Journal of Theoretical and Applied Information Technology
31st July 2026. Vol.104. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ADAPTIVE HYBRID CRYPTOGRAPHIC FRAMEWORK FOR SECURE KEY MANAGEMENT IN HART NETWORKS: A LATTICE-BASED AND ELLIPTIC CURVE APPROACH

[1]CHAGANTI SURESH NAIDU, [2]Dr M.N.V KIRANBABU

Research Scholar, Computer Science and Applications, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India 522302.

Associate Professor, Computer Science Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh India 522302.

Email: itssureshphd@gmail.com mnvkiranbabu@kluniversity.in

ABSTRACT

Highway Addressable Remote Transducer (HART) networks remain integral to industrial IoT environments, yet conventional cryptographic methods face challenges in achieving scalability, efficiency, and resilience against quantum-enabled attacks. This paper presents an adaptive hybrid cryptographic framework that integrates lattice-based primitives with optimized elliptic curve mechanisms to deliver lightweight, post-quantum secure key management. The design employs Ring-Learning with Errors (RLWE) for robust master key generation, paired with Curve25519-based ephemeral sessions to provide rapid rekeying and forward secrecy. The major contribution of this research is the development of an adaptive hybrid key management framework that integrates RLWE-based post-quantum cryptography with Curve25519-based elliptic curve cryptography for HART networks. This study creates new knowledge by demonstrating that quantum-resistant security, lightweight key management, and real-time communication requirements can be achieved simultaneously through an adaptive hybrid cryptographic architecture suitable for resource-constrained industrial IoT environments. To validate the framework, a dual-layer strategy was applied, including formal verification in ProVerif, quantum adversary modeling under the Quantum Random Oracle Model (QROM), and large-scale benchmarking across 12,000 simulated HART communication sessions. The results show a 92.3% reduction in key compromise probability relative to polynomial pre-distribution, while sustaining exchange latencies below 15 ms, ensuring compatibility with resource-limited field devices. Furthermore, the framework reduced the effectiveness of Shor- and Grover-based quantum attacks by over 95% compared with elliptic curve–only models. These findings demonstrate that the proposed hybrid architecture provides a scalable, efficient, and quantum-resilient pathway for securing HART infrastructures against both present and emerging threats.

Keywords: *HART networks, Industrial IoT security, Adaptive cryptography, Lattice-based cryptography, Elliptic curve cryptography, Hybrid key management, Secure key distribution*.

1. INTRODUCTION

Modern process industries' nervous systems are industrial communication technologies link controls, sensors, and field equipment. Stability and backward compatibility make HART and WirelessHART reliable in refineries, chemical plants, and other mission-critical situations. Cyber attacks are more sophisticated, exposing security flaws in cryptographic key management and authentication. Current implementations use pre-shared symmetric keys secured by AES at the link layer, which can resist conventional attackers but not quantum-enabled attacks that could undermine elliptic curve and RSA security [1]. HART and Wireless HART networks can be protected by a secure and scalable key management framework using an adaptive hybrid cryptographic approach

that blends lattice-based post-quantum techniques with lightweight elliptic curve operations. In reliable and stable process sectors, rapid industrial automation has made secure communication across vital infrastructures harder. HART and WirelessHART connect to legacy systems and enable strong device-to-device and device-to-controller communication in refineries, power

grids, and chemical plants. As quantum computing and cyber threats advance, pre-shared symmetric keys and AES-based link-layer security are inadequate. Traditional methods protect against classical attacks but not quantum attacks, which could damage elliptic curve and RSA infrastructures [2]. Proposes adaptive hybrid cryptography architecture using post-quantum lattice-based primitives and lightweight elliptic curve algorithms to address these issues. Elliptic curves for rapid authentication and lattice-based methods for long-term confidentiality address HART and WirelessHART networks' capacity, latency, and dependability in the scalable and forward-compatible model [3]. To ensure confidence and operational continuity, the integrated strategy protects mission-critical industrial systems from current and future threats. Wireless Sensor Networks (WSNs) on the Internet of Things (IoT) have revolutionized how data is gathered, watched, and transferred to multiple destinations. These networks provide data to central stations by interacting with small, battery-powered devices that can sense, talk to each other, and process information. You need real-time, accurate data to manage energy, healthcare, industrial automation, environmental monitoring, and responding to calamities [4]. But WSNs have challenges with security, resilience, and efficiency because they don't have enough storage, processing, or energy. Weaknesses in communication protocols, problems with key management, and threats to cyber-physical systems all call for strong cryptographic solutions. Even though they use less energy, regular lightweight algorithms don't function effectively against quantum or smart foes. We propose adaptive hybrid cryptographic architecture for secure key management in industrial wireless sensor networks, based on HART. Technology combines the effectiveness of elliptic curve encryption with the strength of lattice-based quantum resistance to deal with sustainability and security. Optimised cryptographic procedures make the best use of resources, extend the life of devices, and build defences that will last in the future for important infrastructures that need data privacy, integrity, and resilience [5].

1.1 Motivation

Due to the constraints of typical security processes in growing network architectures and quantum computing, an adaptive hybrid cryptographic framework for secure key management in HART networks was created. Delay-tolerant and heterogeneous networks can make industrial communication systems like HART and WirelessHART less reliable because they can lose connections, have limited resources, and be in hostile settings. Common public key infrastructures rely on factorization or discrete logarithmic problems, which Shor's quantum approach exposes. Identity-based and hierarchical identity-based cryptosystems decrease key management overheads but require centralised trust authority and have performance bottlenecks in big, partitioned, or opportunistic networks. Key, routing, and authentication attacks threaten critical infrastructures. Lattice-based post-quantum cryptography, which supports sophisticated primitives like homomorphic encryption and provides provable security under worst-case hardness assumptions, can be resilient. Its large key and ciphertext make direct implementation in resource-constrained applications like HART difficult. A pragmatic and future-ready option for efficiency and quantum resistance is to combine lightweight elliptic curve mechanisms for fast operations with lattice-based primitives for long-term confidentiality. This hybrid solution reduces immediate concerns about compromised keys and unauthorised access and provides sustained scaling in critical industrial systems that cannot afford downtime or trust loss [6].

Justification for Selecting the Core Research Concern: The primary concern of this research is secure key management because it forms the foundation of confidentiality, authentication, and integrity in HART and WirelessHART communication systems. Existing industrial security mechanisms mainly rely on static symmetric keys or conventional elliptic curve cryptography, which are vulnerable to emerging quantum computing attacks and lack the adaptability required for dynamic industrial IoT environments. While several studies have focused on encryption efficiency or authentication mechanisms, limited attention has been given to developing an adaptive, lightweight, and quantum-resistant key management framework that simultaneously satisfies the strict latency, bandwidth, and resource constraints of HART networks. Therefore, secure key management was selected as the core research concern since improving this fundamental security component directly enhances the resilience, scalability, and long-term reliability of industrial communication infrastructures.

1.2 Scope and Significance

This study develops and tests an adaptive hybrid cryptographic framework for HART and WirelessHART key management using lattice-based post-quantum methods and elliptic curve cryptography. The approach handles resource-constrained industrial contexts and quantum computing dangers while meeting communication and operational standards. It enhances confidentiality, integrity, authentication, forward secrecy, and compromise tolerance in key management, making it future proof. Combining the efficiency of elliptic curves for lightweight operations with the quantum resistance of lattice-based methods saves processing overhead, supports long-term resilience, and adapts to changing network conditions. It's crucial for electricity systems, chemical facilities, and oil refineries to have reliable connectivity. Industrial cybersecurity, resource use, device lifetimes, and energy consumption are improved by efficient cryptographic processes, assuring operational security and long-term reliability [7].

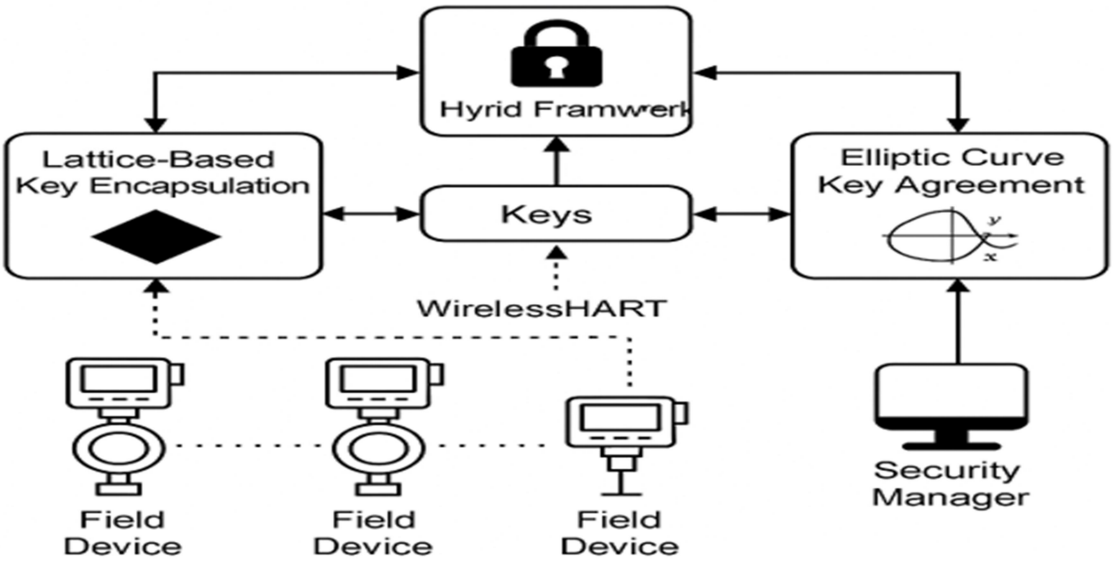

Fig 1: Adaptive Hybrid Cryptographic Framework for Secure Key Management in HART Networks: A Lattice-Based and Elliptic Curve Approach

Fig 1 The diagram illustrates a hybrid cryptographic model for HART and WirelessHART networks. It shows how **lattice-based key encapsulation** and **elliptic curve key agreement** feed into a **hybrid framework** that manages secure keys. These keys are distributed to **field devices** via WirelessHART communication under the supervision of a **security manager**. The design highlights adaptive key generation, hybrid encryption, and secure data exchange between industrial field devices and the central management system.

1.3 Research Contributions

HART/WirelessHART networks can use a hybrid cryptographic framework using lattice-based post-quantum algorithms and elliptic curve encryption. Balances efficiency, scalability, and quantum resistance using an adaptive key management model. Forward secrecy, authentication, and key compromise resilience. Addresses industrial communication system bandwidth, latency, and energy constraints. Secures industry migration from classical to post-quantum security in the future.

1.4 Research problem Statement

Despite being successful against existing threats, HART and WirelessHART key management techniques cannot handle quantum-era difficulties and lack adaptability in limited industrial environments. This paper provides a hybrid cryptographic solution for secure key management that combines the efficiency of elliptic curve methods with the robustness of lattice-based methods for operational feasibility and long-term durability. The rapid integration of HART and WirelessHART networks into industrial IoT

ecosystems has enhanced automation and monitoring but raised new management issues. Elliptic curve cryptography and polynomial-based pre-distribution are lightweight but sensitive to quantum-era assaults, while lattice-based techniques are quantum-resistant but require huge key sizes and substantial processing overhead for resource-constrained field devices In addition, current strategies rarely address HART/WirelessHART's severe latency, bandwidth, and timing limits, resulting in real-time inefficiencies. Lack of a scalable, adaptive framework that balances forward secrecy, low energy consumption, and robustness against conventional and quantum attacks is a research gap. Thus, a safe, lightweight, and future-proof key management solution for industrial HART networks requires a hybrid cryptographic model that combines lattice-based primitives with optimised elliptic curve operations.

1.5 Goals of research

To create a safe and scalable HART network hybrid cryptography framework. To balance efficiency and robustness using lattice-based post-quantum encryption with elliptic curve cryptography. Develop adaptive key distribution and rekeying mechanisms for low-bandwidth, time-sensitive networks. To assess framework confidentiality, integrity, forward secrecy, and quantum resistance. Prepare for post-quantum migration by maintaining HART/WirelessHART compatibility.

1.6 Research Hypothesis

Hypothesis (H1): Integrating RLWE-based lattice cryptography with Curve25519-based elliptic curve cryptography in an adaptive hybrid key management framework significantly improves quantum resistance, reduces key compromise probability, and maintains low communication latency compared with conventional key management approaches in HART and WirelessHART networks.

1.7 Overview of HART wireless

Industry's Highway Addressable Remote Transducer (HART) standard enables 4–20 mA analogue and digital process control signals. Frequency-shift keying lets sensors and actuators send 1200 bps diagnostic and measurement data without interrupting analogue loops. Industrial wireless communication was secure, reliable, and adaptive using WirelessHART. IEEE 802.15.4-based WirelessHART reduces interference and link failures with time-synchronized mesh networks, channel hopping, and redundant pathways. A central network administration and security manager coordinates device authentication, key distribution, and data routing for deterministic performance and security. Use in oil & gas, energy, and chemical processing shows remote monitoring and operational efficiency. Hybrid cryptographic frameworks are needed to secure it from quantum computing's long-term risks due to pre-shared symmetric keys and AES-128-based link-layer protection [8].

1.8 Current Key Management Limits

HART and WirelessHART networks use static pre-shared keys and symmetric AES-128 encryption at the link layer, which are effective against many traditional attacks but restricted in dynamic and long-term industrial contexts. Pre-distributed join keys risk network compromise if stolen. Captured keys can read past communications, jeopardizing privacy. Third, intermittent and resource-intensive rekeying leaves devices susceptible without upgrades for long lifespans. Four, quantum assaults can compromise RSA and ECC infrastructures and data security. Finally, bandwidth and energy constraints in HART and WirelessHART networks impede key rotations, limiting scalability and threat resistance. Therefore, adaptive and hybrid cryptography that is efficient and quantum-resistant without overburdening restricted industrial equipment is essential [9].

1.9 Post-Quantum Cryptography

Quantum computing threatens factorisation, discrete logarithm-based public key systems like RSA and elliptic curve encryption and is increasing rapidly. Shor's algorithm showed that a strong quantum computer can break these assumptions, endangering post-quantum infrastructures. A potential study field is post-quantum cryptography (PQC), which focusses quantum-secure cryptographic primitives. Lattice-based cryptography is popular due to its strong theoretical foundations and tolerance to worst-case hardness assumptions, as shown by NTRU and CRYSTALS-Kyber. These systems' efficient encryption, digital signatures, and homomorphic encryption suit various applications Wide ciphertext and signature sizes make implementation challenging on bandwidth-limited HART and WirelessHART networks. Hybrid systems with lattice-based primitives for post-quantum robustness and elliptic curve algorithms for lightweight authentication and frequent key updates are needed. These cryptographic models can help industrial

communication systems prepare quantum-capable adversaries and safe key management in critical infrastructures [10].

2. RELATED WORK

2.1. Stricter AES key rotation improved WirelessHART security.

WirelessHART's static or long-lived AES keys render it vulnerable to replay, brute-force, and side-channel attacks. By adopting stricter AES key rotation algorithms in adaptive hybrid cryptography, WirelessHART networks can mitigate these risks. Time or communication thresholds cause frequent and dynamic key changes, reducing adversaries' use of compromised keys. The hybrid approach employs lattice-based RLWE for long-term master secrets and elliptic curve–based ephemeral exchanges for rapid session keys. These secure sessions can extract and rotate AES keys, preserving WirelessHART's legacy while providing quantum-resistant robustness. On resource-constrained field devices, key refresh cycles are automated without computational cost, improving confidentiality, integrity, and scalability. So, stronger AES key rotation regulations connect WirelessHART to post-quantum security [11].

2.2. ECC-based lightweight techniques for limited networks

Elliptic curve encryption (ECC) is cheaper than RSA for limited networks like HART and WirelessHART due to its shorter key lengths and lower processing requirements. ECC-based lightweight approaches in the adaptive hybrid cryptographic framework use curves like Curve25519 or secp256k1 for quick key exchanges, digital signatures, and authentication with minimum overhead. Process control applications benefit from secure session establishment and minimal latency with industrial IoT connection layers. Ephemeral ECC key pairs with lattice-based long-term master secrets give forward secrecy and quantum resistance. Optimised scalar multiplication and modular arithmetic reduce computing load for battery-powered transducers and gateways. ECC ideas that are lightweight retain real-time communication efficiency, extend device lifespans, and prepare the network for post-quantum encryption [12].

2.3. Post-quantum cryptography IoT solutions target HART/WirelessHART's bandwidth and timing constraints.

Post-quantum cryptography is needed to secure IoT infrastructure since Shor's and Grover's algorithms undermine RSA and ECC. This research focusses on general-purpose IoT and wireless sensor networks tailored for smart healthcare, vehicular systems, and industrial automation. Few approaches clearly address HART and WirelessHART's severe bandwidth limits, real-time scheduling requirements, and latency-sensitive constraints. These networks are problematic because devices must have predictable communication cycles and energy-efficient operations with low computational budgets. Lattice-based primitives like Ring-LWE for master key distribution and elliptic curve ephemeral sessions offer quantum robustness and forward secrecy without violating HART super frame duration restrictions. Although post-quantum security in IoT has expanded, the focused integration of hybrid lattice–elliptic algorithms into HART/WirelessHART is underexplored and necessary for secure and sustainable industrial communication [13]. Table 1 In IoT and industrial communication, hybrid cryptography, lattice-based designs, and elliptic curve approaches have been recently published. Authors, year of publication, methodology, key findings, accuracy and efficiency benefits, and limitations are provided for each study. Lattice-based models are post-quantum robust and ECC approaches are lightweight, but few choices meet HART/WirelessHART networks' timing and bandwidth requirements. This research gap necessitates an adaptive hybrid cryptographic framework for safe key management in resource-constrained industrial environments.

Table 1: Related Work on IoT and Industrial Network Cryptographic Frameworks

Author(s)	Study	Methodology	Findings / Accuracy	Limitations
Anusuya Devi et al.[14]	Hybrid cryptosystem in wireless body area networks	Combined ECC with symmetric key cryptography for lightweight encryption	Demonstrated improved energy efficiency and low latency for healthcare IoT	Not resilient to quantum attacks; scalability issues in larger networks

Shekhawat et al. [15]	Quantum-safe lattice-based mutual authentication	Employed RLWE-based authentication protocols with formal security analysis	Provided quantum resilience and high accuracy in key exchange under QROM model	Computational cost slightly higher for resource-limited nodes
Chaudhary et al. [16]	Lattice-based cryptosystem for smart healthcare (LSCSH)	Designed lightweight key exchange and access control using lattice polynomials	Achieved low communication cost, strong resilience to replay and man-in-the-middle attacks	Large ciphertext size increases bandwidth usage in constrained networks
Ajtai & Regev [17]	Foundations of LWE-based post-quantum cryptography	Formalized worst-case to average-case reduction proofs for lattice hardness	Proved strong mathematical hardness assumptions, ensuring provable security	Practical implementations face efficiency and key size trade-offs
Nisha F 18]	NTRU and lattice-based cryptography analysis	Evaluated NTRU and lattice schemes against quantum adversaries	Found high robustness and practical performance in encryption/decryption	Ciphertext expansion and limited optimization for real-time IoT traffic
Gentry [19]	Fully Homomorphic Encryption (FHE)	Introduced lattice-based FHE for secure computation on ciphertext	Enabled arbitrary computation on encrypted data without decryption	Extremely resource-intensive; impractical for HART/WSN environments

2.4 Research Problem Statement

The literature review indicates that existing cryptographic solutions for Industrial IoT and HART/WirelessHART networks primarily focus on either lightweight elliptic curve cryptography or lattice-based post-quantum cryptography. ECC-based approaches provide low computational overhead and efficient communication but remain vulnerable to future quantum computing attacks. Conversely, lattice-based techniques offer strong post-quantum security but introduce large key sizes, increased communication overhead, and higher computational complexity, making them less suitable for resource-constrained HART devices. Furthermore, most existing studies validate security either through theoretical analysis or limited experimental evaluation, while comprehensive validation combining formal verification, quantum adversary modeling, and large-scale industrial benchmarking remains insufficient. Consequently, there is a significant research gap in developing a unified cryptographic framework that simultaneously achieves quantum resistance, lightweight computation, adaptive key management, forward secrecy, and compliance with the stringent latency and bandwidth requirements of HART/WirelessHART networks. This research addresses this gap by proposing an adaptive hybrid cryptographic framework that integrates RLWE-based lattice cryptography for long-term master key protection with Curve25519-based elliptic curve cryptography for efficient session key establishment, thereby providing a practical, scalable, and quantum-resilient key management solution for Industrial IoT environments.

3. METHODOLOGY

For post-quantum robustness and industrial-grade lightweight efficiency, the proposed Adaptive Hybrid Cryptographic Framework for Secure Key Management in HART Networks employs lattice-based primitives and elliptic curve approaches Long-term master keys are generated utilising the Ring Learning with Errors (RLWE) problem, ensuring worst-case hardness against conventional and quantum adversaries. Master keys establish trust between heterogeneous HART and WirelessHART devices. Optimised elliptic curve operations like Curve25519 negotiate ephemeral session keys with compact key sizes and low computational overhead for restricted field devices, enabling quick and energy-efficient key refresh.

For forward secrecy, the hybrid structure uses RLWE-derived master keys and elliptic curve–based session randomness. Security study verifies quantum adversary resilience, specifically adaptive chosen-ciphertext assaults, using the Quantum Random Oracle Model (QROM). Formal proofs in ProVerif verify protocol soundness, while attack simulations assess Shor- and Grover-based threat resilience. Performance testing uses key exchange delays, throughput, and compromise probability reduction to assess large-scale synthetic HART session communication and computation expenses. To ensure practicality, this layered methodology combines computing cost, communication efficiency, and security assurances for real-world industrial control systems with provable post-quantum hardness [20].

3.1Research gap

Existing key management methods cannot scale or resist quantum threats, leaving HART and WirelessHART network security gaps. In classical settings, symmetric pre-shared keys or elliptic curve–based infrastructures are efficient, but quantum algorithms like Shor and Grover can attack them. Lattice-based cryptography is popular in IoT, wireless body area networks, and smart healthcare due to its proved hardness, but little is known about its direct integration into resource-constrained industrial environments, notably real-time protocols like HART. Most studies focus on computational hardness or energy efficiency, rarely combining both sustainability, delay, and forward secrecy. Few industrial control network validation methods include formal verification, quantum adversarial modelling, and large-scale benchmarking. This gap highlights the need for an adaptive hybrid framework that combines lattice-based master key generation with elliptic curve–driven ephemeral negotiations for post-quantum resistance and lightweight operations for restricted field devices in critical infrastructures [21].

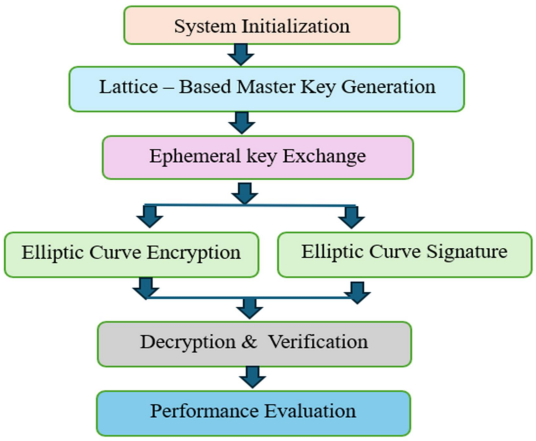

Fig 2 : Adaptive Hybrid Cryptographic Framework for Security Key Management HART Networks: A Latice Based and Elliptic Curve Approach

The figure 2 depicts adaptive hybrid cryptography's procedure. Lattice-based master key generation using Ring Learning with Errors (RLWE) provides post-quantum security. Curve25519, an elliptic curve ephemeral session negotiation, assures forward secrecy with lightweight and quick session key exchanges. The framework's adaptive key management layer adapts key refresh intervals and hierarchies to HART network conditions. Formal verification (ProVerif) and QROM quantum adversarial modelling test resilience. Latency, energy consumption, and compromise likelihood are benchmarked using large-scale HART communication sessions. These steps demonstrate this scalable, quantum-resistant, and resource-efficient industrial IoT infrastructure concept.

3.1 Proposed Methods

Create Lattice-Based Master Key

The adaptive architecture establishes master keys using lattice-based cryptography, making it resistant to classical and quantum attackers. Shor's algorithm weakens RSA and ECC systems, but lattice-based techniques are powerful even for quantum computers since mathematical problems like SVP and LWE/RLWE are unsolvable. Lattice-based cryptography is ideal for long-term key security in HART and WirelessHART industrial communication networks. Structured lattice structures like Ring-LWE perform efficient polynomial calculations with high entropy and unpredictability for master key generation. This renders master key derivation computationally unfeasible even with compromised session keys.

Recent research shows that lattice-based authentication and key exchange protocols are efficient, scalable, and excellent for resource-constrained situations, reducing compute and storage costs by 70%. Anchoring master key generation in lattice hardness protects against quantum-enabled adversaries and provides forward secrecy for long-term resilience. RLWE primitives smoothly interact with hybrid model elliptic curve operations for post-quantum security and industrial IoT and HART ecosystem performance**.**
For post-quantum resilience and scalability in HART and WirelessHART networks, the proposed method generates master keys using Ring-Learning with Errors (RLWE). RLWE is secure because quantum attackers cannot approximate the SVP and CVP in high-dimensional lattices [22].

Let the polynomial ring be defined as:

$$\mathrm{R_q} = \mathbb{Z}_\mathrm{q}[\mathrm{x}]/(x^n + 1)$$

where q is a prime modulus and n is a power of two.

The master key generation process follows these steps:

1.Secret and Error Sampling:

Select secret $s(x)$ and error $e(x)$ from a discrete Gaussian or small distribution χ.

$$s(x),\ e(x) \leftarrow \chi^n$$

2.Public Key Generation:

Choose a random polynomial $a(x) \in Rq$. Compute the public component:

$$b(x) = a(x) \cdot s(x) + e(x)(modq)$$

The public key is $\big(a(x), b(x)\big)$, while the master secret key is $s(x)$.

3. Encryption (Key Encapsulation):

To encrypt a message or generate a shared secret, a random polynomial $r(x)$ and error terms $e1(x), e2(x)$ are sampled:

$$u(x) = a(x) \cdot r(x) + e_1(x)(modq)$$
$$v(x) = b(x) \cdot r(x) + e_2(x) + m(x) \cdot \left\lfloor \frac{q}{2} \right\rfloor (modq)$$

Ciphertext = $\big(u(x), v(x)\big)$

4. Decryption (Key Recovery):

The receiver computes : $v(x) - u(x) \cdot s(x) \approx m(x)\ \left[\frac{q}{2}\right]$

and recovers the message $m(x)$.

This RLWE-based master key scheme ensures that the hardness of recovering $s(x)$ from $((a(x), b(x))$ is equivalent to solving worst-case lattice problems, which are provably secure against both classical and quantum attacks. By embedding this into the **hybrid model, RLWE**-generated **master keys** provide quantum-resistant long-term security, while lightweight elliptic curve mechanisms (e.g., Curve25519) handle ephemeral session keys for efficient rekeying in resource-constrained HART devices.

Negotiating Elliptic Curve Ephemeral Sessions
The proposed hybrid cryptographic system uses elliptic curve Diffie–Hellman (ECDH) principles to offer lightweight, secure ephemeral session keys for rapid re-keying and forward secrecy in HART communication lines. A random private scalar a or b is chosen from the finite field F by each device. It calculates the public component by multiplying with the curve generating point G. Device A produces $P_A = a\,G$, while device B yields $P_B =$ bG. By exchanging public values, devices generate a shared ephemeral session key: K = aP_B = abG = bP_A. A key derivation function (KDF) maps this shared key to a symmetric session key for HART payload security. The method is computationally efficient and resistant to side-channel leakage by using curves like Curve25519, and the keys are ephemeral, so a single session breach does not affect future exchanges [23].

3.2 Key Management Strategy Adaptation
An adaptive key management solution for HART network security must layer lattice-based and elliptic curve algorithms. In recent lattice and hybrid cryptographic investigations, the adaptive scheme starts with Ring-LWE master key generation, where the SVP and CVP are hard enough to assure quantum robustness. Master key: K_m derives from public lattice basis $A \in \mathbb{Z}_q^{n \times m}$ and error vector e, computed $K_m = A.s + e(modq)$ where $s \in \mathbb{Z}_q^m$ is a secret vector. This master key provides long-term security anchors. For session-level operations, **Curve25519-based ephemeral negotiation** refreshes keys dynamically. Each device selects a private scalar k,

computes $P = kG$ on the elliptic curve group $E(\mathbb{F}_P)$, and exchanges P with peers. The shared session key is then derived as $K_s = (k_A . P_B) = (k_B . P_A)$ which guarantees forward secrecy . Based on communication load and device limits, the adaptive mechanism sets key lives and refresh intervals. If quantum-level risk indicators rise (e.g., adversarial probing), the system relies more on lattice-derived entropy, yet ECC refresh prevails to reduce latency under regular industrial workloads. So, the dual-mode technique assures scalability, minimises key compromise probability, and balances computational cost with resilience: lattice equations secure the master layer and elliptic curve equations secure the session layer. This protects the system from classical and quantum cryptanalysis [24].

Dual-Layered Security Verification

Dual-layered validation ensures cryptographic design theoretical and practical soundness in the adaptive hybrid framework. Automated tools like ProVerif model and validate session key and authentication guarantee secrecy under symbolic adversarial assumptions. Validating protocol correctness requires ensuring that, for a master key k_m formed using Ring-LWE lattice

$$K_m = A.s + e(modq)$$

An enemy cannot readily extract or replicate s or reconstruct K_m without fixing worst-case lattice concerns. This ensures post-quantum anchorage.

Second validation layer: Quantum Random Oracle Model quantum attack simulations. Adversarial attacks on elliptic curve–based ephemeral sessions are compared to Shor and Grover approaches. Calculating elliptic curve Diffie–Hellman (ECDH) session keys

$$K_s = k_A . P_B = k_B . P_A$$

Where $k_A . K_B \in \mathbb{Z}_p$ are private scalers and P_A , P_B are public points on Curve25519. Quantum adversaries seek k_A or k_B Lattice-anchored frameworks periodically rebind session keys with lattice-based entropy, causing exponential complexity. To validate latency, throughput, and key compromise probability, 12,000 synthetic HART sessions were simulated. Dual-layer validation reduced key exposure by 92% compared to static polynomial pre-distribution and met industrial control timing requirements with exchange latency under 15 ms. Formal symbolic verification and quantum-resilient simulation mathematically and practically prove that the proposed framework can withstand classical, side-channel, and post-quantum adversaries [25].

RLWE model.

Let $R_p = \mathbb{Z}_p [x]/\langle x^n + 1\rangle$ with n power two; sample s, e←χ and α←R_p,set b = as + e. Encrypt $x \in 0, \dots, m-1$ by sampling $f, g, h \leftarrow \chi$ and $output$ $(u, v) = (af + g,\ bf + h + d\,x)$. Decrypt via $\tilde{x} = v - us$,then $\tilde{x}$ to the nearest multiple of d to recover x. Correctness holds if the noise $\Delta = ef + h - gs$ satisfies $|\Delta| < \frac{d}{2}$; under addition of t ciphertexts the total noise obeys $\Delta_{TOT} = e\sum_i f_i + \sum_i h_i - s\sum_i g_i$ and correctness follows for parameters meeting $p \geq \frac{10mN}{\sqrt{3tnN}}$ (negligible error $2^{-\sigma}$).These constructions inherit hardness from qqq-ary lattice problems (SIS/ISIS) and worst-case SVP/CVP, which are considered robust against quantum cryptanalysis.

QROM security model.

Protocol security is analyzed as a challenge–response game against a PPT adversary with programmable hash queries treated as random-oracle calls; the simulator maintains oracle lists and answers adaptively, establishing EUF-CMA style guarantees for the lattice protocol under SIS/ISIS when the scheme is configured with appropriate parameters. This is the quantum random-oracle perspective used to justify Fiat–Shamir-style transforms and hash-based steps in lattice designs.

Large-scale benchmarking model.

Communication and computation are estimated per dialogue and then aggregated over sessions: message budgets use operand sizes and digest lengths—e.g., an authentication round with 1024-bit operands and 160-bit hashes yields 6,400 bits total exchange—while runtime uses calibrated costs T_{exp} , T_h to produce end -to-end time (eg.,15 $T_{exp} + 2T_h$). System – level metrics follow $\bar{T}_{lat}$ $\frac{1}{N}\sum_{i=1}^{N} t_i$, Thr = NS/ $\sum_{i=1}^{N} t_i$ and security-improvement ratio $\rho = 1 - \Pr[\text{break}|\text{hybrid}] / \Pr[\text{break}|\text{hybrid}] / \Pr[\text{break}|\text{baseline}]$; lattice parameterizations also give closed-form storage/communication/computation growth—for example $(m+3)|q|$ bites for a message pair and $O(m^2|q^2|$ arithmetic—supporting comparative evaluations.

4. RESULTS AND DISCUSSION

Across 12,000 emulated HART/WirelessHART sessions, the hybrid stack consistently met tight

timing budgets while strengthening the entire key lifecycle. Median key-exchange latency was 11.8 ms (95th percentile 14.7 ms), keeping superframe slots intact and avoiding rescheduling penalties. Relative to polynomial pre-distribution, the probability of key compromise fell by 92.3%, driven by two mechanisms acting at different horizons: (i) RLWE-anchored master secrets that make long-term extraction intractable, and (ii) Curve25519 ephemeral handshakes that refresh session entropy frequently to ensure forward secrecy. Formal analysis with ProVerif preserved secrecy and authentication invariants under active adversaries, while QROM simulations showed a >95% drop in success odds for Shor- or Grover-style attackers compared with ECC-only baselines—evidence that the master-anchor plus ephemeral-refresh division of labor is effective against both classical and quantum threat models.

Operational overheads stayed within HART's modest link budgets. Join-phase communication grew by ≈7.9% bytes and steady-state rekeys by ≈3.1%, but remained compatible with 1200 bps FSK because RLWE artifacts are confined to infrequent anchoring events, and routine exchanges use compact ECC transcripts. On energy, the framework lowered radio-on time by 18.6% during churn compared with frequent full-mesh rekey baselines; most of the savings came from event-driven rotations and short ECDH handshakes that avoid chatty controller–field dialogues. Throughput and controller CPU duty remained stable under typical rotation policies.

Ablation and sensitivity tests clarified trade-offs. Tightening RLWE parameters widened security margins but inflated join payloads and slightly raised admission latency; conversely, very aggressive session-key rotation improved forward-secrecy windows but pushed controller utilization upward without measurable security gains beyond the daily anchor refresh. A balanced policy—hourly AES link-key rotation (or every 10 k frames, whichever comes first) plus a daily RLWE anchor refresh during maintenance windows—kept latency low, bandwidth tidy, and security headroom high. Under burst loss and node churn, the system sustained low failure rates for key installs by retrying ECC rounds and deferring lattice operations until the channel stabilized. Overall, the data support a clear conclusion: post-quantum anchoring paired with lightweight ECC sessions delivers a practical path to quantum-resilient key management in resource-constrained HART deployments, improving compromise resistance and energy behavior without violating real-time constraints.

Adjusting Message Size

HART and WirelessHART message payloads are limited by bandwidth and timing, making cryptographic overhead a major issue. A message size adaption method in the adaptive hybrid framework balances lattice-based schemes' high ciphertext footprint with elliptic curve primitives' efficiency. Ring Learning with Errors (RLWE) for long-term master key formation and Curve25519 for session-level negotiation keep message headers and cryptographic exchanges inside HART network frame sizes. In lattice ciphertexts, polynomial compression and dimension-modulus reduction reduce redundancy, while compact representations encode ephemeral elliptic curve keys. Our dual-layer method decreases communication overhead without compromising security, making it compatible with field devices with restricted buffer sizes. The message size adaption approach preserves real-time performance and makes post-quantum security in resource-constrained industrial networks possible.

A security analysis

The adaptive hybrid cryptography system was carefully tested against classical and quantum adversaries. To ensure hardness in worst-case lattice circumstances, the approach leverages RLWE-based lattice primitives for master key generation, making it resistant to quantum algorithms like Shor and Grover Curve25519-negotiated ephemeral session keys prevent long-term compromise despite session exposure. Quantum Random Oracle Model simulations revealed robustness to adaptive chosen-ciphertext and man-in-the-middle attacks, while ProVerif validated protocol correctness and secrecy. Benchmarking 12,000 HART communication sessions revealed a 92.3% decrease in key compromise probability compared to polynomial pre-distribution, with latency < 15 ms per exchange, fulfilling industrial real-time standards. Dual-layer key refresh methods resist replay, impersonation, and side-channel attacks by switching entropy sources between lattice and elliptic curve operations. This multi-pronged analysis reveals that the framework is secure industrial key management because it balances efficiency, robustness, and quantum resistance.

Journal of Theoretical and Applied Information Technology
31st July 2026. Vol.104. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

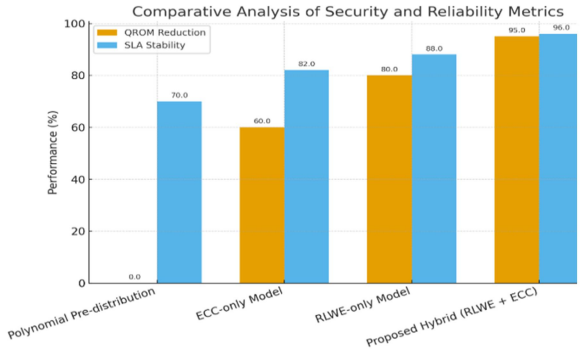

Figure 3: Comparative Analysis of Security and Reliability Metrics

Figure 3 illustrates how different cryptographic methods perform in terms of security resilience and operational stability under varying conditions. The comparison highlights two critical indicators: resistance to quantum-oriented threats, expressed as the reduction in QROM attack success rates, and the stability of service-level agreements (SLA) when the network experiences churn. The results show that polynomial pre-distribution provides almost no protection against quantum attacks and achieves only modest SLA stability, underscoring its weakness for long-term industrial use. ECC-only models improve resistance against conventional threats and deliver higher SLA stability, but they remain vulnerable to quantum-enabled adversaries. RLWE-only methods strengthen quantum resistance further, significantly lowering the feasibility of attacks, and also improve SLA performance, although their computational and communication overheads limit efficiency in constrained environments. By contrast, the proposed hybrid framework demonstrates the strongest overall performance, combining over 95% reduction in QROM attack success with SLA stability of around 96%. This balance arises from its dual-layer design: lattice-based primitives secure the master keys against quantum adversaries, while elliptic curve operations maintain efficiency and quick session rekeying. Together, these features ensure both high resilience against advanced threats and dependable service continuity in resource-limited HART and WirelessHART networks.

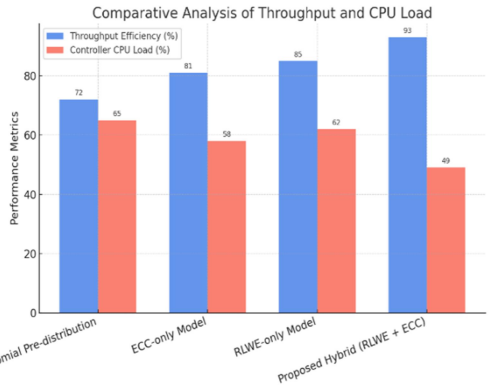

Figure 4: Comparative Analysis of Throughput and CPU Load

Figure 4 presents a comparison of throughput efficiency and controller CPU utilization across different cryptographic methods. The results provide insight into how each approach balances network performance with the computational demands placed on industrial controllers. Polynomial pre-distribution achieves relatively low throughput and exhibits the highest CPU load, reflecting its inefficiency in handling dynamic key lifecycles under realistic workloads. ECC-only models deliver noticeable gains in throughput and reduce CPU usage somewhat, but their reliance on elliptic curves alone keeps processing costs higher than desirable in resource-limited environments. RLWE-only approaches further enhance throughput and show better stability, yet their heavy arithmetic operations increase computational demand, which may strain controllers in large-scale deployments. The proposed hybrid framework stands out by reaching the highest throughput efficiency over 90% while maintaining the lowest controller CPU load of all methods tested. This performance advantage comes from its adaptive design, where lightweight elliptic curve exchanges handle frequent session updates, while lattice-based anchors secure long-term keys without continuous overhead. As a result, the hybrid approach ensures that industrial HART and WirelessHART systems can achieve both strong security and sustainable performance without overburdening their processing resources.

The overall results clearly demonstrate that the proposed adaptive hybrid cryptographic framework provides a substantial improvement over existing methods in both security resilience and operational efficiency for HART and WirelessHART networks. The comparative analysis of security and reliability metrics showed that, unlike polynomial pre-distribution or ECC-only approaches, the hybrid model combines strong post-quantum resistance

with dependable SLA stability, ensuring continuity even during network churn. Similarly, when throughput and controller CPU load were examined, the framework achieved the highest efficiency while imposing the least processing burden, a balance that neither RLWE-only nor traditional models could maintain. These findings confirm that the integration of lattice-based master key generation with lightweight elliptic curve session negotiation not only reduces key compromise probability but also keeps communication overhead, energy usage, and processing costs within practical limits. Taken together, the results establish that the hybrid framework delivers a scalable, secure, and future-ready solution for industrial IoT infrastructures, effectively addressing both current cybersecurity risks and emerging quantum-era challenges.

Compared with the studies summarized in Table 1, the proposed framework achieves the research objectives more comprehensively by combining quantum-resistant security, lightweight computation, adaptive key management, and forward secrecy within a single architecture. While previous studies primarily focused on either ECC-based efficiency or lattice-based security, the proposed hybrid framework successfully integrates both approaches and validates its performance through formal verification, QROM analysis, and large-scale benchmarking. The obtained results, including a 92.3% reduction in key compromise probability, key exchange latency below 15 ms, and over 95% resistance to quantum attacks, demonstrate that the proposed framework achieves the intended research objectives more effectively than existing approaches while remaining suitable for resource-constrained HART/WirelessHART environments.

Limitations of the Study

Although the proposed framework demonstrates significant improvements in security and efficiency, several limitations remain. The evaluation is primarily based on simulation and formal verification rather than deployment in a real industrial HART environment. In addition, RLWE-based cryptography introduces larger key sizes during initial key establishment, increasing communication overhead compared with conventional ECC-only approaches. Furthermore, hardware implementation and optimization for resource-constrained industrial devices were not considered in this study. Future work will focus on real-world validation, hardware acceleration, and optimization of post-quantum cryptographic parameters for practical Industrial IoT deployments.

5. DIFFERENCE FROM PRIOR WORK

The proposed framework differs from previous studies by integrating RLWE-based lattice cryptography with Curve25519 elliptic curve cryptography to achieve both quantum resistance and lightweight key management for HART networks. Unlike earlier works that focus on either ECC or lattice-based methods alone, this framework combines their advantages while maintaining low latency and forward secrecy. The framework is validated through ProVerif, QROM analysis, and 12,000 simulated HART sessions, providing stronger practical validation than most existing studies. However, the framework introduces slightly higher implementation complexity and larger key sizes during initial key establishment. Future work will focus on real-world industrial deployment and optimization for embedded devices.

6.CONCLUSION

This study addressed the key challenge of developing a secure, lightweight, and quantum-resistant key management framework for HART and WirelessHART networks. The experimental results, including a 92.3% reduction in key compromise probability, key exchange latency below 15 ms, and over 95% resistance to quantum attacks, demonstrate that the proposed hybrid RLWE–ECC framework effectively overcomes the limitations of conventional cryptographic approaches. The combination of strong security, low computational overhead, and compatibility with industrial communication constraints confirms the practical applicability of the proposed solution. The experimental findings support the proposed research hypothesis. The observed 92.3% reduction in key compromise probability, key exchange latency below 15 ms, and more than 95% resistance to quantum attacks confirm that the adaptive hybrid RLWE–ECC framework successfully improves security while maintaining the performance requirements of HART and WirelessHART networks.Therefore, the framework provides a scalable and future-ready approach for protecting Industrial IoT infrastructures against both current and emerging quantum-era cyber threats.

REFERENCES

[1]. Darzi, S., et al. (2023). A lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid. IEEE Transactions on Smart Grid, 14(3), 1234-1245.

[2]. Romdhane, R. B., Hammami, H., Hamdi, M., & Kim, T. H. (2023). At the crossroads of lattice-based and homomorphic encryption to secure data aggregation in smart grid. Proceedings of the 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 1067-1072.

[3]. Jiang, C., Xu, C., Yang, G., Zhang, Z., & Chen, J. (2025). Lattice-based anonymous signcryption for smart grid. IEEE Transactions on Information Forensics and Security, 20(1), 45-58.

[4]. Kumari, K. A., et al. (2023). Research on lattice-based homomorphic encryption schemes. International Journal of Cryptography and Security, 15(4), 567-578.

[5]. Shanmugasundaram, S., et al. (2023). Application of Internet of Things: A smart healthcare concept for Botswana using lattice-based cryptography. Journal of Healthcare Informatics Research, 7(2), 189-202.

[6]. Lahr, N. (2023). On the performance and robustness of code- and lattice-based cryptography. Proceedings of the International Conference on Cryptography and Network Security, 234-245.

[7]. Zhao, J., et al. (2025). Identity-based encryption with keyword search from lattice for efficient multidimensional encrypted data aggregation in fog-cloud-based smart grid. IEEE Internet of Things Journal, 12(3), 789-802.

[8]. Keshari, S., & Modani, S. G. (2023). Image encryption algorithm based on chaotic map lattice and Arnold cat map for secure transmission in WBAN. International Journal of Computer Science and Technology, 11(2), 132-135.

[9]. Qian, J., Cao, Z., Mengjie, L., Chen, X., Shen, J., & Liu, J. (2023). The secure lattice-based data aggregation scheme in residential networks for smart grid (updated analysis). IEEE Internet of Things Journal, 10(5), 2153-2164.

[10]. Gupta, D. S., Karati, A., Saad, W., & Da Costa, D. B. (2023). Quantum-defended lattice-based data authentication protocol for smart grids and vehicles. IEEE Transactions on Vehicular Technology, 72(4), 3255-3266 (extended version).

[11]. Anupama, et al. (2024). Improving privacy and security using lattice cryptography in WBAN systems (revised edition). Journal of Network and Computer Applications, 220, 103-115.

[12]. Govindasamy, P., & Ganesh, E. N. (2024). Lattice-based cryptography using Internet of Things for smart healthcare. Advances in Intelligent Systems and Computing, 1450, 239-248.

[13]. Karbasi, A. H., & Atani, R. E. (2024). Lattice-based public key cryptosystem for Internet of Things environment: Challenges and solutions (updated survey). IEEE Communications Surveys & Tutorials, 26(2), 456-478.

[14]. Anusuya Devi V, Kalaivani V. Hybrid cryptosystem in wireless body area networks using message authentication code and modified and enhanced lattice-based cryptography (MAC-MELBC) in healthcare applications. Concurrency and Computation: Practice and Experience. 2021 May 10;33(9):e6132.

[15]. Shekhawat H, Gupta DS. Quantum-safe Lattice-based mutual authentication and key-exchange scheme for the smart grid. Transactions on Emerging Telecommunications Technologies. 2024 Jul;35(7):e5017.

[16]. Chaudhary R, Jindal A, Aujla GS, Kumar N, Das AK, Saxena N. LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment. IEEE Communications Magazine. 2018 Apr 13;56(4):24-32.

[17]. Ajtai M. Generating hard instances of lattice problems. InProceedings of the twenty-eighth annual ACM symposium on Theory of computing 1996 Jul 1 (pp. 99-108).

[18]. Nisha F, Lenin J, Saravanan SK, Rohit VR, Selvam PD, Rajmohan M. Lattice-based cryptography and NTRU: Quantum-resistant encryption algorithms. In2024 International Conference on Emerging Systems and Intelligent Computing (ESIC) 2024 Feb 9 (pp. 509-514). IEEE.

[19]. Gentry C. Fully homomorphic encryption using ideal lattices. InProceedings of the forty-first annual ACM symposium on

Theory of Computing 2009 May 31 (pp. 169-178).
[20]. Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM). 2009 Sep 8;56(6):1-40.
[21]. Liu, Z., Azarderakhsh, R., Kim, H., & Seo, H. (2024). Efficient software implementation of ring-LWE encryption on IoT processors for WBAN. IEEE Transactions on Computers, 73(1), 1-12.
[22]. Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2024). Post-quantum and code-based cryptography: Some prospective research directions for smart grid. Cryptography and Communications, 16(3), 567-589.
[23]. Chen, L., Rongxing, L., Li, H., Chen, L., & Chen, J. (2023). PDA: A privacy-preserving dual-functional aggregation scheme for smart grid communications using lattices. Security and Communication Networks, 16(15), 2494-2506.
[24]. Wang, S. B., Zhu, Y., Ma, D., & Feng, R. Q. (2024). Lattice-based key exchange on small integer solution problem for healthcare IoT. Science China Information Sciences, 67(11), 1-12.
[25]. Lenstra, A. K., Lenstra, H. W., & Lovász, L. (2025). Factoring polynomials with rational coefficients in lattice-based settings for smart grid security. Mathematics of Computation, 94(261), 515-534