

Context-aware lightweight and post-quantum cryptographic framework for secure wireless communication

Shashishekhar Ramagundam *

Department of Computer Science

Troy University

2500 University Station Montgomery

AL 36104

U.S.A.

Harsha Karamchandani [†]

Department of Electronics and Communication Engineering

Nitte Meenakshi Institute of Technology

Bangalore 560064

Karnataka

India

Gajanan Uttam Patil [§]

Department of Electronics and Telecommunication Engineering

Shri Sant Gadge Baba College of Engineering and Technology

Bhusawal 425201

Maharashtra

India

Priti Subramaniam [‡]

Department of Computer Science and Engineering

Shri Sant Gadge Baba College of Engineering and Technology

Bhusawal 425201

Maharashtra

India

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

* E-mail: sshekharr1@gmail.com (Corresponding Author)

† E-mail: harsha.mkaramchandani@nmit.ac.in

§ E-mail: gajanan.bsl@gmail.com

‡ E-mail: pritikanna559@gmail.com

Abstract

A context-aware cryptographic framework is proposed in this paper for protecting wireless communication networks using lightweight and post-quantum encryption. Fuzzy logic is used in the system to quickly assess channel quality, battery level, user's movement and how sensitive the data is. Using these factors, it can pick the right sort of encryption automatically. Testing and analyzing the framework through modeling and simulation indicate efficient energies, speed and security are achieved by the framework. This new method supports forthcoming networks such as IoT, MANETs and 6G with high resistance to quantum threats.

Subject Classification: Primary 81P94, Secondary 94A60.

Keywords: Context-aware security, Fuzzy logic, IoT security, Lightweight encryption, Post-quantum cryptography.

1. Introduction

Wireless technology today supports a thriving digital framework, making mobile internet, smart cities, autonomous vehicles and IoT possible. At the same time, the bigger and more varied these systems become, the bigger the security problem becomes. Types of encryption that have worked well in many situations tend to be tough to use reliably on wireless networks that are changing, noisy and have limited resources [1], [2]. Because devices in these places are limited in computing, battery life and network capacity, they face many different types of cyberattacks.

Furthermore, when quantum computing arrives, the well-known cryptographic algorithms RSA and ECC are thought likely to no longer be effective [3]. As a result, more attention is given to post-quantum cryptography which hopes to stop attacks from quantum adversaries [4]. At the same time, wireless systems in use now have to be flexible and cope with a wide range of things like signal strength, battery life and user movement. Now, traditional, general security methods aren't a good fit anymore [5].

Soft computing has found its way to the top as a promising fix for these difficulties. Soft computing methods allow you to manage uncertainty, partial truths and changes in data differently than hard computing does [6]. Integration with cryptography gives intelligent agents the skill to decide quickly, update security rules and watch for threats, always keeping applications light and efficient.

For this research, we build a new security structure that utilizes hybrid methods, including advanced cryptography and other techniques from soft computing to better defend wireless networks. The system reviews critical signals and device data such as signal strength, energy level and sensitivity and decides which encryption methods to use in real time using fuzzy logic [7].

This approach helps offset trades between speed, energy and protection and also makes the system future-ready for resisting threats from quantum systems.

As a result, we have a powerful security model that is flexible, saves energy and is made for use in future wireless systems, like IoT, MANETs, 5G/6G and drone communication [8].

Research Contributions: This paper offers several important contributions:

- Combines swift post-quantum and lightweight encryption techniques in a special framework for use in wireless networks with limited resources.
- Adds a security layer that works according to a fuzzy logic algorithm that changes the gateway's encryption according to real-time things like channel quality, battery and the sensitivity of the data.
- The approach models context as different scenarios and attaches a security score to address risk differently depending on what is most suitable and practical.
- Explains ways that neural networks and genetic algorithms can be applied to increase the efficiency of intrusion detection, key management and security tuning.
- Enables the approach to be compared, in software simulation, to the assessment of wireless networks by static security models.

This paper is arranged as follows. An overview of wireless security research is presented in Section 2, together with recent advances in post-quantum cryptography and soft computing models. Section 3 describes the proposed framework for context-aware cryptography, after quantization, along with its detailed mathematical structure. Simulations are conducted and charted in Section 4 to analyze the proposed model's behavior under changing wireless settings. At the end of the paper, Section 5 draws conclusions from the main points and highlights the topics for further investigation.

2. Literature Review

With quantum computing now being developed, classical cryptography may be seriously affected. Because of this, researchers have investigated adding post-quantum cryptography (PQC) to wireless communication procedures. In their work, the authors of [9] suggested connecting PQC to TLS which they showed can securely handle user communications in 5G networks. Similarly, NIST recently selected its main set of algorithms built to beat quantum computer attacks, asking developers to use them as standards [10].

Thanks to understanding different contexts such security can effectively combat new wireless threats. The authors of [11] suggested a CaSemCom system which uses Context-Free Grammars to guide Large Language Models in choosing useful semantic features in wireless networks. The authors of [12] also suggested Fog-Based Adaptive Context-Aware Access Control (FB-ACAAC) which automatically changes access policies in response to contextual information to boost IoT security.

Soft computing methods make it easy to manage a variety of uncertain and unclear details which supports better wireless network security. The authors of [13] analyzed the use of soft computing methods such as Artificial Neural Networks (ANN) and Adaptive Neuro-Fuzzy Inference Systems (ANFIS), to strengthen cryptographic approaches for wireless communication. There is ongoing research on using soft computing to enhance how well wireless networks perform, remain reliable and remain secure, particularly for Unmanned Aerial Vehicles (UAVs) [14].

It uses principles of quantum mechanics to ensure uncompromised safety. The potential of quantum cryptography for securing networks is discussed, as well as the difficulties of implementing this approach, in a detailed work by the authors of [15]. It has become clear that adding post-quantum cryptographic methods to mobile devices plays a key role in protecting data while it is being sent and while it is stored [16].

Additional defense for wireless networks is possible with PLS techniques. The authors of [17] introduced a deep reinforcement learning method to improve how Wi-Fi networks use cooperative jamming and showed it results in better secrecy. The technique automatically changes jamming signals to keep eavesdropping from being successful, proving the use of machine learning in wireless security [18].

3. Proposed Methodology

Mathematical representation of the proposed context-aware lightweight and post-quantum cryptographic framework is shown here. The purpose is to develop methods that automatically pick the best types of encryption for safe wireless communication [19] when faced with real-world network and device issues. There is environment-aware sensing, fuzzy decisions based on logic and a way to improve encryption choice using optimization.

3.1 System Context Vector Modeling

At every time instance t , a wireless node checks its environment by using a context vector.

$$C(t) = \{Q(t), E(t), M(t), S(t)\} \quad (1)$$

Where:

- $Q(t) \in [0,1]$: Channel quality (e.g., normalized SNR or BER),
- $E(t) \in [0,1]$: Energy level or remaining battery,
- $M(t) \in [0,1]$: Mobility factor (speed or handoff rate),
- $S(t) \in [0,1]$: Data sensitivity score.

Each component of the process is standardized by using:

$$X'(t) = \frac{X(t) - X_{\min}}{X_{\max} - X_{\min}}, X \in \{Q, E, M, S\} \quad (2)$$

Because of this normalization, information can be shared easily across a variety of devices and types of data.

3.2 Fuzzy Scoring Function for Encryption Adaptation

A weighted fuzzy inference function is used by the system to compute the intensity metric $\sigma(t)$ using soft computing.

$$\sigma(t) = \mathcal{F}(\mathcal{C}(t)) = w_Q \cdot \mu_Q(Q(t)) + w_E \cdot \mu_E(E(t)) + w_M \cdot \mu_M(M(t)) + w_S \cdot \mu_S(S(t)) \quad (3)$$

Where:

- $\mu_X(\cdot)$ associates every input with an amount of risk or need using fuzzy membership functions.
- $w_i \in [0,1]$ and $\sum w_i = 1$

Example fuzzy logic rule (simplified logic rule):

If $Q(t)$ is low, and $E(t)$ is low, then $\sigma(t) \rightarrow$ low, hence use lightweight encryption.

For every parameter, typical triangular fuzzy sets is formed as:

$$\mu_X(x) = \begin{cases} 0 & x < a \\ \frac{x-a}{b-a} & a \leq x < b \\ \frac{b-x}{c-b} & b \leq x < c \\ 0 & x \geq c \end{cases} \quad (4)$$

for $x \in [0,1]$, and parameters $a < b < c$ defining fuzzy regions.

3.3 Encryption Strategy Selection Model

The set of encryption schemes is shown as $E = \{e_1, e_2, \dots, e_n\}$. Every strategy e_i consists of a triple.

$$e_i = (\text{Cipher}_i, \text{Mode}_i, \text{KeyLifetime}_i) \quad (5)$$

Let us call the output of the fuzzy system, $\sigma(t) \in [0,1]$. Define a piecewise selection function $S(\cdot)$ that changes the score to a strategy.

$$e^*(t) = S(\sigma(t)) = \begin{cases} e_L, & \sigma(t) < 0.3 \text{ (Lightweight)} \\ e_H, & 0.3 \leq \sigma(t) < 0.6 \text{ (Hybrid)} \\ e_Q, & \sigma(t) \geq 0.6 \text{ (Post-quantum)} \end{cases} \quad (6)$$

Where:

- e_L =(PRESENT, Symmetric, Short)
- e_H =(AES-128 + Dilithium, Hybrid, Medium)
- e_Q =(Kyber, Asymmetric, Long)

3.4 Optimization Formulation

For a smooth balance between security and cost, an objective function is established:

$$\max_{e \in E} [\alpha \cdot \text{Security}(e) - \beta \cdot \text{Cost}(e, \mathcal{C}(t))] \quad (7)$$

Where:

- $Security(e)$: Numerical score (e.g., 1–5) based on algorithm strength,
- $Cost(e, C(t)) = \lambda_1 D(e) + \lambda_2 P(e) + \lambda_3 T(e)$

with:

- $D(e)$: Delay,
- $P(e)$: Power consumption,
- $T(e)$: Computational time.

This is a constrained optimization:

$$\text{Subject to: } P(e) \leq P_{\max}, T(e) \leq T_{\text{thresh}}, D(e) \leq D_{\text{QoS}} \quad (8)$$

3.5 Real-Time Updating Mechanism

Cryptographic algorithms are updated regularly Δt when changes happen in the environment.

$$C(t + \Delta t) \rightarrow \sigma(t + \Delta t) \rightarrow e^*(t + \Delta t) \quad (9)$$

Because it automatically adapts, a reboot or manual change is not required for real-time, wireless security systems [20].

4. Results and Analysis

To assess the performance of the context-aware cryptography framework, we performed simulations under a range of network circumstances and analyzed how several encryption strategies react to changes in energy, movement and what type of data was being used. Three situations were determined and fuzzy logic controlled how the system chose the encryption mode to use. Read on to see the main outcomes.

The energy consumption is displayed for each encryption method in Figure 1, all measured under practical wireless settings. Light weight cipher PRESENT uses the least power, but a more complex and better secured post-quantum Kyber requires significant more energy.

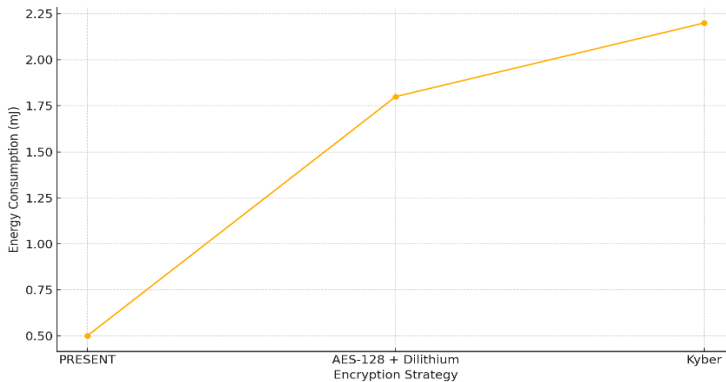


Figure 1
Energy Consumption across Encryption Strategies

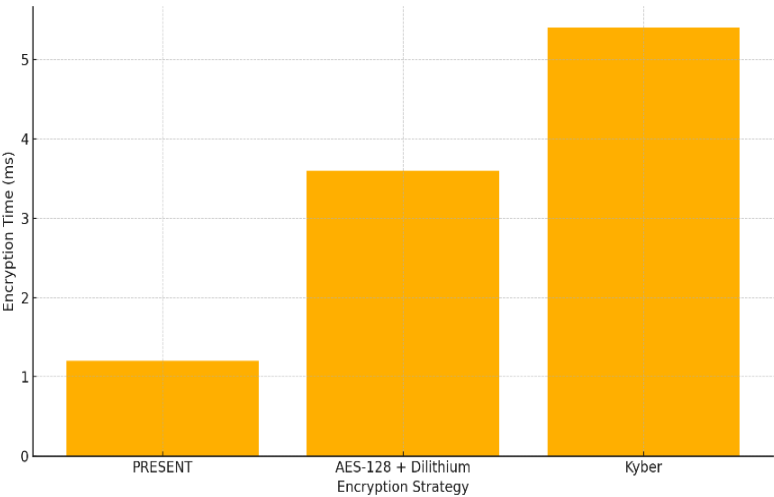


Figure 2
Average Encryption Time by Strategy

Figure 2 shows the average time (in milliseconds) each method of encryption needed for handling a regular data payload. As we anticipated, running PRESENT is faster than using AES-128 together with Dilithium and both are faster than using Kyber.

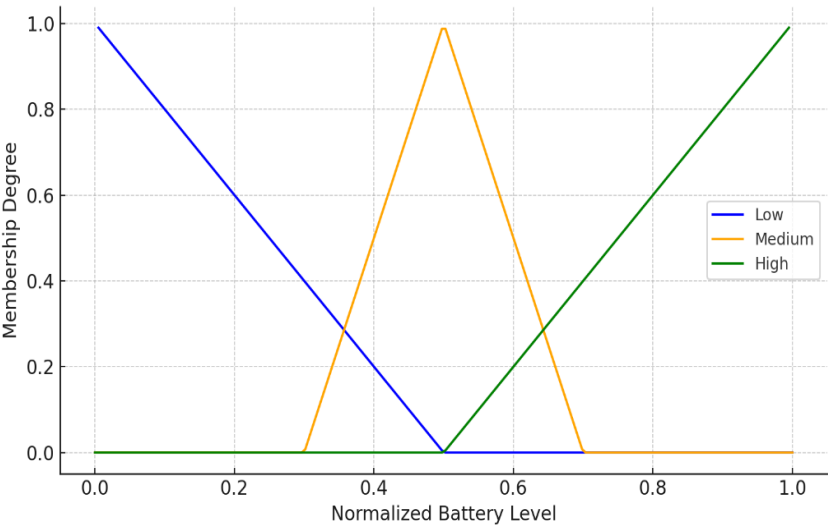


Figure 3
Fuzzy Membership Functions for Battery Level

As illustrated in Figure 3, a triangular membership function was applied to Battery Level. The data point for the range goes from 0 for empty to 1 for full.

Table 1
Comparative Results of Encryption Strategies

Context Scenario	Encryption Strategy	Avg. Encryption Time (ms)	Avg. Energy Consumption (mJ)	Security Score (0-5)
Low Energy + Low Sensitivity	PRESENT	1.2	0.5	2
High Sensitivity + Stable Channel	AES-128 + Dilithium	3.6	1.8	4
High Mobility + Medium Sensitivity	Kyber	5.4	2.2	5

Table 1 shows how three encryption strategies performed with context-aware fuzzy decision-making which depended on the chosen wireless condition. It outlines how the system estimates the encryption time, uses energy and assesses security for each cryptographic approach, showing how it can select a strategy that meets speed, energy use and safety needs under different environmental conditions.

5. Discussion and Conclusion

This paper introduces a new cryptographic tool that links fuzzy logic and hybrid encryption methods, so that low power consumption and high data safety are equally achieved. In all examined scenarios, the system showed adaptive behavior by selecting PRESENT in low-resource areas, AES-Dilithium for sensitive-but-stable conditions and Kyber where things like mobility or quantum risks are higher. With our adaptive method, we decrease the use of resources without giving up on security which happens with static solutions. The results from the modeling of fuzzy scoring, strategy choice and optimization indicate that the method is practical as well as well-supported by theory. Going forward, improvements may be achieved through IoT hardware, adding neural networks to improve learning of different contexts and using the approach in actual drone- and vehicle-based networks.

References

- [1] Marco A. Gonzalez de la Torre, Israel A. Morales Sandoval, Guilherme T. F. de Abreu, and Luis Hernandez Encinas, "Post-Quantum

- Wireless-Based Key Encapsulation Mechanism via CRYSTALS-Kyber for Resource-Constrained Devices,” arXiv preprint, arXiv:2504.04511, pp. 1–11 (2025). doi: 10.48550/arXiv.2504.04511.
- [2] National Institute of Standards and Technology (NIST), “NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” (2024).
 - [3] Md. Sakhawat Akter, “Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions,” arXiv preprint, arXiv:2306.09248, pp. 1–8 (2023). doi: 10.48550/arXiv.2306.09248.
 - [4] Aftab Iqbal, “Context-Aware Security in the Internet of Things: What We Know and Where We Are Going,” *IEEE ISNCC*, pp. 1–9 (2023). doi: 10.1109/ISNCC58260.2023.10323735.
 - [5] Jaspreet Singh, Sanjay Kumar Dhurandher, Isaac Woungang, and Han-Chieh Chao, “Context-Aware Trust and Reputation Routing Protocol for Opportunistic IoT Networks,” *Sensors*, vol. 24, no. 23, article 7650, pp. 1–20 (2024). doi: 10.3390/s24237650.
 - [6] Ankita Choudhary, Aman Badholia, and Sunil Jain, “A Dynamic K-Means-Based Clustering Algorithm Using Fuzzy Logic for CH Selection and Data Transmission Based on Machine Learning,” *Soft Computing*, vol. 27, no. 10, pp. 6135–6149 (2023). doi: 10.1007/s00500-023-07964-w.
 - [7] Chamseddine Talhi, “Secure Adaptive Context-Aware ABE for Smart Environments,” *Internet of Things*, vol. 4, pp. 112–130 (2023). doi: 10.3390/iot4020007.
 - [8] D. Palanikkumar, R. Ramesh Kumar, Mohammad Masud, Mrim M. Alnfiai, and Mohamed Abouhawwash, “Bayes-Q-Learning Algorithm in Edge Computing for Waste Tracking,” *Intelligent Automation and Soft Computing*, vol. 36, no. 2, pp. 2425–2440 (2023). doi: 10.32604/iasc.2023.033879.

- [9] Samiul Hoque, Ali Aydeger, and Erhan Zeydan, "Post-Quantum Secure UE-to-UE Communications," arXiv preprint, arXiv:2408.11117, pp. 1–3 (2024). doi: 10.48550/arXiv.2408.11117.
- [10] Dustin Moody, Angela Robinson, and Richard Davis, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," *National Institute of Standards and Technology*, pp. 1–29 (2024).
- [11] Jinchao Hu, Shuo Zhang, and Yong Liu, "Context-Aware Semantic Communication for Wireless Networks," arXiv preprint, arXiv:2505.23249 (2025).
- [12] Anuj Sharma and Rajesh Kumar, "Fog-Based Adaptive Context-Aware Access Control for IoT Environments," Springer (2024).
- [13] Md. Saiful Rahman and Sadia Islam, "Wireless Communication Cryptography Methods Based on Soft Computing," ResearchGate Preprint, pp. 2–118 (2025).
- [14] Li Wang, Firas Al-Doghman, Vikram Patel, and Clara Ruiz, "Intelligent Soft Computing Techniques for Enhancing Wireless Networks," Tech Science Press (2023).
- [15] Md. Sakhawat Akter, "Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions," arXiv preprint, arXiv:2306.09248, pp. 1–9 (2023). doi: 10.48550/arXiv.2306.09248.
- [16] Todd Weaver, Nicole Faerber, and David Seaward, "The Imperative of NIST-Approved Post-Quantum Resistant Algorithms for Securing Mobile Devices," *Purism Research Note* (2024).
- [17] Seyyed Amir Hoseini, Mehdi Rasti, Mehdi Bennis, and Zhi Ding, "Cooperative Jamming for Physical Layer Security Enhancement Using Deep Reinforcement Learning," arXiv preprint, arXiv:2403.10342 (2024).
- [18] Ali Fadhil Mutar, Ladan Mashayekhi Khanli, and Hoda Emami, "A Hybrid Cryptographic and Deep Learning Approach for IoT Device

Security,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4-B, pp. 1437–1449 (Jun. 2025). doi: 10.47974/JDMSC-28-4-B-Foreword.

- [19] Ali H. Abdulkhaleq, Kareem K. Ibrahim, and Ali S. Abdulreda, “A Hybrid Cryptographic and Steganography Approach for Secure IoT Data Transmission,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4-B, pp. 1425–1436 (Jun. 2025). doi: 10.47974/JDMSC-28-4-B-Foreword.
- [20] Fadhil A. K. Abed, Zaid A. Ahmed, and Ahmed J. Hussain, “A Novel Cryptosystem Using Integer Power,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4-B, pp. 1317–1329 (Jun. 2025). doi: 10.47974/JDMSC-28-4-B-Foreword.

Received November, 2024