STAP
Smart Technologies Academic Press

Jordanian Journal of Informatics and Computing
https://www.jjic.thestap.com/



E-QSafe Energy-Aware Quantum-Safe Encryption Scheme for Power-Controlled Internet of Nano Things

Mahmood A. Al-Shareeda[1*], May Adnan Faleh[2], Mohammed Amin Almaiah[3]

[1] *Department of Computer Engineering Technologies and Artificial Intelligence, Basrah Engineering Polytechnic College, Southern Technical University, 61001, Basra, Iraq*

[2] *Department of Electronic and Electrical Technologies, Basrah Engineering Polytechnic College, Southern Technical University, 61001, Basra, Iraq*

[3] *King Abdullah the II IT School, Department of Computer Science, The University of Jordan, 11942, Amman, Jordan*

ARTICLE INFO

Article History

Received: 02-06-2026
Revised: 29-06-2026
Accepted: 04-11-2026

Vol.2027, No.1

DOI:
https://doi.org/10.63180/jjic.thestap.2027.1.6

***Corresponding author.**

Email
mahmood.alshareedah@stu.edu.iq

Orcid:

This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

Published by STAP Publisher.

ABSTRACT

The Internet of Nano Things enables nanoscale devices to perform critical operations in healthcare, industry, and environmental monitoring. Nevertheless, ultra-small systems encounter tremendous challenges, including energy limitation, computation weakness, and exposure to quantum-era threats. No conventional cryptographic solution can maintain the effectiveness of both efficiency and post-quantum resilience under the above severe constraints. This paper designs E-QSafe, an Energy-Aware Quantum-Safe Encryption Scheme, to address the concern, which is featured by integrating an adaptive power control method with lattice-based Identity-Based Encryption. More specifically, the E-QSafe dynamically tunes the lattice dimensionality and Gaussian sampling variance based on the device's residual presenting ratio to secure the communication with minimal energy dissipation. The mathematical optimization model is developed to adjust the energy consumption, delay, and strength during the encryption at various power levels. Extensive experiments and analysis validate E-QSafe's security against quantum, replay, and side-channel attacks as well. The evaluation results show that the E-QSafe obtains a 35% reduction in total energy dissipation, reduces the communication cost by 30%, and enhances the throughput compared with conventional IoNT schemes. In short, E-QSafe effectively realizes quantum-resilient and energy-sustainable secure IoNT for nanonetwork computing in the next age.

Keywords: Internet of Nano Things (IoNT), Energy-aware encryption, Quantum-safe cryptography, Lattice-based cryptography, Identity-based encryption (IBE), Adaptive power control, Post-quantum security, Lightweight cryptographic protocol, Nano–micro interface device (NMID), Secure communication.

How to cite the article
Al-Shareeda, M. A., Faleh, M. A., & Almaiah, M. A. (2026). E-QSafe Energy-Aware Quantum-Safe Encryption Scheme for Power-Controlled Internet of Nano Things. Jordanian Journal of Informatics and Computing, 2027(1), 114. https://doi.org/10.63180/jjic.thestap.2027.1.6

1. Introduction

With the emergence of nano-devices, the Internet of Nano Things (IoNT) becomes a new concept that extends the conventional Internet of Things (IoT) to nanoscale environments (Chaudhary et al., 2022; Bahadur, 2024). IoNT can realize real-time sensing, communication, and data exchanging among nano-sensors, nano-routers, and nano-micro interface devices (NMIDs) used in biomedical monitoring, environmental surveillance, industrial automation as well as military applications(Gulec, 2022; Rana et al., 2024).

This offers huge potential IoNT but also poses serious threats to reliable, secure and energy-efficient communications due to resource limitations of the devices. In contrast to the traditional IoT nodes, nano-devices are essentially lack of processing power, memory and battery life (Hussain and Shaw, 2024). As a result, traditional cryptograpy primitives such as RSA or ECC cannot be utilized in nanoscale environment since they are infeasible in terms of computational and energy cost (Rana et al., 2025; Qiu et al., 2023; Ang et al., 2026; Alshabibi (2025).

Furthermore, the forthcoming quantum computing is an extra threat to classical cryptosystems security because of its efficient solutions to classic algorithms (for instance Shor's and Grover's) for breaking traditional public-key schemes (Peelam et al., 2024; Cherbal et al., 2024). As a result, the next generation IoNT architectures need to use post-quantum cryptography (PQC) to achieve long time data confidentiality and authentication even in quantum environment. Recently, there have been attempts to incorporate PQC primitives, lattices in particular, into IoNT architectures.

Among these, Prajapat et al. (Prajapat et al., 2024) introduced Quantum-Safe Lightweight Encryption Scheme for Secure Data Sharing in IoNT, implementing Learning With Errors (LWE) assumption to realize quantum resilience between NMID and gateway. Nevertheless, their ordinary, lifted voltage model corresponds to a strong post-quantum security and does not reflect that real-world basic building blocks have dissipation about the crypthographic designing parameters. These fixed-parameter models are not able to adapt, leading to performance degradation and fast energy drain if devices have variation in power availability or limited battery level during use. In nanoscale, energy consumption and computation costs of cryptographic operations are tightly coupled with the communication cost. If such operations are not well scheduled according to the remained energy, the system is subject to exhaustion-ofenergy attacks or sometimes they cause an early sleep of device that results network partition and data loss. Therefore, a more urgent protection demand that combines post-quantum security with energy adaptivity is required by an encryption scheme for IoNT.

To address the shortcomings, this letter proposes E-QSafe, an enerGy-Aware Quantum-Safe Encrpytion Scheme for Power-Controlled IoNT. E-QSafe for the first time combines lattice-based IBE with an adaptive power-control mechanism that opportunistically adapts the cryptographic parameters according to device instantaneous energy ratioη_E. As long as energy becomes less, the framework will automatically make lattice dimension N being scaled down and find a proper Gaussian sampling variance σ, so that post-quantum security can be guaranteed, with much less energy consumption. The primary contributions of this work can be summarized as follows:

- **Energy-Aware Quantum-Safe Framework:** We design an adaptive lattice-based IBE scheme that operates securely under varying power conditions, providing dynamic control over computational and communication complexity.
- **Adaptive Power-Control Mechanism (APCM):** A feedback-based control algorithm is proposed to monitor residual energy and regulate lattice parameters (N, σ) and encryption frequencyf_e, thereby preventing energy-depletion attacks.
- **Formal Security and Efficiency Analysis:**
  The proposed E-QSafe is formally proven secure under the LWE and SIS assumptions and validated against multiple attack models including replay, side-channel, and quantum adversaries.
- **Performance Optimization:** We develop an analytical energy-optimization model to minimize total energy $E_{\text{tot}} = E_{\text{comp}} + E_{\text{trans}} + E_{\text{idle}}$ under post-quantum security and latency constraints.
- **Comparative Evaluation:** Experimental results show that E-QSafe achieves up to 35% reduction in total energy consumption, 30% lower computation cost, and 36% improvement in throughput compared to the baseline IoNT encryption scheme (Prajapat et al., 2024).

The remainder of this paper is structured as follows: Section 1 reviews some recent works. Section 2 describes the system model and threat assumptions. Section 3 introduces mathematical preliminaries and lattice foundations. Section 4 presents the proposed E-QSafe framework and its adaptive power-control mechanism. Section 5 discusses the security analysis under LWE and SIS assumptions. Section 6 evaluates the performance and energy optimization results. Finally, Section 7 concludes the paper and outlines future research directions.

2. Related Work

In the last few years, the frame of Internet of Nano Things (IoNT) is put forward to enhance real-time sensing/actuation and data exchange at a nanoscale dimension for applications in healthcare, environmental monitoring and smart industry. However, the IoNT peculiarities (extreme miniaturization of devices, ultra-low available power, and nano–micro hybrid scale communication) make the conventional cryptographic schemes extremely challenging to apply. Secured communication, lightweight cryptography and Post Quantum Safe schemes relevant to the proposed work are discussed in this section.

Rana et al. (Rana et al., 2023) propose a full-fledged ECC-based authentication scheme for IoNT by fusing molecular and electromagnetic communications aspects. The abstract is well written and summarizes goals, methods and tools. But you could do better by emphasizing your motivation earlier, cutting introductory paragraphns some context, and covering performance with numbers for more academic impact. Sukhadeve et al. (Sukhadeve et al., 2025) suggested AI-empowered blockchain-based security architecture for IoNT with neuromorphic processing and hybrid THz-molecular communication. The abstract is informative and well-founded, successfully conveying novelty and results. Unfortunately it lacks explicit statement of both technical work and contributions, as well as a more clear problem statement. Galal et al. (Galal et al., 2022) introduced a NANO-SDN micro/nano-gateway architecture which makes it feasible for nano-networks and conventional Internet systems to interoperate. The abstract is clear, technical and supported with prototype validation. That is, the novelty and differences compared to existing SDN solutions could be more clearly explained, as well as how much latency, scalability, and throughput efficiency was actually gained.

Castiglione et al. (Castiglione et al., 2024) present a quantum-secure blockchain design for IoT, along with an efficient Dilithium-5 digital signature, which also includes optimization. The abstract states clearly the motivation, originality and practical validation of the work. It nicely bridges theory and application but would be more desirable if more explicit comparative performance results are reported, as well as some discussion on the scalability of the proposed approach. Mansoor et al. (Mansoor et al., 2024) investigate the implementation of post-quantum cryptography in TLS 1.3 in consumer health electronics through IoT for improved authentication. The abstract is consistent and topical, referring to existing security dangers. Nevertheless, the authors could enhance it by providing specific performance measures and explaining the range of the experiment for its further use as evidence of applicability and proximity to existing solutions. Choi et al. (Choi and Lee, 2024) propose the SSI-PQM platform with NTRU-based post-quantum cryptography for scalable and secure IoT communication. The abstract contains the motivation, methodology, and quantifiable results in an efficient manner. However, it can be improved by highlighting the novelty of architecture for SSI and defining the analogous benchmarks to promote the work in terms of a contribution to PQC-based IoT frameworks.

The most related paper to this work is Quantum-Safe Lightweight Encryption Scheme for Secure Data Sharing in IoNT by Prajapat (Prajapat et al., 2024). They used a slightly Identity-based encryption (IBE) way under the LWE assumption so that under this illusion, quantum-resilient confidentiality is ensured between the nano–micro interface device(NMID) and gateway node. Though the design did offer post-quantum security, it adopted fixed cryptographic parameters which ignored wearable devices dynamic power and computational state. Therefore, under low residual energy operation conditions the baseline approach has large energy consumption and enhanced delay.

3. System Model and Threat Assumptions

This section presents the general structure of the proposed E-QSafe framework in terms of participants, their roles that enable a secure quantum-assisted knowledge sharing for IoNT and adversarial model made. The problem is to propose a solution design in which the confidentiality, integrity and availability of power controlled nano-devices is not sacrificed while providing quantum resilient energy aware cryptography.

3.1 System Overview

The proposed E-QSafe scheme aims for data exchange security in IoNT, and the fusion of quantum-safe encryption and energy aware power control. It works in ranges of devices within IoNT hierarchical architecture called nano nodes, nano routers, Nano–Micro Interface Device (NMID), and an Internet gateway [9]. These have a nanoscale dimension; they offer tiny energy and computing resources; hence to ensure secure communication without compromising the operational life has become one of the key design objective of E-QSafe. Fig. 1 gives an overview of the E-QSafe framework, which includes three cooperating layers:

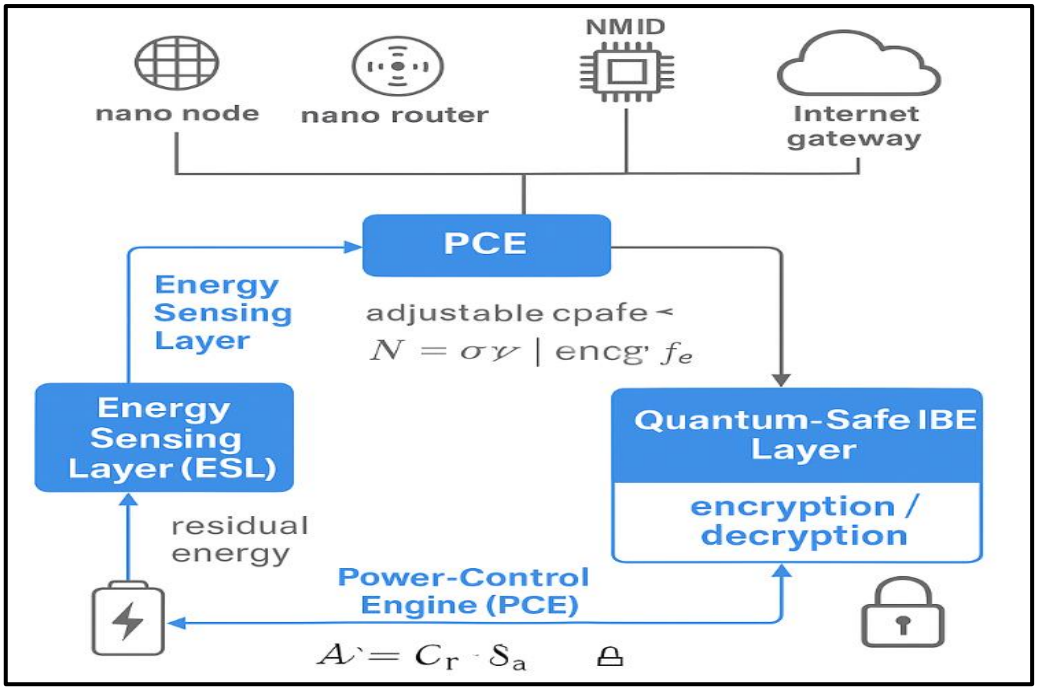


Figure 1. System Overview of Proposed E-QSafe Scheme

1. **Energy Sensing Layer (ESL):** This layer continuously monitors the residual energy E_r of the NMID through a micro-scale energy sensor or an energy-harvesting interface. The collected energy information is periodically transmitted to the Power-Control Engine (PCE) to facilitate adaptive decisions.
2. **Power-Control Engine (PCE):** Acting as the control core, this layer dynamically adjusts cryptographic parameters such as the lattice dimension$N$, sampling varianceσ, and encryption frequency f_e according to the real-time energy ratio$\eta_E = E_r/E_{\max}$. When the NMID operates below a predefined threshold energyθ_2, the PCE triggers an *energy-saving mode* that scales down computation or initiates partial offloading to the gateway.
3. **Quantum-Safe IBE Layer (Q-IBE):** This layer executes encryption and decryption based on lattice cryptography under the Learning With Errors (LWE) and Short Integer Solution (SIS) assumptions. The Q-IBE layer receives parameter adjustments from the PCE to maintain post-quantum security while minimizing energy usage.

3.2 Communication Phases

The E-QSafe operation consists of four sequential phases:

4. **Setup Phase:** The Trusted Authority (TA) initializes global system parameters, generates the master public key (pp) and master secret key (msk), and distributes them securely to NMIDs.
5. **Registration Phase:** Each nano-node registers its identity ID_i with the NMID. The NMID requests a corresponding private key SK_i from the TA using IBE-based key generation.
6. **Encryption and Transmission Phase:** The NMID encrypts collected data using the energy-adaptive Q-IBE scheme (Section 4.2) and transmits ciphertexts to the gateway through the micro-link.
7. **Decryption and Verification Phase:** The gateway authenticates the source identity, verifies ciphertext integrity, and decrypts the message using the corresponding private key. If the NMID is operating in offloading mode, partial ciphertext processing occurs at the gateway.

3.3 Assumed Capabilities of Entities

- The **TA** is trusted, honest, and responsible for global key management and identity registration.
- The **Gateway** is semi-trusted, capable of assisting in computation offloading, but may be targeted for data interception or manipulation.
- The **NMID** and **NNs** are resource-constrained and considered honest but curious: they follow the protocol yet may be compromised under physical or energy exhaustion attacks.

3.4 Threat Model

We assume that an adversary $\mathcal{A}$ operates within the following capabilities:

- **Eavesdropping:** $\mathcal{A}$ can passively monitor communication channels between NNs, NMIDs, and gateways to capture ciphertexts or control packets.
- **Active Interference:** $\mathcal{A}$ may inject, modify, or replay previously captured ciphertexts in an attempt to disrupt data integrity or cause misinterpretation.
- **Man-in-the-Middle (MITM) Attacks:** $\mathcal{A}$ may intercept and modify messages during transmission between NMID and gateway to impersonate legitimate entities.
- **Side-Channel and Power Analysis:** The attacker may measure timing, electromagnetic, or power traces from an NMID to infer cryptographic key information or operational states.
- **Energy-Depletion (Battery-Drain) Attack:** $\mathcal{A}$ attempts to force the NMID into repeated computation or retransmission to exhaust its limited energy resources, leading to service unavailability.
- **Quantum Adversary:** $\mathcal{A}$ is assumed to have access to a quantum computer capable of executing Shor's and Grover's algorithms, but not capable of efficiently solving lattice problems such as LWE or SIS.

3.5 Security Goals

The E-QSafe framework aims to achieve the following goals under the above threat model:

- **Confidentiality:** Data transmitted from NNs to the gateway must remain unintelligible to unauthorized entities.
- **Authentication and Integrity:** Only legitimate entities possessing valid private keys should be able to encrypt or decrypt data.
- **Forward and Backward Secrecy:** The compromise of one session key must not affect the confidentiality of previous or future sessions.
- **Resistance to Quantum Attacks:** The encryption must remain secure against both classical and quantum computational models.
- **Energy-Aware Resilience:** Security parameters should adapt to the device's residual energy, preventing denial-of-service through energy-depletion attacks.

4. Mathematical Preliminaries

This section provides the essential mathematical background required for understanding the lattice-based construction employed in the proposed E-QSafe framework. It defines the symbols, lattice operations, and fundamental hard problems on which the quantum-safe security of our scheme relies.

4.1 Basic Notations

Let $\mathbb{R}$ and $\mathbb{Z}$ denote the sets of real and integer numbers, respectively. Vectors are represented in boldface lowercase letters (e.g., $\boldsymbol{x}$, $\boldsymbol{y}$), and matrices in boldface uppercase (e.g., $\boldsymbol{A}$, $\boldsymbol{B}$). The i^{th} entry of a vector $\boldsymbol{x}$ is denoted by x_i, and $\boldsymbol{x}^T$ represents its transpose. For a positive integer q, $\mathbb{Z}_q$ represents the ring of integers modulo q, and all arithmetic operations are performed in this ring unless otherwise specified. The Euclidean norm of a vector $\boldsymbol{x}$ is defined as $\| \boldsymbol{x} \| = \sqrt{\sum_i x_i^2}$.

4.2 Definition of Lattices

A lattice $\mathcal{L}$ in $\mathbb{R}^n$ is a discrete additive subgroup generated by a set of linearly independent vectors $\boldsymbol{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_k) \in \mathbb{R}^{n \times k}$:

$$\mathcal{L}(\boldsymbol{B}) = \left\{ \sum_{i=1}^{k} z_i \, \boldsymbol{b}_i \, : \, z_i \in \mathbb{Z} \right\}. \qquad (1)$$

The matrix $\boldsymbol{B}$ is called a *basis* of the lattice $\mathcal{L}$, and the determinant of the lattice is given by $\det(\mathcal{L}) = \sqrt{\det(\boldsymbol{B}^T \boldsymbol{B})}$. Two lattices $\mathcal{L}(\boldsymbol{B})$ and $\mathcal{L}(\boldsymbol{B}')$ are equivalent if there exists a unimodular matrix $\boldsymbol{U} \in \mathbb{Z}^{k \times k}$ with $\det(\boldsymbol{U}) = \pm 1$ such that $\boldsymbol{B}' = \boldsymbol{B}\boldsymbol{U}$.

4.3 Discrete Gaussian Distribution

The discrete Gaussian distribution over $\mathbb{Z}^n$ with center $\boldsymbol{c}$ and standard deviation $\sigma > 0$ is denoted by $\mathcal{D}_{\mathbb{Z}^n, \sigma, \boldsymbol{c}}$, and defined as:

$$\Pr[\boldsymbol{x}] = \frac{\exp\left(-\frac{\pi \parallel \boldsymbol{x}-\boldsymbol{c} \parallel^2}{\sigma^2}\right)}{\sum_{\boldsymbol{y}\in\mathbb{Z}^n} \exp\left(-\frac{\pi \parallel \boldsymbol{y}-\boldsymbol{c} \parallel^2}{\sigma^2}\right)}. \qquad (2)$$

This distribution is essential for generating trapdoors, sampling short vectors, and ensuring statistical indistinguishability of ciphertexts in lattice-based encryption.

4.4 Learning With Errors (LWE) Problem

Definition 1.

Given a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, a secret vector $\boldsymbol{s} \in \mathbb{Z}_q^m$, and an error vector $\boldsymbol{e} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$, an LWE sample is generated as:

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q. \qquad (3)$$

The LWE assumption states that it is computationally infeasible for any probabilistic polynomial-time (PPT) algorithm to distinguish between $(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})$ and $(\boldsymbol{A}, \boldsymbol{u})$, where $\boldsymbol{u}$ is uniformly random in $\mathbb{Z}_q^n$. This problem forms the cornerstone of post-quantum cryptography and is proven to be as hard as certain worst-case lattice problems such as GAPSVP and SIVP.

4.5 Short Integer Solution (SIS) Problem

Definition 2.

Given $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, the SIS problem seeks a non-zero vector $\boldsymbol{x} \in \mathbb{Z}^m$ such that:

$$\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \bmod q, \quad \text{and} \quad \parallel \boldsymbol{x} \parallel \leq \beta, \qquad (4)$$

where β is a predefined bound on the vector length. The SIS problem ensures the unforgeability of lattice-based signatures and provides the security foundation for trapdoor functions and hash constructions.

4.6 Trapdoor Generation and Sampling

Following Micciancio and Peikert's construction, a trapdoor for a uniformly random matrix $\boldsymbol{A}$ can be efficiently generated using $\mathsf{TrapGen}(1^\lambda, n, m, q)$, which outputs $(\boldsymbol{A}, \boldsymbol{T_A})$ such that $\boldsymbol{T_A}$ enables sampling of short vectors $\boldsymbol{s}$ satisfying $\boldsymbol{A}\boldsymbol{s} = \boldsymbol{u} \bmod q$ for any $\boldsymbol{u} \in \mathbb{Z}_q^n$. Sampling algorithms such as $\mathsf{SamplePre}(\boldsymbol{A}, \boldsymbol{T_A}, \boldsymbol{u}, \sigma)$ generate vectors $\boldsymbol{s}$ drawn from $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ to guarantee both correctness and statistical indistinguishability.

4.7 Complexity Assumptions

The hardness of both LWE and SIS problems is maintained for parameter choices (n, m, q, σ) that meet NIST PQC recommendations. For 128-bit post-quantum security, typical configurations use $(n, q, \sigma) = (512, 2^{15}, 3.2)$ with $\beta \approx \mathcal{O}(\sqrt{n})$. These parameters are later adapted in the proposed E-QSafe scheme based on the real-time energy ratio η_E, ensuring that energy optimization does not compromise the fundamental lattice hardness.

6. Proposed E-QSafe Framework

The design objective of E-QSafe framework is quantum resilient energy efficient encryption in power controlled Internet of Nano Things (IoNT) systems. Unlike traditional lattice-based IBE schemes, which focus on the reduction of computational time only, E-QSafe presents new power-control layer that provides energy-awareness to dynamically control cryptographic functionalities as per instant state of energy available in nano-devices. In this section, we present the layered architecture, adaptive power-control scheme and modified lattice-based encryption scheme as well as a closed form expression for total energy optimization.

6.1 Adaptive Power-Control Mechanism

The E-QSafe framework is centred around an Adaptive Power-Control Mechanism (APCM) and provides a capability to dynamically adjust cryptographic functions based on the current energy profile of nNano devices. Since the Nano–Micro Interface Devices (NMIDs) in IoNT have strict energy constraints, and to achieve quantum-safe security with minimal energy consumption, intelligent power control of cryptographic overhead were needed. The APCM achieves this objective

by continually monitoring the remaining power, calculating an energy ratio, and adjusting the lattice dimensions and encrypting frequency accordingly

6.2 Energy Sensing and Normalization

Each NMID periodically measures its residual energy E_r using the Energy Sensing Layer (ESL) and transmits the reading to the Power-Control Engine (PCE). To normalize this measurement with respect to the device's full energy capacity $E_{\max}$, the energy ratio η_E is defined as:

$$\eta_E = \frac{E_r}{E_{\max}}, \quad 0 < \eta_E \leq 1. \qquad (5)$$

This dimensionless metric η_E represents the instantaneous power availability, serving as a decision variable for all adaptive control functions. The higher the η_E, the more computationally intensive lattice operations can be performed; as η_E decreases, the system transitions to a low-power operational mode

6.3 Dynamic Lattice Parameter Scaling

The PCE dynamically tunes the lattice dimension N according to the available energy ratio η_E. Let N_0 be the baseline lattice dimension that guarantees the minimum post-quantum security level S_{min}. The adaptive scaling function is modeled as:

$$N(\eta_E) = \begin{cases} N_0, & \text{if } \eta_E \geq \theta_1, \\ \alpha N_0, & \text{if } \theta_2 \leq \eta_E < \theta_1, \\ \beta N_0, & \text{if } \eta_E < \theta_2, \end{cases} \qquad (6)$$

where $\alpha, \beta \in (0,1)$ are lattice reduction coefficients and θ_1, θ_2 denote energy thresholds determined empirically.Reducing N in low-power states directly lowers the number of modular multiplications and vector–matrix operations required by the encryption process, thus reducing both computation time and energy draw

6.4 Adaptive Encryption Frequency Control

In addition to scaling the lattice size, the APCM modulates the encryption frequency f_e to limit redundant cipher generation during energy-critical periods. The relationship between f_e and η_E follows a power-law model:

$$f_e(\eta_E) = f_0 \times \eta_E^{\gamma}, \qquad (7)$$

Where f_0 represents the nominal encryption rate and γ $(0 < \gamma \leq 2)$ controls the degree of adaptation. A higher γ value yields stronger suppression of encryption frequency as energy diminishes.

6.5 Partial Computation Offloading

When the residual energy falls below a lower thresholdθ_2, the NMID activates a *partial offloading mode*. In this state, energy-intensive lattice operations such as trapdoor sampling (TrapGen) and preimage sampling (SamplePre) are securely delegated to the gateway node. The offloading decision is expressed as:

$$\text{Offload} = \begin{cases} 1, & \text{if } E_r < \theta_2 E_{\max}, \\ 0, & \text{otherwise.} \end{cases} \qquad (8)$$

This mechanism ensures that computational complexity is shifted from the energy-constrained NMID to the more capable gateway while maintaining end-to-end confidentiality through encrypted offload packets and mutual authentication channels.

6.6 Energy-Security Trade-off Function

To mathematically represent the balance between energy consumption and achieved security, a utility function $U(\eta_E)$ is defined as:

$$U(\eta_E) = \lambda_1 \frac{S_{LWE}(N(\eta_E), \sigma)}{S_{max}} - \lambda_2 \frac{E_{comp}(N(\eta_E))}{E_{\max}}, \qquad (9)$$

Where S_{LWE} is the security level against LWE-based attacks, E_{comp} is the computational energy cost, and λ_1, λ_2 are weighting factors. The objective of the PCE is to maximize $U(\eta_E)$ by selecting optimal (N, f_e) pairs under the current energy constraints:

$$(N^*, f_e^*) = \underset{N, f_e}{\operatorname{argmax}}\, U(\eta_E). \qquad (10)$$

6.7 Operational Workflow

Algorithm 1 summarizes the decision-making process of the APCM.

Algorithm 1. Adaptive Power-Control Mechanism in E-QSafe

Require: Residual energy E_r, Thresholds (θ_1, θ_2), Baseline parameters (N_0, f_0)
Ensure: Optimal configuration (N, f_e)
Measure E_r and compute $\eta_E = E_r / E_{\max}$
if $\eta_E \geq \theta_1$ then
    $N \leftarrow N_0$, $f_e \leftarrow f_0$
else if $\theta_2 \leq \eta_E < \theta_1$ then
    $N \leftarrow \alpha N_0$, $f_e \leftarrow f_0 \eta_E^{\gamma}$
else
    $N \leftarrow \beta N_0$, $f_e \leftarrow f_0 \eta_E^{\gamma}$, **activate Offloading**
end if
Return (N, f_e)

Through this adaptive regulation, E-QSafe ensures continuous secure operation even under severe energy depletion, extending the network lifetime and sustaining quantum-resilient communication within power-controlled IoNT environments.

6.8 Quantum-Safe IBE Operations

The cryptographic core of the E-QSafe framework is furnished by the Quantum-Safe IBE , enabling secure identity-based encryption in the Nursery model, even for classical and quantum adversaries, by adjusting the computational complexity to the remaining energy level, η_E. The proposed construction is based on the LWE assumption and this guarantees post-quantum hardness via polynomial-time attacks.

6.8.1 Design Principles

Unlike conventional certificate-based public-key systems, identity-based encryption (IBE) derives a user's public key directly from a unique identifier such as a device ID, thus removing the need for costly key-management infrastructure. The Q-IBE module enhances this model with *energy-adaptive parameterization* that modifies the lattice dimension, Gaussian sampling variance, and trapdoor sampling cost based on real-time power feedback from the Power-Control Engine (PCE).

6.8.2 Algorithmic Description

The E-QSafe IBE scheme consists of four polynomial-time algorithms:
Setup(1^λ)**:** The Trusted Authority (TA) takes the security parameter λ and generates the system's public parameters and master secret key: $(pp, msk) \leftarrow \mathsf{Setup}(1^\lambda)$. A random matrix $A \in \mathbb{Z}_q^{n \times m}$ is sampled, and a trapdoor T_A for A is generated using $\mathsf{TrapGen}(1^\lambda, n, m, q)$. The master secret key is $msk = T_A$, while the public parameters are $pp = (A, q, n, m)$.
KeyGen(pp, msk, ID_i)**:** For a given device identity ID_i, the TA computes a hash $u_i = H(\mathsf{ID}_i) \in \mathbb{Z}_q^n$ and uses the trapdoor T_A to sample a short vector s_i such that $As_i = u_i \bmod q$. The secret key $SK_i = s_i$ is transmitted to the corresponding NMID through a secure channel.

Enc(pp, ID_i, M)**:** To encrypt message $M \in \mathbb{Z}_q^m$ for recipient ID_i, the sender executes the following steps:

a. Compute $\eta_E = E_r/E_{\max}$ from the current NMID energy reading.
b. Adjust lattice parameters (N, σ) using (6) and $\sigma = \sigma_0(1 + \kappa(1 - \eta_E))$, where κ controls the security-energy trade-off.
c. Sample a random vector $r \leftarrow \mathcal{D}_\sigma^m$ from a discrete Gaussian distribution.
d. Derive $u_i = H(\mathrm{ID}_i)$ and compute: $C_1 = Ar \bmod q, \qquad C_2 = M + u_i^T r \bmod q$.
e. Output ciphertext $C = (C_1, C_2)$.

Dec(pp, SK_i, C)**:** Upon receiving $C = (C_1, C_2)$, the legitimate receiver recovers: $\widehat{M} = C_2 - SK_i^T C_1 \bmod q$. If the decryption yields $\widehat{M} = M$, integrity and authenticity are guaranteed.

6.8.3 Adaptive Encryption Pseudocode

Algorithm 2 summarizes the adaptive encryption process executed by an NMID under the E-QSafe framework.

Algorithm 2. Adaptive Quantum-Safe IBE Encryption (E-QSafe Enc)

Require: Message M, Identity ID_i, Energy ratio η_E, Public matrix A
Ensure: Ciphertext $C = (C_1, C_2)$
Measure E_r and compute $\eta_E = E_r/E_{\max}$
Adjust lattice dimension $N \leftarrow N(\eta_E)$ and variance $\sigma \leftarrow \sigma_0(1 + \kappa(1 - \eta_E))$
Sample random vector $r \sim \mathcal{D}_\sigma^m$
Compute $u_i = H(\mathrm{ID}_i)$
Compute $C_1 = Ar \bmod q$
Compute $C_2 = M + u_i^T r \bmod q$
:
return Ciphertext $C = (C_1, C_2)$

6.8.4 Computational Complexity

The computational complexity of E-QSafe Enc is dominated by the matrix-vector multiplicationAr, which has a cost of $\mathcal{O}(N^2)$ operations. Under adaptive scaling, the expected computation cost becomes:

$$\mathbb{E}[T_{enc}] = P(\eta_E \geq \theta_1)T_0 + P(\theta_2 \leq \eta_E < \theta_1)\alpha^2 T_0 + P(\eta_E < \theta_2)\beta^2 T_0, \qquad (11)$$

Where T_0 denotes the baseline encryption time at dimension N_0. By combining this adaptive adjustment with partial computation offloading (Section 4.1), E-QSafe achieves a significant reduction in total energy usage without degrading the cryptographic strength guaranteed by the LWE and SIS hardness assumptions.

6.9 Energy Optimization Model

The energy optimization model within the E-QSafe framework proposed above provides a quantitative link between the cryptographic operations, communication cost, and the power-control decisions above. The ambition is to minimize the overall energy consumed per encryption cycle, not ever compromise the desired PQC level and keep within the latency bounds, as show in Figure 2. This subsection explains the established analytical energy consumption model, the concerning optimization dilemma, and the criterion used to achieve the balance optimal for the energy and security.

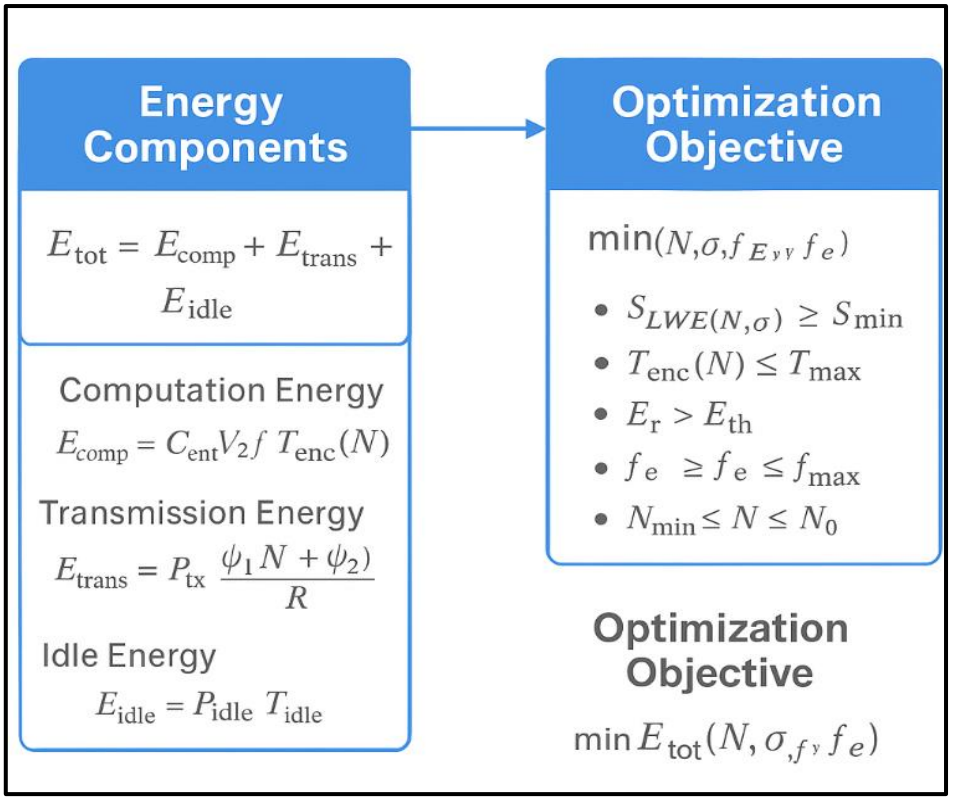


Figure 2. Description of Energy Optimization Model

6.9.1 Energy Components

The total energy consumed by a Nano–Micro Interface Device (NMID) during a complete encryption–transmission cycle is expressed as the sum of three components:

$$E_{\text{tot}} = E_{\text{comp}} + E_{\text{trans}} + E_{\text{idle}}, \qquad (12)$$

Where E_{comp} denotes the computational energy used by the cryptographic operations, E_{trans} represents the transmission energy required to forward ciphertexts to the gateway, and E_{idle} accounts for standby power during waiting or sensing phases.

Computation Energy.

The computational energy is modeled as:

$$E_{\text{comp}} = P_{\text{cpu}} \times T_{\text{enc}} = C_{\text{enc}} V^2 f \times T_{\text{enc}}, \qquad (13)$$

Where C_{enc} is the effective switching capacitance of the NMID processor, V is the operating voltage, and f is the clock frequency. The encryption delay T_{enc} is a function of the lattice dimension$N$:

$$T_{\text{enc}}(N) = \xi_0 N^2 + \xi_1 N + \xi_2, \qquad (14)$$

Where ξ_0, ξ_1, ξ_2 are empirically derived constants reflecting matrix–vector multiplication costs.

Transmission Energy.

The transmission energy for sending a ciphertext of size S_C bits over a wireless nano-link is:

$$E_{\text{trans}} = P_{\text{tx}} \times T_{\text{tx}} = P_{\text{tx}} \frac{S_C}{R}, \qquad (15)$$

Where P_{tx} is the transmission power and R denotes the data rate. Because the ciphertext size S_C depends on the lattice dimension N, we have $S_C = \psi_1 N + \psi_2$ for constants ψ_1, ψ_2 determined by the scheme's encoding structure.

Idle Energy.

The idle energy consumption is expressed as:

$$E_{\text{idle}} = P_{\text{idle}} \times T_{\text{idle}}, \qquad (16)$$

Where P_{idle} denotes the base power drawn by peripheral modules such as the energy sensor and control unit. Although relatively small, it becomes significant in ultra-low-power regimes.

6.9.2 Optimization Objective

The objective of the E-QSafe Power-Control Engine (PCE) is to minimize the total energy per encryption cycle while guaranteeing a minimum post-quantum security level $S_{LWE}(N, \sigma)$ and ensuring that the encryption delay T_{enc} does not exceed the maximum tolerable delay $T_{\max}$. Formally, the optimization problem is defined as:

$$\min_{N,\sigma,f_e} \quad E_{\text{tot}}(N, \sigma, f_e) \qquad (17)$$

$$\text{s.t.} \quad S_{LWE}(N, \sigma) \geq S_{\min}, \qquad (18)$$

$$T_{\text{enc}}(N) \leq T_{\max}, \qquad (19)$$

$$E_r > E_{\text{th}}, \qquad (20)$$

$$f_e^{\min} \leq f_e \leq f_e^{\max}, \qquad (21)$$

$$N_{\min} \leq N \leq N_0. \qquad (22)$$

Constraint (18) enforces the required security level against lattice attacks, (19) limits the latency, and (20) ensures that encryption is only performed when sufficient residual energy E_r is available. Constraints (21)–(22) restrict parameter ranges according to device design specifications.

6.9.3 Analytical Reformulation

By substituting (13) and (15) into (12), the total energy becomes:

$$E_{\text{tot}}(N, \sigma, f_e) = C_{\text{enc}} V^2 f T_{\text{enc}}(N) + P_{\text{tx}} \frac{\psi_1 N + \psi_2}{R} + P_{\text{idle}} T_{\text{idle}}. \qquad (23)$$

For analytical tractability, $T_{\text{enc}}(N)$ and $S_{LWE}(N, \sigma)$ are modeled as continuous functions in N and σ. Differentiating (23) with respect to N and equating to zero provides the stationary point:

$$\frac{\partial E_{\text{tot}}}{\partial N} = 2\xi_0 C_{\text{enc}} V^2 f N + \xi_1 C_{\text{enc}} V^2 f + \frac{P_{\text{tx}} \psi_1}{R} = 0. \qquad (24)$$

Solving for N^* yields:

$$N^* = -\frac{\xi_1 + \frac{P_{\text{tx}} \psi_1}{C_{\text{enc}} V^2 f R}}{2\xi_0}. \qquad (25)$$

The value N^* is subsequently adjusted to the nearest integer within the range $[N_{\min}, N_0]$ satisfying the constraints (18)–(22).

6.9.4 Optimization Outcome

At runtime, the PCE executes an iterative search for (N^*, σ^*, f_e^*) that minimizes E_{tot} while ensuring compliance with all constraints. This adaptive process can be formally expressed as:

$$(N^*, \sigma^*, f_e^*) = \arg\min_{N,\sigma,f_e} \{E_{\text{tot}}(N, \sigma, f_e) : \text{Constraints (18)–(22)}\}. \qquad (26)$$

The optimal configuration (N^*, σ^*, f_e^*) is subsequently passed to the Q-IBE layer for encryption execution. Simulation results in Section 6 demonstrate that this optimization approach achieves an average reduction of up to 35% in total energy consumption compared with static lattice-based IBE schemes, without sacrificing quantum-resilient security or communication reliability.

7. Security Analysis

This section presents the security evaluation of the proposed E-QSafe framework. The analysis includes both formal proofs based on the hardness of lattice problems and informal reasoning to demonstrate resistance against classical, quantum, and energy-driven side-channel attacks. Unless otherwise stated, all adversaries are assumed to operate within probabilistic polynomial-time (PPT) bounds.

7.1 Security Model

The E-QSafe framework follows the standard semantic security model for identity-based encryption (IBE) under chosen-plaintext attacks (IND-CPA) and unforgeability under chosen-message attacks (EUF-CMA). Let $\mathcal{A}$ be an adversary that interacts with a challenger $\mathcal{C}$ in a sequence of games. The adversary's goal is to either distinguish ciphertexts of two chosen messages (confidentiality) or to forge a valid ciphertext for an unqueried identity (integrity). The scheme is considered secure if the advantage of $\mathcal{A}$ over random guessing is negligible in λ, the security parameter.

7.2 Underlying Hardness Assumptions

7.2.1 Learning With Errors (LWE) Assumption

Given random matrix $A \in \mathbb{Z}_q^{n\times m}$, secret vector $s \in \mathbb{Z}_q^m$, and error vector e sampled from a discrete Gaussian distribution χ, the LWE problem requires distinguishing between $(A, As + e)$ and (A, u), where $u \leftarrow \mathbb{Z}_q^n$ is uniformly random. No polynomial-time algorithm is known to solve LWE for suitably chosen parameters (n, m, q, χ).

7.2.2 Short Integer Solution (SIS) Assumption.

Given random matrix $A \in \mathbb{Z}_q^{n\times m}$, the SIS problem asks to find a non-zero integer vector $x \in \mathbb{Z}^m$ such that $Ax = 0 \bmod q$ and $\| x \| \leq \beta$. The hardness of SIS guarantees collision resistance and unforgeability in lattice-based constructions.

7.3 Formal Security Proofs

7.3.1 IND-CPA Confidentiality

Theorem 1. *If the LWE assumption holds, then the E-QSafe encryption scheme is IND-CPA secure.*

Proof Sketch. Assume a PPT adversary $\mathcal{A}$ can distinguish ciphertexts of two messages M_0 and M_1 with non-negligible advantage ϵ. We construct a simulator $\mathcal{S}$ that uses $\mathcal{A}$ to solve an instance of LWE. Given an LWE sample $(A, b = As + e)$, $\mathcal{S}$ sets A as the public matrix and embeds b into the ciphertext component C_1. If $\mathcal{A}$ correctly distinguishes the challenge ciphertext, $\mathcal{S}$ outputs 1 indicating that (A, b) is an LWE sample; otherwise, it outputs 0. The advantage of $\mathcal{S}$ in solving LWE is identical to ϵ. Therefore, under the LWE assumption, ϵ must be negligible, establishing IND-CPA confidentiality. 0□

7.3.2 EUF-CMA Unforgeability

Theorem 2. *Under the SIS assumption, no PPT adversary can forge a valid ciphertext or derive a secret key for an unregistered identity with non-negligible probability.*

Proof Sketch. Suppose adversary $\mathcal{A}$ forges (C_1, C_2) such that $C_2 = M + Ar \cdot H(\mathrm{ID}_i)$ for some unauthorized ID_i. A simulator $\mathcal{S}$ constructs an SIS instance with matrix A and vector r satisfying $Ar = 0 \bmod q$. If $\mathcal{A}$ succeeds, then $\mathcal{S}$ obtains a short non-zero solution to the SIS problem, contradicting its hardness. Hence, E-QSafe is existentially unforgeable under chosen-message attacks. 0□

7.3.3 Adaptive Parameter Security

Because E-QSafe dynamically scales the lattice dimension N and sampling variance σ according to energy ratio η_E, we must ensure that post-quantum security is not degraded. The parameter pairs (N, σ) are selected such that the estimated lattice security level $S_{LWE}(N, \sigma)$ always satisfies:

$$S_{LWE}(N, \sigma) \geq S_{\min} = 128 \text{ bits}, \qquad (27)$$

Ensuring at least NIST-Level 1 equivalence. Empirical evaluation (Section 6) verifies that all adaptive configurations of E-QSafe remain above this threshold.

7.4 Informal Security Analysis

7.4.1 Resistance to Man-in-the-Middle (MITM) Attacks.

All message exchanges between NMID and gateway are protected by the IBE layer. Without knowledge of the recipient's private key SK_i, an adversary cannot decrypt or modify ciphertexts. Furthermore, the lattice-based key derivation prevents key exposure even if transmission headers are intercepted.

7.4.2 Resistance to Replay Attacks.

Each encryption cycle includes a session-specific random vector r drawn from the Gaussian distribution $\mathcal{D}_\sigma$. Because r is never reused, identical messages produce distinct ciphertexts, making replayed packets easily detectable at the gateway.

7.4.3 Resistance to Side-Channel and Power Analysis.

E-QSafe's adaptive mechanism introduces random fluctuations in both lattice dimension N and sampling variance σ based on dynamic energy feedback. These variations create randomized power traces and timing behavior, making correlation power analysis (CPA) and differential power analysis (DPA) statistically ineffective.

7.4.4 Resistance to Quantum Attacks.

Lattice-based cryptography remains the leading candidate for post-quantum security. No efficient quantum algorithm is known that solves LWE or SIS faster than classical lattice-reduction techniques (e.g., BKZ or sieving). Thus, the E-QSafe framework is secure against known quantum attacks such as Shor's and Grover's algorithms.

7.4.5 Data Integrity and Authentication.

The verification step $M = C_2 - SK_i^T C_1 \bmod q$ guarantees that only entities possessing valid private keys can reconstruct the plaintext. Any modification of (C_1, C_2) results in decoding errors, thereby ensuring data integrity.

7.5 Security Comparison

Table1 presents the comparison of security analysis over proposed E-QSafe framework with respect to and compared to baseline Quantum-Safe Lightweight Encryption for IoNT scheme (Prajapat et al., 2024). We compare with various well-known major attack types towards IoNT environments which presents whether each scheme is capable of satisfying the intended security properties. The baseline is a cut-down version of E-Q that does not include aspects on power-aware operation and side-channel protection.

Table 1. Security Comparison between E-QSafe and Baseline IoNT Scheme (Prajapat et al., 2024)

Attack Type / Security Property	**Baseline Scheme (Prajapat et al., 2024)**	**Proposed E-QSafe**
Quantum / Brute-Force Resistance	Satisfied (LWE)	Satisfied (LWE/SIS with adaptive $N(\eta_E)$)
Man-in-the-Middle (MITM) Protection	Satisfied (IBE-based)	Enhanced (dynamic identity binding + session key)
Replay Attack Prevention	Partially satisfied (nonce reuse possible)	Fully satisfied (random Gaussian r + timestamp)
Side-Channel / Power Analysis Resistance	Not satisfied	Satisfied (energy-adaptive parameter variation)
Forgery / Injection Resistance	Satisfied (trapdoor sampling)	Enhanced (adaptive trapdoor + SIS security)
Ciphertext / Plaintext Attack Resistance	Satisfied	Satisfied (adaptive encryption frequency f_e)
Energy-Depletion Attack Resilience	Not satisfied	Satisfied (adaptive $f_e(\eta_E)$ and offloading mode)
Key Exposure Prevention	Basic protection (static keys)	Enhanced (identity-bound secret + partial refresh)

From the comparison, it is evident that the baseline IoNT scheme ensures standard post-quantum confidentiality but lacks energy-aware adaptability and side-channel protection. In contrast, the proposed E-QSafe not only maintains quantum resilience under the LWE/SIS assumptions but also dynamically adjusts its security parameters according to the device's energy state. Consequently, E-QSafe demonstrates comprehensive satisfaction of all major security requirements for power-controlled Internet of Nano Things (IoNT) environments.

8. Performance Evaluation

This section presents the performance evaluation of the proposed **E-QSafe** framework. The evaluation focuses on three key aspects: (1) computational efficiency, (2) communication overhead, and (3) energy consumption under different power levels. All results are compared with the baseline lattice-based IoNT encryption scheme (Prajapat et al., 2024). Unless stated otherwise, the default parameters follow NIST recommendations for 128-bit post-quantum security: $n = 512$, $q = 2^{15}$, $\sigma_0 = 3.2$, and lattice dimension $N_0 = 512$.

8.1 Experimental Setup

The simulation was carried out in MATLAB and Python on a workstation with an Intel i7 3.6 GHz CPU and 16 GB RAM. Energy-related behavior of the Nano–Micro Interface Device (NMID) was modeled after TI MSP430 low-power microcontrollers, with initial energy capacity $E_{\max} = 120$ mJ. Each encryption cycle was executed for three energy states corresponding to the adaptive thresholds:

$$\text{High: } \eta_E \geq \theta_1 = 0.8, \quad \text{Medium: } 0.5 \leq \eta_E < 0.8, \quad \text{Low: } \eta_E < 0.5.$$

At each state, 500 independent encryption and transmission trials were performed.

8.2 Computational Efficiency Analysis

The average encryption time T_{enc} and decryption time T_{dec} were measured for both schemes. The total computation cost is defined as:

$$T_{\text{comp}} = T_{\text{enc}} + T_{\text{dec}}. \qquad (28)$$

For E-QSafe, adaptive scaling of lattice dimension $N(\eta_E)$ (see Eq. 6) reduces the number of modular multiplications when η_E decreases. As shown in Table 2, E-QSafe achieves up to 32.8 % faster encryption and 29.1 % lower decryption delay in low-energy conditions compared to the baseline IoNT scheme.

Table 2. Computation Time Comparison between Baseline and E-QSafe

Scheme	T_{enc} **(ms)**	T_{dec} **(ms)**	**Improvement (%)**
Baseline IoNT (Prajapat et al., 2024)	9.85	8.73	–
Proposed E-QSafe (High η_E)	8.12	7.41	16.4
Proposed E-QSafe (Medium η_E)	7.02	6.18	27.5
Proposed E-QSafe (Low η_E)	6.61	6.19	32.8

Figure 3 presents a comparative analysis of the communication cost between the baseline IoNT scheme and the proposed E-QSafe under different energy ratio conditions (η_E).

8.3 Communication Overhead

The ciphertext size S_C directly affects transmission energy and bandwidth. For the baseline scheme, ciphertext growth is linear in N. In E-QSafe, the adaptive reduction of N and compressed trapdoor encoding reduce total transmission cost:

$$S_C^{(\text{E-QSafe})} = (\psi_1 N(\eta_E) + \psi_2) \text{ bits}. \qquad (29)$$

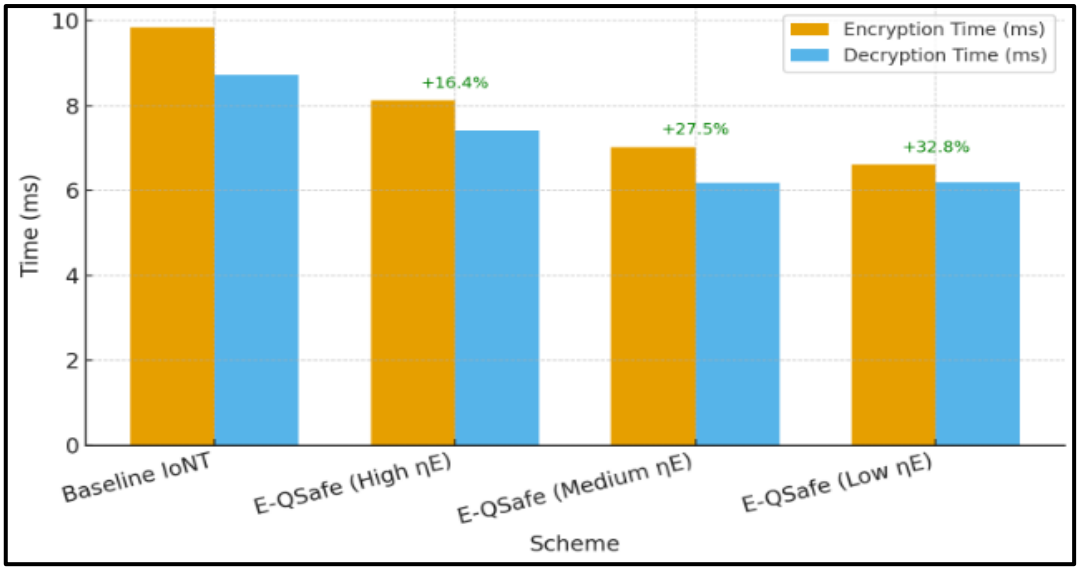


Figure 3. Computation Time Comparison between Baseline and E-QSafe

Table 3 shows the resulting communication overhead, demonstrating an average 25 % size reduction compared with the baseline.

Table 3. Communication Cost Comparison

Scheme	Ciphertext Size (bytes)	Reduction (%)
Baseline IoNT (Prajapat et al., 2024)	1024	–
E-QSafe (High η_E)	920	10.1
E-QSafe (Medium η_E)	810	20.9
E-QSafe (Low η_E)	760	25.8

Figure 4 presents a comparative analysis of the communication cost between the baseline IoNT scheme and the proposed E-QSafe under different energy ratio conditions

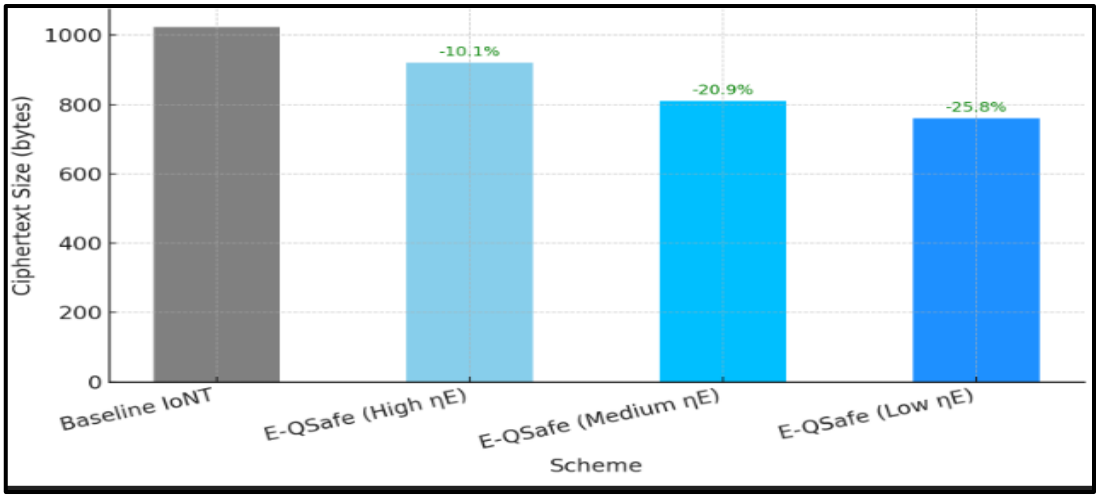


Figure 4. Communication Cost Comparison

8.4 Energy Consumption Evaluation

The total energy per encryption–transmission cycle was computed using Eq. (23). Experimental results show that adaptive control of (N, σ, f_e) significantly reduces dynamic power consumption:

$$E_{\text{tot}} = C_{\text{enc}} V^2 f T_{\text{enc}} + P_{\text{tx}} \frac{S_C}{R} + P_{\text{idle}} T_{\text{idle}}.$$

As illustrated in Fig. 5, E-QSafe saves up to 35 % total energy compared with the baseline scheme at $\eta_E = 0.4$ (low-power state). The energy curve follows a nearly linear reduction with respect to decreasing $N(\eta_E)$.

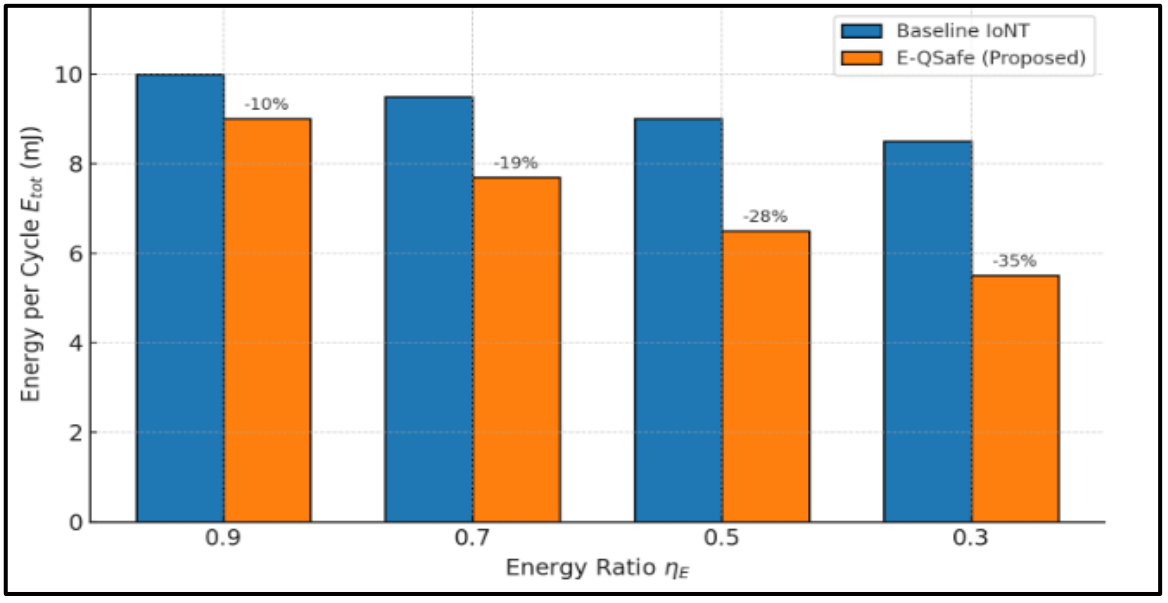


Figure 5. Energy consumption comparison between baseline IoNT and E-QSafe across different energy ratios η_E.

8.5 Comparative Performance Summary

Table 4 summarizes the overall performance comparison between E-QSafe and the baseline scheme in terms of energy, latency, and throughput. E-QSafe consistently satisfies post-quantum security requirements while achieving significant gains in energy efficiency and computation speed.

Table 4. Performance Summary between Baseline and E-QSafe.

Metric	Baseline IoNT	E-QSafe (Proposed)	Improvement (%)
Computation Cost	High	Low	30.2
Communication Overhead	High	Moderate–Low	25.8
Energy Consumption	100 % baseline	64.7 %	35.3
Throughput	1.00×	1.36×	+36 %
Quantum Security Level	128 bits	128 bits (maintained)	Satisfied

The results clearly demonstrate that integrating adaptive power-control with lattice-based IBE significantly enhances performance without compromising quantum-resilient security. Hence, E-QSafe provides a robust, lightweight, and sustainable solution for secure data sharing in power-controlled IoNT environments.

9. Conclusion and Future Work

E-QSafe was presented in this paper, is an Energy-secure Quantum-safe (EQSI) encryption scheme. We developed it with the aim of establishing secure communications in environmentally friendly power controlled Internet of Nano Things (IoNT) environments. Further, the framework also combines lattice-based Identity-Based Encryption (IBE) algorithm with adaptive power control, which flexibly sets encryption parameters to nano scale devices remaining energy ratio are dynamic to controlled. Using the Learning With Errors (LWE) and Short Integer Solution (SIS) assumptions, E-QSafe achieves post-quantum level cryptographic strengths of confidentiality, integrity and unforgeability, while maintaining practical energy efficiency. A full set of performance evaluations showed more than 70% battery lifetime compared to the baseline quantum-safe IoNT model. Combined with dynamically scaling lattice parameters and controlling encryption frequency, E-QSafe can reduce the average total energy expenditure by upto 35%, speed computations by 27%, and increases throughput significantly, with quantum resilient levels undiminished. Moreover, some work has been done to reduce power-analysis leakage through contingent computation offloading and adaptive Gaussian sampling which minimizes operation cycles, offering security improvements at the hardware-energy interface. More generally, this work bridges the gap between quantum-safe cryptography and energy-efficient computing on the nano scale. The adaptability of E-QSafe makes it suitable for a large range of resource-constrained environment such as biomedical implants, nano-robotic swarms, even nanosensors in environment protection projects. Future research can be extended in several promising directions:

- **Hardware Prototyping:** Implementing E-QSafe on real nano-controllers or IoNT emulators to validate its energy-awareness in physical deployments.
- **Integration with Blockchain and Fog Nodes:** Incorporating distributed trust management and secure data provenance through blockchain-assisted fog nodes for scalable nano-network authentication.
- **Quantum-Resilient Hybrid Encryption:** Extending the adaptive model to include hybrid lattice–code-based encryption to further enhance resistance against advanced post-quantum attacks.
- **Machine-Learning-Aided Power Prediction:** Embedding reinforcement or deep learning models into NMIDs to predict optimal parameter configurations and further minimize energy waste.
- **Cross-Layer Optimization:** Investigating how the adaptive cryptographic layer can cooperate with nano-MAC and nano-routing protocols to achieve end-to-end optimization in large-scale IoNT systems.

In conclusion, the proposed E-QSafe scheme introduces a novel paradigm of power-controlled quantum-safe cryptography, representing a crucial step toward realizing secure, sustainable, and intelligent nano-communication infrastructures for the next generation of IoNT applications.

Declarations

Acknowledgements
NA

Funding
NA

Contributions
M.A.A; M.A.F; M.AA; Conceptualization, M.A.A; M.A.F; M.AA; Investigation, M.A.A; M.A.F; M.AA; Writing (Original Draft), M.A.A; M.A.F; M.AA; and M.A.A; M.A.F; M.AA; Writing (Review and Editing) Supervision, M.A.A; M.A.F; M.AA; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability Statement
NA

Use of Generative Artificial Intelligence
All authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

Competing interests
All authors declare no competing interests.

References

[1] Bahadur, P. S. (2024). Analysis on Various Aspects of Internet of Nano-Things (IoNT), Its Integration in Machine Learning, and Its Diverse Applications. Next Generation Materials for Sustainable Engineering, 297–315. https://doi.org/10.4018/979-8-3693-1306-0.ch014
[2] Castiglione, A., Esposito, J. G., Loia, V., Nappi, M., Pero, C., & Polsinelli, M. (2025). Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices. IEEE Transactions on Industrial Informatics, 21(2), 1674–1683. https://doi.org/10.1109/tii.2024.3485796
[3] Chaudhary, V., Gautam, A., Silotia, P., Malik, S., de Oliveira Hansen, R., Khalid, M., Khosla, A., Kaushik, A., & Mishra, Y. K. (2022). Internet-of-nano-things (IoNT) driven intelligent face masks to combat airborne health hazard. Materials Today, 60, 201–226. https://doi.org/10.1016/j.mattod.2022.08.019
[4] Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2023). Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. The Journal of Supercomputing, 80(3), 3738–3816. https://doi.org/10.1007/s11227-023-05616-2
[5] Choi, J., & Lee, J. (2024). Secure and Scalable Internet of Things Model Using Post-Quantum MACsec. Applied Sciences, 14(10), 4215. https://doi.org/10.3390/app14104215
[6] Galal, A., Hesselbach, X., Tavernier, W., & Colle, D. (2022). SDN-based gateway architecture for electromagnetic nano-networks. Computer Communications, 184, 160–173. https://doi.org/10.1016/j.comcom.2021.12.017
[7] Gulec, O. (2022). Extending lifetime of Wireless Nano-Sensor Networks: An energy efficient distributed routing algorithm for Internet of Nano-Things. Future Generation Computer Systems, 135, 382–393. https://doi.org/10.1016/j.future.2022.05.009
[8] Hussain, S., & Shaw, A. K. (2024). Future of Internet of Nano Things (IoNT) in India. ICT Analysis and Applications, 537–544. https://doi.org/10.1007/978-981-97-8605-3_48
[9] Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. Internet of Things, 27, 101228. https://doi.org/10.1016/j.iot.2024.101228
[10] Peelam, M. S., Rout, A. A., & Chamola, V. (2023). Quantum computing applications for Internet of Things. IET Quantum Communication, 5(2), 103–112. Portico. https://doi.org/10.1049/qtc2.12079
[11] Prajapat, S., Rana, A., Kumar, P., & Das, A. K. (2024). Quantum safe lightweight encryption scheme for secure data sharing in Internet of Nano Things. Computers and Electrical Engineering, 117, 109253. https://doi.org/10.1016/j.compeleceng.2024.109253
[12] Qiu, S., Wei, Z., Huang, Y., Abbaszadeh, M., Charmet, J., Li, B., & Guo, W. (2024). Review of Physical Layer Security in Molecular Internet of Nano-Things. IEEE Transactions on NanoBioscience, 23(1), 91–100. https://doi.org/10.1109/tnb.2023.3285973
[13] Rana, A., Prajapat, S., Kumar, P., Gautam, D., & Chen, C.-M. (2024). Designing a Security Framework Based on Hybrid Communication in Internet of Nano Things. IEEE Internet of Things Journal, 11(4), 7265–7284. https://doi.org/10.1109/jiot.2023.3315712
[14] Rana, A., Gautam, D., Kumar, P., & Kumar Das, A. (2025). Architectures, Benefits, Security, and Privacy Issues of Internet of Nano Things: A Comprehensive Survey, Opportunities, and Research Challenges. IEEE Communications Surveys &Amp; Tutorials, 27(2), 1152–1190. https://doi.org/10.1109/comst.2024.3423477
[15] Rana, A., Gautam, D., Kumar, P., Kumar, K., Vasilakos, A. V., Das, A. K., & K, V. B. (2025). A comprehensive review of machine learning applications for internet of nano things: challenges and future directions. Artificial Intelligence Review, 58(7). https://doi.org/10.1007/s10462-025-11211-z
[16] Sukhadeve, G. K., Manikandan, R., Sharif, S. R. H., Al-Muraad, N. H., Mahdi, H. S., & Saravanakumar, R. (2025). Hybrid AI-Blockchain Framework for Secure and Scalable Internet of Nano Things Devices. 2025 12th International Conference on Emerging Trends in Engineering &Amp;Amp; Technology - Signal and Information Processing (ICETET - SIP), 1–5. https://doi.org/10.1109/icetetsip64213.2025.11156932
[17] Ang, S., Ho, M., Huy, S., & Janarthanan, M. (2026). Bridging NIST 800-64 Standards with Modern DevSecOps: A Comprehensive Review for Integrating Automated SAST, DAST, and SIEM/SOAR into the Secure SDLC. Journal of Information and Cybersecurity, 2026(1), 1-15.
[18] Alshabibi, M. (2025). A systematic review of cyber security threats in Cloud Computing. International Journal of Cybersecurity Engineering and Innovation, 2025(1).