# Machine Learning-based Exploratory Performance Analysis of CRYSTALS-Kyber–AES Hybrid Post-Quantum Cryptographic Systems

Muhammed Shehu
Computer Science Department,
Federal University Lokoja

Taiwo Kolajo
Computer Science Department,
Federal University Lokoja

Emeka Ogbuju
Computer Science Department,
Miva Open University, Abuja

## ABSTRACT
Selecting suitable parameter configurations in hybrid post-quantum cryptographic systems is not only a matter of security strength but also of performance efficiency under varying system and network conditions. Many existing studies focus mainly on security guarantees, with limited attention to how different configurations behave in real deployment environments. This creates a gap in understanding how to balance security requirements with practical performance. This study explores the use of machine learning as a data-driven approach to analyze and predict performance trends in a hybrid cryptographic system that combines **CRYSTALS-Kyber** (a lattice-based post-quantum key encapsulation mechanism) with the **Advanced Encryption Standard (AES)**. A controlled environment for the experimental was developed using Python-based tools. Multiple configurations of AES key sizes (128, 192, 256 bits) and Kyber variants (Kyber512, Kyber768, Kyber1024) were evaluated under different network and computational conditions. The dataset result captured key performance metrics such as network latency, encryption latency, decryption latency, throughput, and CPU utilisation. Different machine learning models, including Random Forest, XGBoost, Linear Regression, Decision Tree, LightGBM, and Multilayer Perceptron (MLP), were trained and evaluated using MAE, RMSE, and $R^2$ metrics. The results show that while some models, particularly Random Forest and LightGBM, achieved relatively lower prediction errors for certain metrics, the overall predictive strength across tasks remained weak, with most $R^2$ values close to zero or negative. This indicates that the performance behaviour of the hybrid cryptographic system is influenced by complex and highly variable interactions that are not easily captured using standard supervised learning models and the current feature set.

## Keywords
Post-Quantum Cryptography, CRYSTALS-Kyber, Advanced Encryption Standard, Performance Analysis, Machine Learning, Hybrid Cryptographic Systems, System Optimization.

## 1. INTRODUCTION
Recent digital systems rely deeply on cryptography to secure communication channels, protect sensitive data, and support trust in online transactions. Technologies such as secure web communication, electronic banking, cloud services, and digital identity systems all rely on a well-established cryptographic scheme like the Advanced Encryption Standard (AES) for data encryption and RSA or Elliptic Curve Cryptography (ECC) for key exchange and digital signatures [12], [4]. These cryptosystems systems have served reliably for a long term and form the backbone of today's information security infrastructure.

However, the consistent progress in quantum computing has presents a serious challenge to many of these classical cryptographic schemes. The theoretical capability of quantum algorithms, especially Shor's algorithm, shows that widely used public-key cryptosystems such as RSA and ECC could be broken efficiently once large-scale quantum computers become practi**cal** [14]. While symmetric sachems like AES are more resilient, they are still affected by Grover's algorithm, which reduces their effective security strength and may require larger key sizes to remain secure [5]. This evolving threat led to the growing global efforts toward developing Post-Quantum Cryptography (PQC) Scheme, which works toward design cryptographic schemes and system that can withstand attacks from both classical and quantum computers [13].

Among the different PQC approaches, lattice-based cryptography scheme has received enormous attention due to its strong mathematical background and relatively efficient performance. One of the most prominent outcomes of the National Institute of Standards and Technology (NIST) PQC standardization process is **CRYSTALS-Kyber**, was selected as a standard for key encapsulation mechanisms (KEMs) **[**18**]**. Kyber was designed to provide quantum-resistant key exchange while maintaining practical performance for real-world deployment.

With these advancements, there hasn't been a full and immediate transition from classical cryptography to fully post-quantum systems in reality. Most real-world systems are expected to adopt **hybrid cryptographic architectures**, where classical algorithms (such as AES) are combined with PQC schemes like Kyber. In such systems, Kyber is use for secure key exchange, while AES handles enormous data encryption. This hybrid approach provides a safer migration path, allowing systems to remain secure against both classical and future quantum threats **[**13**]**

While hybrid cryptographic scheme improve security, they also introduce new challenges related to performance. Different configurations, such as the choice of Kyber variant (Kyber512, Kyber768, Kyber1024) and AES key size (128, 192, 256 bits), have different computational costs, memory requirements, and sensitivity to network conditions. Basically, these systems typically rely on predefined parameter settings based on preset security levels. The unique characteristics of real-world environments, where system resources, workload, and network conditions might change dramatically over time, are not taken into account by this static method. In some deployment settings, this could result in needless overhead, decreased efficiency, or subpar system performance **[**7**]**, **[**15**]**.

These limitation raises an essential question: **Can data-driven methods be used to better understand and possibly predict how different cryptographic configurations will perform under different system conditions?**

Machine learning provides a greater approach to address this challenge. It is best for modelling complex relationships between multiple interacting factors, such as algorithm parameters, system resource usage, and network characteristics. Instead of relying on fixed rules, machine learning models can learn patterns from observed data and provide little knowledge on how different configurations behave in practice.

This idea motivate, this study into investigating the use of machine learning to analyze and model the performance behaviour of a hybrid **CRYSTALS-Kyber–AES** cryptographic system. A controlled experimental environment was developed to simulate different parameter configurations and operating conditions. From this environment, a dataset was generated capturing key performance metrics, including encryption latency, decryption latency, network latency, throughput, and CPU utilisation. Multiple machine learning models were then trained and evaluated to assess their ability to predict these performance metrics.

The main contributions of this study are as follows. First, it provides a structured and reproducible experimental framework for generating performance data in hybrid post-quantum cryptographic systems under varying system and network conditions. Second, it offers a comparative evaluation of different machine learning models applied to cryptographic performance prediction tasks. Third, it highlights the limitations of current modelling approaches and shows that system-level and network-related factors often have a stronger influence on performance than cryptographic parameter choices alone.

The study also contributes to the ongoing discussion and research in making post-quantum cryptography not only secure but also practical and efficient in real-world deployments and lays the groundwork for further research on adaptive cryptographic scheme that can intelligently balance security and performance based on real-time conditions.

# 2. RELATED WORKS

The rapid advancement of quantum computing has triggered a major shift in cryptographic research, with increasing attention given to the development and evaluation of post-quantum cryptographic (PQC) schemes. A significant body of work has focused on analysing the security and performance of both classical and emerging quantum-resistant algorithms, as well as exploring practical pathways for their deployment in real-world systems.

A number of PQC methods have been put forth and assessed in response to this problem, with lattice-based cryptography emerging as one of the more promising approaches. **[**2**]** found that many PQC schemes can be implemented with reasonable computational cost after comparing the performance of PQC algorithms like SPHINCS+ and Dilithium against traditional methods. Likewise, **[**5**]** investigated the energy consumption of NIST PQC candidates and showed that schemes like Kyber and SABER demonstrate relatively efficient performance compared to alternatives such as Classic McEliece.

Beyond standalone PQC schemes, recent research has explored **hybrid cryptographic architectures** that combine classical and post-quantum techniques as a transitional solution. **[**10**]** proposed a hybrid framework integrating CRYSTALS-Kyber with AES and Quantum Random Number Generation (QRNG), demonstrating improved security properties and functional correctness of the combined system. While their work validated the feasibility of hybrid cryptographic designs, it relied on fixed parameter configurations and did not address how different configurations perform under varying operational conditions.

Other studies have focused on benchmarking and optimising the performance of cryptographic algorithms. **[**6**]** evaluated a multivariate polynomial-based signature scheme using the SUPERCOP benchmarking framework and reported improvements in key size and computational efficiency.

Despite these advances, most existing studies share a common limitation. They primarily focus on **benchmarking performance metrics under fixed configurations**, rather than developing mechanisms for **predicting or adapting performance dynamically**. In real-world environments, system conditions such as CPU load, memory availability, network latency, and data volume can vary significantly, affecting the efficiency of cryptographic operations. However, there is limited research on how these factors interact with cryptographic parameters to influence overall system performance.

A few emerging studies have begun to explore the use of machine learning in systems optimisation and performance modelling. Machine learning has been successfully applied in areas such as network performance prediction, resource allocation, and system tuning. Its ability to model complex and nonlinear relationships makes it a suitable candidate for analysing cryptographic performance behaviour. However, its application specifically to **hybrid post-quantum cryptographic systems** remains largely underexplored.

This gap forms the basis for the present study. Unlike prior work that focuses mainly on security evaluation or static benchmarking, this research investigates the use of machine learning as a tool for analysing and modelling performance behaviour in a hybrid **CRYSTALS-Kyber–AES** cryptographic system. The study does not assume that performance can be perfectly predicted; rather, it seeks to understand the extent to which performance trends can be learned from data, and to identify the key factors influencing these trends.

The study contributes to the emerging area of **data-driven cryptographic system analysis**, where performance is not treated as a fixed property of an algorithm, but as a dynamic outcome influenced by both cryptographic parameters and system-level conditions. This perspective is important for future work on adaptive cryptographic systems that aim to balance security and efficiency in real-world deployments.

# 3. MATERIALS AND METHODS

## 3.1 Methodology Overview

This study adopted an experimental, data-driven approach to investigate the performance behaviour of a hybrid **CRYSTALS-Kyber–AES** cryptographic system under controlled system and network conditions. The methodology was structured to ensure that data generation, modelling, and evaluation were carried out in a reproducible and systematic manner. The process began with the design of a controlled experimental environment in which different cryptographic parameter configurations were executed repeatedly under varying computational and network conditions. The data generated from these experiments were then processed into a structured dataset, which formed the basis for machine learning

modelling. Finally, a conceptual framework for adaptive parameter selection was proposed based on the insights obtained from the modelling results.

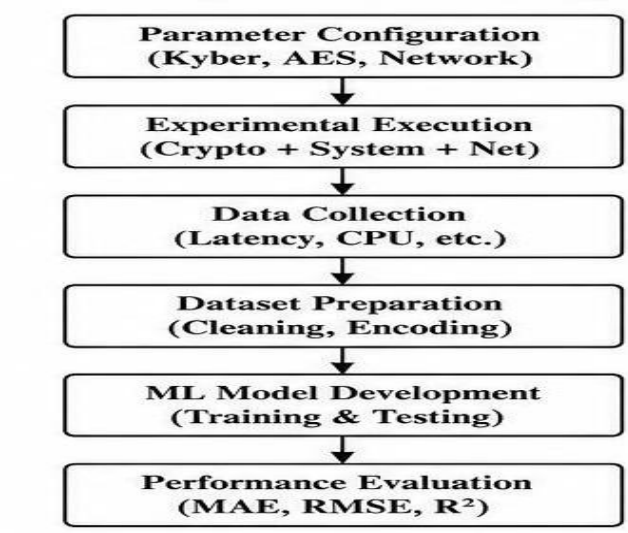


Fig 1 **High-Level Methodological Flow – Experimental Pipeline**

## 3.2 Experimental Design and Data Collection

A hybrid cryptographic framework combining CRYSTALS-Kyber for key encapsulation and AES for symmetric encryption was implemented within a controlled environment. The experimental design allowed systematic variation of cryptographic parameters alongside system and network conditions. The Kyber variants considered were Kyber512, Kyber768, and Kyber1024, while AES key sizes included 128-bit, 192-bit, and 256-bit configurations. These combinations were executed under different computational constraints and simulated network conditions to observe their performance behaviour.

The experimental environment was implemented using a containerised architecture to ensure consistency across runs. Each experiment involved the execution of key generation, encapsulation and decapsulation using Kyber, followed by encryption and decryption operations using AES. Performance metrics were collected at each stage, including encryption latency, decryption latency, CPU utilisation, throughput, and network latency. To improve reliability, each configuration was executed multiple times, and the results were averaged to reduce the effect of transient system noise.

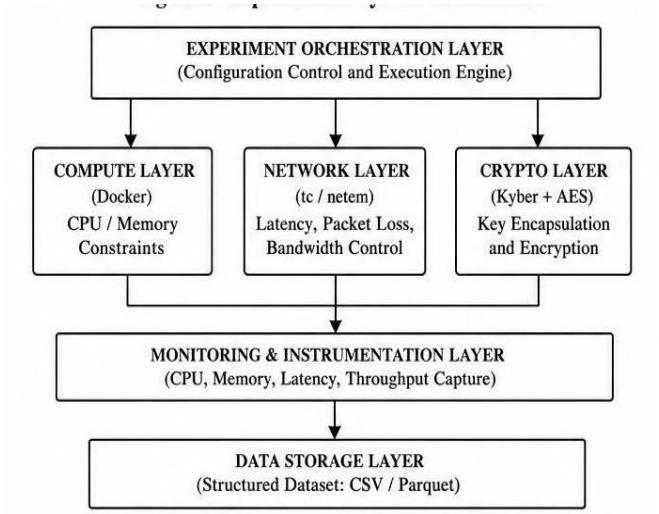


**Fig 2 Experimental System Architecture**

## 3.3 Experimental Workflow

The experimental workflow was designed to ensure repeatability and consistency across all runs. Each experiment began with the definition of a configuration file specifying the parameter combinations and system conditions to be tested. The orchestration layer then instantiated containerised environments and applied the required computational and network constraints. A brief warm-up phase was executed to stabilise system performance before measurements were taken. During each run, cryptographic operations were performed, and performance metrics were recorded continuously. After execution, the environment was reset to eliminate any carry-over effects before the next run commenced. This process ensured that each observation was independent and comparable across configurations.

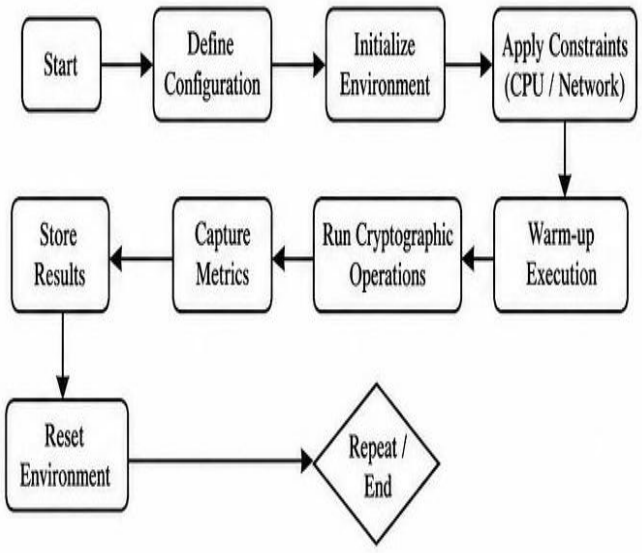


**Fig 3: Experimental Workflow Sequence**

## 3.4 Dataset Preparation and Feature Engineering

The data collected from the experimental runs were transformed into a structured dataset suitable for machine learning analysis. Each record in the dataset represented a complete execution cycle under a specific configuration. The

input features included cryptographic parameters such as Kyber variant and AES key size, as well as system-level conditions like network latency, packet loss, bandwidth, and CPU constraints. The output variables consisted of observed performance metrics including encryption latency, decryption latency, CPU usage, and throughput.

The data preprocessing involved cleaning to remove anomalies, normalization to ensure consistent scale across features, and encoding of categorical variables. To understand relationships between variables and to guide feature selection, correlation analysis was also performed. These steps ensured that the dataset was good for modelling and reduced the risk of bias or instability in the learning process.

## 3.5 Machine Learning Model Development

Series of machine learning models was used to capture different types of relationships within the dataset. Linear Regression was used as a baseline to model simple linear dependencies, while Decision Trees provided interpretable nonlinear modelling. Random Forest and gradient boosting models such as XGBoost and LightGBM were included to capture complex interactions and improve predictive stability. A Multilayer Perceptron was also implemented to explore the capability of neural networks in modelling nonlinear patterns.

The models were trained and evaluated using a standard train-test split combined with cross-validation to ensure generalisation. Model performance was assessed using Mean Absolute Error, Root Mean Square Error, and the coefficient of determination ($R^2$). Hyperparameters were tuned to optimise performance while avoiding overfitting.

**Table 1: Machine Learning Hyperparameters**

| Model | Parameter 1 | Parameter 2 | Parameter 3 | Parameter 4 |
|---|---|---|---|---|
| **Linear Regression** | fit_intercept | Positive | normalize | copy_X |
| **Decision Tree** | max_depth | min_samples_split | min_samples_leaf | criterion |
| **Random Forest** | n_estimators | max_depth | min_samples_split | max_features |
| **XGBoost** | n_estimators | learning_rate | max_depth | subsample |
| **Light GBM** | num_leaves | learning_rate | n_estimators | feature_fraction |
| **MLP** | hidden_layer_sizes | Activation | learning_rate_init | max_iter |

**Table 2: Optimised Hyperparameter Values**

| Model | Value 1 | Value 2 | Value 3 | Value 4 |
|---|---|---|---|---|
| **Linear Regression** | True | False | True | None |
| **Decision Tree** | 10 | 5 | 2 | squared_error |
| **Random Forest** | 200 | 15 | 4 | Sqrt |
| **XGBoost** | 300 | 0.05 | 6 | 0.8 |
| **LightGBM** | 31 | 0.05 | 300 | 0.8 |
| **MLP** | (128,64) | relu | 0.001 | 500 |

## 3.6 Conceptual Adaptive Framework

Although an adaptive system was not implemented in this study, a conceptual framework was developed to illustrate how machine learning could be integrated into a real-time cryptographic system. In this framework, system conditions are continuously monitored and passed into a trained model, which predicts expected performance outcomes. Based on these predictions and predefined security constraints, an appropriate parameter configuration is selected for execution. Feedback from the system is then used to update the model over time.

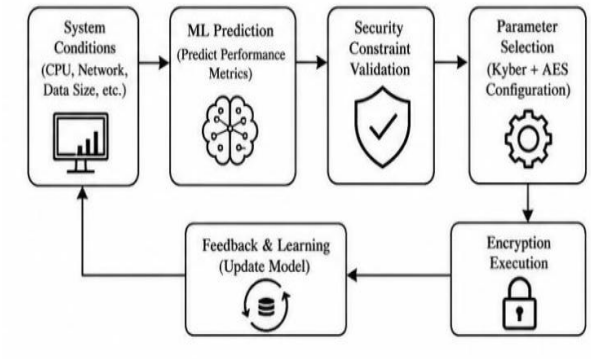


**Figure 4: Conceptual Adaptive Framework**

## 3.7 Tools and Technologies

Python was use as the primary development environment for implementation due to its strong support for both cryptography and machine learning. liboqs and PyCryptodome were used for implementation as the Cryptographic operations, while Pandas, NumPy, Scikit-learn, XGBoost, and LightGBM where use for data processing and modelling. Containerisation was achieved using Docker to ensure consistent experimental conditions, while network behaviour was simulated using traffic control tools. Monitoring tools were used to capture system-level metrics, ensuring correct and comprehensive data collection.

## 3.8 Implementation Challenges

Different difficulties were encountered during the implementation. Variability in execution timing due to system load was addressed through repeated experimentation and averaging. Ensuring consistency and accuracy across experimental runs required strict container isolation and environment control. Network simulation introduced additional complexity, as unrealistic conditions had to be avoided through careful tuning. Finally, maintaining dataset quality required attention to feature balance and reproducibility, which was acquired through structured configuration management and version control.

# 4. OVERVIEW OF EXPERIMENTAL RESULTS

The experimental implementation output a comprehensive dataset capturing the behaviour of the hybrid **CRYSTALS-Kyber–AES** cryptographic system under different parameter configurations and operating conditions. The dataset included variables such as encryption latency, network latency, decryption latency, throughput, CPU utilisation, AES key size, and Kyber variant.

While Initial analysis focused on understanding the relationships among these variables using visual and statistical techniques. These included comparative analysis across parameter configurations, trend plots, and correlation analysis. The aim at this stage was not prediction, but to establish observable patterns and dependencies within the system.

## 4.1 Behavior of Cryptographic Performance Metrics

The relationship between cryptographic processing time and network conditions revealed questionable variability across all configurations. Encryption latency generally increased with higher Kyber parameter sizes, reflecting the additional computational cost associated with stronger security levels.

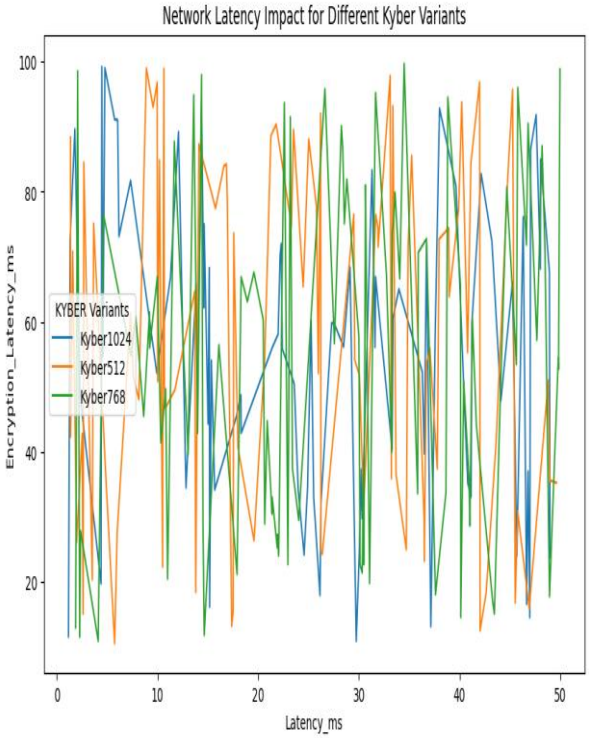


**Figure 6: Network Latency vs Encryption Latency Across Kyber Variants**

The view trend shows that the Kyber512 consistently produced lower latency values compared to Kyber768 and Kyber1024. Kyber1024 have the highest variability, particularly under unstable network conditions. With this, it indicates that higher-security configurations are more sensitive to environmental fluctuations, especially in network-dependent systems or distributed.

The same pattern was observed when comparing encryption latency across Kyber variants.

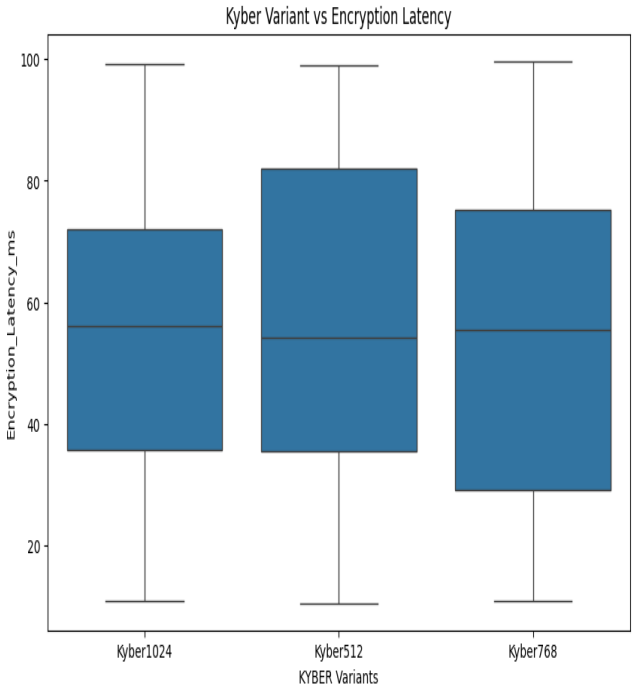


**Figure 7: Kyber Variants against Encryption Latency**

The figure confirms the expected trade-off between security strength and computational efficiency. When ever parameter size increases, encryption time also increases due to more complex polynomial operations and larger key sizes.

The decryption latency analysis also follows the same trend.

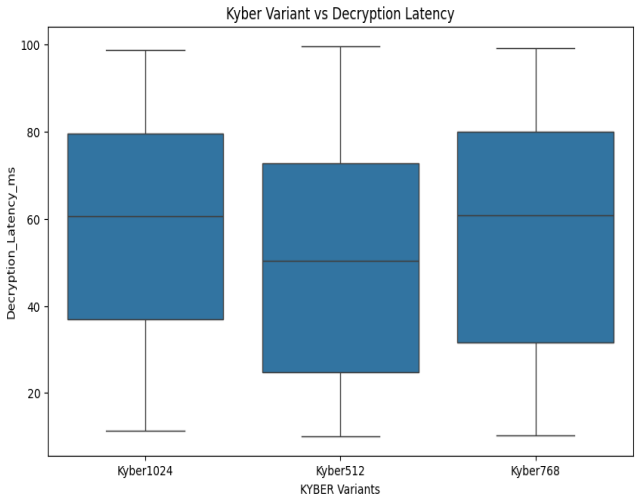


**Figure 8: Kyber Variants against Decryption Latency**

Kyber512 maintains the lowest decryption time, while Kyber1024 gain the highest computational overhead. These results reinforce the importance of balancing security requirements with acceptable system performance in real-world deployments.

## 4.2 Correlation Analysis of System Variables

For better Clarity the interaction between variables, a correlation heatmap was generated.

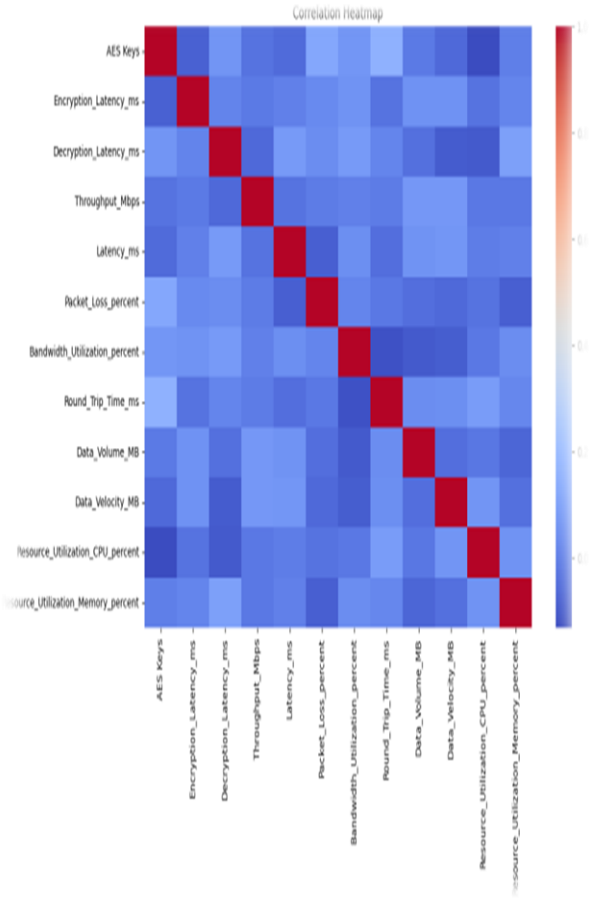


**Figure 9: Correlation Heatmap of System Features**

The correlation analysis has shows that most relationships between variables are weak to moderate. Encryption latency and decryption latency exhibit a gentle positive relationship, indicating that both are affected by similar computational factors. Network-related variables such as latency and packet loss show weak positive relationships with cryptographic delays, suggesting that poor network conditions trifle increase processing time.

Throughput shows weak negative correlations with latency and CPU utilisation, indicating that system performance reduce under higher load or poorer network conditions. Importantly, no single variable that significantly explains system performance, confirming that the behaviour of the cryptographic system is driven by multiple interacting factors.

## 4.3 Machine Learning Model Performance

The stage two of the analysis involved assessing the ability of machine learning models to forecast system performance metrics based on the available features. Multiple regression models were trained and evaluated using MAE, RMSE, and $R^2$ metrics.

### *4.3.1 Network Latency Prediction*

The Table 3 present the performance of models predicting network latency.

**Table 3: Model Performance for Network Latency Prediction**

| Model | MAE | RMSE | $R^2$ Score |
|---|---|---|---|
| **Linear Regression** | 12.16 | 14.36 | -0.063 |
| **Decision Tree** | 17.36 | 21.10 | -1.293 |
| **Random Forest** | 11.33 | 13.50 | 0.061 |
| **XGBoost** | 12.11 | 14.12 | -0.027 |
| **LightGBM** | 14.12 | 16.05 | -0.327 |
| **MLP** | 13.79 | 17.27 | -0.537 |
| **Ensemble** | 12.76 | 14.91 | -0.146 |

Random Forest achieved the best performance amidst the models, with the lowest RMSE and a slightly positive $R^2$ value. However, the $R^2$ score remains very low, showing that the model explains only a small portion of the variance in network latency. The negative $R^2$ scores observed in most models suggest that the predictive performance is weak and close to or worse than a simple baseline.

This shows that the network latency is influenced by complex and possibly random factors that are not fully captured in the dataset.

### *4.3.2 Encryption Latency Prediction*

Table 4 present the results for encryption latency prediction.

**Table 4: Model Performance for Encryption Latency Prediction**

| Model | MAE | RMSE | $R^2$ Score |
|---|---|---|---|
| **Linear Regression** | 30.35 | 33.82 | -0.303 |
| **Decision Tree** | 34.18 | 39.91 | -0.814 |
| **Random Forest** | 27.98 | 31.69 | -0.144 |
| **XGBoost** | 28.49 | 32.63 | -0.213 |
| **LightGBM** | 30.05 | 34.05 | -0.321 |
| **MLP** | 30.98 | 35.14 | -0.407 |
| **Ensemble** | 28.40 | 32.31 | -0.189 |

Random Forest again shows the lowest error values, but all the models recorded negative $R^2$ scores. This ascertain that encryption latency is difficult to model using the current feature set and modelling approach. The results imply that encryption latency is influenced by nonlinear interactions and environmental variability that are not easily captured by standard regression models.

### *4.3.3 Decryption Latency Prediction*

Table 5 present the results for decryption latency prediction.

**Table 5: Model Performance for Decryption Latency Prediction**

| Model | MAE | RMSE | $R^2$ Score |
|---|---|---|---|
| **Linear Regression** | 23.16 | 27.42 | 0.015 |
| **Decision Tree** | 33.78 | 41.40 | -1.247 |
| **Random Forest** | 24.17 | 27.70 | -0.006 |
| **XGBoost** | 23.61 | 27.84 | -0.016 |
| **LightGBM** | 25.41 | 29.96 | -0.176 |
| **MLP** | 22.43 | 27.47 | 0.011 |
| **Ensemble** | 24.05 | 28.05 | -0.036 |

Linear Regression and MLP recorded little positive $R^2$ values, which indicate weak but detectable patterns in the data as compared to encryption latency, decryption latency which appears to follow more stable trends, though the predictive strength remains limited.

### *4.3.4 CPU Utilisation Prediction*

Table 6 present the results for CPU usage prediction.

**Table 6: Model Performance for CPU Usage Prediction**

| Model | MAE | RMSE | $R^2$ Score |
|---|---|---|---|
| **Linear Regression** | 18.19 | 21.99 | -0.157 |
| **Decision Tree** | 22.05 | 27.28 | -0.782 |
| **Random Forest** | 17.81 | 20.85 | -0.041 |
| **XGBoost** | 17.69 | 21.71 | -0.128 |
| **LightGBM** | 16.47 | 20.67 | -0.022 |
| **MLP** | 18.64 | 23.35 | -0.305 |
| **Ensemble** | 17.96 | 21.22 | -0.078 |

LightGBM acquired the lowest error values, but the $R^2$ score remains negative. This suggests that CPU utilisation patterns are influenced by system-level noise and background processes, making them difficult to predict accurately.

### *4.3.5 Throughput Prediction*

Table 7 present the results for throughput prediction.

**Table 7: Model Performance for Throughput Prediction**

| Model | MAE | RMSE | $R^2$ Score |
|---|---|---|---|
| **Linear Regression** | 279.33 | 318.02 | -0.060 |
| **Decision Tree** | 343.12 | 412.61 | -0.785 |
| **Random Forest** | 272.57 | 308.74 | 0.001 |
| **XGBoost** | 277.27 | 317.97 | -0.060 |
| **LightGBM** | 290.73 | 348.77 | -0.275 |
| **MLP** | 296.29 | 335.49 | -0.180 |
| **Ensemble** | 276.51 | 313.78 | -0.032 |

Throughput prediction shows to be the most challenging task. Only Random Forest acquires a marginally positive $R^2$ value, which is effectively negligible. This implies that throughput is highly sensitive to dynamic factors such as data flow variability.

## 4.4 Discussion of Findings

The overall results reveal that while machine learning models may capture limited patterns in cryptographic system performance, their predictive ability remains modest across most workloads. The persistently low or negative R2 values show that performance results cannot be reliably predicted with the existing feature set and modeling approach.

A significant insight from the analysis is that **network-related factors and system-level have a stronger influence on performance than cryptographic parameters alone**. This further explains why models struggle to generalize, as these factors introduce variability that is difficult to model using static features.

Findings also suggest that performance behaviour in hybrid cryptographic systems is inherently complex and may require advanced approaches, such as temporal modelling, real-time monitoring data, or hybrid simulation-learning methods, to achieve meaningful predictive accuracy.

Instead of confirming strong predictive capability, this study highlights the **difficulties of applying machine learning to cryptographic performance modelling**, and underline the need for richer datasets and more sophisticated modelling techniques.

# 5. REFERENCES

[1] G. Aceto, V. Persico, and A. Pescapé, 'A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges,' *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3467-3501, 2019.

[2] D. Dziechciarz and M. Niemiec, 'Efficiency Analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments,' *Electronics*, vol. 14, no. 1, p. 70, 2024.

[3] E. Mumuni, A. Alhassan, and N. Sulemana, 'Success Factors of Electronic (E) Agriculture in Ghana: Lessons from MoFA and Cowtribe,' *Ghana Journal of Science, Technology and Development*, vol. 9, no. 1, pp. 1-17, 2023.

[4] V. K. Ralegankar *et al.*, 'Quantum cryptography-as-a-service for secure UAV communication: applications, challenges, and case study,' *IEEE Access*, vol. 10, pp. 1475-1492, 2021.

[5] P. Radanliev, 'Artificial Intelligence and Quantum Cryptography,' *Journal of Analytical Science and Technology*, vol. 15, no. 1, p. 4, 2024.

[6] C. A. Roma, C.-E. A. Tai, and M. A. Hasan, 'Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms,' *IEEE Access*, vol. 9, pp. 71295-71317, 2021.

[7] R. Kandakatla and K. Rajakumari, 'Hyperparameter-Tuned Machine Learning Model for the IDs Security in Cloud Environment,' in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, 2024, pp. 1-8.

[8] R. Kuang, M. Perepechaenko, R. Toth, and M. Barbeau, 'Benchmark Performance of a New Quantum-Safe Multivariate Polynomial Digital Signature Algorithm,' in *International Conference on Quantum Computing and Engineering*, 2022, pp. 454-464.

[9] A. Sahoo, I. A. Kumar, and S. M. Rajagopal, 'Comparative Study of Cryptographic Algorithms in Post Quantum Computing Landscape,' in *2024 International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, 2024, pp. 36-40.

[10] J. Sharma, S. Singh, M. Gayathri, R. Kumar, and A. Alkhayyat, 'Quantum-Enhanced Lattice Cryptography: AES Encryption with Crystal Kyber and QRNG IV,' in *Data Analytics for Smart Robotics and Its Applications*. Cham: Springer Nature Switzerland, 2025, pp. 257-273.

[11] R. A. Grimes, *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*. John Wiley & Sons, 2019.

[12] A. Mardon *et al.*, *Cryptography*. 2021.

[13] P. V. Ankunda, 'Future-Proofing Medical Devices: A Hybrid Approach To Security In The Post-Quantum Computing Era,' Doctoral dissertation, California State Polytechnic University, Pomona, 2023.

[14] S. Özeren, 'A Study On Crystals-Kyber And Its Masked Implementations,' Master's Thesis, Middle East Technical University, 2023.

[15] M. Al Khaldy, 'Survey on Hybrid Cybersecurity Approaches: Machine Learning, Fuzzy Systems, and Cryptographic Techniques,' 2024, doi: 10.20944/preprints202412.2524.v1.

[16] A. K. Bishwas and M. Sen, 'Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat,' arXiv preprint arXiv:2411.09995, 2024.