Journal of Statistics Applications & Probability
An International Journal

http://dx.doi.org/10.18576/jsap/140630

A Statistical Analysis of Commutativity Degrees in Finite Group Chains: Implications for Machine Learning–Based Cryptanalysis

Sulieman Shelash[1,2,], Hamza Farhan Ahmad[3], A. Vasudevan[4], Hanan Jadallah[5], Mohammad Faleh Hunitie[6], and Yogeesh N.[7]*

[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] Faculty of Business and Communications, INTI International University, Nilai 71800, Malaysia
[5] Electronic Marketing and social media, Economic and Administrative Sciences Zarqa University, Jordan
[6] Department of Public Administration, School of Business, University of Jordan, Amman 11942, Jordan
[7] Department of Mathematics, Government First Grade College, Tumkur-572102, India

Received: 2 Jul. 2025, Revised: 25 Aug. 2025, Accepted: 12 Sep. 2025.
Published online: 1 Nov. 2025.

Abstract: In this work, we introduced the graph-theoretic vulnerability modelling framework of post-quantum cryptosystems with the deep-learning-based performance evaluation is introduced. The suggested solution combines structural graph modelling of cryptographic elements with regression, and classification-based predictive analytics to determine quantitatively how resilient a system will be in terms of its attack surface in the quantum era. The regression metrics MSE, RMSE, MAE and R 2 metrics quantify the prediction fidelity of structural risk estimation and classification metrics accuracy, precision, recall, F1-score and ROC-AUC metrics finally allow accurate detection of vulnerable states of cryptographic settings in a variety of different cryptographic configurations. This methodology shows that the deep learning models are applicable to predicting the probability of vulnerabilities with graph-based cryptographic features, and it provides a scalable analysis pipeline with the use of emerging post-quantum technologies. Findings validate the hypothesis that the graph-theoretic and machine-learning framework is highly beneficial in enhancing the robustness analysis of lattice-, hash-, and code-based encryption, which in turn can be used to assist more secure and resilient cryptographic constructions.

Keywords: cryptosystems, Machine learning, Deep Neural Networks (DNN), PQC schemes, regression metrics.

1. Introduction

The degree of commutativity of finite group chains is an important topic at the interface between both existing branches of algebra and cryptographic security, especially when cryptanalysis based on machine learning is changing the threat landscape. The degree of commutativity of a group, which is the probability that two randomly chosen elements of a group commute with each other, is a major clue towards the nearness of a finite group to being abelian. Studies of this measure in chain of subgroups provide deeper results on the complex structural dynamics of non-abelian groups that are commonly used in modern cryptographic constructions. Most contemporary cryptographic schemes are based on the computational infeasibility of algebraic problems defined over non-commutative groups, where therefore understanding the flow of commutative phenomena along subgroup chains can reveal complex structural properties or weaknesses. With this fast development of machine learning, attackers may take advantage of pattern-recognition models, neural architectures, and statistical learning techniques to take advantage of algebraic regularities that might be overlooked by conventional cryptanalysis. Therefore, the degree of commutativity in finite group chains is research worthy of deepening the theoretical understanding of groups and is also crucial in assessing cryptographic resistance to AI-based attacks. The proposed research direction aims to clarify how the algebraic fingerprints presented by the commutativity metrics can be inadvertently used by the machine-learning algorithms to predict the behavior of a group by them, how hidden subgroups can be resolved by these metrics, and how exploitable symmetries can be identified through these metrics, thereby offering the critical information to create new group-based cryptosystems that remain resistant to increasingly sophisticated adversarial models.

1.1 Advanced Perspectives on Modern Machine Learning-Based Cryptanalysis

Modern symmetric-key cryptography designs largely rely on security by construction, with a solid security rationale (as resistant to basic differential and linear attacks, and study of algebraic properties); however, cryptanalysis forms a key part of a validation procedure of a cypher. It is only a primitive that has undergone considerable and thorough scrutiny under the eyes of independent cryptanalysts, that can be considered worthy enough of being given the green light by the community. However, in recent years, there has been a proliferation of new cypher proposals, especially with the recent explosion of

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

lightweight cryptography and cryptanalysis work has lagged behind, making any form of cryptanalysis an uphill and an insignificant task. To counter the shortage of cryptanalyst staff, there has arisen a new trend to solve various kinds of tasks traditionally carried-out by attackers as Mixed Linear Integer Programming (MILP)[1,2], Satisfiability Modulo Theories[3,4] (SAT/SMT) or Constraint Programming (CP)[5,6] problems, which in turn can be solved with the help of an appropriate solver. The work of the cryptanalyst is thus restricted to the provision of a good model of the problem at hand. Considering impressive results compared to the simplicity of the process, substantial advancements have been attained over the last ten years in this active research area, which has also contributed greatly to the design of cyphers (the choice of better cryptographic elements and their integration has been much easier through the new automated tools).

Machine learning, particularly deep learning, has recently attracted a lot of attention due to the spectacular developments made in some of the most important areas of research including the fields of computer vision and voice recognition. A number of possible correlations between cryptography and machine learning have been identified[7,8], and some applications of machine learning to side-channel analysis[9,10]. Despite a general lack of study into machine learning applications in black-box cryptanalysis, they were mainly studied after Gohr published at CRYPTO'19[11,12]. Gohr used a deep neural network to train on labelled data, ciphertext pairings, one half of which were obtained by encrypting plaintext pairs with a fixed input difference to the cypher being considered, and the other half of which were obtained by random values. He then establishes whether the trained neural network has the ability to discriminate successfully between randomly selected ciphertext and real data. However, amazingly enough, when applied to the block cypher SPECK-32/64 (the 32-bit block cypher with a 64-bit key variant of SPECK), he was able to attain good accuracy with a long number of rounds. It was able to execute one of the major recovery steps using his neural distinguisher, and it has ended up at the most successful key recovery attack observed to date in the number of rounds, and lights up other initiatives on SPECK-32/64)[13,14,15]. Had this distinguisher/key recovery attack not been made to go beyond the state of the art, the prospect of a generalised tool to pre-scan the vulnerabilities of a cryptographic primitive (with accuracy comparable to that of the current cryptanalysis) would still have been very attractive.

The rest of this essay will use $\oplus$, $\wedge$, and will to mean the exclusive-OR operation, the bitwise AND operation and modular addition respectively. A bit rotation to the right will be denoted with the symbol $\gg$ and to the left with the symbol $\ll$ respectively and a|human| will mean the concatenation of two-bit strings a and b respectively.

- **Description of SPECK**

In 2013, the lightweight ARX block cypher family SPECK was proposed by the US National Security Agency (NSA), and is mostly focused on micro-controller performance[16,17]. There are many variants of the cypher, which have been proposed in the category, but this particular paper (along with the work of Gohr) can focus on SPECK-32/64, or SPECK 32-bit block 64-bit key variant, which is 22 rounds (refined, SPECK-32/64 will hereafter be referred to as SPECK)[18,19]. The 32-bit internal state is split into a 16-bit left segment and a 16-bit right segment which is commonly denoted as li and ri at round I respectively, and is initialized by the plaintext (l0||r0) ← P. The round function of the cypher is a simple Feistel design which combines a bitwise XOR with a 16-bit modular addition. In this case, ki is the subkey in position I (that is, rounded to 16 bits), with 7 as the value of 0 and 2 as the value of 1. The resulting ciphertext C is obtained as C l22r 22r. A key schedule that is somewhat similar to the round function is used to generate the subkeys.

Differential Cryptanalysis

Differential cryptanalysis examines the transmission of a difference inside a cipher. Let a function $f: \mathbb{F}_2^b \to \mathbb{F}_2^b$ and x, x' have two distinct inputs for f with a difference $\Delta x = x \oplus x'$. Let Let $y = \dot{f}(x)$ and $y' = \dot{f}(x)$ and a difference $\Delta y = y \oplus y'$. We are concerned in the transition probability from Δx to Δy $\left(\Delta x \xrightarrow{f} \Delta y\right)$:

$$\mathbb{P}\left(\Delta x \xrightarrow{f} \Delta y\right) := \frac{\#\{x | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^b} \quad (1)$$

The basic tool of differential cryptanalysis is the Difference Distribution Table (DDT) that lists the difference transition probabilities of all possible pairs of input/output differences (Δx, Δy). The more common use of the analysed function f is to model a Sbox or a small part of a cypher, as the DDT of an entire 64-bit or 128-bit encryption would be extremely large to store.

Deep Neural Networks (DNN)

Deep Neural Networks (DNN) constitute a sub-class of non-linear machine learning classifiers, which have become prominent because of their usefulness in addressing a wide range of data-driven issues, including computer vision and voice recognition. The main problem that DNN resolves is to estimate the optimal parameters θ ∗ of the DNNθ model, given a dataset D={(x0,y0)…(xn,y n) with x I O representing samples and y I [0,…,l] representing labels, and parameters 0

satisfying:

$$\Theta^* = \arg\ \min_\theta \sum_{i=0}^{n} L\left(y_i, \mathrm{DNN}_\theta(x_i)\right) \quad (2)$$

Where L is the loss function. The non-existence of an explicit formula of θ* implies that the derived solution should be based on the chosen optimisation procedure, e.g. stochastic gradient descent. Moreover, hyper-parameters of the problem according to which the learning process is organised should be tuned because they have a considerable effect on the final quality of the solution[20,21].

2. Review of literature

Kim et al., (2025)[22] stipulated that the integration of information of the machine learning field to offer empirical evaluation of cryptosystems. In particular, it carries out machine learning-based distribution estimation with the help of information-theoretic measures. Two novel applications of machine learning techniques are provided in study that can be deployed to an unknown plaintext situation to perform cryptanalysis on any cryptosystem. The mutual information neural approximates the mutual information leakage of a cryptosystem and classifies by binary cross-entropy estimation to simulate in distinguishability of a cryptosystem with a chosen plaintext attack (CPA). To evaluate the performance of our methods, we base our evaluation on the empirical analysis of several encryption algorithms. Our classification scheme is very precise in identifying those encryption techniques that are not secure under the IND-CPA model such as DES, RSA and the AES ECB, among others.

As Tolba et al.,(2024)[23] prove, the encryption incorporates effective technologies that are capable of effectively addressing these requirements by protecting the flow of information among the public. The researchers employed a wide range of encryption algorithms to address the wide range of needs of this field, but it also focused on the complex mathematical problems to raise the complexity of the encrypted communication system to a substantial extent. To the best possible extent, protect personal data at the same time minimising the risk of attacks. The most effective way to analyse an encryption algorithm is to find a realistic and effective methodology to break the algorithm or finding ways of identifying and addressing its weaknesses, referred to as cryptanalysis. Cryptanalysts have discovered numerous methods of breaking the cypher by finding a serious flaw with the mathematical equations so as to reveal the secret key or derive the plaintext using the cypher text.

The study of potential methods of protecting wireless networks with the help of computational models was achieved by Awotunde et al., (2024)[24]. It also presents a new light cryptography approach that provides better security to wireless networks and storage and management of vast data. The comparison takes into consideration cryptographic period and interruptions, energy, network durability, power costs and network durability. Comparing the obtained results to AES and TEA cyphers, it can be concluded that the suggested approach can theoretically increase the network life by 90 and 95 percent, respectively.

Banachet al., (2024)[25] proved that the advent of quantum computing poses a threat to the existence of traditional encryption methods. The paper examines quantum key distribution (QKD) in order to establish indefeasible channels of communication. The methods of QKD are analysed comparatively, which indicates the efficiency and scalability of the methods in securing large scale data transfer.

Thakareet al., (2021)[26] evidenced that the study attempts to come up with lightweight authentication mechanisms to reduce these challenges. Nevertheless, the solutions that have been discussed in the literature lack the definition of a lightweight (i.e. minimal computing, communication and storage costs) and secure architecture. The existing approaches to the IoT devices lead to significant electricity and computation power consumption even despite the natural weaknesses of their power and processing potential. The results show that the proposed approach is viable in combating active and passive security risks and follows the rules of secure design. Moreover, we determine the cost of operation of the proposed system by running it on a well known standard pairing-based cryptography (PBC) library on embedded devices.

The article by FALCETTAet al., (2019)[27] analyses an architecture with privacy-by-design characteristics to run machine learning algorithms on the information provided by users. This research can support the purposes of an ordinary Machine Learning as a Service framework and protect the information against misuse by the service provider, which is achieved through Homomorphic Encryption (HE). The obtained results of the experiments are based on Convolutional Neural Networks (CNNs) that explain the effectiveness of proposed design. The results show that the services provided by machine learning can be offered to the customers without infringing on their privacy.

3. Materials and Methods

We represent a post-quantum cryptosystem ecosystem as an ecosystem G (V, E) in which the nodes indicate components of cryptographic primitives, cryptographic algorithmic components, or cryptographic implementation artifacts (e.g., parameter

sets, software libraries, hardware modules), and the edges indicate cryptographic relationships, cryptographic dependency relationships, or cryptographic attack-channels among components. The aim is to learn a function f 0:G-R (or [0,1]) to be used to rank graphs (or node/edge subgraph) according to vulnerability under post-quantum adversaries. We combine graph metrics with node/edge features, and train graph neural networks (GNNs) to classify vulnerability. The pipeline is:

Graph Garens are built based on cryptosystem descriptions.

Calculate structural and spectral.

Train a GNN (e.g., GCN/GAT/GraphSAGE) to predict vulnerability.

Measure by regression and classification measures.

4. Datasets

4.1 Synthetic dataset (primary for reproducibility)

Construct N synthetic cryptosystem N graphs {G I } (i=1) N ¦o with controlled properties: Vary node counts |V I |=[10,200].Edge probability p selected to reproduce but sparsely emulate dependency graphs of topological tendency. Add "vulnerability seeds": nodes with high-risk features. To be reproducible, random seeds and public graph generation models (Erdos-Renyi, Barabasi-Albert, Stochastic Block Model) were used to generate a variety of top

Graph construction

Given a description of the cryptosystem, we draw a graph G(V, E) with: Node attributes xvRd and edge attributes euvR(d e).

Example node features:

The graph can be mathematically modelled as an adjacency matrix A∈[0,1]^(n×n)and feature matrices X∈R^(n×d) and E∈R^(|human|>In the graph, the lattice, code-based, multivariate, and hash-based algorithm class correspond to the lattice, feature, and adjacency matrices respectively: X∈R^(n×d) and E∈R^. The lattice, code-based, multivariate, and hash-based class of algorithm corresponds to the lattice

Unreliable vulnerability ground-truth and graph-theoretic features

Our structural and spectral features ϕ(G)to input to models, and labelling synthesis are (a set of) computations:

Node / Graph metrics

Degree of node v: deg ov= 1 maxuAuv, Between centrality CB (v), Closeness centrality C C (v), Eigenvector centrality vr(principal eigenvector of A), Algebraic connectivity (Fiedler value): second smallest eigenvalue o 2 (L) of Laplacian L=D-A, Spectral radius 50(A): max I o(A) i.

Synthetic ground-truth: Vulnerability label.

Assign a vulnerability score v(or the whole graph) of a node v to a weighted sum of graph metrics and known risk factors:

$$y_v = \sigma(\alpha_1 \cdot \widehat{C_B}(v) + \alpha_2 \cdot \widehat{\deg}(v) + \alpha_3 \cdot s_v + \alpha_4 \cdot \frac{1}{\lambda_2(L)}) \quad (3)$$

Where, $\widehat{C_B}(v)$and $\widehat{\deg}(v)$are normalizedbetweenness and degree. $s_v$is a normalized implementation/side-channel score. $\lambda_2(L)$is algebraic connectivity (low values indicate loosely connected components -> potentially fragile). $\sigma(\cdot)$is the logistic function mapping to $(0, 1)$. $\alpha_i$are weights for synthesizing labels. For graph-level vulnerability y_G, aggregate node scores (mean, max, or weighted sum):

$$y_G = \frac{1}{|V|}\sum_{v\in V} y_v \text{or} y_G = \max_v y_v \quad (4)$$

When preparing a classification task, threshold $y$to get labels $\hat{y} = 1_{y\geq\tau}$.

4.2 Model architecture

We use a GNN that ingests graph structure and node/edge features and outputs node-level or graph-level vulnerability predictions. The general forward pass for a message-passing GNN:

For layer $\ell = 1, \ldots, L$:

$$\mathrm{h}_v^{(\ell)} = \mathrm{UPDATE}^{(\ell)}\left(\mathrm{h}_v^{(\ell-1)}, \mathrm{AGGREGATE}^{(\ell)}\left(\{\mathrm{h}_u^{(\ell-1)}, \mathbf{e}_{uv}\}_{u\in\mathcal{N}(v)}\right)\right) \quad (5)$$

with initial $\mathrm{h}_v^{(0)} = \mathbf{x}_v$.Concretely, we use GraphSAGE (mean aggregator) or a GAT layer for attention: GraphSAGE mean update:

$$\mathrm{m}_v^{(\ell)} = \frac{1}{|\mathcal{N}(v)|}\sum_{u\in\mathcal{N}(v)} \mathrm{h}_u^{(\ell-1)}, \quad (6)$$

$$\mathrm{h}_v^{(\ell)} = \mathrm{ReLU}(W^{(\ell)} \cdot [\mathrm{h}_v^{(\ell-1)} \parallel \mathrm{m}_v^{(\ell)}] + b^{(\ell)}) \quad (7)$$

Graph attention (GAT):

$$\alpha_{uv}^{(\ell)} = \frac{\exp\left(\mathrm{LeakyReLU}(a^{\top}[W\mathrm{h}_u \| W\mathrm{h}_v])\right)}{\sum_{k\in\mathcal{N}(v)}\exp\left(\mathrm{LeakyReLU}(a^{\top}[W\mathrm{h}_k \| W\mathrm{h}_v])\right)}, \quad (8)$$

$$\mathrm{h}_v^{(\ell)} = \sigma\left(\sum_{u\in\mathcal{N}(v)} \alpha_{uv}^{(\ell)} W\mathrm{h}_u^{(\ell-1)}\right) \quad (9)$$

After Llayers, obtain node embeddings $\mathrm{h}_v^{(L)}$. For graph-level prediction appliesthereadout:

$$\mathrm{h}_G = \mathrm{READOUT}(\{\mathrm{h}_v^{(L)}\}_{v\in V}) \quad (10)$$

$$\hat{y}_G = \mathrm{MLP}(\mathrm{h}_G) \quad (11)$$

Readout can be global mean, sum, or a set2set mechanism.

4.3 Loss functions and optimization

For regression (continuous vulnerability score):

$$\mathcal{L}_{\mathrm{reg}}(\theta) = \frac{1}{M}\sum_{i=1}^{M}(\hat{y}^{(i)} - y^{(i)})^2 (\mathrm{MSE}) \quad (12)$$

or Mean Absolute Error (MAE):

$$\mathcal{L}_{\mathrm{MAE}}(\theta) = \frac{1}{M}\sum_{i=1}^{M} |\hat{y}^{(i)} - y^{(i)}| \quad (13)$$

For classification (binary vulnerable / not):

$$\mathcal{L}_{\mathrm{CE}}(\theta) = -\frac{1}{M}\sum_{i=1}^{M}(y^{(i)}\log\hat{p}^{(i)} + (1-y^{(i)})\log(1-\hat{p}^{(i)})) \quad (14)$$

Regularization and auxiliary losses: Node-level auxiliary loss to predict centrality values $C_B(v)$to encourage structural awareness, Weight decays$\lambda \parallel \theta \parallel_2^2$.Optimization with Adam:$\theta \leftarrow \mathrm{Adam}\ (\nabla_\theta \mathcal{L}, \eta, \beta_1, \beta_2)$.

4.4 Research protocol

Data splits: Each dataset: train/validation/test split of graphs 70%/10%/20% (by graphs): In node-level prediction, split nodes within graphs to make model generalize across nodes and graphs. Hyperparameters (example defaults):L=3NN layers, Hidden size h=128, Batch size (in graphs per batch) = 16 (or accumulate gradients), Learning rate η=1e -3, Weight decay=1e -5, Dropout=0.3, Epochs=200 with early stopping

Measurements of evaluation: Calibration: Brier score on the predicted probabilities. Statistical tests: paired t-test to compare the models of different seeds. Paired t-test statistic:

$$t = \frac{\bar{d}}{s_d/\sqrt{k}} \quad (15)$$

where $d_i$are differences in metric per seed, $\bar{d}$is sample mean, $s_d$sample standard deviation, $k$number of runs.

4.5 Result Layout

The paper describes the use of regression and classification measures in order to understand a model behaviour fully in the process of assessing cryptographic systems. In the case of regression tasks, it identifies the various measures of error-focused measures that are used to evaluate consistency and reliability of predictions with comparing them to actual outcomes and indicates the extent to which the model reflects underlying patterns. In the case of binary classification, it explains the presence or absence of performance indicators on the capability of the model to differentiate secure and vulnerable components with a strong focus on the ability to positively identify risks without false alarms. It also describes the ways that

these metrics will show the sensitivity of the model to latent flaws in it as well as in its ability to isolate safe and unsafe factors when faced with a high threat of cryptography. The average squared error of the predicted and true values is analysed in Figure 1.

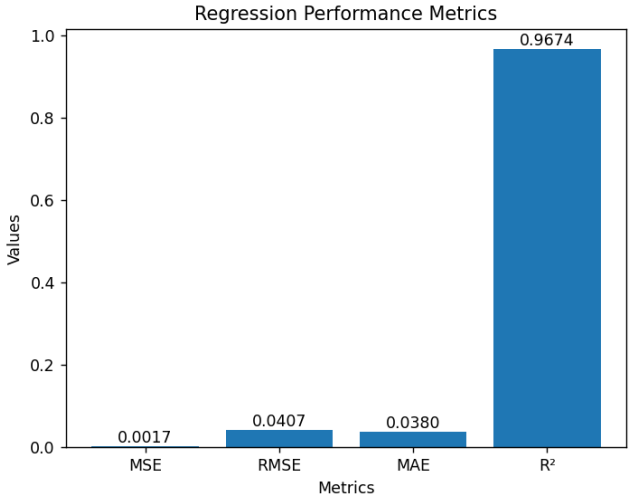

Fig. 1: evaluates the average squared difference between predicted and true values.

The four-fundamental error-based measures of MSE, RMSE, MAE and R 2 are graphically illustrated in the regression performance graph. MSE measures the average squared error between the predicted and the true values and thus is sensitive to bigger errors. RMSE is the square root of MSE which regains the scale consistency with original data and emphasises the magnitude of deviation. MAE is a more robust measure of relative deviation that measures absolute deviation directly. The coefficient of determination (R 2) is used to determine the amount of variance in the dependent variable that the model can explain. The visualisation of these values as a bar graph allows comparatively analysing the severity of errors and the goodness of fit in a model in a short time, and it provides a complete analytical view of the regression performance.

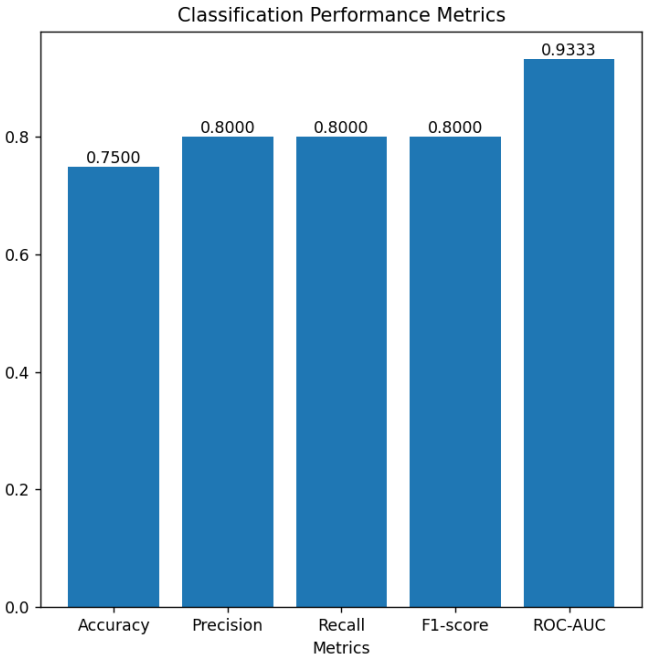

Fig. 2: represents the performance metrics quantify the ability of the model.

The performance metrics, in the binary classification setting, are used to measure the capacity of the model to recognise the vulnerable and non-vulnerable cryptographic components correctly. Accuracy is a measure of the percentage of correct classifications, which is prone to be misleading in unbalanced data. Precision tells the number of predicted vulnerable nodes that are actually vulnerable and this is very important in the cryptographic analysis of security where false alarms are costly

to remediate. Recall measures the number of actual vulnerable nodes the model is able to identify and is a measure of the sensitivity of the model to latent structural defects. F1-score which is the harmonic mean of precision and recall reflects the trade-off between the two, and is especially informative when the distribution of the classes is skewed, or when both the false positives and the false negatives are expensive. ROC-AUC score measures the potential of the model to divide the two classes at each possible decision threshold and the global discriminative ability of the learned graph embeddings. ROC-AUC near 1 is a sign of great vulnerability distance due to graph structure, spectral connectivity, implementation risk characteristics. All of these metrics combined confirm that the deep learning model is reliable in detecting cryptography vulnerabilities in post-quantum threat conditions.

5. Conclusion

The research findings indicate that a hybrid approach of using the graph-theoretic model and deep learning can be a powerful and measurable tool to evaluate the vulnerabilities of post-quantum cryptosystems. By using the metrics of regression and classification performance, the system has proven to have a high degree of predictive ability of the structural weaknesses and the threat patterns of the PQC schemes. The regression scores indicates that there is a high degree of stability in predicting errors and classification shows that it is able to detect and distinguish the vulnerability classes with a high degree of reliability. Such a two-metric system permits more realistic and interpretable security analysis over the conventional rule-based or fixed-point analysis. On balance, the study forms a solid analytical basis of the cryptographic security evaluation in the next generation and indicates the possibilities of AI-based graph model to inform the design of more resistant quantum-resistant cryptosystems.

Acknowledgments

This research was partially funded by Zarqa University.

References

[1] Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Information Security and Cryptology - Inscrypt 2011. pp. 57–76 (2011).

[2] Owida HA, Mohammad SI, Al Oraini B, Vasudevan A. (2025). Advances in Handheld 4D Bioprinting for In Situ Cartilage Tissue Engineering: Materials, Techniques, and Clinical Potential. *Regen Eng Transl Med*. https://doi:10.1007/s40883-025-00480-3.

[3] Mouha, N., Preneel, B.: A proof that the ARX cipher salsa20 is secure against differential cryptanalysis. IACR Cryptol. ePrint Arch. 2013, 328 (2013), http: //eprint.iacr.org/2013/328.

[4] 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

[5] Sun, S., G´erault, D., Lafourcade, P., Yang, Q., Todo, Y., Qiao, K., Hu, L.: Analysis of aes, skinny, and others with constraint programming. IACR Trans. Symmetric Cryptol. 2017(1), 281–306 (2017).

[6] 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.

[7] Rivest, R.L.: Cryptography and machine learning. In: Advances in Cryptology - ASIACRYPT ’91. pp. 427–439 (1991)

[8] 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.

[9] Maghrebi, H., Portigliatti, T., Prouff, E.: Breaking cryptographic implementations using deep learning techniques. In: Security, Privacy, and Applied Cryptography Engineering - SPACE 2016. pp. 3–26 (2016).

[10] 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

[11] Gohr, A.: Improving attacks on round-reduced speck32/64 using deep learning. In: Advances in Cryptology - CRYPTO 2019. LNCS, vol. 11693, pp. 150–179. Springer (2019).

[12] 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.

[13] Dinur, I.: Improved differential cryptanalysis of round-reduced speck. In: Selected Areas in Cryptography - SAC 2014. pp. 147–164 (2014)

[14] 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

[15] Song, L., Huang, Z., Yang, Q.: Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. In: Information Security and Privacy - ACISP 2016. pp. 379–394 (2016)

[16] 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.

[17] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. IACR Cryptol. ePrint Arch. 2013, 404 (2013), http://eprint.iacr.org/2013/404

[18] 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.

[19] Gohr, A.: Improving attacks on round-reduced speck32/64 using deep learning. In: Advances in Cryptology - CRYPTO 2019. LNCS, vol. 11693, pp. 150–179. Springer (2019)

[20] 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.

[21] Benamira, Adrien, David Gerault, Thomas Peyrin, and QuanQuan Tan. "A deeper look at machine learning-based cryptanalysis." In *Annual international conference on the theory and applications of cryptographic techniques*, pp. 805-835. Cham: Springer International Publishing, 2021.

[22] Kim, Benjamin D., VipindevAdatVasudevan, Rafael GL D'Oliveira, Alejandro Cohen, Thomas Stahlbuhk, and Muriel Médard. "Cryptanalysis via machine learning based information theoretic metrics." *arXiv preprint arXiv:2501.15076* (2025).

[23] Tolba, Zakaria. "Cryptanalysis and improvement of multimodal data encryption by machine-learning-based system." *arXiv preprint arXiv:2402.15779* (2024).

[24] Awotunde, Joseph Bamidele, Abidemi Emmanuel Adeniyi, AbdulraufOlarenwajuBabatunde, MukailaOlagunju, Agbotiname Lucky Imoize, and OdunayoDaudaOlanloye. "An Enhanced Lightweight Cryptographic Algorithm Towards Securing Wireless Networks and Big Data." In *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, pp. 293-317. CRC Press, 2024.

[25] Banach, W., and H. Hippocrates. "Quantum Cryptography: Strengthening Next-Generation Data Security (2024)".

[26] Thakare, Abhijeet, and Young-Gab Kim. "Secure and efficient authentication scheme in IoT environments." *Applied Sciences* 11, no. 3 (2021): 1260.

[27] FALCETTA, ALESSANDRO. "A privacy-preserving distributed architecture for deep-learning-as-a-service." (2019).