International Journal of Artificial Intelligence and Mathematical Sciences

January - June 2026 Vo5. Issue No. 01
ISSN Online: 2958-0153 and Print: 2958-5228
DOI: https://doi.org/10.58921/ijaims.v5i1.185

Lightweight Post Quantum Homomorphic Encryption for Secure Network Traffic Intrusion detection

[1*]Mariam Nayab, [1]Muhammad Sajid Qureshi, [1]Abdul Jabbar

khanmaryam85854@gmail.com, sajid.qureshi@riphah.edu.pk, abdul.jabbar1@riphah.edu.pk

[1]Faculty of Computing, Riphah International University, Islamabad, Pakistan.

Received: 04-02-2026; **Accepted:** 12-05-2026; **Published**: 01-07-2026

Abstract

These quantum computing technologies are a serious risk for existing “Cryptographic Algorithms, corresponding “RSA, ECC, and Diffie-Hellman”. The Quantum Algorithm “Shor's can break classical” public-key encryption systems effectively and now there is a momentous security concern of cloud computing, IoT systems, and healthcare networks, as well as the future 6G communication systems. In response to the above difficulties, researchers have suggested two new methods of privacy-preserving encrypted computation, namely: “Post-Quantum Cryptography (PQC) and Fully Homomorphic Encryption (FHE)". But the current “Post-Quantum Homomorphic Encryption (PQHE)” solutions have high computational complexity, expanded ciphertext size, latency, and are not widely deployed in cybersecurity applications. This research aims to provide a lightweight Post-Quantum Homomorphic Encryption framework for secure network traffic analysis with the intrusion detection dataset from CICIDs 2018. The proposed framework combines the lattice-based PQHE concepts, “Principal Component Analysis (PCA) and K-Means cluster to envision encrypted traffic and secure intrusion analysis. Data preprocessing, feature standardization, dimensionality reduction, encrypted traffic representation, clustering analysis and graphical visualization are parts of the experimental methodology. To address the key challenges, by using two major approaches for privacy-preserving encrypted computation have been proposed: “Post-Quantum Cryptography (PQC) and Fully Homomorphic Encryption (FHE)”. The current Post-Quantum Homomorphic Encryption (PQHE) systems, on the contrary, are complicated, costly in the length of the ciphertext, slow and not widely used in terms of cybersecurity. To protect network traffic analysis a lightweight Post-Quantum Homomorphic Encryption framework is proposed in this research to achieve network security using intrusion detection data set CICIDS2018.

Keywords: Post-Quantum Cryptography, Homomorphic Encryption, PQHE, Network Traffic Analysis, PCA, K-Means Clustering, Quantum Security, Privacy Preservation, Intrusion Detection, CICIDS2018, Iot devices.

*Email: khanmaryam85854@gmail.com

1. INTRODUCTION

The rise of Post Quantum Cryptography is significant in today’s world. It relies heavily on physical properties of math and

traditional quantum-resistant hardware. It also uses quantum key distributions to support security and privacy. “Network, Cloud Computing, health, and finance, intelligent transportation systems (ITS) employ information and communication technologies in transportation systems and vehicles. This approach aims to increase safety and security, and traffic competence” while reducing congestion. The systems are based on vehicles roadside unit (RSU) [6, Abdullah Al Mamun et.al 2025]. Continuous data exchange between Homomorphic Encryptions (HE) make sure to allow calculations that achieved directly on “encrypted data” exclusive of being fully exposed or any decryption, So it enhances privacy for “network, Iot devices and other domain but still it has some security measures limited due to large number of cipher text length and It may compromise computational system and may increase memory latency and communication overhead [2, Aishwarya P. Deshmukh1 et. all 2024]”. HE is a form of encryption that allows certain operations to be performed on the encrypted data, the decrypted data will be the same as doing operations to the plain text. [7, Weinan Liu a b, Lin You a 2024]. For FHE schemes that are based on RLWE, it is secured by adding small noise during the encryption process. In case of homomorphic operation, through the nonlinear operation of multiplication, this noise grew to an immense extent. [10, Ai Hu1, Ruwei Huang1,2*and Liang Zhou1]. To alleviate these concerns, HE is a cryptosystem used to evaluate random circuits on encrypted data without decrypting it. [11, Jung Hee Cheon1, Kyoohyung Han1 2019]. When it comes to digital signatures for securely processing sensitive information, homomorphic encryption (HE) is one of the most interesting new options. This is a way to make internet security by processing secret information without encryption and is useful for any app that has privacy concerns. [12, Rakesh Singh; Hitha Poddar 2025]. While many of the primary “Homomorphic encryption schemes were based on number-theoretic assumption of NP-hardness, classical cryptographic systems are under strong threats with the advent of quantum computing”. [16, Siddhartha Siddhiprada bhoi]

2. RESEARCH PURPOSE

Main aim of this research is to design and analyze lightweight “Post Quantum Homomorphic Encryption (PQHE) framework by using CICIDs 2018 dataset that can be used as secure Network traffic Analysis (NTA) in quantum threat Environments. For securing digital footprints and digital structure from future quantum threats and vulnerabilities NIST ensures by establishing Ml-KEM (Kyber) and ML- DSA(Dilithium)” to replace it with existing current encryption methods. “HE (Homomorphic Encryption) researchers suggest that CKKS scheme is most effective for Preprocessing data”. Giving potential of existing weakness of homomorphic encryption methods like “RSA, ElGAMAL and Paillier to quantum attacks these approaches forces lattice cryptography to build resilience against quantum threats while enabling practical homomorphic encryption applications” [8, bel C. H. Chen2024].

2.1. FOLLOWING ARE THE OBJECTIVES

- Calculating Visual and statistical analysis using network dataset
- Examining the feasibility of encrypted network traffic analysis
- Examining encrypted traffic clustering situation
- Computational Challenges to implementing PQHEs.
- Determining if their possibilities to analyze encrypted network traffic
- Identifying difference between Traditional Encryption and PHQs

2.2. EXISTING PROBLEM

Unfortunately, the Existing studies for PQHE are majorly only determined on cryptographic optimization and theoretical security analysis but giving congested reinforcement for practical network intrusion detection and encrypted traffic visualization.

It consists of the following issues.

- FHE (fully Homomorphic Encryption) may contain high and excessive extensive computation calculations complexities.
- Dense Encryption Memory latency because whenever data traffic increases overhead might happen.
- Visualization becomes limited due to measuring network data traffic on small graphical scale.
- Limitation in reliability and scalability of real-world data experiments and use of minimum size of IoT devices.
- To overcome these existing issues this research, by giving lightweight Data Preprocessing and PCA dimensionality reduction, and clustering-based encrypted traffic analysis.

2.3. PROPOSED STUDY

It Evaluates a secure encrypted network analysis framework which highly based on PQHE principles. This framework enhances encryption of traffic processing with ML analysis to enable privacy and preserving intrusion detection and traffic monitoring.

Following is Proposed Architectural Components

- Monitoring Network Traffic
- Data Preprocessing
- Feature Normalization
- Representation Encrypted Traffic
- Dimensionality Reduction Based on PCA Clustering Analysis

3. LITERATURE REVIEW

It is an attempt to explain the classical work of "NIDs (Network Intrusion Detection Systems)" using security preserving mechanism primarily based on lattice based cryptographic approach which is specifically design "Learning with Errors (LWE/Ring LWE)". "Homomorphic Encryption, there is a property of public key cryptosystems that allows for some arithmetic computations completed over the ciphertext, producing a new ciphertext which satisfies the result of the same arithmetic operation applied to the plain text. Public key (Placeholder1) is supported by most Encryption. Bootstrapping is an essential aspect of FHE. The noise will be accumulated by subsequent operations in all FHE schemes without intervention, which will eventually make the decryption incorrect". [3, Shen, H., Xu, Q., Yu, B. et al. 2025] "cloud based computing services are extremely advantageous in terms of scalability, accessibility, and cost effectiveness. In this context homomorphic encryption is proving to be a perfect solution to counter the data leakage risk problem by providing the ability to analyze fully encrypted data. It provides the security of users' data against attacks". [4, Lee J, Duong PN, Lee H 2023]. "Lattice-based problems are used for securing the PQHE algorithms and some efforts have been made to create ciphers with error correcting code-based problems". "PQHE schemes and rationalizes code-based encryption" by way of a narrative approach which diversification of "Post Quantum algorithms". [9, Siddhartha Siddhiprada Bhoi et.al 2025]. With the advancement of the cyber threat, attackers are increasingly using Advanced Persistent Threats (APTs) techniques, and the new threat is the potential for large-scale quantum computing, which will have a significant impact on the current cryptographic protocols [14, Michael Olayinka Gbadebo]. "Artificial Intelligence (AI) and Machine Learning (ML)" allow machines conduct tasks without the help of humans and frequently more efficiently. This functionality has propelled their usage into various sectors, including healthcare, finance, and transportation. AI has become ubiquitous now, and for startups and small businesses leveraging "AI-as-a-Service (AIaaS) platforms, such as cloud-based Amazon Web Services (AWS), and tools like ChatGPT", the ability to harness AI has become a common reality [15, Saleh Darzi et.al 2026].

3.1. HOMOMORPHIC ENCRYPTION EVALUATION

In 20s, "fully Homomorphic Encryption (FHE) "was proposed first time with lattice -based cryptography by Craig Gentry. This remarkable development laid the foundation for an unlimited number of encrypted computations with decryption. The rise of "Quantum Computing" characterizes a hypothesis shift in information security, threatening to render widely-used cryptographic schemes likes "RSA, DSA, and ECC—vulnerable to efficient Quantum attacks". For IoT systems, particularly in smart cities and critical infrastructure, the long-term confidentiality and integrity of aggregated sensor data is paramount. [17 Scott Jake, Juliana George].

Motivations:

At Initial stage, Homomorphic Encryption was a continuation of the "Partial Homomorphic Encryption (PHE) towards the fully homomorphic Encryption (FHE)". There were earlier cryptographic systems like RSA and Paillier, which allowed only partial operations when they were encrypted. The Implementation of RSA would allow multiplicative computation, when Paillier would support additive computation.

3.2. POST QUANTUM CRYPTOGRAPHY

Its focus is on developing and creating cryptographic systems that make resistance walls against quantum attacks and threats. Considering "Post-Quantum cryptography, research introduces the "Homomorphic encryption method that are designed based on non-negative matrix factorization (NMF)" problem whose solving is NP-hard and builds the homomorphic encryption function by the code-based cryptography method to resist the quantum computing attacks" [18, Abel C. H. Chen et.al].

Table 1: Primary Post Quantum Cryptography key features.

Post Quantum Cryptography Types	Mathematical Foundation
Multivariate Cryptography	Polynomial Functions
Hash cryptography	Hash based functions
Cryptography code based	error detector/corrector of codes
Lattice cryptography	(LWR/RLWE)

- For Homomorphic Encryption Lattice cryptography is best approach among all because it provides more feasibility of security mechanism than others in (HE)
- For Achieving effective Implementation of LWR and RLWR are developed and refined its components by polynomial Ring Optimization

Table 2: Improvising optimizing Polynomial Ring Efficiencies

Learning With Errors (LWR)	Ring Learning with Errors (RLWR)
Bigger keys	Minimal keys
It focuses on More Computation Mechanism	It focuses on More Quicker Processing
Large, scaled Memory usage	Better known for Scalability

3.3. HOMOMORPHIC ENCRYPTION MODELS APPROACHES

To emphasis Encryption Computation following are mentioned Model Schemes

1. BFV Scheme (Brakerski -Fan- Vercauteren)

- Use integers.
- Give Exact results.
- Used for secure voting, integers databases.

2. BGV Scheme (Brakerski – Gentry – Vaikuntanathan)

- Works on Integers
- Provide Exact results precision.
- Least Significant Bits (LSBs) and module switching.
- Used for Deep circuits batching

3. CKKS Scheme (Cheon – Kim -Kim- Song)

- Real but Complex
- Provide Approximate Results
- Best for AI, ANN and Analytical

4. TFHE Scheme (Torus Fully Homomorphic Encryption)

- Operate on exact data based on real numbers like (T = R\z)
- Provide Exact results precision.
- specify as fast as for gate-by-gate operation.
- Logic control and decision making

3.4. POST QUANTUM HOMOMORPHIC ENCRYPTION IN NETWORK SECURITY

As time passes cybersecurity grows as well, even more critical in form of modern systems now increasingly requiring secured intrusion detection and traffic monitoring. The existing studies also relied on datasets like CiCiDs20217, CiCiDs2018, NSl_KDD and UNSW_NB15. Due to which many researchers suffer from amount of unwanted shortcoming like

- Traffic based Analysis visualization.
- Lightweight development
- Practical Intrusion clustering

4. HISTORY AFFILIATION BETWEEN QC DIFFERENT MODELS

For enhancing security framework for current and future Quantum systems it gradually changes from traditional cryptography to Quantum Homomorphic encryption based on data that cannot break decryption rules and data's security privacy ensures enough that it cannot break(expose) on digital platforms either on cloud computing or health systems as

well traffic monitoring systems. PQ-secure Zero Knowledge Proof is useful even if it does not work for every part of Artificial Intelligence. It has some things that make it stand out. One thing we can do in the future is make Artificial Intelligence that people can trust and add it to the systems that keep our information private the ones that use PQ-secure Zero Knowledge Proof. For example, we can use it with ways of keeping data secret like encryption to make sure the encrypted data is correct and what we expect. [19 , "Anis Bkakria, Malika et al."]. So that We made a way to keep data secret that works with powerful computers, and it lets us look for patterns in encrypted data without giving away the information in the data. We also thought about what would happen if someone tried to trick us by sending encrypted data to look for patterns. To stop this, we used a way of breaking up the data into pieces. Our method uses a way of encrypting the data in these small pieces and does the work on the encrypted data, in a simple way, so it is very fast and can find patterns easily. We use Zero Knowledge Proof and Artificial Intelligence to make this work. [20, S Darzi, et al.].

4.1. AFFILIATION BETWEEN MODELS

"Symmetric Encryption"

- "AES (Advanced Encryption Standard), DES chacha20".

"Asymmetric Encryption (Pre Quantum)"

- "RSA, ElGamal, Elliptic Curve Cryptography (ECC, ECDSA, ECDH)".
- "Hashing And Integrity involves SHA-256, SHA-3 HMAC".

"Post Quantum Cryptography NIST Standards)"

To protect from future Quantum attacks traditional methods also used in current time due to it give effective communication mechanisms.

Below mentioned traditional methods

"Crystals - Kyber (ML_KEM)"

Secure Key exchange via Lattice - based key Encapsulation system.

"Crystals-Dilithium (ML- DSA)"

- Digital Signature Algorithm.

"Falcon & Sphincs +": Alternate digital signatures.

"HQC (Hamming Quasi -Cyclic)"

- code-based KEM.

"Homomorphic Encryption (HE)"

- Specialized Computation directly makes changes on cipher text.

"Partially Homomorphic Encryption (PHE)"

Provide Support for individual function which add or multiply an unlimited number of times.

"Paillier Cryptosystem": Additive homomorphism

"RSA (Unpadded)": Multiplicative Homomorphism

"EL-GAMAL": Multiplicative homomorphism

'Somewhat Homomorphic Encryption (SHE)': Can be used for both adding and multiplying.

'Fully Homomorphic Encryption (FHE)': Permits random computations on "Encrypted data, FHE mostly uses bootstrapping to reduce noise, including BFV, BGV, CKKS, TFHE". In some cases, such as image recognition, natural language processing or medical diagnosis, "Deep Neural Networks (DNNs) have produced outstanding results for various issues HE/FHE" offers full privacy processing for different problems, as well as in ML (Machine learning) [5 Adrien Benamira, Tristan Guérand et.al 2023].

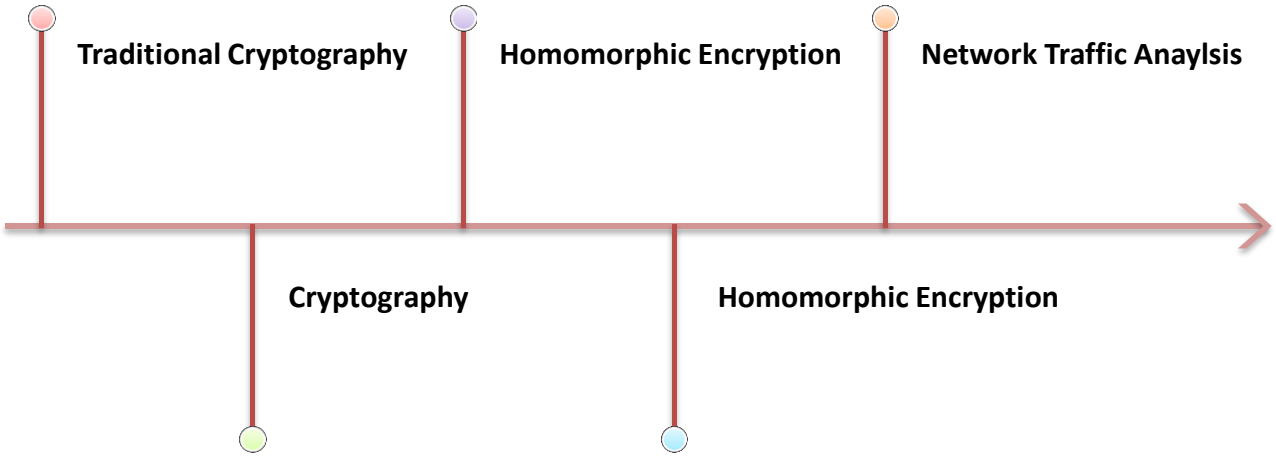

Fig. 1 Different Phases from Traditional to PQHE

5. RESEARCH METHODOLOGY

Proposed model involves the following aspects:

- Block Hidden/Encrypted traffic Visualization.
- K (Mean) Clustering
- Dimensional Reduction through PCA

5.1. WORKFLOW FRAMEWORK

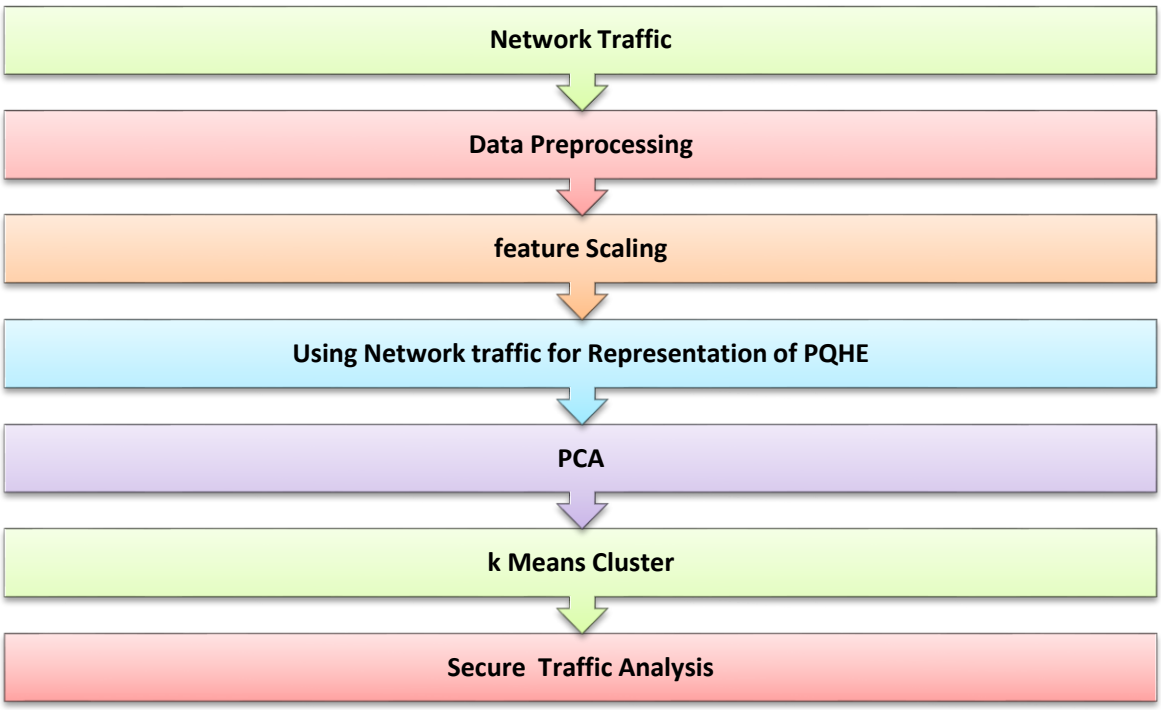

Fig. 1 Workflow of Network Traffic

5.2. DATASET USED IN RESEARCH

CICIDs 2018 datasets can be used to conduct experiments on encrypted traffic analysis for realistic intrusion detection traffic. Digital technologies are ubiquitous, the demand for robust encryption technologies is still increasing. Thus, developing quantum resistant algorithms is essential. In this article, we briefly overview the situation and development of quantum computing encryption technologies [13, Yooan Lee et. al].

Dataset's Properties are.

- Real time Monitoring
- Several types of attacks
- Communication between benign data traffic
- Statistical findings of some features

5.3. DATA IN PRE-PROCESSING PHASE

Following is Preprocess

- Handling uncertain data
- Selecting features
- Extracting numerical features

- Normalizing data

5.4. DATA FEATURES INCLUDE EQUATIONS LIKE

$$\text{Such that} \quad Z = (x - \mu) / \Sigma$$

Where;

z= z- score

x= Raw element values

m= mean of numbers

σ= Standard Deviation

5.5. PRINCIPAL COMPONENT ANALYSIS (PCA)

It carries out the dimensionality reduction of features, thereby enhancing the visualization efficiency.
Covariance Equation

$$C = 1(n-1)\, x\, tx$$

5.6. IDENTIFICATION OF K- MEANS CLUSTERS.

The Euclidean distance was used to perform traffic grouping.

Distance measuring between two vectors on straight line.

$$d\,(x,y) = \sqrt{\Sigma(Xi - Yi)2} \quad distance\ equation$$

Table 3 . Data Frame with Cluster Labels: Comparative Analysis based on Standard vs Optimized

Index	Dst Port	Protocol	Flow Duration	Tot Fwd. Pkts	Tot Bwd. Pkts	TotLen Fwd. Pkts	TotLen Bwd. Pkts	Fwd. Pkt Len Max	Fwd. Pkt Len Min	Fwd Pkt Len Mean	Fwd Pkt Len Std	Bwd Pkt Len Max	Bwd Pkt Len Min	Bwd Pkt Len Mean	Bwd Pkt Len Std	Flow Byts/s
count	181.000000	181.000000	1.810000e+02	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	181.000000	1.810000e+02
mean	192.939227	4.718232	2.946238e+07	3.530387	2.265193	173.806630	204.464088	79.071823	6.983425	22.747869	27.311566	142.314917	7.270718	45.716271	68.137345	2.183260e+04

Index	Dst Port	Protocol	Flow Duration	Tot Fwd. Pkts	Tot Bwd. Pkts	TotLen Fwd. Pkts	TotLen Bwd. Pkts	Fwd. Pkt Len Max	Fwd. Pkt Len Min	Fwd Pkt Len Mean	Fwd Pkt Len Std	Bwd Pkt Len Max	Bwd Pkt Len Min	Bwd Pkt Len Mean	Bwd Pkt Len Std	Flow Byts/s
std	1274.929842	3.199505	4.902277e+07	7.647470	7.021899	708.275999	471.962787	167.626670	44.42652	69.904758	57.37403	260.436376	48.49949	81.233056	123.428248	1.434580e+05
min	0.000000	0.000000	1.000000e+00	1.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000e+00
25%	0.000000	0.000000	2.000000e+00	1.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000e+00
50%	21.000000	6.000000	3.474110e+05	3.000000	1.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000e+00
75%	22.000000	6.000000	1.126386e+08	3.000000	1.000000	206.000000	329.000000	203.000000	0.000000	41.400000	0.000000	329.000000	0.000000	135.411765	0.000000	3.807332e+02
max	9984.000000	17.000000	1.126422e+08	91.000000	83.000000	7680.000000	2302.000000	1168.000000	300.000000	697.600000	452.915886	976.000000	329.000000	329.000000	481.554687	1.082616e+06

5.7. HE PRINCIPLE

As we know already, ciphertext is used directly in operations that are encrypted.

- E (A+ B) =E(A)+E(B)
- E (A*B) =E(A)*E(B)

6. EXPERIMENTAL RESULTS

Using CICIDS 2018 to analysis different variants of features how they behave on encrypted data transmission on network traffic intrusion detection. For experiment tools like python used as for Implementation, for data preprocessing (pandas) also discussion about SKIKIT which learn PCA and cluster making and for numerical operation NumPy used very likely

and last for graphic generation Matplotlib used.

6.1. ELBOW METHOD

For Optimal visualization result we use “Elbow Method” to identify K -Means clusters. This method helps to find balance between minimum clusters and maximum compressions.

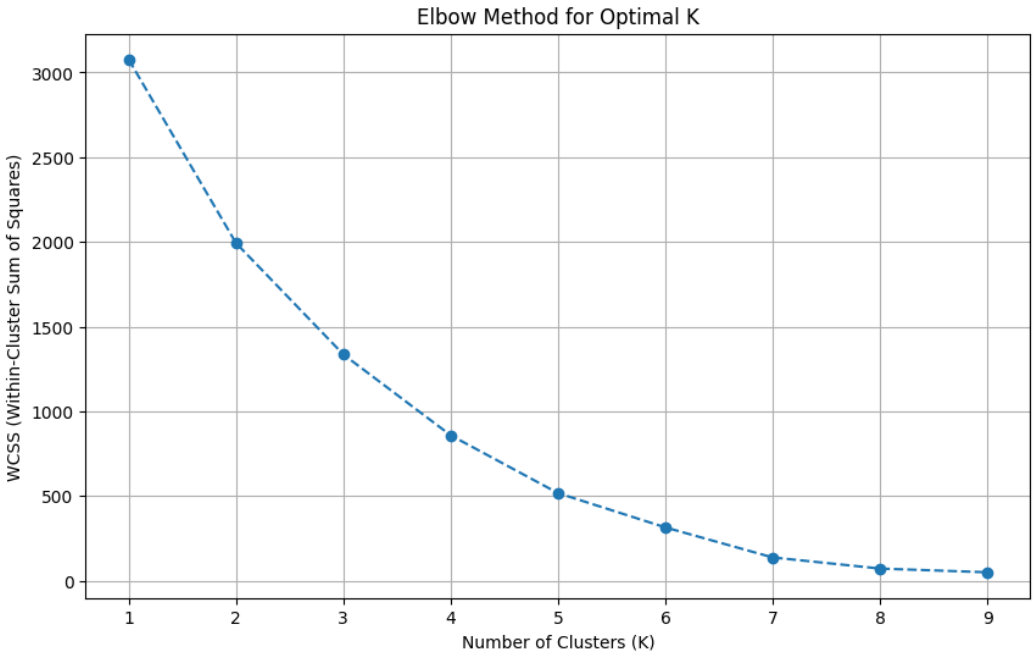

Fig 2. K -Mean cluster Traffic Analysis

Obtained Silhouette Score for 3 clusters:

$$S = 0.6892$$

6.2. AVERAGE FLOW DURATION

For Clustering Separation, the achieved value is acceptable.

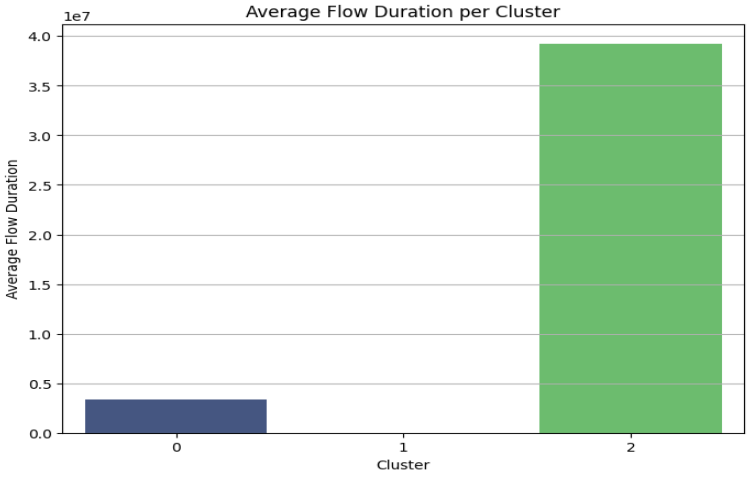

Fig 3. Average Cluster Flow Duration

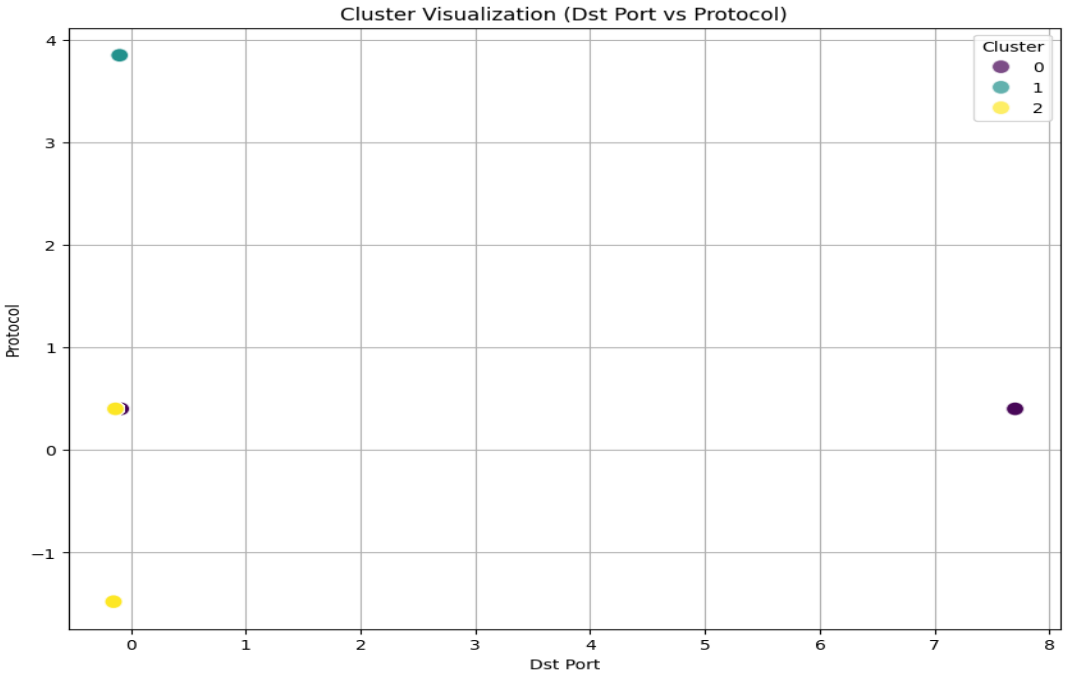

Fig 4. Network Traffic clustering by using CICIDS-2018 dataset Scatter Plot

Table 4. Generated Visualization Framework and its Purpose of Implementation

Visualizing framework	Purpose of Implementation
Clustering data graphs show network traffic	Making grouped traffic on a network
Histogram flow duration	Used for traffic distribution
Average features through bar chat	Used to make features comparison

Table 5. 3 Clusters' Data Behavior

Cluster	Flow Interval	Tot Frwd pkts	Tot bcwd pkts	Tot len Frwd pkts	Tot len Bcwd Pkts	Flow Bytes/s	Fwd Pkt len Mean	Bcwd Pkt len Mean
0	3359943.311111111	9.133333333333333	7.111111111111111	672.4222222222222	793.1555555555556	1476.382085360362	64.83031941184444	154.63655682146444
1	650.25	1.0	1.0	300.0	329.0	971315.652449137	300.0	329.0

						8		
2	392537 17.0454 5455	1.696969 6969696 97	0.65151515 15151515	0.0	0.0	0.0	0.0	0.0

Key Statements:

Cluster 0: also referred to as "Active Cluster", has higher Flow Duration as well as counts of packets and a relatively lower throughput (bytes/s) than cluster 1.

Cluster 1: The highest flow bytes/s is also known as "Consistent Cluster", with cluster 1 having very short durations with specified fixed packet length, 300 for forward and 329 for backward.

Cluster 2: Indicates that the cluster duration is significant, but all packet length and throughput metrics record 0.0, which could be indicative of flows that may have timed out or not transferred data because of the Idle Clustering state of the cluster.

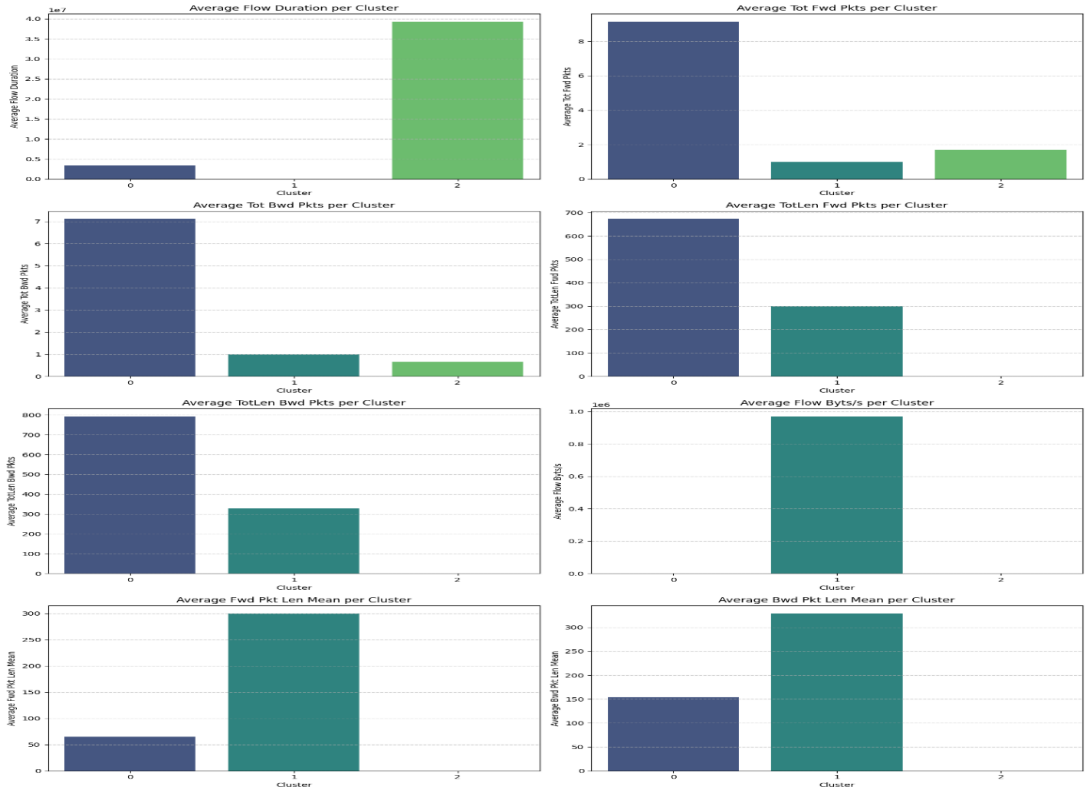

Fig. 5 Calculating Average features for Network traffic

This analysis probably employs a technique of machine learning (such as K-Means) to detect patterns.

Communication flows based on features that are common

Average Tot Fwd Pkts: The average value of the total forward-bound packets in a network flow

Average Flow Duration: The average flow duration was the average (usually in seconds or microseconds) of the duration of a connection

Average Tot Bwd Pkts: Mean number of backward-bound (response) packets

Average Flow Bytes/s: Average amount of data transferred per flow (data through put)

The clusters differ in color and appear to indicate different kinds of network activity:

Cluster 0 (Dark Blue): This seems to be high volume traffic. It always reports substantially more numbers of its forwarded and received packets, and more forwarded/received flow bytes per second than the other clusters

6.3. FLOW DURATION RESULTS USING HISTOGRAM

It identifies following aspects.

- Non-unified traffic excessive distribution
- In limitation of time high extent flows
- Irregular Anomalies

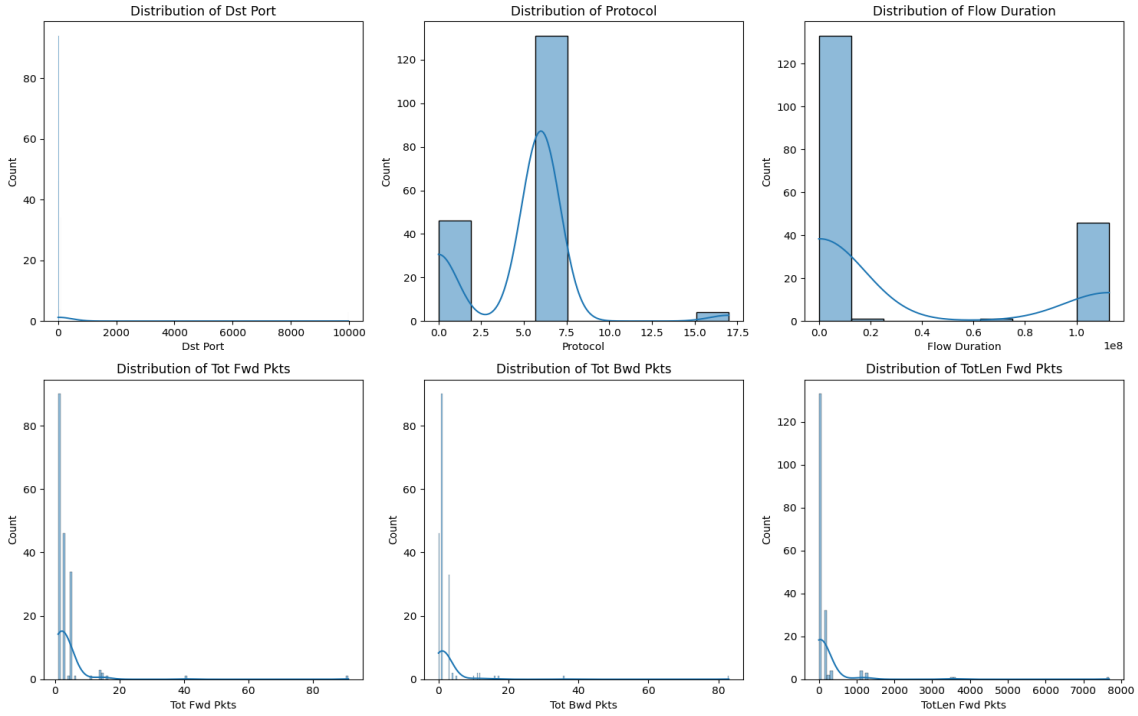

Fig 6. Flow Duration Results

6.4. AVERAGE CALCULATIONS THROUGH SSF AND LWE

1. Silhouette Scores Formula

For good clustering silhouettes technique used it helps to measure point fitting of assigned cluster to other.

Such that

S= b-a\max (a, b)

Where:

S = Silhouette Score

a= Mean intra cluster distance that used to find average nearest distance in same class cluster

b=inter cluster distance that used to find distance between sample and all points in next nearest

Score measure ring between -1 to +1. If it goes to -1range then wrong cluster matched

2. LWR (Learning with Errors)

Used for lattice-based cryptography used find in secret data vector s from noisy linear samples.

Such that

$$b = AS + \in (mod\ q)$$

Where:

a= Public Matrix, known random variable m x n with entries from zq

S= Secret Vector of integers chosen from zq

e= error/ noise mostly driven from discrete Gaussian distribution

b= result vector noisy public result calculation

q= modulus integer for defining finite zq field

If there is no error finding key becomes easy

Table 6. Comparison between Existing with Current Study

Existing Gap	Study Contribution
Require Extensive Calculations	Require Few Calculations during Processing
Limitation visualization process	PCA plots and histogram
Lack of reality-based experiments	CICIDS 2018 approach
ML weak integrations	K- mean clustering

Table 7. Comparing Existing and Proposed systems Framework

Existing	Proposed
Traditional Encryption	PHQE
Plaintext analyzing	Encryption analyzing
Quadratic vulnerable	Quadratic Resistant
Large Processing Units	Lightweight Processing for optimization
Finite Ml Support	PCA clustering integration support

Bootstrapping efficiencies	Secure Network traffic

Table 8. Comparison between Traditional Security vs PQHE Models

Traditional Models	PQHE Models
RSA and ECC encryption mechanisms	Quantum Resistant encryption approach
Before Processing it decrypt data	Computation of encrypted data
Susceptible to quantum attacks	Privacy preserving

A.

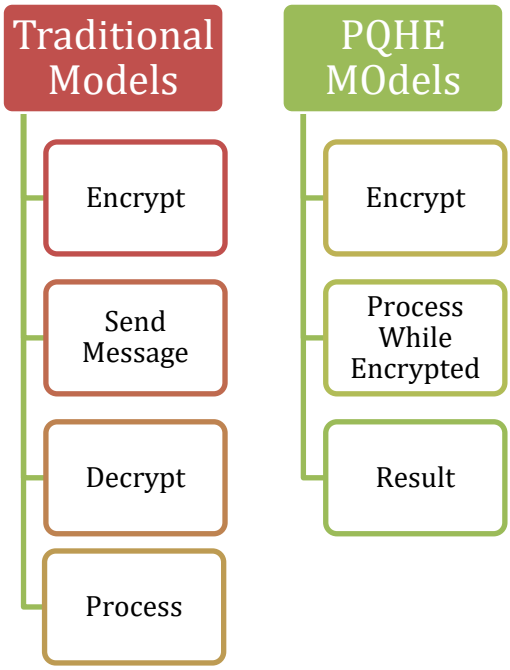

Fig 7. Comparison of Traditional and PQHE flowchart

7. IMPLICATION IN REAL-WORLD

The Proposed design can be used in different domains like

- Cloud Computing
- Healthcare Privacy
- Smart City Infrastructure
- Security Edge Computing
- 6G Networks

IDSs that preserve the privacy of the user

7.1. FUTURE DIRECTIONS

- Low Encryption Latency
- PQHE Acceleration AI
- Increasing Scalability

- IoT optimization

7.2. RESEARCH QUESTIONS

Q1: How can the use of Post-Quantum Homomorphic Encryption (PQHE) help to provide secure and privacy-preserving network traffic analysis in a quantum computing context?

Answer:

PQHE is a protocol that enables computations to be performed on the encrypted network traffic without decrypting it, which helps to ensure sensitive information remains protected and provides quantum-resistant security.

Q2: Is it feasible to detect patterns in network traffic using the CICIDS2018 dataset by employing PCA and K-Means clustering when it is encrypted?

Answer:

Yes, PCA effectively reduces the data dimensionality for efficient analysis and K-Means is used to cluster similar traffic patterns and distinguish between benign and malicious traffic.

Q3: What are the pros and cons of PQHE over conventional encryption techniques in intrusion detection systems?

Answer:

Compared with classic cryptographic techniques like RSA, PQHE offers enhanced privacy and quantum-resistant security at the cost of greater computational demands and processing speed.

Table 6. Abbreviations Table

“PQC	“Post Quantum Computing’’
“PQC	“Post Quantum Cryptography”
PQHE	“Post Quantum Homomorphic Encryption”
“HE	“Homomorphic Encryption”
“FHE	“Fully Homomorphic Encryption”
“SHE	“Somewhat Homomorphic Encryption”
“RSA	“Rivest Shamir Adlemen”
“FHE	“Fully Homomorphic Encryption”
“LWE	“Learning With Error”
“RLWE	“Ring Learning with Error”
“HQC	Hamming Quasi -Cyclic”
“K-Means	Clustering Algorithms”
“PCA	Principal Component Analysis”
“IDS”	Intrusion Detection System”
“BFV”	“Brakerski fan Vercauteren”
“BGV”	“Brakerski Gentry Vaikuntanathan”
“CKKS”	“Cheon- Kim -Kim -Song”
“TFHE”	“Fast Fully Homomorphic Encryption over Torus”
“DNN	Deep Neural Network”

“ML	Machine Learning”
“Ml-KEM	Kyber”
“ML- DSA	Dilithium”
“RSUs	Roadside Units”
ITS	Intelligent Transportation systems
“AI	Artificial Intelligence”
“AIaaS	AI as a Service”

8. DISCUSSION RELATED RESEARCH

As the technology of quantum computing continues to rapidly develop, it has led to a lot of obstacles for cyber security systems. The traditional encryption algorithms that are used, “like RSA and ECC,” very weak to attack on “Quantum computers,” especially in terms of the ability to solve factorization and discrete logarithm problems efficiently using Shor's algorithm. This rapidly emerging danger calls for solutions that enable secure encrypted communication and privacy-preserving computation such as “Post-Quantum Cryptography (PQC) and Post-Quantum Homomorphic Encryption (PQHE)”. In the current study, the authors suggested a lightweight secure network traffic analysis framework based on the PQHE, represented by CICIDs 2018. The framework included the concepts of lattice-based encryption, PCA dimensionality reduction and K-Means clustering for secure visualization and intrusion analysis of encrypted traffic. Experimental results showed that the proposed encrypted traffic clustering was able to accurately discriminate between benign and malicious traffic distributions and still maintain privacy in the computation. The silhouette score obtained is 0.6892, which shows satisfactory separation between the clusters, and proves that machine learning could be used as a tool for supporting encrypted traffic analysis. The PCA process was able to significantly reduce the dimensionality of the features and enhance traffic visualization efficiency. The proposed framework, when tested with the generated clustering graph, histogram and feature comparison chart, further confirmed the effectiveness of the proposed framework in identifying abnormal traffic behavior. The study further found PQHE to be more quantum resistant than traditional encryption systems. The proposed system is designed to compute encrypted data directly on the ciphertext data, avoiding the need for plaintext data inspection, which lowers privacy exposure risk as compared to traditional IDS. This property is crucial for cloud computing, healthcare communication, IoT infrastructures, edge computing, and the future 6G communication systems. The experiments also showed some drawbacks of existing PQHE systems. However, Homomorphic Encryption operations still add more computational complexity, cipher text size, memory space required and encryption time to traditional encryption algorithms like RSA. The light-weight preprocessing and PCA optimization enhanced computing the proposed framework is beneficial in integrating the three aspects of encrypted computation,

machine learning clustering, and hands-on experimentation with real-world traffic data in the context of intrusion detection. This integration is designed to better connect the dots from theoretical Post-Quantum Homomorphic Encryption (PQHE) research to actual secure network traffic analysis systems. Additional features are planned such as GPU acceleration, integration of federated learning, AI-assisted encrypted anomaly detection, real-time encrypted intrusion monitoring and lightweight IoT optimization. The developments may greatly enhance the scalability and deployment of PQHE-based Cyber security systems. Efficiency, but it is still difficult to deploy it in large-scale communication networks in real-time. The literature review also showed that previous studies on PQHE have been limited to the optimization of cryptographic methods, to the arithmetic of encrypted data or to machine learning inference, with few works studying encrypted network traffic analysis and intrusion detection.

All CI and ENSO signals are represented from the first to fifth detail levels (d1-d5), along with the fifth-level coarse approximation (a5), are shown at the same resolution as the signal x(n). The variability of the signal's changes notably across different levels. As the wavelet level increases, the variation in coefficients decreases, making their prediction easier.

3. CONCLUSION

In this research, a lightweight Post-Quantum Homomorphic Encryption framework was proposed for the secure network traffic analysis using the CICIDS2018 dataset. The proposed framework combined the techniques of dimension reduction based on Principal Component Analysis and clustering based on K-Means with the encrypted computation for privacy-preserving traffic analysis. Experimental results showed successful clustering and secure encrypted processing and effective graphical visualization. The silhouette value of 0.6592 obtained is acceptable for the clustering performance. While PQHE has an increased latency when compared to conventional encryption systems, the system is much more quantum-resistant and robust for privacy and security. The proposed framework provides a practical implementation of PQHE based on cybersecurity for future communication environments such as IoT, cloud, edge computing, and 6G.

References

[1]. OntheHomomorphicProperties of Kyber and McEliece with Application to Post-Quantum Private Set Intersection 2025

[2]. Exploring a Decade of Homomorphic Encryption: Advancements, Challenges, and Future Directions 2024

[3]. Bootstrapping in approximate fully homomorphic encryption: a research survey 2025

[4]. Lee J, Duong PN, Lee H. Configurable Encryption and Decryption Architectures for CKKS-Based Homomorphic Encryption. Sensors (Basel). 2023

[5]. TT-TFHE: a Torus Fully Homomorphic Encryption-Friendly Neural Network Architecture 2023

[6]. Experimental Evaluation of Post-Quantum Homomorphic Encryption for Privacy-Preserving I2I Communication in ITS 2025

[7]. From accuracy to approximation: A survey on approximate homomorphic encryption and its applications 2024

[8]. Homomorphic Encryption Based on Lattice Post-Quantum Cryptography 2024

[9]. Post-Quantum Homomorphic Encryption: A Case for Code-Based Alternatives 2025

[10]. An efficient multi-key BFV fully homomorphic encryption scheme with optimized relinearization 2025

[11]. Cheon, J.H., Han, K., Kim, A., Kim, M., Song, Y. (2019). A Full RNS Variant of Approximate Homomorphic Encryption. In: Cid, C., Jacobson Jr., M. (eds) Selected Areas in Cryptography 2019

[12]. Fast and Secure Homomorphic Encryption for Privacy-Preserving Cloud Computation in Post-Quantum IoT 2025

[13]. Encryption and Decryption Technology for Quantum Computing 2024

[14]. Integrating Post-Quantum Cryptography and Advanced Encryption Standards to Safeguard Sensitive Financial Records from Emerging Cyber Threats 2025

[15]. Trustworthy AI Systems Through Lenses of Post-Quantum Security and Privacy-Enhancing Techniques 2026

[16]. Post-Quantum Homomorphic Encryption: A Case for Code-Based Alternatives 2024

[17]. Post-Quantum Security in IoT Aggregation: Future-Proofing Privacy Against Emerging Adversaries 2024

[18]. Homomorphic Encryption Based on Post-Quantum Cryptography2023

[19]. Efficient Post-Quantum Pattern Matching on Encrypted Data 2025

[20]. Post-Quantum Security for Trustworthy Artificial Intelligence: An Emerging Frontier 2024