PLOS ONE

RESEARCH ARTICLE

New key management scheme lattice-based for clustered wireless sensor networks

Jiang Zhang*, Qi Liu

The Second Peoples Hospital of Jingdezhen, Jingdezhen, China

* jdzzhangj@163.com

Abstract

Aiming at the quantum algorithm which can solve the problem of large integer decomposition and discrete logarithm in polynomial time, an anti-quantum computing key management scheme for clustered sensor networks is proposed in this paper. The lattice-based cryptosystem is used to achieve the anti-quantum performance of the key management scheme, and the security of the network is further improved through the mutual authentication of sensor network nodes. Due to the limited storage space of sensor nodes, this paper adopts the cluster management of wireless sensor networks, and most sensor nodes only need a small amount of storage space, thus reducing the deployment cost. Cluster management is suitable for medium and large-scale deployment of sensor networks. Because the data traffic is much larger than that of mutual authentication, the sensor nodes in wireless sensor networks use symmetric keys to communicate with each other after mutual authentication, which can effectively improve the communication efficiency in the case of frequent data communication. Experiments show that the authentication scheme based on lattice cryptosystem proposed in this paper will not improve with the continuous improvement of the security level, and its authentication scale will maintain a relatively stable state, while the algorithm scheme based on RSA will increase the authentication cost with the continuous improvement of the security level, so the scheme proposed in this paper is more suitable for application in the environment with high security level. This scheme can effectively reduce the cost of mutual authentication of sensor nodes, is conducive to the expansion of the network, and can ensure the security of authentication between sensor nodes even in the post-quantum era.

Citation: Zhang J, Liu Q (2023) New key management scheme lattice-based for clustered wireless sensor networks. PLoS ONE 18(8): e0290323. https://doi.org/10.1371/journal.pone.0290323

Editor: Raman Singh, University of the West of Scotland, UNITED KINGDOM

Received: April 2, 2023

Accepted: August 3, 2023

Published: August 30, 2023

Data Availability Statement: DOI:10.5061/dryad.jh9w0vtgw.

Funding: This article was supported by the grant from the Third (03) Specific Project of Jiangxi Province Grant Number [20212ABC03W03]. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing interests: The authors have declared that no competing interests exist.

1. Introduction

Wireless sensor network integrates micro-electric technology, sensor technology and communication technology, and can be widely used in education, military, medical, transportation and other fields [1–5]. The security problems of wireless sensor networks come from the characteristics of wireless communication, the strict limitation of sensor node resources and the extensive and dense distribution area of sensor networks. Therefore, it is urgent to ensure the security of wireless sensor networks [6–9]. In 2016, Mehmood et al. A secure inter-cluster multi-key distribution scheme for wireless sensor networks is proposed [10]. In 2017, Zhang

et al. A key establishment scheme for wireless sensor networks based on polynomial and random key pre-distribution scheme is proposed [11]. In 2022, Kumar et al. The cryptanalysis and improvement of mutual authentication protocol for real-time data access in industrial wireless sensor networks are proposed [12]. At the end of last century, Shor proposed a quantum algorithm to solve the problem of large integer decomposition and discrete logarithm in polynomial time, which made the research of cryptosystem against quantum computing attacks received great attention. At present, the development of special quantum computer is very rapid, and the solving time of traditional mathematical difficult problems such as large integer decomposition and discrete logarithm has reached the order of minutes, which brings a great threat to the classical encryption algorithms based on this kind of difficult problems. Post-quantum cryptography algorithm plays an important role in the security protection of user information in distributed systems in the quantum era when general quantum computers are widely used in the future. Among them, lattice cryptosystem has been concerned and studied by many scholars in recent years because of its advantages in efficiency and security [13–18]. Lattice cipher is a more practical post-quantum cryptographic algorithm [19–22].

1.1. Related work

In 2018, Mehmood et al. proposed a novel secure session key establishment scheme for wireless body area networks in the medical field. In the proposed scheme, in order to address the important issues of security and patient information privacy in wireless body area networks in medical applications, session keys are established for a specific period of time in order to securely communicate information related to patient health vital signs. Important data, ensuring the security and privacy of vital signs related to the human body [23]. In 2019, Bootle et al. proposed the algebraic techniques for short exact lattice-based zero-knowledge argument of knowledge systems [24]. In 2020, Mehmood et al. proposed an energy-efficient and reliable trust-based communication scheme for remote patient monitoring in wireless body-area networks, where trust and privacy-preserving enforcement is critical as important parameters are communicated to remote locations. In WBAN, trust among stakeholders is very important and is considered as a critical success factor for the reliability of information exchange between them [25]. In 2021, Lyubashevsky et al. proposed a shorter lattice-based zero-knowledge argument of knowledge systems via one-time commitments [26]. In 2021, Mehmood et al. proposed an efficient and secure session key management scheme for wireless sensor networks is proposed. In the proposed scheme, the main steps of public-key encryption in asymmetric cryptosystems are minimized, and most public-key encryption operations are based on symmetric-key encryption. This solution can greatly reduce the energy consumption of the wireless sensor network and ensure better security [27]. In 2022, Mehmood et al. proposed a Mobile Agent-Based Energy-Efficient Data Aggregation Scheme for Wireless Body Area Networks. Among the proposed schemes, reliable data aggregation in WBAN is very important to ensure data delivery as soon as possible in healthcare applications. This scheme solves the shortcoming of client-server sending data, and the mechanism of mobile agent proposed in this scheme proves to be a more feasible solution [28]. In 2023, Dharminder et al. [29] an efficient lattice-based authenticated key exchange protocol using a ring-based learning assumption with errors is designed for IoT smart devices, which is robust to different attacks.

In practical applications, most of the existing wireless sensor network key management schemes are based on traditional cryptographic systems such as large integer decomposition and discrete logarithm problems. In the quantum era when general-purpose quantum computers are popularized in the future, these algorithms will pose a huge threat. Therefore, it is necessary to study how to combine sensor network technology with anti-quantum attack

technology, so that wireless sensor networks have the security against quantum computing attacks, and design and optimize the deployment scheme of sensor nodes according to the application scenarios of wireless sensor networks to reduce the deployment time. cost and improve communication efficiency. This paper studies the security protocol based on lattice cryptography, which can provide ideas for the security of wireless sensor networks and better protect the privacy data security of wireless sensor networks.

1.2. Overview of the paper

In practical applications, most of the existing key management is based on traditional cryptosystems such as large integer decomposition and discrete logarithm problems. In the future quantum era of universal quantum computers, these algorithms will pose a great threat. Therefore, it is necessary to research and develop a negotiation method and system based on key update in the post-quantum era. The rest of the paper is organized as follows: in Section 2, we introduce some basic concepts and algorithms of lattice schemes. In Section 3, we give our network model. In Section 4, we proposed a key management scheme. In Section 5, we analyze the correctness, security. In Section 6, finally, we summarize the key management scheme.

2. Preliminaries

Definition 2.1. ([30]). Let Λ be an n-dimensional lattice and $\varepsilon>0$. Then, the smoothing parameter $\eta_{\varepsilon}(\Lambda)$ is the smallest real $s>0$ such that $\rho_{\frac{1}{\sqrt{2\pi}s}}(\Lambda^{*}\backslash\{0\}) \leq \varepsilon$.

Lemma 2.2 ([30]). For any n-dimensional lattice Λ with basis B and $\varepsilon>0$, we have:

$$\eta_{\varepsilon}(\Lambda) \leq \|\tilde{B}\| \cdot \sqrt{\ln(2n/(1+1/\varepsilon))/\pi}$$

Lemma 2.3 ([31]). Let $m,k>1$, Λ be m-dimensional lattice and $c\in Z^{m}$. Then:

$$\Pr_{Z} \leftarrow D_{\sigma}[|z| > k\sigma] \leq 2e^{\frac{-k^{2}}{2}}$$

$$\Pr_{Z} \leftarrow D_{\sigma}^{m}[\|z\|_{2} > k\sigma\sqrt{m}] \leq k^{m}e^{\frac{m}{2}(1-k^{2})}$$

$$\Pr_{Z} \leftarrow D_{\Lambda,\sigma,c}^{m}[\|z\|_{2} > k\sigma\sqrt{m}] \leq 2k^{m}e^{\frac{m}{2}(1-k^{2})}$$

Lemma 2.4 ([31]). Let $Q\in Z^{m\times n}$ and Λ be an n-dimensional lattice. Then, for any $\sigma \in R_{>0}^{m}$ and $s\in R^{m}$ we have:

$$\frac{\rho_{\sigma}(s)}{\sum_{z\in\Lambda}\rho_{\sigma}(Qz)} \leq \frac{\rho_{\sigma}(s)}{\sum_{z\in\Lambda}\rho_{\sigma}(s+Qz)} \leq \frac{1}{\sum_{z\in\Lambda}\rho_{\sigma}(Qz)}$$

Theorem 2.5 ([32]). Let $A\in Z^{n\times m}$ and $W\in Z^{k\times m}$ be arbitrary matrices and denote $w_{i}\in Z^{m}$ to be the i-th row of W. Furthermore, suppose $\sigma=(\sigma_{1},\sigma_{2},\cdots,\sigma_{k})$ satisfies for $\sigma_{i} \geq q^{n/m}\sqrt{\frac{ek}{m}}\|w_{i}\| + 2$. Then, for any $s\in R^{k}$, we have:

$$\frac{\rho_{\sigma}(s)}{\sum_{z\in\Lambda_{q}^{\perp}(A)}\rho_{\sigma}(s+Wz)} \leq \frac{1}{2}$$

Definition 2.6 Module-SIS(MSIS$_{n,m,B}$) ([31]). Given $A \leftarrow R_{q}^{n\times m}$, the Module-SIS problem with parameters $n,m>0$ and $0<B<q$ asks to find $z \in R_{q}^{m}$ such that $Az=0$ over R_{q} and

$0<\|z\|<B$. An algorithm ψ is said to have advantages ϵ in solving $\mathrm{MSIS}_{n,m,B}$ if:

$$\Pr[0 < \|z\| < B \wedge Az = 0 | A \leftarrow R_q^{n\times m}; z \leftarrow \psi(A)] \geq \epsilon$$

Definition 2.7 ($\mathrm{MLWE}_{n,m,\chi}$) ([32]). Given $A \leftarrow R_q^{n\times m}$, a secret vector $s \leftarrow \chi^m$ and error vector $e \leftarrow \chi^n$, the Module-LWE problem with parameters $n,m>0$ and an error distribution χ over R asks the adversary ψ to distinguish between the following the cases: $(A,As+e)$ for A. Then, ψ is said to have advantages ϵ in solving $\mathrm{MLWE}_{n,m,\chi}$ if

$$|\Pr[b = 1 | A \leftarrow R_q^{n\times m}; s \leftarrow \chi^m; e \leftarrow \chi^n; b \leftarrow \psi(A, As + e)]$$

$$-\Pr[b = 1 | A \leftarrow R_q^{n\times m}; \mathrm{b} \leftarrow R_q^n; b \leftarrow \psi(A, \mathrm{b})]| \geq \epsilon$$

Lemma 2.8 (Lattice Trapdoors [30]). $\mathrm{TrapSamp}(1^n,1^m,q)$. That, given any integers $n\geq 1$, $q\geq 2$, and sufficiently large $m = \Omega(n\log q)$, outputs a matrix $A \in Z_q^{n\times m}$ and a trapdoor matrix $T \in Z^{n\times m}$ such that the distribution of A is $negl(n)$-close to uniform.

Lemma 2.9 ([33]). Let n, p be positive integers. Let Λ be a lattice of rank n, and let $V = [-p, p]^n$. Let $T = p\sqrt{5n(1+\delta)/8}$, where

$$\delta = \sqrt{\frac{32(\lambda+1)}{25n\log_2 e}}.$$

Define h the distribution obtained by sampling α from $[-p,p]$ and s from ψ_1^n and outputting $v = \alpha \cdot s$. Further, let $M>1$, $t = \sqrt{(\lambda+2)/(\pi\log_2 e)}$ and definitely

$$\sigma_{\min} = \left(-t + \sqrt{\frac{t^2 + \ln(M)}{\pi}}\right)^{-1} \cdot T.$$

Let $\sigma \geq \sigma_{\min}$. We now define two distributions P_1: Sample $v \leftarrow h$ and $y \leftarrow D_{\Lambda,\sigma}$. Define $z = \mathbf{y} + v$. Output (v, z) with probability

$$\min\left(1, \frac{D_{\Lambda,\sigma}(z)}{M \cdot D_{\Lambda,\sigma}(z-v)}\right).$$

P_2: Sample $v \leftarrow h$ and $z \leftarrow D_{\Lambda,\sigma}$. Output (v, z) with probability $1/M$.

Then, it holds that P_1 outputs something with probability at least $(1-2^{-\lambda})/M$, and that

$$\Delta(P_1, P_2) \leq 2^{-(\lambda+1)}(1 + 1/M) \leq 2^{-\lambda}.$$

3. Network model

Wireless sensor networks generally have two kinds of topologies: planar structure and hierarchical structure. All the nodes in the flat structure network are equal, and there is no bottleneck in principle, so it is relatively robust. However, its biggest disadvantage is that the network size is limited, the routing maintenance cost is high, and the energy consumption is relatively high. In the hierarchical structure, the network is divided into clusters, and each cluster is composed of a cluster head node and multiple cluster members, so it is also called heterogeneous network. Cluster head nodes form a higher-level network, which is responsible for the collection and forwarding of data between clusters. The use of cluster structure can reduce the energy cost caused by transmission and is conducive to network expansion. In this method, the

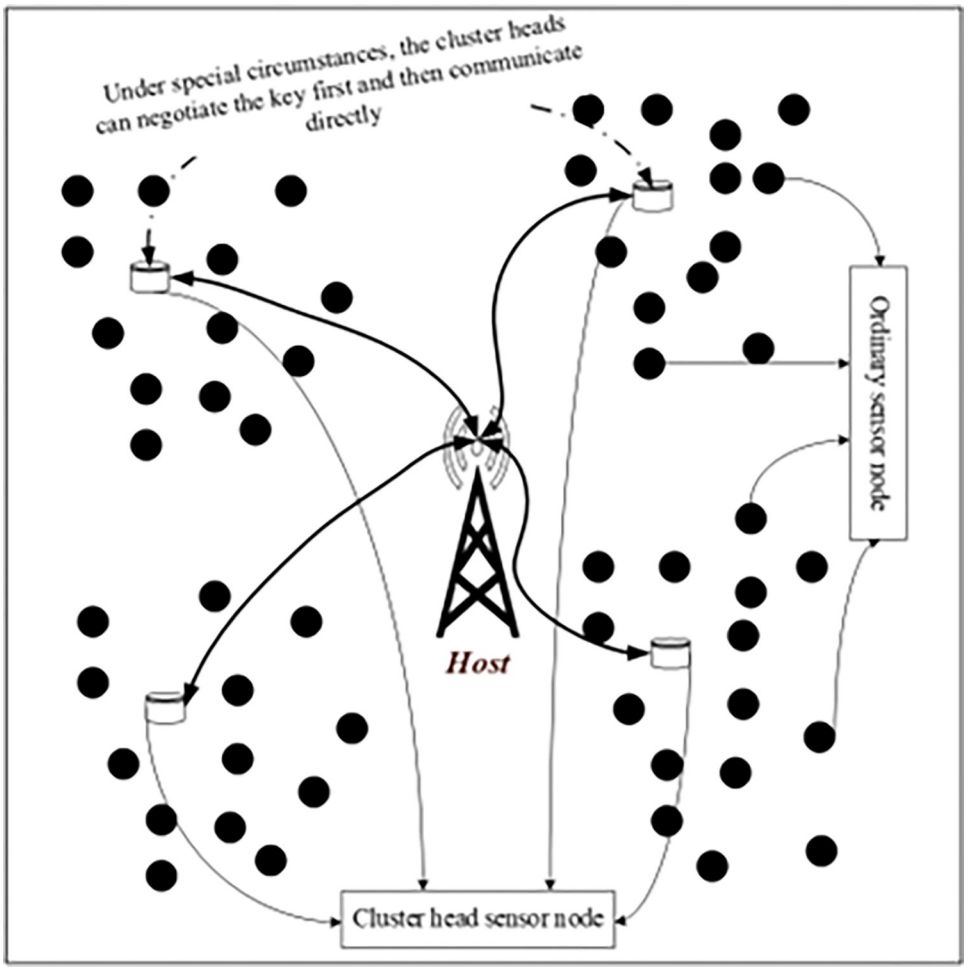

Fig 1. Wireless sensor network model.

https://doi.org/10.1371/journal.pone.0290323.g001

clustered wireless sensor network model will be used to manage the key of the sensor nodes. The sensor network model is shown in Fig 1.

In this paper, an anti-quantum key management method for clustered sensor networks is proposed. The details include:

1. This paper assumes that each cluster head sensor node is assigned its own identity and a pair of public and private keys based on lattice public key cryptosystem. The cluster head sensor node plays a key role in the network, which can communicate directly with the host, collect the information sent by the ordinary sensor node in the cluster and forward it to the host.
2. All sensor nodes in each cluster communicate securely through the symmetric key shared by the cluster, and the ordinary sensor nodes in the cluster can communicate directly. Indirect communication can be carried out through the cluster head and the host or sensor node outside the cluster.
3. When the cluster head sensor node finds that the communication key is not secure, it should deal with it in time and redistribute the new communication key through the host.

4. In special cases, the cluster head sensor node can also communicate directly by negotiating the communication key. In order to further enhance the security of the symmetric key used for communication, the aging of the symmetric key can be specified, which will be invalidated automatically if it exceeds the specified time period.

4. Key management scheme

In the anti-quantum key management method for clustered sensor networks proposed in this scheme, the trusted third-party security host generates the system security parameters needed for the key management scheme. then the identity and public-private key pairs of each cluster head sensor node are generated by these security parameters, and the privacy information is pre-distributed to the corresponding cluster head sensor nodes. The cluster head sensor node plays a key role in the network, collecting the information sent by the ordinary sensor node in the cluster and forwarding it to the host. The sensor nodes in each cluster communicate securely through the symmetric key shared in the cluster, and the ordinary sensor nodes in the cluster can communicate directly. Indirect communication can be carried out through the cluster head and the sensor nodes outside the cluster. When both sides of the communication feel threatened, the cluster head sensor node can also communicate directly by negotiating the communication key. In order to further improve the security of the symmetric key used for communication, the scheme proposed in this paper stipulates that if the specified period of time is exceeded, the symmetric key will automatically expire and the new communication key will be redistributed through the host.

The key management scheme involves a few parameters: a prime q_1 and prime q modulus, $q,q_1 \geq 2$ and integer dimensions $n,k,d,\tau,\lambda \geq 1$. The key management scheme will be generated as shown in the following:

4.1. Sensor node identity and key distribution

1. Distribution of public and private key pairs, communication keys and identification of *Host* (Host) and cluster head sensor nodes
    1. Choose a random public matrix $A \in Z_q^{n\times m}$.
    2. Choose random parameter x: $x_i \leftarrow \{-\tau,\cdots,\tau\}^n$, $i = 1,2,\cdots,Q,h$, where i, h and Q represents the i-th cluster head sensor node, h represents the *Host* and total number of cluster head sensor node respectively.
    3. Compute: $y_i^T = x_i^T \cdot A \mathrm{mod} q$, $i = 1,2,\cdots,Q,h$.
    4. The public key of the *Host* is (A,y_h), the private key of the *Host* is x_h, identification of the *Host* is ID_h.
    5. The public key of the i-th cluster head sensor node is (A,y_i), the private key of of the i-th cluster head sensor node is x_i.
    6. The identification of C^i (the i-th cluster head sensor node) is ID_i, where $ID_i \in \{0,1\}^n, i = 1,2,\cdots,Q$.
    7. The communication key of each cluster head sensor node is k_i, $i = 1,2,\cdots,Q$, which is the symmetric key of some traditional symmetric cryptosystem (RSA encryption system, etc.).

2. Distribution of public and private key pairs, communication keys and identification of ordinary sensor nodes

1. The identification of C_j^i (the i-th ordinary sensor node) is ID_i, $ID_j^i \in \{0,1\}^n, i = 1,2,\cdots,Q, j = 1,2,\cdots,Q_i$, where, i represents that the ordinary sensor node belongs to the i-th cluster, j represents that the ordinary sensor node is the j-th sensor node in the i-th t cluster, and Q_i represents the total number of ordinary sensor nodes in the i-th cluster.
2. The communication key of the ordinary sensor node in each cluster is k_i, i = 1,2,$\cdots$,Q, where, i represents the i-th cluster.
3. The public key of the ordinary sensor node in each cluster is (A,y_i), which is the public key of the i-th cluster head sensor node.

4.2. Communication key invalidation

Assuming that the communication key of the i-th cluster is a failure (including various cases such as theft, etc.), the i-th cluster head sensor node immediately broadcasts a communication key failure information to all sensor nodes in the i-th cluster, and re-authenticates and negotiates the new communication key with the host. Finally, the negotiated new communication key is peer-to-peer sent to the valid sensor node in the i-th cluster. The specific process of renegotiating the new communication key with:

1) First of all, it is necessary to carry out mutual authentication, the authentication process of *Host* to C^i

The i-th cluster head sensor node C^i:

1. Input the public key (A,y_i), the private key x_i, and identification ID_i.
2. Choose random parameter: $\theta_i \leftarrow \{-\tau,\cdots,\tau\}^m$.
3. Compute: $\eta = \theta_i^T \cdot x_i^T \cdot q_1 + ID_i^T \bmod q$
4. Choose a hash function H:

$$H : \{0,1\}^* \rightarrow \{v_1 : v_1 \in \{0,1\} \quad \}.$$

5. Compute: $\mu_i = H(ID_i^T \cdot A)$.
6. Compute: $\eta' = \theta^T \cdot y_i^T \cdot q_1 \bmod q$.
7. Output the signature message (η,η',μ_i), and C^i send the signed message (η,η',μ_i) to *Host*. Otherwise, return to regenerate the signature.

The verification process of Host:

1. Input the public key (A,y_i), the signature message (η,η',μ_i), and the identification ID_i.
2. Compute: $\mu_i' = H(\eta \cdot A - \eta' \bmod q)$.
3. Verification: $\mu_i' \stackrel{?}{=} \mu_i$.

If the above equation is true and the authentication process of *Host* to C^i is successful, proceed to the next step, otherwise terminate the key negotiation process.

2) The authentication process of C^i to *Host*

The host Host:

1. Input the public key (A,y_h), the private key x_h, and identification ID_h.
2. Choose random parameter: $\theta_h \leftarrow \{-\tau,\cdots,\tau\}^m$.
3. Compute: $\eta_h = \theta_h^T \cdot x_h^T \cdot q_1 + ID_h^T \mathrm{mod} q$
4. Compute: $\mu_h = H(ID_h^T \cdot A)$.
5. Compute: $\eta_h^{'} = \theta_h^T \cdot y_h^T \cdot q_1 \mathrm{mod} q$.
6. Output the signature message $(\eta_h, \eta_h^{'}, \mu_h)$, and *Host* send the signed message $(\eta_h, \eta_h^{'}, \mu_h)$ to C^i. Otherwise, return to regenerate the signature.

The verification process of C^i:

1. Input the public key (A,y_h), the signature message $(\eta_h, \eta_h^{'}, \mu_h)$, and the identification ID_h.
2. Compute: $\mu_h^{'} = H(\eta_h \cdot A - \eta_h^{'} \mathrm{mod} q)$.
3. Verification: $\mu_h^{'} \stackrel{?}{=} \mu_h$.

If the above equation is true and the authentication process of *Host* to C^i is successful, proceed to the next step, otherwise terminate the key negotiation process.

3) The *Host* reassigns a new communication key

The *Host* generates a new communication key $k_i^{'}$, encrypts $k_i^{'}$ with its own private key x_h, and then sends the encrypted message $(m_k, m_k^{'}, k_H)$ to the i-th cluster head sensor node C^i. After receiving the message from the host, C^i decrypts the message $(m_k, m_k^{'}, k_H)$ with the public key (A,y_h) of the *Host*. After decryption, the i-th cluster head sensor node C^i obtains a new communication key $k_i^{'}$, and the i-th cluster head sensor node can securely communicate with the *Host* with the new communication key $k_i^{'}$. The specific process is as follows:

The encryption process of Host:

1. Input the public key (A,y_i) of C^i and the new communication key $k_i^{'}$.
2. Choose random parameters: $\theta_k \leftarrow \{-\tau,\cdots,\tau\}^m$, $e \leftarrow \{-\tau,\cdots,\tau\}^n$, $e' \leftarrow \{-\tau,\cdots,\tau\}$.
3. Compute: $m_k = q_1 \cdot A \cdot \theta_k + q_1 \cdot e \mathrm{mod} q$.
4. Choose a random message $k_i^{'}$: $k_i^{'} \in \{0,1\}^*$.
5. Compute: $k_H = H(k_i^{'})$.
6. Compute: $m_k^{'} = q_1 \cdot y_i^{\mathrm{T}} \cdot \theta_k + q_1 \cdot e^{'} + k_i^{'} \mathrm{mod} q$.
7. Output the ciphertext message $(m_k, m_k^{'}, k_H)$, and *Host* send the signed message $(m_k, m_k^{'}, k_H)$ to C^i.

The decryption process of C^i:

1. Input the private key x_i, the ciphertext message $(m_k, m_k^{'}, k_H)$.
2. Compute: $k_H^{'} = H((m_k^{'} - x_i^{\mathrm{T}} \cdot m_k \mathrm{mod} q) \mathrm{mod} q_1)$.
3. Verification: $k_H^{'} \stackrel{?}{=} k_H$.

If the above equation is true and the decryption process is successful, C^i get a new communication key $k_i^{'}$: $k_i^{'} = (m_k^{'} - x_i^{\mathrm{T}} \cdot m_k \mathrm{mod} q) \mathrm{mod} q_1$. Otherwise, decryption fails.

4) ***C*^{i} assign a new communication key for the *i*-th cluster**

The *i*-th cluster head sensor node encrypts the new communication key $k_i^{'}$ with its own private key x_i: and then sends the ciphertext message $(m_i, m_i^{'}, k_i)$ point to point to all valid ordinary sensor nodes of the *i*-th cluster. After receiving the message from the *i*-th cluster head sensor node, the ordinary sensor node of the *i*-th cluster decrypts the ciphertext message $(m_i, m_i^{'}, k_i)$ with the public key of the *i*-th cluster head sensor node. After decryption, the ordinary sensor node of the *i*-th cluster obtains a new communication key $k_i^{'}$, and the specific process of encryption and decryption has referred to the process of *Host* reassigns a new communication key. Finally, the new communication key $k_i^{'}$ can be used to communicate securely with all sensor nodes (including cluster head nodes) of the *i*-th cluster.

4.3. Cluster head node key negotiation process

The communication key is not distributed between the cluster heads, because in general, the cluster heads do not communicate directly. If the cluster head sensor nodes in special cases must communicate directly, they can first authenticate each other and negotiate the communication key between each other. Suppose that the *i*-th cluster head sensor node and the *j*-th cluster head sensor node needs to communicate directly, and the negotiation process is as follows:

1. The *i*-th cluster head sensor node and the *j*-th cluster head sensor node authenticate each other, and the mutual authentication process is referred to the first two steps of communication key invalidation steps. If the authentication is successful, proceed to the next step, otherwise the key negotiation process is terminated.
2. The key agreement process between the *i*-th cluster head sensor node and the *j*-th cluster head sensor node the last step of communication key invalidation steps.
3. Finally, the *i*-th cluster head sensor node and the *j*-th cluster head sensor node obtains the communication key $k_{i \Leftrightarrow j}$, through the process of mutual authentication and negotiation, and the *i*-th cluster head sensor node and the *j*-th cluster head sensor node can communicate securely with the communication key $k_{i \Leftrightarrow j}$ directly.

5. Analysis

5.1. Correctness

The correctness of the decryption in the key management scheme follows from our choice of parameters. Specifically, to show correctness, we follow the proof strategy from [32], we first compute $k_i^{'} = (m_k^{'} - x_i^{\mathrm{T}} \cdot m_k \mathrm{mod} q) \mathrm{mod} q_1$. We have:

$$k_i^{'} = (m_k^{'} - x_i^{\mathrm{T}} \cdot m_k \mathrm{mod} q) \mathrm{mod} q_1$$

$$= ((q_1 \cdot y_i^{\mathrm{T}} \cdot \theta_k + q_1 \cdot e^{'} + k_i^{'} - x_i^{\mathrm{T}} \cdot (q_1 \cdot A \cdot \theta_k + q_1 \cdot e)) \mathrm{mod} q) \mathrm{mod} q_1$$

$$= ((q_1 \cdot y_i^{\mathrm{T}} \cdot \theta_k - q_1 \cdot x_j^{\mathrm{T}} \cdot A \cdot \theta_k + q_1 (e^{'} + x_i^{\mathrm{T}} \cdot e) + k_i^{'}) \mathrm{mod} q) \mathrm{mod} q_1$$

$$= ((q_1 \cdot (e^{'} + x_i^{\mathrm{T}} \cdot e) + k_i^{'}) \mathrm{mod} q) \mathrm{mod} q_1$$

Since we assumed $(n \cdot d \cdot \tau + 1) \leq \frac{q}{2q_1} - \frac{1}{2}$ and $\|k_i^{'}\|_\infty \leq q_1/2$, then $\|q_1 \cdot (e^{'} + x_i^{\mathrm{T}} \cdot e) + k_i^{'}\|_\infty \leq q_1/2$, therefore there is no reduction modulo q_1 in $q_1 \cdot (e^{'} + x_i^{\mathrm{T}} \cdot e) + k_i^{'}$ and hence

$$k_i^{'} = ((q_1 \cdot (e^{'} + x_i^{\mathrm{T}} \cdot e) + k_i^{'}) \mathrm{mod} q) \mathrm{mod} q_1 = k_i^{'}.$$

Then

$$k_H^{'} = H(k_i^{'}) = k_H$$

The correctness of the signature in the scheme follows from our choice of parameters. Specifically, to show correctness, we first compute $\mu_H = \eta \cdot A - \eta^{'} \mathrm{mod} q$. We have:

$$\mu_H = \eta \cdot A - \eta^{'} \mathrm{mod} q$$

$$= ((\theta_i^T \cdot x_i^T \cdot q_1 + ID_i^T) \cdot A - \theta^T \cdot y_i^T \cdot q_1) \mathrm{mod} q$$

$$= (\theta_i^T \cdot x_i^T \cdot A \cdot q_1 + ID_i^T \cdot A - \theta^T \cdot y_i^T \cdot q_1) \mathrm{mod} q$$

$$= (\theta^T \cdot y_i^T \cdot q_1 + ID_i^T \cdot A - \theta^T \cdot y_i^T \cdot q_1) \mathrm{mod} q$$

$$= ID_i^T \cdot A \mathrm{mod} q$$

Hence

$$\mu_i^{'} = H(\eta \cdot A - \eta^{'} \mathrm{mod} q) = H(\mu_H) = H(ID_i^T \cdot A \mathrm{mod} q) = \mu_i.$$

5.2. Security

Unforgettability: a successful interaction between the signer and the user can only generate a legitimate signature. Here, it is proved that if there is an adversary $\mathcal{A}$ with the ability to resist unforgeable attacks, then the *MLWE* difficult problem can be solved in the polynomial time algorithm. That is, assuming that there is an adversary $\mathcal{A}$ who can successfully forge a valid message signature with a non-negligible probability δ, then a valid solution to the *MLWE* difficult problem can be found in polynomial time:

***Proof*:** first of all, it is emphasized that the output of the proposed signature authentication scheme is independent of the signature key. For the two main output hashes in the scheme and the signature of the message to be signed, the adversary $\mathcal{A}$ queries the two algorithms. Once the opponent has the ability to resist unforgeable attacks, the challenger T will be able to solve the *MLWE* difficult problems.

***Hash query*:** the challenger T creates an initially empty list L_H to store the hash query value for the message $ID_i^T \cdot A \mathrm{mod} q$. When the challenger T receives a hash query about the message from the adversary $\mathcal{A}$, the challenger T first checks the list L_H to see if the message has been queried. If queried, the message and hash result pair $(ID_i^T \cdot A \mathrm{mod} q, H(ID_i^T \cdot A \mathrm{mod} q))$ is sent to the adversary $\mathcal{A}$, otherwise, the challenger T runs the algorithm to regenerate the hash value $(ID_i^T \cdot A \mathrm{mod} q, H(ID_i^T \cdot A \mathrm{mod} q))$ of a message $ID_i^T \cdot A \mathrm{mod} q$, sends the result to the adversary $\mathcal{A}$, and stores the message and hash result pair $(ID_i^T \cdot A \mathrm{mod} q, H(ID_i^T \cdot A \mathrm{mod} q))$ in the list L_H.

1. Choose random parameters: $\theta_i \leftarrow \{-\tau, \cdots, \tau\}^m$.

2. Compute: $\eta = \theta_i^T \cdot x_i^T \cdot q_1 + ID_i^T \mathrm{mod} q$.
3. Compute: $\mu_i = H(ID_i^T \cdot A)$.
4. Compute: $\eta^{'} = \theta^T \cdot y_i^T \cdot q_1 \mathrm{mod} q$.
5. Compute: $\mu_H = \eta \cdot A - \eta^{'} \mathrm{mod} q$.
6. Compute: $\mu_i^{'} = H(\mu_H)$.
7. Verification: $\mu_i^{'} \stackrel{?}{=} \mu_i$.

Forgery: suppose $\mu_{H,j}$ is the result of a hash query returned to the adversary $\mathcal{A}$, which can be obtained for two different signature pairs $(\eta, \eta^{'}, \mu_{H,j})$ and $(\eta^*, \eta^{'*}, \mu_{H,j}^*)$, then $H(\eta \cdot A - \eta^{'} \mathrm{mod} q) = H(\eta^* \cdot A - \eta^{'*} \mathrm{mod} q)$. Because $\eta \neq \eta^*$ and $\eta \cdot A - \eta^{'} \neq \eta^* \cdot A - \eta^{'*}$, there will have a hash collision. But the hash collision can hardly happen because of the collision resistance of the hash function. Therefore, it can be obtained with a higher probability $\eta = \eta^*$ and $\eta \cdot A - \eta^{'} = \eta^* \cdot A - \eta^{'*}$, then, $\mu_{H,j} = \mu_{H,j}^*$. Finally, it can be claimed that the *MLWE* difficult problem has been successfully solved, the detailed process is as follows:

The $\mu_{H,j}$ is assumed that the challenger returns the result of the hash query to the adversary $\mathcal{A}$. For the signature of the message $(\eta^*, \eta^{'*}, \mu_H^*)$, select different random values $\mu_{H,j}^*, \mu_{H,2}^*, \cdots, \mu_{H,s}^* \leftarrow D_\kappa^n$. The probability of $\mu_{H,j} \neq \mu_{H,j}^*$ can be obtained:

$$\Pr(\mu_{H,j} \neq \mu_{H,j}^*) = (\delta - 1/D_\kappa^n) \times (\frac{\delta - 1/D_\kappa^n}{t} - 1/D_\kappa^n)$$

Therefore, the adversary $\mathcal{A}$ can forge a new signature $(\eta^*, \eta^{'*}, \mu_{H,j}^*)$ and $\eta \cdot A - \eta^{'} = \eta^* \cdot A - \eta^{'*}$ according to the system parameter setting of the signature authentication scheme, the following equation can be obtained:

$$(\eta^{'} - \eta^{'*}) \mathrm{mod} q = (\eta - \eta^*) \cdot A \mathrm{mod} q.$$

Due to $(\eta^{'} - \eta^{'*}) \mathrm{mod} q = (\eta - \eta^*) \cdot A \mathrm{mod} q$, then:

$$\mu_i = H(\eta \cdot A - \eta^{'} \mathrm{mod} q) = H(\eta^* \cdot A - \eta^{'*} \mathrm{mod} q) = \mu_i^{'*}.$$

Next, $(n \cdot d \cdot \tau + 1) \leq \frac{q}{2q_1} - \frac{1}{2}$ and $\|k_i^{'}\|_\infty \leq q_1/2$ can be obtained with a non-negligible probability, that is, a solution of the *MLWE* difficult problem is solved in the polynomial time.

However, because the *MLWE* difficult problem can't be solved in polynomial time, the assumption of adversary $\mathcal{A}$ is not valid. Therefore, the proposed signature authentication of key management scheme satisfies the unforgeability in the random prophecy model.

5.3. Efficiency analysis

In this section, we mainly focus on the algorithm computational complexity between our lattice-based key management protocol and other related secret key protocols, ref. [4] protocol, ref. [15] protocol and ref. [20] protocol. The test environment of this scheme is that the Intel Core i7-12700 processor is configured with 32G-DDR4 memory, the operating system is Windows10; test programming language is Python3.9, and the code function is implemented by PyCryptodome library. The results are shown in Table 1.

According to the above analysis, the message authentication size of the proposed authentication protocol is $m\log(12\sigma)$, which is only related to the message m and the parameter σ. The authentication sizes corresponding to different security levels (such as 64bits, 128bits, 192bits,

Table 1. Comparison with RSA and ECC algorithms.

Security level	RSA algorithm	ECC algorithm	Our algorithm
64 B	4.163KB	1.056KB	59.893KB
128B	8.326KB	2.112KB	61.072KB
192 B	12.489KB	3.168KB	62.557KB
256B	16.652KB	4.224KB	63.981KB
320B	20.815KB	5.028KB	65.026KB
384B	24.978KB	6.336KB	66.133KB
448B	29.141KB	7.392KB	67.317KB
512B	33.304KB	8.448KB	68.587KB

https://doi.org/10.1371/journal.pone.0290323.t001

256bits, 320bits, 384bits,448bits and 512bits) can be calculated when the selected system parameter is $n = 256, q = 2^{32}$. The results are shown in Table 1. The algorithm authentication size corresponding to different security levels of our proposed lattice-based cipher scheme and RSA and ECC authentication algorithms is given. As shown in Table 1, with the continuous improvement of the security level of the RSA algorithm, the required authentication size increases very quickly, which is not suitable for encrypting large data in high-level security. However, the size of the lattice-based authentication proposed in this paper does not change much. The size of the authentication is kept at a stable level, which is more suitable for encrypting large data in high-level security. The size of the certification of the ECC algorithm grows slightly slower than that of the RSA algorithm, but its certification also doubles as the security level of the algorithm increases. In addition, the schemes implemented with RSA and ECC algorithms cannot resist quantum computing attacks, so the lattice-based authentication protocol in this paper has good anti-quantum security. With the development of quantum computers and quantum computing, lattice cryptography will be a very practical cryptographic algorithm in the quantum era.

Therefore, the lattice-based scheme proposed in this paper has better security, and when the security level is higher, the algorithm efficiency has certain advantages.

6. Conclusions

Utilizing the cluster management of wireless sensor networks, most sensor nodes only need a small amount of storage space, effectively reducing deployment costs and reducing the number of mutual authentication between sensor nodes, which is suitable for medium and large-scale deployment of sensor networks. After mutual authentication, the sensor nodes in the wireless sensor network use symmetric keys for data communication. Since the amount of data that needs to be communicated is much greater than the amount of data that needs to be authenticated, the data communication is carried out through the traditional cryptographic system, which effectively improves the data security and communication efficiency. The cluster sensor network key management method proposed in this paper has the advantages of simple process, high security and high efficiency. The use of cluster structure can reduce the cost of frequent mutual authentication brought by transmission, which is beneficial to the expansion of the network. It is suitable for deployment in applications such as forest fire prevention and urban air quality monitoring. Even in the post-quantum era, it can well guarantee the security of mutual authentication between sensor nodes, and has broad practical application prospects. The size of the lattice-based authentication proposed in this paper does not change much with the continuous improvement of the security level of the RSA algorithm. The size of the

certificate is kept at a stable level, which is more suitable for encrypting large data at a high security level.

For future work, we will continue to investigate lattice-based quantum computing-resistant key management schemes that support more flexible signature strategies.

Author Contributions

Conceptualization: Jiang Zhang.

Data curation: Jiang Zhang.

Formal analysis: Jiang Zhang.

Funding acquisition: Jiang Zhang, Qi Liu.

Investigation: Jiang Zhang.

Methodology: Jiang Zhang, Qi Liu.

Project administration: Jiang Zhang, Qi Liu.

Resources: Jiang Zhang.

Software: Jiang Zhang.

Supervision: Jiang Zhang, Qi Liu.

Validation: Jiang Zhang.

Visualization: Jiang Zhang.

Writing – original draft: Jiang Zhang.

References

1. Kizilkaya B., Ever E., Yatbaz H. Y., and Yazici A., "An Effective Forest Fire Detection Framework Using Heterogeneous Wireless Multimedia Sensor Networks," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 18, no. 2, pp.1–21, May 2022.
2. Tang J, Lu X, Xiang Y, Shi C, Gu J. Blockchain search engine: Its current research status and future prospect in Internet of Things network. Future Generation Computer Systems. 2023, 138(1):120–141.
3. Priyadarshi R. and Gupta B., "Area Coverage Optimization in Three-Dimensional Wireless Sensor Network," *Wireless Personal Communications*, vol. 117, no. 2, pp.843–865, 2021.
4. Maller Mary, Bowe Sean, Kohlweiss Markulf, and Meiklejohn Sarah, "Sonic: Zero-knowledge snarks from linear-size universal and updatable structured reference strings," in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, vol. 2019, pp. 2111–2128, 2019.
5. Khot P. S. and Naik U. L., "Cellular automata-based optimised routing for secure data transmission in wireless sensor networks," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 34, no. 3, pp.431–449, May 2022.
6. Al Nuaimi MMK, Rishal KP, Oommen NV, Sherimon PC. Blockchain Implementation Framework for Tracing the Dairy Supply Chain. Lecture Notes on Data Engineering and Communications Technologies. 2023, 142(1):551–560.
7. Tuan N. A., Akila D., Pal S., Sarkar B., Khai Tran T., Mothilal Nehru G., et al., "Dynamic Data Optimization in IoT-Assisted Sensor Networks on Cloud Platform," *Computers, Materials & Continua*, vol. 72, no. 1, pp.1357–1372, 2022.
8. Nain M. and Goyal N., "Energy Efficient Localization Through Node Mobility and Propagation Delay Prediction in Underwater Wireless Sensor Network," *Wireless Personal Communications*, no. 2, pp.1–19, 2021.
9. Zhang J, Li T, Obaidat M S, et al. Enabling efficient data sharing with auditable user revocation for 10V systems. IEEE Systems Journal, 2022, 16(1): 1355–1366.
10. Mehmood A., Umar M. M., and Song H., "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 55, no. 6, pp.97–106, 2016.

11. Zhang J., Li H., and Li J., "Key Establishment Scheme for Wireless Sensor Networks Based on Polynomial and Random Key Predistribution Scheme," *Ad Hoc Networks*, vol. 71, no. MAR., pp.68–77, 2017.
12. Kumar D., Pachigolla S. K., Manhas S. S., and Rawat K., "Cryptanalysis and improvement of mutual authentication protocol for real-time data access in industrial wireless sensor networks," *International Journal of Computers and Applications*, vol. 44, no. 6, pp.521–534, Jun. 2022.
13. Palani U., Amuthavalli G., and Alamelumangai V., "Secure and load balanced routing protocol in wireless sensor network for disaster management," *IET Information Security*, vol. 14, no. 5, pp.513–520, 2020.
14. D'anvers JP, Van Beirendonck M, Verbauwhede I. Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced Implementations. IEEE Transactions on Computers. 2023, 72(2):321–332.
15. Benedikt Bünz Jonathan Bootle, Boneh Dan, Poelstra Andrew, Wuille Pieter, and Maxwell Greg, "Bulletproofs: Short proofs for confidential transactions and more," in 2018 IEEE symposium on security and privacy (SP), pp. 315–334. IEEE, 2018.
16. Li H., Guo F., Wang L., Wang J., Wang B., and Wu C., "A Blockchain-Based Public Auditing Protocol with Self-Certified Public Keys for Cloud Data," *Security and Communication Networks*, vol. 2021, pp.1–10, Feb. 2021.
17. Tahat N., Alomari A. K., Al-Hazaimeh O. M., and Al-Jamal M. F., "An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 4, pp.935–948, May 2020. https://doi.org/10.1080/09720529.2020.1734293
18. Yamamura K, Wang Y, Fujisaki E. Improved lattice enumeration algorithms by primal and dual reordering methods. IET Information Security. 2023, 17(1):35–45.
19. Islam N, Marinakis Y, Olson S, White R, Walsh S. Is BlockChain Mining Profitable in the Long Run. IEEE Transactions on Engineering Management. 2023, 70(2):386–399.
20. Eli Ben-Sasson Iddo Bentov, Horesh Yinon, and Riabzev Michael, "Scalable, transparent, and post-quantum secure computational integrity," Cryptology ePrint Archive, vol. 2018, pp. 46–128, 2018.
21. Zhang J., Cui J., Zhong H., Chen Z., and Liu L., "PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks," *IEEE Trans. Dependable and Secure Comput.*, vol. 18, no. 2, pp.722–735, Mar. 2021.
22. Ametepe A. F.-X., Ahouandjinou A. S. R. M., and Ezin E. C., "Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks," *Wireless Netw*, vol. 28, no. 3, pp.991–1001, Apr. 2022. https://doi.org/10.1007/s11276-022-02903-3
23. Mehmood G, "An efficient and secure session key establishment scheme for health-care applications in wireless body area networks," *J. Eng. Appl.*, 2018, pp:1–6.
24. Bootle J., Lyubashevsky V., and Seiler G., "Algebraic Techniques for Short(er) Exact Lattice-Based Zero-Knowledge Proofs," *in Advances in Cryptology–CRYPTO 2019*, vol. 11692, pp.176–202, 2019.
25. Mehmood G, Khan M Z, Waheed A, Zareei M and Mohamed E M, "A trust-based energy-efficient and reliable communication scheme (trust-based ercs) for remote patient monitoring in wireless body area networks," *IEEE Access*, 2020, pp:1–9.
26. Lyubashevsky V., Nguyen N. K., and Seiler G., "Shorter Lattice-Based Zero-Knowledge Proofs via One-Time Commitments," *in Public-Key Cryptography–PKC 2021*, vol. 12710, pp.215–241, 2021.
27. Mehmood G, Khan M S, Waheed A, Zareei M, Fayaz M, and Sadad T, "An efficient and secure session key management scheme in wireless sensor network," *Complexity*, 2021, pp:1–6.
28. Mehmood G, Khan M S, Fayaz M, Faisal M, Rahman H U, and Gwak J, "An energy-efficient mobile agent-based data aggregation scheme for wireless body area networks," *Computers, Materials & Continua*, 2022, vol. 70, no.3, pp:5929–5948.
29. Dharminder D, Reddy CB, Das AK, Park Y, Jamal SS. Post-Quantum Lattice-Based Secure Reconciliation Enabled Key Agreement Protocol for IoT. IEEE Internet of Things Journal10. 2023, 10(3):2680–2692.
30. Lyubashevsky V., "Lattice Signatures without Trapdoors," *in Advances in Cryptology–EUROCRYPT 2012*, vol. 7237, pp.738–755, 2012.
31. Langlois A. and Stehlé D., "Worst-case to average-case reductions for module lattices," *Des. Codes Cryptogr.*, vol. 75, no. 3, pp.565–599, Jun. 2015.
32. Lyubashevsky V., Nguyen N. K., and Plancon M., "Efficient Lattice-Based Blind Signatures via Gaussian One-Time Signatures," *in Public-Key Cryptography–PKC 2022*, vol. 13178, pp.498–527, 2022.
33. Corentin J., Adeline R. L. and Olivier S., Lattice-Based Signature with Efficient Protocols, Revisited, *eprint.iacr.org*, 1–46, 2022, https://eprint.iacr.org/2022/509.