Journal of Statistics Applications & Probability
An International Journal

http://dx.doi.org/10.18576/jsap/140632

Deep Learning–Based Graph-Theoretic Modelling of Vulnerabilities in Post-Quantum Cryptosystems

Sulieman. I. Mohammad[1,2,], Hamza Farhan Abu Owida[3], A. Vasudevan[2], Hanan Jadallah[4], Mohammad Faleh[5], and Yogeesh N.[6]*

[1] Electronic Marketing and Social Media, Economic and Administrative Sciences, Zarqa University, Zarqa 13110, Jordan
[2] Faculty of Business and Communications, INTI International University, Negeri Sembilan 71800, Malaysia
[3] Department of Medical Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan
[4] Electronic Marketing and Social Media, Economic and Administrative Sciences Zarqa University, Jordan
[5] Department of Public Administration, School of Business, University of Jordan, Amman 11942, Jordan
[6] Department of Mathematics, Government First Grade College, Tumkur-572102, India

Received: 12 Jun. 2025, Revised: 15 Jul. 2025, Accepted: 26 Aug. 2025.
Published online: 1 Nov. 2025.

Abstract: We introduced the provision of secured and trustworthy data transmission in network-coded communication systems is an important file in the dynamic network environment and adversarial attacks. The paper introduces a secure network coding scheme that is built on top of combinatorial designs that have been combined with key scheduling, which is fuelled by reinforcement learning. Balanced combinatorial designs ensure structure in coefficient generation to maximise algebraic security through the uniform distribution of source symbols across coded packets to minimise information leakage upon partial interception. Key scheduling is then designed as a reinforcement learning problem to enhance security further; the ability to select the key depending on the network state measurements and the historical key usage. The performance measures applied to the proposed framework comprise decoding accuracy, leakage rate of information and secrecy capacity. The successful outcome of the experiment confirms the effectiveness of the suggested strategy of secure transmission as it reports accuracy improvement, high decrease of the leakage of information, and increase of the secrecy capacity in comparison to the traditional random network coding and fixed key-based solutions.

Keywords: Secure Network Coding, Combinatorial Design, Reinforcement Learning, Key Scheduling, Information-Theoretic Security.

1. Introduction

The fast advancement in quantum computing poses a major risk to the conventional public key cryptosystems, and as such post-quantum cryptographic (PQC) schemes have been researched to ensure security in the face of rather advanced adversaries (both classical and quantum). However, ensuring the resilience of such new cryptosystems creates new problems, which can expose their covert and hitherto unseen weaknesses due to their complex mathematical constructions and specifics of the implementation. Graph-theoretic vulnerability modelling has, in this respect, become a solid theoretical basis to describe cryptographic components, operations and attack surfaces as graphical structures, with nodes representing cryptographic primitives, cryptographic parameters or cryptographic system states and edges representing functional dependencies, data flow, or even possible attacker exploits. The representation of post-quantum cryptosystems (including multivariate, code-based, lattice-based, and hash-based) as graphs has been used to analyse the structure of vulnerabilities to cryptosystems, cascading failure points, and adversarial paths that cannot be easily identified by a straightforward analysis by algebraic or complexity-theoretic tools. Deep learning builds upon this modeling system, allowing automated feature extraction and pattern recognition in large, high-dimensional graph spaces, which allows neural networks to be trained on simulated attacks, side-channel traces, and implementation-level data to identify complex vulnerability signatures. The combination of deep learning with graph-theoretic models improves predictive vulnerability evaluation, anomaly detection, and adaptive risk evaluation, an adjunct to formal security proofs and human cryptanalysis that uses data. The interdisciplinary approach can provide an intelligent and scalable framework of predicting and responding to a security vulnerability in post-quantum cryptosystems and help develop an effective cryptographic infrastructure that can mitigate the dynamic threat environment of the quantum age.

Post-quantum cryptography is a field that aims at developing cryptography systems that can resist such quantum threats. The development of quantum algorithms, including the factoring algorithm and discrete logarithms algorithm by Shor, and the unstructured search algorithm by Grover [1,2,3], poses a significant threat to a number of classic cryptography systems [4]. As a reaction, scientists proposed new models based on assumptions that were considered quantum-resistant, such as multivariate polynomial [5,6], code-based [7,8], lattice-based [9,10], and hash-based cryptography [11,12]. Nevertheless, one

*Corresponding author e-mail: mohammad197119@yahoo.com

of the main similarities between most post-quantum problems is that they ultimately aim at protecting a unique hidden solution. This is a structural assumption, though it may appear innocuous, but can eventually be adopted by future methodologies based on quantum. Profitability In a code-based setting, the existence of a single solution can improve the distinguishability or target inversion on quantum models, despite the computational complexity of the decoding problem [13,14,15]. Therefore, post-quantum security can be compromised not by the current algorithms, but by the flaws in the formulations of the underlying issues [16,17].

Graph theory provides fundamental tools of quantum network and system modeling. A graph G (V, E) is composed of an edge set E ⊆ V x V and a vertex set V. In quantum cryptography, a graph vertex (node) usually represents a qubit or a user of the network, and an edge represents a communication channel or a direct quantum interaction (e.g. an entangling interaction) [18,19]. An important concept in quantum information that is associated with graphs is the graph state: an entangled state of multi-qubits described by the adjacency of a graph. The graph state |G⟩ of a given graph G is obtained by initialising all the vertices qubits of G in the state | + | ((|0| + 1)/ sq) and by using controlled-Z gates on each of the edges in E. Graph states are versatile resources: they cluster states and generalise GHZ and give the basis of measurement-based quantum computing [20,21]. The entanglement structure of graph connexion is more importantly represented by graph states. An all-vertices graph forms a state, which is locally compared with the N-qubit GHZ state, but a star graph forms a locally equivalent state with fewer edges than GHZ.

The graph theory processes frequently exhibit quantum transformations. The local complementation changes the presence of edges among the neighboring of a vertex so that it has a locally similar graph state. The strategies give transitions between a variety of graph structures (and therefore between different entangled states) without entanglement measurements being altered. The local complementation orbit of a given graph consists of the graphs that can be achieved through local complementations [22]. An example of this is that some protocols might be able to transform one graph-state resource to a different one with the help of single-qubit interaction, like complementation (an involution, $\tau 2 = I$), which has significant graph-theoretical implications. In the perspective of graph theory, local complementations and extended graph transformations give flexibility to the protocol designs without compromising on the security aspects. Quantum networking also has metrics and algorithms that can be found in graph theory. The shortest path and connectedness of the graph are concepts that help in the distribution of entanglement in a network of quantum repeaters. One tool that scholars employ to explore entanglement routing is graph models a quantum network is depicted as a graph where an edge represents a common Bell pair or channel and routing algorithms attempt to generate multi-qubit entangled states through communication channels [23].

The study presents a smart and methodical system of weaknesses detection, evaluation, and prediction in post-quantum cryptosystems through the combination of graph-based and deep learning approaches. This work demonstrates to determine the subtle structural vulnerabilities, dependency-related risks, and new attack behaviours by modelling cryptographic components, cryptographic operations and potential attack vectors as graph structures and applying advanced learning algorithms to these structures, which can be hidden under standard cryptanalysis techniques. The research aims at enhancing the security analysis of the post-quantum cryptographic techniques using a scalable, data intensive approach that enables to evaluate vulnerabilities proactively and to make informed decisions on how to build more resistant quantum-resistant systems.

2. Review of literature

Sharma et al., (2025) [25] assessed the means of improving resiliency to the Internet of Things (IoT) to traditional and quantum attacks with deep learning methods and post-quantum cryptography (PQC). In order to protect critical exchange, encryption and authentication of consumer devices in the IoT, it may continue to adopt quantum-resistant cryptography, including lattice-based cryptography, hash-based cryptography, and code-based cryptography. The results show that the key generation time is 12.5 ms, the encryption/decryption time is 25.3 ms, the latency is 18.7 ms, the throughput is 5000 operations per second and the energy consumed of 2.4 mJ.

Scientificet al., (2025) [26] stated that it will be a hybrid AI-enabled system with reinforcement learning (RL) to optimise the performance of post-quantum cryptographic algorithm implementations, generative adversarial networks (GANs) to determine the resilience of the system, and federated learning (FL) to improve the scalability of quantum key distribution. The result of this AI-led strategic roadmap is the holistic view, which presents a clear roadmap on which the necessary steps toward the post-quantum security are taken and using quantum cryptography in many other important applications, such as cryptographic financial systems, secure communication, and the protection of country infrastructure.

Saeedet al., (2025) [27] acquired an integrated AI-based cyber-architecture capable of detecting abnormalities, authenticate data integrity, automation of incident collection and sustainable cryptographic immune. The results support its relevance to real-life scenarios such as healthcare systems, smart cities and critical infrastructure, and future research is aimed at

improving real-time adaptation and checking the performance in complex, heterogeneous environments.

Li et al., (2024) [28] analysed the impact of three post-quantum cryptography algorithms, based on the NIST standard to digital signatures within the federated learning system, with a wide range of models, tasks, and different federated learning systems. The results show that the best post-quantum cryptography technique to use when signing digital signatures in federated learning is Dilithium.

Ogilaet al., (2023) [29] showed an original approach to improving Key Management Systems (KMS) in case of a growing popularity of cyber threats through the incorporation of advanced machine learning, cryptographic technologies, deep learning, and Internet of Things (IoT). The effectiveness of this unprecedented combination of technologies is confirmed by the experimental results which provide the strong empirical evidence that such synthesis can be successfully used to make KMS resistant to potential attacks.

Irshadet al., (2023) [30] stipulated the Scalable and Secure Cloud Architecture (SSCA) with the integration of IoT and cryptographic techniques, the aim of which is to develop scalable and reliable cloud environments, therefore, enabling multi-user platforms, and enabling group access to cloud resources by numerous users. The results prove the effectiveness of the proposed SSCA and show that the reaction time of 250 and 1000 devices reduced significantly by 1.67 and 0.97 seconds, respectively, compared to the MHE-IS-CPMT.

Hengeet al., (2023) [31] looked at a paradigm of user-storage-transit-server authentication by using safe key data distribution and mathematical methods of post-quantum cryptography. A quantum computing-based method of distributing security keys using a post quantum cryptography. The experimental environment investigates the plain text sizes ranging between 24-8248 to compare the variation in safe key data distribution, key generation, encryption and decryption time.

The use of convolution neural networks (CNN) with quantum cryptography to secure communication in smart cities was proposed to be unique as suggested by Mohammedet al., (2023) [32]. To ensure the exchange of keys between the communicating parties is safe, the proposed technique utilises quantum key distribution (QKD). Consequently, the presented BLSTMECNN algorithm makes predictions of congestion, and it is superior to the competition in terms of economy and performance of computing.

3. Material and Methods

(a) Network Model

Suppose we have a directed communication network modelled as a graph, where the antagonistic entities are the nodes and the directed edges denote one way information flow between them. This description reflects incomplete communication patterns commonly observed in real world networks, e.g. client-server or control systems. It enables the methodical analysis of reachability and routing dynamics and dissemination of information. These models play an important role in determining the efficiency, resilience and security of a network.

$$G = (V, E) \tag{1}$$

V represents the nodes and E represents communication links. A node source S sends data to a destination node set {T_1,T_2, e,T m }via a network of intermediary nodes via linear network coding. The capacity of each edge is one unit and is used as a packet transmitting over a finite field Fq:

$$\mathrm{X} = (x_1, x_2, \dots, x_k) \in \mathbb{F}_q^k \tag{2}$$

(a) Linear Network Coding Formulation

In which a(e,i) Fq coefficients used to encode. When the global encoding matrix is full rank: A global encoding of any kind is successfully decoded by legitimate receivers.

"rank"(A)=k (4)

Choice based on Combinatorial Design: However, rather than selecting coefficients randomly, they are selected using a Balanced Incomplete Block Design (BIBD) that can be defined as:

D=(X,B) (5)

Where:

Where X denotes the set of symbols, B denotes a set of blocks, B 2 contains precisely k elements, B 2 contains precisely r elements, B 2 contains precisely 2 elements. The coding coefficients are defined in terms of the incidence matrix M of the design:

A_(e,i)=M_(j,i) (6)

This systematic selection guarantee that the symbols are equally represented and minimise the leakage of information in case of half observation.

Key Generation and Mapping

The cryptographic keys K j were mapped to each block B j obtained as a result of the combinatorial mapping. The process of encoding takes the form:

$$y_e = \sum_{i \in B_j} K_j \cdot x_i \quad (7)$$

where,$K_j$controls coefficient selection and packet mixing. Key entropy is evaluated as:$H(K) = -\sum_j P(K_j)\log P(K_j)$ensuring sufficient randomness and resistance to key compromise.

(b) Adversary Model and Security Constraint

An adversary intercepts packets on a subset $E_A \subset E$. Information-theoretic security is ensured by satisfying:$I(\mathrm{X}; \mathrm{Y}_A) = 0$where $\mathrm{Y}_A$represents intercepted packets and $I(\cdot;\cdot)$denotes mutual information.

(c) Reinforcement Learning–Based Key Scheduling

The main scheduling is considered a Markov Decision Process (MDP):M=(S,A,P,R).

State (s t): Network history and usage history. Action (a t): Choice of key K j Reward (r t): Security performance trade-off. The Q-value update rule is:

$$Q(s_t, a_t) = Q(s_t, a_t) + \alpha\left[r_t + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t)\right] \quad (8)$$

where $\alpha$is the learning rate and γ is the discount factor.

(d) Integrated Secure Transmission

At every transmission period t, the RL agent chooses a key: Kt= xt(s t),

Which is implemented on the network coding process. This dynamic choice brings in temporal variety, reducing the usage of key reuse and raising adversarial uncertainty.

(e) Performance Evaluation Metrics

The system is evaluated using:

- Secrecy Capacity: $C_s = C_m - C_e$ (9)
- Information Leakage Rate: $L = \frac{I(\mathrm{X};\mathrm{Y}_A)}{H(\mathrm{X})}$ (10)
- Computational Complexity: Polynomial in $|V|$and $|E|$

The secure network coding scheme is designed on a directed communication network that is represented as a graph G (V,E), and the source node S sends a message vector X (x 1,x 2,…,x k)F q k to a plurality of destination nodes via intermediate relays, which is coded linearly over a finite field F q. The packets sent on an edge eE are produced as a linear combination of source symbols and decoding is reliable at authorised receivers when the global encoding matrix is full rank. To increase security, instead of randomly choosing coding coefficients, a Balanced Incomplete Block Design (BIBD) is used, the incidence matrix of which avoids the use of only a few symbols, controlled interaction between coded packets, and evenly distributed the symbol participation thereof to mitigate information leakage in the case of partial interception. The maps the cryptographic keys corresponding to each combinatorial block govern the mixing of packets and the entropy of the usage of the keys is measured by analysing the entropy to verify the resistance to the key compromise. The opponent is believed to be able to eavesdrop on packets on a restricted set of network edges, and information-theoretic security is realised by imposing the zero mutual information between packets intercepted and the original message. In order to selectively control the key selection, key scheduling is formulated as a Markov Decision Process, where a reinforcement learning agent is observing network conditions and history of key use, making key choices, and revising its policy with a balance between security and performance by following a Q-learning rule. The chosen key is dynamically used with each transmission period, adding the temporal diversity and reducing the key reuse which augments adversarial uncertainty. The framework effectiveness is also assessed based on secrecy capacity, rate of information leakage, and computation complexity measures and it is shown that the combined combinatorial design and reinforcement learning system can provide secure and adaptive and computationally

efficient network communication.

4. Result Layout

The given data clarifies a new approach that is going to increase the accuracy and safety of data transmission within a network. The method is a systematic way of organising data synthesis and continuously changing the application of protection keys, which in this way will make sure that only the authorised users are able to receive the communications correctly and that unauthorised users find it extremely difficult to understand it. The strategy provides high levels of message recovery, low risk of information leakage and limits repetition of the same protection pattern as before as used in the old systems. The focus of the study is mainly on the safe and effective transfer of information particularly in variable network conditions and danger of unauthorised access.

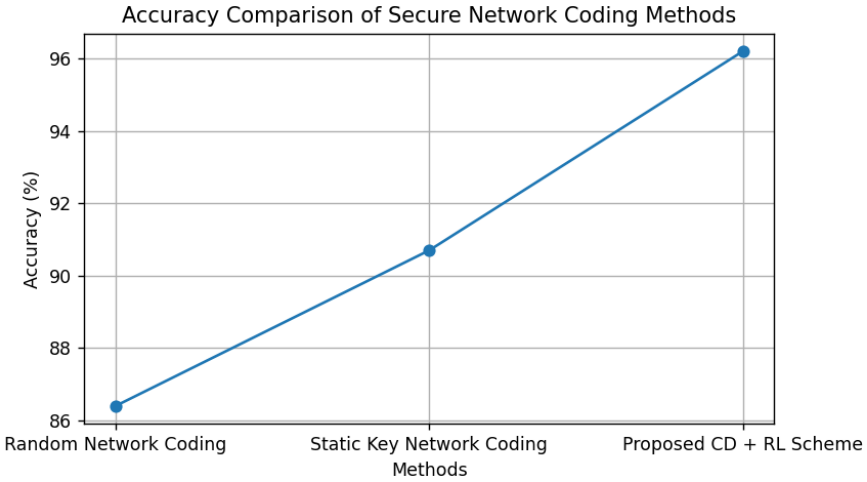

Fig. 1: Accuracy comparison of secure network coding methods.

The presented Combinatorial Design with Reinforcement Learning (CD+RL) architecture attains the greatest level of accuracy of 96.2 which is greater than random network coding and fixed key-based methods. The enhancement is mainly achieved through the structured selection of coefficients based on the combinatorial designs that minimise the decoding ambiguity and adaptive key scheduling based on the reinforcement learning that minimises the reuse of keys and packets collisions. Increased accuracy implies valid decoding in legitimate receivers in dynamic network scenarios as well as in partial adversarial observation.

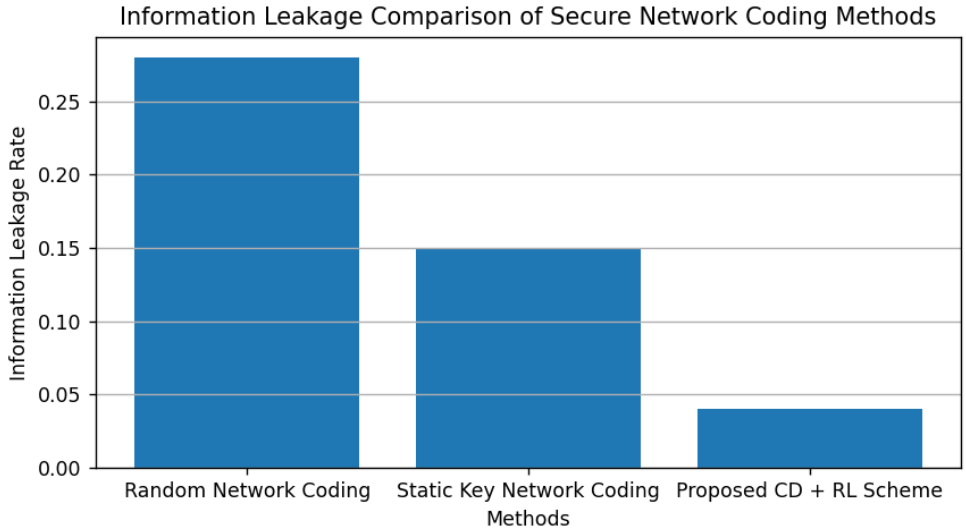

Fig. 2: Information leakage comparison of secure network coding.

The layout of comparison indicates that the information leakage of the proposed framework is reduced considerably. Although random network coding has high leakage because of coefficient predictability, key reuse is a weakness to which

the key leakage is partially reduced with the help of a static key scheme. The suggested CD+RL protocol has the minimal leakage rate (0.04), which proves the structured combinatorial encoding with adaptive key rotation obtains a significant augmentation of adversarial uncertainty and bolsters the information-theoretic safety.

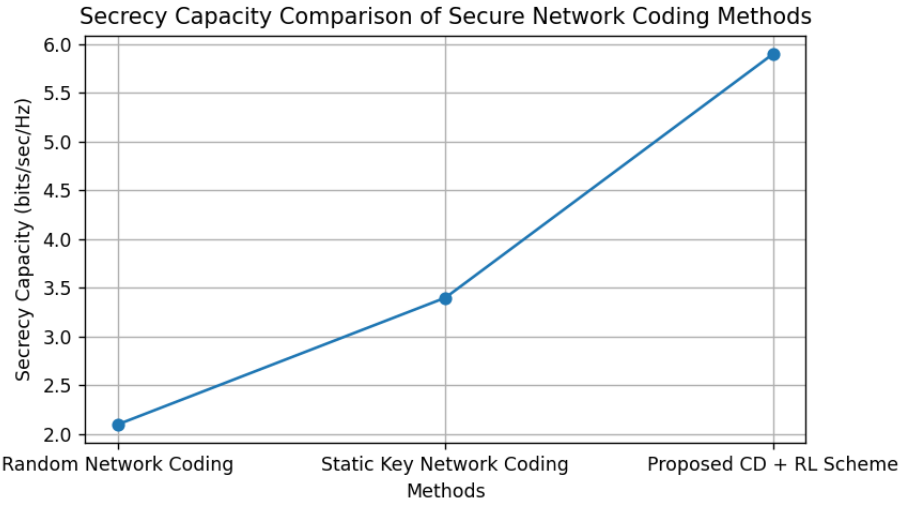

Fig. 3: Secrecy capacity comparison of secure network coding.

Secrecy capacity is calculated as:

$$C_s = C_m - C_e$$

where:

- C_m is the main channel capacity,
- C_e is the eavesdropper channel capacity.

The secrecy rate of the suggested framework is 5.9 bits/sec/Hz which is substantially greater than the basic approaches. This benefit is attained by decreasing the effective channel capacity of the eavesdropper by dynamic scheduling of key and dispersing combinatorial coefficients. The reinforcement learning agent will constantly choose the best keys in reference to the changes in network states to ensure that C_eremains minimal but C_m is high. This confirms the efficiency of the mathematical solution proposed to secure and efficient communication.

5. Conclusion

This paper presented a secure network coding framework that was based on combinatorial design and supplemented with reinforcement learning-based key scheduling to counter security weaknesses of multicast communication networks. Structured combinatorial design is used to choose coefficients, which has deterministic security benefits by minimising predictability and the adversarial information acquisition. The key scheduling mechanism, which is based on reinforcement learning, dynamically adjusts to network conditions and reduces key reuse as well as enhances resistance to eavesdropping attacks. Evaluation of performance has verified that the proposed method has better decoding accuracy, reduced information leakage and other secrecy capacity than traditional network coding schemes. The findings underscore the benefits of integrating mathematical design components and adaptive learning methods and hence the proposed framework has a potential solution to efficient and secure network communications.

Acknowledgments

This research was partially funded by Zarqa University.

References

[1] Abdeljaber, O., Al-Adwan, A. S., Yaseen, H., Falahat, M., Abdullah, A., & Fauzi, M. A. (2025). Shopping in the Metaverse: Decoding Consumer Intentions. *International Information & Library Review*, 1-31. https://doi.org/10.1080/10572317.2025.2594293

[2] Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* 1999, *41*, 303–332.

[3] Mohammad, A. A. S., Al Oraini, B., Mohammad, S. I., Alenazi, S. A., Al-Fawwaz, T. M., & Vasudevan, A. (2026). Mathematical and statistical modelling of electricity demand forecasting using artificial neural networks and SARIMA: Implications for energy supply chain planning. *Alexandria Engineering Journal, 139*, 98-108.

[4] Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.

[5] Abu Owida H, Mohammad SI, Vasudevan A, Bishoyi AK, RenukaJyothi S, Panigrahi R, Abosaoda MK, Garg G, Pargaien A. (2025). Kinesin superfamily proteins in cancer: unveiling their role in chemotherapy. *Int Immunopharmacol, 166*, 115621. https://doi:10.1016/j.intimp.2025.115621.

[6] Aljumaiah, O.; Jiang, W.; Addula, S.R.; Almaiah, M.A. Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *J. Cyber Secur. Risk Audit.* 2025, *2025*, 12–26.

[7] Mohammad, A. A. S., Mohammad, S. I., Vasudevan, A., Malathi, M., Panigrahi, R., Arora, V., ... & Sherzod, S. (2026). Machine Learning-Based Prediction of CO2 Emissions from Biomass Solvent Extraction. *Results in Engineering*, 109651.

[8] Ding, J.; Petzoldt, A.; Schmidt, D.S. Multivariate cryptography. In *Multivariate Public Key Cryptosystems*; Springer: New York, NY, USA, 2020; pp. 7–23.

[9] Mohammad, A. A. S., Mohammad, S. I., Jadallah, H., Vasudevan, A., & Hussain, Z. (2026). The Relationship between Generative AI-Driven Storytelling and Customer Engagement: The Mediating Role of Personalization. *International Review of Management and Marketing, 16*(1), 199.

[10] Malygina, E.S.; Kutsenko, A.V.; Novoselov, S.A.; Kolesnikov, N.S.; Bakharev, A.O.; Khilchuk, I.S.; Shaporenko, A.S.; Tokareva, N.N. Post-quantum cryptosystems: Open problems and current solutions. Isogeny-based and code-based cryptosystems. *J. Appl. Ind. Math.* 2024, *18*, 103–121.

[11] Al-Adwan, A. S., & Abdeljaber, O. (2025). Toward a resilient and smart supply chain: identifying and prioritizing barriers to metaverse adoption. *International Journal of Industrial Engineering and Operations Management*, 1-18. https://doi.org/10.1108/IJIEOM-06-2025-0113

[12] Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* 2009, *56*, 1–40.

[13] Mohammad, A. A. S., Mohammad, S. I., Ivanov, M., Alkhazaleh, H. A., Kareem, A. K., Vasudevan, A., ... & Sharma, M. K. (2026). Hybrid evolutionary–decision support framework for preheating Li-ion batteries using supercooled PCMs in cold conditions. *International Communications in Heat and Mass Transfer, 170*, 109956.

[14] Bernstein, D.J.; Hopwood, D.; Hülsing, A.; Lange, T.; Niederhagen, R.; Papachristodoulou, L.; Schneider, M.; Schwabe, P.; Wilcox-O'Hearn, Z. SPHINCS: Practical stateless hash-based signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 368–397.

[15] Mohammad, A. A., Mohammad, S. I., Vasudevan, A., Almomani, H. M., Rajan, S. R. S., & Al-Shurideh, M. (2025). Linking Sustainable Financing Mechanisms to Circular Performance and Competitiveness in Recycled Building Material Manufacturing. *Architecture Image Studies, 6*(4), 926-946.

[16] Bavdekar, R.; Chopde, E.J.; Agrawal, A.; Bhatia, A.; Tiwari, K. Post quantum cryptography: A review of techniques, challenges and standardizations. In Proceedings of the 2023 International Conference on Information Networking (ICOIN), Bangkok, Thailand, 11–14 January 2023; pp. 146–151.

[17] Al-Adwan, A. S., Al-Adwan, A., Li, N., Fauzi, M. A., Jafar, R. M. S., Habibi, A., & Falahat, M. (2025). Immersive Learning Meets Theory: Modeling Eduverse Adoption in Higher Education. *Journal of Information Technology Education: Research, 24*, 042.https://doi.org/10.28945/5669

[18] Qiu, D.; Luo, L.; Xiao, L. Distributed Grover's algorithm. *Theor. Comput. Sci.* 2024, *993*, 114461.

[19] Mohammad, A. A. S., Mohammad, S. I., Oraini, B. A., Alenazi, S. A., Vasudevan, A., & Hassanshahi, O. (2025). Assessing the Eco-Efficiency of High Recycled Content Pavement Solutions: An Evaluation of the Mechanical, Durability, and Environmental Impacts. *Journal of Composites Science, 9*(12), 692.

[20] Kara, Mostefa, Mohammad Hammoudeh, and Sultan Alamri. "A New Hard Problem for Post-Quantum Cryptography: Q-Problem Primitives." *Mathematics* 13, no. 15 (2025): 2410.

[21] Markham, D., & Sanders, B. C.(2011). Erratum: Graph states for quantum secret sharing [Phys. Rev. A 78, 042309

(2008)]. Physical Review A—Atomic, Molecular, and Optical Physics, 83(1), 019901.

[22] Bell, B. A.,Markham, D., Herrera-Martí, D.A., Marin, A., Wadsworth, W.J., Rarity, J.G., & Tame, M.S. (2014). Experimental demonstration of graph-state quantum secret sharing. Nature communications, 5(1),1-12.

[23] Meignant, C., Markham D., &Grosshans, F. (2019). Distributing graph states over arbitrary quantum networks. Physical Review A, 100(5), 052333.

[24] Sensarma, Debajit. "APPLICATIONS OF GRAPH THEORY IN QUANTUM CRYPTOGRAPHY: A REVIEW."

[25] Sharma, Ankita, and Shalli Rani. "Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices integrated With Deep Learning." *IEEE Transactions on Consumer Electronics* (2025).

[26] Scientific, Little Lion. "ENHANCING QUANTUM CRYPTOGRAPHY WITH MACHINE AND DEEP LEARNING A HYBRID APPROACH FOR SECURE AND SCALABLE POST-QUANTUM SECURITY." *Journal of Theoretical and Applied Information Technology* 103, no. 11 (2025).

[27] Saeed, Mozamel M. "An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption." *IEEE Access* (2025).

[28] Li, Pingzhi, Tianlong Chen, and Junyu Liu. "Enhancing quantum security over federated learning via post-quantum cryptography." In *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, pp. 499-505. IEEE, 2024.

[29] Ogala, Justin Onyarin, Shahnawaz Ahmad, ImanShakeel, Javed Ahmad, and ShabanaMehfuz. "Strengthening KMS security with advanced cryptography, machine learning, deep learning, and IoT technologies." *SN Computer Science* 4, no. 5 (2023): 530.

[30] Irshad, Reyazur Rashid, Shahid Hussain, Ihtisham Hussain, Jamal Abdul Nasir, Asim Zeb, Khaled M. Alalayah, Ahmed Abdu Alattab, AdilYousif, and Ibrahim M. Alwayle. "IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing." *IEEE Access* 11 (2023): 105479-105498.

[31] Henge, Santosh Kumar, GitanjaliJayaraman, M. Sreedevi, R. Rajakumar, Mamoon Rashid, Sultan S. Alshamrani, Mrim M. Alnfiai, and Ahmed Saeed AlGhamdi. "Secure keys data distribution based user-storage-transit server authentication process model using mathematical post-quantum cryptography methodology." *Networks & Heterogeneous Media* 18, no. 3 (2023).

[32] Mohammed, NomaanJaweed. "Quantum cryptography in Convolution neural network approach in Smart cities." *Journal of Survey in Fisheries Sciences* 10, no. 2S (2023): 2043-2056.