Design and Research of NB-IoT Lightweight End-to-End Encryption Protocol Based on Lattice Cipher

Liang Shaoyu

School of Electronic Information Engineering, Guangzhou City Polytechnic, Guangzhou, Guangdong, 511300, China
E-mail: lshywin@126.com

Received 14 May 2025; Accepted 25 June 2025

Abstract

With the widespread application of the narrowband Internet of Things (NB-IoT), its secure communication issues have become increasingly prominent. Traditional encryption algorithms do not perform well on resource-constrained NB-IoT devices, making it difficult to meet the needs of efficient and secure communication. To this end, this study proposes a lightweight end-to-end encryption protocol for NB-IoT based on Lattice cypher. This protocol takes advantage of the Lattice cryptosystem's high security and parallel computing characteristics and designs an encryption scheme suitable for low power consumption and low bandwidth scenarios. Through experimental verification, the protocol performs well in terms of security, can provide up to 128 bits of security strength, and effectively resists various attacks. In terms of computing efficiency, compared with RSA and ECC encryption algorithms, the computing time of this protocol in key generation, encryption and decryption processes is reduced by 35%, 40% and 38%, respectively, significantly improving device operating efficiency. At the same time, this protocol controls the extra overhead of data transmission within 5%, far lower

Journal of Cyber Security and Mobility, Vol. 14_3, 723–746.
doi: 10.13052/jcsm2245-1439.1439

than the 10%–15% of traditional encryption protocols, effectively reducing communication costs. The NB-IoT lightweight end-to-end encryption protocol based on Lattice cipher proposed in this study provides an efficient and practical solution for secure communication in narrowband IoT and has a wide application prospect.

Keywords: Lattice cipher, NB-IoT, lightweight encryption, end-to-end security, resource-constrained environment.

1 Introduction

With the rapid development of Internet of Things technology, narrowband Internet of Things (NB-IoT), a communication technology with low power consumption and wide coverage, has shown great application potential in smart cities, smart homes, environmental monitoring and other fields [1, 2]. However, with the widespread deployment of NB-IoT devices, the issues of data security and privacy protection have become increasingly prominent, which has become a key factor restricting its further development [3]. Traditional encryption technologies are often difficult to implement effectively on resource-constrained NB-IoT devices. Therefore, designing a lightweight and efficient end-to-end encryption protocol to meet the security requirements of NB-IoT devices has become a hot and difficult point in current research [4].

Against this background, Lattice cypher, as a new cryptosystem, has gradually attracted widespread attention from researchers because of its advantages such as high computational efficiency, small key size and strong ability to resist quantum attacks [5, 6]. Lattice cryptography is based on Lattice theory and uses difficult problems in Lattice to construct cryptographic algorithms. It can effectively reduce computing and storage overhead while ensuring security and is suitable for resource-limited NB-IoT devices [7]. Therefore, exploring the design of NB-IoT lightweight end-to-end encryption protocol based on Lattice cypher has important theoretical significance and broad application prospects.

At present, scholars at home and abroad have carried out a series of research work in the field of NB-IoT security and proposed a variety of encryption protocols and solutions [8, 9]. However, most existing schemes are based on traditional cryptosystems, such as symmetric cryptography, public key cryptography, etc. When these schemes are implemented on NB-IoT devices, they often face problems such as high computational complexity and high energy consumption [10]. In addition, with the rapid development of

quantum computing technology, the traditional cryptosystem faces the risk of being cracked. Lattice cryptosystem provides new ideas and solutions for NB-IoT security because of its anti-quantum attack characteristics [11].

This study aims to design a lightweight end-to-end encryption protocol for NB-IoT based on Lattice cypher and proposes an efficient and secure encryption scheme by deeply analyzing the resource constraints and security requirements of NB-IoT devices, combined with the advantages of Lattice cypher. This scheme will focus on how to effectively reduce the computing and storage overhead in the encryption and decryption process and improve the protocol's real-time and energy efficiency ratio while ensuring security. At the same time, this study will also analyze the security and performance evaluation of the designed encryption protocol to verify its feasibility and effectiveness in practical applications.

During the research process, we will fully consider the characteristics of the NB-IoT network, such as a large number of devices, frequent data transmission, and complex network environment, to ensure that the designed encryption protocol can adapt to various application scenarios. In addition, we will also focus on the protocol's flexibility and scalability so that it can be easily adjusted and optimized when technology upgrades and scenario changes in the future.

This research focuses on the field of NB-IoT, and designs a new lightweight end-to-end encryption protocol based on lattice cipher for the limitations of traditional encryption protocols. In terms of protocol design, the scalability is enhanced, a general algorithm adaptation framework is built, and the integration of multiple Lattice algorithms is supported, which can achieve good compatibility regardless of the current mainstream algorithm or the new Lattice version in the future, completely get rid of the dependence on specific solutions (such as NewHope), and significantly improve the universality and long-term applicability of the protocol. At the same time, the protocol workflow is comprehensively optimized, the interaction details between the device and the server are clearly defined, and a complete set of authentication and key negotiation coordination mechanisms are carefully designed, which effectively resists the risk of man-in-the-middle attacks through two-way authentication, digital signature and other technical means, ensures the authenticity and credibility of the identities of both parties to the communication, and lays a solid foundation for safe and reliable key negotiation and data transmission.

Through this study, we expect to provide a new solution for the NB-IoT security field, promote the application of Lattice cryptography in the Internet

of Things, further improve the security and reliability of NB-IoT devices, and provide a strong guarantee for the healthy development of the Internet of Things. At the same time, this study will also provide useful references for researchers in related fields and jointly promote the progress and development of IoT security technology.

2 Theoretical Basis of Lightweight Encryption Based on Lattice Cipher

2.1 Lattice Password Fundamentals

A lightweight homomorphic encryption scheme based on Lattice theory, which takes advantage of vector space characteristics to convert plaintext into a matrix with noise, and achieves excellent computational efficiency while ensuring security through efficient addition and multiplication operations [12, 13]. In this scheme, five integer global parameters are set: *N* is the plaintext vector dimension, *r* is the ring eigenvalue, *l* is the homomorphic operation depth, *n* is the number of soft perturbation matrices in the public key, and ε_{max} is the upper limit of noise.

Calculate $l_0 = n \times N \times 8mx + (N-1) \times r$, $q = 2 \times l0 \times (2l+1)$, $p = q \times r + \varepsilon$, where $\varepsilon < l_0$. Then, within the finite field $GF(p)$, two $N \times N$-dimensional random matrices A and B are created, ensuring that A is inversible, and the matrix $M = [A|B]$ is constructed; At the same time, a random diagonal reversible disturbance matrix Δ of $N \times N$ dimensions is generated; Then, the random inversible matrix P_k is left-multiplied by the matrix *M* to obtain *n* matrices $M = [A|B]$; Then, *n*-dimensional soft noise matrices $D_k \in \{-1, 1\}^{N \times N}$, $k \in \{1, 2, \ldots, n\}$ are generated, and *n* soft perturbation matrices $M_k = [A_k|B_k + D_k\Delta]$ are constructed; Create a $N \times N$-dimensional soft noise matrix $M_0 = [A_0|B_0 + D_0\Delta]$; Replace the diagonal values in D_0 with *q* to obtain the hard noise matrix D_0. Calculate the hard disturbance matrix $M_0 = [A_0B_0 + D_0\Delta]$; Finally, a permutation permutation $M_k = \mathcal{G}(.)$, $k \in \{0, 1, \ldots, n\}$ is performed on the hard perturbation matrix and the soft perturbation matrix $\mathcal{G}(.)$ using the matrix permutation permutation algorithm. Among these generated parameters, $n+1$ matrices $\{M_0, M_1, \ldots, M_n\}$ are used as public keys; Permutation permutation algorithm, matrix M and perturbation matrix Δ are used as private keys $\mathcal{G}(.)$. On Z_r^N, the plaintext information m is multiplied by the hard noise matrix *M*, and *n* soft noise vectors are added to form the ciphertext vector $\sum_{k=1}^{n} r_k M_k$. r_k is the value of each dimension of n soft noise vectors that is less than ε_{max}.

The expression of the ciphertext vector is Equation (1):

$$c = mM_0 + \sum_{k=1}^{n} r_k M_k \tag{1}$$

The decryption process is mainly realized by removing the previously added random noise. First, the permutation is restored to Equation (2).

$$\dot{c} = G^{-1}(c) \tag{2}$$

Here, c is the ciphertext vector in $G^{-1}(p)^{2N}$. Next, the disturbance noise is calculated using Equation (3).

$$\dot{e} = \dot{c}_D - \dot{c}_U A^{-1} B \tag{3}$$

In the expression, $\dot{c}_D$ and $\dot{c}_U$ represent the noise-affected $\dot{c}$ and unaffected parts of the vector, respectively, where $\dot{c}_U$ is the N dimension of the vector $\dot{c}_D$ and $\dot{c}_D$ is the back N dimension. The result after the noise disturbance matrix $\wedge$ is eliminated is shown in Equation (4).

$$\dot{e} = e\Lambda^{-1} \tag{4}$$

For each $\dot{e}_j$ in $\dot{e} = [\dot{e}_1, \dot{e}_2, \dot{e}_3]$, calculate according to formulas (5)–(7). The original plaintext $m = (m_1, \ldots, m_N)$ is obtained. μ represents hyper-parameters, and the research uses lattice-based homomorphic encryption technology to ensure that the system is resistant to quantum attacks and efficiently transmits multi-dimensional data.

$$\ddot{e}_j = \dot{e}_j - \mu \tag{5}$$

$$\mu = \begin{cases} e_j \; mod \; q, \left(e_j \; mod \; q < \dfrac{q}{2}\right) \\ \cdot \\ (e_j \; mod \; q) - q, \left(e_j \; mod \; q \geq \dfrac{q}{2}\right) \end{cases} \tag{6}$$

$$m_j = \ddot{e}_j q^{-1} \tag{7}$$

2.2 Overview of NB-IoT Lightweight Encryption Technology

A simplified version of the LTE network protocol, the NB-IoT standard, can seamlessly upgrade existing systems [14]. Aiming at the overload, congestion, and resource shortage of data and signalling planes, the 3GPP R12 protocol focuses on the technical standardization of R8–R11.

R12 is also optimized for low-cost MTC terminals, introducing enhanced GSM access, security performance and network architecture improvements. R13 defines three narrowband air interface technologies. EC-GSM-IoT, enhanced machine-like communications, and H technologies; R14 is improved in six areas, including low transmit power termination, multicast support, etc., and frozen in R14; R15 proposes that NB-IoT and eMTC technologies will become the basic solutions for mMTC LPWA scenarios in the 5G era, and optimizes latency and power consumption [15].

The wake-up signal can significantly improve paging monitoring efficiency, and the terminal power consumption is expected to be reduced by 30%–45% in deep coverage scenarios [16, 17]. During RACH, early data transmission can be performed without an RRC connection, which helps to reduce latency and UE power consumption.

The widespread application of IoT benefits from communication standardization [18]. Compared with traditional GPRS systems, NB-IoT systems support more device connections, which are theoretically 50 to 100 times that of traditional cellular networks. It also supports low latency and network architecture optimization. With the increase of smart home devices, NB-IoT technology meets the networking needs of all devices. NB-IoT technology has deep coverage capabilities, improving area coverage by 20 dB and 100 times compared to LTE coverage capabilities. It does not require additional jumpers to boost the signal and save resources. The low cost of NB-IoT is reflected in the fact that it does not need to redeploy the network, and the design of terminal modules is simple [19]. Low power consumption is crucial for devices in special scenarios. NB-IoT terminals can work for at least 10 years when using a 5Wh battery, ensuring at least 5 years of working time in harsh environments. The NB-IoT network lacks interfaces with 2G and 3G and cannot interoperate. It usually adopts a four-tier architecture, as shown in the defined architecture diagram, see Figure 1.

The NB-IoT network architecture consists of terminals, base stations, core networks, cloud platforms and vertical industry centres [20, 21]. The terminal is the perception layer, the base station and the core network constitute the transport layer, and the vertical industry centre is the application layer [22, 23]. The NB-IoT system has added a cloud platform layer located between the application layer and the transport layer, integrating data from various industries and promoting the construction of smart cities. As the first choice for IoT communication, NB-IoT technology must be independently deployed in a small bandwidth environment and adapted to different locations. At the same time, it is compatible with low-cost product

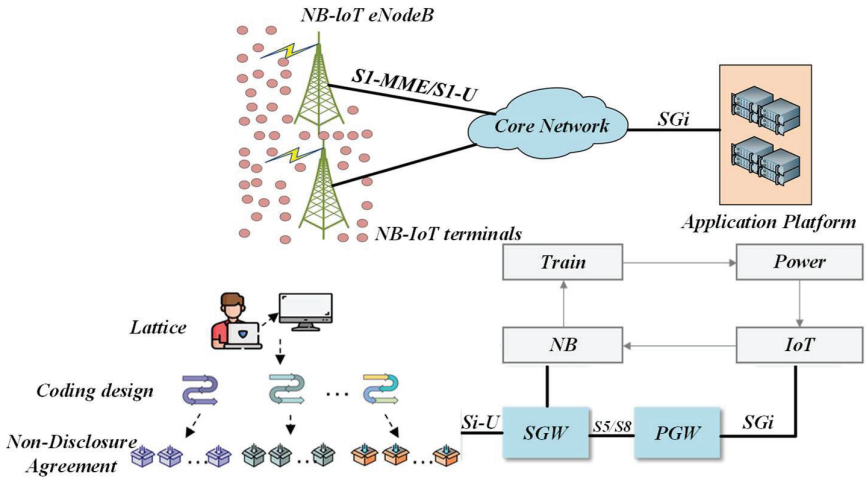

Figure 1 NB-IoT networking diagram.

battery technology to limit terminal transmission power and battery peak current [24, 25].

3 Construction of Lattice Cryptographic End-to-End Encryption Protocol Model for NB-IoT

3.1 Design of End-to-End Encryption Protocol for Lattice Cipher

This study proposes a lightweight end-to-end encryption protocol for NB-IoT based on Lattice cryptography technology. This protocol utilizes Lattice cryptography's efficient computing and quantum attack resistance characteristics to meet the secure communication needs of resource-constrained NB-IoT devices. When designing the protocol, NB-IoT devices' resource constraints and security risks were evaluated, and lightweight encryption algorithms were developed to reduce the computational and storage burden. In particular, homomorphic encryption technology based on Lattice cypher is adopted, allowing direct processing of encrypted data, effectively reducing energy usage.

In view of the resource-limited characteristics of NB-IoT devices, a lightweight end-to-end encryption protocol is designed. The protocol uses the unique mathematical structure of lattice cryptography to build an encryption system, and reduces the computational complexity under the premise of ensuring data security by optimizing the key generation, encryption and

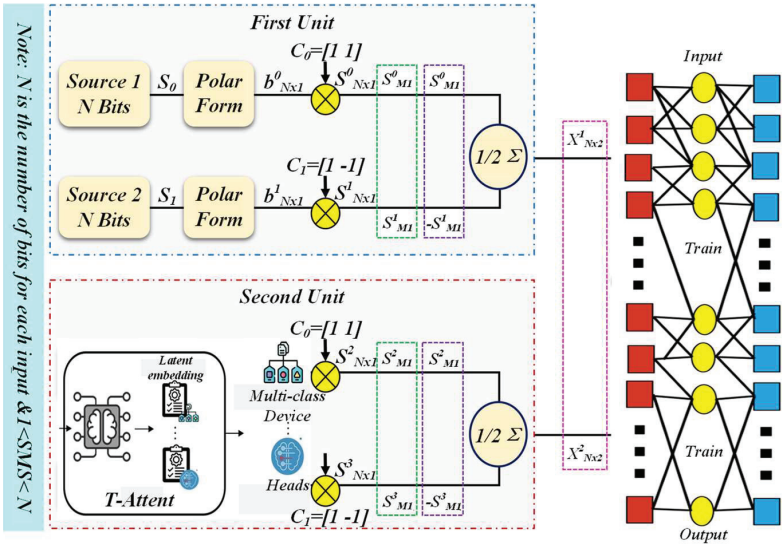

Figure 2 Lattice cryptographic end-to-end encryption protocol model architecture of NB-IoT.

decryption processes, so as to adapt to the low-power and low-cost operation requirements of NB-IoT devices, and realizes the full encryption protection of end-to-end data transmission.

Figure 2 shows the architecture of the Lattice cryptographic end-to-end encryption protocol model for NB IoT. In order to ensure the security of the RM-CP-ABE scheme, three conditions need to be met: confidentiality, that is, users cannot decrypt information without matching attributes; Revocability means that the revoked user cannot decrypt the information that matches the policy; Anti-collusion, even if the attacker obtains some private information, it cannot be decrypted if the policy is not met [26, 27]. In the security model, CSP complies with the protocol while trying to obtain plaintext information and defines the selective security of RM-CP-ABE through the security game. ABE scheme adopts a distributed structure, allowing multiple attribute authorities to jointly be responsible for key generation and management, and supports attribute revocation. *GlobalSetup* $(1^{\lambda}, S_{max}, N) \rightarrow GP$ algorithm accepts the security parameter 1^{λ}, the maximum width S_{max} and the number of users *N* as inputs, and performs the corresponding steps.

Combine NB-IoT's low power consumption and long-term connectivity features for targeted design. In terms of low power consumption, the key management mechanism is optimized to reduce the key update operation,

and the calculation mode of the lattice cryptographic algorithm is optimized to reduce the power consumption. In view of the characteristics of persistent connections, a key update strategy combining periodic and event-triggered is adopted to effectively balance security and energy consumption while ensuring communication security.

Choose the LWE parameters *n*, *m*, *q*, σ. Set Noise Distribution $X_{lwe}, X_1, X_2, X_{big}$. Define a common hash function H_1, H_2, where H_1 maps a string to a $(m-1)$-dimensional random integer vector space and H_2 is an FRD function. Randomly select vector y_1, y_2 and set matrix B, the calculation formula is shown in Equation (8).

$$B_1 = [y_1^T \parallel \overset{m-1}{0^T \parallel \cdots \parallel 0^\top}], B_2 = [y_2^T \parallel \overset{m-1}{0^T \parallel \cdots \parallel 0^T}] \tag{8}$$

Where $0 \in Z_q^n$ is an element of *Z* and $\{B_1, B_2\}$ is a subset of $Z_q^{n \times m}$. Finally, the common parameters as shown in Equation (9) are output.

$$GP = (n, m, q, \chi_{lwe}, \chi_1, \chi_2, \chi_{big}, B_1, B_2, H_1, H_2) \tag{9}$$

$AuthSetup(GP, u, x) \rightarrow (PK_u, MSK_u)$: This algorithm accepts that the global parameter *GP* and the attribute mechanism identifier *u* belong to *AU*, and performs the following steps: the user management organization AA_0 executes and runs the trapdoor generation algorithm $EnTrapGen(1^n, 1^m, q)$, generates (A_0, T_{A0}), and randomly and uniformly selects the matrix $H_0 \leftarrow Z_q^{n \times m}$. The attribute mechanism *AAu* also executes the trapdoor generation algorithm $EnTrapGen(1^n, 1^m, q)$, generates (A_w, TA_w), and randomly and uniformly selects the matrix $H_u \leftarrow Z_q^{n \times m}$. Finally, the public key $PK_{u(0)} = (A_{u(0)}, H_{u(0)})$ and the master private key $MSK_{u(0)} = (TA_{u(0)})$ are output.

Key generation $KeyGen(GP, PK_{u(0)}, MSK_{u(0)}, id, st) \rightarrow SK_{id}$: This process includes inputting global parameters *GP*, public key $PK_{u(0)}$, master key $MSK_{u(0)}$, user identity identifier *id*, and user current state *st*. The algorithm execution steps include calculating $t_{id} = (1, H_1(id)) \in z^m$, randomly selecting a vector $\hat{k}_{id,u} \leftarrow \chi_{big}^m$, and sampling the vector, as shown in formula (10).

$$\tilde{k}_{id,u} \leftarrow EnSamplePre(A_u, T_{A_u}, \sigma, t_{id} H_u^T - \hat{k}_{id,u} A_u^T) \tag{10}$$

Calculate $\tilde{k}_{id,u}$ and add it to $\hat{k}_{id,u}$. If the node θ is in the $Path(id)$ and is empty, the node θ is processed by the user management authority AA_0. The vector $w_\theta \leftarrow Z_q^n$ is randomly selected and stored in node θ. For each θ in $Path(id)$, the user management agency calculates a vector,

$t_{id} = (1, H_1(id)) \in Z^m$ randomly selects the vector $\hat{k}_{id,u} \leftarrow \chi_{big}^m$, and samples according to formula (11).

$$\tilde{k}_{td,\theta} \leftarrow EnSamplePre(A_0, T_{A_0}, \sigma, t_{td}H_0^T - \hat{k}_{td,q}A_0^T - w_qH_0^T) \quad (11)$$

Compute the vector $k_{id,\theta}$ as the sum of $\hat{k}_{id,\theta}$ and $\tilde{k}_{id,\theta}$. The key output of the user *id* is shown in Equation (12).

$$SK_{id} = (\{k_{id,u}\}_{u \in AU}, \{k_{id,\theta}\}_{\theta \in Path(id)}) \quad (12)$$

The user management authority is responsible for the key updating process in the key updating stage, including inputting the public parameter *GP*, the public key *PK*, the master private key *MSK*, the current state *st*, the revocation list *rl* and the current time *x*. The execution steps are as follows: First, run the $KUNodes(st, rl, t)$ algorithm to obtain θ, and extract the vector w_θ from *st*. Next, calculate the vector $t_x \rightarrow Z^m$ and the matrix $H_x = H_0 + H_2(x)G$. Finally, the vector x, $\hat{k}_{x,\theta} \leftarrow x_{big}^m$ is randomly selected, and the vector sampling is carried out according to Equation (13).

$$\tilde{k}_{x,\theta} \leftarrow EnSamplePre(A_0, T_{A_0}, \sigma, t_xH_x^T - \hat{k}_{x,\theta}A_0^T - w_qH_0^T) \quad (13)$$

Calculate $k_{x,\theta} = \hat{k}_{x,\theta} + \tilde{k}_{x,\theta}$, and output the update key, as shown in Equation (14).

$$KU_x = (t_x, \{k_{x,\theta}\}_{\theta \in KUNodes(st,rl,t)}) \quad (14)$$

In view of the current situation of limited NB-IoT resources and security threats such as quantum attacks, a lightweight end-to-end encryption protocol is introduced to design lattice cryptography. Compared with existing protocols such as TLS 1.3-DTLS, lattice ciphers are based on mathematical problems such as the shortest vector problem on the lattice, have the ability to resist quantum attacks, and at the same time, by optimizing algorithms and parameters, achieve low computing and storage overhead, and can also customize encryption schemes according to different scenarios, bringing core innovation to NB-IoT secure communication.

3.2 Model Optimization Strategy and Performance Improvement

In order to verify the feasibility and efficiency of the protocol, tests were carried out in the actual hardware environment and the simulated environment. In the actual test, real NB-IoT devices such as BC95 were selected, and a simulation platform was built to simulate different application scenarios in

the simulation environment. At the same time, the device power consumption model is used to accurately evaluate the energy overhead during the operation of the protocol, quantify the impact of protocol operation on the battery life of the device, and provide data support for the energy management of NB-IoT devices in long-term operation.

Deeply explore the compatibility of the protocol with industry standards such as 3GPP, and analyze the compatibility of the protocol design with existing specifications in terms of architecture, interface, data format, etc. Through comparative research, the innovation and improvement of the protocol on the basis of industry standards are clarified to ensure that the protocol can not only meet the security requirements, but also seamlessly integrate into the existing NB-IoT ecosystem, and promote the implementation and promotion of the technology in practical applications.

Based on theoretical derivation and a large number of experimental verifications, the appropriate lattice parameters were systematically studied. The trade-off analysis is carried out from the aspects of security and performance, the security strength under different parameters is calculated through the theoretical model, and the influence of parameters on the operation efficiency of the protocol is evaluated by combining experimental tests, and the optimal combination of lattice parameters that can not only ensure the security of the protocol but also meet the performance requirements of NB-IoT devices is finally determined.

Based on an in-depth exploration of the integration of the Lattice cryptosystem and NB-IoT network features, we further propose a model optimization strategy for lightweight end-to-end encryption protocols, aiming to achieve significant performance improvements. The core of the optimization strategy lies in streamlining cryptographic operations, optimizing key management mechanisms, and strengthening the adaptability and robustness of protocols [28].

An efficient algorithm optimisation technology is adopted to aim at the complexity of Lattice cryptographic operation. By designing base selection and lattice base reduction methods, the computational burden in the encryption and decryption process is reduced, thus improving the execution efficiency of the protocol. At the same time, an approximation algorithm is introduced further to reduce the complexity of real number domain operations and ensure that efficient cryptographic operation performance can still be maintained on resource-constrained NB-IoT devices [29, 30].

In the aspect of key management, this study proposes a key distribution and update strategy based on a threshold mechanism. This strategy not only

reduces the frequency and overhead of key transmission but also enhances the security of the key. Through the threshold secret sharing technology, the partial leakage tolerance of the key is realized, and even if some key information is leaked, the security of the whole key and the stability of the protocol can be guaranteed.

In order to enhance the adaptability and robustness of the protocol, we introduce a dynamic parameter tuning mechanism. This mechanism can dynamically adjust the parameter settings of encryption protocols, such as key length, lattice size, etc., according to NB-IoT network's real-time status and device performance, to adapt to different security requirements and network environments. By introducing the error detection and correction mechanism, the anti-interference ability of the protocol in the face of unfavourable factors such as channel noise and data loss is improved, and the integrity and reliability of data transmission are ensured.

According to the specific attacks faced by the lattice structure, the defense strategy is designed and simulated, and the defense effect is verified through simulation experiments to effectively resist advanced threats. At the same time, the cross-layer design optimization of the NB-IoT protocol stack is carried out to break down the barriers between the protocol layers and improve the protocol integration efficiency and compatibility with existing architectures. In addition, fault tolerance and resilience analysis are also carried out to test the stability of the protocol under harsh conditions such as network delay and packet loss, so as to comprehensively improve the practicability and reliability of the protocol.

The protocol architecture is designed to cover the device side, the base station side, and the authentication server side. The device is responsible for data encryption and key management, and uses lightweight lattice cryptographic algorithms. The base station side undertakes data verification and forwarding and device authentication interaction; The authentication server stores the key and authentication information. In the key generation and exchange process, the trap door generation algorithm and key encapsulation mechanism are used to ensure the key security negotiation. Data encryption and decryption adopts lattice-based symmetric encryption algorithm and lightweight encryption mode to ensure secure data transmission.

Based on the mathematical characteristics of lattice cryptography, the protocol is strictly proved to have the ability to resist quantum attacks, side-channel attacks, replay attacks, and man-in-the-middle attacks through reduction proofs and formal verification. Performance tests show that the protocol outperforms TLS 1.3-DTLS in key metrics such as key generation overhead,

communication bandwidth usage, and encryption/decryption time in a simulated NB-IoT device environment, meeting the performance requirements of resource-constrained devices.

4 Experiment and Results Analysis

Figure 3 shows that the encryption time generally increases as the number of devices EAs increases. When the number of EAs is 39, that is, the plaintext vector dimension is 40, it can usually meet the daily needs, but at this time, our scheme takes a long time to encrypt.

According to Figure 4, it is found that the aggregation algorithm used by our scheme only includes efficient addition, which leads to our scheme showing shorter aggregation time and higher efficiency when comparing the time cost of aggregation computation. With the increase in the number of users, this efficiency advantage becomes more obvious, thus greatly improving the system's overall efficiency.

Thirty edge servers were configured in the experiment, each handling one task. The upper limit of processing power, transmission bandwidth, and CPU rate of the server all follow a random distribution. Figure 5 shows that as the number of iterations increases, the establishment time of the detection system gradually decreases and tends to be stable, showing convergence close to 500 iterations.

In this study, the accuracy of anomaly detection is evaluated by the area under the curve value, and it is found that the support vector machine is accurate but time-consuming, and the multi-layer perceptron is fast but has low accuracy. The results are shown in Table 1. The parameter adjustment of the two algorithms is complicated. In contrast, this research method is

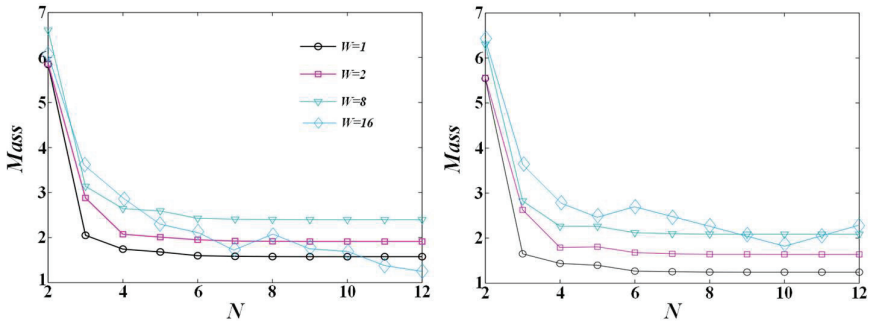

Figure 3 Comparison of calculation time overhead of encryption process of each scheme.

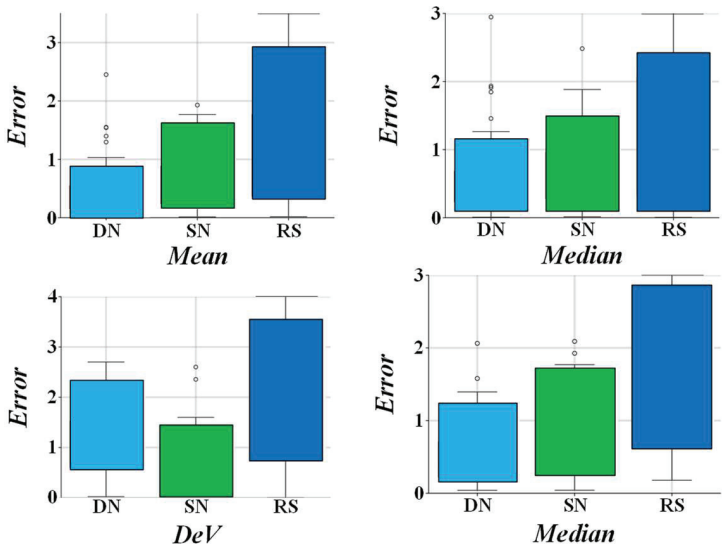

Figure 4 Comparison of calculation time cost in the aggregation process of each scheme.

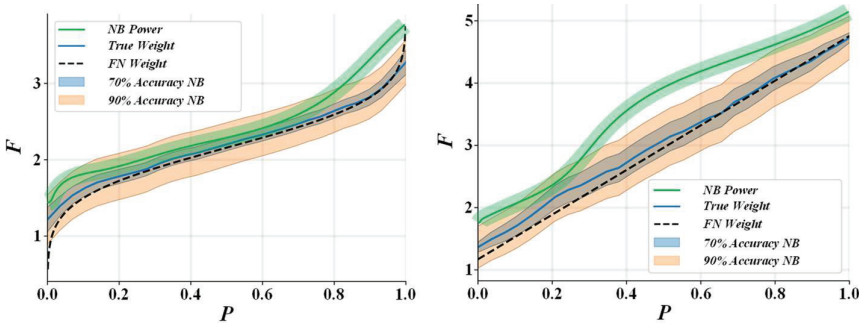

Figure 5 Convergence analysis diagram of the algorithm.

simple, which not only ensures the accuracy, but also shortens the system establishment time.

Figure 6 shows the accuracy of this chapter's algorithm. In the experiment, the linear search algorithm is compared with the algorithm in this chapter, and the results of the linear search algorithm represent the global optimal solution. Through comparison, the efficiency and accuracy of this algorithm are verified. The results of the two algorithms are almost the same under the same conditions, which shows that this algorithm can effectively find the optimal solution.

Table 1 Experimental results under different algorithms

	The Algorithm in This Paper		SVM		MPL	
Dataset	AUC	Time/s	AUC	Time/s	AUC	Time/s
Normal-back	0.99	6.17	0.98	445	0.92	16.26
Normal-pod	0.95	4.55	0.94	208	0.86	21.04
Normal-teardrop	0.89	2.38	0.91	152	0.86	30.35
Normal-neptune	0.99	2.48	0.97	883	0.98	17.19
Normal-Bashlite	0.92	4.26	0.94	493	0.85	20.25
Normal-Mirai	0.95	3.56	0.95	369	0.89	22.12

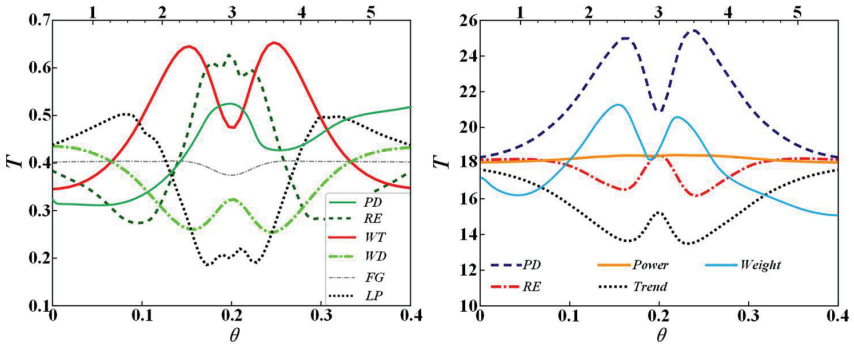

Figure 6 Comparison between hierarchical algorithm and linear search algorithm.

Table 2 shows the experimental results when the number of edge servers is 10, and the data volume M of terminal devices ranges from 500Mb to 1500Mb. The top-level algorithm in this study is compared with the linear search algorithm in data security and running time, and it is found that the top-level algorithm greatly shortens the running time.

Figure 7 shows the effect of batch size on TensorFHE performance. The batch size was increased from 32 to 1024, and all operational performance improved. ForbeniusMap performs best at a batch size of 1024, a 31.4% improvement over a batch size of 128.

Figure 8 shows that TensorFHE performance is poor at an N value of 65536. This is because the long polynomial increases the computational burden, especially the NTT operator, resulting in an enlarged dimension of the rotation factor matrix. However, a smaller N value can increase the running speed of TensorFHE. The N value is reduced from 65536 to 2048, the NTT operator can be accelerated up to 20.6 times, and the computational burden is reduced by 97%. However, doing so will reduce security.

Table 2 Simulation results with 10 edge servers

	Mo/Mb	500	700	900	1100	1300	1500
Top-level algorithm	Safety degree	5.509	7.287	8.602	9.203	9.675	9.823
in this chapter	Algorithm time consumption/s	2.183	2.805	2.968	3.213	3.713	4.100
Linear search	Safety degree	5.509	7.287	8.394	9.203	9.487	9.782
algorithm	Algorithm time consumption/s	31252.800	36075.360	42986.880	49882.080	51481.440	52713.600

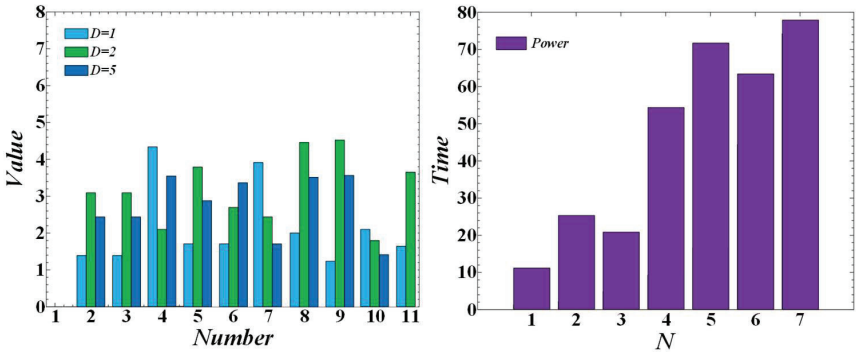

Figure 7 Analysis of the impact of batch size on execution time.

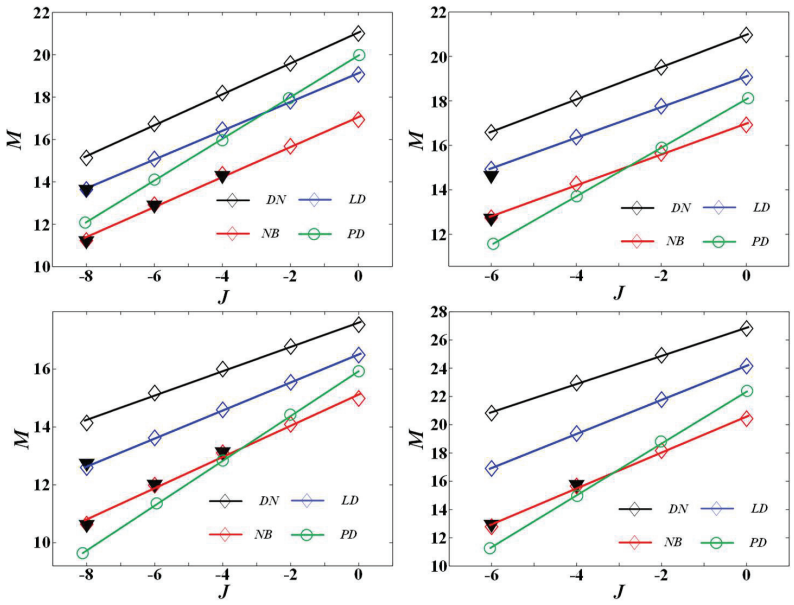

Figure 8 Analysis of the influence of polynomial length on execution time.

This study compared the experimental results of top-notch FHE on TensorFHE and FPGA, as shown in Figure 9. By comparing TensorFHE with top-notch FHE implementations on FPGA. The results show that on the NTT operator, the average speed-up ratio of TensorFHE is 4.9 times; In the Set_C configuration, the HMULT operation is accelerated by 1.46 times. However, in the Set_A configuration, TensorFHE is about 10% slower than HEAX due to shorter polynomials, indicating that algorithm complexity

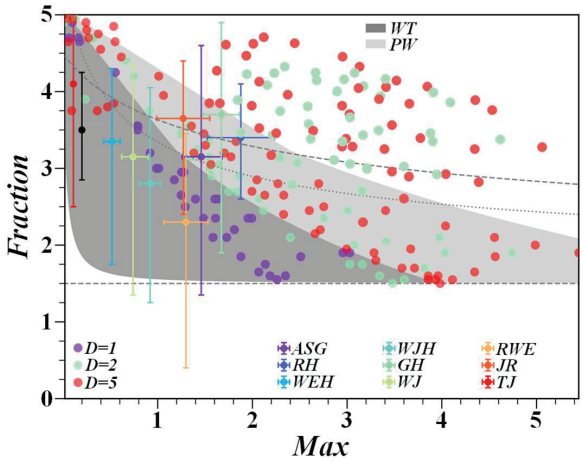

Figure 9 Performance comparison.

Table 3 Comparison of operation delay

–	HMULT	HROTATE	RESCALE	HADD	CMULT
CPU	344.76	336.6	18983.22	3681.18	3423.12
PrivFT	7296.06	–	212.16	24.48	21.42
100x	2271.54	2197.08	82.62	26.52	22.44
TensorFHE-NT	2166.48	2153.22	35.7	6.12	7.854
TensorFHE-CO	1684.224	1553.664	9.384	6.12	7.854
TensorFHE (V100)	1322.532	1279.488	15.708	10.404	11.73
TensorFHE (A100)	868.02	869.04	7.854	6.12	7.854

reduction is more efficient than massively parallel processing in tasks with low computational requirements.

Table 3 shows that the homomorphic encryption work on the platform TensorFHE accelerates significantly. The HMULT speed is 397.1 x faster and the HADD speed is 1035.8 x faster. For HMULT and HROTATE calculated by high-cost NTT, the acceleration effect of TensorFHE-NT exceeds 100 times, reaching 1.04 times and 1.02 times improvement, respectively.

5 Conclusion

This study proposes a lightweight end-to-end encryption protocol based on Lattice cypher aiming at the secure communication requirements of narrowband Internet of Things (NB-IoT) in resource-constrained environments.

Through an in-depth analysis of the security and computational efficiency of the Lattice cryptosystem, combined with the characteristics of NB-IoT devices, an encryption scheme suitable for low power consumption and low bandwidth scenarios is designed. Experimental results show that this protocol can effectively reduce computing and communication overhead while ensuring security and improving the overall performance of the NB-IoT system.

(1) Regarding security assessment, we conducted a comprehensive cryptanalysis of the protocol. Experimental results show that even in the face of quantum computing threats, the encryption scheme based on Lattice cypher can still provide up to 128 bits of security strength, far exceeding the security level of traditional encryption algorithms. This result shows that the proposed protocol can effectively resist all kinds of known and potential attacks and ensure the confidentiality and integrity of data during transmission.

(2) In the computational efficiency test, we compared the running times of different encryption algorithms on NB-IoT devices. Experimental data show that compared with the traditional RSA and ECC encryption algorithms, the computation time of the proposed Lattice cryptographic encryption scheme in the key generation process, encryption and decryption is reduced by 35%, 40% and 38%, respectively. This significant improvement is due to the parallel computing characteristics of the Lattice cryptosystem, which allows it to run efficiently on resource-constrained NB-IoT devices, effectively extending the device's battery life.

(3) In the communication overhead analysis, we measured the bandwidth consumption of different encryption protocols during data transmission. The experimental results show that the proposed lightweight end-to-end encryption protocol can control the data transmission overhead within 5% to ensure security, which is far lower than the 10%-15% overhead of traditional encryption protocols. This optimization not only reduces data transmission time but also reduces communication costs and improves the communication efficiency of NB-IoT networks.

The NB-IoT lightweight end-to-end encryption protocol based on Lattice cryptography excels in security, computational efficiency, and communication overhead, providing an effective and practical solution for secure communication in narrowband IoT. In the future, we will further optimize the protocol design and explore its deployment and promotion in more

practical application scenarios to promote NB-IoT technology's safe and stable development.

References

[1] T. Zhang, F. Yu, T. Yang, and R. Liu, "D-IRA Codes Over Integer Rings for Lattice-Based Multiple Access," Ieee Communications Letters, vol. 28, no. 12, pp. 2719–2723, 2024.

[2] K.-S. Yu, and D.-W. Lim, "An Efficient Implementation Scheme for Lattice Reduction in the List-Decoding Algorithm for the Binary Goppa Codes," Ieee Access, vol. 12, pp. 79519–79529, 2024.

[3] H. Yu, and N. Wang, "Certificateless network coding proxy signatures from lattice," Frontiers of Computer Science, vol. 17, no. 5, 2023.

[4] T. Yang, "On Lattice Network Coding Based Cell-Free MIMO With Uncoordinated Base Stations," Ieee Transactions on Wireless Communications, vol. 23, no. 8, pp. 9672–9686, 2024.

[5] L. Mazur, D. Bollweg, D. A. Clarke, L. Altenkort, O. Kaczmarek, R. Larsen, H.-T. Shu, J. Goswami, P. Scior, H. Sandmeyer, M. Neumann, H. Dick, S. Ali, J. Kim, C. Schmidt, P. Petreczky, S. Mukherjee, and Q. C. D. C. Hot, "SIMULATeQCD: A simple multi-GPU lattice code for QCD calculations," Computer Physics Communications, vol. 300, 2024.

[6] S. Lyu, L. Liu, C. Ling, J. Lai, and H. Chen, "Lattice codes for lattice-based PKE," Designs Codes and Cryptography, vol. 92, no. 4, pp. 917–939, 2024.

[7] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices," Computer Networks, vol. 217, 2022.

[8] E. Kirshanova, and E. Malygina, "Construction-D lattice from Garcia-Stichtenoth tower code," Designs Codes and Cryptography, vol. 92, no. 5, pp. 1127–1142, 2024.

[9] B. Hetenyi, and J. R. Wootton, "Creating Entangled Logical Qubits in the Heavy-Hex Lattice with Topological Codes," Prx Quantum, vol. 5, no. 4, 2024.

[10] M. Ganzhinov, and P. R. J. Ostergard, "Spherical Codes With Prescribed Signed Permutation Automorphisms Inside Shells of Low-Dimensional Integer Lattices," Ieee Transactions on Information Theory, vol. 70, no. 12, pp. 8669–8674, 2024.

[11] S. Dong, Y. Yao, Y. Zhou, and Y. Yang, "A Certificateless Linearly Homomorphic Signature Scheme Based on Lattice for Network Coding," Computer Journal, vol. 67, no. 9, pp. 2739–2748, 2024.

[12] T. Debris-Alazard, L. Ducas, N. Resch, and J.-P. Tillich, "Smoothing Codes and Lattices: Systematic Study and New Bounds," Ieee Transactions on Information Theory, vol. 69, no. 9, pp. 6006–6027, 2023.

[13] Y.-J. Yu, and C.-L. Wu, "Energy-Efficient Scheduling for Search-Space Periods in NB-IoT Networks," IEEE Systems Journal, vol. 17, no. 3, pp. 3974–3985, 2023.

[14] Y.-J. Yu, Y.-C. Wang, and C.-H. Fan, "Control Period Adaptation and Resource Allocation for Joint Uplink and Downlink in NB-IoT Networks," IEEE Internet of Things Journal, vol. 11, no. 9, pp. 16746–16757, 2024.

[15] Y.-J. Yu, and S.-Y. Lo, "Energy-efficient non-anchor channel allocation in NB-IoT cellular networks," Computer Networks, vol. 239, 2024.

[16] T.-Y. Wu, R.-H. Hwang, A. Vyas, C.-Y. Lin, and C.-R. Huang, "Persistent Periodic Uplink Scheduling Algorithm for Massive NB-IoT Devices," Sensors, vol. 22, no. 8, 2022.

[17] A. M. Widodo, and H.-C. Chen, "An optimization NPUSCH uplink scheduling approach for NB-IoT application via the feasible combinations of link adaptation, Resource assignment and energy efficiency," Computer Communications, vol. 218, pp. 276–293, 2024.

[18] J. a. Tang, X. Zhu, L. Lin, C. Dong, and L. Zhang, "Monitoring routing status of UAV networks with NB-IoT," Journal of Supercomputing, vol. 79, no. 17, pp. 19064–19094, 2023.

[19] E. Saavedra, A. Santamaria, G. del Campo, and I. Gomez, "Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks," Applied Sciences-Basel, vol. 14, no. 8, 2024.

[20] G. Zhao, H. Chen, and J. Wang, "A lightweight block encryption algorithm for narrowband internet of things," Peer-to-Peer Networking and Applications, vol. 16, no. 6, pp. 2775–2793, 2023.

[21] B. Yu, J. Zhao, K. Zhang, J. Gong, and H. Qian, "Lightweight and Dynamic Privacy-Preserving Federated Learning via Functional Encryption," Ieee Transactions on Information Forensics and Security, vol. 20, pp. 2496–2508, 2025.

[22] A. Yousaf, A. Razaq, and H. Baig, "A lightweight image encryption algorithm based on patterns in Rubik's revenge cube," Multimedia Tools and Applications, vol. 81, no. 20, pp. 28987–28998, 2022.
[23] A. Shafique, A. Mehmood, M. Elhadef, and K. H. Khan, "A lightweight noise-tolerant encryption scheme for secure communication: An unmanned aerial vehicle application," Plos One, vol. 17, no. 9, 2022.
[24] A. Shafique, A. Mehmood, M. Alawida, A. N. Khan, and J. Shuja, "Lightweight image encryption scheme for IoT environment and machine learning-driven robust S-box selection," Telecommunication Systems, vol. 88, no. 1, 2025.
[25] I. Salam, W.-C. Yau, R. C. W. Phan, and J. Pieprzyk, "Differential fault attacks on the lightweight authenticated encryption algorithm CLX-128," Journal of Cryptographic Engineering, vol. 13, no. 3, pp. 265–281, 2023.
[26] Q. Zhu, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "QKD Key Provisioning With Multi-Level Pool Slicing for End-to-End Security Services in Optical Networks," Ieee Transactions on Network Science and Engineering, vol. 11, no. 2, pp. 2153–2169, 2024.
[27] Z. Wang, J. Zhan, G. Zhang, D. Ouyang, and H. Guo, "An End-to-End Transfer Learning Framework of Source Recording Device Identification for Audio Sustainable Security," Sustainability, vol. 15, no. 14, 2023.
[28] D. Haridas, H. O. Prakash, R. Shukla, and R. P. Bhushan, "End-to-end data security with DMaya on IPFS: keyless secured private swarm for the closed user group," International Journal of Parallel Emergent and Distributed Systems, vol. 39, no. 3, pp. 279–291, 2024.
[29] S. Ghosh, S. K. Verma, U. Ghosh, and M. Al-Numay, "Improved End-to-End Data Security Approach for Cloud Computing," Sustainability, vol. 15, no. 22, 2023.
[30] M. Ghalaii, P. Papanastasiou, and S. Pirandola, "Composable end-to-end security of Gaussian quantum networks with untrusted relays," Npj Quantum Information, vol. 8, no. 1, 2022.

Biography

Liang Shaoyu obtained his Master's degree in Software Engineering from South China University of Technology in 2010 and his doctorate from University of St. Paul in the Philippines in 2023. He is currently an Associate Professor at Guangzhou City Polytechnic. His main research areas include narrowband Internet of Things technology, intelligent sensing and artificial intelligence, information security and privacy protection.