An Efficient Way Of Secured Data Communication Through Classical Channels Via A Unique Quantum Key Distribution In A Photonic Quantum Computer

Mohanbabu Mani[1], Lakshmi Priya Keerthi Gurunathan[2], Ramesh Naidu Annavarapu[3]
[1, 2] Dept of Physics
[3]Associate Professor, Dept of Physics
[1, 2, 3] Pondicherry University

Abstract- *In the long run, Quantum Key Distribution (QKD) joins the race for developing efficient cryptographic algorithms, where it is a solution to communication over insecure channels. The necessity for postquantum cryptographic standards in the era of the evolution of Quantum Computers poses a challenge to the existing algorithms. The solution can be sought out in Quantum Computers by the encryption standards based on the laws of Quantum mechanics. Quantum Key Distribution is one solution to protect the integrity of data transmission, ensured by a series of steps that take care of the confidentiality and non-repudiation of information. An efficient Quantum Key Distribution is implemented in a Photonic Quantum Computer that is almost a room-temperature Quantum Computer. The transmission of data is accomplished by the fundamental laws of Bell's theorem and Quantum entanglement. The ultimate goal of this paper is to retrieve the binary data encoded with minimal loss through the channel created with the help of a circuit programmed in the Nano-photonic processor chip. The program executed the circuit successfully, and nominal bit error was achieved. The research aims to contribute to application in defense communications and future research on similar topics.*

Keywords- Photonic Quantum Computer, Quantum entanglement, Quantum Key Distribution, Quantum teleportation

I. INTRODUCTION

Quantum computing theory, initially proposed by Richard Feynman in 1982 as a notion, has been intensively studied and is widely considered a threat to asymmetric encryption standards. Furthermore, some quantum algorithms may impair symmetric cryptography; nevertheless, using bigger Key spaces can improve the security in symmetric cryptographic algorithms [1]. There are algorithms that can break current asymmetric cryptosystems whose security depends on the difficulty of factoring huge prime numbers and the discrete logarithm issue. Even elliptic curve cryptography, which is extensively a secure and efficient standard, looks vulnerable to quantum computers. As a result, encryption techniques resilient to quantum breakthrough becomes necessary.

The same principles that constitute quantum computers provides an explicitly secure solution to the Key distribution problem. The capacity to identify the existence of an adversary attempting to learn the key is present in Quantum Key Distribution (QKD), which is a novel feature in the world of cryptography. The scientific community has concentrated mainly on exploiting quantum mechanics to provide a safer key distribution algorithm using quantum cryptography. The evolution of Quantum Computers will likely affect current data encryption standards that protrude as the most secure algorithms to date [2]. A solution for classical cryptography becoming obsolete is to develop quantum algorithms that can withstand the impact of quantum computers solving the classical algorithms with arbitrary computing power.

II. LITERATURE SURVEY

A. *Quantum Cryptography*

Quantum computers can tackle quantum mechanical many-body problems that would be hard to solve on a conventional classical computer as the solutions on a conventional computer would take exponentially more extended time to calculate. However, all computations on a quantum computer can be completed in a finite time.

In 1994, Peter Shor proposed employing quantum computers to solve a vital issue in number theory, factorization. He demonstrated how an ensemble of mathematical operations created particularly for a quantum computer might be constructed to allow such a machine to factor enormous numbers far quicker than conventional computers can. With this accomplishment, quantum computing went from a simple academic curiosity to a worldwide fascination [3].

The variety of physical platforms accessible in today's quantum computers is particularly notable: superconducting qubits, trapped ions, photonics, quantum annealers, semiconductor qubits, and Rydberg atoms are already being studied as paradigms for creating quantum computers. Several of these methods have been researched for decades, while others have only recently been identified [4].

According to recent theoretical studies, a Quantum Computer can solve computationally complex problems like factoring numbers and searching databases quicker than a conventional computer [5].

Secret or symmetric key cryptography and public key cryptography, also known as asymmetric cryptography, are the two primary disciplines of classical cryptography. Key distribution systems based on public key cryptography, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Diffie-Hellman, are commonly used to establish a secret key via an insecure channel [6]. Unlike public key cryptography, secret key cryptography does not need to establish a shared secret key prior to communication. Instead, each participant has a private key that is kept confidential and a public key that they may freely disseminate. While the key exchange is unnecessary, the security of symmetric key cryptography techniques is presently reliant on the untested premise that these difficulties, such as integer factorization or the discrete logarithm problem, are challenging [7]. This indicates that advancements in computing power or the discovery of efficient techniques to tackle the underlying difficulties might make public key cryptography algorithms susceptible. On a quantum computer, algorithms for integer factorization and finding solutions for the discrete logarithm problem in polynomial time have already been developed [5].

B. Quantum Key Distribution

The fundamental concept for Quantum Key Distribution (QKD) protocols entails two parties, Alice, and Bob, who want to exchange a key having access to both a classical communication channel and a quantum communication channel. Eve, an eavesdropper, is believed to have exposure to both channels, but no conclusions were drawn regarding the resources available to Eve.

As stated in the Heisenberg Uncertainty Principle, who was originally referring to a particle's location and momentum, indicated how every measurement of a particle's position would upset its conjugate attribute. As a result, knowing both qualities with confidence at the same time is impossible. This concept can be influenced by quantum cryptography; however, the conjugate attribute is usually the polarisation of photons on distinct bases. The reason for this is because photons can be transferred across fibre optic networks, making them one of the most feasible quantum systems for sending and receiving data [8].

The principle of quantum entanglement is another essential premise on which QKD might be founded. Quantum teleportation is the method of communicating via entangled states with the use of a classical information channel, and it is the foundation of Eckert's protocol.

To explore QKD, we need to understand some Quantum mechanical phenomena.

C. Qubits

A quantum computer's primary unit of information is called a quantum bit or qubit, which is comparable to the classical bit used on regular computers but is more complex. The qubit systems can effectively implement quantum algorithms because the foundational parallelism of computation and extensive storage of information is possible, either according to the Bloch Sphere concept or otherwise, because each state (ψ_n) (Equation 1) is independent of the others and therefore can be used in the computation and storage of information [3].

$$\psi = \Sigma\, a_n\, \psi_n \quad \Sigma \mid a_n \mid^2 = 1 \qquad (1)$$

Where $(\psi(n))$ are the eigen states, n = (1,2,3,4…).

D. *Superposition*

The qubit feature directly results from the qubit's adherence to quantum motion principles. A qubit can occur not only in the states relating to the logical states 0 and 1, as in a classical logic bit but also states corresponding to a mix of all those classical states. In other words, a qubit can be a 0, 1, or both 0 and 1 simultaneously, with a numerical coefficient reflecting the likelihood of each state.

A single photon beam can be employed, with the overall state being a polarisation state, which can be horizontal or vertical about a particular axis. As a result, a qubit can have two values: 0 or 1, which correspond to both eigenstates of a single electron's spin. Because the general state of a qubit may be defined as a vector in the two-dimensional complex space c_2 and the two states constitute the basis of the representation, the state is the superposition of two states having arbitrary complex coefficients.

If a photon is emitted along a path that leads to a half-silvered mirror, it's mirrors divides the light, sending half vertically to detector A and half horizontally to detector B [9].

However, because a photon signifies a single quantised energy level $(E = h(\nu))$ that cannot be separated, it is observed to have equal probability at both A and B [10]. Quantum mechanics forecasts that the photon travels both directions simultaneously, only collapsing to one path upon measurement, i.e., wave function collapse. The linear superposition of the various photon states of prospective routes causes a phenomenon known as single-particle interference.

E. *Quantum Entanglement*

The Einstein, Podolsky, and Rosen (EPR) paradox is a well-known occurrence where they contended that quantum mechanics is just an incomplete theory and not plausible because of its odd entanglement behaviour.

Consider the ground state of a Helium atom. It consists of two electrons with quantum numbers of n=1, l=0, s=1/2, s_z= +1/2 for one and s_z = -1/2 for the other. Consequently, we have j = 0 and 1, $j_z = s_z1 + s_z2 = 0$. As a result, only the j=0 state is permitted. Two electrons in a Helium atom are antiparallel to each other, forming an entangled pair of systems [11].

Quantum Entanglement permits qubits separated by enormous distances to communicate with one other instantaneously, without being constrained by the speed of light. As long as the associated particles are separated, they will stay entangled regardless of their distance of separation. Quantum superposition and entanglement, when combined, result in significantly increased computer capability [12].

F. *Quantum Teleportation*

In classical physics, an entity can be teleported by conducting a measurement to thoroughly characterise the object's attributes, and then sending that information to another place and reconstructing the entity. The greatest number of distinct messages that may be sent if a signal is sent using an item that can be placed into one of N identifiable states is N.

Only two polarisation states are distinct in a single photon: left and right sided. As a result, a single photon can only carry two distinct messages, or one bit of information. Quantum physics enables the creation of qualitatively new logic gates, perfectly secure cryptosystems that integrate telecommunication and cryptography, the compression of two bits of info into one physical bit, and a form of teleportation [13].

A fascinating method for teleporting quantum states utilising EPR states, or entangled states (Equation 2). Abstractly, quantum teleportation may be expressed in the form of two particles, A and B. A has an unknown state in its possession$(|\psi\rangle)$.

$$|\psi> = \alpha|0> + \beta|1> \qquad (2)$$

The goal of teleportation is to move the state $(\psi\rangle)$ from entity A to B. Entangled states are used to accomplish this.

$$|\psi> (\{|0>\}A\{|0>\}B) + \{|1>\}A\{|1>\}B) \quad (3)$$

Both A and B have one qubit from the two-qubit entangled system (Equation 3). For the first two qubits, the state may be recast in the Bell basis, and for the final one, an implied unitary transformation of the state $(|\psi\rangle)$ can be used.

$$(|00> + |11>)|\psi> + (|00> - |11>)\sigma\_Z|\psi> + (|01> + |10>)\sigma\_X|\psi> + (|01> - |10>)(-i\sigma Y|\psi>) \qquad (4)$$

$(\sigma_X), (\sigma_Y), (\sigma_Z)$ are the Pauli matrices in $(|0>, |1>)$ basis.

In the Bell basis, a measurement is performed on A's qubits. B's states are $(|\psi>), (\sigma_z|\psi>), (\sigma_X|\psi>), (-i\sigma_z|\psi>)$depending on the results of these measurements (Equation 4). A communicates the result of its measurement to B, who may subsequently restore the original state $(|\psi>)$ by using the appropriate unitary transformation I, $(\sigma_z), (\sigma_Y)$ or $(i\sigma_Y)$ depending on the result of A's measurement [13].

G. Eckert's protocol

Artur Eckert proposed a new method for distributing quantum keys, in which the key is disseminated using quantum teleportation. Eckert outlines a channel in which a single source emits entangled pairs of particles, which might be polarised photons. The particles are divided, and each pair gives Alice and Bob one particle. To quantify their received particles, Alice, and Bob each would select a random basis. Due to the notion of quantum entanglement, Alice and Bob should predict opposite outcomes for any measurement when they used the same bases [14].

H. Integrated Nanophotonic Quantum Processor

Nanostructured silicon nitride waveguides are used in the nanophotonic chip. These chips are made with the same lithographic technology that is used to create traditional computer processors.

Encoding information on-chip provides for a high level of control and stability over the optical phases used to train algorithms in the device. Laser pulses sent into the chip's left side provide electricity. It creates a programmable quantum state, which is subsequently coupled out of the device and delivered to photon counting detectors [15].
Traditional coherent state laser pulses are pumped into the chip through optical fibres and distributed coherently to power four distinct squeezer devices. At their output waveguides, the squeezers, which are based on micro-ring resonators, individually create a two-mode squeezed vacuum (TMSV) state. Squeezed states are a significant quantum resource that introduce quantum entanglement. Each one of these 4 TMSV states has two modes that correspond to different optical wavelengths, each of the 4 copies being formed in a different spatial mode. The traditional laser pump light is separated from the compressed light by a filtering step. For monitoring, the pumping light is diverted away from the chip. A configurable four-mode interferometer receives the compressed light. When sending the quantum task, the stages of the interferometer are supplied directly from backend platform. The eight-mode programmable Gaussian state that results is then connected off-chip to photon number-resolving sensors for Fock basis readout [16].

I. *Continuous Variable Model*

The CV model is well-suited to modelling bosonic systems like as electromagnetic fields, harmonic oscillators, phonons, Bose-Einstein condensates, or opto-mechanical resonators, as well as situations including continuous quantum operators like position and momentum. The bosonic harmonic oscillator is the simplest basic CV system, characterised by the canonical mode operators $(\hat{a}) and (\hat{a}^{\dagger})$.

The well-known commutation relation $(\hat{a}), (\hat{a}^{\dagger}) = I$, is satisfied by these. Working with quadrature operators is also prevalent.

$$\hat{x}: = \sqrt{\hbar}/2\,(\hat{a} + \hat{a}^{\dagger}) \qquad (5)$$

$$\hat{p}: = -i\sqrt{\hbar}/2\,(\hat{a} - \hat{a}^{\dagger}) \qquad (6)$$

The Hermitian as well as anti-Hermitian components of the operator $\hat{a}$ are proportional to these self-adjoint operators (Equation 5). As a single wire in a quantum circuit, we may imagine a fixed harmonic oscillator mode inside an optical fibre as well as waveguide on a photonic device [17].

The basic ingredient in both CV quantum computation and the qubit model is, qumodes in CV and qubits in the qubit model. Quadrature $(\hat{x}, \hat{p})$ and Mode operators $(\hat{a}), (\hat{a}^{\dagger})$ for CV (Equation 6) and Pauli operators $(\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)$ for Qubit models are relevant operators. For CV common states include coherent states $(|\alpha>), \text{squeezed states}(|z>)$, and number states $(|n>)$ and Pauli eigenstates $(|0/1>, |\pm>, |\pm i>)$ for Qubit models.

III. METHODS AND MATERIALS

Coherent state laser pulses are pumped into the chip through optical fibres and distributed coherently to power four different squeezer devices.

Squeezed states are a significant quantum resource that introduces quantum entanglement. A configurable four-mode interferometer receives the compressed light. The interferometer stages are supplied directly from Strawberry Fields when sending the quantum task. Strawberry Fields is an open-source photonic quantum computing architecture used to construct and simulate quantum photonic circuits with continuous variables [16]. The eight-mode programmable Gaussian state that results is then connected off-chip to photon number-resolving sensors for Fock basis readout. The two-mode squeezed vacuum states are formed by squeezing eight modes, four pairs entangled by a 50/50 beam splitter. We divide the modes into signal modes (modes 0–3) and idler modes (modes 4–7). The signal and idler modes are then applied identically by a completely programmable arbitrary 4 X 4 unitary consisting of Mach-Zehnder interferometers having changeable phases. Finally, photon-counting measurements are used to independently read out each of the eight modes [18].

The circuit is based on Bell's theorem and the fundamental principles of Quantum Teleportation. The Experimental setup uses the Photonic chip as the Quantum channel to generate entangled fock states, which are then measured by applying gates to determine the key value and use classical computation as the classical communication channel for the transmission of data. Considering the quantum channel, the generation of the secret Key is attained here. The circuit used to execute the QKD contains three modes; where the first mode is the secret information to be shared by Alice with Bob. In the second mode, Alice chooses a random coherent state for the combined measurement of the unknown state with the base Alice chose.

The states are entangled, and the Homodyne Quadrature measurements are done for position (x) (Equation 5) and momentum (p) (Equation 6). The base state qumode and the base Bob chose to measure the secret Key is now entangled. The Quadrature measurement is then shared with Bob for final measurement, where Bob applies quantum gates to measure and arrive at the unknown state.

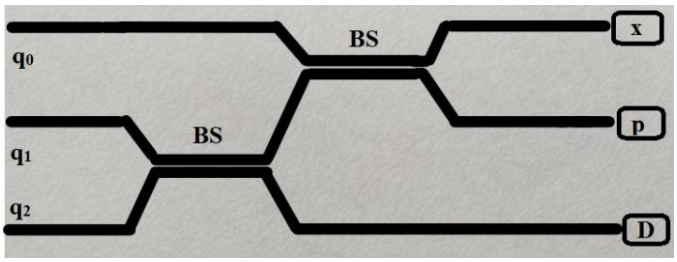

Figure 1: Linear interferometer part of the circuit used in the experimental setup.

The sequence of key values processed by Bob can be combined and formed as a complete secret key. The obtained secret Key can be subjected to Parameter Estimation and Privacy Amplification over a classical channel to arrive at the final Key for transmitting encrypted data. Based on Bell's theorem, as the modes of Alice and Bob are entangled, the further entanglement of the unknown state with Alice's mode and measurement of the state parameter will give Bob the state when he measures it with quantum gates (Equation 4). If an intruder tries to gain access to the channel and measures the state, then the entangled states are not entangled anymore and, therefore, can be detected after the sifting of keys.

The circuit is built with three qumodes, Beam Splitter gates to obtain entanglement of states, Homodyne measurement gates for quadrature measurement, and Displacement gates for the position (x) and momentum (p) separately. Initially, two modes, one referring to Alice (mode 1) and the other to Bob (mode 2), are entangled using the Beam splitter gate. The unknown state (mode 0), which Alice uses to encode the bit of information, is then entangled with mode 1. Finally, Homodyne measurement is performed by measuring x and p for mode 0 (Equation 5) and mode 1 (Equation 6**Error! Reference source not found.**), respectively. The result of the quadrature measurement is now stored in the quantum memory, and then Bob in mode 2 applies the Displacement gate to measure the x and p quadrature for mode 0 and mode 1, respectively. From the visualization of these measurements from the density matrix of the fock states, Bob measures the probability of position and momentum of the unknown state where it is now resolved to a classical bit and transmitted through the classical communication channel [19].

The laser pump is applied to the chip via optical fibres; the modes are then squeezed to form a maximally squeezed state except for the q0 (mode 0), which contains the unknown coherent state. Then the photons reach the linear interferometer region where different unitary values can be applied using quantum gates specifically designed for single, two, and multi-mode circuits. The detector detects the photons and measures the homodyne, position, and momentum of the acquired states (Figure 1)

IV. COMPUTATIONS AND RESULTS

The detectors measure the states, which are the position and momentum of the entangled states. We can visualize the probability of finding photons in the quadrature state. We found that the sample data provided the probability at 1st fock state. This proves that the photons are entangled (Figure 2).

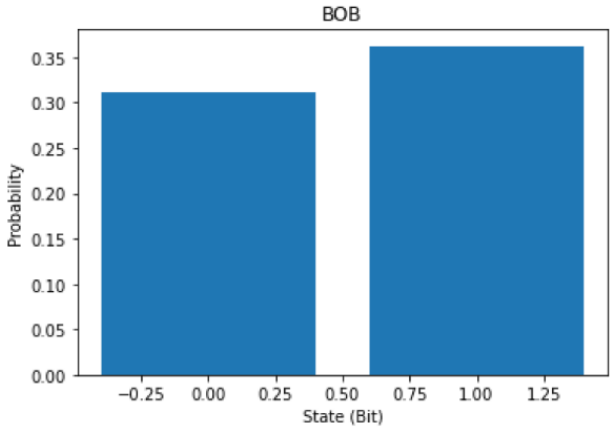

Figure 2:Bob (mode 2) fock state measurement.

Further, the calculated fock state measurement is combined, and a primary value which Alice and Bob encoded and measured respectively, and post-processing of the data is done. We considered roughly 100 bits for calculation, and the mode 0 result is Alice's bit (Figure 3); mode 1 results will be Alice's base (Figure 4). The measurement of the entangled state resolves it into a classical bit which Bob acquires as his primary key (Figure 5).

```
print(alice_message)
```

```
[1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0,
 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1,
 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0,
 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0]
```

Figure 3:Alice's message.

```
print(alice_bits)
```

```
[0 1 1 0 1 0 1 1 0 1 1 1 0 0 1 1 0 0 0 0 1 0 1 0 0 1 0 1 1 1 1 0 1 0 0 1 0
 0 0 1 0 1 1 1 1 0 0 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 1 1 1 0 0 1 0 1 1 0 0 0
 0 0 0 0 0 1 1 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1]
```

Figure 4:Alice's Bits.

```
print(secret_key)
```

```
[0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1,
1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0,
0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1,
1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1]
```

Figure 5:Bob's Primary Key.

This primary key is then subject to error mitigation and parameter estimation process, where the final secret key for Alice and Bob is acquired. Key sifting takes place through the classical communication channel, and the garbage i.e., Bits mutated by noise over the channel is removed from the primary keys (Figure 5).

```
Alice's Random Key string = [1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1]
Bob's Random Key string = [1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1]
```

Figure 1:Parameter estimation.

ALICE'S SECRET KEY

```
print(alice_key)
```

```
[0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0,
0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0,
1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0,
1]
```

BOB'S SECRET KEY

```
print(bob_key)
```

```
[0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0,
0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0,
1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0,
1]
```

Figure 2:Secret key.

For parameter estimation, a random string from the primary keys of Alice and Bob (*Figure 1*) is taken and compared. The count is specified as 15 during experimentation, and the secret key, except for sample bits used for estimation, is the final key (*Figure 2*) that is used for encrypting that data and transmission through insecure classical communication channels.

V. CONCLUSION

Based on the experimental data, the secret key obtained has 85 bits from the range of 100; this is because the photonic quantum processor produces significantly less noise than superconducting qubits carrying discrete-model quantum computers. This reduced noise is because photons don't easily interact with the environment around them compared with qubits. But there are possibilities for noise to enter the channel and cause errors in the bit generation. Sometimes, the entangled states will only stay short enough for the detectors to measure them, producing measurement errors. Quantum systems create noise; therefore, the noise is tolerated to some extent. The error rate more than the expected error rate for the quantum system will tell us the presence of an Eavesdropper.

VI. ACKNOWLEDGMENT

The authors acknowledge Xanadu and IBM Quantum Computation facility for their great help in accessing the facilities.

DECLARATIONS

Funding

Not Applicable

Competing Interests

Not Applicable

Affiliations

Department of Physics, School of Physical, Chemical and Applied Sciences, Pondicherry University, Puducherry –- 605 014, India.

Ethics approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent to participate.

Not Applicable

Consent for publication

We consent to the publication of this article.

Availability of data and materials

There is no data that can be available.

Code Availability

Not Applicable

Authors' Contributions

Mohanbabu Mani: Conceptualization, Writing - original draft

Lakshmi Priya Keerthi Gurunathan: Editing, Reviewing, and Validation

Ramesh Naidu Annavarapu: Reviewing, Editing, and Supervision.

All authors read and approved the final manuscript.

REFERENCES

[1] R. A. F. &. N. M. Imam, " An Effective and enhanced RSA based Public Key Encryption Scheme (XRSA).," International Journal of Information Technology, pp. 2645-2656, 2022.

[2] S. &. G. A. Choudhary, "AKAME: A post-quantum authenticated key-agreement and message encryption scheme based on ring-LWE.," International Journal of Information Technology, pp. 1669-1676, 2022.

[3] A. Steane, "Quantum computing," Reports on Progress in Physics, vol. 61, no. 2, p. 117, 1998.

[4] T. D. J. F. L. R. N. Y. M. C. &. O. J. L. Ladd, "Quantum computers.," Nature, pp. 45-53, 2010.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM review, pp. 303-332, 1999.

[6] P. &. P. B. R. Sharma, "Cryptanalysis of a secure and efficient Diffie–Hellman based key agreement scheme," International Journal of Information Technology, pp. 1-9, 2023.

[7] P&. M. K. Mullai, "Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified Swarm Optimization and Particle Swarm Optimization for mobile devices.," International Journal of Information Technology, pp. 551-564, 2021.

[8] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, vol. 85, no. 2, p. 441, 2000.

[9] S. E. &. Y. Y. Harris, "Photon switching by quantum interference.," Physical review letters, p. 3611, 1998.

[10] W. S. C. P. R. &. B. D. Marshall, " Towards quantum superpositions of a mirror.," Physical Review Letters,, p. 130401, 2003.

[11] R. H. P. H. M. &. H. K. Horodecki, "Quantum entanglement," Reviews of modern physics, p. 865, 2009.

[12] R. T. F. S.-M. T. W. H. S. T. L. M. .. &. Z. A. Ursin, "Entanglement-based quantum communication over 144 km.," Nature physics, pp. 481-486, 2007.

[13] G. Brassard, "Teleportation as a quantum computation.," arXiv preprint quant-ph, p. 9605035, 1996.

[14] A. K. Ekert, "Quantum Cryptography and Bell's Theorem," in Quantum Measurements in Optics, Springer, 1992, pp. 413-418.

[15] M. Arrazola, V. Bergholm, K. Brádler, T. R. Bromley, M. J. Collins, I. Dhand, A. Fumagalli, T. Gerrits, A. Goussev and L. G. Helt, "Quantum circuits with many photons on a programmable nanophotonic chip," Nature, vol. 591, no. 7848, pp. 54-60, 2021.

[16] N. I. J. Q. N. B. V. A. M. &. W. C. Killoran, "Strawberry fields: A software platform for photonic quantum computing.," Quantum, p. 129, 2019.

[17] Y. &. S. M. Fang, "Nanoplasmonic waveguides: towards applications in integrated nanophotonic circuits.," Light: Science & Applications, pp. e294-e294, 2015.

[18] E. Z. K. E. C. T. &. R. J. N. Dimitriadou, "Design of ultrafast all-optical 4-bit parity generator and checker using quantum-dot semiconductor optical amplifier-based Mach-Zehnder interferometer.," Journal of Computational Electronics, pp. 481-489, 2013.

[19] M. Michler, K. Mattle, H. Weinfurter and A. Zeilinger, "Interferometric Bell-state analysis," Physical Review A, vol. 53, no. 3, p. R1209, 1996.