www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 15 Issue 01 January 2026, Page No. 28121-28128
ISSN: 2319-7242 DOI: 10.18535/ijecs/v15i01.5370

Based Eavesdropping Detection to Enhance QKD Security and Scalability

[1]D. Mahaboob Basha, [2]Raghavendra Kumar V, [3]O.Kiran Kumar, [4]A.Mallikarjuna

[1] Assistant Professor in Computer science and Applications, Department of Computer Science, St. Joseph's Degree College, Sunkesula Road, Kurnool.
[2] Assistant Professor in Computer science and Applications, Department of Computer Science, St. Joseph's Degree College, Sunkesula Road, Kurnool.
[3] Assistant Professor in Computer science and Applications, Department of Computer Science, St. Joseph's Degree College, Sunkesula Road, Kurnool.
[4] Assistant Professor in Computer science and Applications, Department of Computer Science, St. Joseph's Degree College, Sunkesula Road, Kurnool.

Abstract
Quantum key distribution (QKD) and quantum message encryption protocols promise a secure way to distribute information while detecting eavesdropping. However, current protocols may suffer from significantly reduced eavesdropping protection when only a subset of qubit are observed by an attacker. The eavesdropping detection is enhanced through a Quantum Fourier Transform (QFT)-based method, and classical-channel hardening using post-quantum or classical authenticated encryption by proposed hybrid QKD framework leveraging recent advances specifically combining a modern security-proof for Twin-Field Quantum Key Distribution (TF-QKD). The key rate, error resilience, and security under realistic channel noise and detector imperfections are analyzed. Therefore, this framework shows better improvement in security towards key rates over longer distances and stronger eavesdropper detection compared to traditional QKD protocols. Hence, this proposed system shows better results interms of accuracy, security and efficiency.

KEYWORDS: Quantum key distribution (QKD), Twin-Field Quantum Key Distribution (TF-QKD), Quantum Fourier Transform (QFT), security

I. Introduction

Communications have emerged as a response to the advancements of quantum computers. Shor's algorithm has demonstrated that, given a powerful enough quantum computer, problems such as factorization and discrete logarithms could be solved exponentially faster compared to the best-known classical algorithms (e.g., GNFS). This translates into a need to substitute currently used public key cryptography (PKC) algorithms. Specifically, Rivest-Shamir-Adleman (RSA) and elliptic curve (EC) cryptography algorithms must be substituted by new, quantum-resistant alternatives.

Although the timeline for such a powerful quantum computer to be available remains uncertain, the migration of communications systems towards implementing quantum-resistant schemes should be performed as soon as possible, as it presents several challenges, some of which we address in this work, that require a timely controlled transition. Moreover, "harvest now, decrypt later" (HNDL) attacks allow adversaries to already collect encrypted versions of long-lived data today, which can later on be decrypted by means of a quantum computer. Thus, not only will classical cryptographic schemes be compromised in the near future, but the confidentiality of current communications is already at risk.

In anticipation of future cryptographic challenges, standards development organizations (SDOs) such as NIST, ETSI, ITU-T, ISO/IEC, IETF, and IEEE are actively working on evolving to the next era of quantum-resistant cryptographic schemes. Among the most developed alternatives to replace traditional PKC algorithms are post-quantum (PQ) cryptography and quantum key distribution (QKD).

While PQ cryptography relies on mathematical assumptions (e.g., lattice problems, hash functions) for which Shor's algorithm provides no known advantage, QKD relies on the delivery of quantum signals among two authorized partners; in this scenario, eavesdropping on the key distribution can be detected, and thus the key distribution protocol can be aborted. Otherwise, if no eavesdropper is detected, the shared secret transmitted between Alice and Bob can be considered information-theoretically secure (ITS).

The two approaches fundamentally differ in their security paradigms: PQ cryptography maintains computational security against quantum computers via different mathematical assumptions, while QKD aims for ITS security during key distribution. Despite their different mechanisms, both strategies effectively mitigate the advantages that Shor's algorithm provides against classical PKC.

Nevertheless, it is worth mentioning that the security of subsequent use of these keys for symmetric encryption depends on the method used. Computationally secure symmetric encryption, such as the Advanced Encryption Standard (AES) algorithm, remains 'only' computationally secure, but is still considered secure against quantum computers if sufficiently large keys are employed. To achieve ITS secure communications, QKD must be combined with an ITS encryption primitive, such as one-time pad (OTP). However, the large key sizes required by OTP – at least as long as the message itself limit its practical use. Given the existing challenges of both PQ cryptography and QKD, combining PQ cryptography and QKD can create a synergistic approach, leveraging the strengths of both technologies and providing a more robust security against quantum threats.

Information Security considerations have always been crucial for communications. Rapid advancement in information technology and related sectors has contributed significantly to social stability and national security. However, as security threats become more urgent, there is an increasing need for information security. Quantum Key Distribution (QKD) has played a pivotal role in heralding a new era of quantum-enhanced information security by providing key distribution with information-theoretic security. This technology has been instrumental in the advancement of the field of cryptography beyond classical limitations. When combined with single-use cipher techniques, QKD offers the highest level of security for transmitting private messages. Numerous QKD networks have been tested in the field and were subsquently introduced to the market. The development of various QKD methods can generally be classified into two main categories: discrete variable coding and continuous variable coding. This particular QKD methodology employs quantized information carriers, such as the spin orientation or temporal alignment of individual photons. Continuous Variable Quantum Key Distribution (CV-QKD), which utilizes coherent states, is rapidly gaining traction due to its compatibility with existing telecommunication devices. For example, CV-QKD can employ a coherent receiver alongside a commercial continuous-wave laser. CV-QKD has made great progress in system implementation, security analysis, and protocol design. Rapid improvements in performance, efficiency, and system reliability have advanced CV-QKD systems from early feasibility demonstrations to the next phase of development. This progress has been accompanied by significant enhancements in security proofs. Modern network architecture is now in its third phase of development, largely driven by the full integration of coherent communication. This article provides a detailed overview of the CV-QKD system structure, its key modules, major system implementations, and the concept of CV-QKD using coherent states.

II. Literature Survey

N. Ul Ain, et al. [15] proposes a method to enhance the security of the BB84 protocol, to reduce susceptibility to attacks and eavesdropping. The improved BB84 protocol utilizes 9, 12, and 16 quantum bits along with two, and three bases to significantly bolster security. This allows authorized parties to eliminate the use of compromised keys. Additionally, the study implements the E91 QKD protocol utilizing the Entanglement Pair Generation (EPR) method to produce secure keys. While the existing E91 protocol

ensures security through Bell's theorem and Bell's inequality, it overlooks the impact of noise, leading to inaccuracies in eavesdropper detection. Whenever an eavesdropper attempts to measure the quantum state, the proposed E91 protocol collapses its state from $|10\rangle$ to $|11\rangle$, setting the first Qubit to $|1\rangle$ and the other Qubit to $|0\rangle$, thus providing the eavesdropper with incorrect information, accompanied by a phase angle of 15π /8. This leads to a misconception, preventing eavesdroppers from obtaining useful details about transferred quantum states.

S. Ricci, P. Dobias, L. Malina, J. Hajny and P. Jedlicka, et al. [16] present a concrete 3-key combiner system implemented on a Field Programmable Gate Arrays (FPGA) platform. Our system involves a pre-quantum Key EXchange scheme (KEX), a post-quantum key encapsulation mechanism, and a Quantum Key Distribution (QKD) algorithm. The proposed 3-key combiner is proven to be secure in the quantum standard model and it is INDistinguishable under a Chosen-Ciphertext Attack (IND-CCA). Our combiner can run in small FPGA platforms due to its relatively low resources usage. In particular, the key combiner without QKD is able to output up to 1 624 keys per second and the key combiner with QKD is able to output up to 9.2 keys per second.

O. Shirko and S. Askar, et al.[17] a software-defined networking (SDN) technique is introduced to circumvent this drawback by utilising the flexibility provided by the SDN paradigm for better QKD network management. In particular, a novel survivability model called software-defined quantum key relay failure (SDQKRF) is proposed in this paper in which a new function is developed and added to the SDN controller. According to the simulation results, SDN over a QKD network using the SDQKRF model is more reliable and performs better in terms of the key generation ratio, key utilisation rate, recovery after failure, avalanche effect, and service blocking rate than a regular QKD network without the SDQTRF model.

I. B. Djordjevic, et al.[18] proposed hybrid QKD protocol, Alice simultaneously performs discrete modulation (DM)-based encoding for CV-QKD subsystem and time-phase encoding for DV-QKD on a transmitter side and transmits such hybrid encoded pulse with optimized average number of photons per pulse. On receiver side, Bob employs a 1:2 optical space switch to select either DV-QKD receiver or CV-QKD receiver with the optimized probability of selection. Other compatible CV-QKD and DV-QKD protocols can also be used in hybrid QKD. The proposed hybrid QKD protocol significantly outperforms previously introduced both Gaussian modulation (GM)- and DM-based CV-QKD protocols as well as DV-QKD protocols in terms of both secret-key rate and achievable transmission distance.

A. Bhatia, S. Bitragunta and K. Tiwari, et al.[19] present a Physical Unclonable Function (PUF)-based authenticated QKD protocol (PUF-AQKD), which avoids the necessity for authenticated classical channels and is useful in mitigating MITM attacks. The fundamental concept of PUF-AQKD is to implement a phase shift in the basis used for polarizing the transmitted qubits. The phase shift is dictated by PUFs, which are anticipated to result in analogous (correlated) responses for devices manufactured under similar conditions but dissimilar responses in different conditions. An adversary lacking a correlated PUF response shared by Alice and Bob would inadvertently increase the Quantum Bit Error Rates (QBER) observed at Bob's end. We present a mathematical model to assess the efficacy of the proposed PUF-AQKD method and perform simulations utilizing the NetSquid simulator.

I. B. Djordjevic, et al. [20] post-quantum cryptography (PQC) is proposed as an alternative to QKD. However, the PQC protocols are based on conjecture that there are no polynomial time algorithms to break the PQC protocols. To overcome key challenges of both post-quantum cryptography and QKD, we propose to use the QKD only in initialization stage to set-up corresponding cybersecurity protocols. The proposed concept is applied to both computational security and PQC protocols. The proposed QKD-enhanced cybersecurity protocols are tolerant to attacks initiated by quantum computers.

N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik and M. Z. Win, et al.[21] secret key rate (SKR) of a continuous variable QKD (CV-QKD) system using multiple-input multiple-output (MIMO) transmission and operating at terahertz (THz) frequencies. Distinct from previous works, we consider a practical "restricted" eavesdropping scenario in which Eve can collect only a fraction of photons lost in the

environment. We propose a system model for the MIMO THz CV-QKD system that accounts for restricted eavesdropping via a lossy wireless channel between Alice and Eve. We derive for this system new SKR expressions for both coherent-state-based and squeezed-state-based CV-QKD protocols. Our results show that previous analysis assuming unrestricted eavesdropping leads to overly pessimistic SKRs, and that in practice, the achievable SKR can be significantly increased under restricted eavesdropping.

Y. Tanizawa et al., [22] presents the development and evaluation of the proof-of-concept (PoC) system for the QKD network and a quantum secure cloud, especially applied to the genome medicine domain. The PoC system was developed at Tohoku University and Toshiba sites to address the "cancer clinical sequencing" use case. We evaluated three practical scenarios with the PoC system: 1) real-time transmission of genome analysis data; 2) "expert panel," an online video conference for medical experts' discussion; and 3) distributed backup of genome analysis data.

H. Wang et al., [23] resilient QKD-integrated optical networks against single link failure. By analyzing and quantifying the key provisioning services, we constructed the secret-key flow model (SKFM) for the failure-affected and failure-unaffected cases. Based on the SKFM, a secret-key recovery strategy (SKRS) including three algorithms (i.e., one-path recovery method (OPRM), multi-path recovery method (MPRM), and time window-based recovery method (TWRM)) is designed to recover failure-affected key provisioning services in the network. The simulation work has been conducted to evaluate the performance of OPRM, MPRM, and TWRM in terms of key-service recovery ratio, secret-key recovery ratio, wavelength consumption ratio, and secret-key consumption ratio.

C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang and C. Pei, et al. [24] propose a continuous-variable quantum key distribution (CVQKD) scheme at terahertz (THz) bands based on multicarrier multiplexing (MCM) technology. In this scheme, multiple Gaussian modulated subcarriers are coupled to transmit multipath superposed thermal Gaussian states. At the receiver, optical discrete Fourier transform (ODFT) is used to demultiplex the received subcarriers, and the keys can be generated in parallel by homodyne detection and post processing. We analyze the security of the scheme against the optimal collective Gaussian attack under indoor environment and in inter-satellite links respectively.

M. Mehic, S. Rass, E. Dervisevic and M. Voznak, et al. [25] a novel solution for designing a Key Management System resistant to DoS attacks. Our solution allows applications to function securely in environments with fewer keys. In addition, we have provided approaches for allocating and managing QKD resources to avoid malicious key reservations. Simulation experiments verified the proposed solutions.

III. Quantum-Classical Hybrid Framework For Qft-Based Eavesdropping Detection To Enhance Qkd Security And Scalability

In this section, Quantum-Classical hybrid framework for QFT-based Eavesdropping detection to enhance QKD security and scalability framework is observed in figure 1. Protocol Selection — TF-QKD use the TF-QKD variant whose security is guaranteed and generate weak coherent pulses, send over optical fiber (or other quantum channel), with a middle node as in TF-QKD architecture. Eavesdropping Detection QFT-based Method is implemented for the protocol that embed QFT-based interference checks to detect partial-qubit interception. The relevant detection metrics is computed to reveal eavesdropper's presence even if only subset qubits are intercepted and periodically insert QFT-tests among transmission frames. Classical-Channel Security and Hybrid Encryption is used for classical authenticated encryption (or post-quantum algorithms) over the classical channel for basis reconciliation and authentication inspired by hybrid quantum-classical frameworks after quantum key generation. The quantum part is compromised to ensure that classical communications (public discussions) remain secure. The realistic fiber-loss, channel noise, detector dark counts / afterpulses are simulated and key generation rate, quantum bit error rate (QBER), and eavesdropping detection probability with/without QFT enhancement is compared.

Longer secure key-distribution distances compared to standard QKD, thanks to TF-QKD for better eavesdropping detection (including partial-qubit attacks) via QFT-based detection. Enhanced classical-

channel security through hybrid encryption reducing reliance on classical authentication assumptions with more realistic and deployable QKD architecture aligned with integration into existing telecom infrastructure.

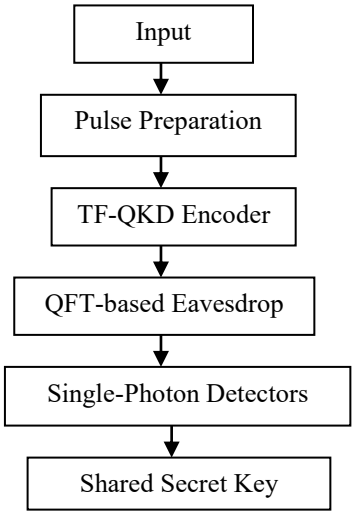

Figure.1: Quantum-Classical Hybrid Framework for QFT-Based Eavesdropping Detection to Enhance QKD Security and Scalability Framework

In quantum cryptography, particularly in Quantum Key Distribution (QKD), pulse preparation is the crucial process of generating precisely controlled optical pulses that encode quantum information (qubits) for transmission between parties. This involves creating and manipulating weak coherent pulses of light to represent quantum states while minimizing errors and preventing eavesdropping. An TF-QKD Encoder (Twin-Field Quantum Key Distribution) is a sophisticated system, often FPGA-based, that generates precise light pulses with controlled intensity and phase patterns, enabling two distant parties (Alice & Bob) to send signals to an untrusted node (Charlie) for single-photon interference, creating a secure key, overcoming distance limits by exploiting phase encoding and vacuum states for high-speed, long-distance quantum security.

QFT-based eavesdropping in quantum cryptography uses the Quantum Fourier Transform (QFT) to enhance eavesdropping detection in Quantum Key Distribution (QKD) by detecting disturbances in quantum states, making attacks more costly, and can even enable protocols where Eve's measurement on a subset of qubits is detected, improving security beyond standard protocols like BB84, often by leveraging QFT's ability to transform between bases and reveal errors. It's not about performing the eavesdropping with QFT, but using QFT to spot the eavesdropper by analyzing interference patterns. Single-Photon Detectors (SPDs) are crucial for Quantum Key Distribution (QKD) by detecting individual light particles (photons) used to create secure keys, with top performers like Superconducting Nanowire SPDs (SNSPDs) offering high efficiency and speed, while room-temperature SPADs (Single Photon Avalanche Diodes) provide compact, scalable alternatives, enabling quantum-safe communication by leveraging quantum mechanics to detect eavesdropping attempts.

In quantum cryptography, a shared secret key is established using quantum mechanics principles (like BB84 or E91 protocols) where photons (qubits) are sent, allowing two parties (Alice & Bob) to create a random, identical key, guaranteed secure because any eavesdropper (Eve) attempting to measure the quantum states inevitably disturbs them, which Alice and Bob detect, forcing a restart. This quantum key, derived from shared random outcomes and authenticated classically, then secures subsequent data encryption via methods like one-time pads, leveraging quantum properties for unbreakable secrecy, though a small initial pre-shared key might be needed for authentication, note Wikipedia and MDPI.

IV. Result Analysis

In this section, result analysis of Quantum-Classical hybrid framework for QFT-based Eavesdropping detection to enhance QKD security and scalability framework is observed. The proposed system is compared with existing system with parameters interms of accuracy, security and efficiency.

Table.1: Performance Comparison

Parameters	Existing System	Proposed System
Accuracy	94.1	96.2
Security	94.6	97
Efficiency	95.2	98.4

In figure.2, accuracy comparison graph is observed. In this analysis, proposed system and existing system are compared with accuracy parameter and shows high accuracy for proposed system.

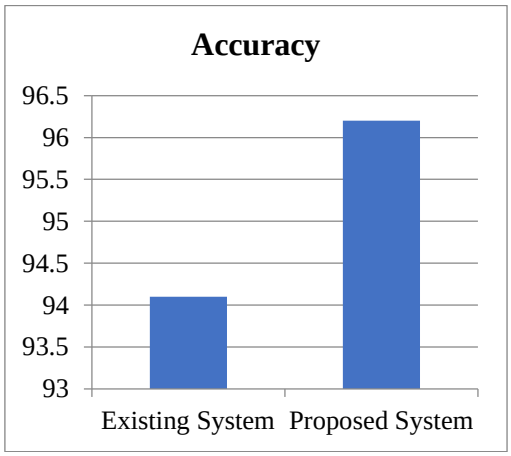

Figure.2: Accuracy Comparison Graph

Security comparison graph is observed in figure.3. In this analysis, proposed system and existing system are compared with security parameter and shows high security for proposed system.

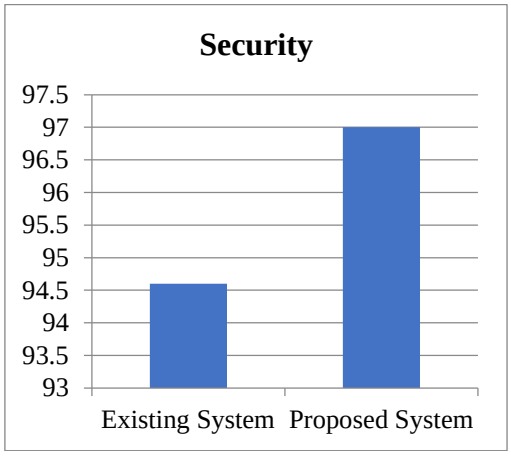

Figure.3: Security Comparison Graph

Efficiency comparison graph is observed in figure.4. In this analysis, proposed system and existing system are compared with efficiency parameter and shows high efficiency for proposed system.

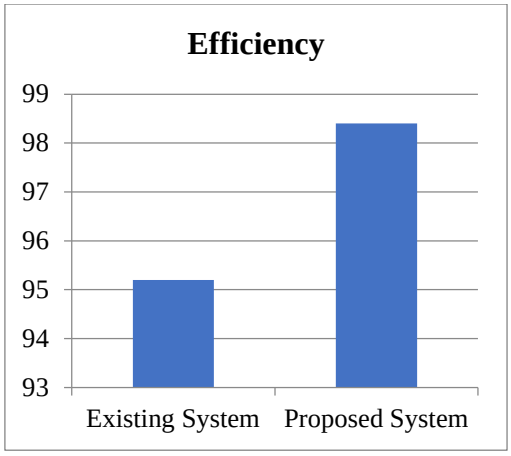

Figure.4: Efficiency Comparison Graph

V. Conclusion

The exponential growth of Internet of Things (IoT) ecosystems has introduced unprecedented security challenges, necessitating innovative solutions that transcend classical cybersecurity paradigms. The QKD protocol design (TF-QKD), eavesdropping detection (QFT-based), and hybrid encryption for classical channels by modern hybrid quantum-classical cryptographic framework. This proposed system shows and improved key rates over longer distances, stronger security (both quantum and classical channels), and realistic deployability based on simulated analysis. The next generation of secure communication networks across telecom infrastructure, finance, healthcare, and critical government systems as quantum communication technology matures like hybrid frameworks. In future, by integration with quantum-resistant classical cryptography standards shows better enhancement.

VI. References

1. C. Rubio García, A. Cano Aguilera, C. Stan, J. José Vegas Olmos, S. Rommel and I. Tafur Monroy, "Enhanced Network Security Protocols for the Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution," in IEEE Journal on Selected Areas in Communications, vol. 43, no. 8, pp. 2765-2781, Aug. 2025, doi: 10.1109/JSAC.2025.3568011.
2. S. L. Birhanu, M. Ghadimi, Y. Hai, P. Seeling, R. Bassoli and F. H. P. Fitzek, "A Survey of Continuous Variable Quantum Key Distribution in Quantum Communication," in IEEE Access, vol. 13, pp. 166027-166061, 2025, doi: 10.1109/ACCESS.2025.3610519.
3. J. Jordan-Parra, M. Garcia-Romero, J. Gil-Lopez, J. A. Ruiz-De-Azua and J. Paradells, "Satellite Quantum Key Distribution: Analysis, Modeling, Performance Evaluation, and Validation," in IEEE Open Journal of the Communications Society, vol. 6, pp. 8241-8271, 2025, doi: 10.1109/OJCOMS.2025.3614698.
4. Y. Dong, J. Peng and X. Sun, "Continuous-Variable Quantum Key Distribution Scheme with Odd Coherent States," in Chinese Journal of Electronics, vol. 27, no. 2, pp. 433-438, March 2018, doi: 10.1049/cje.2017.10.005
5. M. Y. Al-Darwbi, A. A. Ghorbani and A. H. Lashkari, "QKeyShield: A Practical Receiver-Device-Independent Entanglement-Swapping-Based Quantum Key Distribution," in IEEE Access, vol. 10, pp. 107685-107702, 2022, doi: 10.1109/ACCESS.2022.3212787.
6. Y. -L. Tang et al., "Field Test of Measurement-Device-Independent Quantum Key Distribution," in IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 116-122, May-June 2015, Art no. 6600407, doi: 10.1109/JSTQE.2014.2361796.
7. S. Yan, J. Wang, J. Fang, L. Jiang and X. Wang, "An Improved Polar Codes-Based Key Reconciliation for Practical Quantum Key Distribution," in Chinese Journal of Electronics, vol. 27, no. 2, pp. 250-255, March 2018, doi: 10.1049/cje.2017.07.006.
8. X. Liu, J. Wang, R. Li and C. Zhang, "Security Analysis of Stochastic Routing Scheme in Grid-Shaped Partially-Trusted Relay Quantum Key Distribution Network," in Chinese Journal of Electronics, vol. 27, no. 2, pp. 234-240, March 2018, doi: 10.1049/cje.2018.01.013.

9. K. -S. Shim, Y. -h. Kim, I. Sohn, E. Lee, K. -i. Bae and W. Lee, "Design and Validation of Quantum Key Management System for Construction of KREONET Quantum Cryptography Communication," in Journal of Web Engineering, vol. 21, no. 5, pp. 1377-1417, July 2022, doi: 10.13052/jwe1540-9589.2151.
10. C. Biswas, M. M. Haque and U. Das Gupta, "A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconciliation Analysis in Quantum Cryptography," in IEEE Access, vol. 10, pp. 72743-72757, 2022, doi: 10.1109/ACCESS.2022.3188798.
11. E. H. Laaji and A. Azizi, "A Combination of BB84 Quantum Key Distribution and an Improved Scheme of NTRU Post-Quantum Cryptosystem," in Journal of Cyber Security and Mobility, vol. 11, no. 5, pp. 673-694, September 2022, doi: 10.13052/jcsm2245-1439.1152.
12. J. Li et al., "A Survey on Quantum Cryptography," in Chinese Journal of Electronics, vol. 27, no. 2, pp. 223-228, March 2018, doi: 10.1049/cje.2018.01.017.
13. D. Pan et al., "The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet," in IEEE Communications Surveys & Tutorials, vol. 26, no. 3, pp. 1898-1949, thirdquarter 2024, doi: 10.1109/COMST.2024.3367535.
14. H. -C. Chen, C. Damarjati, E. Prasetyo, C. -L. Chou, T. -L. Kung and C. -E. Weng, "Generating Multi-Issued Session Key by Using Semi Quantum Key Distribution With Time-Constraint," in IEEE Access, vol. 10, pp. 20839-20851, 2022, doi: 10.1109/ACCESS.2022.3151890.
15. N. Ul Ain et al., "A Novel Approach Based on Quantum Key Distribution Using BB84 and E91 Protocol for Resilient Encryption and Eavesdropper Detection," in IEEE Access, vol. 13, pp. 32819-32833, 2025, doi: 10.1109/ACCESS.2025.3539178.
16. S. Ricci, P. Dobias, L. Malina, J. Hajny and P. Jedlicka, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 12, pp. 23206-23219, 2024, doi: 10.1109/ACCESS.2024.3364520.
17. O. Shirko and S. Askar, "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking," in IEEE Access, vol. 11, pp. 21641-21654, 2023, doi: 10.1109/ACCESS.2023.3251649.
18. B. Djordjevic, "Hybrid QKD Protocol Outperforming Both DV- and CV-QKD Protocols," in IEEE Photonics Journal, vol. 12, no. 1, pp. 1-8, Feb. 2020, Art no. 7600108, doi: 10.1109/JPHOT.2019.2946910.
19. A. Bhatia, S. Bitragunta and K. Tiwari, "PUF-AQKD: A Hardware-Assisted Quantum Key Distribution Protocol for Man-in-the-Middle Attack Mitigation," in IEEE Open Journal of the Communications Society, vol. 6, pp. 4923-4942, 2025, doi: 10.1109/OJCOMS.2025.3575206.
20. B. Djordjevic, "QKD-Enhanced Cybersecurity Protocols," in IEEE Photonics Journal, vol. 13, no. 2, pp. 1-8, April 2021, Art no. 7600208, doi: 10.1109/JPHOT.2021.3069510.
21. N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik and M. Z. Win, "MIMO Terahertz Quantum Key Distribution Under Restricted Eavesdropping," in IEEE Transactions on Quantum Engineering, vol. 4, pp. 1-15, 2023, Art no. 4100315, doi: 10.1109/TQE.2023.3264638.
22. Y. Tanizawa et al., "Quantum Key Distribution Network and Quantum Secure Cloud Technologies for Genome Medicine Use Cases," in IEEE Transactions on Quantum Engineering, vol. 6, pp. 1-15, 2025, Art no. 4101215, doi: 10.1109/TQE.2025.3611335.
23. H. Wang et al., "Resilient Quantum Key Distribution (QKD)-Integrated Optical Networks With Secret-Key Recovery Strategy," in IEEE Access, vol. 7, pp. 60079-60090, 2019, doi: 10.1109/ACCESS.2019.2915378.
24. C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang and C. Pei, "Multicarrier Multiplexing Continuous-Variable Quantum Key Distribution at Terahertz Bands Under Indoor Environment and in Inter-Satellite Links Communication," in IEEE Photonics Journal, vol. 13, no. 4, pp. 1-13, Aug. 2021, Art no. 7600113, doi: 10.1109/JPHOT.2021.3098717.
25. M. Mehic, S. Rass, E. Dervisevic and M. Voznak, "Tackling Denial of Service Attacks on Key Management in Software-Defined Quantum Key Distribution Networks," in IEEE Access, vol. 10, pp. 110512-110520, 2022, doi: 10.1109/ACCESS.2022.3214511.