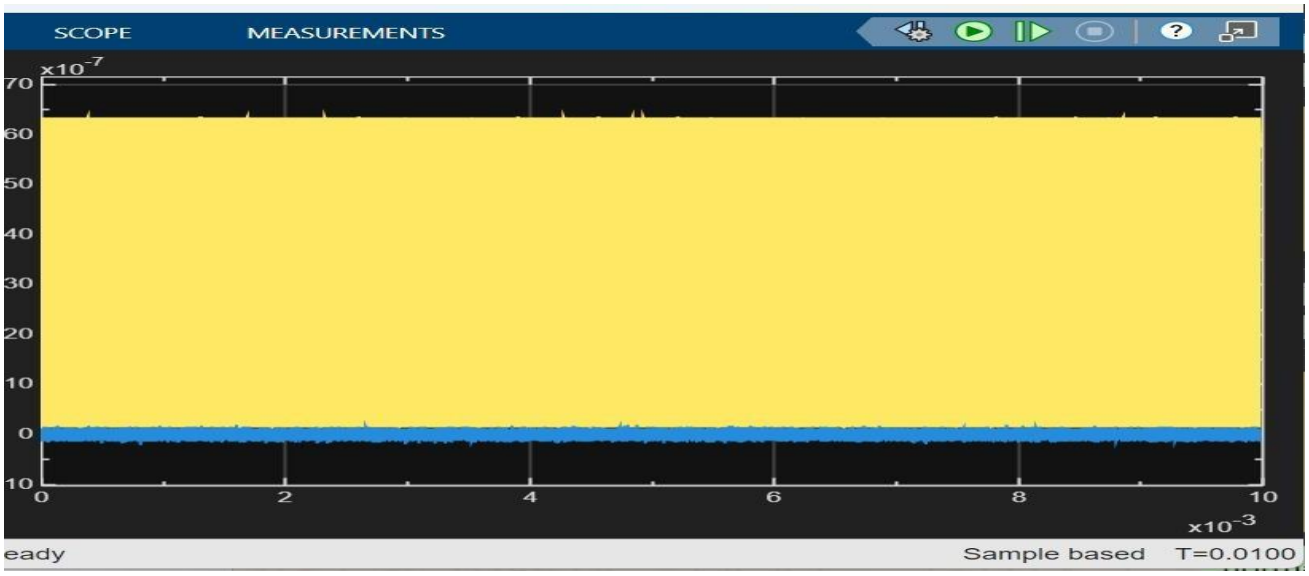


Figure 5 Energy Output after VOA

3.1.2 Quantum State Preparation Using Binary Bernoulli Generator

Randomness is one of the most important requirements in quantum communication. In this work, random bit generation is performed using the **Binary Bernoulli Generator** available in MATLAB/Simulink.

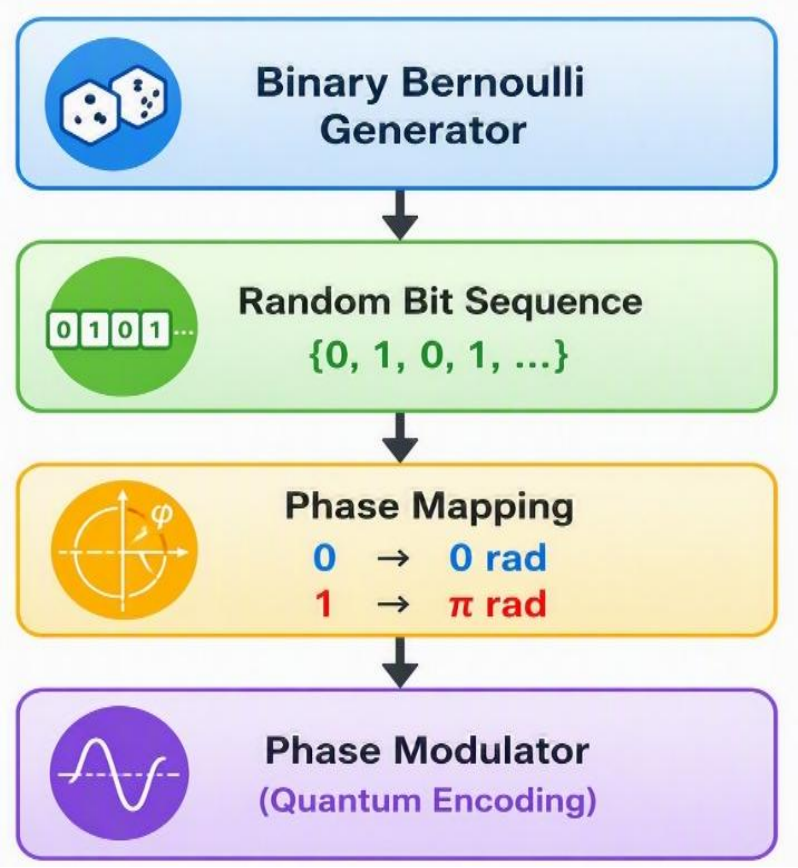


Figure 6.Use of Binary Bernoulli Generator

The generator produces statistically independent binary values according to:

[P(X=1)=0.5]

[P(X=0)=0.5]

These bits are mapped into quantum phase values:

Bit 0 is encoded as a phase shift of 0 radians.

Bit 1 is encoded as a phase shift of π radians.

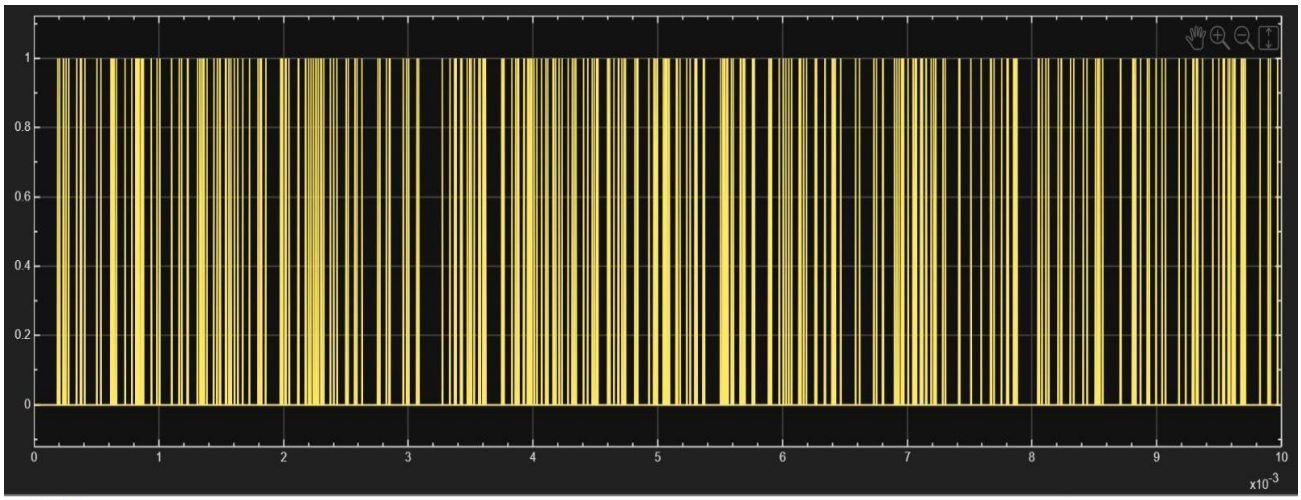
The generated phase sequence is applied through a phase modulation subsystem and stored for subsequent decoding at Alice's receiver.

Advantages of Binary Bernoulli Generator

The use of a Binary Bernoulli Generator offers several benefits for simulation-based studies:

- Direct integration into MATLAB/Simulink.
- Reproducible simulation results.
- Low computational overhead.
- Adjustable probability distributions.
- Easy interfacing with MATLAB Function blocks.

Compared with hardware-based True Random Number Generators (TRNGs), the Binary Bernoulli Generator provides a practical solution for simulation and debugging because experiments can be repeated under identical conditions. However, in real-world quantum communication systems, TRNGs or Quantum Random Number Generators (QRNGs) offer stronger unpredictability.



Statistics

MATLAB Function	Max	Min	Peak to Peak	Mean	Standard Deviation	Median	RMS
Time	193.1060 us	0.0000 s					
Value	1	0	1.0000	0.0001	0.0082	0.0000	0.0082

Figure 7. Random Phase Encoding using Binary Bernoulli Generator

3.1.3 Bob's Encoding Module

According to DL04-based QSDC schemes reported in the literature, Bob can encode information by manipulating the phase of the received quantum states. In differential phase encoding, a logical "0" is represented by preserving the existing phase relationship, whereas a logical "1" is represented by introducing a phase inversion between successive pulses. Such encoding enables information transmission through relative phase differences and can improve resistance to channel disturbances. Although differential phase encoding was studied as part of the theoretical framework of this work, its implementation was beyond the scope of the developed MATLAB/Simulink model and is proposed for future investigation.

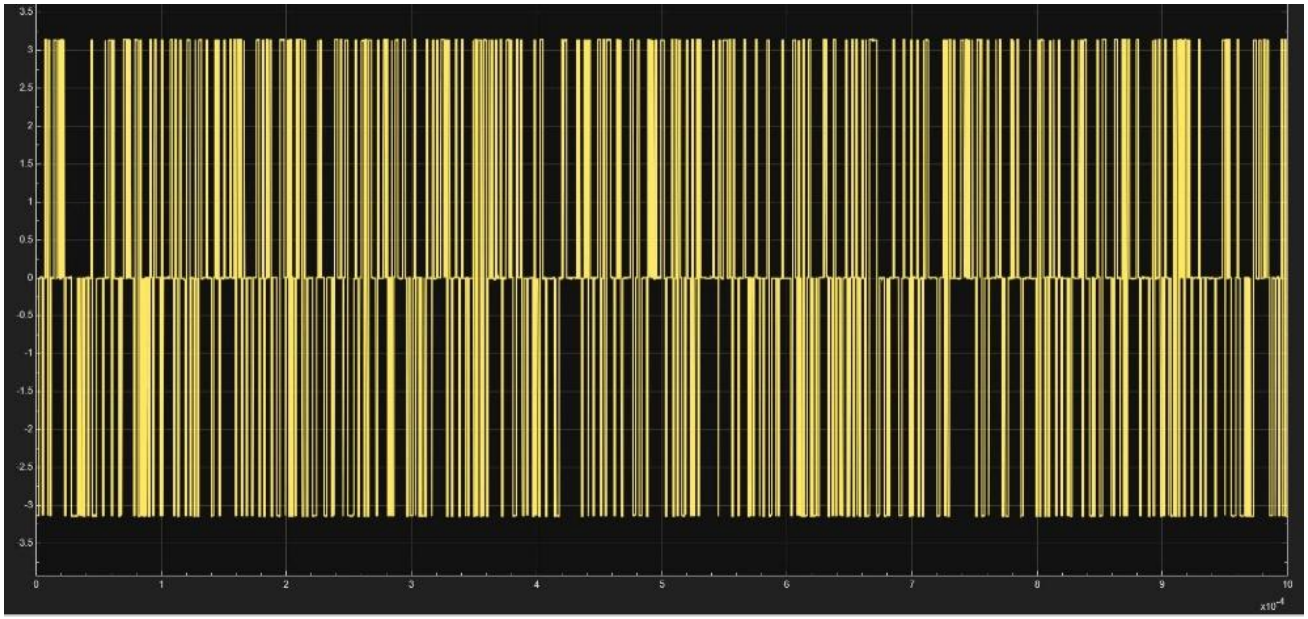


Figure 8. Output Phase After Phase Modulation

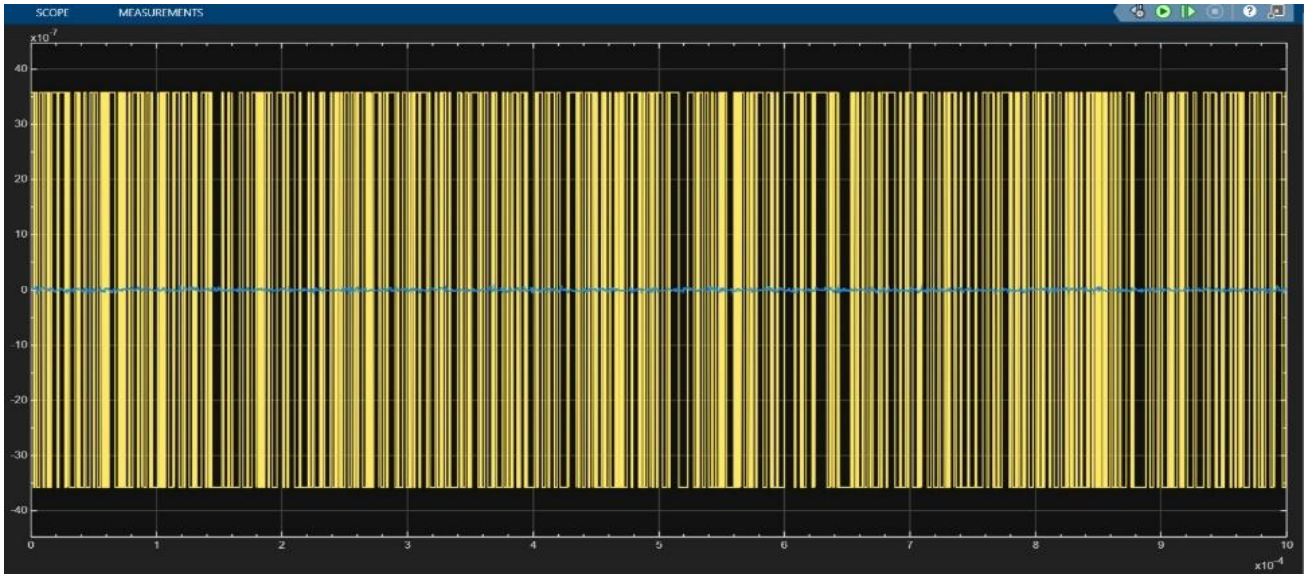


Figure 9.Output Energy After Phase Modulation

3.1.4 Quantum Channel Module

The implemented DL04 channel assumes ideal operating conditions:

- No attenuation
- No phase drift
- No dark counts
- No eavesdropping
- Perfect synchronization

The objective is to validate protocol operation before introducing realistic impairments.

3.1.5 Detection and Post-Processing

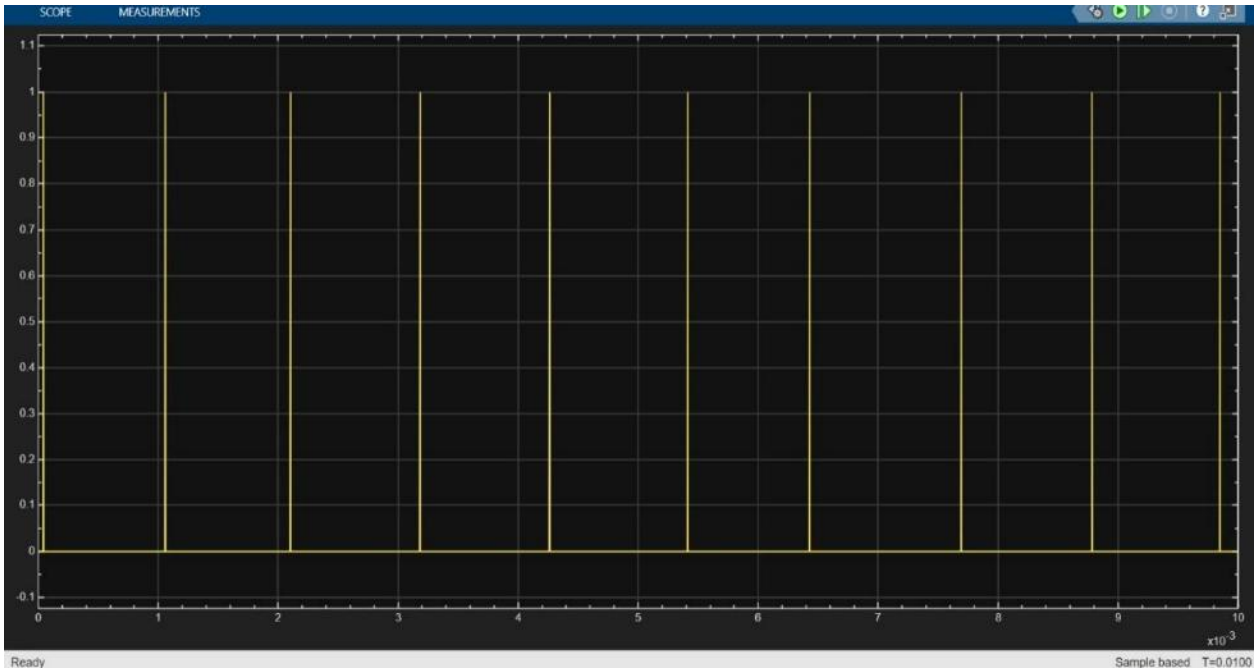


Figure 10.SPD Clicks at Bob's End

Detection is performed using Single Photon Detector (SPD) logic. The received quantum pulses generate SPD click events, which are recorded and used to determine the phase transitions observed at the receiver. In the implemented DL04 model, Alice stores a reference sequence by computing the XOR relationship between the current phase value and the previous phase value of the transmitted pulse sequence. This stored XOR pattern serves as the expected phase-transition reference for message recovery.

After transmission and detection, the sequence derived from SPD click events is compared with Alice's stored XOR sequence. Matching outcomes indicate correct transmission, while mismatches represent transmission errors. The Quantum Bit Error Rate (QBER) is then evaluated from the number of detected discrepancies between the two sequences:

QBER = N_error / N_total

Where:

•N_error = Number of mismatches between the SPD-derived sequence and the stored XOR reference sequence.

•N_total= Total number of evaluated bits.

This comparison process enables verification of transmission integrity and provides a quantitative measure of protocol performance under the simulated conditions. In the ideal-channel implementation developed in this work, the SPD results closely matched the stored XOR reference sequence, resulting in a QBER approaching zero and confirming correct protocol operation.

3.2 Ping-Pong MATLAB Implementation

The Ping-Pong protocol was implemented using MATLAB scripts to analyze its behavior under different operating conditions.

The simulation includes:

- Bell State Generation
- Classical-to-Qubit Mapping
- Unitary Encoding Operations
- Bell-State Measurement
- Noise Modeling
- Eavesdropping Scenarios

Performance metrics evaluated include:

- Fidelity
- QBER
- Security Bit Error Rate (SBER)

Multiple simulation runs were conducted for different:

- Noise levels
- Attack probabilities

Allowing comprehensive performance evaluation.

4. RESULTS AND DISCUSSION

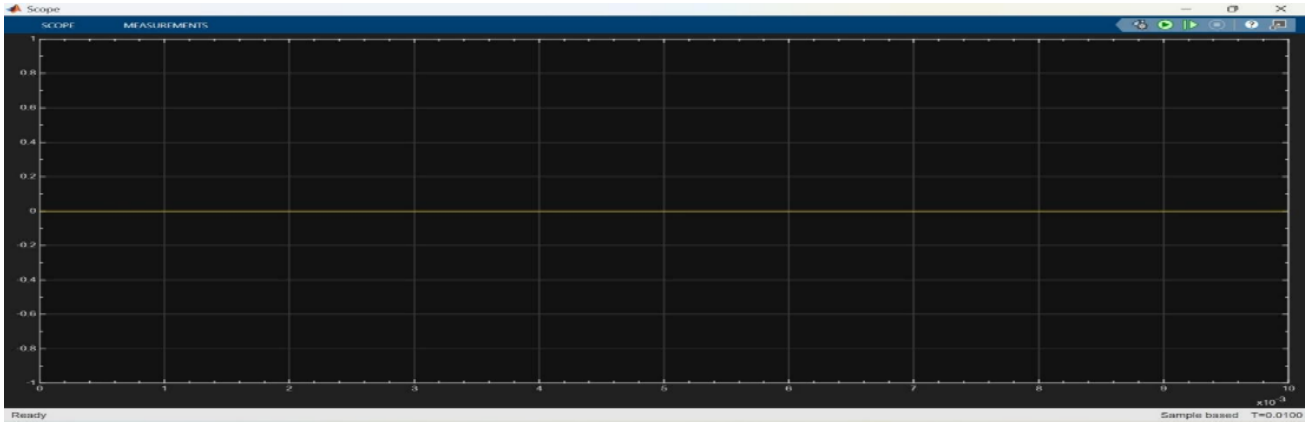


Figure 11. QBER Calculation.

4.1 DL04 Protocol Results

The DL04 implementation for qber check was evaluated under ideal channel conditions.

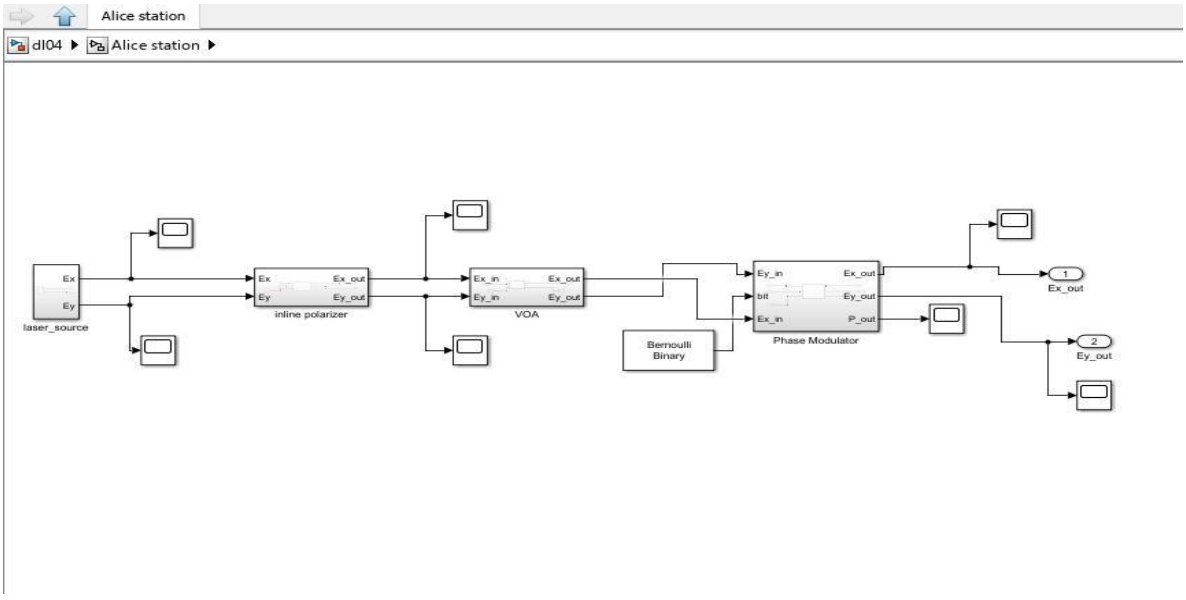


Figure 12 Alice Node Simulink Model

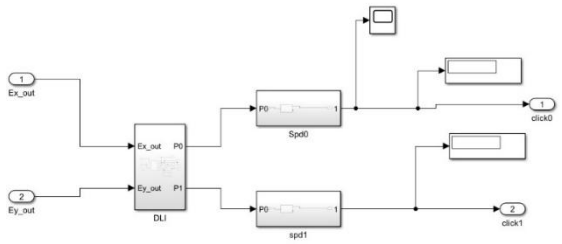


Figure 13 Bob Station Simulink Model

Results indicate:

- Successful weak coherent pulse generation.
- Correct random phase preparation.
- Quantum communication Feasibility check by qber estimation..
- Proper detector operation.

The calculated QBER remained approximately zero throughout the simulation, confirming correct implementation of protocol operations under ideal conditions.

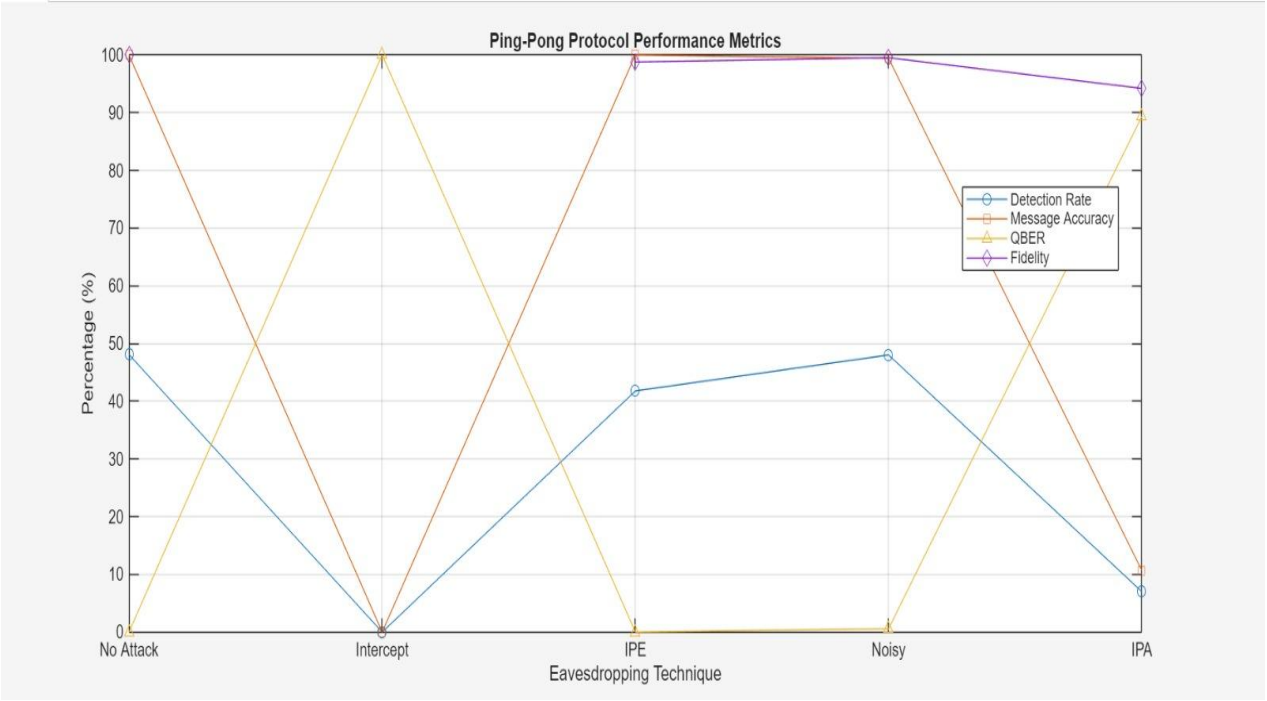


Figure 14.Performance Under Different Eavesdropping Attacks

4.2 Ping-Pong Protocol Results:

Simulation results demonstrate :

- Increasing eavesdropping activity causes degradation in communication reliability and security metrics.
- Increasing noise also degrades the quality of qubits being transmitted.
- A significant drop in accuracy to 50% was observed in no attack and ideal scenario because of the pobability that the qubits containing the messages are measured in right bases is dependent upon the number of states used in communication and if exact information about the basis are not transfered beforehand the receiving party uses basis randomly and in that complete scenario the message is decoded only if the combination of basis being received and the basis chosen by the receiving party for measurement fits right in otherweise the basis are lost so if we use two states for transmission the message accuracy decreases to 50%.

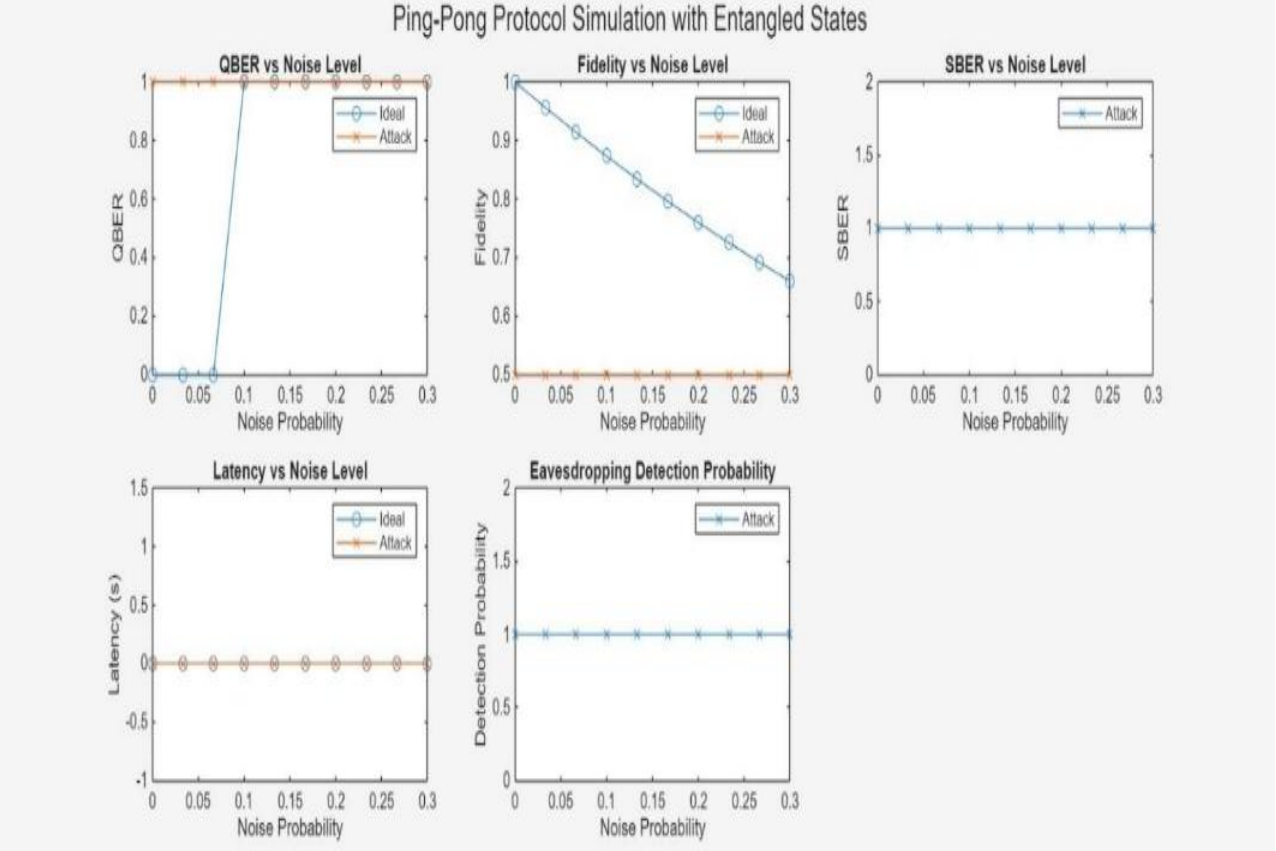


Figure 15.Performance Metrics with Increasing Noise

The following trends were observed:

- Fidelity decreases with increasing noise.
- QBER increases as channel conditions deteriorate.
- SBER rises in the presence of attacks.
- Communication reliability decreases under adverse channel conditions.

These results validate the theoretical security mechanisms of the Ping-Pong protocol and demonstrate its susceptibility to channel impairments while retaining eavesdropping detection capability.

4.3 Comparative Analysis

Table 1.Comparative Analysis of DL04 and Ping-Pong.

Parameter	DL04	Ping-Pong
Information Carrier	Weak Coherent Pulses	Entangled Qubits
Tool Used	MATLAB/Simulink	MATLAB
Randomness Source	Binary Bernoulli Generator	MATLAB Random Functions
Channel Studied	Ideal	Multiple Scenarios
Attack Analysis	Theoretical	Simulated
Complexity	Lower	Higher
Experimental Feasibility	Higher	Lower

The DL04 protocol offers a relatively practical implementation pathway due to its compatibility with weak coherent pulse sources and conventional optical components. In contrast, the Ping-Pong protocol provides deeper entanglement-based security but requires more sophisticated quantum resources.

5. CONCLUSION

This paper presented simulation-based investigations of two Quantum Secure Direct Communication protocols: DL04 and Ping-Pong. A MATLAB/Simulink implementation of the DL04 protocol was developed using a Binary Bernoulli

Generator for random quantum-state preparation and evaluated under ideal channel conditions. The results demonstrated successful message transmission with near-zero QBER, confirming the correctness of the implementation.

Additionally, the Ping-Pong protocol was analyzed under multiple noise levels and eavesdropping scenarios using MATLAB. The simulations showed that noise and attacks significantly influence fidelity, QBER, and SBER, while also enabling attack detection through disturbances in the communication channel.

The developed framework provides a practical platform for understanding QSDC systems and can be extended to include realistic channel impairments, advanced attack models, quantum random number generators, and future hardware implementations.

6. REFERENCES

[1] G. L. Long and X. S. Liu, "Theoretically Efficient High-Capacity Quantum Key Distribution Scheme," *Physical Review A*, vol. 65, 032302, 2002.

[2] D. Pan, G. L. Long, L. Yin, Y. B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, "The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, 2024

[3] S. Gupta, "Experimental Simulation of the Quantum Secure Direct Communication Using MATLAB and Simulink," *European Physical Journal Plus*, vol. 138, no. 913, 2023.

[4] J. Y. Hu et al., "Experimental Quantum Secure Direct Communication with Single Photons," *Light: Science & Applications*, vol. 5, e16144, 2016.

[5] G. L. Long and X. S. Liu, "Theoretically Efficient High-Capacity Quantum Key Distribution Scheme," *Physical Review A*, vol. 65, 032302, 2002.

[6] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," *Physical Review Letters*, vol. 89, no. 18, 187902, 2002.