entropy

MDPI

Article

Anti-Quantum Lattice-Based Ring Signature Scheme and Applications in VANETs

Chunhong Jiao [1,*] and Xinyin Xiang [2,3]

[1] School of Physics, Xi'an Jiaotong University City College, Xi'an 710018, China
[2] School of Information, Xi'an University of Finance and Economics, Xi'an 710100, China; xxy@xaufe.edu.cn
[3] China (Xi'an) Institute for Silk Road Research, Xi'an University of Finance and Economics, Xi'an 710100, China
* Correspondence: jiaoch@xjtucc.edu.cn or gigi7944@163.com

Abstract: Message authentication is crucial because it encourages participants to accept countermeasures and further transmit messages to legitimate users in a network while maintaining the legitimacy of the identity of network members. An unauthorized user cannot transmit false messages to a given network. Although traditional public key cryptography is suitable for message authentication, it is also easy to manage and generate keys, and, with the expansion of an entire network, the system needs a lot of computing power, which creates additional risks to network security. A more effective method, such as ring signature, can realize this function and guarantee more security. In this paper, we propose an anti-quantum ring signature scheme based on lattice, functionality analysis, and performance evaluation to demonstrate that this scheme supports unconditional anonymity and unforgeability. After efficiency analysis, our scheme proved more effective than the existing ring signature schemes in processing signature generation and verification. The proposed scheme was applied to VANETs that support strong security and unconditional anonymity to vehicles.

Keywords: anti-quantum; ring signature; lattice-based cryptography; anonymity

check for updates

Citation: Jiao, C.; Xiang, X. Anti-Quantum Lattice-Based Ring Signature Scheme and Applications in VANETs. *Entropy* **2021**, *23*, 1364. https://doi.org/10.3390/e23101364

Received: 10 September 2021
Accepted: 13 October 2021
Published: 19 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

User privacy protection is one of the main goals of modern cryptography, but a digital signature, as a cryptographic primitive to realize the main functions, such as identity authentication, does not consider privacy as a security goal. The public key of the signer is the necessary information to verify the validity of the signature, so the identity of the signer of the digital signature is always visible to the verifier. This explicit validity verification method cannot meet the needs of users in some scenarios. Cryptography primitives, such as group signature [1] and ring signature [2], focus on the protection of user privacy in the above scenarios. They allow the signer to sign in the name of the group, and the verifier can only confirm that the signature is generated by a user in the group but cannot know the specific identity of the signer. Between the two, the group signature system has the role of group administrator, responsible for managing group members and tracking the identity of signers. The group in the ring signature system is completely self-organized; there is no special organization, and the anonymity of the signature cannot be revoked, which provides a higher level of privacy protection. The premise of the ring signature is similar to that of the group signature, both of which hide the identity of the signer within a certain group, but there are significant differences. In the group signature scheme, the group administrator can revoke the anonymity of the group signature, while, in the ring signature, there is no centralized organization, and the group that hides the identity of the signer can be selected by the signer himself immediately. There is no need for any co-operation among users. This means that the ring signature supports stronger anonymity.

In recent years, message authentication in the blockchain has become extremely vital as it encourages users to accept messages and transmit them to other users in the network.

To a certain extent, blockchain [3] technology enables the co-operation and value flow between individuals who do not trust each other. However, the data transmission and storage on blockchain are publicly visible, which can be provided to any information query, and can only protect the privacy of both parties through the form of "pseudo anonymity." In order to meet the needs of this technology, the ring signature is more likely to solve the privacy protection problem of blockchain so as to meet the need for user identity anonymity and transaction information unforgeability. In contrast to classical cryptography, recent studies have shown that lattices are enjoying widespread interest in cryptography. Lattice-based cryptography is widely believed to be resistant against quantum computers, which prompts us to design secure cryptographic schemes as an ideal candidate. In 2008, Gentry et al. [4] employed a novel technique called preimage sampling function (PSF) and built a lattice-based signature scheme in the random oracle model. In 2009, Buchmann et al. [5] designed a Merkle tree signature scheme in the random oracle model under the worst-case hard lattice problems. Subsequently, Boyen et al. [6] proposed the construction of a short signature from hard lattices without random oracles. Previous lattice-based signature schemes used the trapdoor function on the lattice to generate credentials for users in the group. Because of the system parameters required by the trapdoor, the actual size of the signature was too large. More precisely, to improve the efficiency of the signature, it is natural to ask whether we can design a ring signature scheme with enhanced security and better efficiency, so it seems feasible to construct the cryptosystem as we do from lattices.

1.1. Related Works

Rivest et al. [2] first proposed the notion of a ring signature scheme in 2001. They presented a ring signature scheme based on the Rabin trapdoor function and RSA trapdoor permutation and proved the security of the proposed scheme under the random oracle model. In the ring signature, any user can sign any message on behalf of the whole ring, and any verifier who obtains the ring public key can verify whether the signature comes from the ring. It is worth noting that, if only the ordinary ring signature scheme is used to solve the problem of privacy protection in the blockchain, the fund holder can sign the same fund many times under the protection of the ring signature and cannot be detected. Brakerski et al. [7] proposed an efficient general framework to construct ring signature schemes under the standard model. Specifically, the scheme defines the concept of the ring trapdoor function and shows how to construct ring signatures using the ring trapdoor. In 2014, Liu et al. [8] proposed a linkable ring signature with unconditional anonymity; the formal security model definition and proof are given. However, the above ring signature is mainly based on a public key certificate, which has the burden of key management and cannot often avoid the complex problem of the user's public key certificate management.

Duan et al. [9] presented a ring confidential transaction protocol for blockchain-enabled systems. Because of the threat from quantum computing technology, the traditional cryptosystem based on number theory problems (such as the large integer factorization problem and the finite field discrete logarithm problem) will be broken; if the ring signature is still constructed based on number theory, the security of the ring signature cannot be guaranteed in the quantum era. In recent years, a new cryptosystem based on lattice theory [10–12] has become a research topic for the post-quantum cryptography era because of its advantages of better progressive efficiency, parallelism, simple operation, resistance to quantum attacks, and the existence of worst-case random instances. In 2018, Wang et al. [13] presented an anti-quantum ring signature scheme without trapdoors; their scheme adopted the Gaussian "tail-cut" factor, which leads to a relatively long signature length. Torres et al. [14] put forth the first lattice-based one-time linkable ring signature in the random oracle model, which uses the rejection sampling technique to make the distribution of the output signature independent of the distribution of the private key of the signature, thus further improving the efficiency of signature generation. Torres et al. [15] extended the scheme of [14] and proposed a ring signature scheme supporting multiple inputs and multiple outputs, which is more practical. Cui et al. [16] proposed a lattice-based

ring signature scheme and vehicular ad hoc network (VANET) privacy preservation; the scheme has high-level security and traceability while ensuring anonymity and is a ring signature scheme based on the hardness problem, which can effectively solve the privacy protection problem in VANETs. Combining the lattice signature and the ring signature, Lui et al. [17] presented a double authentication prevention scheme, which provides secure authentication but lacks full anonymity. In addition, the above schemes demonstrate that the message is transmitted securely from the sender to the receiver and can only be received securely by the receiver. Subsequently, Esgin et al. [18] solved several problems in transferring the design idea of Kohlweiss et al. [19] to lattices; they designed a one-to-many protocol based on the SIS problem [20] in modular lattices and constructed a ring signature scheme with a logarithmic level signature size. Feng et al. [21] proposed a general design framework of a traceable ring signature and constructed a lattice traceable ring signature scheme based on Stern's protocol. This scheme utilizes techniques of preimage sampling and rejection sampling, and the generation of a key using a trapdoor generation algorithm. It also provides secure authentication, but the efficiency of the scheme is limited by the use of non-interactive zero-knowledge proofs.

1.2. Motivation

In huge networks, the privacy of communication is very important. If a legal member of the group securely transmits a message and the message is incorrectly modified by a malicious user, the consequences may affect other users. Owing to the existence of these malicious operations, it is necessary to provide an efficient and secure mechanism to strengthen privacy protection. Although some schemes provide necessary privacy protection, there are many difficulties in distinguishing the malicious operations of authorized users and unauthorized users. A ring signature can hide the signer's identity from a group, which can better solve these issues.

In this paper, an efficient and secure anti-quantum ring signature scheme is proposed in combination with lattice-based cryptography and ring signature. It helps to verify information and protect the user's identity privacy. On one hand, most of the proposed lattice-based ring signature schemes are mainly based on two types of problems: small integer solution (SIS) problems and learning with errors (LWEs); they all have an important characteristic in that the time spent solving the two kinds of problems is equivalent to the time spent solving the worst-case hardness problem. On the other hand, in our scheme, our sample is bimodal, having two centers at Se and $-Se$, namely, D^m_σ (the distribution can be scaled up to $D^m_{Se,\sigma}$ or $D^m{}_{-Se,\sigma}$) is under the bimodal distribution. Since our scheme does not adopt the Gaussian "tail-cut" factor, the sampling process can produce shorter signatures. Furthermore, we adopt the encoding function $F : \{0,1\}^\kappa \to \mathbb{B}^n_\eta$ to map $h : \{0,1\}^* \to \{v : v \in \{-1,0,1\}^n, \|v\|_1 \leq \kappa\}$ to $\mathbb{B}^n_{2q}$ (where $\mathbb{B}^n_{2q}$ denotes a set of binary vectors of length n and weight $\eta = 2q$,η that is constant). This method can greatly speed up the signature and verification.

1.3. Our Contribution

As privacy protection is a significant concern, this paper proposes a ring signature scheme based on anti-quantum lattice-based cryptography to solve the vulnerability of the existing schemes to quantum attacks. The ring signature scheme is designed based on the lattice assumption and can support anti-quantum security. The specific research contents include:

(1) Combining lattice-based cryptography with a ring signature, we construct a secure lattice-based ring signature under the random oracle model. The proposed scheme satisfies unconditional anonymity and unforgeability. The unforgeability of the proposed ring signature scheme is reduced to the difficult assumption of the small integer solution (SIS) on the lattice.

(2) Our scheme also provides a certain degree of unconditional anonymity for ring members and ensures signature unforgeability.

(3) We give a detailed performance analysis and provide applications of our scheme in VANETs, and the results show that our scheme is significantly better than the ongoing schemes. Our scheme satisfies security requirements in VANETs.

1.4. Outline

The rest of the paper is organized as below. Some preliminaries, such as assumptions and lemmas, are introduced in Section 2. The security model and the architecture of our proposed scheme are described in Sections 3 and 4, respectively. The correctness and security analysis are provided in Section 5. The performance evaluation is provided in Section 6. We give the related applications in VANETs in Section 7 and present an extension of the scheme in Section 8. Finally, the conclusions are given in Section 9.

2. Preliminaries

2.1. Notations

If X is a set, then $x \to X$ means the entity of picking uniformly random x in X. Let $\mathfrak{D}$ be a Gaussian distribution and PPT be probabilistic polynomial time; $\mathbb{R}$ and $\mathbb{Z}$ denote real numbers and integers, respectively. $\mathbb{R}$ or $\mathbb{Z}$ is named by lower-case letters (e.g., x) and matrices by bold upper-case letters (e.g., A); A^T is the transposition of A. "||" means the concatenation of strings or matrix columns; vectors are in column form. *negl* (n) means a negligible function, and a function $\omega(f(n))$ denotes $\omega(f(n))$ grows faster than $cf(n)$ with any constant $c > 0$. For any matrix $X \in \mathbb{R}^{n \times k}$, we use $s_1(X) = \max_{||u||=1} ||Xu||$ to denote the largest singular value (also known as the spectral norm) of X.

2.2. Lattices and Lattice Problems

Given m to be linearly independent vectors $B = (b_1, \cdots, b_m) \in \mathbb{R}^{m \times m}$, an m-dimensional lattice Λ is defined as $\Lambda = L(B) = Bc = \{\sum_{i=1}^{m} b_i c_i, c_i \in \mathbb{Z}^m\}$, where $\Lambda = L(B)$ is a basis of B.

For $m \geq n \geq 1$ and $q \geq 2$, a matrix $A \in \mathbb{Z}_q^{n \times m}$, the lattice is defined as $\Lambda_q^{\perp}(A) = \{e \in \mathbb{Z}^m, Ae = 0 \bmod q\}$, and $\Lambda_q^u(A) = \{e \in \mathbb{Z}^m, Ae = u \bmod q\}$. Thus, $\Lambda_q^u(A)$ is obviously a co-set of $\Lambda_q^{\perp}(A)$; namely, $\Lambda_q^u(A) = t + \Lambda_q^{\perp}(A)$. Where t is an arbitrary solution (over $\mathbb{Z}_q^m$) of the equation $Ae = u \bmod q$, this is the integer lattice called a q-ary lattice.

Let L be a subset of $\mathbb{Z}^m$. For any vector $c \in \mathbb{R}^m$ and any positive parameter $\delta \in \mathbb{R}$, let $\rho_{\delta,c}(x) = \exp(\frac{-\pi \|x-c\|^2}{\delta^2})$ be a Gaussian-shaped function on $\mathbb{R}^m$ with center c and parameter δ. Next, for every $y \in L$, we set $\rho_{\delta,c}(L) = \sum_{x \in L} \rho_{\delta,c}(x)$ to be the sum of $\rho_{\delta,c}(x)$ over L with parameters (δ, c) and $D_{L,\delta,c}(y) = \frac{\rho_{\delta,c}(y)}{\rho_{\delta,c}(L)}$. For simplicity, $\rho_{\delta,0}$ and $D_{L,\delta,0}$ are abbreviated as ρ_δ and $D_{L,\delta}$, respectively.

Here, we recall the shortest vector problem (SVP) over lattices. For a lattice basis B and an approximation factor γ, its goal is to find the shortest non-zero vector in a lattice $L(B)$.

2.3. Hard Problems for q-ary Lattices

The security of our proposed scheme rests on the following hardness problems that cannot be solved in polynomial time with non-negligible advantage. The related problem is described as follows.

Definition 1. (*SIS problem): The SIS problem is given* (m, q, β) *and* $A \in \mathbb{Z}_q^{n \times m}$*; its goal is to compute a non-zero vector* $x \in \mathbb{Z}_q^m$ *such that* $Ax = 0 \bmod q$ *with* $\|x\| \leq \beta$.

Ajtai [22] first showed that the SIS problem is hard on average. Later, Micciancio et al. [23] formalized its notion and determined that the SIS problem is regarded as a worst-case hard lattice problem. Micciancio et al., showed that solving the average-case SIS problem was reduced to worst-case, approximating the SVP within certain $\beta \cdot \widetilde{O}(n)$ *factors.*

Lemma 1. [24] *For any* $k \geq 1$*, if* $\Pr[\|s\| > k\sigma\sqrt{m} : s \leftarrow D_\sigma^n] < k^n e^{\frac{1}{2}(1-2^{k^2})}$ *holds, this means* $\Pr[|\langle s, r \rangle| > r : s \leftarrow D_\sigma^n] < 2e^{\frac{r^2}{2\|v\|^2\sigma^2}}$*, where* $v \in \mathbb{R}^n$ *and* $\sigma, r > 0$.

Lemma 2. [24] *If* $\Pr[D_{\sigma}^{n}/D_{v,\sigma}^{n} < e^{\frac{\beta}{12}+\frac{1}{2}\beta^{2}} : s \leftarrow D_{\sigma}^{n}] = 1 - 2^{-100}$ *holds for any vector* $s \in \mathbb{Z}^{n}$ *and* $\sigma = \beta\|v\|, \beta > 0$.

Lemma 3. *For any matrix* $A \in \mathbb{Z}_{q}^{n\times m}$ *and* $S \in \{-d,\ldots,d\}^{m\times k}$, *there is another different* $S' \in \{-d,\ldots,d\}^{m\times k}$ *that satisfies* $AS = AS' \bmod q$ *with a probability not beyond* $1 - 2^{-100}$, *where* $m > 64 + n\log q/\log(2d+1)$.

2.4. Chameleon Hash Function

A construction of chameleon hash consists of the following algorithms CHF = (HGen, Hash, Col).

HGen: On input, a security parameter λ outputs $(hk, td) \leftarrow HGen(\lambda)$, where the hash key is hk and the trapdoor td.

Hash: On input, the hash key hk and vectors μ and r output the hash value $h \leftarrow Hash(hk, \mu, r)$.

Col: On input, the trapdoor td, r' and a message μ', output $r' \leftarrow Col^{-1}(td, \mu', \mu, r)$ such that $Hash(hk, \mu', r') = Hash(hk, \mu, r)$.

Chameleon hash function supports the property of enhanced collision resistance, which was applied to the design of our scheme.

3. System Models

3.1. Basic Model

A basic model in our proposed scheme is illustrated in Figure 1, where $P_1, P_2, \ldots, P_k$ denotes ring members. In this model, new ring members and other members will form a common ring; we call a group of possible signers a ring. The ring members can create the actual signature, and other ring members who cannot generate an efficient signature are called non-signers. For example, in a network model of VANETs, most information, such as beacon messages periodically broadcast by vehicles and public messages broadcast by roadside units, do not need to be kept secret, but these messages are associated with responsibility. Before using the message, it is necessary to verify whether the message comes from a legitimate network member and to check the authenticity of the message, so signature technology is required. The vehicle will use the ring member to sign and issue follow-up messages so as to effectively hide its real identity on the premise of ensuring the authenticity of the messages and to realize anonymous communication in the VANETs. Applying ring signature technology helps vehicles construct a ring with nearby vehicles through roadside facilities, and the real identity of the signer can be identified according to the signed message so as to realize the unconditional anonymous communication of vehicles in VANETs.

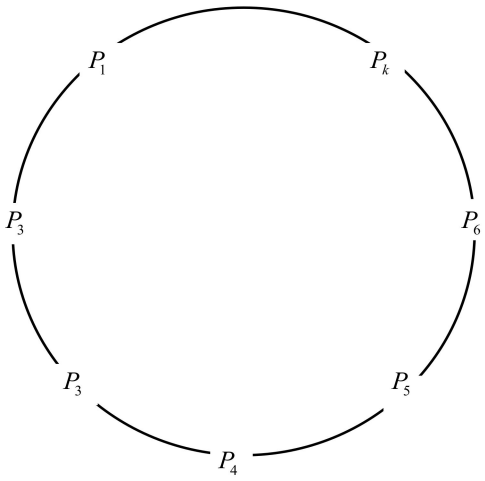

Figure 1. Framework of ring signature.

As the main method of resisting quantum attack, lattice-based cryptography has been widely considered. In addition, ring signature has good anonymity and unforgeability, so we believe that the ring signature scheme based on the lattice hard problem can effectively solve the privacy protection problem in practical applications (such as VANETs).

3.2. Threat Model

For our proposed lattice-based ring signature scheme, we considered a widely accepted threat model [2]. In terms of the model, an adversary $\mathcal{A}$ cannot distinguish that the member of a ring created a given signature among the communicated entities in the application environment. Furthermore, any communicating entities (unauthorized users or attackers) cannot output signatures. Specific details are described as follows.

Anonymity. The following game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$ is used to define the anonymity of the ring signature scheme:

(1) $\mathcal{A}$ creates a group of public parameters $\mathcal{P} = (L, n, m, q)$, a ring $R = (pk_1, \ldots, pk_n)$, two secret keys (sk_{i_0}, sk_{i_1}), and a message μ.
(2) $\mathcal{A}$ is permitted to make ring-signing queries and corruption queries. $\mathcal{C}$ responds with $\sigma_L(\mu) = Sign(pk_s, sk_s, R, \mu)$ as a ring-signing query. The signer of an index s performs a corruption query. Finally, $\mathcal{C}$ sends sk_s to $\mathcal{A}$.
(3) $\mathcal{A}$ requests a challenge to $\mathcal{C}$ with the values (i_0, i_1, R, μ); $\mathcal{C}$ calculates two challenge signatures. $\sigma_{i_0} = Ring - sign(\mathcal{P}, sk_{i_0}, R, \mu)$ and $\sigma_{i_1} = Ring - sign(\mathcal{P}, sk_{i_1}, R, \mu)$; $\mathcal{C}$ responds to $\mathcal{A}$ with $\sigma_{i_0}, \sigma_{i_1}$.
(4) $\mathcal{A}$ responds a guess b' and wins the game if $b' = b$.

Unforgeability. To enable signature verification:

$Sign - Verify(R, \mu, \sigma_L(\mu)) = 1$ forgery is implemented when an unauthorized user obtains the private key from $R = (pk_1, \ldots, pk_n)$ or a ring member that has previously signed a message. The unforgeability with insider corruption is defined as the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

(1) $\mathcal{A}$ creates a group of public parameters $\mathcal{P} = (L, n, m, q)$, a ring $R = (pk_1, \ldots, pk_n)$, two secret keys (sk_{i_0}, sk_{i_1}), and a message μ.
(2) $\mathcal{A}$ is permitted to make ring-signing queries and corruption queries. $\mathcal{C}$ responds with $\sigma_L(\mu) = Sign(pk_s, sk_s, R, \mu)$ as a ring-signing query. The signer of an index s performs a corruption query. Finally, $\mathcal{C}$ sends sk_s to $\mathcal{A}$.
(3) $\mathcal{A}$ sends the result $(R, \mu^*, \sigma_L(\mu)^*)$ to the challenger, and $\mathcal{A}$ is considered as successful if $Sign - Verify(R, \mu^*, \sigma_L(\mu)^*) = 1$, where $\mu^* \notin \mu$.

4. The Proposed Scheme Description

In this section, to facilitate the description of our scheme, we use a bimodal Gaussian distribution as a major building block for our ring signature scheme. The aim is to make sampling rejection more effective, and the procedures for rejecting sampling are illustrated in [24].

With the technique employed in [25], we present a ring scheme over lattices and prove its security under the SIS problem. The relevant steps are as follows:

Key generation: Given a security parameter, and some other parameters n, m, q, i, j, let $A_i \in \mathbb{Z}_{2q}^{n \times m}$ and $S_i \in \mathbb{Z}_{2q}^{m \times n}$ be public/private keys of the user with index i, respectively, such that key pairs meet $A_i S_i = qI_n \bmod 2q$ (where $i \in L = \{1, 2, \ldots, n\}$, S_i is invertible). Let a hash function be $h : \{0,1\}^* \to \{v : v \in \{-1, 0, 1\}^n, \|v\|_1 \leq \kappa\}$ and nearly injective mapping be $F : \{0,1\}^\kappa \to \mathbb{B}_{2q}^n$ ($\mathbb{B}_{2q}^n$ denotes a set of binary vectors of length n and weight $2q$). For $\hat{A} = (A_1, A_2, \ldots, A_n), A_i \in \mathbb{Z}_{2q}^{n \times m}$ and $\hat{S} = (S_1, S_2, \ldots, S_n), S_i \in \mathbb{Z}_{2q}^{n \times m}$, this is $(pk, sk) = (\hat{A}, \hat{S})$. The system publishes $\mathcal{P} = (L, pk, h, F, n, m, q)$. The relevant details are shown in the following Algorithm 1.

Algorithm 1 KeyGen algorithm

Input: A security parameter λ
Output: The public parameters $\mathcal{P}$
1: Let $L = \{1, 2, \ldots, n\}$ and q be a prime number;
2: Define three sets $D^m_{\sigma_1}, D^m_{\sigma_2}, D^m_{\sigma_3}$, hash function $h : \{0,1\}^* \to \{v : v \in \{-1, 0, 1\}^n, \|v\|_1 \leq \kappa\}$, and nearly injective mapping $F : \{0,1\}^\kappa \to \mathbb{B}^n_{2q}$;
3: Set $\hat{A} = (A_1, A_2, \ldots, A_n), A_i \in \mathbb{Z}^{n\times m}_{2q}$ and $\hat{S} = (S_1, S_2, \ldots, S_n), S_i \in \mathbb{Z}^{m\times n}_{2q}$ such that $A_i S_i = qI_n \mathrm{mod} 2q$;
4: Set $(pk, sk) = (\hat{A}, \hat{S})$;
5: Output $\mathcal{P} = (L, pk, h, F, n, m, q)$.

Ring-Sign: On input, a message μ, a long-term key S_j, a ring of n members with public keys $\hat{A} = (A_1, A_2, \ldots, A_n)$, a user i selects uniform value $k_i \leftarrow D^m_{\sigma_1}$ and calculates $x_i = A_i y_i \mathrm{mod} 2q$ with the random vector $y_i \leftarrow D^m_{\sigma_2}$, and outputs the signature $\sigma_L(\mu)$ as illustrated in Algorithm 2 of the message μ. Then, the user i performs the following computations:

(1) For all $i \in L$, calculate $h_i = x_i + A_i k_i \mathrm{mod} 2q$, where $L = \{1, 2, \ldots, n\}$.
(2) Calculate $e = (\sum_{i\in L} h_i \mathrm{mod} 2q, \mu)$ and $\tilde{e} = F(e)$.
(3) Pick a random bit $b \in \{0, 1\}$; calculate $s_j = y_j + k_j + (-1)^b S_j \tilde{e}$, where $i = j$.
(4) For $i \neq j$, compute $s_i = y_i + k_i \mathrm{mod} 2q$.
(5) Publish $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$.

Algorithm 2 Ring-signing algorithm

Input: A message μ, a long-term key S_j, public keys $\hat{A} = (A_1, A_2, \ldots, A_n)$
Output: The signature $\sigma_L(\mu)$
1: Calculate $h_i = x_i + A_i k_i \mathrm{mod} 2q$, $x_i = A_i y_i \mathrm{mod} 2q$, where $i \in L = \{1, 2, \ldots, n\}$;
2: Calculate $e = (\sum_{i\in L} h_i \mathrm{mod} 2q, \mu)$ and $\tilde{e} = F(e)$;
3: For $i \in L = \{1, 2, \ldots, n\}$ and $i \neq j$, compute $s_i = y_i + k_i \mathrm{mod} 2q$;
4: Pick $b \in \{0, 1\}$; compute $s_j = y_j + k_j + (-1)^b S_j \tilde{e}$, where $i = j$;
5: Continue the next steps with probability $\frac{1}{M \exp(-\frac{\|S_j \cdot e\|^2}{2\sigma^2}) \cosh(\frac{\langle s_j, S_j \cdot e\rangle}{\sigma^2})}$,
otherwise **Restart**;
6: Output $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$.

Ring-Verify: Given a signature $\sigma_L(\mu)$, a message μ, and a bit b, the algorithm outputs a response and answers: accept or reject (as illustrated in Algorithm 3). The signature $\sigma_L(\mu)$ can be checked and only accepted under the following conditions: $\|s_i\|_2 \leq B_2$ and $\|s_i\|_\infty \leq q/4$ for $1 \leq i \leq n$, where B_2 is the valid bounds [26].

(1) $s_i \leftarrow D^m_{\sigma_3}$
(2) $e = (\sum_{i\in L} A_i s_i + q\tilde{e} \mathrm{mod} 2q, \mu)$

If the above verifications hold, the signature is valid and the verifier outputs 1; otherwise, it outputs 0.

Algorithm 3 Ring-verify algorithm

Input: The signature $\sigma_L(\mu)$; public keys $\hat{A} = (A_1, A_2, \ldots, A_n)$
Output: Accept or Reject
1: **If** $s_i \leftarrow D^m_{\sigma_3}$, then **continue**;
2: else if $\|s_i\|_2 \leq B_2$, then **continue**;
3: else if $\|s_i\|_\infty \leq q/4$, then **continue**;
4: **else if** $e = (\sum_{i\in L} A_i s_i + q\tilde{e} \mathrm{mod} 2q, \mu)$, then **Accept**,
else Reject;
5: Output Accept or Reject.

Theorem 1. *Define* $B_2 = \eta\sigma\sqrt{m}$ *and* $q/4 > \sqrt{(\lambda+1)In2 + 2In(m)}\sigma$ *and a signature* $\sigma_L(\mu)$. *These parameters are created based on Algorithm 2. Then, the output of Algorithm. 3 outputs accept with probability* $1 - \lambda/2$ *if* $\sigma_L(\mu)$ *is valid*.

Proof. In terms of Lemma 2 and Lemma 3, we find that the bound on Euclidean norm is $B_2 = \eta\sigma\sqrt{m}$, and, for any $\eta > 1$, there is a probability $\Pr[\|s_i\|_2 \geq \eta\sigma\sqrt{m}] > 1 - \lambda/2$. According to Lemma 2 and Lemma 3, we find that the bound on infinity norm is $\|s_i\|_\infty \leq q/4$. In fact, it satisfies the following conditions $q/4 > \eta\sigma > \sqrt{(\lambda+1)In2 + 2In(m)}\sigma$ unless its probability is $\lambda/2$. □

5. Correctness and Security Analysis

5.1. Correctness

The correctness of the signature can be well verified. In fact, the signer outputs the form of the signature $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$, where $s_i \leftarrow D^m_{\sigma_3}$. The signature is valid if the following details are true:

$$\begin{aligned} &\textstyle\sum_{i\in L} A_i s_i + q\widetilde{e} = \sum_{i\in L, i\neq j}(A_i y_i + A_i k_i) + q\widetilde{e} + A_j s_j \\ &= \textstyle\sum_{i\in L} x_i + \sum_{i\in L, i\neq j} A_i k_i + A_j((-1)^b S_j \widetilde{e} + k_j) + q\widetilde{e} \\ &= \textstyle\sum_{i\in L} x_i + \sum_{i\in L} A_i k_i + (-1)^b q\widetilde{e} + q\widetilde{e} \\ &= \textstyle\sum_{i\in L} h_i \mathrm{mod} 2q \end{aligned} \tag{1}$$

Therefore, $e = h(\sum_{i\in L} h_i \mathrm{mod} 2q, \mu)$.

5.2. Security Analysis

Lemma 4. *For the tuple* (i_0, i_1, R, μ), *a message* μ, *the ring* $R = (A_1, A_2, \ldots, A_n)$, *and* i_0 *and* i_1 *are indices with* A_{i_0}, A_{i_1}. *If the SIS problem is hard,* $\sigma_{i_0} \leftarrow Sign(sk_{i_0}, R, \mu)$ *and* $\sigma_{i_1} \leftarrow Sign(sk_{i_1}, R, \mu)$ are computationally indistinguishable.

Proof. Let $Y_{b,\mathcal{P},sk_{i_b},\mu}$ be some uniform distribution in ring R; there is a random variable describing the output of $Ring - sign(b, sk_{i_b}, R, \mu)$ with ring R, where sk_{i_b}, μ denotes a group of arbitrary inputs and $b \in \{0, 1\}$. If the domains of the above variables are different, it means that the signature fails. Then, we have

$$\Delta(Y_{0,\mathcal{P},sk_{i_0},\mu} - Y_{1,\mathcal{P},sk_{i_1},\mu}) = n^{-\omega(1)} \tag{2}$$

Therefore, σ_{i_0} and σ_{i_1} have the same domain distribution within a negligible statistical distance of $\Delta(Y_{0,\mathcal{P},sk_{i_0},\mu} - Y_{1,\mathcal{P},sk_{i_1},\mu})$, and this means that σ_{i_0} and σ_{i_1} are computationally indistinguishable. □

Theorem 2. (Anonymity): *Our ring signature scheme is anonymous under the hardness of SIS*.

Proof. To prove the security of our scheme, there are the following two cases: ① Signatures created by ring signers and non-signers are entirely indistinguishable. ② The attacker cannot obtain the private key of the signer by utilizing the public key of all ring members in polynomial time. □

On one hand, in Algorithm 2, the signer using its private key generates the tuples $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$. For $1 \leq i = j \leq L$, $s_j = y_j + k_j + (-1)^b S_j \widetilde{e}$; whereas the other part is produced utilizing public keys of the ring non-signer, i.e., $s_i = y_i + k_i$, where $1 \leq i \neq j \leq L$. In the meantime, we rewrite this part $s_i = (y_i + (-1)^b S_i \widetilde{e}) + (k_i - (-1)^b S_i \widetilde{e}) \mathrm{mod} 2q = y'_i + k'_i \mathrm{mod} 2q$, where

$y'_i = y_i + (-1)^b S_i\widetilde{e}$,$k'_i = k_i - (-1)^b S_i\widetilde{e}$, which means that the probability of distinguishing between the uniformly created sample and the $s_i = y'_i + k'_i \bmod 2q$ sample is negligible. Thus, in the attacker's view, the signatures created by the ring signer and the ring non-signer are indistinguishable.

On the other hand, assume that there exists an adversary $\mathcal{A}$ generating a forgery $\sigma_L(\mu)^*$ with probability ε'. We build an algorithm $\mathcal{C}$ that utilizes $\mathcal{A}$ to solve the instance of the SIS problem with probability ε. To respond to $\mathcal{A}$'s queries, $\mathcal{C}$ maintains three lists h, F, and $\mathcal{G}$, which are initialized to null and store tuples of values. Then, $\mathcal{C}$ interacts with $\mathcal{A}$ as follows:

In the Setup phase, $\mathcal{C}$ produces $A_i \in \mathbb{Z}_{2q}^{n\times m}$ and $S_i \in \mathbb{Z}_{2q}^{m\times n}$. $\mathcal{C}$ stores the tuple (i, A_i, S_i), where $i \in L = \{1, 2, \ldots, n\}$ in list $\mathcal{G}$ and the related parameters $(A_1, A_2, \ldots, A_n)$ are given to $\mathcal{A}$. In the query phase, $\mathcal{C}$ responds to the three queries of $\mathcal{G}$ as below:

Hash queries: $\mathcal{C}$ submits a random value $y_i \leftarrow D_{\sigma_2}^m$ to $\mathcal{A}$ and stores (y_i, h_i) in h-list. In addition, $\mathcal{C}$ picks a random value e to $\mathcal{A}$ and stores it in F-list.

Corruption queries: $\mathcal{C}$ searches for the tuple (i, A_i, S_i) in $\mathcal{G}$-list and responds to $\mathcal{A}$ with S_i.

Signing queries: $\mathcal{C}$ calculates the signature with the below steps:

(1) For all $i \in L = \{1, 2, \ldots, n\}$, calculate $h_i = x_i + A_i k_i \bmod 2q$, $x_i = A_i y_i \bmod 2q$, where $i \in L = \{1, 2, \ldots, n\}$.
(2) Calculate $e = (\sum_{i\in L} h_i \bmod 2q, \mu)$ and $\widetilde{e} = F(e)$.
(3) Pick a random bit $b \in \{0, 1\}$; calculate $s_j = y_j + k_j + (-1)^b S_j\widetilde{e}$, where $i = j$.
(4) For $i \neq j$, compute $s_i = y_i + k_i \bmod 2q$.
(5) Publish $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$.

$\mathcal{C}$ returns the signature $\sigma_L(\mu)$ to $\mathcal{A}$.

Analysis. In a way, $\mathcal{A}$ performs the Ring-signing with (i_0, i_1, R, μ) and public key pk_{i_0}, pk_{i_1} over ring R; $\mathcal{C}$ retrieves the tuple (y_i, h_i) in h-list. $\mathcal{C}$ calculates the challenge signature $\sigma_L(\mu)^*$ and sends $\sigma_L(\mu)^*$ to $\mathcal{A}$. Finally, $\mathcal{A}$ outputs a guess $b \in \{0, 1\}$. From the viewpoint of $\mathcal{A}$, the behavior of $\mathcal{C}$ is statistically close to the one provided by the real adaptive security experiment. We find that the ring members calculate $e^* = (\sum_{i\in L} h_i \bmod 2q, \mu^*)$, $\widetilde{e}^* = F(e^*)$, ${s_j}^* = y_j + k_j + (-1)^b S_j\widetilde{e}^*$(for $i = j$), and ${s_i}^* = y_i + k_i$(for $i \neq j$). $\mathcal{C}$ outputs $\sigma_L(\mu)^* = (\{{s_i}^*\}_{i\in L=\{1,2,\ldots,n\}}, e^*)$ as a signature of μ^*.

If $\mathcal{A}$ provides another success probability in distinguishing between i_0 and i_1 with a non-negligible probability, it seems to contradict Lemma 4. Thus, we declare that the advantage of $\mathcal{A}$ guessing the correct information in the simulated anonymous game is negligible.

Theorem 3. (Unforgeability): *Our ring signature scheme is unforgeable by insider corruption assuming that the SIS problem is hard.*

Proof. To prove the security of our scheme, the following two cases were considered: ① The attacker cannot break the security assumption of the scheme. ② The attacker cannot find the collision in the anti-collision hash function. Regarding the above two problems, we start the proof of this part. □

Assume that there exists an adversary $\mathcal{A}$ that creates a forgery $\sigma_L(\mu)^*$ with probability ε'. We build an algorithm $\mathcal{C}$, which utilizes $\mathcal{A}$ to solve the instance of the SIS problem with probability ε. Then, $\mathcal{C}$ interacts with $\mathcal{A}$ as follows:

$\mathcal{C}$ picks $i \in L = \{1, 2, \ldots, n\}$ and guesses the size of the challenge ring. In addition, $\mathcal{C}$ selects a vector $t = (t_1, t_2, \ldots, t_n)$. To respond to $\mathcal{A}$'s hash queries and signing queries in the random oracle, $\mathcal{C}$ will maintain three lists, h, F, and $\mathcal{G}$, which are initialized to be empty and will store tuples of values. For any $i \in L = \{1, 2, \ldots, n\}$ and $i \notin t$, $\mathcal{C}$ produces $A_i \in \mathbb{Z}_{2q}^{n\times m}$ and $S_i \in \mathbb{Z}_{2q}^{m\times n}$. $\mathcal{C}$ stores the tuple (i, A_i, S_i), where $i \in L = \{1, 2, \ldots, n\}$ in list $\mathcal{G}$ and the relevant parameters $(A_1, A_2, \ldots, A_n)$ are sent to $\mathcal{A}$.

Query Phase: $\mathcal{C}$ responds to adaptive queries from $\mathcal{A}$ on any message μ as follows:

Hash queries: $\mathcal{C}$ submits a random value $y_i \leftarrow D_{\sigma_2}^m$ to $\mathcal{A}$ and stores (y_i, h_i) in h-list. In addition, $\mathcal{C}$ sends a random value e to $\mathcal{A}$ and stores it in F-list.

Corruption queries: $\mathcal{C}$ searches for the tuple (i, A_i, S_i) in $\mathcal{G}$-list and responds to $\mathcal{A}$ with S_i.

Signing queries: $\mathcal{C}$ calculates the signature $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$ for the requested message and returns the signature $\sigma_L(\mu)$ to $\mathcal{A}$.

Namely, $\mathcal{A}$ receives signature $\sigma_L(\mu)$ and computes as follows:

$$\begin{aligned}&\Pr[Forge - sign_{\mathcal{A}}(\lambda) = 1] = \Pr[Forge - sign_{\mathcal{A}}(\lambda) = 1 \cap Hash - collision_{\mathcal{A}}(\lambda)]\\&+\Pr[Forge - sign_{\mathcal{A}}(\lambda) = 1 \cap \overline{Hash - collision}_{\mathcal{A}}(\lambda)]\\&\leq \Pr[Hash - collision_{\mathcal{A}}(\lambda)] + \Pr[Forge - sign_{\mathcal{A}}(\lambda) = 1 \cap \overline{Hash - collision}_{\mathcal{A}}(\lambda)]\end{aligned}$$

where $\Pr[Forge - sign_{\mathcal{A}}(\lambda) = 1]$ represents that $\mathcal{A}$ can find the probability of collision in the hash function, and $\Pr[Hash - collision_{\mathcal{A}}(\lambda)]$ denotes the probability of creating a forgery of the signature.

Challenge: Finally, $\mathcal{A}$ outputs a forgery signature $\sigma_L(\mu)^* = (\{s_i{}^*\}_{i\in L=\{1,2,\ldots,n\}}, e^*)$. If $R^* = R$, $\mathcal{C}$ aborts. Otherwise, $\mathcal{C}$ skips the tuple (y_i, h_i) in h-list and outputs $\sigma_L(\mu)^*$ as a collision of μ.

Analysis. To some extent, the view of $\mathcal{A}$ in the adaptively chosen message attack is the same as the view provided by $\mathcal{C}$. For each distinct query h_i and F, $\mathcal{C}$ returns $e = (\sum_{i\in L} h_i \mathrm{mod} 2q, \mu)$ and $\widetilde{e} = F(e)$. Through the unified output characteristics of the constructed hash function, it is the same as a uniform random value of $(\sum_{i\in L} h_i \mathrm{mod} 2q, \mu)$ in the real environment. Thus, $\mathcal{A}$ outputs a valid forgery $\sigma_L(\mu)^*$ negligibly close to ε.

Suppose $\mathcal{A}$ creates a response $(s_i, \widetilde{e})$ in the hash query, which is $h(A_i s_i + q\widetilde{e}, \mu) = h(A_i s_i{}^* + q\widetilde{e}^*, \mu^*)$ f or two different signatures (s_i, e, μ) and $(s_i{}^*, e^*, \mu^*)$. From the above signature, there is a hash collision if $\mu^* \neq \mu$ or $A_i s_i + q\widetilde{e} \neq A_i s_i{}^* + q\widetilde{e}^*$ holds. However, this is impossible according to the characteristics of hash function. Thus, $\mu^* = \mu$ or $A_i s_i + q\widetilde{e} = A_i s_i{}^* + q\widetilde{e}^*$. The following equation holds:

$$A_i(s_i - s_i{}^*) = 0 \mathrm{mod} 2q$$

since $\|s_i\|_\infty \leq q/4$ and $\|s_i{}^*\|_\infty \leq q/4$, this is $s_i - s_i{}^* \neq 0 \mathrm{mod} 2q$, where the condition on $\|s_i - s_i{}^*\|$ is $2B_2$. This means that the SIS problem can be solved.

According to the proof of [26], suppose $\mathcal{C}$ publishes a forgery e_t to the forger as a response. Then, we set a ring signature (s_t, e_t) for a message μ. Therefore, for any different values $(e'_1, e'_2, \ldots, e'_\rho) \leftarrow \mathrm{T}^k$ and $b \leftarrow \mathrm{T}^n$. The algorithm of the same time-complexity as the forger observes $(e_t - e'_t) \neq 0 \mathrm{mod} 2q$ with probability is:

$$\Pr[(e_t - e'_t) \neq 0] = (\varepsilon - \frac{1}{\mathrm{T}_k^n})(\frac{\varepsilon - \frac{1}{\mathrm{T}_k^n}}{b} - \frac{1}{\mathrm{T}_k^n}) \tag{3}$$

Next, $\mathcal{C}$ produces a response s_j to $\mathcal{A}$. We assume that there is a ring signature $(e^*, s_j{}^*)$ of μ^*, and $\mathcal{A}$ picks the various $(s_1{}^*, s_2{}^*, \ldots, s_n{}^*)$. Since $\widetilde{e} = F(e)$, $\widetilde{e}^* = F(e^*)A_j s_j + q\widetilde{e} \neq A_j s_j{}^* + q\widetilde{e}^*$; this is $A_j(s_j - s_j{}^*) \neq q(\widetilde{e}^* - \widetilde{e})$. Since $\widetilde{e}^* - \widetilde{e} \neq 0 \mathrm{mod} 2$, this is $s_j - s_j{}^* \neq 0 \mathrm{mod} 2q$. Furthermore, we find $\|\widetilde{e}^* - \widetilde{e}\|_\infty \leq q/2$; this implies $v = s_j - s_j{}^* \mathrm{mod} 2q$. Thus, $A_i v = 0 \mathrm{mod} 2q$; $\|v\| \leq 2B_2$. It means that we can obtain the solution to the SIS problem.

In other words, so long as $\mathcal{A}$ successfully breaks through the strong unforgeability of our scheme, $\mathcal{C}$ can effectively solve the SIS problem. Thus, the probability of successfully solving the SIS problem is negligible.

On the other hand, if a hash collision does not exist in our scheme, that means $\mathcal{A}$ generates the forged valid signature on message μ if $\mathcal{A}$ finds the private key of $\mathcal{C}$ using R. In fact, the hardness of the SIS problem, the problem of $\Pr[Forge - sign_{\mathcal{A}}(\lambda) =$

$1 \cap \overline{Hash - collision}_{\mathcal{A}}(\lambda)]$, is the probability of finding a private key by utilizing the corresponding public key, but the case is negligible.

6. Performance Evaluation

6.1. Parameter Selection

There are some parameters in our ring signature scheme, as illustrated in Table 1, that were chosen in the same way as [14]. They are secure against direct lattice attacks in terms of the algorithm Hermite factor δ, using the value of $\delta = 1.007$. In addition, the complexity of the SIS problem should be achieved by appropriate selection of parameters n, m, q, κ, where κ represents the challenge size that meets $2^{\kappa} \cdot \begin{pmatrix} n \\ \kappa \end{pmatrix} \geq 2^{-100}$. Then, the correctness error of the rejection sampling will be within at most 2^{-100}. As illustrated in Lemma 1 and Lemma 2, the equation below holds that

$$\frac{D_{\sigma}^{m}(s_j)}{MD_{v,\sigma}^{m}(s_j)} = \frac{1}{M \exp(-\frac{\left\|S_j \cdot e\right\|^2}{2\sigma^2}) \cosh(\frac{\langle s_j, S_j \cdot e \rangle}{\sigma^2})} \leq 1 \tag{4}$$

Thus, we set $M = \dfrac{1}{\exp(-\frac{\left\|S_j \cdot e\right\|^2}{2\sigma^2}) \cosh(\frac{\langle s_j, S_j \cdot e \rangle}{\sigma^2})}$. For $\sigma = 12\left\|S_j \cdot e\right\|$ from Lemma 2, M = 1.0027.

Next, we analyzed the parameters in the proposed scheme that satisfied the following conditions, as shown in Table 1.

Table 1. Parameter settings.

Parameter	Description	Sample
n	Polynomial ring degree	512
q	Large prime	2^{25}
m	Polynomial ring size	6
λ	Security parameter	100
δ	Hermite factor	1.007
κ	Random Oracle weight	14
η	Correctness	1.1
$\sigma_1 = 12\sqrt{\kappa}$	Rejection sampling	45
M_1	Rejection sampling	1.0027
$\sigma_2 = 12\eta\sigma_1\sqrt{m\kappa}$	Gaussian standard deviation	$2^{12.5}$
M_2	Rejection sampling	1.0027
$\sigma_3 = 12\eta\sigma_2\sqrt{m}$	Gaussian standard deviation	$2^{17.5}$
M_3	Rejection sampling	1.0027
Public key size	$n^2 m \log 2q$	4992 KB
Secret key size	$n^2 m \log 2q$	4992 KB
Signature size	$nm \log(12\sigma)$	672 KB

6.2. Efficiency Analysis

We analyzed the performance of elements of our scheme, such as the public key size, private key size, and signature size; the related details of the efficiency analysis are shown in Table 2. Then, we computed the signature size for the different security levels, such as 100, 128, 256, and 512 bits, and the results are shown in Table 2.

Table 2. Comparison of different security levels.

Security Level (bits)	Signature Size (KB)
100	672
128	684
256	768
512	825

As shown in Figure 2, the signature size of our proposed scheme increased rapidly as the security level increased. However, the increase in signature size in this scheme was small. The size of the signature remained stable regardless of the security level. In addition, the proposed scheme resisted quantum attacks. Thus, with the advent of quantum computers, lattice-based cryptography will gradually be integrated into practical scenarios in the future quantum age.

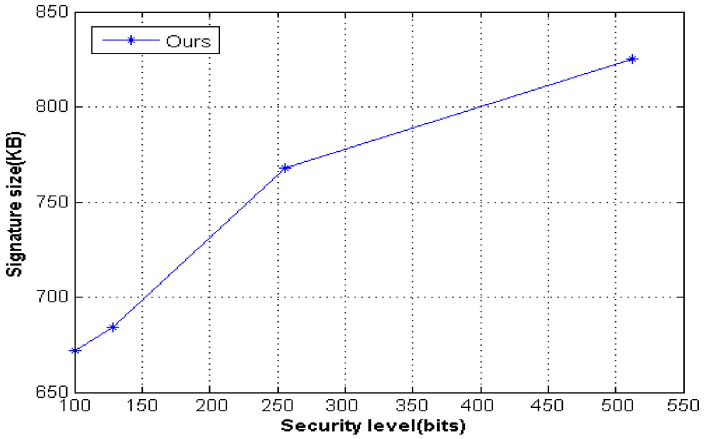

Figure 2. Different security levels of our scheme.

6.3. Performance Comparison

In our scheme, the ring contains n members; the total space complexity is $O(n)$. Suppose that the time of multiplication operation is T_{mult}, non-interactive zero-knowledge proof operation is T_n, and hash operation is T_h. We provided a comparison of our scheme and the relevant schemes in terms of ring-sign, ring-verify costs, and signature length, as illustrated in Table 3. The addition was neglected in our scheme.

Table 3. Comparison costs of relevant schemes.

Schemes	Ring-Sign Costs	Ring-Verify Costs	Signature Length
Cui et al. [16]	$5nT_{mult}$+T_h	$5nT_{mult} + T_n$	$2(n+1)m$
Liu et al. [17]	$2nT_{mult} + nT_h$	$2nT_{mult} + nT_h$	$(n+1)m$
Mundhe et al. [27]	$(3n+1)T_{mult} + 2T_h$	$2nT_{mult} + 2T_h$	$(n+1)m$
Feng et al. [21] scheme 1	$nT_{mult} + T_n + 2T_h$	$nT_{mult} + T_n + 2T_h$	$(n+1)m$
Feng et al. [21] scheme 2	$3nT_{mult} + T_n + 2T_h$	$3nT_{mult} + T_n + 2T_h$	$(n+1)m$
Han et al. [28]	$4nT_{mult} + 2T_h$	$4nT_{mult} + 2T_h$	$(n+1)m$
Ours	$(2n-1)T_{mult} + 2T_h$	$(n+1)T_{mult} + 2T_h$	$nm + \kappa(\kappa \leq m)$

From Table 3, we found that our scheme was highly efficient, and the computational costs of ring signature generation and verification were lower than those in the literature [16,17,21,27,28]. Next, we performed the functionality comparison of the related schemes, as shown in Table 4. In Table 4, we compared the performance of our proposed scheme with the current prevailing schemes, i.e., Wang et al. [11], Cui et al. [16], Liu

et al. [17], Mundhe et al. [27], Feng et al. [21], Han et al. [28], Cai et al. [29]. The scheme of Cai et al. [29] could not resist quantum attack. Mundhe et al. [27], Han et al. [28], and our scheme satisfied both unconditional anonymity and strong unforgeability.

Table 4. Functionality comparison of relevant schemes.

Schemes	Unconditional Anonymity	Strong Unforgeability	Message Integrity
Wang et al. [11]	No	Yes	Yes
Cui et al. [16]	No	No	Yes
Liu et al. [17]	No	No	Yes
Mundhe et al. [27]	Yes	No	Yes
Feng et al. [21]	No	No	Yes
Han et al. [28]	Yes	Yes	Yes
Cai et al. [29]	No	No	Yes
Ours	Yes	Yes	Yes

We performed the same scenario as the literature [30] and applied the relevant operation parameters. Next, we evaluated the performance of the related schemes under the same quantum environment. In Figure 3, we provided the ring-sign and ring-verify operation times of the relevant schemes for the numbers of ring members. In addition, our scheme was a ring signature scheme without a trapdoor; we can confirm that our scheme functioned better than the other schemes.

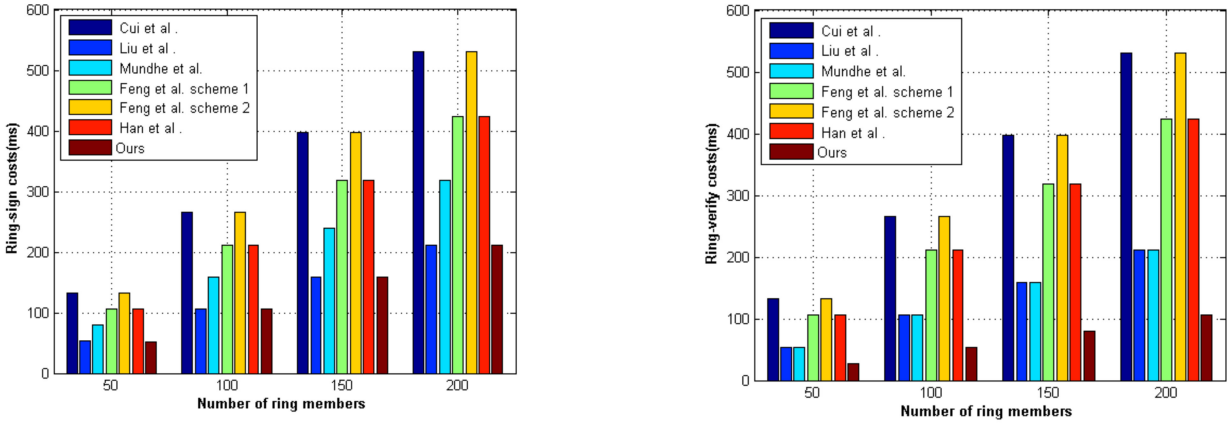

Figure 3. Computation costs of the different schemes.

7. Sharper Ring Rignatures

We presented another extension of the scheme that achieves faster key generation, signature, and verification than most (traditional or lattice-based) signature schemes. We chose the relevant parameters, including a high-security environment against quantum attacks. The details are described as follows.

Key generation: Given a security parameter λ, and some other parameters n, m, q, i, j, for any integer q, we write $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ for simplicity. The ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ is isomorphic to $\mathbb{Z}_q$. Let a hash function $h : \{0,1\}^* \to \{v : v \in \{-1,0,1\}^n, \|v\|_1 \leq \kappa\}$, nearly injective mapping $F : \{0,1\}^\kappa \to \mathbb{B}_{2q}$ and $i \in L = \{1,2,\ldots,m\}$, $A = (a_1, a_2, \ldots, a_{m-1})$, $a_i \in R_q$, where $A \in R_q^{1\times(m-1)}$. Let $A_{q,i} \in R_q^{1\times(m-1)}$ and $S_{q,i} \in R_q^{(m-1)}$ be public/private keys of the user with index i, respectively, such that key pairs meet $A_{q,i}S_{q,i} = a_i$ ($S_{q,i}$ is invertible). Let $A_{2q,i} = [2A_{2q,i}, q - 2a_i] \in R_{2q}^{1\times m}$; this is $pk = (\{A_{2q,i}\}_{i\in L}, \{A_{q,i}\}_{i\in L-1},)$, $sk = \{S_{q,i}\}_{i\in L}$. The system publishes $\mathcal{P} = (L, pk, h, F, n, m, q)$.

Ring-Sign: On input a message μ, a long-term key $S_{q,j}$, a ring of m members with public keys pk, a user i selects a uniform value $k_i \leftarrow D_{\sigma_1}^m$ and performs the algorithm

$x_i = A_{2q,i}y_i \bmod 2q$ with the random vector $y_i \leftarrow D_{\sigma_2}^m$, and outputs the signature $\sigma_L(\mu)$ of the message μ. Then, the user i performs the following computations:

(1) Set $S_{q,j}^T \in R_q^{(m-1)\times 1}$ and $S_{2q,j}^T = (S_{q,j}^T, 1) \in R_{2q}^{m\times 1}$ such that $A_{2q,i}S_{2q,i} = q$.
(2) For all $i \in L$, calculate $h_i = x_i + A_{2q,i}y_i \bmod 2q$, where $L = \{1, 2, \ldots, m\}$.
(3) Calculate $e = (\lfloor \sum_{i\in L} h_i \rfloor_d, \mu)$, where $\lfloor \sum_{i\in L} h_i \rfloor_d$ denotes high-order bits of $\sum_{i\in L} h_i$.
(4) Calculate $\widetilde{e} \leftarrow F(e)$.
(5) Pick a random bit $b \in \{0, 1\}$; calculate $s_j = y_j + k_j + (-1)^b S_{2q,j}\widetilde{e}$, where $i = j$.
(6) For $i \neq j$, compute $s_i = y_i + k_i \bmod 2q$.
(7) Publish $\sigma_L(\mu) = (\{s_i\}_{i\in L=\{1,2,\ldots,n\}}, e)$.

Ring-Verify: Given a signature $\sigma_L(\mu)$, a message μ, and a bit b, the algorithm outputs a response and answers: accept or reject. The signature $\sigma_L(\mu)$ can be checked and is only accepted under the following conditions: $\|s_i\|_2 \leq B_2$ and $\|s_i\|_\infty \leq q/4$ for $1 \leq i \leq n$.

(1) $s_i \leftarrow D_{\sigma_3}^m$
(2) $e = (\lfloor \sum_{i\in L} A_{2q,i}s_i + q\widetilde{e} \rceil_d, \mu)$

If the above verifications hold, the signature is valid, and the verifier outputs 1; otherwise, it outputs 0.

8. Applications in VANETs

Vehicular ad hoc networks (VANETs) are a kind of mobile ad hoc network that can intelligently control the entire traffic process and improve traffic efficiency and security. They include two communication modes: vehicle to vehicle (V2V) and vehicle-to-infrastructure (V2I). In VANETs, there exist three types of entities that include the trusted authority (TA), on-board units (OBUs), and roadside units (RSUs), as shown in Figure 4.

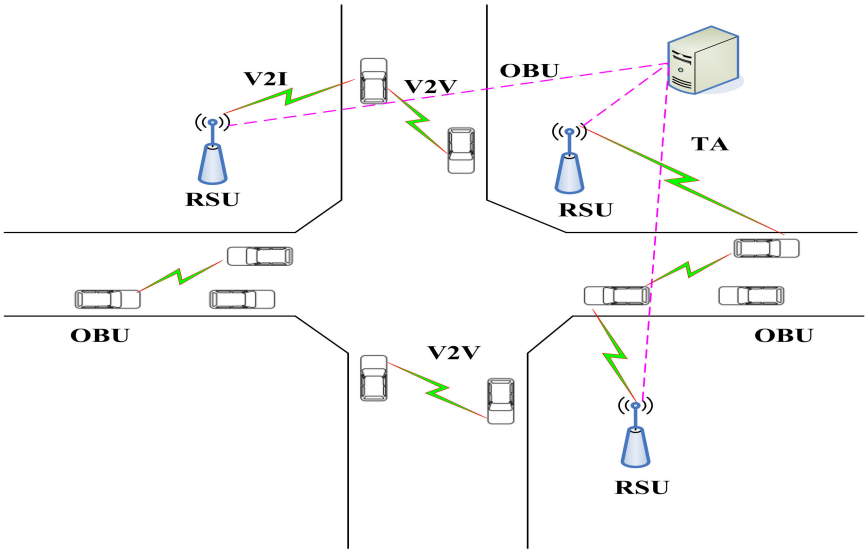

Figure 4. The architecture of a VANET.

TA: TA is responsible for the enrollment of the OBUs and RSUs and produces the system's public parameters and private key.

OBU: The OBU can share the corresponding traffic information with other vehicles or RSU under the support of the DSRC protocol. Each vehicle is equipped with an OBU. The OBU can send basic information to the RSU and OBUs of other vehicles and verify the received information. Each OBU contains a tamper-proof device (TPD) and a global positioning system (GPS), which ensure that the information stored in it will not be disclosed. The GPS is used to provide geographic location and time information services while driving.

RSU: The RSU is a fixed infrastructure installed along the roadside. The RSU enters VANETs through wireless connection and is managed by the traffic management department through trusted authorization. The RSU verifies the signature immediately after receiving the information from the vehicles. If the signature is valid, the RSU can broadcast the vehicle's identity information. Otherwise, the RSU discards the relevant information. In addition, the RSU communicates with neighbor RSUs at the same time.

To achieve security authentication, we considered a new privacy protection scheme for VANETs, where the connected vehicles form a common ring with nearby vehicles. In our network model, most information comprised vehicles periodically broadcasting sign messages and RSUs broadcasting public information, but the message was associated with responsibility. Before confirming whether the message came from a legal member of the network, we had to verify it effectively, so we used ring signature technology. The vehicles used the ring signature to sign the subsequent messages so as to effectively hide their real identity under the premise of ensuring the authenticity of the message and to realize anonymous communication in the VANETs. We applied the ring signature to the RSU to help the vehicles quickly form a ring with nearby vehicles.

8.1. Experimental Simulation

Without a loss of generality, assume that, in a heavily vehicular area of the city, there are enough vehicles and enough time to form a ring. The time of signature generation is acceptable relative to the time of passing by the base station, which means that our proposed scheme can meet the requirements of composing rings and generating ring signatures. We used the network simulator NS3 [31] to simulate our scheme and employed an Intel Core2 (TM) i5-7300 with 3.4-GHz frequency rate and Windows 10 platform to implement the experiment. We simulated the operation of the vehicle network communication scheme in a real traffic environment. Since the speed is affected by the number of vehicles, we simulated a 1 km-long intersection situation and considered the average speed of the vehicle to be 20 km/h. The RSU was located in the middle of the intersection, the fixed speed was 50 B/s in the network bandwidth, and the transmission bound of the vehicle was 100 m, as illustrated in Table 5. In addition, the area of the simulation was 1×1 km^2, which was controlled by an RSU.

Table 5. Simulation parameters.

Parameter	Value
Speed of vehicle	20 km/h
Transmission range	100 m
Time interval	2 s
MAC type	IEEE 802.11p
Number of lanes	4

8.2. Simulation Results

We evaluated the effectiveness of our proposed scheme from two aspects: end-to-end delay (E2ED) and throughput (THP). E2ED represents the average delay time spent by data packets. THP represents the average number of bits of information transmitted per unit time, as shown in Figures 5 and 6.

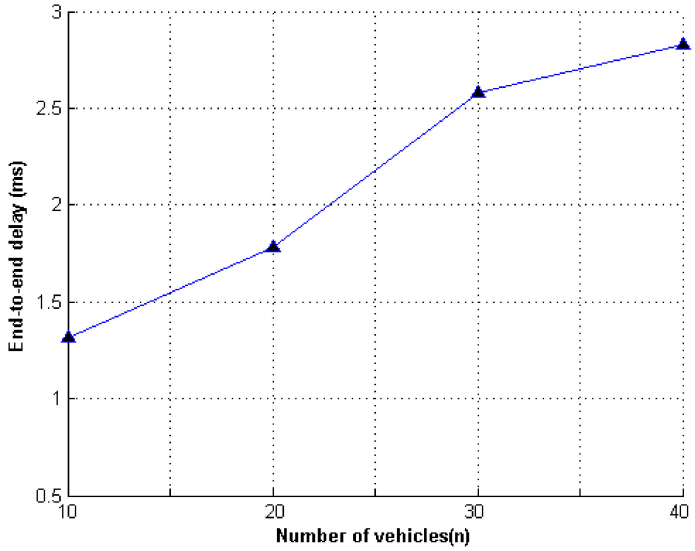

Figure 5. The vehicle density and E2ED delay.

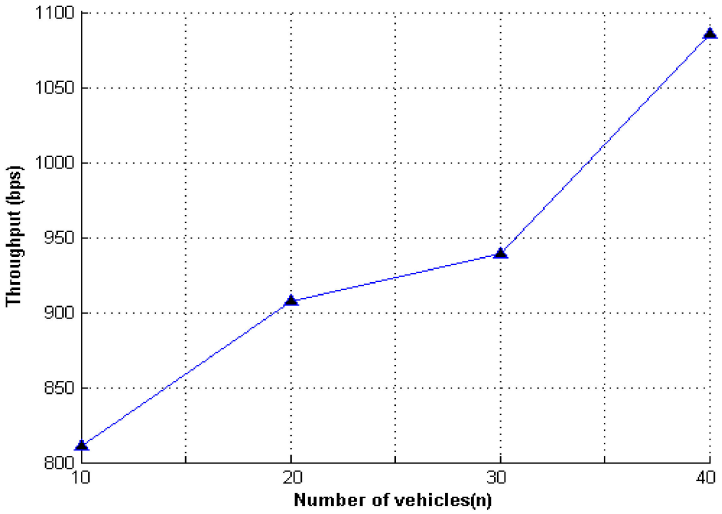

Figure 6. The vehicle density and data throughput.

Figures 5 and 6 show the simulation results of the experiment. The message authentication delay values were related to vehicle density, where vehicle density represented the number of vehicles within the range of the RSU at a given time. With the continuous increase in vehicles, the scale of the formed ring continued to change. Therefore, with the increase in ring members, the message authentication delay and throughput continued to increase as the vehicle density increased.

9. Conclusions

The post-quantum secure ring signature is an important part of post-quantum cryptography and provides a cryptographic tool for user privacy protection in the post-quantum era. Most existing lattice-based ring signature schemes rely on the lattice-based trapdoor function, but the parameters are too large and the efficiency is low, resulting in their inefficiency. In this paper, we proposed a way of building a lattice-based ring signature scheme without a trapdoor. This scheme is a practical lattice-based dynamic ring signature scheme that is suitable for large-scale and scalable application scenarios. Then, we proved its security under the hardness of the SIS problem: the construction satisfied the properties of anonymity and unforgeability. Finally, we applied our scheme to the VANETs, and the simulation results showed that our scheme was feasible. In addition, the development of

quantum computers has made an impact on classical cryptography, and the reconstruction of public key cryptography based on the hard problems of anti-quantum computing is the main development direction in the future.

Author Contributions: Conceptualization, C.J.; methodology, C.J.; software, X.X.; formal analysis, X.X.; investigation, C.J.; writing—original draft preparation, C.J.; writing—review and editing, C.J.; supervision, X.X.; funding acquisition, X.X. All authors have read and agreed to the published version of the manuscript.

Funding: The Natural Science Basic Research Plan in Shaanxi Province of China (No. 2019JM261), the Foundation of China (Xi'an) Institute for Silk Road Research (No. 2016SY19), and the Support Research Foundation of Xi'an University of Finance and Economics (No. 18FCZD01).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that the research has no conflict of interest to report regarding the present study.

References

1. Chaum, D.; Van Heyst, E. Group Signatures. In *Eurocrypt*; Cramer, R., Ed.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3494, pp. 457–473.
2. Rivest, R.; Shamir, A.; Tauman, Y. *How to Leak a Secret, Advances in Cryptology-ASIACRYPT 2001*; Laboratory for Computer Science, Massachusetts Institute of Technology: Cambridge, MA, USA, 2001.
3. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 September 2021).
4. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In Proceedings of the 40th Annual ACM Symposium on Theory of Computing STOC'08, Victory, BC, Canada, 17–20 May 2008; pp. 197–206.
5. Buchmann, J.; Lindner, R.; Ruckert, M.; Schneider, M. Post-quantum cryptography: Lattice signatures, computing. *Computing* **2009**, *86*, 105–125. [CrossRef]
6. Boyen, X. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 499–517.
7. Brakerski, Z.; Kalai, Y.T. A framework for efficient signatures, ring signatures and identity-based encryption in the standard model. *IACR Cryptol. ePrint Arch.* **2010**, *2010*, 86.
8. Liu, J.K.; Au, M.H.; Susilo, W.; Zhou, J. Linkable ring signature with unconditional anonymity. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 157–165. [CrossRef]
9. Duan, J.; Gu, L.; Zheng, S. ARCT: An efficient aggregating ring confidential transaction protocol in blockchain. *IEEE Access* **2020**, *8*, 198118–198130. [CrossRef]
10. Jia, H.; Tang, C.; Zhang, Y. Lattice-based logarithmic-size non-interactive deniable ring signatures. *Entropy* **2021**, *23*, 980. [CrossRef] [PubMed]
11. Wang, Z.; Tang, D.; Yang, H.; Li, F. A public key encryption scheme based on a new variant of LWE with small cipher size. *J. Syst. Archit.* **2021**, *117*, 102165. [CrossRef]
12. Xiang, X.Y.; Li, H.; Wang, M.Y.; Zhao, X.W. Efficient multi-party concurrent signature from lattices. *Inf. Process. Lett.* **2016**, *116*, 497–502. [CrossRef]
13. Wang, S.; Zhao, R. Lattice-based ring signature scheme under the random oracle model. *Int. J. High-Perform. Comput. Netw.* **2018**, *11*, 332–341. [CrossRef]
14. Torres, A.; Steinfeld, R.; Sakzad, A.; Liu, J.K.; Kuchta, V.; Bhattacharjee, N.; Au, M.H.; Cheng, J. Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringct v1.0). In Proceedings of the Australasian Conference on Information Security and Privacy, Wollongong, Australia, 11–13 July 2018; Volume 2018, p. 379. Available online: http://eprint.iacr.org/2018/379.pdf (accessed on 10 September 2021).
15. Torres, W.A.; Kuchta, V.; Steinfeld, R.; Sakzad, A.; Liu, J.K.; Cheng, J. Lattice RingCT v2.0 with multiple input and multiple output wallets. *IACR Cryptol. ePrint Arch.* **2019**, *2019*, 569.
16. Cui, Y.; Cao, L.; Zhang, X.; Zeng, G. Ring signature based on lattice and VANET privacy preservation. *Chin. J. Comput.* **2017**, *40*, 1–14.
17. Liu, J.; Yu, Y.; Jia, J.; Wang, S.; Fan, P.; Wang, H.; Zhang, H. Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks. *Tsinghua Sci. Technol.* **2019**, *24*, 575–584. [CrossRef]
18. Esgin, M.F.; Steinfeld, R.; Sakzad, A.; Liu, J.K.; Liu, D. Short lattice-based one-out-of-many proofs and applications to ring signatures. In *Applied Cryptography and Network Security—ACNS 2019*; Springer: Cham, Germany, 2019; pp. 67–88.

19. Groth, J.; Kohlweiss, M. One-out-of-many proofs: Or how to leak a secret and spend a coin. In *Advances in Cryptology—EUROCRYPT 2015, Part II*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 253–280.
20. Langlois, A.; Stehle, D. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.* **2015**, *75*, 565–599. [CrossRef]
21. Feng, H.; Liu, J.; Li, D.; Li, Y.-N.; Wu, Q. Traceable ring signatures: General framework and post-quantum security. *Des. Codes Cryptogr.* **2021**, *89*, 1111–1145. [CrossRef]
22. Ajtai, M. Determinism versus non-determinism for linear time RAMs (extended abstract). In Proceedings of the 31st Annual ACM Symposium on Theory of Computing, Atlanta, GA, USA, 1–4 May 1999; ACM Press: New York City, NY, USA, 1999; pp. 632–641.
23. Micciancio, D.; Regev, O. Worst-case to average-case reductions based on Gaussian measures. In Proceedings of the 45th Annual Symposium on Foundations of Computer Science, Rome, Italy, 17–19 October 2004; IEEE Computer Society Press: Piscataway, NJ, USA, 2004; pp. 372–381.
24. Lyubashevsky, V. Lattice signatures without trapdoors. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012; Springer: Berlin/Heidelberg, Germany, 2012.
25. Zhang, Y.; Liu, Y.; Guo, Y.; Zheng, S.; Wang, L. Adaptively secure efficient (H)IBE over ideal lattice with short parameters. *Entropy* **2020**, *22*, 1247. [CrossRef] [PubMed]
26. Ducas, L.; Durmus, A.; Lepoint, T.; Lyubashevshy, V. Lattice signatures and bimodal gaussians. In *Advances in Cryptology-CRYPTO 2013*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8042, pp. 40–56.
27. Mundhe, P.; Yadav, V.K.; Verma, S.; Venkatesan, S. Efficient lattice-based ring signature for message authentication in VANETs. *IEEE Syst. J.* **2020**, *14*, 5463–5474. [CrossRef]
28. Han, L.; Cao, S.; Yang, X.; Zhang, Z. Privacy protection of VANET based on traceable ring signature on ideal lattice. *IEEE Access* **2020**, *8*, 206581–206591. [CrossRef]
29. Cai, Y.; Zhang, H.; Fang, Y. A conditional privacy protection scheme based on ring signcryption for vehicular Ad Hoc networks. *IEEE Internet Things J.* **2021**, *8*, 647–656. [CrossRef]
30. Cao, J.; Yu, P.; Xiang, X.; Ma, M.; Li, H. Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system. *IEEE Internet Things J.* **2019**, *6*, 9794–9805. [CrossRef]
31. Secure Hash Standard. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. Available online: http://csrc.nist.gov/publications/fips/fips1802/fips180-2.pdf (accessed on 20 July 2018).