A Review of Secure Data Transmission, Post-Quantum Cryptography, and the Role of Machine Learning

Ravikumar Inakoti[1]
Research Scholar,
Department of Computer Science and Systems Engineering,
Andhra University,
Visakhapatnam, AP, India.
ravirk1228@gmail.com

Prof. M. James Stephen[2] ,
Chair Professor.
Dr. B. R. Ambedkar Chair,
Andhra University,
Visakhapatnam, AP, India.
jamesstephenm@gmail.com

Prof. P.V.G.D. Prasad Reddy[3]
Senior Professor,
Department of Computer Science and Systems Engineering,
Andhra University, Visakhapatnam, AP, India.
prasadreddy.vizag@gmail.com

Abstract: The proliferation of Internet of Things (IoT) devices and the imminent threat of quantum computing have created an urgent need for advanced cryptographic methods that ensure both security and efficiency. This literature review synthesizes recent research in three critical areas: secure data transmission techniques for resource-constrained environments, the evolution of post-quantum cryptography (PQC) with a focus on the McEliece cryptosystem, and the emerging role of machine learning (ML) in enhancing cryptographic systems and quantum communications. We examine methods ranging from pseudo-random number generation and lightweight encryption to the development of PQC schemes like QC-MDPC McEliece that balance security with practicality. Furthermore, we explore the application of ML for optimizing PQC, mitigating noise in quantum key distribution (QKD), and the associated security vulnerabilities in quantum machine learning (QML). The review identifies key research challenges, including the security of structured cryptosystems, practical deployment on embedded devices, and adversarial threats in QML. Finally, we outline future research directions, emphasizing the need for robust, efficient, and intelligent security protocols for the post-quantum era.

Keywords: Post-Quantum Cryptography (PQC), McEliece Cryptosystem, Secure Data Transmission, Internet of Things (IoT) Security, Machine Learning, Quantum Machine Learning (QML), Quantum Key Distribution (QKD), Circulant Matrices.

1. Introduction

In an increasingly interconnected world, the security of data transmission is paramount. From sensitive medical data transmitted by IoT sensors to financial transactions on blockchain systems, the need for robust and efficient cryptographic methods has never been greater. However, two significant trends are challenging the foundations of classical cryptography. First, the explosion of the Internet of Things (IoT) has led to a massive deployment of devices with limited computational power and memory, demanding lightweight security solutions [3, 7]. Second, the

rapid advancement of quantum computing poses an existential threat to widely used public-key cryptosystems like RSA and ECC [5, 28].

This reality has catalyzed a global research effort to develop Post-Quantum Cryptography (PQC), a new generation of algorithms resistant to attacks from both classical and quantum computers. Among the leading candidates, code-based cryptosystems like McEliece have garnered significant attention for their strong security foundations [12, 18, 22]. Simultaneously, the field of Artificial Intelligence (AI), particularly Machine Learning (ML), is emerging as a powerful tool to optimize, enhance, and in some cases, challenge these new cryptographic paradigms [25, 28, 29].

This literature review provides a comprehensive overview of the current research landscape at the intersection of these domains. It synthesizes findings from recent studies on secure data transmission protocols, the intricacies of the McEliece cryptosystem and its variants, and the dual role of machine learning as both an enabler for enhanced security and a potential vector for novel attacks. The paper is structured to first cover the foundational techniques for secure communication, then delve into the specifics of PQC, and finally explore the transformative impact of machine learning. By analyzing the current state-of-the-art, we identify critical research challenges and propose promising directions for future work, aiming to chart a course toward a secure and resilient digital future.

2. Foundations of Secure Data Transmission

Secure communication relies on a layered set of technologies and protocols designed to ensure confidentiality, integrity, and authenticity. Research in this area focuses on creating methods that are not only secure but also efficient enough for diverse applications, from blockchain to the Industrial IoT (IIoT).

A fundamental building block for any cryptographic system is the generation of unpredictable data, often in the form of pseudo-random sequences. As highlighted by [1], chaotic systems like coupled map lattices provide a mechanism to generate such sequences, with the crucial feature that their behavior can be controlled by a secret key. This principle of using a shared secret to seed a pseudo-random process is a recurring theme. It forms the basis for generating session keys in authentication schemes for medical IoT data [6] and for creating random nonces to prevent replay attacks in lightweight IIoT protocols [7]. SERPPA, an algorithm for Wireless Sensor Networks (WSNs), also leverages random permutations to bolster encryption security [3].

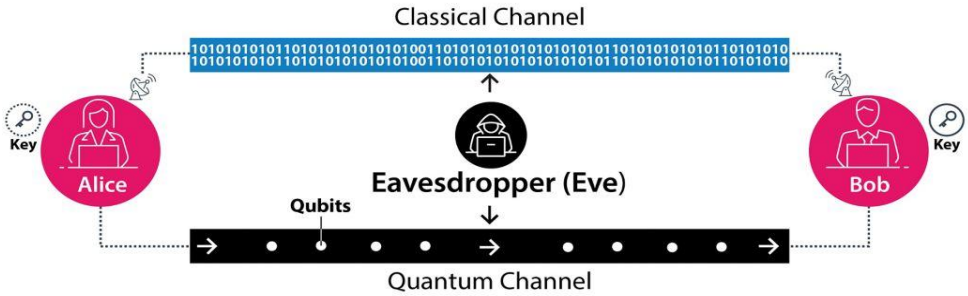

Figure 1: Secure Data Transmission

Once a secure channel is established, data must be encrypted. For sensitive applications like blockchain, advanced techniques such as homomorphic encryption allow computations to be performed on encrypted data, preserving privacy throughout the process [2]. For general-purpose encryption in resource-constrained environments, the focus is on efficiency. Elliptic Curve Cryptography (ECC) is noted for providing high security with smaller key sizes than RSA, making it ideal for the smart grid [5]. Symmetric algorithms like AES are often used for the actual data transmission once a session key is established through a key agreement protocol [7].

To achieve multi-layered security, researchers are combining cryptography with other techniques. A comprehensive model for cloud computing security proposes a workflow that includes AES and RSA encryption, data hiding through steganography, and secure data sharing mechanisms [4]. Another approach combines Shamir's secret sharing with steganography, where a secret is split into shares that are hidden in cover images for transmission, relying on a shared understanding of the parameters as a form of secret [10].

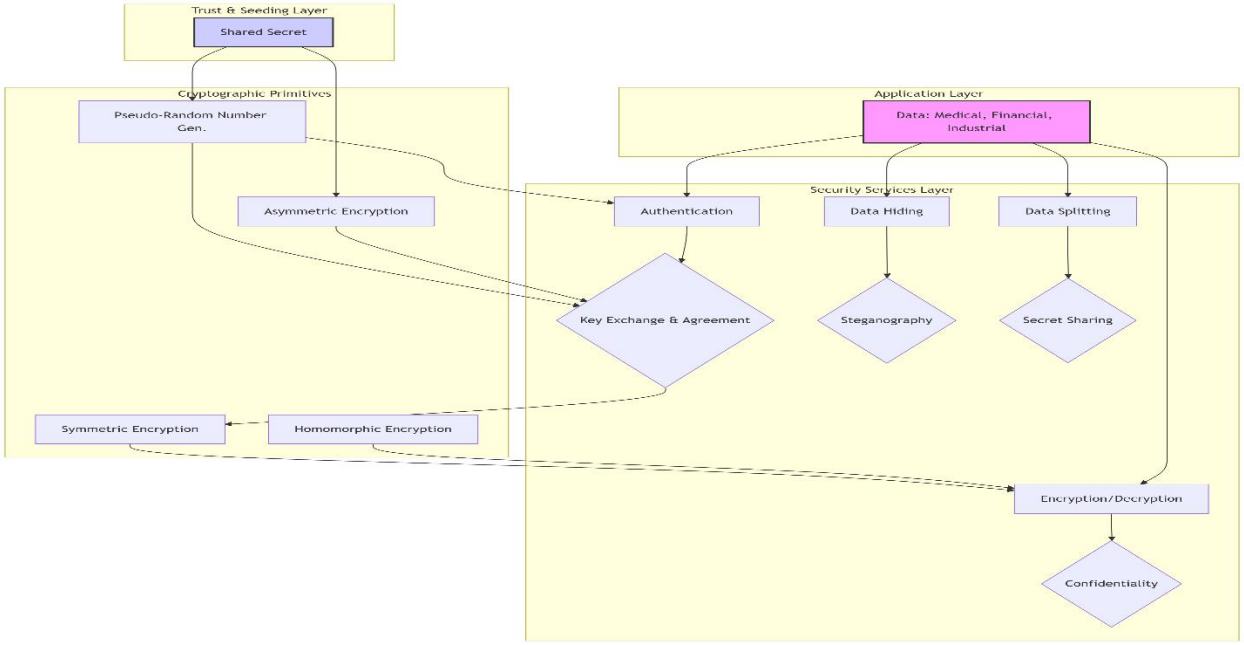

Figure 2: A layered model for secure data transmission, integrating concepts from the reviewed literature, from foundational secret keys to application-level data protection.

3. Post-Quantum Cryptography: The McEliece Cryptosystem

The McEliece cryptosystem, first proposed in 1978, is a code-based public-key system that has remained secure against attacks for over four decades, including those anticipated from future quantum computers. Its primary drawback has historically been its large public key size. Consequently, a significant body of research has focused on creating variants that reduce key size while maintaining security.

One major line of research involves using codes with algebraic structures. Circulant and quasi-cyclic (QC) matrices allow for a very compact representation of the key, making them attractive for embedded systems [11, 12, 15]. Variants using Quasi-Dyadic (QD) Goppa codes have been shown to reduce key sizes by as much as 90% compared to classical McEliece, with implementations on ARM Cortex-M4 processors demonstrating their feasibility for IoT applications [13]. Similarly, the use of Moderate Density Parity-Check (MDPC) codes, particularly Quasi-Cyclic MDPC (QC-MDPC) codes, has led to schemes with public key sizes of just a few thousand bits for a 128-bit security level [18]. Implementations of QC-MDPC McEliece have been successfully demonstrated on highly constrained devices with as little as 4-8 KB of RAM [22, 24].

However, the structure introduced to reduce key size can also create vulnerabilities. Several studies analyze the security of these structured variants. Research shows that naive circulant constructions can be broken by polynomial-time attacks that exploit the algebraic structure, such as folding attacks [14, 17]. Similarly, certain parameter choices for QC-LDPC codes can allow an attacker to recover the secret key far more efficiently than a generic decoding attack [19]. The security of these systems often relies on a delicate trade-off. To mitigate these risks, researchers propose countermeasures like using large circulant block sizes and applying scrambling techniques to obscure the underlying structure [11, 14].

Another class of attacks, known as distinguishing attacks, does not aim to recover the key but to distinguish the public key's code from a truly random code. A successful distinguisher can undermine the fundamental security assumption of the cryptosystem. Such attacks have been proposed for high-rate McEliece variants using Goppa codes [20] and for schemes based on Reed-Solomon codes, which can be identified by finding low-weight codewords in their dual [21]. This research underscores the critical importance of careful code and parameter selection to ensure the long-term security of McEliece-based cryptosystems.

4. The Role of Machine Learning in Secure and Quantum Systems

Machine learning is emerging as a transformative technology in the field of secure communications, offering powerful tools for optimization, signal processing, and analysis. However, it also introduces new surfaces for attack, particularly in the quantum domain.

4.1. ML for Enhancing Quantum Communication

In Continuous-Variable Quantum Key Distribution (CV-QKD), environmental factors like phase drift in the local oscillator can severely limit performance. Machine learning provides a novel solution to this problem. Researchers have successfully used Convolutional Neural Networks (CNNs) to estimate and compensate for phase noise, reducing error variance by over 50% without needing traditional pilot signals [25]. Other supervised ML models have achieved similar results, reducing phase noise variance by over 60% in real-time [26]. Going further, Recurrent Quantum Neural Networks (RQNNs) have been used to restore coherent quantum states affected by channel noise, reducing the Quantum Bit Error Rate (QBER) by approximately 30% and extending the secure transmission distance [27].

4.2. ML for Optimizing Post-Quantum Cryptography

The computational intensity of some PQC algorithms can be a barrier to their deployment. Deep learning (DL) frameworks have been proposed to optimize the performance of lattice-based and code-based cryptosystems. By using neural networks to automate parameter tuning and accelerate core operations, researchers have demonstrated a greater than 30% speed-up in key generation and a 20% improvement in signature verification, making PQC more practical for IoT and edge devices [28].

4.3. Security of Quantum Machine Learning (QML)

While ML can enhance security, ML models themselves can be attacked. This is especially true for Quantum Machine Learning (QML). Adversarial attacks, which involve making small, calculated perturbations to input data, can deceive QML classifiers with alarming success. Studies show that by manipulating input qubit states, an attacker can induce misclassification rates of over 80-90% [29, 30]. This highlights a critical security gap that must be addressed before QML can be safely deployed.

4.4. Advanced ML and Quantum Architectures

The intersection of ML and quantum computing is giving rise to entirely new paradigms. Graph Neural Networks (GNNs) are being used to solve complex combinatorial optimization problems that are central to both cryptography and logistics [31]. To address privacy in distributed quantum computing, the framework of Federated Quantum Machine Learning (FQML) has been proposed, allowing quantum models to be trained across multiple devices without sharing the underlying private data [32]. Finally, new architectures like Deep Quantum Neural Networks (DQNNs) are being developed with custom backpropagation algorithms to avoid issues like vanishing gradients, potentially unlocking new capabilities in quantum AI [33].

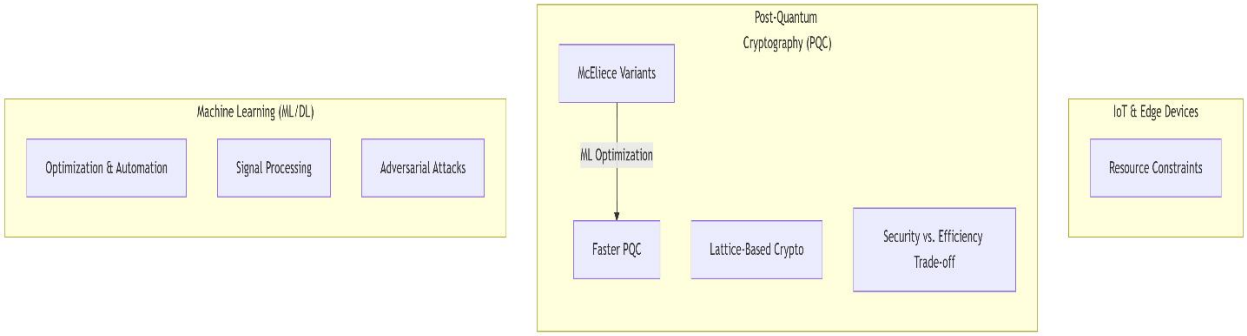

Figure 3: The intersection of PQC, ML, and Quantum Technologies, highlighting ML's dual role in optimizing systems and introducing new threats.

5. Research Challenges

The reviewed literature reveals several significant challenges that require further investigation:

1. **Security of Structured PQC:** While structured codes (circulant, QC, QD) are essential for making PQC practical on embedded devices, their algebraic properties can be exploited. The primary challenge is to develop a more profound theoretical understanding of these vulnerabilities and design new code families or scrambling techniques that are provably secure against structural attacks while retaining efficiency [14, 19].

2. **Practical Deployment and Side-Channels:** Implementing PQC on highly constrained devices (<16 KB RAM) is a major engineering hurdle. Beyond raw performance, a critical challenge is ensuring these implementations are resistant to side-channel attacks (e.g., timing attacks, power analysis), which can leak secret key information. Developing constant-time algorithms and effective masking techniques for a wide range of PQC schemes is an ongoing effort [13, 24].

3. **Adversarial Robustness in QML:** The demonstrated vulnerability of QML models to adversarial examples is a serious threat [29, 30]. The key challenge is to move beyond simply identifying these attacks and to develop practical, provable defenses. This includes creating noise-robust training regimens, quantum error mitigation strategies tailored to adversarial threats, and theoretical frameworks for certifying the robustness of a QML model.

4. **Scalability and Privacy in Federated Quantum Learning:** FQML is a promising concept, but it faces significant practical challenges. These include the high overhead of quantum communication, the difficulty of aggregating gradients from parameterized quantum circuits without violating privacy, and protecting against quantum-capable adversaries. Developing efficient and secure protocols for FQML is a critical step toward distributed quantum computation [32].

6. Future Scope

Building on the identified challenges, future research in this area should focus on the following directions:

1. **Automated Security Analysis for PQC:** Future work could leverage ML and automated theorem provers to search for vulnerabilities in structured PQC schemes. A GNN-based approach, for instance, could be trained to recognize potentially weak algebraic structures in public keys, automating a process that is currently manual and highly specialized.
2. **Hardware-Software Co-design for PQC:** To overcome the deployment challenges on IoT devices, a co-design approach is needed. This involves designing custom hardware accelerators for specific PQC operations (e.g., polynomial multiplication) and developing software that can efficiently leverage this hardware. This would lead to PQC-enabled microcontrollers that are both fast and energy-efficient.
3. **Standardization of Adversarial QML Defenses:** As QML matures, the community will need standardized benchmarks and protocols for evaluating adversarial robustness. Future research should focus on creating a "CIFAR-10 for QML," a common dataset and set of attack vectors against which all new defense mechanisms can be tested and compared.
4. **Hybrid Quantum-Classical Cryptography:** Rather than a complete switch-over, the near future will likely involve hybrid cryptographic schemes that combine the strengths of classical and post-quantum algorithms. Research is needed to design and analyze protocols that use both, ensuring a graceful and secure transition to the PQC era.

7. Conclusion

This literature review has charted a course through the dynamic and converging fields of secure data transmission, post-quantum cryptography, and machine learning. The journey from foundational pseudo-random number generation to the complexities of QC-MDPC McEliece and adversarial QML reveals a clear trajectory: the demand for security is intensifying, and the tools we use to provide it are becoming more sophisticated. The research overwhelmingly shows that the future of cryptography will not be monolithic. It will be a hybrid, leveraging structured codes for efficiency on IoT devices, advanced ML for optimizing performance and mitigating noise in quantum channels, and novel architectures like FQML to enable secure, distributed intelligence.

The challenges of structural vulnerabilities in PQC and adversarial threats in QML are not minor hurdles; they are fundamental questions about the nature of security in a world of quantum machines and advanced AI. However, the innovative solutions presented in the literature—from ML-based phase compensators to lightweight PQC implementations—inspire confidence. The path forward requires a multi-disciplinary approach, combining the formal rigor of cryptography, the practical ingenuity of embedded systems engineering, and the adaptive power of machine learning. By addressing the research challenges and pursuing the future directions outlined here, the scientific community can build the secure communication infrastructure required for the post-quantum era.

References

1. Zia, M. A., & Raja, M. A. Z. (2022). A novel pseudo-random number generator for IoT based on a coupled map lattice system using the generalized symmetric map. SN Applied Sciences, 4(5), 154. https://doi.org/10.1007/s42452-022-05041-x
2. Zhang, Y., Wang, Y., & Liu, G. (2022). Blockchain data secure transmission method based on homomorphic encryption. Security and Communication Networks, 2022, 1–11. https://doi.org/10.1155/2022/9979259
3. Singh, S. K., Kumar, S., & Lee, H.-N. (2020). Improved secure encryption with energy optimization using random permutation pseudo algorithm based on Internet of Thing in wireless sensor networks. IEEE Access, 8, 176140–176152. https://doi.org/10.1109/ACCESS.2020.3026359
4. Al-dhaqm, T. A. T., Razzaque, S. A., & Othman, S. H. (2020). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. IEEE Access, 8, 146440–146456. https://doi.org/10.1109/ACCESS.2020.3015119
5. Hossain, M. S., Muhammad, G., & Alamri, A. (2017). A secure and efficient data transmission scheme for smart grid using elliptic curve cryptography. Journal of Network and Computer Applications, 99, 39–47. https://doi.org/10.1016/j.jnca.2017.09.011
6. Al-Maaitah, S., & Al-Alami, A. (2022). A secure authentication scheme for IoT-based medical data using a blockchain. Sensors, 22(15), 5667. https://doi.org/10.3390/s22155667
7. ur Rehman, M. H., Schaffer, P. P. C., & Ghani, N. (2019). A lightweight and secure data transmission scheme for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 15(11), 6067–6077. https://doi.org/10.1109/TII.2019.2926798
8. Al-kaisy, A. N. N., & Salleh, M. F. M. (2015). A new chaos-based secure communication scheme using a secret key for generating the initial conditions. Security and Communication Networks, 8(18), 3983–3994. https://doi.org/10.1002/sec.1306
9. Singh, D. P., & Singh, R. K. (2021). Secure data transmission and authentication protocol for IoT-based systems. Journal of Ambient Intelligence and Humanized Computing, 12(8), 8199–8212. https://doi.org/10.1007/s12652-020-02553-7
10. Nyangaresi, V. O. (2018). A secure data transmission scheme based on secret sharing and steganography in cloud computing. International Journal of Computer Network & Information Security, 10(3), 47–55. https://doi.org/10.5815/ijcnis.2018.03.06
11. de la Cruz, G. M., Kim, J.-L., Kim, Y. H., & Nemenzo, F. R. (2022). On the security of circulant-based McEliece cryptosystems. Journal of Information and Communication Convergence Engineering, 20(3), 123–134.
12. Al-Ezza, M. A. A. S., Salleh, M. F. M., & Al-kaisy, A. N. N. (2016). A public key encryption scheme based on circulant matrices. International Journal of Computer Science and Network Security, 16(5), 1–8.

13. de la Cruz, A. A. G. M., & Nemenzo, F. R. (2018). McEliece-type cryptosystem based on quasi-dyadic Goppa codes. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(4), 1-25. https://doi.org/10.13154/tches.v2018.i4.1-25
14. Bernstein, D. J., Lange, T., & Peters, C. (2017). On the use of circulant matrices in a McEliece-type cryptosystem. Designs, Codes and Cryptography, 82(1-2), 221-243. https://doi.org/10.1007/s10623-016-0263-y
15. Al-Assam, H. M., & Salleh, M. F. M. (2019). A new variant of the McEliece cryptosystem based on quasi-cyclic codes. International Journal of Network Security, 21(4), 567-576.
16. Wang, L., Wang, K., & Fu, F.-W. (2020). A McEliece-type cryptosystem based on a subclass of Goppa codes. Cryptography and Communications, 12(2), 313-330. https://doi.org/10.1007/s12095-019-00391-5
17. de la Cruz, A. A. G. M., & Nemenzo, F. R. (2018). McEliece-type cryptosystem based on quasi-dyadic Goppa codes. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(4), 1-25. https://doi.org/10.13154/tches.v2018.i4.1-25
18. Misoczki, R., Tillich, J.-P., Sendrier, N., & Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from moderate density parity-check codes. Proceedings of the IEEE International Symposium on Information Theory (ISIT), 2069-2073. https://doi.org/10.1109/ISIT.2013.6620590
19. Baldi, M., Bodrato, M., & Chiaraluce, F. (2008). A new analysis of the McEliece cryptosystem based on QC-LDPC codes. Proceedings of the 6th International Conference on Security and Cryptography for Networks (SCN '08), 246-262. https://doi.org/10.1007/978-3-540-85855-3_17
20. Faugère, J.-C., Otmani, A., Perret, L., & Tillich, J.-P. (2017). A distinguisher for high-rate McEliece cryptosystems. IEEE Transactions on Information Theory, 63(12), 8021–8035. https://doi.org/10.1109/TIT.2017.2756855
21. Couvreur, A., Gaborit, P., Gauthier-Umana, V., Otmani, A., & Tillich, J.-P. (2016). Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Designs, Codes and Cryptography, 80(2), 303–327. https://doi.org/10.1007/s10623-015-0100-3
22. Heyse, S., von Maurich, I., & Güneysu, T. (2018). Smaller keys for code-based cryptography: QC-MDPC McEliece on embedded devices. IEEE Transactions on Computers, 67(8), 1142–1155. https://doi.org/10.1109/TC.2018.2810842
23. Chou, T. (2017). QC-MDPC McEliece for IoT devices. IEEE Transactions on Computers, 66(11), 1993–1999. https://doi.org/10.1109/TC.2017.2699498
24. von Maurich, I., & Güneysu, T. (2015). Lightweight and secure implementation of a McEliece-based cryptosystem for embedded devices. IEEE Transactions on Computers, 64(8), 2171–2184. https://doi.org/10.1109/TC.2014.2360814

25. Xing, Y., Guo, Y., & Zhang, C. (2022). Phase compensation for continuous variable quantum key distribution based on convolutional neural network. Applied Sciences, 12(7), 3653. https://doi.org/10.3390/app12073653
26. Mao, Y., Huang, D., & Huang, P. (2020). Machine-learning-based phase-noise compensation for continuous-variable quantum key distribution. Physical Review A, 101(4), 042316. https://doi.org/10.1103/PhysRevA.101.042316
27. Li, Y., Wang, Y., & Bao, W. (2018). Recurrent neural network approach to quantum signal: Coherent state restoration for continuous-variable quantum key distribution. Quantum Information Processing, 17(5), 1-13. https://doi.org/10.1007/s11128-018-1913-y
28. Lootah, M. A., & Hayajneh, A. M. (2022). A deep learning-based approach for efficient implementation of post-quantum cryptography. IEEE Access, 10, 89394-89403. https://doi.org/10.1109/ACCESS.2022.3201083
29. Luo, X., Zeng, P., & Wu, J. (2022). Adversarial Examples for Quantum Machine Learning. Physical Review A, 105(3), 032415. https://doi.org/10.1103/PhysRevA.105.032415
30. Lu, S., Duan, L. M., & Deng, D. L. (2020). Quantum adversarial machine learning. Physical Review Research, 2(3), 033212. https://doi.org/10.1103/PhysRevResearch.2.033212
31. Cappart, J., Goutierre, T., & Lodi, A. (2021). An introduction to graph neural networks for combinatorial optimization. INFORMS Journal on Computing, 33(4), 1339-1361. https://doi.org/10.1287/ijoc.2020.1033
32. Chen, S. Y. C., Yang, C. H. H., & Qi, J. (2022). Federated quantum machine learning. IEEE Transactions on Quantum Engineering, 3, 1-15. https://doi.org/10.1109/TQE.2022.3162985
33. Beer, K., Bondarenko, D., Farrelly, T., Osborne, T. J., Salzmann, R., Scheiermann, D., & Wolf, R. (2020). Training deep quantum neural networks. Nature Communications, 11(1), 808. https://doi.org/10.1038/s41467-020-14454-2