The Bioscan
AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES
21(2): 1077-1082, 2026
www.thebioscan.com

Quantum Based Private Chat Space for Secure Organization

Mrs. J. Prabavadhi[1*], Amirtha Varshhini. S[2], Bhuvaneshwari. S[2], Priyadarshini. R[2], Yuavsri. M[2]
[1*]Assistant Professor, Department of Information Technology,
Manakula Vinayagar Institute of Technology, Puducherry, India.
Email: praba0885it@gmail.com
[2]UG Student, Department of Information Technology,
Manakula Vinayagar Institute of Technology, Puducherry, India.
DOI: https://doi.org/10.63001/tbs.2026.v21.i02.pp1071-1076

KEYWORDS:
Quantum, cryptography, Quantum Key Distribution, chatspace

Received on:
30-03-2026

Accepted on:
19-04-2026

Published on:
29-04-2026

ABSTRACT

The project "Quantum-Based Private Chatspace for Secure Organization" focuses on developing a secure communication platform tailored for organizational use. Leveraging quantum communication technologies, it aims to establish a chat environment capable of protecting sensitive information. The system will utilize quantum key distribution (QKD) to create and exchange cryptographic keys that are inherently resistant to eavesdropping, laying a solid foundation for secure communication. Key features will include end-to-end encryption, message integrity checks, and user authentication to meet enterprise-level security demands. The implementation of quantum security protocols will greatly strengthen data privacy and confidentiality, offering a cutting-edge defense against modern cyber threats. Furthermore, the project will involve a detailed assessment of potential security risks and rigorous testing to validate the system's reliability and real-world applicability, thereby promoting advanced communication solutions in organizational settings.

INTRODUCTION

Quantum theory, often referred to as quantum mechanics, is a fundamental scientific model that explains the behavior of matter and energy at atomic and subatomic scales. Developed over many years through the contributions of numerous physicists, it has profoundly advanced our understanding of microscopic phenomena. The journey of quantum theory began in the late 19th century, with a key milestone in 1900 when Max Planck introduced the idea that energy is emitted in discrete packets called quanta through his work on blackbody radiation. This concept laid the foundation for the emerging field.In 1905, Albert Einstein expanded on this framework by explaining the photoelectric effect, revealing that light itself behaves as discrete energy packets known as photons. Building further on these ideas,

Niels Bohr proposed a quantum model for the hydrogen atom in 1913, offering insight into the emission of spectral lines.Later developments brought new concepts, including wave-particle duality, introduced by Louis de Broglie, which proposed that particles like electrons exhibit characteristics of both particles and waves. In 1926, quantum theory was formalized through two major approaches: Erwin Schrödinger's wave equation and Werner Heisenberg's matrix mechanics.In 1935, the Einstein-Podolsky-Rosen (EPR) paradox raised questions about the completeness of quantum mechanics. It introduced the idea of quantum entanglement, where particles become so strongly linked that the state of one instantly affects the other, regardless of distance. This phenomenon, although challenging classical views, later became the basis for advanced quantum technologies such as Quantum Key Distribution (QKD).QKD is a breakthrough in secure communication that leverages the unique principles of quantum mechanics to generate and distribute encryption keys. Its progress over the decades has led to substantial advancements in cryptographic security.

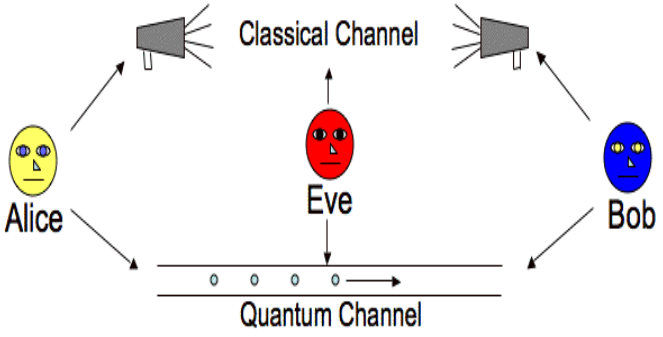

Fig .1 Quantum Key Distribution

The diagram represents how QKD functions between two users—traditionally named Alice and Bob. They communicate using two channels: a quantum channel for transmitting quantum bits (qubits) and a classical channel for public verification. When Alice sends qubits to Bob, any attempt by a third party (like Eve) to intercept the transmission will inevitably disturb the quantum state, exposing the eavesdropping attempt due to the nature of quantum measurement.After the quantum exchange, Alice and Bob use the classical channel to compare certain data and agree on a shared secret key without revealing it. This method secures communication based on the laws of quantum physics rather than computational complexity.A key protocol, BB84, introduced by Charles Bennett and Gilles Brassard in 1984, marked a significant advancement in QKD. It uses principles such as superposition and measurement uncertainty, where Alice encodes qubits in randomly chosen bases (rectilinear or diagonal), and Bob measures them with random bases as well. Matching basis choices result in a shared secret bit.

Post-Quantum Cryptography Integration (Ongoing Research) With the development of quantum computers posing risks to traditional encryption methods, current research is focused on integrating QKD with post-quantum cryptographic algorithms, forming a hybrid system resistant to both classical and quantum attacks. QKD's foundation relies on principles like entanglement and superposition, as seen in protocols such as E91 and variations using decoy states. These techniques ensure both security and intrusion detection, making QKD a cornerstone for future-proof communication in the quantum era.

LITERATURE SURVEY

This paper examines the growth of Quantum Key Distribution (QKD) networks, focusing on their path toward what is termed the "Qinternet." It looks at advancements, obstacles, and future possibilities for QKD networks, emphasizing their importance in creating quantum-secure communication for encrypting online data. Instead of relying on traditional encryption methods like SSL and TLS, the authors propose using QKD for HTTPS standards. This would allow for more secure key exchanges between users and servers, enhancing privacy during online interactions. The term "Qinternet"[1] suggests a future where quantum technologies significantly enhance online security. The paper outlines critical milestones and innovations that have influenced QKD networks, offering insights into the ongoing development of a quantum-secure internet.

This paper investigates a QKD method that merges discrete modulation with continuous-variable techniques. "Quantum Scissors" refers to an enhancement or protocol related to this research. The authors explore how these two approaches work together to strengthen the performance and security of quantum key distribution. Key topics likely include the fundamental principles, experimental setups, security evaluations, and practical impacts of this hybrid method in quantum communication. The authors present a model that truncates unused qubits and applies Noiseless [2] Linear Amplification to quantum states. This method can produce shared QKD keys of 16 and 24 bits through continuous truncation and amplification. However, the model faces challenges in technical implementation alongside other security technologies. The paper highlights the generation of shared QKD keys that can integrate with AES and other cryptographic algorithms.

This paper introduces a new QKD scheme centered on receiver device independent entanglement swapping. This approach aims to improve both security and practicality in QKD systems. The name "QKeyShield" [3] suggests a focus on protecting quantum communication from various forms of attack. The authors discuss the theoretical underpinnings, experimental applications, and security evaluations of QKeyShield in quantum communication. They propose a model that creates secure QKD keys for transfer between sender and receiver. In this model, the keys are generated using quantum entanglement, linking the sender's and receiver's states to produce secure QKD keys for encryption. The key benefit of this model is the inherent connection between the states of the sender and receiver.

The paper "Sending-or-Not-Sending Twin-Field Quantum Key Distribution With Measurement Imperfections" introduces a new method for quantum key distribution (QKD) that uses the twin-field approach. This method involves deciding whether to transmit or withhold quantum states, especially in light of measurement errors in the communication system. These errors are assessed by the receiver's state, the channel's activity status, and the availability of the quantum channel at a given time. Based on these factors, the twin-field method decides if the sender and receiver should share quantum states. This strategy minimizes collisions of quantum states during transmission and ensures secure key and data sharing, which is its main advantage. However, it has downsides, including high time complexity and a significant rejection rate. Sharing keys [4] over a common quantum channel can limit its availability for other transmissions. The paper provides a clearunderstanding of secure key sharing using the twin-field approach.

The "Patterning-Effect Calibration Algorithm for Secure Decoy State Quantum Key Distribution" outlines a method to fix patterning problems in secure decoy-state quantum key distribution systems. The study focuses on creating a method to reduce or fix patterning effects, which boosts the security and reliability of QKD protocols. The authors produce secure decoy states that detect and stop eavesdropping, significantly improving quantum communication security. The calibration algorithm ensures the accuracy of these decoy states, which monitor the transmission of QKD keys between users. By incorporating decoy states in the quantum channel,[5] overall security increases. The main drawback of this method is the added complexity of the channel mechanism, which can lower computational efficiency. The paper offers insights into using decoy states in QKD key distribution.

The paper "Quantum Key Distribution Based on Random Grouping Bell State Measurement" outlines a QKD system that uses random grouping for measuring Bell states. In this process, entangled particles are grouped randomly, and their combined states are assessed, helping to create secure cryptographic keys. The advantage pis that this randomness enhances key distribution security, making it harder for eavesdroppers [8] to succeed. Random grouping complicates interception, making it more difficult for attackers. However, this approach may face increased computational and experimental challenges, needing advanced quantum technologies and precise calibration to ensure system effectiveness.

Software-Defined Networking (SDN) is used in the study "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking" to present a new security model for QKD networks. This model allows for real-time management and optimization of security features in [9] QKD networks, adjusting to new threats. The key benefit is better adaptability and responsiveness to security issues, as SDN supports immediate changes to network settings. This integration helps allocate resources effectively, boosting the overall strength of QKD networks against cyber threats. However, it may require advanced infrastructure and protocols to connect SDN with QKD systems, as well as strong encryption methods to protect the quantum communication environment.

Proper implementation and testing are crucial for making this security model work effectively.

ARCHITECTURE

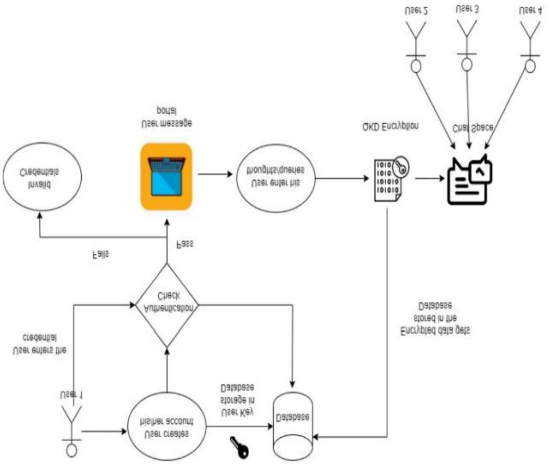

Figure 2: Architecture

This diagram represents a **Quantum-Based Private Chat Space for Secure Organization**, ensuring encrypted communication using **Quantum Key Distribution (QKD)** for high security.

1. ***User Registration & Authentication***
   a) **User 1** creates an account.
   b) The system generates a **User Key**, which is securely stored in a **Database**.
   c) The user then enters their credentials for login.
   d) An **Authentication Check** is performed:
   - If **failed**, the user gets an **InvalidCredentials** message.
   - If **passed**, the user is directed to the**User Message Portal**.

2. ***User Communication Process***
   a) The authenticated user enters their **thoughts or queries** in the chat portal.
   b) The system applies **Quantum Key Distribution (QKD) Encryption** to encrypt the message.
   c) The **encrypted message** is stored securely in the **Database**.

3. ***Message Distribution to Users***
   a) The encrypted message is sent to the **Chat Space**.
   b) **Other users (User 2, User 3, User 4)** in the chat space can access the messages securely.

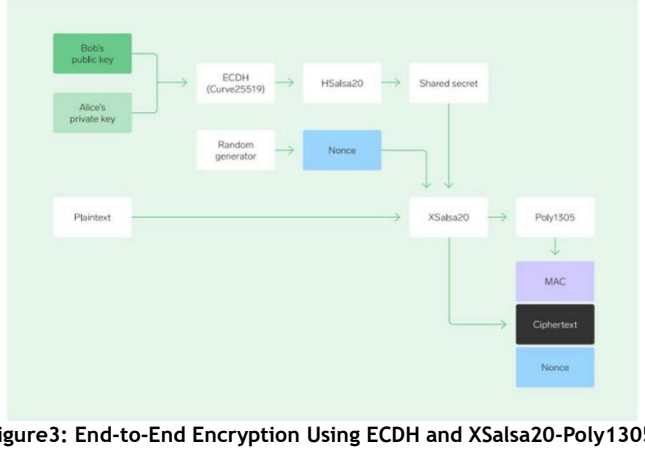

Figure3: End-to-End Encryption Using ECDH and XSalsa20-Poly1305

1.Key Exchange using ECDH (Curve25519): Bob's public key and Alice's private key are combined using Elliptic Curve Diffie-Hellman (ECDH) with Curve25519.This generates a shared secret, which both Alice and Bob can compute independently but no third party can derive.

***2.Deriving the Encryption Key*:** The shared secret is processed using HSalsa20 to derive a secure encryption key.

3.Generating a Nonce: A random generator produces a nonce (a unique, one-time-use number).The nonce ensures that the encryption remains unique for each message, preventing replay attacks.

***4.Encrypting the Plaintext*:** The plaintext message is encrypted using XSalsa20, a stream cipher derived from Salsa20.XSalsa20 takes in the shared secret and the nonce to perform the encryption.

5. Message Authentication using Poly130: The encrypted data is passed through Poly1305, an authentication function that generates a Message Authentication Code (MAC).This ensures that the ciphertext has not been tampered with during transmission.

***6.Final Encrypted Output*:** The final encrypted message consists of:

a) MAC (Message Authentication Code):
Prevents tampering and ensuresthe message comes from a trusted sender.

b) Ciphertext (the encrypted message) :
Ensures confidentiality—only authorized parties can read the message.

c) Nonce (Number used once) :
Prevents replay attacks and ensures freshness and uniqueness in encryption.

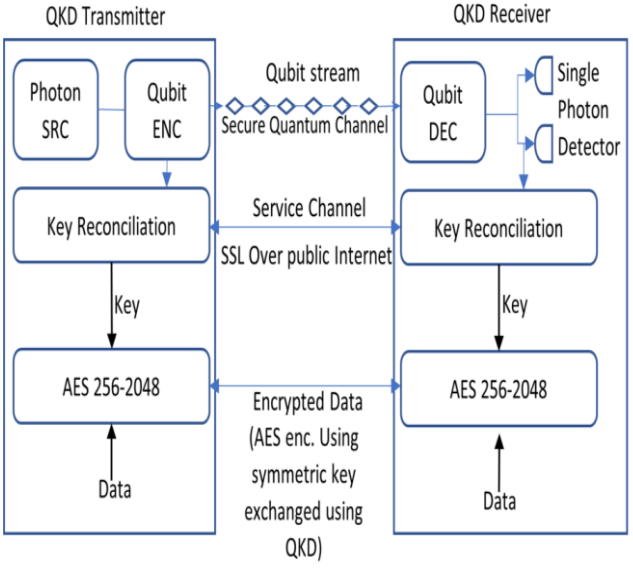

Fig 4. Working of Proposed solution

PROPOSED SOLUTION

Our proposed solution transforms secure organizational communication using Quantum Key Distribution (QKD) based on the BB84 protocol. This modern cryptographic approach is more secure than traditional methods, using qubits and secure bases to create encryption keys unique to each communication channel.

Only users in a specific channel can access the messages, ensuring complete confidentiality. We further enhance security by developing a dedicated private chat platform, avoiding risks from third-party tools. This ensures a secure, isolated space for sensitive communication.

To strengthen encryption, quantum-resistant algorithms can also be integrated, and issues like noise or errors in quantum transmission are managed through key purification and error correction techniques. Tools like IBM Qiskit or Google Cirq can be used for implementation.

This figure shows how Quantum Key Distribution (QKD) is used along with classical encryption (AES) to provide secure communication:

QKD Transmitter:

- Photon Source & Qubit Encoder: Generates and encodes quantum bits (qubits).
- Secure Quantum Channel: Qubits are transmitted through this channel.
- Key Reconciliation: Ensures both sender and receiver agree on the same encryption key.
- AES Encryption: The agreed key is used to encrypt data (using AES 256-2048).

QKD Receiver:

- Qubit Decoder & Photon Detectors: Receives and decodes the incoming qubits.
- Key Reconciliation: Matches the sender's key securely.
- AES Decryption: The encrypted data is decrypted using the symmetric key.

SSL over Public Internet is used as a classical channel to share encrypted data safely.

In Figure 4 it is shown as the workflow of the proposed solution by means of both classical as well as quantum channel cryptographic technique.

The graph Fig 5.4 illustrates the key bit agreement between Alice and Bob in a quantum key distribution (QKD) process, showing a perfect match across all 10 bit indices. This perfect agreement indicates enhanced security, as it suggests that no eavesdropping has occurred during transmission. In QKD protocols like BB84, quantum mechanics ensures that any interception by an eavesdropper would disturb the qubits and introduce detectable errors. Since Alice and Bob observe no mismatches, they can be confident that their communication was secure. Furthermore, the use of random bases for encoding and measurement, along with the public discussion of bases (not the key itself), adds an additional layer of protection. This process allows them to establish a shared, secret key that is both tamper-evident and immune to classical interception methods, thereby significantly enhancing the overall security of their communication.

IMPLEMENTATION

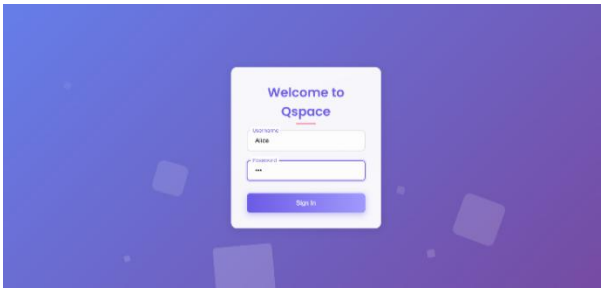

Fig 5 .1.Login page

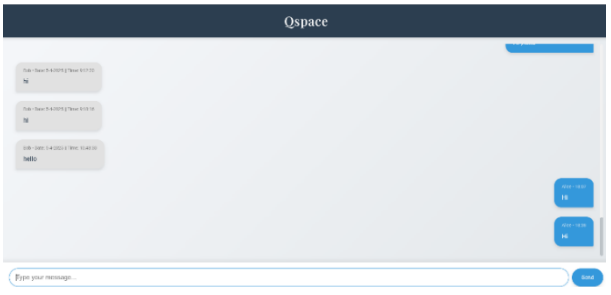

Fig 5.2 Chat UI

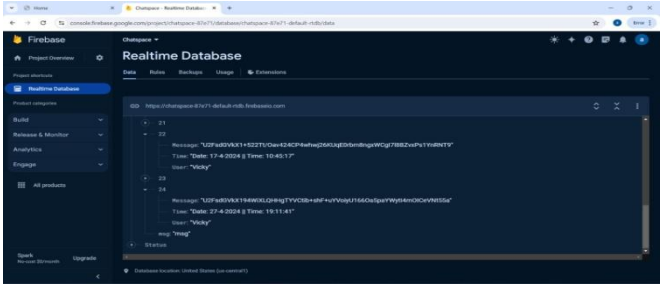

Fig 5.3 Firebase

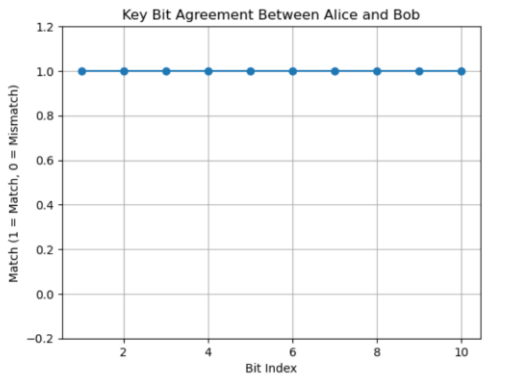

Fig 5.4 Bits Matched

FUTURE WORK

The current implementation focuses on secure text-based communication between users within a private organization. future extensions of this system envisage several advancements to broaden its scope and practical applications. one major enhancement involves incorporating quantum-secure document sharing, enabling users to exchange sensitive files using dynamically generated quantum keys. real-time video conferencing over quantum-encryptedchannels is also a key direction, ensuring highly secure audio-visual interactions. Additionally, support for secure multimedia file transfers, including images and videos, will be integrated using hybrid encryption models that combine quantum keys with fast symmetric algorithms. Cross-device key synchronization will ensure continuity and security of communication across multiple platforms. The system will also be extended to facilitate group communication with quantum group key management and role-based access controls. To guarantee communication integrity and traceability, blockchain-based audit logging using quantum-generated hashes will be introduced. Finally, a hybrid quantum-classical architecture will be implemented to allow for scalable, compatible, and transition-friendly deployment in modern network environments.

CONCLUSION

The papers provide an overview of Quantum Computing and its limitations in various areas. They also introduce Cryptography and Quantum Key Distribution (QKD). Additionally, they explore the possibility of combining these two technologies to create a hybrid system for secure data storage.

ACKNOWLEDGEMENT

The authors express sincere gratitude to the anonymous reviewers for their valuable feedback, which contributed significantly to the refinement of this paper. Special thanks are also extended to the project supervisor for their guidance and unwavering support throughout the completion of this work.

REFERENCE

1. Yuan Cao, Yongli Zhao, Qin Wang, Jie Zhang, Soon Xin Ng, Lajos Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet" (IEEE Xplore Issue:18 Jan, 2022)
2. Masoud Ghalaii, Carlo Ottaviani, Rupesh Kumar, Stefano Pirandola, "Discrete-Modulation Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors" (IEEE Xplore Issue: 23 Jan, 2020)
3. Mohammed Y. Al-Darwbi, Ali A. Ghorbani, Arash Habibi Lashkari, "QKeyShield: A Practical Receiver Quantum Key Distribution" (IEEE Xplore Issue: 6 Oct, 2022)
4. Ming-Shuo Sun, Chun-Hui Zhang, Xiao Ma, Xing-Yu Zhou, Qin Wang, "Sending-or-Not-Sending Twin-Field Quantum Key Distribution With Measurement Imperfections" (IEEE Xplore Issue: 10 Jun, 2022)
5. Xiang Kang, Feng-Yu Lu, Shuang Wang, Jia-Lin Chen, Ze-Hao Wang, "Patterning-Effect Calibration Algorithm for Secure Decoy-State Quantum Key Distribution" (IEEE Xplore Issue: 3 Oct, 2022)
6. Omar Amer, Vaibhav Garg, Walter O. Krawec, "An Introduction to Practical Quantum Key Distribution" (IEEE Xplore Issue: 1 Mar, 2021)
7. Ragini Verma, Anshul Jaiswal, Anh T. Pham, "Design and Analysis of Octa-phase Shift Keying Based Quantum Key Distribution System" (IEEE Xplore Issue: 15 Aug, 2023)
8. Dan Song, Dongxu Chen, "Quantum Key Distribution Based on Random Grouping Bell State Measurement" (IEEE Xplore Issue: 16 Apr, 2020)
9. Omar Shirko, Shavan Askar, "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking" (IEEE Xplore Issue: 2 Mar, 2023)
10. Evgeniy O. Kiktenko, Aleksei O. Malyshev, Maxim A. Gavreev, Anton A. Bozhedar, "Lightweight Authentication for Quantum Key Distribution" (IEEE Xplore Issue: 22 April, 2020)
11. Hsing-Chung Chen, Cahya Damarjati, Eko Prasetyo, Chao-Lung Chou, "Generating Multi-Issued Session Key by Using Semi Quantum Key Distribution With Time Constraint" (IEEE Xplore Issue: 15 Feb, 2022)
12. Rahul Jain, Carl A. Miller, Yaoyun Shi, "Parallel Device-Independent Quantum Key Distribution" (IEEE Xplore Issue: 9 Apr, 2020)
13. Shen-Shen Yang, Zhen-Guo Lu, Yong-Min Li, "High Speed Post-Processing in Continuous-Variable Quantum Key Distribution Based on FPGA Implementation" (IEEE Xplore Issue: 6 April, 2020)
14. Ye Chongqiang, Li Jian, Chen Xiubo, Tian Yuan, Hou Yanyan, "An Efficient Semi-Quantum Key Distribution Protocol and Its Security Proof" (IEEE Xplore Issue: 11 Mar, 2022)
15. Hongyi Zhou, Kefan Lv, Longbo Huang, Xiongfeng Ma, "Quantum Network: Security Assessment and Key Management" (IEEE Xplore Issue: 10 Jan, 2022)
16. Mehrdad Tahmasbi, Matthieu R. Bloch, "Toward Undetectable Quantum Key Distribution Over Bosonic Channels" (IEEE Xplore Issue: 18 Aug, 2020)
17. Zi-Ang Ren, Yi-Peng Chen, Jing-Yang Liu, Hua-Jian Ding, Qin Wang, "Implementation of Machine Learning in Quantum Key Distributions" (IEEE Xplore Issue: 24 Nov, 2020)
18. Yaru Fu, Yang Hong, Tony Q. S. Quek, Hong Wang, Zheng Shi, "Scheduling Policies for Quantum Key Distribution Enabled Communication Networks" (IEEE Xplore Issue: 6 Aug, 2020)
19. Ayan Biswas, Anindya Banerji, Pooja Chandravanshi, Rupesh Kumar, "Experimental Side Channel Analysis of BB84 QKD Source" (IEEE Xplore Issue: 9 Sep, 2021)
20. KyungHyun Han, Ali Raza, Seong Oun Hwang, "CAPTCHA-Based Secret-Key Sharing Using Quantum Communication" (IEEE Xplore Issue: 1 Dec, 2021)