Securing Internet of Vehicles with a provable secure post-quantum mutually authenticated protocol based on Small Integer Solution

WenBin Hsieh*
Department of Green Energy and Information Technology, National Taitung University
Taitung, 950309, Taiwan
[e-mail: wbhsieh@nttu.edu.tw, d9802106@mail.ntust.edu.tw]
*Corresponding author: WenBin Hsieh

Received June 30, 2024; revised August 17, 2024; accepted September 10, 2024; published October 31, 2024

Abstract

As technology advances, vehicular ad hoc networks (VANETs) have evolved into the Internet of Vehicles (IoVs), transforming the IoT landscape. IoV integrates automotive sensor to collect data from the environment, vehicles, and drivers, using wireless links that are vulnerable to attacks. This necessitates strong security measures to protect confidential data shared between vehicles and Road Side Units (RSUs). While earlier protocols are susceptible to quantum computer-enabled attacks, Gupta et al. proposed an identity-based mutual authentication protocol to address these concerns. However, this paper identifies several flaws in Gupta et al.'s protocol and introduces an enhanced identity-based mutual authenticated key agreement protocol that leverages small integer solution (SIS) problems. The security and efficiency of the proposed quantum-resistant protocol can be further enhanced by meticulously adjusting parameters, including lattice structures, computational complexity, and elliptic curve configurations such as curve order and field size. Furthermore, we utilize BAN logic for rigorous security validation of our solution, supplemented by performance benchmarks including communication efficiency and computational overhead, in comparison to related protocols. Additionally, we present a critical design perspective for key negotiation solutions. While no protocol is flawless at inception, our proposed solution substantially improves security in the IoT domain.

Keywords: Security, Internet of Things, Post-Quantum Cryptography (PQC), IoT Security

1. Introduction

Over the past few decades, variants of mobile ad hoc networks (MANETs) developed from Vehicular Ad Hoc Networks (VANETs) have played an important role in wireless communication systems. VANET inherits the characteristics of MANET as freely connected objects that can move randomly and communicate wirelessly. In a VANET, vehicles such as buses and cars function as mobile nodes, responsible for transmitting information among them and with traffic controllers [1,2]. Vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) are two primary modes to communicate within a VANET. Both communication types are regulated by the Dedicated Short Range Communications (DSRC) protocol. To facilitate and maintain this protocol, an On-Board Unit (OBU) is a special wireless equipment installed on vehicles to exchange information with nearby cars and other network nodes. Additionally, wireless devices known as Roadside Units (RSUs) are installed along the roadways to support and extend communication within the network. This structure of a VANET has limited ability to compute, store, and process information gathered by itself and other devices in the infrastructure. Due to the increasing number of vehicles on the network, VANET is converted into Internet of Vehicles (IoVs) [3]. Intelligent Vehicle Control is an example of a typical use of IoT in Intelligent Transportation Systems. That is, enabling smart vehicle control, smart dynamic information services, and smart road traffic management within an extensive network. [4]. Automotive sensor platforms are made possible by the Internet of Vehicles and can gather data from other cars, the environment, and drivers. All for better traffic regulation, pollution prevention, and navigation safety. As previously stated, the Internet of Vehicles (IoVs) is a network that allows cars to talk to each other, to pedestrians' handheld devices, to RSUs, and to public networks. through the use of Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Road (V2R), Vehicle-to-Human (V2H), and Vehicle-to-Sensor (V2S) interconnection, as shown in **Fig. 1** [5].

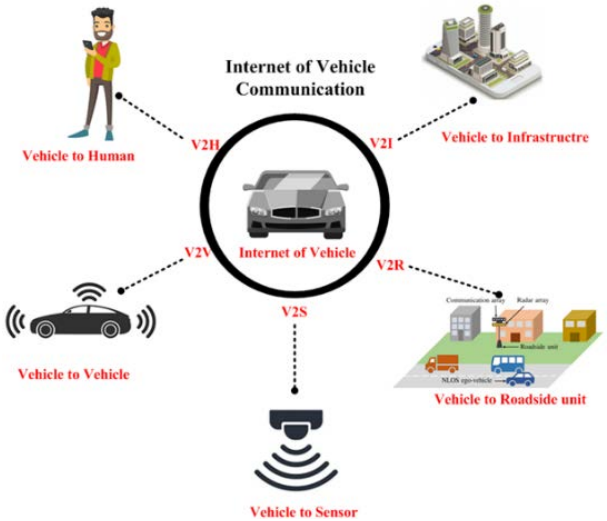

Fig. 1. Five types of network communication in IoV [5]

As a result, this creates a network in which smart gadgets are members. In the Internet of Vehicles, wireless open links are used for communication, providing attackers with complete access to these channels. Therefore, robust security measures are essential to safeguard the exchange of sensitive or confidential information between the vehicle and RSUs. In the context

of the IoV, vehicles and RSUs collectively function as "edge nodes." Any errors arising from changes in sensitive information can result in serious consequences, potentially leading to traffic accidents and endangering human lives. Hence, edge nodes in the Internet of Vehicles need to verify one another and preserve the accuracy of shared data. Because of this, an authenticated key agreement (AKA) protocol is required so that edge nodes in the Internet of Vehicles (IoVs) can safely exchange sensitive data.

2. Related works

Edge nodes on the Internet of Vehicles need to produce secret session keys in order to securely connect and authenticate with one another. The foundation for such secure key exchange was established in 1976 when Diffie and Hellman [6] introduced a key agreement protocol, which for the first time enabled the remote negotiation of session keys between participants without prior knowledge of each other. However, pioneering innovations frequently rely on assumptions that may subsequently be revealed as insufficient. Since the D-H protocol does not provide any authentication mechanism, various attacks have been proposed. In order to enhance the security and efficiency of D-H protocol, many improvements [7-12] using different authentication techniques have been proposed. Elliptic curve cryptography was utilized by Mohammadali et al. [13] to create an identity-based key establishment mechanism for smart grids. However, some security issues in [13] were discovered and fixed by Mahmoud et al. [14]. They used the Random Oracle Model (ROM) [15] to evaluate the security of their protocol and verified that anonymity and untraceability were satisfied. For wireless sensor networks, Bala et al. [16] utilized the operation of elliptic curve scalar multiplication to propose an ID-2PAKA protocol. After that, a provable secure ID-based 2PAKA protocol for VANETs under the Gap Diffie-Hellman assumption was developed by Dang et al. [17]. They demonstrated its safety in the extended Canetti-Krawczyk (eCK) security model [18] and asserted that the proposed protocol was better in terms of both cost and security. In 2019, a VANET-compatible ID-2PAKA protocol was proposed by Li et al [19]. Their system takes two rounds to create session keys and does away with the need for intricate pairing operations. Jiang et al. [20] subsequently developed an authentication system for IoV based on physical unclonable functions. However, All AKA protocols mentioned above were found to be vulnerable to quantum attacks.

To counter the threat posed by quantum computers, cryptography related to the lattice-based hardness problems has been widely adopted. The lattice hard assumption was first suggested by Ajtai [21], leading to the rapid proliferation of protocols [22-26] based on this foundation. Wang et al. [27] further proposed a new extension of the SIS/ISIS problem and the Bi-SIS/Bi-ISIS problem based on a novel hard lattice problem. The CBi-ISIS problem and other decisional problems were also present by Wang et al. They developed a lattice-based key agreement protocol for two parties (LB-2PKA) based on these new problems. The proposed protocol is similar to the classic D-H protocol. However, the LB-2PKA proposed by [27] does not include authentication, making it vulnerable to a variety of attacks, inclusive of the renowned man-in-the-middle (MITM) exploit [28]. Gupta and Biswas [29] provided some security protection and designed two LB-2PAKA protocols to improve the protocol proposed in [28]. However, the protocol in [29] lacks formal proof and has expensive communication, storage and computational costs. Then Rana et al. [30] created a key agreement protocol on the Ring Learning with Errors (RLWE) problem, which is included in lattice-based cryptography. Islam et al. [31] introduced a provably secure identity-based two-party authenticated key agreement protocol, which relies on CBi-ISIS and Bi-SIS problems based on lattice hard assumptions. Additionally, they formally demonstrated their protocol using

ROM. In [32], Gupta et al. presented a two-party authenticated key agreement (LB-ID-2PAKA) protocol that employs identity-based and lattice-based cryptography. However, we found that the protocol in [32] is vulnerable to impersonation attacks and only achieves weak perfect forward secrecy. Therefore, in order to solve the problems of the Gupta protocol, we propose an improved mutual authenticated key agreement protocol (MAKA). The following is a summary of this article's primary contributions:

(1) We identify the vulnerabilities in Gupta et al.'s protocol and propose an improved identity-based mutual authenticated key agreement protocol, leveraging small integer solution (SIS) problems to counter the threat posed by quantum computers. The proposed protocol enhances security without adding significant computational, storage, and communication overhead.
(2) The fundamental security of the proposed protocol has been validated in [32], and we further substantiate its security properties by employing Burrows-Abadi-Needham (BAN) logic [33]. These proofs collectively reinforce the protocol's security.
(3) We emphasize a critical aspect: in key agreement protocols, it is vital to authenticate the key material by verifying its origin or ensuring its integrity. Neglecting this can expose the protocol to attacks such as impersonation.

This paper's remaining structure is set up as follows. The preliminaries are reviewed in section 3. In section 4, we depict the flaws or vulnerabilities of Gupta et al.'s protocol. Section 5 presents the details of the proposed protocol. Section 6 gives security analysis and performance comparison. Lastly, in section 7, a conclusion is given.

3. Preliminary

3.1 Lattice

Because of its robustness, lattice becomes a potent tool for cryptography in the future. In the presence of quantum computers, the cryptographic designs can be strengthened by the computational hardness of lattice problems. Any regular structure of form can be called a lattice The following can be used to establish the mathematical definition of the lattice:

Theorem 1. A lattice denoted by $\mathcal{K}$ with a set of vectors $x_1, x_2, x_3, \ldots, x_n \in R^m$ can be defined as:

$$\mathcal{K}(x_1, x_2, x_3, \ldots, x_n) = \{\sum_{i=1}^{n} a_i x_i : a_i \in Z^+\} \quad (1)$$

A basis vectors consists of the vectors x_1, x_2, x_3, …, x_n which must be linearly independently sets. The lattice's dimensions and rank are m and n respectively, as shown in equation (1).

The following formula may be used to determine the minimal distance of $\mathcal{K}$, which is the shortest non-zero vector in $\mathcal{K}$:

$$D_{min}(\mathcal{K}) = \min_{x \in \mathcal{K} \setminus \{0\}} \|x\| \quad (2)$$

Furthermore, a lattice $\mathcal{K}$ can have more than one basis, but it always needs one. However, there are the same number of elements in each set. Therefore, the lemma is defined as

Lemma 1. To produce the lattice $\mathcal{K}$, there has to be a minimum of one basis.

The basis of $\mathcal{K}$ can be expressed as a matrix X = $[x_1, x_2, x_3, \ldots, x_n] \in Z^{m \times n}$. Sets of basis vectors make up the columns of this matrix, which is known as the basis matrix. Now, the following equation may be used to further define a lattice $\mathcal{K}$:

Theorem 2. Let X = $[x_1, x_2, x_3, \ldots, x_n] \in Z^{m\times n}$ be a basis matrix, the matrix X can generate lattice $\mathcal{K}$ in R^m that is represented as $\mathcal{K}$(X) = [Xv : $v \in Z^n$] which Xv represents a general scalar dot product of vectors (matrix-vector multiplication).

The shortest vector problem (SVP) and the closet vector problem (CVP) are two examples of the fundamental hardness assumptions on lattices $\mathcal{K}$. The goal of SVP is to locate, on a given lattice $\mathcal{K}$, the shortest non-zero vector (with the least Euclidian norm). The idea of CVP is to locate the vector in $\mathcal{K}$ that is closest to the provided vector. The following is a definition of the assumptions:

Theorem 3. Shortest Vector Problem (SVP)

It is challenging to find a non-zero vector $v \in \mathcal{K}$(X) satisfied $\|v\|=D_{min}(\mathcal{K})$ given a lattice $\mathcal{K}$(X) and its basis matrix X $\in Z^{m\times n}$.

Theorem 4. Closest Vector Problem (CVP)

Considering a lattice $\mathcal{K}$(X), its basis matrix X $\in Z^{m\times n}$ and a vector $v \notin \mathcal{K}$, locating a non-zero vector $u \in \mathcal{K}$(X) such that $\|v-u\|=D_{min}(\mathcal{K})$ is difficult.

For an integer modulo $q \approx poly(m)$, a lattice $\mathcal{K}$ satisfying $Z_q^m \subseteq \mathcal{K} \subseteq Z^m$ is called a ***q-ary* lattice**. A ***q-ary* lattice** has the following definition:

Theorem 5. Considering a m-by-n modular matrix X $\in Z_q^{m\times n}$ for ($n > m$) and $n \approx poly(m)$, we can write two q-*ary* lattices $\Lambda_q^{\perp}$ and Λ_q as follows:

$$\Lambda_q^{\perp}(X) = \{ a \in Z^n : Xv = 0 \bmod q\} \tag{3}$$

And

$$\Lambda_q(X) = \left\{ v \in Z^n : v = X^T w \bmod q, \forall w \in Z^m \right\} \tag{4}$$

***Q-ary* lattices** have been the hard-on-average difficulty in many lattice-based innovations. Hard computational problems related to q-*ary* lattices are heavily used in developing cryptographic communication protocols. This article mainly involves two main problems on q-*ary* lattices (equations (3) and (4)), which are described as follows:

Theorem 6. Small Integer Solution (SIS) Problem

Let $n \in \mathbb{N}$, m, q, α be functions with domain $\mathbb{N}$. Consider $\alpha \in Z^+$ and a modular X $\leftarrow \cup(Z_q^{n\times m})$. Finding a vector $v \in Z^n \backslash \{0\}$ such that Xv = 0 mod q with $\alpha \geq \|v\|$ is a challenging task.

Theorem 7. Inhomogeneous Small Integer Solution (ISIS) Problem

Let $n \in \mathbb{N}$, m, q, α be functions with domain $\mathbb{N}$. Given a modular X $\leftarrow \cup(Z_q^{n\times m})$, $\alpha \in Z^+$ and a random vector $w \in Z_q^n$. It is difficult to obtain a vector $v \in Z^n \backslash \{0\}$ such that Xv = w mod q with $\|v\| \leq \alpha$.

According to [21, 34], quantum assaults cannot breach SIS and ISIS difficulties. In addition, the improvements of [35, 36] in [21] indicated that the SIS/ISIS problem is on par with other challenging problems like SVP, SIVP (shortest independent vector problem), and so on. Furthermore, an enhanced version of the SIS/ISIS problem was also put up by Wang et al. [27]. The new hardness problem is named as biliteral SIS/ISIS problem (Bi-SIS/Bi-ISIS). Different from the SIS/ISIS problem, the Bi-SIS/Bi-ISIS problem uses a n-by-n matrix X $\in Z_q^{n\times n}$ with rank m rather than a m-by-n matrix X $\in Z_q^{m\times n}$. The Bi-SIS/Bi-ISIS mathematical conundrum is defined as follows.

Theorem 8. Biliteral Small Integer Solution (Bi-SIS) Problem

Considering a n-by-n modular matrix X $\in Z_q^{n\times n}$ with rank equals m, an integer q and $\alpha \in Z^+$. It is difficult to locate two nonzero integer vectors v, $w \in Z^+\backslash\{0\}$ such that

$w^{\mathrm{T}}\mathrm{X} = 0^{\mathrm{T}} \bmod q$, where $\alpha \geq \|w\|$

and

$\mathrm{X}v = 0 \bmod q$, where $\alpha \geq \|v\|$

Theorem 9. Biliteral Inhomogeneous Small Integer Solution (Bi-ISIS) Problem

Considering a modular matrix X $\in Z_q^{n\times n}$ with rank equals m, an integer q and two vectors $s, t \in Z^n$and $\alpha \in Z^+$. It is hard to find two nonzero integer vectors v, $w \in Z^+\backslash\{0\}$ such that

$w^{\mathrm{T}}\mathrm{X} = s^T \bmod q$ and $\|w\| \leq \alpha$

and

$\mathrm{X}v = t \bmod q \ \ \|v\| \leq \alpha$

Lemma 2. In polynomial time, the Bi-SIS/Bi-ISIS problem can be simplified to the SIS/ISIS problem.

Theorem 10. Computational Bi-ISIS (CBi-ISIS) Problem

Let $D = \{\mathrm{z} \in Z^n\backslash\{0\} : \|z\| \leq \beta$ and $\beta \in Z^+\}$, given the tuple$\langle \mathrm{X}, \mathrm{X}v, w^{\mathrm{T}}\mathrm{X}\rangle$, where vectors $v, w \in D$. It is hard to compute $w^{\mathrm{T}}\mathrm{X}v \bmod q$.

Theorem 11. Computational Bi-ISIS (CBi-ISIS) assumption

Given $m \in Z^+$ which represents a security parameter, an integer $n = poly(m)$, a prime $q = poly(m)$, and $\beta = poly(m)$ be a real, such that $\beta \cdot \sqrt{\omega(m \log m)} \leq q$. Let $D = \{\mathrm{z} \in Z^n\backslash\{0\} : \|z\| \leq \beta$ and $\beta \in Z^+\}$, given a random modular matrix $\mathrm{X} \in Z_q^{n\times n}$ of rank m and vectors v, $w \in D$. Then given a probabilistic polynomial time (PPT) algorithm $\mathcal{A}$, the following inequality holds true.

$\Pr[\mathcal{A}(\mathrm{X}, \beta, \mathrm{X}v, w^{\mathrm{T}}\mathrm{X}) = w^{\mathrm{T}}\mathrm{X}v] \leq \epsilon$

Proposition 1 [10, Proposition 4.7]. Given a security parameter $m \in Z^+$, $n = poly(m)$, $\beta = poly(m)$, as well as a prime q satisfied $\beta \cdot \sqrt{\omega(m \log m)} \leq q$. The average case of the SIS and ISIS problems is as difficult as approximating the problems $SIVP_\gamma$ and $GapSVP_\gamma$ in the worst case to within certain $\gamma = \beta \cdot \tilde{O}(\sqrt{n})$.

3.2 Forward Secrecy

In AKE, forward secrecy is explicitly intended as a desired property. The concept of forward secrecy first introduced in [37] and was formalized later in [38-41] for the AKE protocol. In a nutshell, it guarantees the session key's security even in the event that the participants' long-term secret is subsequently revealed [37]. In 1992, Whitfield Diffie [42] gave the following concept.

Theorem 12. If the corruption of long-term keys does not compromise previous session keys, then a protocol is considered to have perfect forward secrecy [42].

Namely, even if the parties are later corrupted, the attacker cannot obtain the session key once it has been removed from the owner's memory. In 2001, the concept of weak perfect forward secrecy (weak-PFS) [40] was first defined by Krawczyk. The concept is defined as follows:

Theorem 13. If an attacker $\mathcal{M}$, who has learnt the private keys of both peers to the session, is unable to identify the key of any session for which the session and its matching session are clean, then the key-exchange protocol supports weak PFS (wPFS) [2].

That is, Weak perfect forward secrecy can guarantee the confidentiality of previously established session keys when long-term keys are compromised, but only for sessions where the adversary does not aggressively intervene, such as recording all transmissions or modifying messages exchanged between parties. The main difference between PFS and wPFS is the adversary's initiative.

4. Analysis of the protocol of Gupta et al.

Gupta et al.'s protocol has three phases. For details, please refer to [32]. During the session key generation phase, Gupta et al. use timestamps as part of the key material, they don't clearly state the purpose. However, it is generally used to resist replay attacks. They also try to use long-term private keys to protect the short-term secrets of session keys. Nonetheless, Gupta et al.'s solution still has flaws and vulnerabilities. we proceed directly to the analysis in this section.

4.1 Disadvantages of timestamps

4.1.1 Servers.

NTP networks, akin to websites or servers, are susceptible to unexpected outages, which can result in devices losing synchronization. To mitigate the impact of such disruption, it is imperative for systems to have access to redundant servers, ensuring continuity in accurate time synchronization.

4.1.2 Precision of Time Servers.

Although most NTP networks are designed to provide accurate and reliable time data, not all servers guarantee precise synchronization. Various factors, including human errors or technical constraints, can introduce inaccuracies. For example, an NTP server might be configured to a different time zone or may not correctly adjust for daylight saving time. To maintain high accuracy, it is crucial to ensure that the selected NTP server operates within the appropriate time zone and adheres to local DST protocols.

4.2 Violation of perfect forward secrecy

Let's consider the following scenario, assuming there exists an active adversary who collected the exchanged information between node i and node j. That is, the adversary has the following information $\{A_i, B_i, T_i, S_i, P_i\}$ and $\{B_j, T_j, S_j, P_j\}$. The adversary compromises node i and obtains the long-term private key sk_i after the expiration of the session key and its removal from memory. The adversary can compute

$$\delta_i = H_2(B_i \| P_i \| T_i)$$
$$S_i = (sk_i + \delta_i \cdot x_i)$$

Since the adversary knows δ_i, S_i, and sk_i, he can further calculate the following equation:

$$x_i = \frac{S_i - sk_i}{\delta_i}$$

Then the adversary can use x_i to get $k_i = B_2 \cdot x_i$. Finally, the adversary can compromise the past session key K by computing $H_3(k_i||ID_i||ID_j||T_i||T_j||P_i||P_j)$. A compromise of a long-term private key not only discloses past session keys, but also future session keys. Therefore, an adversary may collect ciphertext in advance and wait for the long-term key to be compromised before decrypting the ciphertext. Therefore, Gupta et al.'s protocol cannot resist active attackers to achieve perfect forward secrecy. It can only provide weak perfect forward secrecy (wPFS).

4.3 Impersonation attack

In Gupta et al's protocol, the amount of key agreement information sent by the initiator and the responder is not the same. The initiator sends $\{A_i, B_i, T_i, S_i, P_i\}$ and the responder replies $\{B_j, T_j, S_j, P_j\}$. If the adversary eavesdrops on the initiator and replays it as $\{A_e, B_i, T_e, S_i, P_i\}$, where $A_e = X \cdot x_e$ and T_e is a new timestamp. Then the responding node computes

$$S_i^T \cdot X \stackrel{?}{=} P_i + h_{\mathrm{i}} \cdot P + \delta_i \cdot B_{\mathrm{i}}$$

Since the tuple $\{B_i, S_i, P_i\}$ is unchanged, the equation holds as in the previous session. The corresponding node regards the adversary as the initiator (node i) and uses A_e to calculate $k_j = x_j^T \cdot A_e = x_j^T \cdot X \cdot x_e$ and the session key $K_j = H_3(k_j||ID_i||ID_j||T_e||T_j||P_i||P_j)$. Next, the corresponding node replies the new tuple $\{B_j, T_j, S_j, P_j\}$ to the adversary. The adversary computes $k_e = B_j \cdot x_e = x_j^T \cdot X \cdot x_e$. Therefore, the adversary can impersonate as the initiator (node i) and calculates the same session key $K_e = H_3(k_e||ID_i||ID_j||T_e||T_j||P_i||P_j)$ with the node j.

4.4 Unidentified interaction

As we can see, the initiator sends $\{A_i, B_i, T_i, S_i, P_i\}$ and the responder replies $\{B_j, T_j, S_j, P_j\}$ in Gupta et al.'s protocol. It is not clear how the receiver can identify the other party from the exchanged messages, since each element in the tuple looks like a random number.

5. The proposed protocol

In the conclusion, you can reiterate the main points of the paper, but do not duplicate the abstract as a conclusion. You can elaborate on the importance of the task or suggest applications and extensions.

5.1 Security requirement and symbols

5.1.1 Security requirement

Mutual Authentication (MA) and Authentication Key Agreement (AKA) are the two main security criteria of the ***I***mproved ***L***attice-***B***ased and ***ID***entity-based ***M***utual ***A***uthenticated ***K***ey ***A***greement (ILB-ID-MAKA) protocol.

- MA Security: The ILB-ID-MAKA protocol makes sure that only the edge nodes and their partners who set up the session key know what it is. When establishing session keys, edge nodes are able to authenticate with one another.
- AKA Security: It ensures that only edge nodes participating in the ILB-ID-MAKA protocol are capable of computing the common session key. It is also guaranteed that the established session key is semantically secure.

5.1.2 ILB-ID-MAKA protocol

In this section, the Improved LB-ID-MAKA (ILB-ID-MAKA) protocol is proposed. The protocol allows two edge nodes N_1 and N_2 to negotiate a common session-key in an IoV environment. Two edge nodes are involved in the improved LB-ID-MAKA protocol. The protocol is started by the sender node (N_1), and requests are answered by the receiver node (N_2), and a trustworthy third-party PKG is employed to retrieve the private key $\boldsymbol{sk_i}$ of each edge node N_i. In order to distribute the private key $\boldsymbol{sk_i}$, PKG first uses each node's identity IDi to authenticate the node N_i in an off-line mode, and then uses the identity ID_i to calculate the private key $\boldsymbol{sk_i}$ of N_i. The proposed improved protocol is comprised of three stages: *Setup*, *Private key extraction* and *Session key generation*. The details of three phases are depicted as follows and the symbols used are defined **Table 1**.

Table 1. Symbols

Symbols	Meaning
m	Parameters of security
n	Indicates an integer
q	Indicates a prime number
d	Indicates PKG's master secret key
P	Indicates PKG's master public key
X	A matrix from $Z_q^{n\times n}$
$H_i(\cdot)$	Cryptographic hash function, where i = 1, 2
N_i	The i-th node
sk_i	A private key of N_i

(A) The phase of *Setup*

In this phase, the PKG generate global system parameters. The security parameter m is inputted into this phase. Then a list of parameters including global parameters is produced as outputs. The PKG carries out the following actions:

- Selects a modular $X \in Z_q^{n\times n}$ and an integer $n \geq 2m \log q$ where q is a prime with a condition $q \geq \alpha \cdot \sqrt{\omega(m \log m)}$.
- Chooses a vector $d \in Z_q^n$ at random and computes $P = d^T \cdot X$ as the master public key.
- Picks three cryptographic hash functions $H_i : \{0, 1\}^* \rightarrow Z_q^*$, where $i = \{1, 2, 3\}$.
- Global parameters $\tau = \{q, n, P, X, H_i(\cdot)\}$ is then outputted publicly and keeps the master secret d.

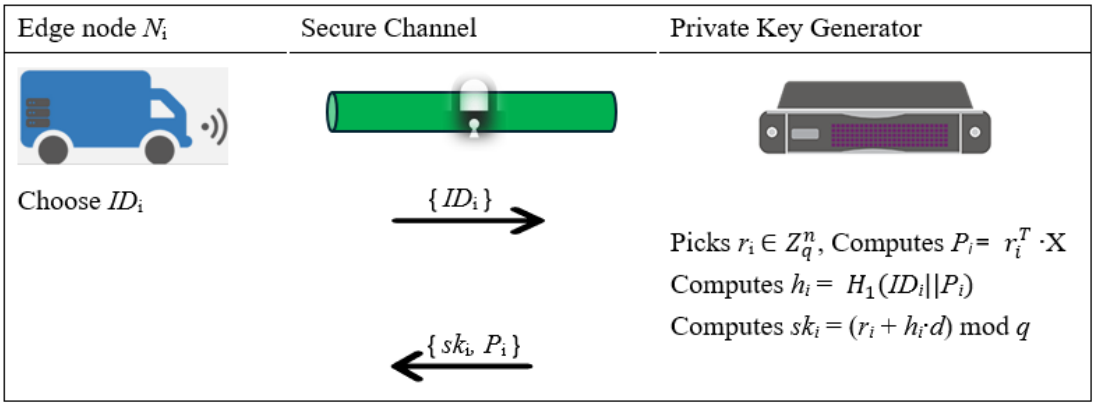

Fig. 2. The phase of extracting private key

(B) The phase of *Private key extraction*

In this phase, the PKG issues the private key sk_i to each edge node N_i, $i = \{1, 2\}$. The process in this phase is as follows.

- The identity ID_i of the edge node N_i is sent to the PKG in a mode that is offline.
- After receiving ID_i, the authenticity of N_i and its ID_i is verified by the PKG.
- After successful verification, the PKG carries out the subsequent actions:
  - Selects a vector $r_i \in Z_q^n$ at random and computes $P_i = r_i^T \cdot X$.
  - Calculates $h_i = H_1(ID_i||P_i)$ and computes the edge node N_i's private key as

$$sk_i = (r_i + h_i \cdot d) \bmod q$$

  - Sends (sk_i, P_i) to edge node N_i through a secure channel.

Fig. 2 shows the steps of private key extraction of the proposed ILB-ID-MAKA protocol.

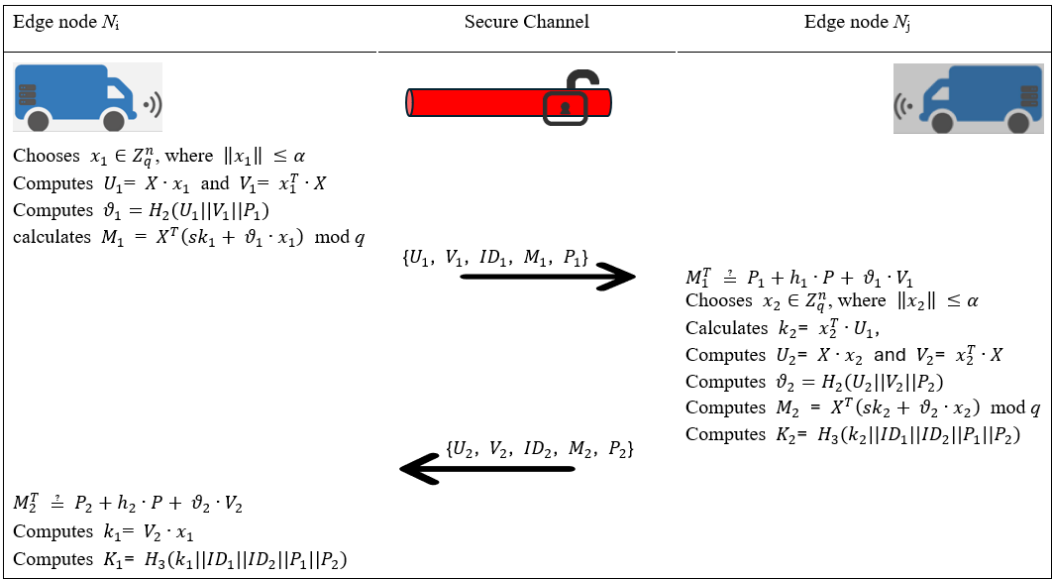

Fig. 3. Session key generation phase

(C) The phase of *Session key generation*

Edge nodes N_1 and N_2 negotiates a shared session key during the session key generation phase. The following are the procedures for this phase.

- N_1 selects a random vector $x_1 \in Z_q^n$ such that $\|x_1\| \leq \alpha$ for $\alpha \in Z^+$, then and calculates $U_1 = X \cdot x_1$ and $V_1 = x_1^T \cdot X$.
- N_1 computes $\vartheta_1 = H_2(U_1||V_1||P_1)$ and calculates $M_1 = X^T(sk_1 + \vartheta_1 \cdot x_1)$ mod q.
- Next, node N_1 transmits the tuple $\{U_1, V_1, ID_1, M_1, P_1\}$ to node N_2 through a public channel.
- On receiving $\{U_1, V_1, ID_1, M_1, P_1\}$ from N_1, N_2 checks whether

  $M_1^T \stackrel{?}{=} P_1 + h_1 \cdot P + \vartheta_1 \cdot V_1$

- After successful verification, N_2 randomly selects $x_2 \in Z_q^n$ such that $\|x_2\| \leq \alpha$ for $\alpha \in Z^+$, and calculates $k_2 = x_2^T \cdot U_1$, $U_2 = X \cdot x_2$ and $V_2 = x_2^T \cdot X$.
- N_2 then computes $\vartheta_2 = H_2(U_2||V_2||P_2)$ and $M_2 = X^T(sk_2 + \vartheta_2 \cdot x_2)$ mod q.
- Finally, N_2 computes the session key as

  $K_2 = H_3(k_2||ID_1||ID_2||P_1||P_2)$

  and sends the tuple $\{U_2, V_2, ID_2, M_2, P_2\}$ to N_1 through a public channel.

- After N_1 receives the tuple sent by N_2, N_1 checks whether

  $M_2^T \stackrel{?}{=} P_2 + h_2 \cdot P + \vartheta_2 \cdot V_2$

- After successful verification, N_1 calculates $k_1 = V_2 \cdot x_1$ and calculates the session key in this way

  $K_1 = H_3(k_1||ID_1||ID_2||P_1||P_2)$

Be aware that during the session key is generated, k_1 and k_2 have the same values as

$$k_1 = k_2 = x_2^T \cdot X \cdot x_1$$

6. Security Analysis and Performance Comparison

6.1 Security analysis

In this section, we provide a comprehensive exposition of both the correctness and security proofs pertaining to the proposed ILB-ID-MAKA protocol.

Proposition 2. The ILB-ID-MAKA protocol's correctness is proven, wherein a designated verifier node can validate the legitimacy of the incoming messages through the designated equation.

$$M_i^T \stackrel{?}{=} P_i + h_i \cdot P + \vartheta_i \cdot V_i \quad \text{for i = 1, 2}$$

Proof.

$$\begin{aligned} M_i^T &= (X^T(sk_i + \vartheta_i \cdot x_i))^T \\ &= (sk_i + \vartheta_i \cdot x_i)^T X \\ &= (r_i + h_i \cdot d + \vartheta_i \cdot x_i)^T X \\ &= \left(r_i^T + h_i \cdot d^T + \vartheta_i \cdot x_i^T\right) X \\ &= \left(r_i^T \cdot X + h_i \cdot d^T \cdot X + \vartheta_i \cdot x_i^T \cdot X\right) \end{aligned}$$

$$= P_i + h_i \cdot P + \vartheta_i \cdot V_i$$

If the node *i*'s long-term private key sk_1 is compromised. The adversary computes the following equation

$$S_1 = X^T(sk_1 + \delta_1 \cdot x_1) = X^T \cdot sk_1 + \delta_1 \cdot X^T \cdot x_1$$
$$S_1 - X^T \cdot sk_1 = \delta_1 \cdot X^T \cdot x_1$$
$$\frac{S_1 - X^T \cdot sk_1}{\delta_1} = X^T \cdot x_1$$

, which equals to formula $X\vec{a} = \vec{b}$. It is difficult to find $\vec{a}$ $(= x_1)$.

Proposition 3. After successful execution of the ILB-ID-MAKA protocol, the public session key K is exchanged between nodes N_1 and N_2.

Proof. During the key agreement process, N_1 computes $k_1 = V_2 \cdot x_1 = x_2^T \cdot X \cdot x_1$, and N_2 computes $k_2 = x_2^T \cdot U_1 = x_2^T \cdot X \cdot x_1$. Hence, k_1 and k_2 are equal. Therefore, nodes N_1 and $N2$ both negotiate a common session key.

Proposition 4. The proposed protocol can achieve mutual authentication and key agreement.

Proof. The analysis of the strength of the security of the ILB-ID-MAKA protocol using the random oracle model (ROM) is similar to [32]. Interested readers can refer to [32] to verify the security of AKA. This work formalizes and demonstrates its ability to achieve the security of MA by further utilizing BAN logic.

BAN logic is a useful tool for characterizing and verifying authentication protocols. José M. Sierra et al. [43] also proved the validity of BAN foundations.

We first establish certain key logical postulates of BAN logic (**Table 3**) and, for convenience, provide some notations (**Table 2**) utilized in the BAN logic analysis.

To demonstrate that the proposed protocol offers secure mutual authentication and authentication between two nodes, we have to accomplish the following objective:

- **Goal 1**: $N_i \mid\equiv N_i \overset{K}{\leftrightarrow} N_j$, where $i \neq j$.
- **Goal 2**: $N_j \mid\equiv N_j \overset{K}{\leftrightarrow} N_i$, where $j \neq i$.

Generic form: The following are the generic formats of the messages that are transmitted in the proposed protocol between nodes N_i and N_j:

M1. $N_i \rightarrow N_j$: $\langle U_i, V_i \rangle_{(P.P_i)}$
M2. $N_j \rightarrow N_i$: $\langle U_j, V_j \rangle_{(P.P_j)}$

Idealized form: In ILB-ID-MAKA to idealized forms, the transmitted messages between the nodes N_i and N_j are arranged as follows:

M1. $N_i \rightarrow N_j$: $\langle \overset{U_i}{\rightarrow} N_i, V_i \rangle_{P_i^{-1}}$

M2. $N_j \rightarrow N_i$: $\langle U_j, \overset{V_j}{\rightarrow} N_j \rangle_{P_j^{-1}}$

Table 2. The BAN logic notations

Symbol	Definition
$P \mid\equiv X$	Indicates that P believes the statement X. P may behave as though X is true.
$P \lhd X$	Indicates that P sees the statement X.
$\#(X)$	Indicates that the formula X is fresh.
$P \mid\Rightarrow X$	Indicates that P control X; P has jurisdiction over X.
$P \mid\sim X$	Indicates that P said X. At one time, P sent (and believed) a message X.
(X, Y)	The equation X or Y is one part of the formula (X, Y).
$\langle X\rangle_Y$	The equation X is combined with the formula Y.
$\{X\}_K$	The equation X is encrypted by the key K.
$P \overset{K}{\leftrightarrow} Q$	Denotes that K is the shared key for communication between P and Q, and no principal except P or Q will ever find out about it.
$\overset{K}{\rightarrow} P$	K is the public key of P
$\frac{P}{Q}$	Means if P is true then Q is true.

Table 3. The BAN logic postulates

Symbol	Definition
$\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P\{X\}_K}{P \mid\equiv Q \mid\sim X}$	The message-meaning rule (R_1)
$\frac{P \mid\equiv \overset{K}{\rightarrow} Q, P \lhd \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$	The message-meaning rule (R_2)
$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$	The nonce verification rules (R_3)
$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$	The jurisdiction rules (R_4)
$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$	The freshness-conjuncatenation rule (R_5)
$\frac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv (X)}$	The belief rules (R_6)
$\frac{P \mid\equiv \overset{K_P^{-1}}{\longrightarrow} (P), P \mid\equiv \overset{K_Q}{\longrightarrow} (Q), P \mid\equiv \overset{K_Q^{-1}}{\longrightarrow} (Q),}{P \mid\equiv P \overset{SK}{\leftrightarrow} Q}$	The qualified key-agreement rule (R_7)

Assumptions: The following are the initial assumptions of ILB-ID-MAKA:

A1. $N_i \mid\equiv \#(U_j)$, where $i \neq j$

A2. $N_i \mid\equiv \#(V_j)$, where $i \neq j$

A3. $N_i \mid\equiv N_j \mid\Rightarrow \#(U_j)$, where $i \neq j$

A4. $N_i \mid\equiv N_j \mid\Rightarrow \#(V_j)$, where $i \neq j$

A5. Ni $\mid\equiv$Pj, where i $\neq$ j

A6. $N_i \mid\equiv N_j \mid\Rightarrow N_j \mid\sim X$, where $i \neq j$

A7. $N_i \mid\equiv N_j \mid\Rightarrow N_j \overset{k_j}{\leftrightarrow} N_i$, where $i \neq j$

A8. $N_i \mid\equiv \overset{P_j}{\rightarrow} N_j$, where $i \neq j$

BAN logic proof. Here, we use the BAN logic rules and the assumptions to verify the safe authentication and to validate the aforementioned testing goals.

- From M1, we have
  S1: $N_j \lhd \langle \overset{U_i}{\rightarrow} N_i, V_i \rangle_{P_i^{-1}}$
- From S1, A8 and R2, we get
  S2: $N_j \mid\equiv N_i \mid\sim \langle \overset{U_i}{\rightarrow} N_i, V_i \rangle$
- From S2, A1, A2, A3, A4, A5 and R6, we have
  S3: $N_j \mid\equiv \overset{U_i}{\rightarrow} N_i$
- From S3, A7, R6 and R7, we get
  S4: $N_j \mid \equiv N_j \overset{K}{\leftrightarrow} N_i$, , where $j \neq i$. (**Goal 2**)
- From M2, we have
  S5: $N_i \lhd \langle A_j, \overset{V_j}{\rightarrow} N_j \rangle_{P_j^{-1}}$
- From S5, A8 and R2, we get
  S6: $N_i \mid\equiv N_j \mid\sim \langle A_j, \overset{V_j}{\rightarrow} N_j \rangle$
- From S6, A1, A2, A3, A4, A5 and R6, we have
  S7: $N_i \mid\equiv \overset{V_j}{\rightarrow} N_j$
- From S7, A7, R6 and R7, we get
  S8: $N_i \mid \equiv N_i \overset{K}{\leftrightarrow} N_j$, , where $i \neq j$. (**Goal 1**)

As can be seen from Goals 1 and 2, It is obvious that both node *i* and node *j* can securely authenticate against each other using the suggested protocol.

6.2 Informal security analysis

This section discusses the various security characteristics of the proposed LB-ID-MAKA protocol.

- Man-in-the-middle (MITM) attack: In the proposed protocol, signatures are used by both nodes N_1 and N_2 for mutual authentication. N_1 and N_2 exchange their messages $\{U_1, V_1, ID_1, M_1, P_1\}$ and $\{U_2, V_2, ID_2, M_2, P_2\}$ with each other for verification. Both nodes N_1 and N_2 can verify the transmitted messages by using the equation $M_i^T \stackrel{?}{=} P_i + h_i \cdot P + \vartheta_i \cdot V_i$ for both parties. This verification shows that the correct session key *K* was generated between N_1 and N_2. Let an adversary $\mathscr{A}$ attempts to assault the suggested protocol using a Man-in-the-Middle (MITM) attack. However, $\mathscr{A}$ must solve the CBi-ISIS hard problem to do this. Therefore, the proposed ILB-ID-MAKA protocol resists MITM attacks.
- Full perfect forward secrecy (FPFS): In the case that an adversary $\mathscr{A}$ obtains N_1 and N_2's private keys and then wishes to retrieve the previous session keys in the proposed LB-ID-MAKA protocol. $\mathscr{A}$ is unable to access the prior secret key as only the edge nodes to whom the ephemeral secret values x_1 and x_2 belong are aware of them. Furthermore, $\mathscr{A}$ cannot compute x_1 and x_2 from V_1 and V_2 due to the hard assumptions on the lattice of Bi-SIS and CBi-ISIS. Even if edge node *i* is corrupted, the adversary cannot get the past ephemeral secret x_i because of the hardness of the SIS problem.

Hence, the proposed protocol offers not only weak perfect forward secrecy but also full perfect forward secrecy.

- Key-control resilience: In the proposed improved LB-ID-MAKA protocol, both edge nodes N_1 and N_2 selected ephemeral values x_1 and x_2 randomly to compute $k = x_2^T \cdot X \cdot x_1$, and calculate the common session key $K = H_3(k||ID_1||ID_2||P_1||P_2)$. Therefore, N_1 and N_2 cannot force each other to choose K as a small value or a pre-selected entity. Since the corresponding user has access to the pre-selected K and the small K may be easily guessable, in all scenarios, there is a chance that the adversary or the user may misuse the session key K. Thus, the proposed ILB-ID-MAKA protocol satisfies the NKC property.
- Unknown key-share (UKS) attack: In the proposed protocol, both nodes N_1 and N_2 use their identities ID_1 and ID_2, with the key related message U_1 and V_2 to calculate the session key K. The signatures M_1 and M_2 are used to verify key related messages. Furthermore, the secret values sk_1 and sk_2 of N_1 and N_2 are kept confidential from $\mathcal{A}$. Therefore, $\mathcal{A}$ has no way of knowing the generated session key. Hence, the proposed protocol can defend against UKS attacks.
- Known key security (KKS) attack: In the proposed protocol, the session key $K = H_3(k||ID_1||ID_2||P_1||P_2)$ are computed by two edge nodes N_1 and N_2. The key material $k = x_2^T \cdot X \cdot x_1$ is the same on both nodes. Obviously, $\mathcal{A}$ cannot compute keys for other sessions by using the value of the current session key K, since different ephemeral values are used in each specific session. Therefore, the proposed ILB-ID-MAKA can withstand KKS attacks.
- Impersonation attack: Suppose an adversary eavesdrops the transmitted messages $\{U_i, V_i, ID_i, M_i, P_i\}$ and wants to impersonate the node i to other nodes. $\mathcal{A}$ has no knowledge of sk_i, he/she cannot combine U_e with sk_i to generate a new M_i'. Therefore, $\mathcal{A}$ cannot pass the signature authentication to impersonate the node i. The proposed protocol is resistant to impersonation attacks.

The security comparison with the protocol of Gupta et al. is shown in **Table 4**. And comparing with the performance in the next section, it is obvious that the proposed protocol is more secure under the same computing, storage and communication costs.

Table 4. Comparison of several protocols for security properties

Protocol	Man-in-the-middle	No key control	Unknown key-share	Known-key security	Perfect Forward Secrecy	Impersonation attack
Gupta et al. [29]	✓	✓	✓	✓	×*	×
The proposed	✓	✓	✓	✓	✓	✓

6.3 Performance comparison

In this section, the performance analysis of the proposed ILB-ID-MAKA protocol is discussed by measuring the computation as well as storage and communication costs. A comparison study of the proposed ILB-ID-MAKA protocol with various existing competing technologies is also shown. To keep the analysis concise and explicit, we choose the value n

$= m\log q$ for $q = m^2$ to analyze the performance of the proposed protocol. Under these conditions, it is adequate to guarantee the security of the Bi-SIS and CBi-ISIS assumptions.

- **Computation cost**: The analysis only considers time-consuming operations. The first time-consuming operation is $P = d^{\mathrm{T}} \cdot \mathrm{X}$, which is $O(n^2 \cdot |q^2|) = O(m^2 \log^4 m)$ where $|q^2|$ is the cost of the multiplication of two integers in Z_q^*. The second time-consuming operation is $P_i = r_i^T \cdot \mathrm{X}$ which has a complexity of $O(n^2 \cdot |q^2|) = O(m^2 \log^4 m)$. Next, private key $sk_i = (r_i + h_i \cdot d)$ costs a complexity of $O(n^2 \cdot |q^2|) = O(m^2 \log^4 m)$. Then the participant's session key generation and the verification process include the overhead of computing $U_{\mathrm{i}} = \mathrm{X} \cdot x_{\mathrm{i}}$, $V_{\mathrm{i}} = x_i^T \cdot \mathrm{X}$, $k_{\mathrm{i}} = V_{\mathrm{j}} \cdot x_{\mathrm{i}}$ and $M_i^T = (X^T(sk_i + \vartheta_i \cdot x_i))^T$ respectively. Thus, the computation cost for the generation of the secret session key is calculated as $O(n^2 \cdot |q^2|) = O(m^2 \log^4 m)$. Therefore, the computation's order for generating the session key is $O(n^2 \cdot |q^2|) = O(m^2 \log^4 m)$ which incurs a cost of $4n^2 \cdot |q^2| + 2n \cdot |q|$. The overall computational overhead of the proposed ILB-ID-MAKA protocol is estimated as $6n^2 \cdot |q^2| + 3n \cdot |q| = 96m^2 \log^4 m + 12m \log^2 m$ for $n = m \log q$ and $q = m^2$.
- **Communication cost**: The overhead for transmitting a message tuple $\{U_i, V_i, ID_i, M_i, P_i\}$ requires $(4n+1) \cdot |q| = (4m \log q + 1) \cdot \log q = 16m \log^2 m + 2 \log m$.
- **Storage cost**: Secret value d takes into account $n \cdot |q|$ in storage overheads, while X needs $n^2 \cdot |q|$. Therefore, the overall storage cost consumed by the proposed ILB-ID-MAKA protocol is considered to be $(n^2 + n) \cdot |q| = 8m^2 \log^3 m + 4m \log^2 m$.

The performance of our protocol is compared with similar protocols. It is obvious that our solution is more efficient or more secure than other protocols and can be implemented on the Internet of Vehicles (IoV) scenario. The state-of-the-art technologies for quantum security [29-32] are considered to exhibit the performance of the suggested technology. Protocols [31, 32] is a key agreement protocol based on IBC, while [29, 30] are based on PKI. As is well known, PKI-based protocols have additional certificate management burdens compared to IBC-based protocols. The protocol's various costs, including computation, storage, and communication costs [29-32], were evaluated, with the results presented in **Tables 5** and **6**. This comparative analysis validates the benefits of the proposed protocol.

Table 5. Evaluation of similar lattice-based protocols in terms of computation costs (taking into account lattice's operations).

Protocol	Order of execution	Total cost
Islam et al. [31]	$O(n^2 \cdot \|q^2\|)$	$8n^2 \cdot \|q^2\| + 5n \cdot \|q\| = 128m^2 \log^4 m + 20m \log^2 m$
Gupta et al. [29]	$O(n^3 \cdot \|q^2\|)$	$n^3 \cdot \|q^2\| + 5n^2 \cdot \|q^2\| + 2n \cdot \|q\| = 32m^3 \log^5 m + 80m^2 \log^4 m + 8m \log^2 m$
Rana et al. [30]	$O(n^3 \cdot \|q^2\|)$	$3n^3 \cdot \|q^2\| + 4n^2 \cdot \|q^2\| + 3n \cdot \|q\| = 96m^3 \log^5 m + 64m^2 \log^4 m + 12m \log^2 m$
Gupta et al. [32]	$O(n^2 \cdot \|q^2\|)$	$6n^2 \cdot \|q^2\| + 3n \cdot \|q\| = 96m^2 \log^4 m + 12m \log^2 m$
The proposed	$O(n^2 \cdot \|q^2\|)$	$6n^2 \cdot \|q^2\| + 3n \cdot \|q\| = 96m^2 \log^4 m + 12m \log^2 m$

Table 6. Comparison of several protocols for storage and communication.

Protocol		Storage	Communication
Islam et al. [31]	Primitive	$x \in Z_q^n$, $A \in Z_q^{n\times n}$	$\{ID_i, R_i, X_i, Y_i, s_i\}$
	Length (in bits)	$\approx 8m^2\log^3 m + 4m\log^2 m$	$\approx 16m\log^2 m + 2\log m$
Gupta et al. [29]	Primitive	$d \in Z_q^n$, $X \in Z_q^{n\times n}$	$\{A_i, B_i, T, S_i, P_i\}$
	Length (in bits)	$\approx 8m^2\log^3 m + 4m\log^2 m$	$\approx 16m\log^2 m + 2\log m$
Rana et al. [30]	Primitive	$x, e \in Z_q^{n\times n}$	$\{ID_i, X_u, G_w, G_3, C_u\}$
	Length (in bits)	$\approx 16m^2\log^3 m$	$\approx 16m^2\log^3 m + 6\log m$
Gupta et al. [32]	Primitive	$A \in Z_q^{n\times n}$	$\{H(u), S_{1_i}, S_{2_i}\}$
	Length (in bits)	$\approx 8m^2\log^3 m$	$\approx 12m\log^2 m$
The proposed	Primitive	$d \in Z_q^n$, $X \in Z_q^{n\times n}$	$\{U_i, V_i, ID_i, M_i, P_i\}$
	Length (in bits)	$\approx 8m^2\log^3 m + 4m\log^2 m$	$\approx 16m\log^2 m + 2\log m$

7. Conclusion and Future Work

This study introduces a mutual authenticated key negotiation protocol, leveraging identity-based an lattice cryptography, tailored for the Internet of Vehicles framework. The proposed ILB-ID-MAKA protocol further strengthens the security of the Gupta et al.'s protocol while retaining the original advantages, such as eliminating the overhead of the management of certificates that is needed by PKI-based protocols. In addition to verifying the security of this protocol using Gupta et al.'s Random Oracle Model, we employ BAN logic to further demonstrate its security. Our outcomes demonstrate that the proposed ILB-ID-MAKA protocol is resilient to security risks such as MITM, UKS, KKS, PFS, key-control, impersonation attacks and quantum attacks without increasing any computational cost and is more reliable and more efficient that is appropriate for IoVs' lightweight devices.

In [44], Devarajan et al. introduce a blockchain-enabled secure federated learning system model for vehicular networks (BSFLVN), which employs Local Differential Privacy (LDP) [45] to safeguard the privacy and security of both local and global model updates. This approach highlights a promising direction for future research, where the integration of Post-Quantum Cryptography (PQC) with LDP could yield advanced privacy-preserving systems that offer robust resistance to quantum attacks while maintaining strong privacy guarantees.

References

[1] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommun. Syst.*, vol.50, no.4, pp.217-241, 2012. Article (CrossRef Link)

[2] C. Wu, Y. Ji, F. Liu, S. Ohzahata, T. Kato, "Toward Practical and Intelligent Routing in Vehicular Ad Hoc Networks," *IEEE Trans. Veh. Technol.*, vol.64, no.12, pp.5503-5519, 2015. Article (CrossRef Link)

[3] J. Contreras-Castillo, S. Zeadally, J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet Things J.*, vol.5, no.5, pp.3701-3709, 2018. Article (CrossRef Link)

[4] R. Gasmi and M. Aliouat, "Vehicular Ad Hoc NETworks versus Internet of Vehicles - A Comparative View," in *Proc. of 2019 International Conference on Networking and Advanced Systems (ICNAS)*, Annaba, Algeria, pp.1-6, 2019. Article (CrossRef Link)

[5] S. S. Abisha, Future of the Internet of Vehicles: Principles and Challenges, TranspireOnline.blog, 2021. [Online]. Available: https://transpireonline.blog/2021/06/10/future-of-the-internet-of-vehicles-principles-and-challenges/ [Accessed: Nov. 5, 2023].
[6] W. Diffie, M. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol.22, no.6, pp.644-654, 1976. Article (CrossRef Link)
[7] G.P. Biswas, "Diffie–Hellman technique: Extended to multiple two-party keys and one multi-party key," *IET Inf. Secur.*, vol.2, no.1, pp.12-18, 2008. Article (CrossRef Link)
[8] E. Bresson, O. Chevassut, D. Pointcheval, "Provably secure authenticated group Diffie-Hellman key exchange," *ACM Trans. Inf. Syst. Secur.*, vol.10, no.3, 2007. Article (CrossRef Link)
[9] D. S. Gupta, S. K. H. Islam, M. S. Obaidat, "A Secure Identity-Based Three-Party Authenticated Key Agreement Protocol Using Bilinear Pairings," in *Proc. of International Conference on Innovative Data Communication Technologies and Application*, Springer, pp.1-11, 2019. Article (CrossRef Link)
[10] Y. Liu, Y. Wang, G. Chang, "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol.18, no.10, pp.2740-2749, 2017. Article (CrossRef Link)
[11] I. R. Jeong, J. O. Kwon, D. H. Lee, "Strong Diffie-Hellman-DSA Key Exchange," *IEEE Commun. Lett.*, vol.11, no.5, pp.432-433, 2007. Article (CrossRef Link)
[12] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *J. Supercomput.*, vol.76, pp.7081-7106, 2020. Article (CrossRef Link)
[13] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, A. Mohammadi-Nodooshan, "A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid," *IEEE Trans. Smart Grid*, vol.9, no.4, pp.2834-2842, 2018. Article (CrossRef Link)
[14] K. Mahmood, J. Arshad, S. A. Chaudhry, S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *Int. J. Commun. Syst.*, vol.32, no.16, 2019. Article (CrossRef Link)
[15] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. of CCS '93: Proceedings of the 1st ACM conference on Computer and communications security*, pp.62-73, 1993. Article (CrossRef Link)
[16] S. Bala, G. Sharma, A. K. Verma, "PF-ID-2PAKA: Pairing Free Identity-Based Two-Party Authenticated Key Agreement Protocol for Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol.87, no.3, pp.995-1012, 2016. Article (CrossRef Link)
[17] L. Dang et al., "Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks," *Int. J. Distrib. Sens. Netw.*, vol.14, no.4, 2018. Article (CrossRef Link)
[18] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," in *Proc. of International Conference on Advances in Cryptology – EUROCRYPT 2001*, LNCS, vol.2045, Springer, pp.453-474, Heidelberg, 2001. Article (CrossRef Link)
[19] Q. Li et al., "A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for Vehicular Ad Hoc Networks," *Secur. Commun. Netw.*, vol.2019, 2019. Article (CrossRef Link)
[20] Q. Jiang et al., "Three-factor authentication protocol using physical unclonable function for IoV," *Comput. Commun.*, vol.173, pp.45-55, 2021. Article (CrossRef Link)
[21] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. of Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pp.99-108, 1996. Article (CrossRef Link)
[22] M. Ajtai and C. Dwork, "The First and Fourth Public-Key Cryptosystems with Worst-Case/Average-Case Equivalence," *Electronic Colloquium on Computational Complexity*, vol.14, no.097, ECCC, Citeseer, 2007. Article (CrossRef Link)
[23] D. S. Gupta, G. P. Biswas, and R. Nandan, "Security weakness of a lattice-based key exchange protocol," in *Proc. of 2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, pp.1-5, 2018. Article (CrossRef Link)

[24] L. Ducas et al., "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," *IACR Trans. Cryptogr. Hardw. Embedded Syst.*, vol.2018, no.1, pp.238-268, 2018. Article (CrossRef Link)
[25] D. Micciancio, "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions," *Comput. Complexity*, vol.16, no.4, pp.365-411, 2007. Article (CrossRef Link)
[26] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. of International Symposium Algorithmic Number Theory*, LNCS, vol.1423, pp.267-288, Springer, 1998. Article (CrossRef Link)
[27] S. Wang et al., "Lattice-based key exchange on small integer solution problem," *Sci. China Inf. Sci.*, vol.57, no.11, pp.1-12, 2014. Article (CrossRef Link)
[28] D. S. Gupta and G. Biswas, "Cryptanalysis of Wang et al.'s lattice-based key exchange protocol," *Perspect. Sci.*, vol.8, pp.228-230, 2016. Article (CrossRef Link)
[29] D. S. Gupta and G. Biswas, "A novel and efficient lattice-based authenticated key exchange protocol in C-K model," *Int. J. Commun. Syst.*, vol.31, no.3, 2018. Article (CrossRef Link)
[30] S. Rana and D. Mishra, "Lattice-based key agreement protocol under ring-LWE problem for IoT-enabled smart devices," *Sādhanā*, vol.46, no.2, pp.1-11, 2021. Article (CrossRef Link)
[31] S. H. Islam, S. Zeadally, "Provably secure identity-based two-party authenticated key agreement protocol based on CBi-ISIS and Bi-ISIS problems on lattices," *J. Inf. Secur. Appl.*, vol.54, 2020. Article (CrossRef Link)
[32] D. S. Gupta, S. Ray, T. Singh, M. Kumari, "Post-quantum lightweight identity-based two-party authenticated key exchange protocol for Internet of Vehicles with probable security," *Computer Communications*, vol.181, pp.69-79, 2022. Article (CrossRef Link)
[33] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Computer Systems*, vol.8, no.1, pp.18-36, 1990. Article (CrossRef Link)
[34] D. S. Gupta, G. Biswas, "Design of lattice-based ElGamal encryption and signature schemes using SIS problem," *Trans. Emerg. Telecommun. Technol.*, vol.29, no.6, 2018. Article (CrossRef Link)
[35] C. Gentry, C. Peikert, V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of STOC '08: Proceedings of the fortieth annual ACM symposium on Theory of computing*, pp.197-206, Victoria, British Columbia, Canada, May 17-20, 2008. Article (CrossRef Link)
[36] D. Micciancio, O. Regev, "Worst-case to average-case reductions based on Gaussian measures," in *Proc. of 45th Annual IEEE Symposium on Foundations of Computer Science*, pp.372-381, 2004. Article (CrossRef Link)
[37] W. Diffie, P. C. Van Oorschot, M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol.2, no.2, pp.107-125, Jun. 1992. Article (CrossRef Link)
[38] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," in *Proc. of International Conference on Advances in Cryptology – EUROCRYPT 2001*, LNCS, vol.2045, pp.453-474, 2001. Article (CrossRef Link)
[39] V. Shoup, "On Formal Models for Secure Key Exchange," *Cryptology ePrint Archive*, Paper 1999/012, 1999. Article (CrossRef Link)
[40] H. Krawczyk, "HMQV: A High-Performance Secure Diffie-Hellman Protocol," in *Proc. of 25th Annual International Cryptology Conference on Advances in Cryptology – CRYPTO 2005*, LNSC, vol.3621, pp.546-566, Springer, Berlin, Heidelberg, 2005. Article (CrossRef Link)
[41] B. LaMacchia, K. Lauter, A. Mityagin, "Stronger Security of Authenticated Key Exchange," in *Proc. of Provable Security, First International Conference, ProvSec 2007*, LNCS, vol.4784, pp.1-16, Springer, 2007. Article (CrossRef Link)
[42] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol.2, pp.107-125, 1992. Article (CrossRef Link)
[43] J. M. Sierra, J. C. Hernández, A. Alcaide, and J. Torres, "Validating the Use of BAN LOGIC," in *Proc. of Computational Science and Its Applications - ICCSA 2004, International Conference*, LNCS, vol.3043, pp.851-858, Assisi, Italy, May 14-17, 2004. Article (CrossRef Link)
[44] G. G. Devarajan, M. Thirunnavukkarasan, S. I. Amanullah, T. Vignesh, & A. Sivaraman, "An integrated security approach for vehicular networks in smart cities," *Transactions on Emerging Telecommunications Technologies*, vol.34, no.11, 2023. Article(CrossRef Link)

[45] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, “Local privacy and minimax bounds: sharp rates for probability estimation,” in *Proc. of NIPS'13: Proceedings of the 26th International Conference on Neural Information Processing Systems*, vol.1, pp.1529-1537, Curran Associates Inc., Red Hook, NY, USA, 2013. Article(CrossRef Link)

Wen-Bin Hsieh earned his Ph.D. in 2013 from the National Taiwan University of Science and Technology. With over a decade of experience supporting government initiatives in information security and cryptography, he previously served as an assistant professor in the Department of Computer Science & Information Engineering and the Innovation Frontier Institute at National Taipei University of Technology. Currently, he is an assistant professor in the Department of Green Energy and Information Technology at National Taitung University. His research interests encompass machine learning, financial technology, cryptography, communication protocols, network security, and mobile communications.