INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 1, PP. 5-10
Manuscript received March 4, 2022; revised January, 2023. DOI: 10.24425/ijet.2022.143902

Improved Framework for Blockchain Application Using Lattice Based Key Agreement Protocol

Zahraa Ch. Oleiwi, Rasha Ail Dihin, and Ali H. Alwan

***Abstract*—One of the most recent challenges in communication system and network system is the privacy and security of information and communication session. Blockchain is one of technologies that use in sensing application in different important environments such as healthcare. In healthcare the patient privacy should be protected use high security system. Key agreement protocol based on lattice ensure the authentication and high protection against different types of attack especially impersonation and man in the middle attack where the lattice-based protocol is quantum-withstand protocol. Proposed improved framework using lattice based key agreement protocol for application of block chain, with security analysis of many literatures that proposed different protocols has been presented with comparative study. The resultant new framework based on lattice overcome the latency limitation of block chain in the old framework and lowered the computation cost that depend on Elliptic curve Diffie-Hellman. Also, it ensures high privacy and protection of patient's information.**

***Keywords*—key agreement protocol; lattice based protocol; mutual authentication; Diffie-Hellman protocol; forward secrecy**

I. Introduction

IN any communication system one of the essential issues is the security of data that transmitted among users in the system to ensure such security and authentication between principles [1]. Key establishment should be done as the first step of the session. Key agreement process is one of the key establishments approaches to generate session key used to protect data with the help of cryptography algorithm. In key agreement, all the communicated principles cooperate to derive the session key as a function of exchanged information (public key) by insecure channel of communication, where all parties shared particular independent information as input of key derived function [1].

Due to insecure channel of exchanged input of function, the key agreement protocol should be built depending on hardness of mathematical problem such as discrete logarithm and lattice problem [2].

Diffie-Hellman protocol that based on hardness of discrete logarithm problem. Furthermore, DH achieves most important security property called forward secrecy that ensure prevent adversary from using session key later [2].

Mingping and Jianhua [3] produced anonymous one-way Authentication Key Exchange protocol which was characterized by efficient, high security and strong anonymity. This new protocol depends on Oracle prove model with XCR and Gap-DH signature. Generalized new Diffie-Hellman key exchange protocol by Reddy[4]. The new proposed protocol provided DSA signature and authentication to DH key exchange which made it suitable for many applications such as cloud computing, resource sharing, internet banking and distributed computing application.

Yuwen and Gabriela [5] implemented Diffie-Hellman key agreement protocol on Resperry pi system. TCP/IP was the based communication protocol with resistance against man in middle attack. Furthermore Miller-Rabin algorithm was used to generate large prime number. As it clear from results of implementation of this project that the system could resist keys up to 19 digits with exponentially increasing of time exactly after keys of 15 digits.

Based on lattice hard problem proposed key exchange protocol that withstand quantum produced by Sonika and Sahadeo [6] under MaTRU cryptosystem. This proposed protocol overcome the weakness and failure of Lie et al protocol against MITM man in the middle attack by using TTP trust third party [6].

Another key exchange protocol based on Lattice hardness problem was proposed by Saurabh and Mishra [7] using RLWE ring learning with errors and provable securely with Oracle model. It is clear that this new protocol solves the problem of protocol-based theory number problem such as discrete logarithm, so this proposed protocol was robust against quantum computer-based attack.

In [8] Nsikak and Manmeet was proposed new framework based on Elliptic Curve Diffie-Hellman algorithm (ECDH) to produce key agreement protocol for block chain in order to exchange data from sensor of client to edge node. Their proposal framework achieved high security with small length of key.

Ring learning with error (LWE) based key exchange (KAE) protocol using key with small size was present by Zilong and Honggang [9]. This proposed protocol makes use of all features of lattice-based protocol such as simplicity, efficiency, hardness problem withstands against quantum attack, authentication, and forward secrecy.

Zahraa Ch. Oleiwi is with College of Computer Science and Information Technology, University Al-Qadisiyah, Iraq (e-mail: zahraachaffat@gmail.com).

Rasha Ail Dihin is with Faculty of Education for Girls, University of Kufa, Najaf, Iraq (e-mail: rashaa.aljabry@uokufa.edu.iq).

Ali H. Alwan is with Alkafeel University, Najaf, Iraq (e-mail: ali.hasan@alkafeel.edu.iq).

A. Motivation and Contribution

The sensitive and important medical information pf patient in the health system required high secure provable key agreement protocol to ensure protection to the privacy to the patient information and authentication service between service provider and patient. On the other hand, according to the limitation of monitoring devices the protocol should be lightweight with low complexity of time and computation cost. Therefore, we propose lattice-based authentication and key agreement protocol for medical application by improved the scheme in [8] and overcome the latency disadvantage generated according to the natural work of blockchain by using the proposed protocol in [9] which based on lattice.

The paper is organized as follows: The key agreement protocol application is produced in Section II. In Section III, security analysis of protocol explained. In Section IV, proposed protocol is presented. Section V presents security analysis of proposed protocol.

II. KEY AGREEMENT PROTOCOL APPLICATIONS

A. Medical And Healthy Application

In medical and health system there are most researches that concerned with applying authentication and key agreement protocol in order of keep out the security and authentication of communication in these systems.

Identity-based anonymous authentication and key agreement protocol (IBAAKA) for WBAN wireless body area network in cloud-assisted environment was proposed by Mahender Kumar [10] to provide mutual authentication and user anonymity. This protocol was processed the security in cloud computing which used to provide storage for WBAN in order to prevent the limitation of services produced to patients.

Another protocol was proposed by Ankur Gupta et al. [11], to established key agreement protocol for WBAN in health system with aim of protect health data that monitored remotely using communication system in WBAN. Ankur lightweight proposed protocol to overcome weakness of Li et al. mutual authentication protocol against attack. This protocol provided security requirements such as integrity, authentication and confidentiality of the information with less computations and by using simple operation for instance, XOR, hash function. So, this protocol characterized by its lightweight and efficiency properties.

In Remote surgery system the security considers as essential issue to protect data transmission from the attacker.

Due to important and sensitive information in this system secure and new mutual authentication and key agreement protocol was produced by Kuljee Kaur et.al [12]. In his research, Kuljee designed proposed protocol that provided secure communication between trusted authority, arm of robot and surgeon. Here the trusted authority helps to achieve mutual authentication between arm of robot and surgeon.

Depending on ECC Elliptic Curve Cryptography new key agreement protocol was designed by Steve O. Maikol et.al. [13] to provide protection and privacy of patient information which is vulnerable to different kind of attacks. Steve in its proposed design consist from two-layer authentication and signature where the ECC play the role of cryptography system that protect the key from impersonation adversary. ECC also used in algorithm of digital signature.

Mostafa f. moghadam et al. [14] designed another authentication and key agreement protocol depending on ECDH as a strong security tool to overcome and faced the weakness of other key agreement protocol against attacker, where the ECDH provide mutual authentication and create unique strong session and symmetric key for each session of communication among nodes in WSN that used in health field.

Quantum Diffie-Hellman had important effective role in design the Group key agreement to establish secure protocol to protect information shared through e-healthy system in smart cities as in [5]. Vankamamidi S. Naresh et al. [15] proposed architecture of three layers for smart healthcare city supported by multi-agent system. This proposed system achieved high security and robust against attacks based on quantum.

B. Internet of Thing and Block Chain Application

Depending on Elliptic curve Diffie-Hellman Nsikak and Manmeet [16] solved the problem of key agreement problem in sensing application based on Blockchain, with standard encryption algorithm. In this system the communication parities are miner node and blockchain clients that participated in generated shared secret key that used to derive the session key which used to protect data between communication parities.

For internet of vehicles application Zisang et al. [17] proposed RSU-assisted authentication and key agreement protocol depending on blockchain and multi-TA network. This protocol provided mutual authentication between communications parties in this system trust authority and vehicle node. As a result, this protocol solved less efficient authentication caused by TA computation problems.

For IOT environment application Daya S. Gupta et al. [18] designed secure identity based 2PAKA protocol that was characterized by high efficiency and low computation and communication cost as compared with another two parities authentication key agreement protocol that had weakness against different attacks and suffer from high cost of required storage, communication and computation. Important facility of that protocol was authentication mutual provided between users in IOT system in the aim of initiated session key used to protect information shared among authenticated parties.

Many researches for designing proposed key agreement protocol in IOT environment had been produced due to importance of IOT in different sensetive application especially Health application. So the high secure protocol are potential factor was needed to protect sensetive information between users. R. Vinoth [19] proposed secure multi-factor authenticated key agreement that achived security and authentication between user and remote sensing device.

III. SECURITY ANALYSIS AND COMPARATIVE STUDY

A. Internet of Thing and Block Chain Application

This section discusses which of bellow security attributes the proposed protocol which described in section (2) has [20]:

1 Withstand against different kind of attack.

2 Forward secrecy: communicated parities use session key to encrypt instead of shared key in order to prevent attack to decryption later even if know the shared key as well as it cannot use the session key of previous session because the users forget the session key after they used it.

3 Mutual authentication: each user (parties) proves them identity to each other.

4 User anonymity: it is one of the privacy concept concerns with user unknown identifier so the user be unreachable.

5 Session key security: Session key was established and protected using cryptography algorithm such as elliptic curve cryptography ECC.

B. Mathematical Example to achieve some of the security measures in protocol design

To design protocol with bellow security attributes

1- Shared secret

2- Authentication

3- Identity protection

4- Denial of service (DOS) protection

These above attributes are required for (IKE, IKEv2, and JFK)

1. To achieve first measure (shared secret) Diffie-Helllman key exchange is used 1- to generate key. Suppose we have A and B party:

$$A \rightarrow B: g^a$$
$$B \rightarrow A: g^b$$

(A) concludes

$Knows(Y, g^{ab}) \xrightarrow{yields} (Y = A)\ OR\ Knows(Y, b)$

2. To achieve second measure (Authentication) using challenge response

$$A \rightarrow B: g^a, A$$
$$B \rightarrow A: g^b, sig_B\{g^a, g^b, A\}$$
$$A \rightarrow B: sig_A\{g^a, g^b, B\}$$

Where A and B are identifier for two party

(A) concludes

Received (B, msg1) and Sent (B, msg2)

3. To achieve second measure (Identity Protection) using encrypted signature:

$$A \rightarrow B: g^a, A$$
$$B \rightarrow A: g^b, E_K\ \{sig_B\{g^a, g^b, A\}\}$$
$$A \rightarrow B: E_K\{sig_A\{g^a, g^b, B\}\}$$

4. To achieve second measure (DOS protection) by using cookie as in JFK protocol

$$A \rightarrow B: g^a, A$$
$$B \rightarrow A: g^b, hash_{KB}\ \{g^b, g^a\}$$

$$A \rightarrow B: g^a, g^b, hash_{KB}\ \{g^b, g^a\}$$
$$E_K\{sig_A\{g^a, g^b, B\}\}$$
$$B \rightarrow A: g^b, E_K\ \{sig_B\{g^a, g^b, A\}\}$$

5- Now when step (4) has been completed all four security attributes was achieved.

C. Security Analysis of Protocol of Medical Application

Most of the recent protocols of key agreement in the medical and health field are presented in section 2. Some of these protocols used for communication system WBAN, Cloud, WSN, and smart health city. Table I illustrates the analysis and compares between these protocols.

TABLE I
SECURITY ATTRIBUTES OF PROPOSED PROTOCOLS IN MEDICAL APPLICATION.

Protocol	withstand against attack	forward secrecy	mutual authentication	user anonymity	Session key security	communication cost (in bit)
[10]	Resist against MIM, stolen, impersonation attack	Yes	Yes	Yes	Yes	3440
[11]	Resist against Eavesdropping, replay, impersonation attack	yes	yes	yes	Yes	5280
[12]	Offline password guessing, replay, stolen, impersonation, MIM,DoS attack	yes	yes	yes	yes	No light weight
[13]	MIM and impersonation	no	no	no	yes	No light weight
[14]	Stolen, DOS, replay, stolen MIM, Offline password guessing attack	yes	no	no	yes	1504
[15]	Quantum based attack	Security based on unconditional security of the Quantum Diffie-Hellman				

D. *Protocol of Internet of Thing and Block Chain Application Security Analysis*

Most IOT protocol should be characterized light weight properties therefore it depends on XOR operation and simple cryptography system with hash function to ensure low computation and computation (time and storage) cost. Table II illustrates the analysis and compares between these protocols.

TABLE II
SECURITY ATTRIBUTES OF PROPOSED PROTOCOLS IN IOT AND BLOCKCHAIN APPLICATION.

Protocol	withstand against attack	forward secrecy	mutual authentication	user anonymity	session key security	communication cost (in bit)	Computation cost in (ms)
[16]	Replay attack	yes	yes	yes	yes	736	98.2
[17]	replay, VN capture, Jamming impersonation , wrong password login/update attack	yes	yes	yes	yes	1088	0.434
[18]	MIM, impersonation , Unknown-key share,	yes	yes	no	yes	2G1	17.868
[19]	replay, stolen, impersonation , MIM, DoS attack	yes	yes	yes	yes	3040	4.15485

*G1 is multiplicative group mod q, $q > 2^k$, k is security parameter.

IV. PROPOSED LATTICE BASED KEY AGREEMENT SCHEME

As we mention previous the scheme in [8] can be improved by using key agreement protocol based on lattice that used in [9] in the aim of provide high security against different type of attack as well as this protocol be lightweight so it can be used in medical and IOT application according to simple linear algebra used in Lattice. So, this ensure solving the problem of Key Agreement in application of block chain system.

The key agreement process between miner node and block chain client can be designed based on lattice problem as bellow:

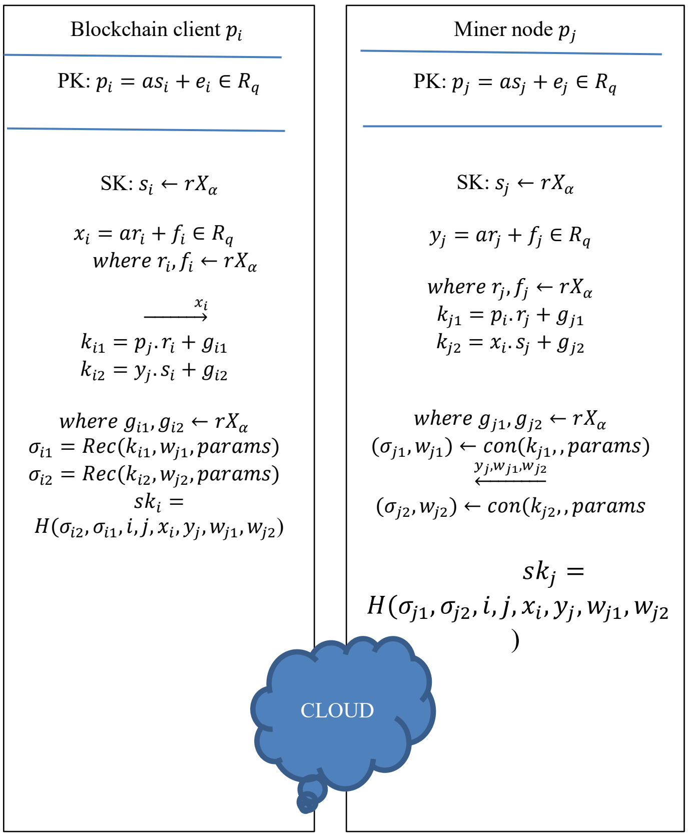
Blockchain client p_i
PK: $p_i = as_i + e_i \in R_q$
SK: $s_i \leftarrow rX_\alpha$
$x_i = ar_i + f_i \in R_q$
$where\ r_i, f_i \leftarrow rX_\alpha$
$\xrightarrow{x_i}$
$k_{i1} = p_j.r_i + g_{i1}$
$k_{i2} = y_j.s_i + g_{i2}$
$where\ g_{i1}, g_{i2} \leftarrow rX_\alpha$
$\sigma_{i1} = Rec(k_{i1}, w_{j1}, params)$
$\sigma_{i2} = Rec(k_{i2}, w_{j2}, params)$
$sk_i = H(\sigma_{i2}, \sigma_{i1}, i, j, x_i, y_j, w_{j1}, w_{j2})$
Miner node p_j
PK: $p_j = as_j + e_j \in R_q$
SK: $s_j \leftarrow rX_\alpha$
$y_j = ar_j + f_j \in R_q$
$where\ r_j, f_j \leftarrow rX_\alpha$
$k_{j1} = p_i.r_j + g_{j1}$
$k_{j2} = x_i.s_j + g_{j2}$
$where\ g_{j1}, g_{j2} \leftarrow rX_\alpha$
$(\sigma_{j1}, w_{j1}) \leftarrow con(k_{j1},, params)$
$\xleftarrow{y_j, w_{j1}, w_{j2}}$
$(\sigma_{j2}, w_{j2}) \leftarrow con(k_{j2},, params$
$sk_j = H(\sigma_{j1}, \sigma_{j2}, i, j, x_i, y_j, w_{j1}, w_{j2}$
$)$
CLOUD

Fig. 1. key agreement process between blockchain client and miner node

Now both block chain client and miner node have its secret session key

$$sk_j = H(\sigma_{j1}, \sigma_{j2}, i, j, x_i, y_i, w_{j1}, w_{j2})$$

And

$$sk_i = H(\sigma_{i2}, \sigma_{i1}, i, j, x_i, y_i, w_{j1}, w_{j2})$$ respectively.

Bellow Table III describes the parameter in above protocol.

TABLE III
NOTATION DESCRIPTION OF PROPOSED AKE PROTOCOL.

parameter	definition
$\boldsymbol{R_q = Z_q[x]/(x^n)}$	*ring where n* is power of 2
$\boldsymbol{H: \{0,1\}^* \rightarrow \{1,0\}^k}$	Hash function to derive session key *where k is length of session key* Random oracle model simulates hash function
$\boldsymbol{X_\alpha}$	Discrete Gaussian distribution *where* $\alpha \epsilon R^+$
$\boldsymbol{\alpha \epsilon R_q}$	Public parameter is selected from R_q *uniformly*
Blockchain client $\boldsymbol{p_i}$	Initiator party
Miner node $\boldsymbol{p_j}$	Responder party
$\boldsymbol{s_i \leftarrow rX_\alpha}$	Static secret key of blockchain party
$\boldsymbol{p_i = as_i + e_i \in R_q}$	Public key of blockchain party *where* $e_i \leftarrow rX_\alpha$
$\boldsymbol{s_j \leftarrow rX_\alpha}$	Static secret key of miner node party
$\boldsymbol{p_j = as_j + e_j \in R_q}$	Public key of miner node party *where* $e_j \leftarrow rX_\alpha$

V. EVALUATION AND SECURITY ANALYSIS

In this work the most important performance and security measures used is the computational time and privacy protection against different type of attack especial impersonation and man in middle attack. The most important feature that found in [9] which we use to be added to framework in [8] is that the session key is generated random uniformly and it was independently from the massages that exchanged through the session this feature increases the robust against adversary. Table (IV) illustrates the comparison between three protocols.

TABLE IV
THE PERFORMANCE AND SECURITY ATTRIBUTES AS COMPARISON STUDY BETWEEN THREE PROTOCOLS.

Protocol	withstand against attack	session key security	Computation cost with k bit security	PFS	signature	Time complexity
[8]	Impersonation attack	Private key randomly and public key is point of Elliptic curve	$O(K^3)$	yes	explicit	Depend of the ECDM
[9]	Quantum resist-attack	Based on algorithm which is probabilistic polynomial time and uniformly random	$O(K^2)$	yes	implicit	Faster and based on lightweight simple operation
Proposed	Impersonation, MIM attack, Quantum resist-attack	Based on algorithm which is probabilistic polynomial time and uniformly random	$O(K^2)$	yes	both	Faster and based on lightweight simple operation

CONCLUSION

This paper presents the security analysis of most recent literature of proposed key agreement protocol in different protocol and comparative study for their security properties.

There are essential considerations should be taken at account when design robust and good protocol:

1. Requirements of applications for instance: there are time-sensitive application (medical, health and real time application), high privacy and top-secret information (military of country) application with computation limitation application, and application that resistance against different type of attack.
2. Attacks capability and their adversarial goal. what the attack can know?
3. Mathematical formula of the algorithm that generate key session should be hard enough to achieve all security properties. at the same time the protocol should base on simple operation to overcome time and cost of computation and connection complexity.

The framework of literature [8] is improved by using lattice based key agreement that proposed in [9] instead of elliptic curve Diffie Hellman (ECDH) which used in the step of key agreement layer of the framework in [8] to generate secret session key between block chain client and miner node.

The resultant new framework is more security and robust against different kind of attack due to using of kea based on ring learning with error so all the advantage of proposed protocol in [9] add to the framework in [8] as well as the weakness of latency in [8] where the computation time depend on (ECDH) is overcame in the new resultant protocol.

ACKNOWLEDGEMENTS

This study was completely supported by the authors and Faculty of Computer Science and Mathematics, University of Kufa. The authors would like to thanks the Faculty of Computer Science and Mathematics, University of Kufa for the support.

REFERENCES

[1] A. Abdelhaliem, “Anovel provably secure key agreement protocol based on binary matrices.” 2020.

[2] A. Rawat and M. Deshmukh, “Tree and elliptic curve based efficient and secure group key agreement protocol,” J. Inf. Secur. Appl., vol. 55, 2020, https://doi.org/10.1016/j.jisa.2020.102599

[3] M. Qi and J. Chen, “An efficient on-way authintication key exchange protocol for anonymity network,” IEEE, vol. 1937–9234, 2020. https://doi.org/10.1109/JSYST.2020.2986506

[4] Y. venkatramn. Raddy, “Fixing the generalized integrated diffie-hellman -DSA key exchange protocol,” Ann. R.S.C.B, vol. 25, no. 3, 2021.

[5] G. Mogos and Y. Wang, “Diffie-hellman protocol on raspberry pi,” ECS, no. 1813, 2021. https://doi.org/10.1088/1742-6596/1813/1/012047

[6] S. Padhye and S. Singh, “MaTRU-KE: A key exchange protocol based on MaTRU CRYOTOSYSTEM,” *WILEY*, vol. 18, 2018. https://doi.org/10.1002/dac.3886

[7] D. Mishra and S. Rana, “Lattice-based key agreement protocol under ring-LWE problem for IoT-enabled smart devices,” *Springer*, 2021.

[8] N. Owoh and M. Singh, “Applying Diffie-Hellman algorithim to sole the key agreement prolem in mobile blockchain-based sensing application,” *IJACSA*, vol. 10, no. 3, 2019. https://doi.org/10.14569/IJACSA.2019.0100308

[9] H. Hn and Z. Wang, “Efficient KEA-style lattice-based authentication key exchange,” 2018. https://doi.org/10.1007/978-981-13-3095-7_8

[10] M. Kumar and S. Chand, “A lightweight cloud-Assisted-Based Annonymous authintication and key agreement protocol for secure wireless body area network,” *IEEE*, no. 1937–9234, 2020.

[11] G. Song, Y. Ju, H. Soyama, T. Ohashi, and M. Sato, “Aprovably secure and efficient anonymous mutual authintication and key agreement protocol for wearalbe devices in WBAN,” *Pro Pro*, vol. 090, no. 1, pp. 1–10, 2020. https://doi.org/10.1016/j.comcom.2020.06.010

[12] K. Kaue, S. Garg, and G. Kaddom, “Secure Authintication and key Agreement protocol for tactile internet-based Tele-Surgery Ecosystem,” *IEEE*, no. 152059, 2020. https://doi.org/10.1109/ICC40277.2020.9148835

[13] S. Olesen Maikol and A. Shagid Khan, “A novel authintication and key agreement scheme for countering MITI and Implement attack in medical facilities,” *Int. J. Integr. engineeing*, vol. 13, no. 2, 2021.

[14] M. Moghadam, M. Nikooghhadam, M. Baqer, M. Alishahi, L. Mortazavi, and A. Mohajerzadel, “An efficient authintication and key agreement scheme based on ECDH for wireless sensor network,” *IEEE*, 2020. https://doi.org/10.1109/ACCESS.2020.2987764

[15] V. Naresh, M. Nasralla, and S. Reddi, “Quantumm diffie-hellman extended dynamic Quantumm Group key agreement for e-Healthcare multi-agent system in smart cities,” *MDPI*, vol. 20, no. 3940, 2020. https://doi.org/10.3390/s20143940

[16] N. Owoh and M. Singh, “Applying diffe-hellman algorthim to solve key agreement problem in mobile blockckchain-based sensing applicationpius,” *IJACSA*, vol. 10, no. 3, 2019. https://doi.org/10.14569/IJACSA.2019.0100308

[17] Z. Xu, W. Liang, K. ching li, J. Xu, and H. Jin, “A Blockchain -based roadside unit-assisted authintication and key gremeent protocol for internet of vehicle,” *pre-proof*, 2020.

[18] D. sagar gupta and S. . Islam, “A provably secure and ligtwigh identity-based tow-party authentication key agreement protocol for IIOT environment,” *IEEE*, vol. 01:09:13, 2020. https://doi.org/10.1109/JSYST.2020.3004551